NethSecurity

Nethesis Srl and the NethSecurity project contributors

13 giu 2026

Informazioni

Collegamenti esterni

- Sito ufficiale
- Manuale sviluppatori
- Aiuto su Community

CAPITOLO 1

Introduzione

1.1 Informazioni su NethSecurity

NethSecurity è una soluzione di Unified Threat Management (UTM) che offre una suite completa di funzionalità di sicurezza, tra cui firewall, filtraggio dei contenuti, ispezione approfondita dei pacchetti (DPI) tramite Netifyd, hotspot, VPN e un controller remoto opzionale. È progettato per essere facile da installare e configurare, rendendola una scelta adatta sia per piccole e medie imprese (PMI) che per organizzazioni di livello enterprise.

NethSecurity è basato su OpenWrt, una popolare distribuzione Linux per dispositivi embedded. Questo offre numerosi vantaggi, tra cui:

- flessibilità: può essere installato su un'ampia gamma di hardware
- personalizzazione: può essere personalizzato per soddisfare le esigenze specifiche di ciascuna organizzazione
- supporto della community: beneficia della grande e attiva community NethServer

NethSecurity include una varietà di funzionalità di sicurezza, tra cui:

- Firewall: il firewall di NethSecurity offre la stateful inspection dei pacchetti e il filtraggio per proteggere le reti da accessi non autorizzati
- Filtraggio dei contenuti DNS: la funzionalità di filtraggio dei contenuti di NethSecurity blocca l'accesso degli utenti a siti web inappropriati o dannosi
- Deep Packet Inspection (DPI): NethSecurity utilizza Netifyd per eseguire la DPI, che consente di ispezionare il contenuto dei pacchetti e identificare il traffico dannoso o indesiderato.
- Icaro hotspot: Icaro hotspot è una soluzione di captive portal che può essere utilizzata per gestire e autenticare gli utenti sulle reti wireless.
- VPN: OpenVPN, IPSec e Wireguard sono protocolli VPN open-source popolari che possono essere utilizzati per creare tunnel sicuri tra reti.
- Controller remoto: NethSecurity offre una funzionalità di controller remoto, che consente agli amministratori di gestire centralmente più installazioni di NethSecurity da un'unica interfaccia.

- Informativa sulla privacy: per soddisfare i requisiti di privacy, utilizzare questo *comando* per abilitare un collegamento all'Informativa sulla privacy nella pagina principale.

Oltre a queste funzionalità di sicurezza, NethSecurity include anche una serie di altre funzionalità, come:

- qualità del servizio (QoS): la funzionalità QoS di NethSecurity consente agli amministratori di dare priorità al traffico e garantire che le applicazioni critiche dispongano sempre della larghezza di banda necessaria.
- Supporto IPv6: NethSecurity supporta IPv6, il protocollo Internet di nuova generazione

1.2 Ottenere supporto

Vuoi saperne di più o cerchi aiuto? Dai un'occhiata alla nostra fantastica community!

Se si desiderano ulteriori dettagli tecnici, consultare il manuale per sviluppatori.

I bug possono essere discussi e segnalati all'interno del forum della community. Un sistema pubblico di tracciamento delle segnalazioni è disponibile su GitHub.

CAPITOLO 2

Note di rilascio

NethSecurity changelog delle release.

- Elenco dei bug noti
- Discussioni su possibili bug

2.1 Modifiche principali del 25-03-2026

Versione dell'immagine: *8.7.2* (basata su OpenWrt 24.10.5)

Avvertimento: Se si sta ripristinando un backup dalla versione 8-24.10.0-ns.1.6.0 o precedente, consultare la sezione *Ripristinare il backup da versioni precedenti* alla fine di questa sezione.

Nuove funzionalità

- Monitoraggio in tempo reale dei flussi di rete: visualizzare i flussi attivi con metriche dettagliate (origine, destinazione, protocollo, applicazione, banda) tramite l'integrazione del motore netifyd rifattorizzato.
- Miglioramenti alla scansione di rete: aggiunte funzionalità di ordinamento e filtraggio per i risultati della scansione di rete, analogamente a quanto avviene per i lease statici e dinamici.
- Configurazione MTU peer WireGuard: consentire la modifica dell'MTU per i peer WireGuard per ottimizzare le connessioni su reti con vincoli specifici.

Miglioramenti

- Aggiornato nginx alla versione upstream per migliorare la postura di sicurezza e ridurre i falsi positivi nelle rilevazioni di vulnerabilità.
- Threat Shield DNS: è stato rimosso l'indicatore di affidabilità dalle blocklist basate sulla community per ridurre la confusione; l'indicatore di affidabilità ora viene visualizzato solo per le liste Yoroi enterprise.
- Scan Network: visibilità migliorata delle prenotazioni IP e risoluzione dei nomi host corretta per tutti i dispositivi scansionati.

Correzioni di bug

- Reverse Proxy: comportamento incoerente del certificato predefinito corretto; ora il certificato predefinito viene applicato correttamente sia all'interfaccia di amministrazione che ai servizi di reverse proxy.
- WireGuard: risolto il problema delle risposte DNS che non raggiungevano i client a causa di un formato di indirizzo errato (notazione CIDR mancante).
- WireGuard: rimossi gli elementi vuoti duplicati nella configurazione della lista allowed_ips.
- WireGuard: risolto il problema per cui la zona WireGuard era erroneamente disponibile per altri tipi di interfaccia.
- Port Forwarding: corretta la validazione dell'interfaccia utente per la selezione del protocollo «ALL»; ora i campi delle porte vengono disabilitati correttamente e viene impedita la combinazione con altri protocolli.
- Snort/IPS: risolto il problema di configurazione sui sistemi con più di 16 core CPU logici; ora il numero di thread e di code viene correttamente limitato a un massimo di 16.
- Flashstart: gli IP bypassati fissi venivano ancora reindirizzati alla regola DNS catch-all; ora i bypass eludono correttamente il filtraggio catch-all.
- Flashstart: modificato dal riavvio forzato del firewall a un ricaricamento graduale durante l'aggiornamento della configurazione ProPlus, evitando interruzioni di connessione durante gli aggiornamenti.
- OpenVPN Roadwarrior: aggiunta la funzionalità di rinnovo dei certificati e la visibilità della data di scadenza (certificati CA e server); vengono visualizzati avvisi per i certificati che scadono entro un mese.
- MultiWAN: corretta la modifica delle regole per mantenere le opzioni di origine e destinazione precedentemente configurate invece di ripristinare i valori predefiniti.
- QoS: valori invertiti corretti di banda upload/download per le interfacce non-WAN (LAN).
- Bonding di rete: aggiunte impostazioni predefinite di monitoraggio del collegamento (monitoraggio MII ogni 100 ms) per garantire che la modalità active-backup commuti correttamente sull'interfaccia di backup.
- Migrazione: corretto il problema delle regole del firewall erroneamente etichettate come «automated» dopo la migrazione; ora le regole sono correttamente modificabili.
- Interfacce di rete: risolto un problema di corrispondenza regex delle VLAN dopo la migrazione, in cui le VLAN sui bridge (ad esempio, br111.112) venivano interpretate erroneamente come bridge.
- DPI: configurazione del limite di logging fissato; sintassi corretta di rate per nftables hardcoded per prevenire errori di ricaricamento del firewall.
- PPPoE: risolti i crash di pppd con SIGILL durante la negoziazione LCP su specifici ISP; disabilitato FORTIFY_SOURCE per risolvere problemi con memcpy.
- Gateway predefinito WireGuard: risolto il problema della mancanza del gateway predefinito dopo la disconnessione del tunnel su sistemi con una sola WAN; assegnata la metrica predefinita corretta per le interfacce WAN.

- Configurazione di WireGuard: risolti i fallimenti silenziosi quando l'indirizzo IP pubblico non può essere risolto; ora gestisce correttamente i fallimenti nella risoluzione DNS senza bloccare l'installazione.

2.1.1 Ripristinare il backup da versioni precedenti

Quando si ripristina un backup dalla versione 8-24.10.0-ns.1.6.0 o precedente, l'interfaccia utente e il reverse proxy potrebbero non essere disponibili perché nginx non riesce ad avviarsi. In questo caso, è possibile verificare eventuali problemi eseguendo:

```
/usr/sbin/nginx -c /etc/nginx/uci.conf -T
```

Potrebbe essere visualizzato un errore di configurazione di nginx:

```
"module \"ngx_http_ubus_module\" is already loaded"
```

Questo accade perché il vecchio backup contiene il file `/etc/nginx/module.d/luci.module`, che è in conflitto con la nuova versione upstream di nginx. Per risolvere, eseguire:

```
rm -f /etc/nginx/module.d/luci.module && /etc/init.d/nginx restart
```

2.2 Modifiche principali del 30-10-2025

Versione dell'immagine: `8.7.1` (basata su OpenWrt 24.10.3)

Correzioni di bug

- Risolto il problema per cui dnsmasq poteva essere arrestato da keepalived anche quando non era in modalità HA.

2.3 Modifiche principali del 29-10-2025

Versione dell'immagine: *8.7.0* (basata su OpenWrt 24.10.3)

Nuove funzionalità

- L'Alta Disponibilità è ora pronta per l'ambiente di produzione dopo approfonditi test e una riprogettazione; il design è cambiato rispetto alla versione beta e richiede una riconfigurazione.
- Nuova interfaccia utente per tunnel WireGuard per la creazione e la gestione di VPN direttamente dall'interfaccia, con supporto per più server e condivisione tramite file o codice QR. I tunnel WireGuard esistenti creati da riga di comando vengono migrati automaticamente alla nuova interfaccia utente.
- Gestione migliorata della protezione contro DDoS e flood; configurazione centralizzata sotto Threat Shield IP.
- Aggiunta una allowlist di URL locali a Threat Shield DNS per un controllo più granulare.
- Introdotti template di configurazione automatica per le zone GUEST e DMZ.
- Aggiunta l'opzione per scaricare i backup non crittografati localmente utilizzando un pulsante dedicato.
- I server DNS configurati manualmente ora hanno sempre la precedenza su quelli forniti dall'ISP tramite DHCP o PPPoE.

- Comportamento DHCP migliorato con FlashStart: non è necessario definire il DNS nelle opzioni DHCP quando FlashStart è attivo.
- Le regole di port forwarding generate dal sistema sono ora visibili ma di sola lettura, chiaramente contrassegnate come automatiche.
- Threat Shield IP inserisce automaticamente nella whitelist gli IP dei servizi enterprise di Nethesis per prevenire falsi positivi.
- Aggiunto il supporto per i gruppi DH 19, 20 e 21 di IPSec.
- Aggiunto il controllo degli accessi per i gruppi di unità, restrizioni basate su IP, ottimizzazioni delle prestazioni e miglioramenti dell'interfaccia utente nel controller.
- I dati e i log del controller sono ora trasmessi attraverso il tunnel VPN per una maggiore sicurezza.
- Aggiunto campo descrizione dell'unità sincronizzato tra le unità e il controller.
- Aggiunta la configurazione MTU per risolvere problemi di connettività su reti di bassa qualità.
- Introdotto l'accesso di supporto remoto (nethsupport) tramite codice temporaneo; non sono richieste credenziali o 2FA, con revoca automatica al termine della sessione.

Correzioni di bug

- Corretto l'abilitazione/disabilitazione delle regole di port forwarding tramite il menu kebab quando sono configurati oggetti di tipo domain set.
- Migliorata la validazione dell'inoltro delle porte per rifiutare IP non validi quando è definita una porta di destinazione.
- Risolto il problema per cui i tunnel OpenVPN con compressione LZO non riuscivano ad avviarsi.
- Le configurazioni QoS e MultiWAN ora si aggiornano correttamente quando un'interfaccia WAN viene rimossa.
- Le regole DPI ora bloccano correttamente il traffico ICMP; risolto il segfault all'avvio e migliorate le prestazioni sotto carico.
- Funzionalità del menu kebab corretta nell'inoltro delle porte quando vengono utilizzati i domain set nella sezione "limita accesso a".
- Gli indicatori di utilizzo del certificato del reverse proxy ora mostrano lo stato corretto.
- Corretto un problema nel controller in cui l'autenticazione a due fattori (2FA) poteva attivarsi dopo l'annullamento della configurazione; ora si attiva solo dopo una conferma OTP riuscita.
- Il server DHCP ora risponde con un singolo messaggio per richiesta quando sono configurate più istanze di dnsmasq.

2.4 Modifiche principali del 30-06-2025

Versione dell'immagine: `8-24.10.0-ns.1.6.0`

Nuove funzionalità

- Alta disponibilità: aggiunto il supporto per cluster a due nodi in modalità backup. Failover automatico in pochi secondi. Configurazione tramite riga di comando.
- Flashstarto ProPLus: aggiunto il supporto per configurazioni multi-profilo, blocklist dinamiche e una gestione migliorata del client DNS.
- Procedura guidata di sicurezza: assiste nella configurazione iniziale della sicurezza (password, ssh e interfaccia utente). Appare dopo l'accesso se non è ancora stata completata e può essere saltata.
- Archiviazione persistente automatica per i log: lo spazio libero su disco viene assegnato automaticamente ai log per impostazione predefinita, prevenendo la perdita dei log durante il riavvio. Gli amministratori possono modificare la destinazione.
- Threat Shield: gestione degli IP bloccati dall'interfaccia utente: aggiunta un'interfaccia per visualizzare, cercare e sbloccare gli IP. Le blocklist IPv4 e IPv6 sono gestibili dall'interfaccia utente.
- Stato di sincronizzazione del service center: la pagina dell'abbonamento ora mostra lo stato della connessione, l'ora dell'ultima sincronizzazione e un pulsante `Sincronizza ora`.
- SNAT limitato per interfaccia: consente regole SNAT su specifiche interfacce di rete. semplifica configurazioni avanzate di routing e failover. gestibile tramite interfaccia utente.
- Filtraggio dei lease statici: aggiunto un filtro per i lease statici DHCP per interfaccia, per una gestione più semplice di configurazioni complesse.
- Versione nei log di migrazione: i log di migrazione e le esportazioni ora includono le versioni dello strumento di migrazione e del sistema di destinazione.

Correzioni di bug

- OpenVPN: risolto il problema per cui utenti AD rinominati/eliminati potevano ancora accedere con le vecchie credenziali. Il tracciamento degli accessi ora si aggiorna correttamente.
- Firewall: impediti i nomi delle zone del firewall che iniziano con numeri: evita problemi nell'applicazione delle regole.
- Port forward: consente l'inoltro delle porte senza specificare un indirizzo di destinazione.
- Certificati: è possibile eliminare le richieste Let's Encrypt anche se ancora in sospeso.
- OpenVPN: i tunnel net-to-net OpenVPN con trattini nel nome possono ora essere modificati dopo la migrazione.
- Log: risolto un problema per cui i log potevano occupare il filesystem root dopo un ripristino.
- OpenVPN RW: regolata la rinegoziazione per prevenire disconnessioni inaspettate con determinati metodi di autenticazione.

2.5 Modifiche principali del 10-04-2025

Versione dell'immagine: `8-24.10.0-ns.1.5.1`

Correzioni di bug

- Bond: risolto il problema per cui le interfacce bond non caricavano correttamente il modulo kernel appropriato
- Traffico in tempo reale: valori del traffico regolati per essere più accurati tra le varie tabelle
- Threat Shield DNS/IP: risolto un problema grafico in cui sembrava che fossero state abilitate più liste rispetto a quelle effettivamente attive
- Monitoraggio: rimossa la visualizzazione dell'IP WAN se l'interfaccia è offline
- UI: velocizzata del doppio l'interfaccia utente comprimendo i dati inviati al browser

---

2.6 Modifiche principali del 08-04-2025

Versione dell'immagine: `8-24.10.0-ns.1.5.0`

Questa versione risolve un bug individuato nella versione precedente a causa del rafforzamento del backend API.

Non sono state apportate ulteriori modifiche rispetto alla versione 1.5.0-rc1 in questo rilascio.

2.7 Modifiche principali del 28-03-2025

Versione dell'immagine: `8-24.10.0-ns.1.5.0-rc1`

Questa versione include nuove interfacce utente per servizi precedentemente accessibili solo tramite riga di comando, oltre a miglioramenti della sicurezza e correzioni di bug.

Nuove funzionalità e miglioramenti

- IPS: L'interfaccia utente è stata rilasciata
- Threat Shield DNS: l'interfaccia utente è stata rilasciata
- IP/MAC Binding: l'interfaccia utente è stata rilasciata
- Netify Informatics: L'interfaccia utente è stata rilasciata per la registrazione dei servizi
- FlashStart DNS: Miglioramenti all'implementazione. La gestione DNS di NethSecurity è ora indipendente dal DNS utilizzato per FlashStart, evitando qualsiasi interazione con i servizi del firewall. I server DNS esterni non sono più necessari per le reti non filtrate.
- Sono state apportate varie modifiche per rafforzare il sistema, tra cui: rafforzamento delle API, il servizio SNMP è ora disabilitato per impostazione predefinita, modifiche alla gestione dei backup (solo per abbonamento)

Correzioni di bug (questa è una lista limitata delle segnalazioni più frequenti)

- Migrazione: Problema con il nome del dispositivo OpenVPN quando supera i 16 caratteri
- Migrazione: Perdita della configurazione per tunnel OpenVPN con nomi simili
- Migrazione: Interruzione della migrazione del client Road Warrior se manca un certificato utente
- MultiWAN non consente al firewall di inviare traffico all'esterno se la rotta con la metrica più bassa non è disponibile
- L'esportazione JSON del tunnel OpenVPN include solo il primo endpoint remoto, omettendo gli altri
- L'abilitazione della registrazione nei firewall rules può sovraccaricare la CPU
- Le regole Netmap non vengono caricate dopo un aggiornamento di versione
- L'interfaccia web del server OpenVPN va in crash se il database utenti viene rimosso
- Firewall: la zona "any" viene visualizzata come inattiva
- Port forwarding: errore durante l'assegnazione di un oggetto con un intervallo di IP

2.8 Modifiche principali del 18-12-2024

Versione dell'immagine: `8-23.05.6-ns.1.4.1`

Questa versione si concentra su un monitoraggio locale migliorato e aggiunge alcune funzionalità sperimentali.

Nuove funzionalità e miglioramenti

- La funzionalità di monitoraggio in tempo reale ora consente di filtrare i dati del traffico selezionando un host e una delle seguenti opzioni: applicazione, host remoto o protocollo
- Monitoraggio in tempo reale: aggiunti grafici di latenza e tasso di perdita
- Miglioramento della configurazione di rete di Netifyd: la configurazione è stata aggiornata per migliorare le prestazioni di rete limitando il numero di interfacce che vengono ispezionate.
- Garantire un comportamento coerente nella registrazione dell'hostname nei log di nginx: in precedenza, i log di nginx includevano l'hostname due volte, causando incoerenza all'interno di Grafana.
- MultiWAN: aggiungere regole di routing per il traffico iniziato dal router
- La configurazione di FlashStart viene ora automaticamente disabilitata se non è presente un abbonamento attivo.
- Phonehome: raccoglie statistiche sull'utilizzo di threat shield DNS

Funzionalità sperimentali

Le seguenti funzionalità sono sperimentali e devono essere configurate dalla CLI:

- Associazione MAC: introdotta l'associazione MAC tramite prenotazione DHCP per migliorare la sicurezza della rete associando indirizzi MAC specifici a indirizzi IP designati
- Supporto NUT: configurare dispositivi UPS con NUT. Questa funzionalità non è ufficialmente supportata su macchine con una sottoscrizione
- Configurazione di WireGuard: configurare WireGuard tramite la CLI, consentendo la gestione di più istanze server e peer
- Intrusion Prevention System (IPS): introdotta la configurazione di Snort tramite CLI, consentendo la gestione di regole e politiche

Correzioni di bug

- Regole del firewall: riferimento a ipset non rimosso durante la modifica della regola di input
- Port forwarding: riferimento a ipset non rimosso durante la modifica della regola di input
- Oggetti firewall: le modifiche al set di host non sono riflesse nelle regole nft
- OpenVPN Road Warrior: correggere il problema di routing con l'indirizzo di gestione del bond
- Archiviazione: il disco non è stato visualizzato nell'interfaccia utente dopo l'aggiornamento del sistema
- Flashstart: risolto un problema che impediva l'invio del heartbeat
- Migrazione: gli account VPN non sono visibili se il nome utente contiene lettere maiuscole
- Dashboard: messaggio di errore non corretto nonostante la risposta API sia avvenuta con successo
- Monitoraggio: errore quando OpenVPN RoadWarrior ha una configurazione incompleta
- Migrazione: l'importazione dell'alias PPPoE non riesce con errore di argomento non valido

2.9 Modifiche principali del 17-10-2024

Versione dell'immagine: `8-23.05.5-ns.1.3.0`

Questa versione si concentra sul monitoraggio, sui miglioramenti della migrazione e su una migliore integrazione con NethSecurity Controller.

Il changelog dettagliato è disponibile qui

Nuove funzionalità e miglioramenti

- Aggiornamento a OpenWrt 23.05.5: vedere il changelog upstream
- Gestione centralizzata degli aggiornamenti delle unità: dal controller dovrebbe essere possibile aggiornare l'unità senza interruzioni (pacchetti e/o immagine)
- Pagina di monitoraggio in tempo reale: creare una dashboard completa per il monitoraggio di NethSecurity
- Monitoraggio storico: il monitoraggio storico consente di visualizzare il comportamento del firewall dal NethSecurity Controller

- Supporto degli strumenti per macchine virtuali per KVM e VMware: rimuovere tutti gli strumenti dall'immagine e fornirli come pacchetti opzionali
- Port forwarding: supporto per tutti gli oggetti nel campo di restrizione: implementare il supporto per più tipi di oggetti nel campo «limita accesso da»
- Inventario, statistiche avanzate di utilizzo: raccogliere statistiche anonime sull'utilizzo del sistema
- Miglioramento dell'interfaccia di Threat Shield: esporre le impostazioni di logging e di protezione contro gli attacchi brute force nella pagina di Threat Shield
- Interfaccia NAT helpers: nuova pagina di configurazione dei NAT helper
- Supporto remoto (ns-don): aprire la porta netdata (19999): aggiungere l'accesso alla porta 19999 da tunDON per consentire la visualizzazione dell'interfaccia utente di netdata durante le sessioni di supporto remoto
- Regole NAT: aggiungere «0.0.0.0/0 qualsiasi indirizzo»: aggiungere l'opzione «0.0.0.0/0 qualsiasi indirizzo» tra i suggerimenti per l'indirizzo di destinazione
- Zone e policy: consente di impostare la policy di logging per ciascuna zona
- Pagina DNS e DHCP: la ricerca ora non distingue tra maiuscole e minuscole
- OpenVPN Road Warrior: aggiungere un pulsante per scaricare tutti i certificati OpenVPN associati a una specifica istanza Road Warrior
- UI: migliora l'usabilità, la navigazione, il layout e gli elementi visivi su più pagine
- Migrazione: al termine della migrazione viene creato un file di log con tutte le azioni eseguite; il log è disponibile in `/root/migration.log`
- MultiWAN: migliorare la configurazione predefinita per ripristinare l'uplink dopo che tutte le WAN hanno perso la connettività

Correzioni di bug

- Migrazione: correggere le regole del firewall che utilizzavano la zona blue
- Migrazione: configurazione di rete non migrata se l'alias non ha un gateway
- Migrazione: correzione delle regole del firewall con il servizio «any» che migrano in modo errato
- Migrazione: corregge la visualizzazione errata del flag di autenticazione con password di root
- Migrazione: rinominare le interfacce VPN che causavano un errore del firewall se il nome era troppo lungo
- Migrazione: risolve la mancanza di account_email in ACME che causava un errore nel rinnovo del certificato
- Migrazione: corregge la zona errata per le regole personalizzate di OpenVPN e IPsec
- Migrazione: corregge la zona di riflessione errata sul port forwarding per le VPN
- Migrazione: rimuovere le zone personalizzate durante la migrazione, le zone vengono convertite in reti CIDR
- Migrazione: risolto il problema per cui FlashStart non era abilitato sull'interfaccia guest/blue
- Migrazione: risolto il problema per cui il certificato OpenVPN Road Warrior non veniva esportato se il CN conteneva il carattere punto
- Migrazione: importazione corretta degli utenti OpenVPN Road Warrior senza la proprietà "status"
- OpenVPN Road Warrior: aggiunta l'impostazione di compressione client che mancava nel file .ovpn
- OpenVPN Road Warrior: correggere la gestione del pool di indirizzi IP
- OpenVPN Road Warrior: risolto il problema del CRL scaduto che causava un errore di connessione dopo 6 mesi

- Tunnel OpenVPN tra NS7 e NS8 cifratura: la connessione non riusciva nonostante mostrasse «connesso»
- Client tunnel OpenVPN: correggere la modalità visualizzata
- Client tunnel OpenVPN: modalità «bridged» errata come nuovo valore predefinito, il nuovo valore predefinito è ora «routed»
- Il client tunnel OpenVPN reimposta il cifrario su `AES-128-CBC`: impostare correttamente il cifrario senza reimpostarlo
- Client tunnel OpenVPN: impostare correttamente la modalità «tap» e «tun» durante la creazione del tunnel client
- Impossibile disabilitare l'interfaccia utente LuCI legacy dopo l'aggiornamento del sistema: correggere l'opzione di disabilitazione dell'interfaccia LuCI
- Connessione del controller (ns-plug): forza la pulizia della cache dei pacchetti e la sincronizzazione dello stato dell'unità
- Migrazione: migliorare la migrazione in-place, aggiungere un ritardo prima della scrittura dell'immagine per ridurre i problemi durante la scrittura del kernel
- Conntrack: assicurarsi che counters sia impostato: evitare errori dovuti a counters mancanti.
- Reverse proxy: impostare correttamente il certificato predefinito
- Reverse proxy: correggere la configurazione per consentire l'accesso solo dalla rete specificata
- Netdata: risolto un problema con il processo fping orfano che continuava a eseguire ping su IP rimossi
- Impossibile effettuare il logout mentre è visualizzata una notifica toast: impedire che le notifiche toast blocchino il menu account
- Server API: correggere il riavvio durante l'aggiornamento del pacchetto
- La pagina dell'interfaccia non funziona con QoS abilitato su PPPoE: migliorare il validatore nella pagina di configurazione della rete
- Impossibile duplicare un inoltro di porta: correggere la duplicazione della regola di port forwarding
- Report: disabilitare il pulsante `Apri report` quando l'interfaccia utente è visualizzata dal controller
- Report DPI: risolto arresto anomalo al riavvio di netifyd

2.10 Modifiche principali del 08-08-2024

Versione dell'immagine: `8-23.05.4-ns.1.2.0`

Questa versione si concentra su nuove funzionalità per gli abbonamenti e su un'esperienza utente migliorata.

Il changelog dettagliato è disponibile qui

Nuove funzionalità e miglioramenti

- Aggiornamento a OpenWrt 23.05.4: aggiornare OpenWrt alla versione 23.05.4 con le relative modifiche ai pacchetti e al core
- Liste Threat Shield gratuite per la community: implementare liste Threat Shield gratuite per gli utenti della community, migliorando la protezione complessiva dalle minacce
- Backup remoto per tutte le sottoscrizioni: estendere l'accesso al backup remoto sia alle sottoscrizioni Enterprise che Community con informazioni aggiuntive sul backup

- Nuovo script per aggiornare i pacchetti con logging e accesso al canale stabile: implementare un nuovo script update-packages con logging avanzato e flag force-stable
- Oggetti firewall: implementare oggetti di tipo host set e domain set per una gestione avanzata del firewall
- Aggiunta del supporto agli oggetti nelle regole MultiWAN: implementare il supporto agli oggetti nell'interfaccia utente MultiWAN per gli indirizzi di origine e destinazione
- Aggiunta del supporto agli oggetti nelle regole di Port Forward: aggiunta del supporto agli oggetti per l'indirizzo di destinazione e per l'accesso ristretto nelle regole di Port Forward
- Aggiunta del supporto agli oggetti nelle regole del Firewall: includere il supporto agli oggetti per gli indirizzi di origine e destinazione nelle regole del Firewall
- Prenotazione IP per OpenVPN Road Warrior: migliorare la gestione degli IP riservati nella configurazione di OpenVPN per prevenire conflitti
- Backup: includere l'elenco dei pacchetti installati nel backup per facilitare il ripristino dopo l'aggiornamento dell'immagine
- Certificato Let's Encrypt su porta extra dell'interfaccia web: estendere l'utilizzo del certificato Let's Encrypt alla porta extra di ns-ui
- Server tunnel OpenVPN: aggiungere l'opzione «remote-cert-tls» nel file di configurazione client esportato
- DNS personalizzato per hotspot: aggiunta del supporto per la modifica del DNS predefinito per l'hotspot
- Supporto limitato per adattatori USB-Ethernet: fornire supporto sperimentale per adattatori USB-Ethernet con installazione manuale dei driver
- Supporto limitato per adattatori USB-Seriale: aggiunto supporto sperimentale per adattatori USB-Seriale con installazione manuale del driver

Correzioni di bug

- Negare la creazione di certificati con domini già richiesti: impedire la creazione di certificati duplicati con lo stesso dominio
- Problema di visualizzazione con oggetti DHCP in OpenVPN Road Warrior: correggere i campi mancanti ed errori di visualizzazione nelle opzioni DHCP
- Impossibile creare proxy inversi: correggere l'errore di validazione della configurazione di nginx durante la creazione dei proxy inversi
- Limitare i nomi delle interfacce a 13 caratteri: prevenire il fallimento di mwan a causa di nomi di interfacce troppo lunghi
- OpenVPN, impossibile rimuovere l'IP riservato per il client Road Warrior: risolto il problema per cui l'IP riservato non può essere rimosso per i client Roadwarrior
- Arresto anomalo dell'interfaccia utente con oltre 3000 voci conntrack: corretta l'interruzione dell'interfaccia utente e del servizio rpcd con un numero elevato di voci conntrack
- MultiWAN, avvisi di disconnessione/riconnessione WAN mancanti: nuova implementazione degli avvisi WAN per gestire correttamente gli eventi di connessione e riconnessione
- Controller, visualizzare il nome degli utenti disconnessi: mostrare il nome delle unità disconnesse invece solo dell'UUID
- Controller, visualizzazione porta VPN: aggiunta della visualizzazione della porta VPN nell'interfaccia utente di NS8 per una configurazione più semplice del firewall

- Controller, convalida CN: aggiungere una regola di convalida per il campo nome controller per consentire solo lettere e numeri
- Controller, non rimuovere il file .info alla disconnessione: preservare il file delle informazioni dell'unità per le unità disconnesse
- Controller, le unità alternano continuamente connesso/disconnesso: risolvere il problema della visualizzazione erratica dello stato di connessione per più unità
- Migrazione, servizi DHCP e DNS per la zona blu/guest: abilitare i servizi DHCP e DNS per le zone blu/guest migrate
- Migrazione, IP riservato OpenVPN non assegnato: problema di assegnazione dell'indirizzo IP riservato per certificati migrati
- Migrazione, nome utente FlashStart mancante: risolto il problema per cui il campo nome utente non viene visualizzato nell'interfaccia FlashStart dopo la migrazione
- FlashStart, ridurre il numero di query: modificare la configurazione di dnsdist per ottimizzare la gestione delle query e ridurre le richieste non necessarie

2.11 Modifiche principali del 2024-07-05

Versione dell'immagine: `8-23.05.3-ns.1.1.0`

Questa release si concentra sulla correzione di bug e sull'introduzione di nuove funzionalità.

Il changelog dettagliato è disponibile qui.

Nuove funzionalità e miglioramenti

- Gestione delle connessioni: implementata un'interfaccia per il monitoraggio e il controllo in tempo reale delle connessioni di rete tracciate da conntrack
- Opzione sticky MultiWAN: aggiunta la configurazione sticky nelle regole MultiWAN per mantenere la persistenza della connessione tra le sessioni
- Aggiornamenti delle firme DPI: firme aggiornate di Deep Packet Inspection abilitate per entrambi i tipi di abbonamento, community ed enterprise
- Gestione utenti amministratori: implementate funzioni API per elevare utenti locali allo stato di amministratore e revocare i privilegi di amministratore
- Miglioramento dell'autenticazione LDAP: maggiore flessibilità per Active Directory e configurazioni Distinguished Name LDAP non standard
- Autenticazione del repository delle sottoscrizioni: implementata la verifica di system_key per l'accesso ai repository di pacchetti basati su sottoscrizione

Correzioni di bug

- Utilizzo dello storage NVME: risolto un problema che impediva l'utilizzo dello spazio non allocato dell'unità NVME per la registrazione di sistema
- Validazione del ripristino del backup: aggiunti messaggi di errore specifici per l'inserimento di una passphrase errata durante il processo di ripristino del backup
- Regolazione delle metriche MWAN: allocazione modificata delle metriche dell'interfaccia per iniziare da 20 e incrementare di 10 per un miglior bilanciamento del carico
- Coerenza dell'interfaccia utente per gli aggiornamenti programmati: corretta la visualizzazione persistente degli aggiornamenti programmati completati nell'interfaccia utente
- Etichettatura delle policy MultiWAN: corretto il display errato dell'etichetta «balance» per le policy personalizzate con un solo gateway
- Validazione del modulo MultiWAN e gestione dell'input: implementata una corretta gestione dello stato dei campi di input e della validazione del modulo nell'editor delle policy
- Raffinamento UI/UX MultiWAN: maggiore flessibilità nell'inserimento delle porte e logica di invio dei moduli migliorata per regole e policy
- Funzionalità DHCP post-migrazione: risolto il problema di assegnazione degli indirizzi DHCP dopo la migrazione dalla versione 7.9 alla 8
- Effetto collaterale della creazione dell'account VPN: impedita la rimozione non intenzionale dei nomi visualizzati degli utenti durante la creazione dell'account VPN
- Configurazione della rete di migrazione: implementata la rimozione delle voci gateway superflue dalle interfacce non-red
- Logica di migrazione MultiWAN: aggiunta la disabilitazione automatica delle configurazioni MultiWAN con un solo provider durante la migrazione
- Visualizzazione configurazione IPsec: interfaccia utente corretta per riflettere accuratamente i valori dei parametri personalizzati del tunnel IPsec
- Funzionalità di reverse proxy: risolti i problemi di proxy pass per l'accesso a WebTop dopo la migrazione
- Integrità del database utenti locali: risolta la scomparsa delle voci degli utenti locali dopo gli aggiornamenti di sistema
- Robustezza del sistema di inventario: gestione migliorata dei dispositivi VLAN su interfacce bridge e recupero della configurazione DNS
- Persistenza della configurazione del controller: risolto il problema di corruzione del file di configurazione dopo il salvataggio delle impostazioni dell'interfaccia del cluster
- Flusso di lavoro per la configurazione del controller: modulo di configurazione migliorato con opzioni avanzate e indicazioni più chiare per l'utente

2.12 Modifiche principali del 2024-06-05

Questa è una release di sicurezza

Versione dell'immagine: `8-23.05.3-ns.1.0.1`

Risolta vulnerabilità di sicurezza: GHSA-74xv-ww67-jjpx (la divulgazione sarà pubblicata il 20/06/2024)

Correzioni di bug

- Correzione di sicurezza per GHSA-74xv-ww67-jjpx
- Ipsec: correzione del tunnel non funzionante se la WAN selezionata è una PPPoE su VLAN
- MultiWAN: forza la lunghezza massima per i nomi di regole e policy
- OpenVPN Road Warrior: impedire la creazione di utenti con spazi finali
- Inventario: migliorare la raccolta dei dati per abbonamenti e rete
- Migrazione: correggere la mancata visualizzazione degli utenti OpenVPN Road Warrior nell'interfaccia utente dopo la migrazione
- Server API: stabilità e prestazioni migliorate ottimizzando l'ordine di avvio per garantire un corretto avvio al momento del boot

2.13 Modifiche principali del 22-05-2024

Stabile

Versione dell'immagine: `8-23.05.3-ns.1.0.0`

La versione Stable si concentra sulla correzione dei bug e sul miglioramento dell'esperienza utente complessiva.

Il changelog dettagliato è disponibile qui.

Nuove funzionalità e miglioramenti

- Route: Le regole IPsec ora non sono modificabili
- IPsec: aggiunto un validatore per le reti remote e locali
- Ricaricamento automatico delle pagine VPN: le pagine VPN ora si ricaricano automaticamente
- DHCP: aggiunta la funzionalità di scansione della rete
- IPsec: gestione migliorata di più reti all'interno di un singolo tunnel
- DHCP: l'opzione «force» per DHCP è ora disponibile nell'interfaccia utente
- Threat shield: rimuovere l'elenco enterprise alla rimozione dell'abbonamento
- DPI: rimuovere le firme premium alla deregistrazione
- Abbonamento: migliorare la finestra modale di annullamento registrazione
- Inventario: raccogliere statistiche di utilizzo di base
- IPsec: migliorare la visibilità dell'opzione PFS
- Dashboard: aggiungere una notifica di nuova versione disponibile

- Regole del firewall: migliorare la leggibilità complessiva della pagina
- Zone e policy: cassetto migliorato per la zona WAN
- Dashboard: mostra un avviso se il DNS non è configurato
- Helper NAT: tutti gli helper NAT sono ora inclusi nell'immagine ma disabilitati per impostazione predefinita

Correzioni di bug

- FlashStart: la risoluzione DNS non funziona dopo la disattivazione del servizio
- FlashStart: correggere la prima configurazione
- Let's Encrypt: i certificati non vengono creati
- FlashStart: la regola di reindirizzamento non è efficace
- Firewall: ipset non viene aggiornato dopo la rimozione di un indirizzo
- Migrazione: i gruppi host non vengono importati correttamente nelle regole del firewall
- Regole del firewall: impossibile inserire un indirizzo IP personalizzato
- Threat shield: le modifiche alla allowlist non vengono applicate immediatamente
- Migrazione: impossibile modificare il tunnel IPsec importato
- OpenVPN road warrior: impossibile ricreare un utente precedentemente creato dal database LDAP
- OpenVPN RW: gli host non sono raggiungibili con configurazione bridge
- MultiWAN: l'IP di monitoraggio non viene aggiornato
- Reverse Proxy: la lista degli IP consentiti non dovrebbe essere obbligatoria
- Controller: impossibile connettere l'unità se l'interfaccia utente è disabilitata sulla porta 443
- Abbonamento: impossibile registrare un abbonamento community
- Installazione da USB: tabella delle partizioni non valida
- Migrazione: impossibile avviare l'interfaccia PPPoE
- Threat shield: feed di sottoscrizione vuoto
- Aggiornamenti automatici: il job cron non viene avviato durante la notte
- Scudo delle minacce non avviato dall'interfaccia utente
- Migrazione: l'IP di Threat Shield non viene migrato
- EFI: impossibile utilizzare lo spazio libero come memoria aggiuntiva
- Zona: forza la creazione in minuscolo
- OpenVPN Road Warrior: autenticazione OTP, la VPN si disconnette dopo un'ora
- ns-api: threatshield, impostare ban_nftexpiry e ban_logcount
- Helper NAT: le sessioni FTP attive non trasferiscono file

2.14 Modifiche principali del 29-04-2024

Release Candidate 2

Versione dell'immagine: `8-23.05.3-ns.0.0.5-rc2`

La versione Release Candidate 2 si concentra sulla correzione di bug e sul miglioramento dell'esperienza utente complessiva. Il changelog dettagliato è disponibile qui.

Nuove funzionalità e miglioramenti

- Regole del firewall: visualizzazione migliorata della sezione delle regole.
- FlashStart: aggiunta la funzionalità di risoluzione DNS dopo la disattivazione del servizio.
- Dashboard: organizzazione migliorata delle schede e aggiunta di collegamenti.
- Route: abilitata la creazione di route senza gateway.
- Ricaricamento automatico delle pagine VPN: implementato il ricaricamento automatico dei dati ogni 10 secondi.
- Migrazione alla libreria vue-components: componenti e utilità migrati a vue-components.
- UI: impostare il timeout di rpcd a 300 secondi per supportare attività di lunga durata.
- DHCP: introdotta la funzionalità di scansione della rete.
- Database utenti: ordinati gli utenti per nome utente e garantita l'esecuzione coerente delle query LDAP.
- DHCP: abilitata per impostazione predefinita l'opzione «force» per i server DHCP, opzione resa disponibile nell'interfaccia utente.
- OpenVPN road warrior: implementata l'ordinamento degli utenti OpenVPN road warrior per nome utente.

Correzioni di bug

- Regole del firewall: risolto un problema che mostrava contenuti errati.
- FlashStart: risolto il problema di risoluzione DNS dopo la disattivazione del servizio.
- Route: impedita la modifica delle regole IPsec.
- IPsec: convalida delle reti remote/locali per evitare duplicati.
- Port forwarding: etichetta dell'opzione di riflessione corretta.
- Migrazione: garantita la corretta importazione dei gruppi host nelle regole del firewall.
- Regole del firewall: consentita l'inserimento di indirizzi IP personalizzati.
- Threat shield: applicare immediatamente le modifiche alla allowlist.
- Migrazione: migliorare la migrazione delle opzioni IPSec e consentire la modifica del tunnel IPsec importato.
- OpenVPN road warrior: risolto il problema con la ricreazione dell'utente da LDAP.
- Corretto l'errore di axios durante il salvataggio delle modifiche.
- OpenVPN road warrior: risolto un problema con la configurazione bridge.
- IPsec: gestione migliorata di più reti con un singolo tunnel.
- Zone: corretti gli ID dei pulsanti radio fissi nella pagina Zone.
- FlashStart: corretta una regola di reindirizzamento inefficace.

- Controller: comportamento perfezionato in base alla presenza dell'abbonamento.
- Firewall: ipset aggiornato dopo la rimozione dell'indirizzo IP.

2.15 Modifiche principali del 10-04-2024

Release Candidate 1

Versione dell'immagine: `8-23.05.3-ns.0.0.3-rc1`

La versione Release Candidate 1 si concentra sulla correzione di bug, sull'aggiunta del controller centralizzato e sul miglioramento del processo di migrazione da NethServer 7.

Il sistema di tracciamento dei problemi è stato spostato su GitHub. Il nuovo URL è: https://github.com/NethServer/nethsecurity/issues.

Nuove funzionalità e miglioramenti

- NethSecurity è stato basato nuovamente su OpenWrt 23.05.3.
- Aggiunto il *controller centralizzato* per gestire più istanze di NethSecurity da un'unica interfaccia.
- Reindirizzamenti di porta: supporto per intervalli di porte nel campo della porta di origine.
- Regole firewall: supporto per intervalli IP come regole di destinazione.
- Backup: consentire il download del file di backup dall'interfaccia utente anche se la macchina dispone di un abbonamento enterprise e il server di backup remoto non è disponibile.
- Threat shield: migliorare la visualizzazione della pagina Threat shield se il firewall non ha accesso a Internet.
- Abbonamento: mostrare l'abbonamento anche se la macchina non ha accesso a Internet.
- MultiWAN: gestione migliorata della configurazione della policy di bilanciamento.
- Pagina Rete: lo stato attivo/disattivo delle interfacce di rete ora riflette accuratamente lo stato del cavo invece dello stato del kernel.
- Regole firewall: migliorare la visualizzazione delle regole firewall disabilitate.
- Aggiunta un'opzione per abilitare il link alla privacy policy durante l'accesso.
- Supporto remoto (don): consentire l'accesso all'interfaccia utente e preservare la sessione dopo un riavvio del firewall.
- Utenti: supporto per il bind su database utente LDAP remoti.

Correzioni di bug

- 2FA: abilitare l'autenticazione a due fattori per l'utente solo dopo la verifica dell'OTP.
- Tunnel IPsec: associare correttamente l'interfaccia ipsecX alla WAN selezionata.
- IPsec: assicurarsi di avviare dopo una migrazione anche se la WAN associata non è disponibile.
- Migrazione: rielaborare il processo di migrazione della rete per evitare problemi con la configurazione di bond, bridge e alias.
- Migrazione: visualizzare bond e bridge nella pagina di rimappatura durante la migrazione.

- Migrazione, aggiornamento e backup: implementare nuovi metodi di caricamento e download per evitare problemi con file di grandi dimensioni.
- Migrazione: risolto un problema che impediva l'avvio del server DHCP quando erano presenti opzioni DHCP nella configurazione.
- DPI: prevenire la perdita delle firme Enterprise dopo un aggiornamento.
- Storage: aggiunta la possibilità di ricreare una partizione di storage eliminata.
- Rete: correggere la creazione di VLAN su bridge.
- Port forward e tunnel IPsec: corretta la visualizzazione degli IP WAN, la pagina ora mostra tutti gli alias ed evita i duplicati anche se la WAN non è disponibile.
- Port forwarding: elencare la zona LAN all'interno delle destinazioni hairpin NAT.
- Tunnel OpenVPN: risolto un problema che impediva la modifica di un tunnel P2P.
- Pagina MultiWAN: ordina correttamente le interfacce WAN per priorità.
- Pagina MultiWAN: non mostrare gli alias WAN all'interno della pagina delle policy.
- DHCP: nascondere i lease statici all'interno della scheda dei lease dinamici.
- Proxy pass: risolto un problema che impediva la modifica di una regola di proxy pass.
- Tunnel OpenVPN: corretta la selezione predefinita del cifrario per i tunnel P2P.
- DPI: riavviare netifyd dopo una modifica alla configurazione di rete.
- FlashStart: corregge la registrazione del firewall al servizio FlashStart.
- FlashStart: correggere l'indirizzo DNS secondario.
- Regole del firewall: correggere la presenza di host duplicati negli indirizzi di origine e destinazione.
- OpenVPN Road Warrior: correggere la creazione in massa degli utenti per elenchi di utenti di grandi dimensioni.

Bug noti

I bond di rete presentano ancora alcune problematiche. Se si sta effettuando una migrazione da NethServer 7, si prega di tenere presente quanto segue:

- La VLAN su un'interfaccia bond non viene creata se il bond non ha un ruolo
- Durante la creazione di un bond, a volte l'interfaccia web non mostra i dispositivi da aggiungere al bond
- Il bond appena creato mostra un pulsante con l'etichetta `Configura bond`, ma in realtà non configura il bond stesso, bensì l'interfaccia membro del bond.

Note sull'aggiornamento

Se si sta eseguendo l'aggiornamento da una versione beta precedente e sono stati configurati tunnel IPsec, è necessario eseguire i seguenti comandi dopo l'aggiornamento:

```
uci delete ipsec.ns_ipsec_global.interface
uci commit ipsec
/etc/init.d/swanctl restart
```

2.16 Modifiche principali del 29-02-2024

Beta 2

Versione dell'immagine: `8-23.05.2-ns.0.0.2-beta2`

La versione Beta2 si concentra sul miglioramento della nuova interfaccia utente e sull'ottimizzazione dell'esperienza utente complessiva.

Nuove funzionalità

Nuovi pacchetti inclusi nell'immagine:

- Aggiunto il pacchetto SNMPD per il monitoraggio e la gestione della rete.
- Pacchetto Dyndns incluso per i servizi DNS dinamici.
- Supporto driver ampliato per interfacce di rete meno recenti e ambienti vmnet.

Interfaccia utente (UI):

- La porta UI predefinita è stata cambiata in 9090, accessibile dalla WAN. L'interfaccia utente è inoltre accessibile da LAN e WAN sulla porta 443.
- Interfaccia LuCI disabilitata per impostazione predefinita per un'esperienza semplificata.
- Nuova pagina per configurare le regole Source NAT, Masquerading, No-NAT e netmap.
- Migliorata la leggibilità del conteggio dei pacchetti di rete nella pagina di rete.

Rete:

- Supporto PPPoE con DHCPv6-PD implementato.
- Ora è possibile configurare le interfacce di rete bond dall'interfaccia utente.

DPI:

- Riconfigurazione automatica al cambio di rete abilitata.
- Tutte le interfacce non-WAN vengono visualizzate nella pagina DPI. Per aggiornare la configurazione DPI sulle installazioni esistenti, eseguire:

```
echo '{"changes": {"network": []}}' | /usr/libexec/rpcd/ns.commit call commit
```

Funzionalità aggiuntive:

- Migliorato lo script di installazione `ns-install`: l'installazione è ora più veloce e il sistema viene arrestato al termine del processo di installazione.
- Interfaccia utente di migrazione migliorata per un'esperienza di aggiornamento più fluida.
- Creazione di lease statici DHCP a partire da lease dinamici esistenti.
- Autenticazione a due fattori (2FA) per account amministratore.
- Esperienza di accesso riprogettata con un aspetto più integrato e orientato all'amministratore.
- Hook pre e post commit aggiunti per un controllo API migliorato.
- Funzionalità di opt-in basata su abbonamento per aggiornamenti automatici, accessibile solo agli utenti con abbonamenti attivi.

Correzioni di bug

MultiWAN:

- Flessibilità delle regole migliorata: ora è possibile specificare singoli indirizzi IP (non solo in formato CIDR) nei campi origine/destinazione delle regole.
- Protezione delle policy: impedisce l'eliminazione accidentale delle policy già utilizzate nelle regole.
- Corretto il display del grafico mwan: il grafico mwan all'interno di Netdata ora viene visualizzato correttamente dopo la configurazione multi-WAN.

Firewall:

- Gestione avanzata dei protocolli: crea regole per tutti i protocolli (non solo TCP/UDP) quando viene selezionato «qualsiasi».
- Migliorata la leggibilità delle regole: nelle regole con 2 o più indirizzi di origine/destinazione, solo il secondo indirizzo era immediatamente visibile nel suggerimento.

Inoltro delle porte:

- Configurazione semplificata: le porte di origine e destinazione sono richieste solo per i protocolli TCP/UDP.
- Selezione semplificata del protocollo ALL: quando viene scelto il protocollo «ALL», le altre opzioni di protocollo vengono disabilitate in quanto ridondanti.

Certificati:

- Problema risolto: il certificato personalizzato veniva sovrascritto da un certificato autogenerato quando impostato come certificato predefinito per il FQDN del firewall.
- Visualizzazione corretta del dominio del certificato: nell'elenco dei certificati, il soggetto visualizzato ora corrisponde al certificato client invece che al primo certificato nella catena.
- Correzione dell'eliminazione dei certificati Let's Encrypt: è stata forzata la generazione di una nuova configurazione da parte di acme.sh durante la ricreazione di un certificato Let's Encrypt per lo stesso dominio, invece di riutilizzare quella esistente.
- Richiesta certificato Let's Encrypt: disabilitato il reindirizzamento automatico dalla porta 80 alla 443 per evitare conflitti con acme.sh.

DPI:

- Perdita di configurazione corretta: risolto il problema per cui le configurazioni salvate del filtro DPI venivano eliminate durante l'aggiornamento dalle versioni precedenti

Rete:

- Gestione migliorata delle interfacce: è ora possibile modificare le interfacce anche dopo che la zona associata è stata eliminata.

API:

- Coerenza dei log: i log del server API sono stati standardizzati per il server API di NethSecurity in modo da corrispondere agli oggetti passati agli script.

OpenVPN:

- Risolto il problema di aggiornamento della porta: la modifica della porta del servizio OpenVPN Road Warrior tramite l'interfaccia utente ora si riflette correttamente nell'aggiornamento della configurazione del servizio e nella regola firewall associata.
- Protezione della configurazione: risolto il problema per cui la configurazione RoadWarrior veniva persa durante la modifica della password di un utente.

- Autenticazione avanzata: risolti i problemi di autenticazione di OpenVPN Roadwarrior utilizzando utenti locali in NethSecurity beta1.
- Stato del server tunnel risolto: risolto il problema per cui lo stato del server tunnel non veniva visualizzato correttamente nell'interfaccia utente.

Hotspot:

- Inclusione degli indirizzi MAC: risolto il problema per cui gli indirizzi MAC erano assenti nella sezione `unità` del Hotspot Manager quando l'hotspot si basava su una VLAN.
- Eliminazione VLAN: risolto un problema che impediva l'eliminazione delle VLAN precedentemente utilizzate da hotspot non registrati, anche dopo che la VLAN era stata liberata.
- Visibilità dello stato migliorata: aggiunto lo stato abilitato/disabilitato nella scheda principale per un riferimento rapido.

DHCP:

- Corretto il valore della chiave mancante per un'opzione avanzata preconfigurata, garantendo il corretto funzionamento.
- Visualizzazione migliorata di opzioni multiple tramite la rimozione dell'etichetta ridondante.

IPsec:

- Porta NAT regola IPsec: porta corretta per la regola Allow-IPsec-NAT, cambiata da 500 a 4500 (UDP)
- Regole duplicate: impedita la creazione di regole firewall duplicate durante la creazione dei tunnel
- Correggere l'ortografia dei nomi delle regole IPsec

Bug noti

IPsec:

- Solo la prima subnet nel tunnel IPSec è funzionante: quando si definiscono più di una rete in un tunnel IPSec tra dispositivi diversi, solo la prima rete funziona; il traffico destinato alle altre subnet nel tunnel non viene instradato correttamente. Una soluzione temporanea consiste nel creare più tunnel con subnet individuali. Questo problema non si verifica tra due dispositivi NethSecurity 8 (poiché utilizzano lo stesso demone), ma può verificarsi, ad esempio, tra un NethSecurity 8 e un NethServer 7.9.

2.17 Modifiche principali del 2024-02-01

Beta 1

Versione dell'immagine: `8-23.05.2-ns.0.0.1-beta1`

La release Beta1 segna la transizione verso la nuova interfaccia utente come principale interfaccia di configurazione. Luci rimane attivo per impostazione predefinita per le configurazioni non ancora disponibili nella nuova interfaccia e per scopi di verifica. I bug noti nella nuova interfaccia possono essere trovati qui.

Modifiche principali:

- Aggiunta una pagina dedicata per la gestione dei certificati e delle impostazioni del reverse proxy. Migliorato il processo di importazione per entrambe le configurazioni.
- Introdotta una nuova pagina per la configurazione delle regole del firewall. Si consiglia di utilizzare questa pagina invece di quella di Luci, poiché l'uso di entrambe potrebbe causare incompatibilità.

- Aggiunta una pagina per la configurazione della Qualità del Servizio (QoS) per migliorare la gestione del traffico di rete.
- Aggiunta una pagina per la configurazione di OpenVPN Roadwarrior. Aggiornato il processo di migrazione per la nuova implementazione.
- Introdotta l'opzione per utilizzare una partizione del disco principale come spazio di archiviazione per i log.
- Migliorato il processo di migrazione per multiwan e tunnel OpenVPN, aumentando la compatibilità complessiva del sistema.
- Ottimizzata la gestione degli upgrade e delle migrazioni, con particolare attenzione a una transizione più fluida.
- È stato implementato un nuovo sistema di versionamento per identificare in modo univoco ogni immagine, migliorando la chiarezza nel tracciamento delle release.
- Sono stati incorporati numerosi miglioramenti all'usabilità e risolti problemi nelle pagine esistenti, garantendo un'esperienza più intuitiva per l'utente.

2.18 Modifiche principali del 11-12-2023

Alpha 2

Questa versione alpha è stata specificamente realizzata per scopi di valutazione, con particolare attenzione al test delle funzionalità della nuova interfaccia utente del sistema. Viene fornita la possibilità di provare sia lo sviluppo in corso della nuova interfaccia sia di continuare a utilizzare l'interfaccia consolidata LuCI. I bug noti della nuova interfaccia possono essere trovati qui.

Miglioramenti dell'interfaccia utente

- Risolti numerosi bug su diverse pagine, inclusi DHCP e filtro DPI, migliorando la stabilità complessiva delle pagine.
- Introdotta la pagina di configurazione del tunnel OpenVPN.
- Aggiunta la pagina di configurazione del tunnel IPsec.
- Incorporata la pagina di configurazione Hotspot (Dedalo).
- Implementata la pagina di Backup e Ripristino.
- Introdotta la funzionalità di esclusione nella pagina del filtro DPI.
- Report Netdata esposti all'interno dell'interfaccia utente, con un monitor della latenza ping configurabile.
- Risolto il problema della lingua predefinita per le lingue non tradotte.
- Riorganizzata e migliorata la pagina Network.
- Aggiunta una pagina per gestire gli Aggiornamenti di Sistema.
- Inclusa una pagina di migrazione da NethServer 7.
- Abilitata la funzionalità di ripristino delle impostazioni di fabbrica direttamente dall'interfaccia utente.
- È stata implementata una pagina Utenti VPN in preparazione del prossimo server OpenVPN Road Warrior.

Miglioramenti generali

- Aggiornata la base OpenWrt alla versione 23.05.2.
- È stato stabilito un meccanismo per inviare avvisi ai portali remoti, inclusi my.nethesis.it e my.nethserver.com.
- Aggiunto il supporto per le One-Time Password (OTP) nelle future configurazioni del server OpenVPN Road Warrior.

Nota: la configurazione del bond è ancora in corso e, di conseguenza, le interfacce di rete di tipo bond attualmente non sono funzionanti in questa release.

2.19 Modifiche principali del 31-10-2023

Alpha 1

Questa è una versione alpha, progettata per scopi di valutazione al fine di esplorare le funzionalità del nuovo sistema. È possibile utilizzare la nuova interfaccia, attualmente in fase di sviluppo, oppure l'interfaccia LuCI legacy. Si prega di notare che alcune funzionalità disponibili sulla vecchia interfaccia LuCI verranno rimosse una volta completata la pagina corrispondente sulla nuova interfaccia.

Sebbene l'intera funzionalità del backend sia già operativa e accuratamente testata, la nuova interfaccia non è ancora completa. Alcuni bug della nuova interfaccia sono già noti e possono essere trovati qui.

La nuova interfaccia include le seguenti funzionalità:

- Dashboard
- Gestione degli abbonamenti
- Configurazione di hostname e fuso orario
- Configurazione dello spazio di archiviazione aggiuntivo
- Configurazione dell'interfaccia di rete
- Impostazioni DNS e DHCP
- Configurazione del Routing
- Supporto Multi-WAN
- Opzioni di Port Forwarding
- Gestione di Zone e Policy
- Filtraggio DNS Flashstart
- Filtraggio Deep Packet Inspection (DPI)
- Cambio della password dell'utente root
- Accesso ai log di sistema

2.20 Glossario delle release

Il ciclo di rilascio del software include quattro fasi: Alpha, Beta, Release Candidate (RC) e Stable.

Durante la fase **Alpha**, il software non è stato testato in modo approfondito e potrebbe non includere tutte le funzionalità pianificate. Questa versione non è adatta per ambienti di produzione. Tuttavia, può essere utilizzata per avere un'anteprima delle novità previste nella prossima versione. Si noti che gli aggiornamenti da una release Alpha ad altre release non sono supportati.

La fase **Beta** indica che il software è per lo più completo a livello di funzionalità, ma può ancora contenere numerosi bug noti e sconosciuti. Questa versione non dovrebbe essere utilizzata in ambienti di produzione. Tuttavia, può essere utilizzata per testare il software prima della distribuzione in produzione. Gli aggiornamenti da una release Beta a una release RC o Stable sono supportati, ma potrebbero richiedere una procedura manuale.

Durante la fase di **Release Candidate (RC)**, il software è completo di tutte le funzionalità e non contiene bug noti. Se non emergono problemi importanti, può essere promosso a Stable. Gli aggiornamenti da una versione RC a una

versione Stable sono supportati e dovrebbero essere quasi automatici. Tuttavia, se si è nuovi al software, è consigliabile utilizzarlo in produzione solo se si ha già una certa esperienza con esso.

La versione **Stable** è la più affidabile e sicura da utilizzare in ambienti di produzione. È stata accuratamente testata ed è considerata priva di bug importanti.

CAPITOLO 3

Requisiti di sistema

NethSecurity è attualmente disponibile solo per architettura x86-64.

Requisiti hardware minimi:

- 1 vCPU/core
- 1 GB di RAM
- 1 GB di spazio su disco
- 2 schede di rete Ethernet

Requisiti hardware consigliati:

- 2 vCPU/core
- 2 GB di RAM
- 1 GB di spazio su disco più una memoria USB aggiuntiva per dati persistenti come i log

CAPITOLO 4

Download

La tabella contiene i seguenti link per ciascuna release:

- il file immagine x86-64, utilizzato per installare NethSecurity
- il file sha256sums, che contiene i checksum SHA256 per verificare l'integrità dell'immagine scaricata
- il file SBOM (Software Bill of Materials), in formato CDX (CycloneDX), che contiene l'elenco di tutti i pacchetti software inclusi nell'immagine

Iniziare scaricando l'immagine x86_64 più recente dalla tabella sottostante.

Per la verifica, scaricare anche il file hash ed eseguire il seguente comando in una shell Linux per assicurarsi dell'integrità dell'immagine scaricata:

```
grep nethsecurity-8.7.2-x86-64-generic-squashfs-combined-efi.img.gz sha256sums |␣
↪sha256sum -c
```

Per procedere con l'installazione di NethSecurity, sono disponibili due opzioni: scrivere direttamente l'immagine scaricata sul disco oppure creare una chiavetta USB avviabile. Consultare la pagina *installazione* per istruzioni dettagliate su entrambi i metodi.

You can navigate inside the package repository using the package browser to find all availables releases and download directly images, hash files and packages.

The tables below list the available releases along with their respective download links.

Tabella 1: Versioni stabili

Versione	Immagine	Hash	SBOM
8.7.2	x86-64	SHA256	CDX
8.7.1	x86-64	SHA256	CDX
8.7.0	x86-64	SHA256	CDX
8-24.10.0-ns.1.6.0	x86-64	SHA256	CDX
8-24.10.0-ns.1.5.1	x86-64	SHA256	
8-24.10.0-ns.1.5.0	x86-64	SHA256	
8-23.05.5-ns.1.4.1	x86-64	SHA256	
8-23.05.5-ns.1.4.0	x86-64	SHA256	
8-23.05.5-ns.1.3.0	x86-64	SHA256	
8-23.05.4-ns.1.2.0	x86-64	SHA256	
8-23.05.3-ns.1.1.0	x86-64	SHA256	
8-23.05.3-ns.1.0.1	x86-64	SHA256	
8-23.05.3-ns.1.0.0	x86-64	SHA256	

Tabella 2: Versioni di sviluppo

Versione	Immagine	Hash	SBOM
8.7.2-dev+4f4d313.20260525073014	x86-64	SHA256	CDX
8.7.2-dev+f769537.20260520090549	x86-64	SHA256	CDX
8.7.2-dev+15dfcee12.20260520075017	x86-64	SHA256	CDX
8.7.2-dev+e30c549.20260519082525	x86-64	SHA256	CDX
8.7.2-dev+54e65a2.20260518065451	x86-64	SHA256	CDX
8.8.0-dev.10.20260612084629.6a5566f	x86-64	SHA256	CDX
8.8.0-dev.11.20260612084648.2308c2c	x86-64	SHA256	CDX
8.8.0-dev.5108.20260610101836.5981cbbff	x86-64	SHA256	CDX
8.8.0-dev.6.20260611142438.fc593d7	x86-64	SHA256	CDX
8.8.0-dev.9.20260612084613.d697100	x86-64	SHA256	CDX

CAPITOLO 5

Installazione

Per iniziare il processo di installazione, per prima cosa *scaricare* l'immagine più recente. Una volta completato il download, sono disponibili due metodi per installare NethSecurity:

- Installazione diretta su disco: scrivere l'immagine scaricata direttamente sul disco del computer. Questo metodo consente un processo di installazione semplice e diretto sul dispositivo di memorizzazione.
- Installazione tramite avvio da USB: in alternativa, è possibile creare una chiavetta USB avviabile utilizzando l'immagine scaricata. Avviare il sistema dalla chiavetta USB e digitare un comando per avviare il processo di installazione.

Scegliere il metodo che meglio si adatta alle proprie esigenze e procedere con il processo di installazione di NethSecurity.

5.1 Installazione su bare metal

NethSecurity può essere eseguito da una chiavetta USB o installato direttamente su qualsiasi dispositivo avviabile come dischi rigidi o schede SD.

1. collegare il disco/chiavetta/scheda di destinazione a una macchina Linux desktop
2. trovare il nome del dispositivo disco/chiavetta/scheda, in questo esempio il dispositivo è denominato `/dev/sdd`
3. come utente `root`, scrivere l'immagine scaricata sul dispositivo:

   ```
   zcat nethsecurity-8.7.2-x86-64-generic-squashfs-combined-efi.img.gz | dd of=/dev/
   ↪sdd bs=1M iflag=fullblock status=progress oflag=direct
   ```

4. scollegare il disco/chiavetta/scheda dal desktop e collegarlo al server
5. avviare il server, selezionare il dispositivo corretto (USB, scheda SD o disco rigido) dal menu di avvio
6. il server è installato ed è pronto per essere utilizzato

Scrittura dell'immagine su Windows

Nota: Scrivere l'immagine su una macchina Windows non è consigliato perché potrebbe compromettere la partizione del disco.

Se si utilizza una macchina desktop Windows, sarà necessario un software aggiuntivo per il punto 2. Prima di tutto, assicurarsi di formattare l'unità USB e poi smontarla. Utilizzare uno dei seguenti strumenti per scrivere sulla chiavetta USB:

- Etcher
- Win32 Disk Imager
- Rawrite32

5.1.1 Installare da USB su disco

Il metodo di installazione raccomandato per NethSecurity è su memoria interna, per motivi di robustezza e prestazioni. A tal fine, NethSecurity fornisce un comando specifico per installare i suoi contenuti dalla chiavetta USB sul disco interno:

1. connettersi al server utilizzando VGA, console seriale o SSH
2. accedere con *credenziali predefinite*
3. Eseguire `ns-install` e seguire le istruzioni

Il firewall verrà arrestato al termine dell'installazione. Una volta che il firewall è stato spento, è possibile rimuovere in sicurezza la chiavetta USB e riavviare nuovamente il server.

Nota: La chiavetta USB dovrebbe essere utilizzata solo per l'installazione iniziale di NethSecurity; qualsiasi altro uso è fortemente sconsigliato. Per aggiornare NethSecurity o eseguire un ripristino alle impostazioni di fabbrica, sono già disponibili opzioni documentate tramite l'interfaccia web e la console a riga di comando. Nel caso in cui si perda la password di accesso al firewall e sia necessario eseguire un ripristino alle impostazioni di fabbrica, si consiglia di avviare in modalità failsafe ed effettuare il ripristino da lì, come descritto nella documentazione (:ref:modalità failsafe <failsafe-section>).

5.2 Installazione su macchine virtuali

È possibile utilizzare l'immagine scaricata come disco per una macchina virtuale:

1. estrarre l'immagine scaricata:

   ```
   gunzip nethsecurity-8.7.2-x86-64-generic-squashfs-combined-efi.img.gz
   ```

2. creare una nuova macchina virtuale e selezionare l'immagine non compressa come disco
3. avviare la macchina virtuale

Nota: Se si desidera salvare i log localmente, è consigliato collegare un disco rigido virtuale aggiuntivo alla macchina virtuale e selezionarlo come destinazione per i log nella pagina `Storage` sotto la sezione `Sistema`.

5.2.1 Installazione su Proxmox

L'immagine può essere importata all'interno di Proxmox.

Per prima cosa, assicurarsi di avere 2 bridge di rete differenti. In questo esempio verranno utilizzati `vmbr0` e `vmbr1`. La procedura descritta può essere eseguita anche tramite l'interfaccia utente di Proxmox.

Creare la macchina virtuale, in questo esempio la macchina avrà l'id `401`:

```
qm create 401 --name "NethSecurity" --ostype l26 --cores 1 --memory 1024 --net0 virtio,
↪bridge=vmbr0,firewall=0 --net1 virtio,bridge=vmbr1,firewall=0 --scsihw virtio-scsi-pci
```

Scaricare l'immagine:

```
wget 'https://updates.nethsecurity.nethserver.org/stable/8.7.2/targets/x86/
64/nethsecurity\unhbox\voidb@x\kern\z@\char`\protect\discretionary{\char\
defaulthyphenchar}{}{}8.7.2\unhbox\voidb@x\kern\z@\char`\protect\discretionary{\char\
defaulthyphenchar}{}{}x86\unhbox\voidb@x\kern\z@\char`\protect\discretionary{\char\
defaulthyphenchar}{}{}64\unhbox\voidb@x\kern\z@\char`\protect\discretionary{\char\
defaulthyphenchar}{}{}generic\unhbox\voidb@x\kern\z@\char`\protect\discretionary{\char\
defaulthyphenchar}{}{}squashfs\unhbox\voidb@x\kern\z@\char`\protect\discretionary{\char\
defaulthyphenchar}{}{}combined\unhbox\voidb@x\kern\z@\char`\protect\discretionary{\char\
defaulthyphenchar}{}{}efi.img.gz'
```

Estrarre l'immagine:

```
gunzip nethsecurity-8.7.2-x86-64-generic-squashfs-combined-efi.img.gz
```

Importare le immagini estratte come disco della macchina virtuale:

```
qm importdisk 401 nethsecurity-8.7.2-x86-64-generic-squashfs-combined-efi.img local-lvm
```

Collegare il disco alla macchina virtuale:

```
qm set 401 --scsi0 "local-lvm:vm-401-disk-0"
```

Impostare l'ordine di avvio:

```
qm set 401 --boot order=scsi0
```

Infine, avviare la macchina virtuale.

Agente guest QEMU

L'agente guest QEMU non fa parte dell'immagine NethSecurity ma può essere installato dalla riga di comando. L'agente può funzionare quando la macchina virtuale è in esecuzione su KVM, Proxmox o altri hypervisor basati su QEMU.

Per prima cosa, assicurarsi che la macchina virtuale sia in esecuzione, quindi connettersi alla macchina utilizzando SSH o la console di Proxmox ed eseguire i seguenti comandi:

```
opkg update
opkg install qemu-ga
```

Dopo l'installazione, avviare il servizio:

```
/etc/init.d/qemu-ga start
```

Il QEMU guest agent sarà disponibile sulla macchina virtuale e verrà avviato automaticamente all'avvio.

Nota: A partire dalla versione 8.7.2, i pacchetti extra vengono reinstallati automaticamente dopo l'aggiornamento del sistema. Per le versioni precedenti e per ulteriori informazioni, consultare questa documentazione: *Ripristinare pacchetti aggiuntivi*.

5.2.2 Installazione su VMWare

VMWare può riscontrare problemi durante l'importazione diretta di immagini disco raw. Per garantire un'importazione senza problemi, decomprimere prima il file immagine, quindi convertire l'immagine raw nel formato nativo `.vmdk` di VMWare prima di procedere.

Su Windows, è possibile utilizzare un software come V2V Converter.

Su Linux è possibile utilizzare il comando `qemu-img`. Esempio:

```
qemu-img convert -f raw -O vmdk <source_image.raw> <destination_image.vmdk>
```

Sostituire:

- `<source_image.raw>` con il percorso effettivo della propria immagine disco raw
- `<destination_image.vmdk>` con il nome file .vmdk desiderato

Le seguenti impostazioni della macchina virtuale sono note per funzionare bene con NethSecurity:

- Sistema operativo guest: Altro Linux 5.x o successivo
- Controller SCSI: VMWare Paravirtual
- Adattatori di rete: E1000
- Firmware: BIOS (non UEFI)

VMware open-vm-tools

Gli open-vm-tools di VMware non fanno parte dell'immagine di NethSecurity, ma possono essere installati dalla riga di comando. Gli strumenti funzionano solo quando la macchina virtuale è in esecuzione su hypervisor VMware.

Per prima cosa, assicurarsi che la macchina virtuale sia in esecuzione, quindi connettersi alla macchina utilizzando SSH o la console VMWare ed eseguire i seguenti comandi:

```
opkg update
opkg install open-vm-tools
```

Dopo l'installazione, avviare il servizio:

```
/etc/init.d/vmtoolsd start
```

Gli open-vm-tools di VMware saranno disponibili sulla macchina virtuale e verranno avviati automaticamente all'avvio.

Si noti che dopo un aggiornamento dell'immagine, il pacchetto VMware open-vm-tools verrà rimosso e sarà necessario reinstallarlo. Consultare *Ripristinare pacchetti aggiuntivi* per ulteriori informazioni.

5.2.3 Installazione su Hyper-V

Per garantire un'importazione senza problemi su Hyper-V, decomprimere prima il file immagine, quindi convertire l'immagine raw nel formato nativo di Hyper-V `.vhdx` prima di procedere.

Su Windows, è possibile utilizzare un software come V2V Converter.

Su Linux è possibile utilizzare il comando `qemu-img`. Esempio:

```
qemu-img convert -f raw -O vhdx <source_image.raw> <destination_image.vhdx>
```

Sostituire:

- `<source_image.raw>` con il percorso effettivo della propria immagine disco raw
- `<destination_image.vhdx>` con il nome file .vhdx desiderato

5.2.4 Installazione su VirtualBox

VirtualBox può riscontrare problemi durante l'importazione diretta di immagini disco raw. Per garantire un'importazione senza problemi, decomprimere prima il file immagine, quindi convertire l'immagine raw nel formato nativo `.vdi` di VirtualBox prima di procedere.

Su Windows, Linux e macOS è possibile utilizzare lo strumento integrato *VBoxManage*. Esempio:

```
VBoxManage convertfromraw <source_image.raw> <destination_image.vdi>
```

Sostituire:

- `<source_image.raw>` con il percorso effettivo della propria immagine disco raw
- `<destination_image.vdi>` con il nome file .vdi desiderato

5.3 Configurazione di rete predefinita

Al primo avvio di NethSecurity, il sistema tenterà di configurare le interfacce di rete.

Per impostazione predefinita, la configurazione di rete sarà la seguente:

- L'interfaccia LAN verrà configurata con un indirizzo IP statico di 192.168.1.1.
- L'interfaccia WAN sarà configurata per utilizzare DHCP al fine di ottenere un indirizzo IP dal proprio ISP.

Un'eccezione a questa configurazione di rete predefinita riguarda le macchine virtuali in esecuzione su KVM e sul provider cloud Digital Ocean (droplet). In questo caso, la configurazione di rete sarà la seguente:

- L'interfaccia LAN sarà configurata per utilizzare DHCP al fine di ottenere un indirizzo IP dalla piattaforma di virtualizzazione.
- L'interfaccia WAN sarà configurata per utilizzare DHCP al fine di ottenere un indirizzo IP dal proprio ISP.

Nota: Se si utilizza NethSecurity in un ambiente di produzione, potrebbe essere necessario modificare la configurazione di rete predefinita per soddisfare esigenze specifiche. Ad esempio, potrebbe essere necessario configurare l'interfaccia LAN con un indirizzo IP diverso oppure configurare l'interfaccia WAN per utilizzare un indirizzo IP statico.

CAPITOLO 6

Accesso remoto

6.1 Credenziali predefinite

Le credenziali predefinite sono:

- Utente: `root`
- Password: `Nethesis,1234`

Queste credenziali possono essere utilizzate per accedere all'interfaccia web o tramite SSH:

- Interfaccia utente web: **https://<server_ip>:9090**
- Porta SSH predefinita: **22**

Il nome host predefinito di NethSecurity è: `NethSec`

Se il client ha ricevuto un indirizzo IP dal DHCP di NethSecurity, utilizzerà NethSecurity sia come gateway che come server DNS. In queste condizioni è possibile contattare NethSecurity utilizzando il suo hostname **nethsec** invece di **server_ip**, ad esempio

https://nethsec:9090

Questo hostname può essere modificato nella sezione Impostazioni di sistema.

Nota: La password predefinita per l'utente root è `Nethesis,1234`. Si consiglia di cambiare la password immediatamente dopo il primo accesso.

6.1.1 Reimpostare la password di root

La `root password` può essere reimpostata accedendo alla *Modalità Failsafe*. Una volta in questa modalità, è possibile cambiare la password eseguendo i seguenti comandi.

```
mount_root
passwd
```

Riavviare il firewall con il comando

```
reboot
```

6.2 Interfaccia utente web

L'interfaccia utente di NethSecurity (User Interface), l'interfaccia web ufficiale di NethSecurity, è disponibile sulla porta `9090` al seguente URL: **https://<server_ip>:9090**.

Per facilitare l'accesso, l'interfaccia utente di NethSecurity è disponibile anche sulla porta HTTP standard `443` al seguente URL: **https://<server_ip>** oppure **http://<server_fqdn>**.

Entrambi gli URL sono accessibili dalla LAN e dalla WAN per impostazione predefinita.

6.2.1 Limitazione dell'accesso all'interfaccia utente di NethSecurity

Per impostazione predefinita, questa interfaccia è accessibile sulla porta 9090 sia dalla rete interna (LAN) sia da internet (WAN). Sebbene sia conveniente, ciò può potenzialmente rappresentare un rischio per la sicurezza.

Per mitigare questo rischio, sono disponibili due opzioni (rimuovere o limitare l'accesso):

- rimuovere la regola `Allow-UI-from-WAN`: andare alla pagina delle regole del Firewall, navigare nella scheda `Regole di input` e individuare la regola «Allow-UI-from-WAN». Fare clic sul pulsante *Elimina* per rimuoverla
- limitare l'accesso da IP o reti specifiche: nella pagina delle regole del Firewall, individuare la regola «Allow-UI-from-WAN» e fare clic sul pulsante *Modifica*. Nel campo `Indirizzo sorgente`, inserire gli indirizzi IP o i CIDR di rete dai quali si desidera consentire l'accesso all'interfaccia utente di NethSecurity.

  Ad esempio, per consentire l'accesso solo dalla propria rete domestica, si potrebbe inserire la rete 192.168.1.0/24. Consentire l'accesso solo da indirizzi IP o reti affidabili. Lasciando questo campo vuoto, chiunque su Internet potrà accedere all'interfaccia utente di NethSecurity.

Misure di sicurezza aggiuntive:

- utilizzare una password robusta per l'utente amministratore
- abilitare *l'autenticazione a due fattori (2FA)* per l'utente amministratore
- mantenere il firewall aggiornato con le ultime patch di sicurezza

6.2.2 Modificare la porta dell'interfaccia utente web

Gli utenti possono modificare la porta dell'interfaccia utente di NethSecurity.

Per modificare la porta dell'interfaccia utente di NethSecurity da 9090 a 8181, eseguire:

```
uci set ns-ui.config.nsui_extra_port=8181
uci commit ns-ui && ns-ui
```

Avvertimento: Il controller utilizza la porta 9090 per comunicare con l'unità. Modificare la porta impedirà al controller di gestire NethSecurity.

Se è ancora necessario inoltrare la porta 9090 a un'altra macchina all'interno della LAN, è possibile mantenere il controller connesso lasciando invariato `ns-ui_extra_port` e inoltrando la porta verso la nuova macchina. L'inoltro della porta a un'altra macchina sarà accettabile perché il controller raggiungerà la porta 9090 tramite la VPN.

6.2.3 Disabilitare l'interfaccia utente web sulla porta 443

Sebbene l'esposizione della porta 443 (HTTPS) possa essere necessaria per alcuni servizi, l'accesso diretto all'interfaccia utente di NethSecurity tramite questa porta può rappresentare un potenziale rischio per la sicurezza. Ecco come mantenere in modo sicuro la funzionalità della porta 443 proteggendo al contempo l'interfaccia utente di NethSecurity.

Se non è necessario accedere all'interfaccia utente di NethSecurity tramite la porta 443, disabilitarla per ridurre al minimo le opportunità di attacco. Eseguire i seguenti comandi sul sistema NethServer:

```
uci set ns-ui.config.nsui_enable=0
uci commit ns-ui && ns-ui
```

Questa opzione disabilita l'accesso all'interfaccia utente di NethSecurity sia tramite l'indirizzo IP del server che tramite FQDN sulla porta 443.

Se è necessario utilizzare la porta 443 per altri servizi, configurare il firewall per reindirizzare il traffico destinato alla porta 443 a un server web separato che ospita tali servizi. Assicurarsi che questo server separato disponga di solide misure di sicurezza.

6.2.4 Informativa sulla privacy

In alcuni casi, è necessario visualizzare l'informativa sulla privacy di un prodotto prima dell'accesso. NethSecurity non mostra alcuna informativa sulla privacy per impostazione predefinita, ma è possibile aggiungere un collegamento a un sito web esterno che contiene l'informativa sulla privacy.

Per aggiungere un collegamento all'informativa sulla privacy, accedere alla riga di comando ed eseguire:

```
URL=https://mysite.org/privacy_policy; sed -i "s|PRIVACY_POLICY_URL\: ''|PRIVACY_POLICY_
↪URL: '$URL'|" /www-ns/branding.js
```

Sostituire `https://mysite.org/privacy_policy` con l'URL della propria informativa sulla privacy.

Il link alla privacy policy verrà visualizzato all'interno della pagina di accesso dopo il prossimo aggiornamento della pagina.

6.2.5 Interfaccia utente web legacy

Avvertimento: Le modifiche effettuate tramite l'interfaccia web LuCI possono compromettere il funzionamento dell'interfaccia ufficiale di NethSecurity. Utilizzare a proprio rischio!

NethSecurity offre anche LuCI, l'interfaccia web originale di OpenWrt, che fornisce un'ampia gamma di opzioni di configurazione ma non è ufficialmente supportata. LuCI è disabilitato per impostazione predefinita. Per abilitarla, eseguire:

```
uci set ns-ui.config.luci_enable=1
uci commit ns-ui
ns-ui
```

Una volta abilitato, Luci sarà disponibile solo sulla porta 443 a questo URL: **https://<server_ip>/cgi-bin/luci**

Le modifiche alle seguenti pagine di LuCI sono note per causare comportamenti imprevedibili:

- Scheda accesso HTTP: configura uhttpd che non è presente all'interno di NethSecurity
- Scheda Registrazione: configura logd, che non è presente all'interno di NethSecurity.
- Rete: la configurazione creata con questa pagina non è compatibile con l'interfaccia utente di NethSecurity

Se precedentemente abilitata, l'interfaccia web LuCI può essere disabilitata eseguendo:

```
uci set ns-ui.config.luci_enable=0
uci commit ns-ui
ns-ui
```

6.2.6 Nascondere la versione del server web

Per impostazione predefinita, il server web nginx che serve l'interfaccia utente di NethSecurity include il proprio numero di versione negli header di risposta HTTP. Molte valutazioni delle vulnerabilità si basano sull'identificazione della versione del software, il che può generare falsi positivi quando le correzioni vengono retroportate senza modificare la versione riportata. Sebbene nascondere le informazioni sulla versione non migliori la sicurezza di per sé, può contribuire a limitare l'esposizione di vulnerabilità note e specifiche della versione agli strumenti di scansione automatizzati.

Per disabilitare la visualizzazione della versione di nginx negli header HTTP dell'interfaccia utente di NethSecurity, eseguire i seguenti comandi:

```
uci set ns-ui.config.server_tokens='off'
uci commit ns-ui
reload_config
```

Questa configurazione riguarda solo l'interfaccia utente di NethSecurity. Il reverse proxy ha una propria configurazione separata.

6.3 Interfaccia utente NethSecurity 2FA

Proteggere l'account amministratore di NethSecurity è fondamentale, e l'Autenticazione a Due Fattori (2FA) aggiunge un ulteriore livello di sicurezza oltre alla sola password. La 2FA richiede due passaggi di verifica durante l'accesso. Invece di utilizzare solo una password, sarà necessario anche un codice temporaneo generato da un'app separata sul proprio smartphone o tablet. Questo riduce significativamente il rischio di accessi non autorizzati anche nel caso in cui la password venga compromessa.

Abilitazione dell'autenticazione a due fattori (2FA) nell'interfaccia utente di NethSecurity:

- Accedere all'interfaccia web di NethSecurity
- Fare clic sull'icona utente nell'angolo in alto a destra e selezionare `Impostazioni account`
- Individuare l'opzione Autenticazione a due fattori e fare clic su *Configura 2FA*

Configurazione dell'app di autenticazione:

- Scaricare un'app di autenticazione sul proprio smartphone o tablet. Le opzioni più diffuse includono FreeOTP, Google Authenticator e Microsoft Authenticator.
- Aprire l'app e scansionare il codice QR visualizzato sull'interfaccia web di NethSecurity. Questo aggiungerà l'account NethSecurity all'app di autenticazione.
- Inserire il codice a 6 cifre visualizzato dall'app di autenticazione nel campo One-Time Password (OTP) dell'interfaccia web di NethSecurity.

Il sistema fornirà anche un set di codici di backup. Questi codici possono essere utilizzati per accedere nel caso in cui si perda lo smartphone o l'app di autenticazione. Conservare questi codici in modo sicuro, preferibilmente offline.

6.3.1 Disabilitare l'autenticazione a due fattori (2FA) tramite l'interfaccia web

Se l'amministratore può ancora accedere all'interfaccia web:

1. Fare clic sull'icona utente nell'angolo in alto a destra e selezionare `Impostazioni account`.
2. Scorrere fino alla sezione `Autenticazione a due fattori`.
3. Fare clic su `Revoca 2FA`.
4. Viene visualizzata una finestra di conferma che avverte che il livello di sicurezza sarà ridotto. Fare clic su `Revoca 2FA` per confermare.
5. Se richiesto, inserire la password attuale per autorizzare la modifica.

Dopo la conferma, il badge di stato cambia in disabilitato e al prossimo accesso non sarà più richiesto un OTP.

6.3.2 Disabilitare l'autenticazione a due fattori (2FA) dalla riga di comando (recupero d'emergenza)

Se un amministratore ha perso sia il dispositivo OTP che i codici di recupero e non può più accedere all'interfaccia web, l'autenticazione a due fattori (2FA) può essere reimpostata direttamente dalla shell come `root` tramite SSH.

Eseguire i seguenti comandi, sostituendo <*username*> con il nome dell'account amministratore (utilizzare `root` per l'amministratore predefinito):

```
SECRETS_DIR=/etc/ns-api-server
USERNAME=root   # change to the affected username

rm -f  "${SECRETS_DIR}/${USERNAME}/secret"
rm -f  "${SECRETS_DIR}/${USERNAME}/codes"
printf '0' > "${SECRETS_DIR}/${USERNAME}/status"
```

Dopo questi comandi, l'utente può accedere solo con la propria password. L'autenticazione a due fattori (2FA) può essere riattivata in qualsiasi momento dall'interfaccia web.

Nota: Solo l'account `root` ha accesso SSH per impostazione predefinita. Gli amministratori non-root non possono essere recuperati tramite SSH dall'utente interessato stesso; è necessaria una sessione `root` esistente per eseguire i comandi sopra indicati per loro conto.

6.4 Amministratori dell'interfaccia utente di NethSecurity

L'utente predefinito per accedere all'interfaccia web utente è root, ma è possibile creare altri utenti amministratori con accesso esclusivo all'interfaccia web.

Per creare un utente nel database locale, inserire il `Nome utente` e il `Nome visualizzato`. Assicurarsi di impostare una password per l'utente; questa è obbligatoria per gli utenti amministratori. Se l'utente necessita di accesso amministrativo all'interfaccia web, abilitare l'opzione `Utente amministratore`.

È possibile concedere o revocare l'accesso amministrativo solo agli utenti presenti nel database locale.

6.4.1 Verifica delle azioni utente

Ogni volta che un amministratore accede all'interfaccia utente di NethSecurity, il sistema registra l'evento all'interno del file */var/log/messages*. Esempio di evento di accesso per l'utente *goofy*:

```
Jun 21 09:43:19 NethSec nethsecurity-api[5376]: nethsecurity_api 2024/06/21 09:43:19␣
↪middleware.go:78: [INFO][AUTH] authentication success for user goofy
Jun 21 09:43:19 NethSec nethsecurity-api[5376]: nethsecurity_api 2024/06/21 09:43:19␣
↪middleware.go:186: [INFO][AUTH] login response success for user o
```

Esempio di evento di logout per l'utente *goofy*:

```
Jun 21 09:46:13 NethSec nethsecurity-api[5376]: nethsecurity_api 2024/06/21 09:46:13␣
↪middleware.go:214: [INFO][AUTH] logout response success for user goofy
```

Inoltre, ogni azione eseguita da un amministratore all'interno dell'interfaccia NethSecurity viene registrata nel file */var/log/messages*. Esempio di azione eseguita dall'utente *goofy*:

```
Jun 21 09:43:19 NethSec nethsecurity-api[5376]: nethsecurity_api 2024/06/21 09:43:19␣
↪middleware.go:170: [INFO][AUTH] authorization success for user goofy. POST /api/ubus/
↪call {"path":"ns.dashboard","method":"service-status","payload":{"service":"internet"}}
```

6.5 SSH

Per impostazione predefinita, il sistema accetta connessioni SSH sulla porta standard 22 dalla rete interna (LAN). L'accesso come root è abilitato utilizzando la password predefinita. Per consentire l'accesso SSH da internet (WAN), è necessario aggiungere una regola di input del firewall per la porta di ascolto del server.

Da una macchina Linux, utilizzare il seguente comando:

```
ssh root@192.168.1.1
```

6.6 Console VGA e layout tastiera

Se la macchina dispone di una porta video VGA/DVI/HDMI, collegare un monitor ad essa. In questo modo sarà possibile accedere alla console utilizzando le credenziali predefinite sopra indicate.

Si noti che il sistema è configurato con il layout di tastiera US.

Per modificare temporaneamente il layout della tastiera corrente in italiano, accedere al sistema ed eseguire il seguente comando:

```
loadkmap < /usr/share/keymaps/it.map.bin
```

La configurazione del layout della tastiera può essere salvata scrivendo il codice della mappa dei tasti all'interno di `/etc/keymap`. Esempio per la mappa dei tasti `it` (italiana):

```
echo 'it' > /etc/keymap
grep -q /etc/keymap /etc/sysupgrade.conf || echo /etc/keymap >> /etc/sysupgrade.conf
```

Per ottenere l'elenco delle keymap disponibili, eseguire il seguente comando:

```
ls -1 /usr/share/keymaps/ | cut -d'.' -f1
```

6.7 Console seriale

Se la macchina dispone di una porta seriale (RS-232, tipicamente disponibile con connettore DE-9 o connettore RJ45/8P8C) è possibile accedere direttamente al firewall tramite essa utilizzando un cavo null-modem e un programma terminale. `PuTTY` (versione 0.60 o superiore) è una scelta comune se si utilizza Microsoft Windows, mentre le distribuzioni Linux offrono strumenti come `minicom`, `picocom` o `screen`.

I parametri di accesso predefiniti per NethSecurity 8 sono:

- Velocità di trasmissione: 115200,
- Bit dati: 8
- Parità : Nessuna
- Bit di stop su 1

Questi ultimi tre parametri sono spesso abbreviati come 8N1

6.7.1 Adattatori USB-Seriale

In caso di necessità, NethSecurity può essere utilizzato per accedere a un altro server tramite la console seriale. Se l'hardware non dispone di una porta RS-232, è possibile utilizzare adattatori USB-seriale. Per questo motivo, è possibile scaricare e installare i driver per gli adattatori più comuni su NethSecurity. Questi driver sono forniti così come sono e **non sono supportati da Nethesis** (in caso di utilizzo della versione Enterprise o Subscription).

Sono forniti due pacchetti per l'installazione, che coprono la grande maggioranza degli adattatori disponibili sul mercato.

```
kmod-usb-serial-cp210x - 5.15.162-1 - Kernel support for Silicon Labs cp210x USB-to-
↪Serial converters
kmod-usb-serial-pl2303 - 5.15.162-1 - Kernel support for Prolific PL2303 USB-to-Serial␣
↪converters
```

- Per installare il driver Prolific PL2303:

  ```
  opkg install kmod-usb-serial-pl2303
  ```

- I log mostreranno un output simile al seguente:

  ```
  Aug  6 08:08:17 nsec8 kernel: [ 2346.359247] usb 1-6: new full-speed USB device␣
  ↪number 3 using xhci_hcd
  Aug  6 08:08:17 nsec8 kernel: [ 2346.543052] pl2303 1-6:1.0: pl2303 converter␣
  ↪detected
  Aug  6 08:08:17 nsec8 kernel: [ 2346.550401] usb 1-6: pl2303 converter now attached␣
  ↪to ttyUSB0
  ```

Nota: A partire dalla versione 8.7.2, i pacchetti extra vengono reinstallati automaticamente dopo l'aggiornamento del sistema. Per le versioni precedenti e per ulteriori informazioni, consultare questa documentazione: *Ripristinare pacchetti aggiuntivi*.

CAPITOLO 7

Procedura guidata di configurazione

La prima volta che si accede all'interfaccia utente web, viene avviata una procedura guidata di configurazione. Questo processo guidato può assistere nella creazione di una configurazione iniziale sicura per il firewall e garantisce che l'unità sia pronta per essere distribuita in un ambiente di produzione.

Nota: Per una sicurezza ottimale e per garantire un ambiente di configurazione controllato, si raccomanda vivamente di completare la procedura guidata di configurazione prima di collegare il dispositivo a Internet.

7.1 Benvenuti nella procedura guidata di configurazione

Nella prima pagina della procedura guidata di configurazione, è possibile fare clic su *Inizia il setup* per avviare il processo di configurazione guidata. In alternativa, è possibile fare clic su *Salta procedura guidata* per saltare la procedura guidata e accedere direttamente all'interfaccia web utente. Tuttavia, è fortemente consigliato completare la procedura guidata di configurazione per garantire una configurazione sicura e funzionale.

7.2 Passaggio 1: Cambiare la password di root

È necessario definire una nuova password sicura per l'account root. Questa misura riduce significativamente il rischio di compromissione eliminando la dipendenza da credenziali predefinite pubblicamente note.

Nota:

- La password di root aggiornata verrà applicata immediatamente al momento della conferma.
- Assicurarsi che le nuove credenziali siano archiviate in modo sicuro (ad esempio, utilizzando un password manager) prima di procedere con il passaggio successivo della configurazione.

- Se si riavvia la procedura guidata di configurazione dopo aver cambiato la password di root (ad esempio, chiudendo e riaprendo la scheda del browser), sarà necessario utilizzare la nuova password per accedere all'interfaccia web.

7.3 Passaggio 2: Accesso SSH

È possibile personalizzare l'accesso SSH per soddisfare i requisiti di sicurezza e operativi.

7.3.1 Configurazione di accesso predefinita

- L'accesso LAN è abilitato per impostazione predefinita per consentire l'accesso amministrativo dall'interno della rete locale attendibile.
- L'accesso WAN è disabilitato per impostazione predefinita per prevenire l'esposizione a minacce esterne provenienti da reti non affidabili.

7.3.2 Impostazioni

- **Porta TCP**: la porta di ascolto per SSH può essere modificata se necessario. Il valore predefinito è 22.
- **Accesso root con password**: si consiglia di disabilitare l'accesso root tramite password per SSH. Disabilitare questa opzione riduce significativamente il rischio di accessi non autorizzati, limitando la possibilità di attacchi brute-force alle password.

Nota: Se l'accesso tramite password per l'utente root è disabilitato, è essenziale caricare la chiave pubblica SSH dell'utente root sul dispositivo per garantire il continuo accesso remoto.

7.4 Passaggio 3: Accesso all'interfaccia web sulla porta TCP 9090

Configurare i parametri di accesso per l'interfaccia utente web, che opera sulla porta 9090.

7.4.1 Configurazione predefinita

Per impostazione predefinita, l'accesso all'interfaccia web è abilitato dalla LAN, consentendo la gestione amministrativa dall'interno della rete locale attendibile.

7.4.2 Impostazioni

È possibile scegliere tra le seguenti opzioni di accesso per la connettività WAN:

- **Disabilitato** (consigliato): questa opzione disabilita l'accesso all'interfaccia web dalla WAN, prevenendo l'esposizione a minacce esterne.
- **Abilitato**: l'accesso completo all'interfaccia web è consentito da qualsiasi sorgente WAN. Questa modalità dovrebbe essere utilizzata solo in ambienti sicuri o quando necessario per la gestione remota, e deve essere protetta con credenziali robuste.

- **Limitato**: l'accesso all'interfaccia web dalla WAN è limitato agli indirizzi IP o alle reti specificate. È necessario definire uno o più dei seguenti:
  - Indirizzo IP
  - Reti in formato CIDR (ad es., 192.168.1.0/24)
  - Intervalli di indirizzi IP (ad es., 203.0.113.10-203.0.113.20)

Se si sceglie l'opzione **Limitato**, gli indirizzi IP configurati appariranno alla fine della procedura guidata sotto **Firewall > Regole > Regole di input**.

7.5 Passaggio 4: Interfaccia web e accesso WAN sulla porta TCP 443

Impostare i controlli di accesso per l'interfaccia web e le connessioni WAN sulla porta 443.

- **Servizio dell'interfaccia web sulla porta TCP 443**: per impostazione predefinita, l'interfaccia utente web è disponibile sulla porta TCP 9090. Abilitando questa opzione, l'interfaccia sarà accessibile anche sulla porta TCP 443. Si consiglia di mantenere disabilitato questo accesso aggiuntivo e di utilizzare sempre la porta TCP 9090 per accedere all'interfaccia web.
- **Accesso WAN sulla porta TCP 443**: questa opzione controlla se l'accesso WAN sulla porta 443 è disabilitato (consigliato) o abilitato. Attenzione, lasciando questa opzione disabilitata, i reverse proxy non funzioneranno.

7.6 Passaggio 5: Riepilogo

La pagina di riepilogo offre l'opportunità di rivedere la configurazione dell'unità prima di applicare le modifiche.

Nota: L'accesso WAN all'interfaccia web potrebbe essere limitato dalle impostazioni correnti. L'applicazione delle modifiche mentre si è connessi tramite la porta 443 potrebbe comportare la perdita dell'accesso. Verificare che la configurazione soddisfi le esigenze di accesso remoto, in particolare quando si utilizzano reverse proxy.

Utilizzare il pulsante `Precedente` per tornare indietro ed effettuare eventuali modifiche se necessario. Fare clic su `Fine configurazione` per applicare le modifiche e completare la procedura guidata di configurazione.

CAPITOLO 8

Monitoraggio

NethSecurity offre funzionalità di monitoraggio complete per aiutare gli amministratori a tenere traccia delle prestazioni e dello stato di salute del firewall. Il monitoraggio è essenziale per garantire il funzionamento ottimale del firewall e individuare eventuali problemi che potrebbero comprometterne la funzionalità.

NethSecurity offre due tipi di monitoraggio:

- **Monitoraggio in tempo reale**: sfrutta Netdata, Netify agent e i log per fornire informazioni immediate sulle prestazioni del firewall. Legge i dati dai log e dai database locali, memorizzando le metriche nella RAM. Si noti che queste metriche vengono azzerate a ogni riavvio, garantendo che vengano visualizzati solo i dati più recenti.
- **Monitoraggio storico**: per una visione più completa nel tempo, il monitoraggio storico memorizza i dati su un controller remoto. Questo consente di preservare le metriche anche dopo i riavvii e permette un monitoraggio centralizzato. Si noti che questa funzionalità richiede un abbonamento valido sia sul firewall che sul controller.

8.1 Monitoraggio in tempo reale

Il monitoraggio in tempo reale è una funzionalità essenziale nei moderni sistemi firewall, che consente agli amministratori di avere una visibilità immediata sul traffico di rete, sulle connessioni VPN e sulle minacce alla sicurezza. In NethSecurity, il monitoraggio in tempo reale fornisce dati aggiornati in tempo reale, garantendo che problematiche come congestione della rete, accessi non autorizzati e violazioni della sicurezza vengano individuate e mitigate tempestivamente. Il monitoraggio in tempo reale memorizza i dati in RAM e si azzera a ogni riavvio della macchina.

La pagina `Monitor in tempo reale` fornisce una panoramica completa delle prestazioni e dello stato del firewall, con approfondimenti dettagliati sul traffico di rete. È suddivisa in quattro sezioni principali: `Traffico`, `Live Flows`, `Top Talkers`, `Connettività WAN`, `VPN` e `Sicurezza`.

8.1.1 Traffico giornaliero

Il grafico sottostante legge i dati dal demone dpireport:

- `Traffico totale giornaliero`: questo contatore mostra il volume totale di dati trasferiti attraverso il firewall per la giornata corrente.
- `Traffico recente`: l'istogramma del traffico giornaliero rappresenta visivamente il traffico di rete nel tempo, aggiornato ogni 60 minuti. Aiuta a identificare i periodi di maggiore attività e ad analizzare le fluttuazioni del traffico durante la giornata. Picchi improvvisi o cali potrebbero indicare potenziali problemi di prestazioni o minacce alla sicurezza.
- `Host locali`: questo grafico si concentra sugli host interni (locali) e sul loro traffico. Aiuta a identificare i dispositivi più attivi sulla rete, facilitando la gestione della larghezza di banda e il rilevamento di potenziali rischi di sicurezza interni, come dispositivi compromessi che generano traffico inatteso.
- `Applicazioni`: questo grafico mostra il traffico suddiviso per applicazione, consentendo di monitorare quali software o servizi stanno generando la maggior parte del traffico. È utile per comprendere il comportamento delle applicazioni, rilevare i maggiori consumatori di banda e monitorare la conformità alle policy di utilizzo.
- `Host remoti`: questo grafico elenca gli host esterni (remoti) che hanno scambiato la maggior quantità di dati con la rete. Analizzando questi dati, gli amministratori possono monitorare le interazioni con specifiche entità esterne, aiutando a rilevare fonti esterne malevole o modelli insoliti di traffico in uscita.
- `Protocollo`: questo grafico mostra la ripartizione del traffico giornaliero per protocollo (ad esempio, HTTP, HTTPS, FTP). È utile per identificare quali protocolli stanno consumando la maggior parte della banda e per assicurarsi che le risorse di rete vengano utilizzate in modo appropriato. Un utilizzo elevato di protocolli non familiari può indicare attività non autorizzate.

È possibile restringere la ricerca a un host, un'applicazione o un protocollo specifico facendo clic sull'etichetta corrispondente nella tabella sotto il grafico.

8.1.2 Flussi in tempo reale

La sezione Live Flows fornisce una visualizzazione in tempo reale di tutte le connessioni di rete attive, consentendo agli amministratori di monitorare il traffico mentre si verifica. Questa sezione viene visualizzata in formato tabellare, con ogni riga che rappresenta un singolo flow. La tabella include le seguenti informazioni per ciascuna connessione:

- `Applicazione`: l'applicazione rilevata che genera il traffico.
- `Protocollo`: il protocollo di rete utilizzato per il flusso (ad esempio TCP, UDP, HTTP).
- `Tag`: eventuali tag rilevanti assegnati al flusso per la classificazione (ad es. Outgoing, Remote, Internal)
- `Sorgente`: la sorgente della connessione, che mostra tipicamente l'indirizzo IP e la porta del dispositivo che ha iniziato la connessione.
- `Destinazione`: la destinazione della connessione, che mostra tipicamente l'hostname o l'indirizzo IP e la porta del dispositivo di destinazione.
- `Scarica`: la velocità attuale di trasferimento in download del flusso, che indica la rapidità con cui i dati vengono ricevuti.
- `Upload`: la velocità attuale di trasferimento in upload del flusso, che indica la rapidità con cui i dati vengono inviati.
- `Durata`: il tempo totale durante il quale il flusso è stato attivo dalla sua prima rilevazione. Questo aiuta a comprendere per quanto tempo una determinata connessione è stata mantenuta.
- `Last Seen At`: il timestamp dell'attività più recente per il flow; questo indica quando il flow ha trasmesso o ricevuto dati l'ultima volta, aiutando a identificare connessioni inattive o inattive.

- `Dettagli`: l'icona della lente d'ingrandimento con un segno più; facendo clic su questa icona si apre una vista dettagliata del flow, che mostra tutte le informazioni disponibili, inclusi i dati non visualizzati direttamente nella tabella principale. Questo consente agli amministratori di accedere a tutti i metadati del flow per un'analisi più approfondita o per la risoluzione dei problemi.

Questa tabella in tempo reale consente agli operatori di identificare rapidamente gli utenti intensivi, monitorare il comportamento delle applicazioni e risolvere i problemi di rete man mano che si verificano.

Configurazione

La sezione Live Flows include anche opzioni di configurazione per gestire il comportamento del servizio di monitoraggio dei flussi:

- `Flows Daemon Enabled`: un interruttore per abilitare o disabilitare il servizio di monitoraggio dei flussi in tempo reale; disattivando il daemon si interrompe la raccolta dei dati di flusso in tempo reale.
- `Persistenza dei Flussi dopo la Scadenza`: un'impostazione che determina per quanto tempo i record dei flussi vengono conservati dopo che il flusso è terminato; questo consente agli amministratori di regolare la conservazione dei dati in base alle esigenze di monitoraggio e alla disponibilità di spazio di archiviazione.

8.1.3 Principali interlocutori

Lo scopo principale della sezione Top Talkers è fornire una panoramica iniziale sull'utilizzo della banda, identificando rapidamente i principali "contributori" al traffico di rete. Queste informazioni possono servire come punto di partenza per analisi più approfondite, attività di troubleshooting o per il monitoraggio generale dell'efficienza della rete.

La sezione Top Talkers visualizza i dati di traffico aggiornati ogni 30 secondi, offrendo una panoramica rapida e aggiornata su quali entità stanno generando il maggior traffico di rete. È suddivisa in tre categorie:

- `Host locali`: elenca tutti gli host locali rilevati e il loro stato attuale del traffico, ordinati per volume di traffico. Questo permette di identificare rapidamente quali dispositivi stanno utilizzando più banda, senza distinguere il tipo di connessione o il protocollo.
- `Applicazioni`: mostra tutte le applicazioni rilevate e il loro traffico attuale, ordinate per volume. Questa vista aiuta a comprendere quali servizi o applicazioni stanno consumando la maggior parte delle risorse di rete, indipendentemente dal dispositivo su cui sono in esecuzione.
- `Protocolli`: elenca tutti i protocolli rilevati e il loro traffico attuale, ordinati per volume. Questo fornisce una visione immediata su quali tipi di traffico (ad esempio, HTTP, DNS, SMTP) stanno dominando la rete, senza considerare quale host o applicazione li stia generando.

8.1.4 Collegamenti uplink WAN

La sezione degli uplink WAN fornisce una panoramica delle connessioni WAN, inclusi stato, allocazione della larghezza di banda e dati sul traffico.

Questa pagina mostra le seguenti informazioni:

- `WAN`: elenco delle connessioni WAN con il loro stato attuale (UP/DOWN) e l'indirizzo IP pubblico. Le informazioni sullo stato aiutano a garantire che le connessioni di rete critiche siano online e che eventuali interruzioni vengano affrontate immediatamente. I dati provengono dallo stato mwan3 del firewall.
- `Eventi WAN`: questa sezione elenca i recenti eventi di connessione e disconnessione WAN delle ultime 24 ore, fornendo informazioni sulla stabilità della rete e sulle interruzioni. Aiuta gli amministratori a comprendere la frequenza e la durata delle interruzioni di rete, facilitando la risoluzione dei problemi e la pianificazione della capacità. I dati vengono recuperati dai log delle ultime 24 ore. Se i log non coprono l'intero periodo di 24 ore, i dati potrebbero essere incompleti. I risultati vengono memorizzati nella cache per 5 minuti.

- `Traffico interfaccia WAN`: questo istogramma mostra i dati di traffico per ciascuna connessione WAN negli ultimi 60 minuti, provenienti da Netdata. Aiuta a monitorare le prestazioni in tempo reale e a diagnosticare problemi come il bilanciamento del carico non uniforme o la saturazione del collegamento WAN.
- `Latenza verso <indirizzo>`: questa sezione fornisce dati in tempo reale sulla latenza per un indirizzo IP specifico configurato all'interno del modulo *Monitoraggio latenza del ping*. Il grafico aiuta a monitorare le prestazioni della rete e a identificare potenziali problemi di connettività.
- `Tasso di consegna dei pacchetti verso <indirizzo>`: questa sezione fornisce dati in tempo reale sul tasso di consegna dei pacchetti per un indirizzo IP specifico configurato all'interno del modulo *Monitoraggio latenza del ping*. Se il tasso è inferiore al 100%, ciò potrebbe indicare congestione di rete o problemi di connettività.

8.1.5 VPN

La sezione VPN fornisce approfondimenti dettagliati sui server OpenVPN Road Warrior, sui tunnel OpenVPN e sui tunnel IPsec.

Per ogni server OpenVPN Road Warrior, vengono visualizzate le seguenti informazioni:

- `Stato`: questa sezione mostra lo stato attuale del server OpenVPN. Aiuta gli amministratori a monitorare la disponibilità del servizio VPN e a rilevare eventuali problemi che potrebbero influire sulla connettività degli utenti.
- `Client connessi`: questo visualizza il numero totale di utenti attualmente registrati sul server VPN. Monitorare gli utenti registrati è fondamentale per garantire una corretta pianificazione della capacità e le prestazioni della VPN, soprattutto quando il sistema si avvicina al limite massimo di utilizzo.
- `Traffico totale per ore`: questo grafico mostra il totale dei dati trasferiti da tutti i client VPN durante ciascuna ora, fornendo una panoramica dell'utilizzo della banda VPN. Aiuta a monitorare la quantità di traffico di rete generato dalla VPN e a identificare le ore di maggiore utilizzo, che potrebbero causare problemi di prestazioni.
- `Connessioni giornaliere`: questa sezione elenca tutti gli utenti VPN attualmente connessi e l'orario in cui si sono collegati. È utile per monitorare la durata delle sessioni e rilevare eventuali usi impropri della VPN, come connessioni che durano insolitamente a lungo. I dati provengono dal database locale delle connessioni SQLite.
- `Clienti collegati per ora`: questo grafico mostra il numero di client connessi alla VPN nel tempo. Consente agli amministratori di monitorare l'attività della VPN durante la giornata, aiutando a identificare i periodi di picco e a pianificare un aumento della capacità quando necessario. I dati provengono dal database locale delle connessioni SQLite.
- `Traffico cliente per ora`: questo grafico suddivide il traffico VPN per singolo client nel tempo. Aiuta a rilevare utenti che potrebbero consumare una quantità eccessiva di banda o svolgere attività non autorizzate, facilitando l'identificazione di potenziali minacce interne. I dati provengono dal database locale delle connessioni SQLite.

La sezione Site-to-Site VPN fornisce informazioni su tunnel OpenVPN e IPsec:

- `Tunnel connessi`: questo contatore mostra il numero di tunnel VPN site-to-site attivi.
- `Tunnel configurati`: questo contatore mostra l'elenco di tutti i tunnel VPN site-to-site configurati, inclusi il loro stato e il tipo.
- `Traffico tunnel`: questo istogramma fornisce dati sul traffico in tempo reale per ciascun tunnel VPN site-to-site negli ultimi 60 minuti. Aiuta a rilevare problemi come bassa velocità di trasferimento o instabilità della connessione.

8.1.6 Sicurezza

La sezione sicurezza fornisce informazioni sulla rilevazione di malware e sul monitoraggio degli attacchi, aiutando gli amministratori a identificare e mitigare le minacce alla sicurezza. Per abilitare questa sezione, è necessario abilitare il modulo *Threat shield IP*. I dati provengono dai log relativi alle ultime 24 ore. Se i log non coprono l'intero periodo di 24 ore, i dati potrebbero essere incompleti. I risultati vengono memorizzati nella cache per 5 minuti per migliorare le prestazioni.

La sezione `Blocklist` fornisce una panoramica dei pacchetti bloccati in base alle blocklist abilitate. I grafici disponibili sono:

- `Minacce bloccate`: questo contatore mostra il numero totale di pacchetti bloccati dal firewall a causa del rilevamento di malware per la giornata corrente. Fornisce una panoramica chiara del volume delle minacce intercettate, offrendo agli amministratori una misura dell'efficacia del firewall.
- `Minacce bloccate per ora`: questo grafico tiene traccia del numero di pacchetti bloccati ogni ora. Aiuta a identificare i momenti della giornata in cui la rete è più vulnerabile agli attacchi, facilitando l'adozione di misure preventive.
- `Minacce per direzione`: un grafico che mostra la distribuzione del malware bloccato per catena del firewall. A seconda dell'opzione di registrazione abilitata, il firewall può registrare i pacchetti provenienti dalle seguenti catene:
  - *inp-wan*: pacchetti provenienti dall'interfaccia WAN e destinati al firewall
  - *fwd-wan*: pacchetti provenienti dall'interfaccia WAN e destinati alla rete LAN
  - *fwd-lan*: pacchetti provenienti dalla rete LAN e destinati all'interfaccia WAN
  - *pre-ct*: invio in flooding dei pacchetti che si trovano in stato non valido
  - *pre-syn*: invio massiccio di pacchetti che fanno parte di una connessione TCP e si trovano nello stato SYN
  - *pre-udp*: invio massiccio di pacchetti che fanno parte di una connessione UDP
- `Minacce per categoria`: un grafico che suddivide il malware bloccato per categoria, aiutando gli amministratori a individuare le blocklist più efficaci.

La sezione `Attacchi brute force` fornisce informazioni sul numero di IP bloccati in base al numero di tentativi di accesso non riusciti. I dati provengono dai log relativi alle ultime 24 ore. Se i log non coprono l'intero periodo di 24 ore, i dati potrebbero essere incompleti. I risultati vengono memorizzati nella cache per 5 minuti per migliorare le prestazioni. I grafici disponibili sono:

- `Indirizzi IP Bloccati`: questo contatore mostra il numero totale di indirizzi IP bloccati a causa di attività dannose per la giornata corrente. Aiuta a monitorare il volume dei tentativi di intrusione.
- `Indirizzi IP bloccati per ora`: questo grafico tiene traccia del numero di indirizzi IP bloccati nel tempo, aiutando a identificare i periodi di maggiore attività di attacco.
- `Indirizzo IP bloccato più frequentemente`: questo carattere mostra gli indirizzi IP che sono stati bloccati più frequentemente. È utile per identificare minacce persistenti o fonti di attacco che dovrebbero essere investigate o inserite in blacklist.

8.1.7 Netdata

NethSecurity utilizza Netdata come strumento di monitoraggio in tempo reale. Netdata è uno strumento open-source per il monitoraggio delle prestazioni e la risoluzione dei problemi di sistemi e applicazioni in tempo reale. Fornisce approfondimenti completi sulle prestazioni e sullo stato di salute di sistemi e applicazioni tramite visualizzazioni e metriche dettagliate. Netdata è progettato per essere leggero, veloce e facile da usare.

Netdata è abilitato di default su NethSecurity ed è accessibile dalla rete LAN. Per accedervi, andare alla pagina `Monitoraggio` e fare clic sul pulsante *Apri report* dalla scheda `Report in tempo reale`.

Le metriche di Netdata vengono salvate in RAM e saranno azzerate a ogni riavvio della macchina. Se il firewall è connesso al *controller remoto*, le metriche verranno memorizzate direttamente sul controller e saranno preservate anche dopo i riavvii.

8.1.8 Monitoraggio latenza del ping

Configurare lo strumento di monitoraggio per valutare il tempo di andata e ritorno (round-trip time) e la perdita di pacchetti trasmettendo messaggi ping agli host di rete. Questo strumento viene utilizzato per monitorare la qualità della connettività di rete. È possibile includere uno o più host da monitorare ed è anche possibile aggiungere indirizzi IP all'interno di una VPN per valutare la qualità del tunnel.

Per monitorare un nuovo host o indirizzo IP, fare clic sul pulsante *Aggiungi host* e inserire le informazioni richieste, quindi fare clic sul pulsante *Salva* per confermare le modifiche.

Le modifiche vengono applicate immediatamente. Per rimuovere un host dall'elenco, fare clic sull'icona di eliminazione.

È possibile visualizzare un grafico della latenza del ping accedendo a Netdata dalla pagina del report.

8.2 Storico monitoraggio

Subscription richiesta

Questa funzionalità è disponibile solo se il firewall e il controller dispongono di una subscription valida.

Se l'unità è stata collegata al controller prima che la subscription fosse attiva, lo storico del monitoraggio non verrà abilitato automaticamente. La pagina `Controller` mostrerà un messaggio che indica che il monitoraggio storico è disabilitato.

Per abilitarlo, seguire questi passaggi:

1. Disconnettere l'unità dal controller.
2. Assicurarsi che il NethServer 8 su cui è installato il controller disponga di una subscription valida.
3. Ricollegare l'unità al controller.

Consultare *controller metrics* per ulteriori informazioni.

8.3 Allarmi

Il sistema di allarmi sfrutta la potenza del motore Netdata per un monitoraggio e una segnalazione efficienti.

Il sistema di allarmi dà priorità solo a quegli allarmi che hanno il potenziale di interrompere o compromettere la funzionalità del firewall. Concentrandosi su indicatori critici, gli amministratori possono affrontare in modo efficiente i problemi che rappresentano una reale minaccia per la sicurezza e il funzionamento del firewall.

Se il server dispone di una *Subscription* valida, le notifiche di allerta vengono inviate automaticamente ai server remoti per il monitoraggio e la gestione centralizzata. Sia `my.nethesis.it` che `my.nethserver.com` fungono da hub centrali per la ricezione degli avvisi, consentendo agli amministratori di rimanere informati sullo stato del firewall e di rispondere tempestivamente a eventuali situazioni critiche.

Allarmi implementati:

- Spazio su disco: l'avviso relativo allo spazio su disco viene attivato quando lo spazio disponibile sul disco del sistema raggiunge un livello critico. Questa notifica proattiva aiuta a prevenire potenziali interruzioni affrontando i problemi di spazio su disco prima che possano influire sul funzionamento del firewall.
- Stato MultiWAN (Attivo/Non attivo): questo avviso notifica agli amministratori quando ci sono cambiamenti nello stato del MultiWAN, indicando se le connessioni sono attive o non attive. Una consapevolezza tempestiva dei cambiamenti di stato del MultiWAN è fondamentale per mantenere una connettività Internet continua e affidabile.

CAPITOLO 9

Netify Informatics

Netify Informatics è un servizio cloud di terze parti che utilizza l'analisi e l'intelligenza artificiale per convertire i metadati DPI locali ottenuti da NethSecurity in informazioni di rete di alto livello. La soluzione fornisce approfondimenti su vari aspetti dell'attività di rete, tra cui:

- Device Discovery
- Monitoraggio della larghezza di banda
- Analisi del Rischio e della Reputazione
- Regulatory Compliance
- Geolocalizzazione
- Audit e Forensics

Il servizio riceve dati da netifyd, il motore DPI di NethSecurity che è abilitato per impostazione predefinita sul firewall.

È possibile provare il servizio gratuitamente per 7 giorni. Al termine di questo periodo, si può scegliere il piano che meglio si adatta alle proprie esigenze.

Consultare Netify Informatics Pricing e Netify Informatics FAQ per ulteriori informazioni.

9.1 Prima di iniziare

Assicurarsi di creare un account sul sito web di Netify Informatics; è possibile provare il servizio gratuitamente per 7 giorni. Registrarsi qui: Netify Registration

È possibile gestire in modo granulare clienti diversi, sedi diverse dello stesso cliente e persino firewall diversi all'interno della stessa sede. La piattaforma è organizzata con questi elementi.

- **Organizzazione** : un'organizzazione è essenzialmente un cliente presso cui è presente almeno un firewall NethSecurity; sono supportate più organizzazioni.
- **Sito**: la stessa organizzazione (cliente) potrebbe avere un ufficio a Roma, Firenze e Parigi. Un sito è definito per ciascuna sede fisica per isolare i dati; sono supportati più siti.

- **Agente**: l'agente rappresenta l'unità NethSecurity del cliente. Netify supporta più agenti per sito. In una rete semplice, è probabile che un solo agente rilevi tutti i flussi di traffico sulla rete di un sito.

9.2 Collegare NethSecurity a Netify Informatics

Sono necessari due passaggi per utilizzare il servizio:

1. Abilitare l'invio dei metadati da NethSecurity
2. Effettuare il provisioning di un agente su Netify Informatics.

Avvertimento: È obbligatorio configurare prima l'invio dei dati su NethSecurity **e solo successivamente** effettuare il provisioning dell'agente sulla piattaforma.

9.2.1 1. Abilitare l'invio dei metadati

Accedere alla pagina `Netify Informatics` nella sezione `Monitoraggio` dell'interfaccia web di NethSecurity.

Abilitare l'opzione `Invia i metadati dei flussi di rete a Netify Informatics` e fare clic su `Salva`.

Ogni NethSecurity è associato a un UUID univoco dell'Agent, simile a questo *B3-GV-WQ-SD*. Il codice sarà visibile nella stessa pagina dopo aver abilitato l'opzione *Invia metadati*.

9.2.2 2. Effettuare il provisioning dell'agente

Una volta che si dispone di un account registrato e si è abilitato l'invio dei metadati su NethSecurity, è possibile effettuare il provisioning dell'agente sulla piattaforma Netify Informatics:

1. Copia il codice ottenuto nel passaggio precedente ed effettua l'accesso al sito web di Netify Informatics.
2. Accedere alla `Provision Agent Wizard` all'interno della sezione `Deployment`.
3. Seguire le istruzioni per creare l'organizzazione (il cliente) e incollare l'UUID dell'Agent nel campo appropriato per abilitare l'agent utilizzando il codice ottenuto su NethSecurity.

Da questo momento, Netify Informatics inizierà a mostrare i dati. È possibile quindi collegare altri firewall dello stesso cliente (stessa organizzazione, stesso sito o uno diverso) oppure creare una nuova organizzazione per un cliente differente.

9.3 Deployment Manager

La sezione `Deployment` all'interno di Netify Informatics consente di gestire Agent, Site e Organization. Mentre la gestione di Agent e Site è relativamente semplice, la sezione `Organization Access` permette di aggiungere ulteriori membri all'organizzazione. Questa funzionalità consente ad altri utenti di accedere al pannello Netify e visualizzare tutti i dati pertinenti.

Sono disponibili tre profili:

- Amministratore
- Manager
- Visualizzatore

Il profilo `Administrator`, tipicamente riservato ai colleghi all'interno della propria azienda, concede il livello più alto di permessi, consentendo di visualizzare, creare e modificare le configurazioni all'interno di Netify Informatics.

Il profilo `Manager` è dedicato agli individui che appartengono alla stessa organizzazione (l'azienda cliente). Consente di visualizzare tutte le sezioni all'interno di Netify Informatics, vedere la dashboard di distribuzione e modificare la sezione *Identity manager*, ma non permette di aggiungere altre organizzazioni o effettuare il provisioning di nuovi agent.

Il profilo `Viewer`, probabilmente il più comunemente utilizzato, è destinato a chi (ad esempio, un tecnico IT dell'organizzazione del cliente) può visualizzare tutti i dati all'interno della propria organizzazione ma non ha la possibilità di modificare alcuna configurazione di Netify.

Per invitare qualcuno, è sufficiente fare clic su `Manage Organization`, inserire il loro indirizzo email e scegliere il profilo desiderato. La persona riceverà un invito da Netify tramite email e potrà creare il proprio account.

Nota: Il tipo di profilo può essere modificato in qualsiasi momento da un amministratore, consentendo ad esempio di passare una persona da `Manager` a `Viewer`.

CAPITOLO 10

Subscription

Nethesis offre due tipi di servizi di abbonamento per NethSecurity, che forniscono vantaggi e funzionalità aggiuntive:

- **Subscription Community**: registrazione self-service principalmente adatta a consulenti IT. Per ulteriori informazioni, consultare la pagina piani di abbonamento.

  Il portale di sottoscrizione della community è disponibile su my.nethserver.com

- **Subscription Enterprise**: servizio riservato ai rivenditori Nethesis, si prega di contattare il reparto vendite.

  Il portale di sottoscrizione Enterprise è disponibile all'indirizzo: my.nethesis.it

I vantaggi tipici del servizio in abbonamento includono:

- **Portali di monitoraggio**: gli abbonati possono accedere ai portali di monitoraggio per gestire il proprio abbonamento e ricevere *avvisi* per i server registrati.
- **Firme DPI avanzate**: i firewall con un abbonamento valido hanno accesso a un database molto più ampio di *firme DPI* (oltre 1820 in totale invece di 415) che vengono aggiornate regolarmente.
- **Enterprise Block lists**: I firewall con un abbonamento valido possono acquistare blocklist IP e DNS di alta qualità. Queste liste sono attivamente mantenute, aggiornate molto frequentemente e offrono un'elevata efficacia generando un numero molto basso di falsi positivi; possono essere utilizzate nelle *block list IP* e *block list DNS*.
- **Backup remoto automatico**: gli abbonati possono beneficiare di backup remoti automatici della configurazione del firewall. Questa funzionalità è fondamentale per le aziende che devono garantire la sicurezza dei propri dati e delle configurazioni.
- **Supporto**: gli abbonati possono ricevere supporto prioritario sulle release stabili. Questo può essere fondamentale per le aziende che si affidano a NethSecurity per le proprie operazioni. Vedere anche *Supporto remoto*.
- **Consulenza e personalizzazione**: gli abbonati possono usufruire di servizi di consulenza e assistenza per la personalizzazione, al fine di adattare le funzionalità del server alle specifiche esigenze aziendali.

È importante notare che, sebbene un abbonamento possa non essere necessario per l'uso normale, le aziende con esigenze specifiche o che cercano supporto e funzionalità aggiuntive potrebbero trovare vantaggioso sottoscrivere l'offerta NethSecurity.

10.1 Registrare il sistema

Per registrare il sistema, seguire i passaggi riportati di seguito:

- Accedere al portale Enterprise o Community, aggiungere un nuovo server e copiare il token
- Accedere al firewall e andare alla pagina `Subscription`
- Incollare il token nel campo `Token di autenticazione`
- Fare clic sul pulsante *Registra*

Il sistema si registrerà automaticamente al portale Enterprise o Community corretto.

Si noti che il processo di registrazione richiede una connessione internet attiva.

10.2 Rimuovere l'abbonamento

Quando l'abbonamento scade, o al termine di un periodo di prova, fare clic sul pulsante *Annulla registrazione*.

CAPITOLO 11

Supporto remoto

È necessaria una subscription Enterprise

Questa funzionalità è disponibile solo se il firewall dispone di un abbonamento Enterprise valido.

L'abbonamento *Enterprise* consente di accedere al supporto remoto Nethesis.

La sessione di supporto remoto collegherà il firewall ad una istanza di WindMill ospitato da Nethesis su `sos.nethesis.it`. Il firewall deve poter connettersi all'host sopra indicato sulla porta `1194` UDP. Se la porta `1194` è chiusa, il sistema tenterà di utilizzare come alternativa la porta `443` TCP.

11.1 Gestione delle sessioni

Il supporto remoto deve essere avviato e interrotto dall'amministratore del firewall.

11.1.1 Avvio di una sessione

Per avviare una sessione:

- Accedere alla pagina `Subscription` e andare alla sezione `Supporto remoto`
- fare clic sul pulsante *Avvia sessione*
- Copiare `ID sessione` e condividerlo con il team di supporto.
- la sessione sarà attiva per 24 ore per impostazione predefinita

Il sistema visualizzerà:

- Lo stato attuale della sessione (attiva/inattiva)
- Il tempo di scadenza della sessione
- Il tempo rimanente fino alla scadenza

È possibile visualizzare queste informazioni in qualsiasi momento nella sezione `Supporto remoto` della pagina `Subscription`.

11.1.2 Scadenza della sessione

Le sessioni di supporto remoto presentano il seguente comportamento di scadenza:

- **Sessione predefinita**: scade dopo 24 ore
- **Sessione estesa**: scade dopo 7 giorni dall'ora dell'estensione

Il sistema monitora continuamente la scadenza delle sessioni:

- un processo cron viene eseguito ogni 10 minuti per verificare la presenza di sessioni scadute
- quando una sessione scade, viene automaticamente interrotta
- gli eventi di scadenza della sessione vengono registrati nel registro di sistema

11.1.3 Terminazione di una sessione

Per terminare manualmente una sessione attiva prima della sua scadenza:

- Accedere alla pagina `Subscription` e andare alla sezione `Supporto remoto`
- fare clic sul pulsante *Termina sessione*
- la connessione di supporto remoto verrà immediatamente chiusa

11.2 Interfaccia a riga di comando

Il comando `don` richiede privilegi di root e registra tutte le operazioni nel log di sistema.

Avvia una sessione:

```
don start
```

Questo avvierà una nuova sessione di supporto remoto con una scadenza di 24 ore.

Verificare lo stato della sessione:

```
don status
```

Questo visualizza le informazioni sulla sessione corrente, inclusi:

- ID server
- ID sessione
- Tempo rimanente fino alla scadenza

Estendere una sessione attiva:

```
don extend
```

Importante: L'estensione della sessione è disponibile solo tramite riga di comando. Questa funzionalità estende la sessione dalla durata predefinita di 24 ore a 7 giorni a partire dall'ora corrente.

Interrompere una sessione:

```
don stop
```

Questo termina immediatamente la sessione di supporto remoto e libera tutte le risorse.

Verificare le sessioni scadute:

```
don expire
```

Questo comando viene eseguito automaticamente da cron ogni ora per verificare se la sessione è scaduta. Se la sessione è scaduta, verrà automaticamente interrotta.

Esempi di log:

```
Mar 27 09:24:37 NethSec don: Remote support session started
Mar 27 09:24:54 NethSec don: Remote support session extended by 7 days
Mar 27 09:25:04 NethSec don: Remote support session stopped
```

CAPITOLO 12

Backup e ripristino

NethSecurity offre un sistema di backup flessibile e potente per salvare e ripristinare le impostazioni di configurazione del firewall.

Accedere alla pagina `Backup & Restore` nella sezione `Sistema`, quindi fare clic sul pulsante *Scarica backup*. Se la macchina dispone di un abbonamento Enterprise valido, il backup è *automatico*.

Il backup include tutti i file di configurazione rilevanti e anche l'elenco dei pacchetti aggiuntivi installati dall'utente. L'elenco viene salvato nel file `/etc/backup/installed_packages.txt`.

12.1 Backup

NethSecurity consente la creazione di backup sia cifrati che non cifrati. È sempre possibile scaricare un backup non cifrato facendo clic sul pulsante *Scarica non cifrato*.

Per consentire il download di un backup cifrato, prima fare clic sul pulsante *Configura passphrase* e impostare una password robusta. Successivamente, il pulsante *Scarica cifrato* diventerà attivo.

Nota: Se il backup è crittografato e la password viene persa, non sarà più possibile ripristinare la configurazione.

Per disabilitare i backup crittografati, fare clic sul pulsante *Rimuovi passphrase* e il pulsante *Scarica cifrato* diventerà inattivo.

12.2 Ripristina

Il backup può essere ripristinato dalla scheda `Ripristino` all'interno della pagina `Backup & Restore`. È possibile avviare il processo di ripristino facendo clic sul pulsante *Ripristina backup* e caricando il file di backup. Se la macchina dispone di un abbonamento Enterprise valido, l'interfaccia web presenterà inoltre un elenco di backup disponibili dal server remoto. Se il backup è crittografato, inserire la passphrase e, infine, fare clic sul pulsante *Ripristino* per completare il processo.

Dopo il ripristino il sistema verrà riavviato.

Nota: A partire dalla versione 8.7.2, i pacchetti extra vengono reinstallati automaticamente dopo l'aggiornamento del sistema. Per le versioni precedenti e per ulteriori informazioni, consultare questa documentazione: *Ripristinare pacchetti aggiuntivi*.

12.3 Macchine con un abbonamento

Abbonamento richiesto

Questa funzionalità è disponibile solo se il firewall dispone di un abbonamento valido.

I backup si comportano in modo diverso sui dispositivi con un *abbonamento* attivo.

I backup non cifrati possono comunque essere scaricati direttamente dall'interfaccia di NethSecurity facendo clic sul pulsante *Scarica non cifrato*.

I backup crittografati sono archiviati nel cloud e integrati con il Nethesis Operation Center: questo approccio semplifica la gestione dei backup e il processo di ripristino per i dispositivi basati su abbonamento, che possono interagire direttamente con l'Operation Center e scaricare automaticamente il backup durante il ripristino.

Per abilitare i backup cloud crittografati, è necessario prima configurare una passphrase facendo clic sul pulsante *Configura passphrase* e impostando una password sicura. Una volta impostata la passphrase, è possibile:

- Fare clic sul pulsante *Esegui cloud backup* per creare immediatamente un backup
- Lascia che il sistema crei automaticamente un backup ogni notte

Ogni backup crittografato verrà inviato direttamente al Nethesis Operation Center tramite un canale sicuro. Si noti che la data del backup corrisponde alla data del server. Le date visualizzate nell'elenco dei backup si basano sull'orario del server che memorizza i backup, e non sull'orario del firewall che li ha creati. Questo significa che le date potrebbero differire a seconda delle differenze di fuso orario.

Avvertimento: I backup cloud senza crittografia sono stati deprecati. Per un periodo di tempo limitato, i backup verranno comunque inviati al cloud anche se non sono crittografati. In futuro, solo i backup crittografati verranno inviati al server remoto. Se si dispone di un abbonamento valido, abilitare la crittografia per garantire la sicurezza del backup. Consultare anche *Avviso di crittografia del backup* per ulteriori informazioni.

12.3.1 Avviso di crittografia del backup

Non crittografare il backup rappresenta un rischio per la sicurezza. Se il backup non è crittografato, chiunque abbia accesso al file di backup può leggere le impostazioni di configurazione memorizzate al suo interno.

Ogni notte uno script controllerà se il backup è cifrato. Se il backup non è cifrato, lo script creerà un avviso all'interno del portale remoto my.nethesis.it o my.nethserver.com. Per risolvere l'avviso, è necessario abilitare la cifratura facendo clic sul pulsante *Configura passphrase* e impostando una password robusta. L'avviso verrà risolto automaticamente durante il job cron notturno.

Per disabilitare l'avviso, accedere alla shell ed eseguire:

```
uci set ns-plug.config.backup_alert_disabled=1
uci commit ns-plug
```

La disattivazione dell'avviso comporterà errori silenziosi quando l'invio di backup non crittografati verrà bloccato in futuro. L'amministratore non verrà notificato di questi errori, il che potrebbe portare a problemi di backup non rilevati.

12.4 Personalizzazione del backup

Il backup include tutti i file di configurazione rilevanti. Per elencare i file inclusi nel backup, eseguire il seguente comando:

```
sysupgrade -l
```

Il backup può essere personalizzato aggiungendo file all'elenco di backup. Basta aggiungere una nuova riga al file `/etc/sysupgrade.conf` con il percorso del file da includere nel backup.

Esempio:

```
echo /etc/myfile >> /etc/sysupgrade.conf
```

12.5 Come decrittare un backup

Normalmente, i backup crittografati vengono gestiti direttamente da NethSecurity sia durante la fase di creazione che durante quella di ripristino. Una volta fornita la passphrase, il sistema cripta o decripta automaticamente il file.

In alcuni casi, tuttavia, può essere utile decriptare il backup esternamente (al di fuori del firewall) per eseguire controlli prima di ripristinarlo. Per questo motivo, è possibile utilizzare il seguente comando `gpg` per decriptare il contenuto del backup:

```
gpg --decrypt --passphrase $YOUR_PASSPHRASE --output unencrypted-file.tar.gz --yes $YOUR_
↪ENCRYPTED_BACKUP_FILE
```

CAPITOLO 13

Aggiornamenti

NethSecurity consente due tipi di aggiornamenti, entrambi disponibili dalla sezione `Aggiorna` nel menu `Sistema`:

- aggiornamenti normali per correzioni di bug e patch di sicurezza
- aggiornamenti di sistema per passare a una versione diversa

13.1 Correzioni di bug e di sicurezza

Questi aggiornamenti sono destinati ad aggiornamenti minori e correzioni di bug.

Tipicamente potrebbero essere eseguiti automaticamente, ma in qualsiasi momento è possibile verificare la presenza di nuovi aggiornamenti disponibili facendo clic sul pulsante *Verifica correzioni*. Questi aggiornamenti non richiedono il riavvio di NethSecurity, sono legati a una versione specifica e distribuiti tramite pacchetti.

Quando si utilizza questo metodo, la versione dell'immagine visualizzata all'interno della dashboard non cambia, ma il sistema viene aggiornato con le ultime correzioni.

13.2 Aggiornamenti di sistema

Questi tipi di aggiornamenti comportano la transizione a una nuova versione del firmware che introduce nuove funzionalità, miglioramenti e un supporto hardware più ampio.

Questo tipo di aggiornamento riavvierà il dispositivo (che quindi non sarà raggiungibile per alcune decine di secondi) e poi riscriverà completamente il firmware, preservando tutte le configurazioni. Tuttavia, si consiglia di salvare un backup della configurazione prima di procedere con l'aggiornamento.

Se è disponibile una nuova versione, l'interfaccia utente mostrerà un banner informativo e un pulsante dedicato *Aggiorna sistema* che permetterà di eseguire l'aggiornamento.

In alternativa, è sempre possibile caricare manualmente un'immagine compatibile utilizzando il pulsante *Aggiorna con file immagine* e procedere con l'aggiornamento.

Aggiornamento da riga di comando

È inoltre possibile eseguire un `Aggiornamento di sistema` dalla riga di comando. Per farlo, è sufficiente scaricare il nuovo file immagine; si consiglia di salvarlo all'interno della directory `/tmp`. Successivamente, eseguire il seguente comando:

```
sysupgrade -k -v nethsecurity-<version>-x86-64-generic-squashfs-combined.img.gz
```

Il comando `sysupgrade` scrive il nuovo file immagine sul dispositivo.

13.2.1 Ripristinare pacchetti aggiuntivi

A partire dalla versione 8.7.2, i pacchetti aggiuntivi vengono reinstallati automaticamente dopo l'aggiornamento del sistema. Si noti che la procedura di reinstallazione richiede l'accesso a Internet. In caso di errore, procedere con il ripristino manuale documentato di seguito. Consultare la sezione successiva per le versioni precedenti.

Dopo l'aggiornamento, è possibile eseguire il seguente comando per elencare tutti i pacchetti aggiuntivi:

```
grep overlay /etc/backup/installed_packages.txt
```

Questo comando restituisce tutti i pacchetti extra, consentendo di verificare quali sono installati e presenti sul sistema.

Ripristinare manualmente i pacchetti aggiuntivi

Questa procedura manuale è necessaria solo per le versioni precedenti alla 8.7.2 o se la procedura di reinstallazione automatica non va a buon fine.

Durante l'aggiornamento, il sistema viene completamente riscritto e tutti i pacchetti aggiuntivi installati dall'utente andranno persi. Tuttavia, l'elenco dei pacchetti installati viene salvato nel backup della configurazione, consentendone il ripristino dopo l'aggiornamento.

Dopo l'aggiornamento, assicurarsi che il sistema abbia accesso a Internet, quindi ripristinare i pacchetti precedentemente installati utilizzando i seguenti comandi:

```
opkg update
grep -E '\w+\s+overlay$' /etc/backup/installed_packages.txt | awk '{print $1}' | xargs␣
↪opkg install
```

13.3 Aggiornamenti automatici dei pacchetti

Subscription richiesta

Questa funzionalità è disponibile solo se il firewall dispone di una subscription valida.

Gli aggiornamenti automatici per i pacchetti possono essere abilitati dalla sezione `Aggiorna` nel menu `Sistema`, attivando l'opzione `Aggiornamenti automatici`. Gli aggiornamenti vengono verificati quotidianamente e, se disponibili, vengono scaricati e installati automaticamente.

CAPITOLO 14

Storage

A partire dalla versione 8.6, NethSecurity salva automaticamente i log di sistema su una partizione di storage persistente nelle installazioni bare metal (*fare riferimento alla sezione dedicata qui sotto per le macchine virtuali*).

Questo garantisce che i log rimangano disponibili anche dopo riavvii o arresti imprevisti, anche se lo storage non è stato configurato manualmente. Il periodo di conservazione dei log predefinito è di 52 settimane.

Per **nuove installazioni** il sistema crea automaticamente una partizione dedicata sul disco principale per memorizzare i log.

Per **gli aggiornamenti**:

- se non è stato precedentemente configurato alcun storage, il sistema lo imposta automaticamente utilizzando lo spazio non allocato sul disco principale
- se lo storage era già stato configurato, rimane invariato

Nota: Questo comportamento migliora l'affidabilità e non richiede interventi manuali. Tuttavia, è comunque possibile gestire le impostazioni di archiviazione dall'interfaccia web.

L'archiviazione persistente dei log può essere disabilitata (non raccomandato), oppure spostata su un disco diverso se necessario. Se disabilitata, il sistema la riconfigurerà automaticamente durante un futuro aggiornamento.

14.1 Configurazione manuale

La configurazione manuale dello storage aggiuntivo è ancora disponibile e funziona come segue:

- Se si utilizza un dispositivo aggiuntivo, collegarlo al sistema.
- Accedere alla pagina `Storage` nella sezione `Sistema` nel menu a destra.
- Selezionare il dispositivo di archiviazione su cui devono essere salvati i log.
- Fare clic sul pulsante *Formatta e configura lo storage*.

- Se il dispositivo selezionato è il **disco primario**, il sistema genererà una nuova partizione utilizzando qualsiasi spazio non allocato.
- Se viene selezionato un **disco aggiuntivo**, il sistema cancellerà tutte le partizioni e i dati esistenti e creerà una nuova partizione singola.

Lo storage è quindi:

- Formattato con il filesystem `ext4`
- Montato in `/mnt/data`
- Utilizzato da `rsyslog` per scrivere i log in `/mnt/data/log/messages`. Per ulteriori dettagli, vedere *Rotazione dei log di storage*.
- Sincronizzato quotidianamente (di notte) per dati aggiuntivi come le metriche

Per rimuovere lo storage persistente e tornare al logging in memoria, fare clic sul pulsante *Rimuovi storage*.

14.1.1 Macchine Virtuali

Quando si installa NethSecurity su una macchina virtuale, il metodo raccomandato è generare il disco virtuale dall'immagine ufficiale. In questa modalità, i log non vengono memorizzati in modo persistente per impostazione predefinita. Per abilitare la memorizzazione persistente dei log, è necessario collegare un secondo disco virtuale alla macchina virtuale. In alternativa, è possibile estendere il disco virtuale e utilizzare lo spazio libero su disco per creare una nuova partizione come su un hardware fisico.

14.1.2 Comportamento nelle versioni precedenti alla 8.6

Nelle versioni precedenti di NethSecurity, i log venivano scritti per impostazione predefinita in una **directory volatile in memoria**. Per rendere persistenti i log, era necessario configurare lo storage **manualmente**, utilizzando lo spazio non allocato sul disco di sistema oppure collegando un disco secondario.

Risoluzione dei problemi

In alcune circostanze, potrebbero verificarsi difficoltà nell'utilizzo del disco principale per l'archiviazione dei log, poiché l'interfaccia utente potrebbe non presentare alcuna opzione. In questi casi, il problema deriva solitamente dalla presenza di una partizione preesistente sul disco, che deve essere rimossa preventivamente per garantirne il corretto utilizzo da parte del sistema.

Questo si verifica tipicamente anche dopo aver eseguito un ripristino alle impostazioni predefinite utilizzando la modalità failsafe (che non rimuove la partizione dei log); per consentire al sistema di utilizzare nuovamente lo storage per salvare nuovi log è necessario rimuovere la vecchia partizione.

Questo può essere fatto facilmente in questo modo.

- Verificare se la partizione di log è presente con il comando:

`parted /dev/sda print`:

```
root@NethSec:~# parted /dev/sda print
Model: ATA Hoodisk SSD (scsi)
Disk /dev/sda: 32.0GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:
```

(continues on next page)

(continua dalla pagina precedente)

```
Number  Start   End     Size    File system  Name  Flags
128     17.4kB  262kB   245kB                      bios_grub
 1      262kB   17.0MB  16.8MB  fat16              legacy_boot
 2      17.0MB  332MB   315MB
 3      512MB   32.0GB  31.5GB  ext2
```

La partizione 3 è quella utilizzata per i log.

- per rimuovere la partizione 3 eseguire il comando:

```
parted /dev/sda rm 3
```

- Ora verificare nuovamente la tabella delle partizioni con il comando:

```
parted /dev/sda print
```

La partizione 3 non dovrebbe essere visibile.

Ora lo storage è pronto per essere configurato per i log dall'interfaccia Web.

CAPITOLO 15

Factory reset

NethSecurity offre diverse opzioni per reimpostare il firewall e ripristinarne la funzionalità:

- *Ripristino delle impostazioni di fabbrica*: scegliendo questo metodo vengono cancellati tutti i pacchetti installati e le impostazioni personalizzate, riportando il firewall allo stato originale come dopo l'installazione di NethSecurity.
- *Modalità failsafe*: questa opzione è utile se si è perso il controllo del dispositivo, rendendolo inaccessibile a causa di un errore di configurazione. La modalità failsafe consente di riavviare il firewall in uno stato operativo di base, mantenendo la maggior parte dei pacchetti e delle impostazioni.
- *Modalità di ripristino*: se il firmware del firewall si danneggia, la modalità di ripristino viene in soccorso. Consente di installare un nuovo firmware e di ripristinare una macchina non funzionante.

15.1 Factory reset

In NethSecurity, un ripristino alle impostazioni di fabbrica si riferisce al processo di riportare il dispositivo firewall alle impostazioni e configurazioni originali, come quando è stato installato per la prima volta. Questa procedura cancella tutte le impostazioni personalizzate, le configurazioni, i pacchetti installati e i dati utente presenti sul dispositivo, riportandolo di fatto a uno stato iniziale.

Questa procedura si basa sul completamento del processo di boot. Se il ripristino delle impostazioni di fabbrica non funziona, si consiglia di utilizzare la modalità failsafe.

Per iniziare da zero senza reinstallare il firmware, accedere alla pagina `Factory reset` nella sezione `Sistema`. Fare clic sul pulsante *Esegui factory reset* per ripristinare il firewall allo stato originale. Il processo di factory reset richiederà alcuni secondi per essere completato. Una volta terminato il processo, il firewall si riavvierà automaticamente.

Il ripristino alle impostazioni di fabbrica reinstalla la versione attualmente installata. Ad esempio, se il firewall è stato inizialmente installato con la versione 23.05.0 e poi aggiornato alla 23.05.1, dopo il ripristino alle impostazioni di fabbrica si avrà un'installazione pulita della versione 23.05.1.

Se lo storage su cui è in esecuzione NethSecurity è stato configurato con una partizione per salvare i log, il comando `Factory reset` eseguito dall'interfaccia Web rimuoverà anche la partizione dei log e tutti i suoi dati.

Nota: Se NethSecurity è stato installato tramite una migrazione in-place da NethServer 7, il ripristino alle impostazioni di fabbrica non ripristinerà la configurazione predefinita. Invece, il sistema verrà riavviato con tutte le configurazioni migrate da NethServer 7.

Se si preferisce un nuovo inizio, è possibile procedere con una nuova *installazione* invece di utilizzare il ripristino delle impostazioni di fabbrica.

In alternativa, è possibile seguire questi passaggi:

- Aggiornare NethSecurity con una nuova immagine (se presente) oppure utilizzando un'immagine standard scaricata da *downloading*. Questa operazione sovrascriverà la ROM di NethSecurity con una versione standard, rimuovendo eventuali file di migrazione.
- Ora è possibile eseguire il ripristino alle impostazioni di fabbrica, che porterà a una nuova partenza pulita.

Se si desidera eseguire il ripristino alle impostazioni di fabbrica da riga di comando, è sufficiente eseguire il seguente comando.

```
/usr/libexec/rpcd/ns.factoryreset call reset
```

15.2 Modalità failsafe

NethSecurity fornisce una modalità failsafe che può sovrascrivere la configurazione corrente del dispositivo. Se il dispositivo diventa inaccessibile a causa di un errore di configurazione, la modalità failsafe interviene in soccorso. Quando si avvia il dispositivo in modalità failsafe, esso si inizializza in uno stato operativo di base, utilizzando un insieme di valori predefiniti, permettendo di risolvere manualmente il problema.

Tuttavia, è importante notare che la modalità failsafe non può risolvere problemi più complessi come hardware difettoso o un kernel danneggiato. Sebbene assomigli a un ripristino, la modalità failsafe consente di accedere al dispositivo e ripristinare le impostazioni se necessario, mentre un ripristino cancellerebbe semplicemente tutte le configurazioni.

Il modo più semplice per attivare la modalità failsafe è collegarsi direttamente al firewall utilizzando un monitor VGA/HDMI o un cavo seriale. Per farlo, avviare la macchina, attendere che appaia il menu di avvio Grub e selezionare `NethSecurity (failsafe)`.

È possibile accedere direttamente al firewall tramite la porta seriale utilizzando un cavo null-modem e un comune programma terminale. Per Windows, è possibile utilizzare `PuTTY` versione 0.60 o superiore. Per Linux, le opzioni includono `minicom` e `picocom`. Impostare la velocità di trasmissione (baud rate) a 115200, i bit di dati a 8, la parità su Nessuna e i bit di stop a 1 (abbreviato come 8N1).

Dopo l'accesso alla modalità failsafe, il firewall si avvierà con l'indirizzo di rete 192.168.1.1/24, solitamente sull'interfaccia di rete eth0, e saranno operativi solo i servizi essenziali. È importante notare che il server DHCP sarà inattivo in modalità failsafe. Seguire le istruzioni visualizzate sullo schermo per montare il filesystem root e accedere ad altre utilità secondo necessità.

Se si desidera eseguire il ripristino alle impostazioni di fabbrica in modalità failsafe, è sufficiente eseguire i seguenti comandi.

```
firstboot -y && reboot
```

Nota: Questo comando non eliminerà la partizione di log dal disco se esiste. Se è necessario eliminare la vecchia partizione, fare riferimento alla *Storage* per maggiori dettagli.

15.3 Recupero di emergenza

Il ripristino d'emergenza in NethSecurity, noto anche come unbricking, è una funzionalità che consente di ripristinare il dispositivo firewall in caso di malfunzionamenti gravi. L'unbricking garantisce che anche i problemi più critici possano essere risolti, riportando il dispositivo alla piena funzionalità, salvo guasti hardware.

Se si ha ancora accesso al sistema, è possibile utilizzare i seguenti comandi per scaricare e scrivere l'immagine:

```
ns-download -l
```

Questo comando visualizzerà il percorso dell'immagine scaricata. Utilizzare questo percorso nel comando seguente:

```
sysupgrade -n <download_image_path>
```

Se non è possibile accedere al sistema, *scaricare l'immagine più recente*, quindi seguire le *istruzioni di installazione* per scrivere direttamente l'immagine sul supporto di memorizzazione.

CAPITOLO 16

Controller

Il controller NethSecurity è un'applicazione che può essere eseguita su NethServer 8 (NS8). Il controller consente il controllo remoto di più installazioni NethSecurity, chiamate unità.

Il firewall può funzionare in modo indipendente senza la necessità del controller. Il controller è un componente opzionale che fornisce funzionalità aggiuntive di gestione e monitoraggio per il firewall.

Il controller crea una connessione sicura tra il server centrale e le unità. Ogni firewall si registra presso il server utilizzando un client chiamato ns-plug. Una volta registrato, il server genera una configurazione VPN che viene inviata al firewall. La VPN consente una comunicazione sicura tra il controller e l'unità.

Funzionalità principali:

- **Gestione centralizzata**: Gestire più firewall da un unico server.
- **Comunicazione sicura**: Stabilire una connessione OpenVPN sicura tra il server e i firewall.
- **Configurazione semplice**: Configurare i firewall direttamente dall'interfaccia utente del controller.
- **Monitoraggio e registrazione**: Raccogliere e analizzare i log dai firewall all'interno di Loki per scopi di risoluzione dei problemi e monitoraggio.
- **Visualizzazione delle metriche**: Visualizzare le metriche dai firewall utilizzando la dashboard integrata di Grafana. Le metriche vengono raccolte tramite Prometheus e TimescaleDB.
- **Accesso SSH via web**: Accedere all'interfaccia a riga di comando del firewall utilizzando un client SSH basato su web.

16.1 Installazione e configurazione

Il controller può essere installato su un sistema NethServer 8 dal Software Center. Il modulo si chiama `NethSecurity Controller`.

Dopo l'installazione, è necessario configurare il controller. La configurazione può essere effettuata utilizzando l'interfaccia web di NethServer 8. È necessario impostare i seguenti parametri:

- *Controller hostname*: Il nome di dominio completo per il controller, ad esempio: `mycontroller.nethsecurity.org`. Assicurarsi che il nome host sia risolvibile e raggiungibile dalle unità.
- *Let's Encrypt certificate*: Abilitare o disabilitare il certificato Let's Encrypt per l'interfaccia web del controller. Si consiglia di abilitarlo.
- *VPN network* e *VPN netmask*: la rete e la netmask di OpenVPN. Quando si sceglie la rete, assicurarsi che non si sovrapponga alle reti esistenti all'interno di tutte le unità che saranno collegate al controller. Utilizzare solo reti di classe C come `192.168.7.0` con netmask `255.255.255.0`.
- *Utente amministratore*: Il nome utente dell'amministratore del controller. L'utente amministratore è l'unico utente che può creare e gestire altri utenti all'interno del controller. Lo stesso nome utente viene utilizzato per accedere all'interfaccia Grafana.
- *Password amministratore*: Scegliere una password robusta per l'utente amministratore. Si noti che la password predefinita viene visualizzata solo una volta; conservarla in un luogo sicuro. La stessa password viene utilizzata per accedere all'interfaccia di Grafana. Per motivi di sicurezza, è consigliabile cambiare la password dopo il primo accesso sia per il controller che per l'interfaccia Grafana.

I seguenti parametri sono opzionali:

- *Nome del controller*: Il nome del controller, utilizzato per creare l'autorità di certificazione VPN. È possibile lasciarlo invariato a meno che non vi sia un requisito specifico.
- *Conservazione dei log*: Il periodo di conservazione dei log in giorni, il valore predefinito è 180 giorni. Si applica ai log memorizzati in Loki.
- *Conservazione delle metriche*: Il periodo di conservazione delle metriche in giorni, predefinito a 15 giorni. Si applica alle metriche memorizzate in Prometheus e Timescale.
- *MaxMind license key*: Il controller può geolocalizzare gli indirizzi IP dei client VPN connessi e degli aggressori. Una mappa con la posizione dei client e degli aggressori verrà visualizzata all'interno di Grafana. La chiave di licenza è necessaria per abilitare la funzionalità e scaricare il database MaxMind GeoIP2. Per ottenere una chiave di licenza gratuita, registrarsi sul sito web di MaxMind, quindi accedere alla pagina *Manage License Keys* nella sezione dell'account. Generare una nuova licenza, copiare la chiave di licenza e incollarla nel campo.
- *IP consentiti*: L'elenco degli indirizzi IP o intervalli CIDR che sono autorizzati ad accedere all'interfaccia web del controller. Per impostazione predefinita, l'elenco è vuoto, il che significa che l'accesso è consentito da tutti gli indirizzi IP. È possibile limitare l'accesso a IP o reti specifiche per motivi di sicurezza. Quando abilitato, solo l'endpoint di registrazione (ad es. `https://controller.nethserver.org/api/register`) sarà accessibile dalle unità, consentendo loro di registrarsi presso il controller. Tutto il traffico restante tra il controller e le unità verrà instradato attraverso la connessione VPN. Questa funzionalità richiede la versione 8.6 o successiva dell'unità.

Dopo aver completato la configurazione, il controller è pronto per essere utilizzato e può essere accessibile tramite un browser web all'hostname configurato, ad esempio `https://mycontroller.nethsecurity.org`.

Nota: Per garantire il corretto funzionamento, il controller deve essere accessibile tramite la rete su porte specifiche.

- `Porta TCP 443 (HTTPS)` per accedere alla WebUI e consentire la comunicazione delle unità.

- `Una porta UDP allocata dinamicamente` aperta da NethServer 8 e utilizzata per le connessioni VPN dalle unità; questa porta viene generata casualmente durante la configurazione.

Il numero effettivo della `porta UDP` può essere trovato nella pagina di stato del modulo Controller, nella sezione `OpenVPN UDP Port`. Assicurarsi che queste porte siano aperte su qualsiasi firewall che protegge il nodo su cui è in esecuzione il controller.

16.2 Utenti

Il controller ha due tipi di utenti:

- **Utenti amministratori**: Gli utenti amministratori sono gli unici che possono creare e gestire gli utenti all'interno del controller. Gli utenti amministratori possono inoltre accedere a tutte le unità.
- **Utente standard**: Gli utenti standard possono gestire le unità e le configurazioni del firewall. Questi utenti devono essere associati a un gruppo di unità: potranno accedere solo alle unità associate al proprio gruppo. Se un utente non è associato a nessun gruppo, non avrà accesso ad alcuna unità. Consultare *Gruppi di unità* per ulteriori informazioni sui gruppi di unità.

Un utente amministratore viene creato durante la configurazione del controller dall'interfaccia web di NethServer 8. L'utente amministratore può creare e gestire altri utenti dall'interfaccia web del controller. Un utente può essere associato a un gruppo di unità dall'interfaccia web del controller, all'interno della pagina di gestione utenti.

Si consiglia di creare un utente per ogni persona che necessita di accesso al controller. Quando si crea un nuovo utente, l'amministratore deve specificare il nome utente, il nome visualizzato dell'utente e la password dell'utente. Il nome utente viene utilizzato per accedere al controller, mentre il nome visualizzato viene utilizzato per identificare l'utente nel controller.

L'amministratore può anche:

- reimpostare la password dell'utente ed eliminare gli utenti
- promuovere un utente ad amministratore
- eliminare un account utente

Dopo aver effettuato l'accesso, ogni utente dovrebbe cambiare la propria password e generare una coppia di chiavi SSH per accedere alle unità.

16.2.1 Autenticazione a due fattori (2FA)

Ogni utente del controller può abilitare l'Autenticazione a Due Fattori (2FA) per aumentare la sicurezza dell'account. Per abilitare la 2FA, seguire gli stessi passaggi documentati all'interno dell'interfaccia web del firewall: *Interfaccia utente NethSecurity 2FA*.

L'amministratore può visualizzare lo stato 2FA di ciascun utente all'interno dell'elenco utenti.

Reimpostazione 2FA

Se un amministratore del controller ha perso l'accesso al proprio dispositivo OTP e non riesce ad effettuare l'accesso, la 2FA può essere reimpostata dal nodo NethServer 8 cancellando direttamente i campi `otp_secret` e `otp_recovery_codes` nel database del controller.

Eseguire i seguenti comandi sul nodo NethServer 8, sostituendo `nethsecurity-controller1` con il nome effettivo dell'istanza del modulo controller e `admin` con il nome utente interessato:

```
runagent -m nethsecurity-controller1
source db.env; podman exec -it timescale psql -U "${POSTGRES_USER}" -p "${POSTGRES_PORT}
↪" \
  -c "UPDATE accounts SET otp_recovery_codes='', otp_secret='' WHERE username = 'admin';"
```

Dopo che la query è stata completata, l'utente può accedere utilizzando solo la propria password e ri-registrare un nuovo dispositivo OTP dall'interfaccia utente del controller.

16.3 Unità

Tutti gli utenti possono gestire le unità. Un'unità è un firewall gestito dal controller.

Per collegare una nuova unità al controller, è necessario fare clic sul pulsante *Aggiungi unità* dall'interfaccia web del controller. Quando viene aggiunta una nuova unità, il controller esegue le seguenti azioni:

- crea un identificatore univoco per l'unità
- assegna un indirizzo IP all'interno della rete VPN
- genera una configurazione VPN inclusi i certificati
- memorizza in modo sicuro le credenziali necessarie per accedere al firewall remoto

Un codice di accesso verrà generato e visualizzato sullo schermo. Il codice di accesso deve essere inserito sull'unità per stabilire la connessione con il controller.

Accedere alla pagina `Controller` all'interno dell'interfaccia web dell'unità ed inserire il codice di join nel campo `Join code`. Durante la procedura di join al controller, l'unità scaricherà la configurazione VPN e stabilirà una connessione sicura con il controller. Se la connessione avviene con successo, l'unità verrà visualizzata nell'interfaccia web del controller con lo stato `Connesso`.

Si noti che, se il controller non dispone di un certificato Let's Encrypt valido, sarà necessario disabilitare l'opzione `Verifica certificato TLS` nella configurazione dell'unità.

Quando l'unità è collegata, è possibile accedere all'interfaccia web dell'unità facendo clic sul collegamento *Apri unità* senza dover inserire le credenziali dell'unità.

Nota: L'interfaccia utente dell'unità *deve ascoltare sulla porta 9090* per consentire al controller di accedervi. Il controller accederà all'interfaccia web dell'unità tramite la connessione VPN. La porta 9090 non deve essere aperta dal lato WAN, ma deve essere aperta dal lato VPN per consentire al controller di accedervi.

Rimuovere un'unità

Le unità possono essere disconnesse dal controller facendo clic sul pulsante *Rimuovi unità* dall'interfaccia web del controller. Quando un'unità viene disconnessa, il controller rimuoverà la configurazione dell'unità e la connessione VPN verrà terminata.

Dopo aver rimosso l'unità dall'interfaccia web del controller, accedere all'interfaccia web dell'unità e fare clic su *Disconnetti unità* nella pagina `Controller`: l'unità eliminerà la configurazione VPN.

16.4 Gruppi di unità

I gruppi di unità sono un modo per organizzare le unità all'interno del controller. Ogni utente può essere associato a uno o più gruppi di unità. Quando un utente è associato a un gruppo di unità, può accedere solo alle unità che appartengono a quel gruppo. I gruppi di unità sono utili per limitare l'accesso a unità specifiche per utenti specifici.

Per creare un nuovo gruppo di unità, l'amministratore deve cliccare sul pulsante *Aggiungi gruppo* dall'interfaccia web del controller, all'interno della pagina `Gruppi di unità`. L'amministratore può specificare il nome del gruppo, una descrizione e le unità che appartengono al gruppo.

Una volta che un gruppo di unità è stato creato, l'amministratore può associare il gruppo di unità a un utente. Per farlo, l'amministratore deve accedere all'elenco degli utenti all'interno della pagina `Utenti`. Successivamente, fare clic sul pulsante *Modifica* accanto all'utente e selezionare il gruppo di unità dal menu a discesa `Gruppi di unità`.

16.4.1 Rimozione dei gruppi di unità

Un gruppo di unità può essere rimosso solo quando non ci sono utenti associati ad esso. Questo può essere verificato accedendo alla pagina `Utenti` e cercando eventuali utenti associati al gruppo.

Per rimuovere un gruppo di unità, l'amministratore deve accedere alla pagina `Gruppi di unità` e fare clic sul pulsante *Elimina* accanto al gruppo.

16.4.2 Gruppo di unità migrato

Quando si esegue l'aggiornamento da una versione del controller precedente alla 2.0.0, verrà creato automaticamente un nuovo gruppo di unità `Migrated`. Il gruppo di unità `Migrated` include automaticamente tutte le unità che erano gestite dal controller prima dell'aggiornamento. Inoltre, è associato a tutti gli utenti esistenti per garantire che mantengano l'accesso alle proprie unità dopo la migrazione.

Il gruppo può essere rimosso in sicurezza una volta che non è più necessario.

16.5 Gestione dei log

Quando un'unità viene collegata, rsyslog viene riconfigurato per inviare i log utilizzando il protocollo syslog (RFC 5424). Potrebbero essere necessari alcuni minuti prima che rsyslog inizi a inviare i dati. I log sono etichettati utilizzando l'hostname dell'unità: per garantire il corretto funzionamento dei collegamenti nell'interfaccia utente, assicurarsi che:

- il FQDN dell'unità è univoco all'interno del cluster
- il nome dell'unità è lo stesso del suo hostname

I log possono essere visualizzati facendo clic sul collegamento *Apri log* per ciascuna unità. I log vengono mostrati in una specifica dashboard di Grafana che consente anche la ricerca e il filtraggio.

Nota: Il periodo di conservazione dei log deve essere configurato dall'interfaccia web di NS8.

16.6 Metriche

Ogni unità esporta due tipi di metriche:

- metriche operative di sistema (CPU, memoria, disco, rete): queste metriche vengono raccolte utilizzando Netdata e memorizzate in Prometheus. Non appena un'unità viene connessa, il controller inizia a raccogliere le metriche. Queste metriche sono disponibili a tutti indipendentemente dallo stato dell'abbonamento.
- metriche del firewall (traffico, sicurezza, VPN): queste metriche vengono inviate dall'unità al controller a intervalli fissi. Il controller le memorizza all'interno di un database Timescale. Queste metriche sono disponibili solo per gli utenti con un .

Tutti i dati raccolti e memorizzati all'interno del controller sono contrassegnati da un timestamp utilizzando il Tempo Coordinato Universale (UTC). Questo garantisce coerenza e accuratezza tra diversi fusi orari, facilitando la correlazione degli eventi e l'analisi delle tendenze.

Gli utenti hanno la possibilità di visualizzare i dati nel proprio fuso orario locale modificando le impostazioni dell'ora in Grafana. Per cambiare il fuso orario locale, accedere al menu delle preferenze di Grafana e selezionare il fuso orario desiderato. Questa modifica può essere applicata a ciascuna dashboard individualmente, consentendo di personalizzare la visualizzazione del fuso orario in base alle proprie preferenze.

Le metriche possono essere visualizzate all'interno della dashboard di Grafana. È possibile accedere alla dashboard facendo clic sul collegamento *Apri metriche* per ciascuna unità.

Per impostazione predefinita, solo l'utente admin può accedere al dashboard delle metriche. Se si desidera consentire ad altri utenti di accedere al dashboard delle metriche, è possibile creare un nuovo ruolo e assegnarlo all'utente direttamente dall'interfaccia web di Grafana.

16.6.1 Grafana

Grafana è una piattaforma open-source utilizzata per il monitoraggio e la visualizzazione di dati time-series. Consente di creare dashboard personalizzabili con grafici, diagrammi e tabelle per analizzare metriche di sistema, log e altri dati provenienti da diverse fonti.

Il controller include un'istanza preconfigurata di Grafana che viene utilizzata per visualizzare metriche e log provenienti dalle unità collegate. L'istanza di Grafana è accessibile dall'URL `https://<controller-fqdn>/grafana`.

Per impostazione predefinita, è possibile accedervi utilizzando le credenziali predefinite impostate durante la configurazione del controller. Si consiglia di cambiare la password predefinita dopo il primo accesso. Grafana offre anche funzionalità per la gestione di utenti, team e permessi. Supporta l'autenticazione tramite diversi metodi, inclusi nome utente/password, OAuth, LDAP e altri.

È inoltre possibile creare dashboard personalizzate e avvisi per monitorare le metriche e i log delle unità collegate. Consultare la documentazione ufficiale per ulteriori informazioni su come utilizzare Grafana.

Metriche Prometheus

Le metriche Prometheus vengono raccolte utilizzando Netdata e memorizzate in un database Prometheus.

Le metriche esportate per ciascuna unità includono le seguenti etichette:

- `instance` l'IP VPN della macchina connessa con la porta Netdata (es. `172.19.64.3:19999`)
- `job` corretto in *node*
- `node` l'IP VPN della macchina connessa
- `unit` il nome univoco dell'unità della macchina collegata

Tali metriche sono visibili all'interno della dashboard `Operating system`.

Metriche di Timescale

Subscription necessaria

Questa funzionalità è disponibile solo se il firewall e il controller dispongono di una subscription valida.

Il database Timescale memorizza le stesse metriche della *Monitoraggio in tempo reale*, ma come serie temporali salvate in un database PostgreSQL. Ogni unità invia i dati al controller ogni 15 minuti. Il controller aggrega i dati ogni 15 minuti, il che significa che i dati sono disponibili all'interno delle dashboard al meglio con un ritardo di 15 minuti e al massimo con un ritardo di 30 minuti.

Il controller può eseguire elaborazioni aggiuntive sui dati per fornire ulteriori approfondimenti. Ad esempio, il controller può geolocalizzare gli indirizzi IP dei client connessi e degli aggressori.

Queste metriche sono visibili all'interno delle seguenti dashboard:

- `Traffico di rete`: traffico di rete aggregato come rilevato dall'unità
- `Traffico di rete per client`: traffico di rete per ogni client (host locale) connesso all'unità
- `Traffico di rete per host`: traffico di rete per ciascun host remoto
- `Sicurezza`: eventi di sicurezza rilevati dall'unità
- `VPN`: Statistiche VPN per OpenVPN Road Warrior, tunnel OpenVPN e tunnel IPsec

Nota: Il periodo di conservazione delle metriche deve essere configurato dall'interfaccia web di NS8 e viene applicato sia ai database Prometheus che Timescale.

16.7 Aggiornamenti delle unità

Il controller consente di aggiornare le unità direttamente dall'interfaccia, in modo simile al processo descritto in *l'interfaccia web dell'unità*. Sono disponibili due tipi di aggiornamenti:

- **Aggiornamenti dei pacchetti**: Aggiornare i pacchetti installati sull'unità. Elencare e installare gli aggiornamenti disponibili facendo clic su *Controlla gli aggiornamenti dei pacchetti* nel menu dell'unità. Verrà visualizzata una finestra modale con l'elenco degli aggiornamenti disponibili. Se sono presenti aggiornamenti, applicarli facendo clic sul pulsante *Aggiorna* nella finestra modale. Questa è la prima operazione da provare se *version awareness* impedisce l'accesso all'unità.

- **Aggiornamento del sistema**: Aggiorna il sistema dell'unità. Se è disponibile un aggiornamento dell'immagine, verrà visualizzato un badge nell'elenco delle unità. È possibile programmare un aggiornamento facendo clic sul pulsante *Aggiornamenti di sistema* nel menu dell'unità. Si può programmare l'aggiornamento oppure aggiornare immediatamente l'unità. Questa operazione è disponibile anche come operazione di massa per più unità tramite *Azioni -> Aggiorna sistemi*. Le unità con un aggiornamento dell'immagine programmato avranno un badge dedicato nell'elenco delle unità. È possibile annullare l'aggiornamento programmato facendo clic sul pulsante *Cancella l'aggiornamento programmato dell'immagine* nel menu dell'unità.

Nota: Si prega di notare che le unità potrebbero non inviare informazioni aggiornate durante il processo di aggiornamento se la versione dell'unità è precedente alla 1.3.0. Per aggiornare manualmente le informazioni, utilizzare il pulsante *Sincronizza info unità* nel menu dell'unità.

16.8 Accesso SSH

SSH, o Secure Shell, è un protocollo di rete crittografico per l'esecuzione sicura di servizi di rete su una rete non sicura. SSH fornisce un canale sicuro su una rete non protetta in un'architettura client-server, collegando un'applicazione client SSH a un server SSH.

È possibile connettersi all'unità facendo clic sul collegamento *Apri terminale SSH*. La connessione avviene tramite un client SSH basato su web che consente l'accesso alla shell dell'unità.

È possibile connettersi alle unità utilizzando una coppia di nome utente e password oppure una chiave SSH.

Una volta connessi, la sessione SSH verrà avviata in una nuova scheda del browser. Alcuni browser richiedono l'autorizzazione per aprire popup affinché la sessione SSH funzioni correttamente. Per chiudere la sessione, è sufficiente chiudere la finestra del browser oppure disconnettersi dalla shell utilizzando CTRL + D.

16.8.1 Nome utente e password

L'utente può connettersi utilizzando una coppia di nome utente e password dell'unità nei seguenti scenari:

- L'utente connesso non ha generato una chiave SSH
- La chiave pubblica SSH dell'utente connesso non è stata copiata all'interno del file delle chiavi autorizzate SSH dell'unità

L'interfaccia utente visualizzerà un modulo per inserire nome utente e password. Dopo aver inserito le credenziali, è possibile fare clic sul pulsante *Apri terminale* per avviare la sessione SSH.

16.8.2 Chiave SSH

Una coppia di chiavi SSH è un insieme di due chiavi crittografiche utilizzate per l'autenticazione durante la creazione di una connessione sicura tramite il protocollo SSH (Secure Shell). La coppia è composta da una chiave privata e una chiave pubblica:

1. **Chiave privata**: Questa viene mantenuta segreta e sicura dall'utente. Non dovrebbe mai essere esposta all'esterno. Viene utilizzata per decriptare i dati che sono stati criptati con la chiave pubblica.
2. **Chiave pubblica**: Questa può essere condivisa liberamente ed è utilizzata per crittografare i dati che possono essere decifrati solo con la chiave privata.

Quando ci si connette a un server utilizzando l'autenticazione SSH con coppia di chiavi, si fornisce la propria chiave pubblica al server. Il server quindi cifra un messaggio di sfida con la chiave pubblica fornita. Il client decifra il

messaggio utilizzando la propria chiave privata e invia il risultato al server. Se il risultato è corretto, il server riconosce che si possiede la chiave privata corretta e consente la connessione.

Questo metodo di autenticazione è più sicuro rispetto all'utilizzo di una password, poiché fornisce una forma di autenticazione a due fattori: qualcosa che si possiede (il file della chiave privata) e qualcosa che si conosce (la passphrase per sbloccare la chiave privata).

Per utilizzare una chiave SSH, è necessario generare una nuova coppia di chiavi accedendo alla pagina `Impostazioni account` e facendo clic sul pulsante *Genera coppia di chiavi SSH*. Inserire una passphrase per proteggere la chiave privata e fare clic sul pulsante *Genera chiave SSH*. L'interfaccia utente mostrerà la chiave pubblica, mentre la chiave privata viene conservata in modo sicuro all'interno del controller.

Prima di connettersi all'unità, è necessario copiare la chiave pubblica e incollarla nel file delle chiavi autorizzate SSH dell'unità. È possibile farlo dalla pagina `Gestione unità`, facendo clic sul pulsante *Azioni* e selezionando *Invia la chiave pubblica SSH*. Selezionare le unità a cui si desidera inviare la chiave e fare clic sul pulsante *Invia la chiave SSH*.

D'ora in poi, sarà possibile connettersi all'unità utilizzando la coppia di chiavi SSH. L'interfaccia utente mostrerà un modulo per inserire la passphrase quando si fa clic sul pulsante *Apri terminale*.

È anche possibile revocare la coppia di chiavi SSH facendo clic sul pulsante *Revoca la chiave pubblica SSH* dal pulsante *Azioni*.

16.9 Accounting

Tutte le operazioni eseguite sul controller vengono registrate nel log di NS8. Ecco alcuni esempi di operazioni registrate:

- Accesso e disconnessione dell'utente
- Creazione/modifica/eliminazione utente/cambio password
- Elenco/creazione/rimozione delle unità

Esempio di log NS8:

```
Mar 26 11:08:23 controller.nethserver.net api[64323]: nethsecurity_controller 2024/03/26␣
↪11:08:23 middleware.go:85: [INFO][AUTH] authentication success for user admin
Mar 26 11:08:23 controller.nethserver.net api[64323]: nethsecurity_controller 2024/03/26␣
↪11:08:23 middleware.go:186: [INFO][AUTH] login response success for user admin
```

Ogni unità dispone di un utente rpcd specifico per il controller, utilizzato per le operazioni di gestione. Quando un utente accede all'interfaccia web dell'unità dal controller, tutte le operazioni eseguite vengono registrate nel log dell'unità, identificate dall'utente rpcd. Ad esempio:

```
Mar 26 11:28:52 NethSec nethsecurity-api[4535]: nethsecurity_api 2024/03/26 11:28:52␣
↪middleware.go:166: [INFO][AUTH] authorization success for user␣
↪0a891388811ff8dc0ec2fbed. POST /api/ubus/call {"path":"ns.dashboard","method":
↪"interface-traffic","payload":{"interface":"eth1"}}
Mar 26 11:28:52 NethSec (none) nginx: 172.19.64.1 - - [26/Mar/2024:11:28:52 +0000] "POST␣
↪/api/ubus/call HTTP/1.1" 200 1490 "https://controller.gs.nethserver.net/" "Mozilla/5.0␣
↪(X11; Linux x86_64; rv:122.0) Gecko/20100101 Firefox/122.0"
```

Per determinare chi ha eseguito una specifica operazione, è necessario controllare il log dell'unità identificata dall'utente rpcd e correlare tale informazione con l'azione di accesso effettuata sul controller.

Quando un utente si connette all'unità tramite SSH, l'accesso viene registrato nel log dell'unità, identificato dall'utente SSH. Solitamente, l'utente SSH è root. Ad esempio:

```
Mar 26 11:55:03 NethSec dropbear[22798]: Password auth succeeded for 'root' from 172.19.
↪64.1:46460
```

Se l'utente utilizza una chiave SSH per l'autenticazione, il log conterrà l'impronta digitale della chiave SSH utilizzata per l'autenticazione. Questo rende più semplice associare l'utente SSH alle operazioni eseguite. Esempio:

```
Mar 26 11:09:33 NethSec dropbear[31090]: Child connection from 172.19.64.1:52012
Mar 26 11:09:33 NethSec dropbear[31090]: Pubkey auth succeeded for 'root' with ssh-rsa␣
↪key SHA256:FLecvNRKi0hxxxdjfP0urUZxxx6jxxxxNbZceOPFjyk from 172.19.64.1:52012
```

16.10 Subscription e limitazioni

Subscription necessaria

Alcune restrizioni possono essere superate solo se il firewall dispone di un .

Il comportamento del controller in esecuzione su un NS8 dipende dal suo stato di sottoscrizione.

Controller senza subscription:

- Consente la registrazione di un massimo di 3 unità.
- Solo i firewall della community possono registrarsi con il controller.
- Le metriche storiche non sono accessibili.

Controller con una subscription valida:

- Il numero di unità è illimitato.
- Solo i firewall con una subscription valida possono registrarsi con il controller.
- Le unità con un subscription valida inviano metriche al controller.

16.11 Version awareness

La version awareness è un meccanismo che impedisce all'utente di eseguire operazioni non supportate dalla versione dell'unità. A tal fine, durante la connessione all'interfaccia utente di un'unità, il controller verificherà la versione delle API durante il processo di connessione. Esistono tre possibili scenari:

a. Se le versioni sono compatibili, la connessione procede normalmente.

b. Se il firewall (unità) è significativamente più vecchio del controller, verrà visualizzato un popup che impedisce la connessione. Questo serve a proteggere da potenziali errori.

c. Se il controller è leggermente più vecchio del firewall, verrà visualizzato un avviso relativo alla mancata corrispondenza. Tuttavia, sarà comunque possibile connettersi se si sceglie di procedere.

In qualità di amministratore, non è necessario eseguire alcuna azione specifica per abilitare la version awareness. Questa funziona automaticamente in background. Tuttavia, è consigliabile:

1. Prestare attenzione agli avvisi: se viene visualizzato un avviso di incompatibilità di versione, valutare l'aggiornamento del sistema quando conveniente.
2. Mantenere il sistema aggiornato: verificare regolarmente la presenza di aggiornamenti e applicarli sia al controller che alle unità firewall per garantire la migliore compatibilità e l'accesso alle nuove funzionalità.

3. Segnalare problemi: se si riscontrano comportamenti insoliti o errori, soprattutto dopo aver visualizzato un avviso di versione, seguire la procedura di *risoluzione dei problemi*.

La version awareness è una funzionalità in background che contribuisce a mantenere il sistema NethSecurity operativo senza intoppi. Verificando automaticamente la compatibilità tra il controller e le unità, previene molti potenziali problemi prima che possano influire sulla rete. Anche se non richiede alcuna azione da parte dell'utente, essere a conoscenza di questa funzionalità può aiutare a comprendere e gestire meglio il sistema.

Ignorare la version awareness

Sebbene la version awareness sia una funzionalità utile, conoscendo i rischi e i potenziali problemi, potrebbe essere necessario ignorarla in alcuni casi. Per farlo, la procedura è la seguente:

1. Sul controller, andare alla pagina del gestore delle unità e fare clic su *Ulteriori informazioni* dell'unità a cui si desidera connettersi.
2. Copia il valore di `Unit ID`.
3. Fare clic su *Apri terminale SSH*
4. Quando si apre la finestra modale, è possibile chiuderla in sicurezza. Questo era necessario solo per scambiare alcune credenziali con l'unità.
5. Aprire una nuova scheda e andare a questo URL: `https://<controller-fqdn>/#/controller/manage/<unit-id>/dashboard`. Esempio: `https://controller.nethsecurity.org/#/controller/manage/000000000-0000-0000-0000-000000000000/dashboard`.
6. Sarà possibile accedere all'interfaccia utente dell'unità senza il controllo della versione.

Aggiornare l'unità con SSH

È possibile aggiornare l'unità senza collegarsi ad essa utilizzando il terminale SSH. Seguire i passaggi per connettersi all'unità utilizzando *SSH Access*.

Una volta connessi, è possibile verificare la presenza di aggiornamenti a seconda di ciò che si desidera aggiornare.

a. Installare gli aggiornamenti dei pacchetti sull'unità:
    1. Per verificare la presenza di aggiornamenti per i pacchetti, utilizzare il seguente comando:

    ```
    /usr/libexec/rpcd/ns.update call check-package-updates
    ```

    2. Se si è d'accordo con l'installazione dei pacchetti, è possibile eseguire il seguente comando:

    ```
    /usr/libexec/rpcd/ns.update call install-package-updates
    ```

b. Per aggiornare l'immagine, è possibile semplicemente pianificare l'installazione; si ricorda che questa operazione riavvia il firewall (causando un periodo di inattività).
    1. Verificare se è disponibile un'immagine aggiornata:

    ```
    /usr/libexec/rpcd/ns.update call check-system-update
    ```

    2. Se si desidera procedere con l'aggiornamento, è possibile farlo tramite questo comando:

    ```
    /usr/libexec/rpcd/ns.update call update-system
    ```

CAPITOLO 17

Interfacce di rete

La pagina `Interfacce e dispositivi` configura come il server è collegato alla rete locale (LAN) e/o ad altre reti (ad esempio Internet).

NethSecurity supporta un numero illimitato di interfacce di rete. Qualsiasi rete gestita dal sistema deve seguire queste regole:

- le reti devono essere separate logicamente: ogni rete deve avere indirizzi diversi
- le reti private, come le LAN, devono seguire la convenzione degli indirizzi dal documento *RFC1918*
- le reti devono essere separate fisicamente utilizzando switch diversi oppure separate logicamente utilizzando VLAN (Virtual Local Area Network)

Ogni interfaccia di rete ha una zona specifica che ne determina il comportamento. Una configurazione di rete di base per un router include tipicamente almeno due interfacce, ovvero LAN (Local Area Network) e WAN (Wide Area Network):

- *lan*: rete locale, gli host su questa rete possono accedere a qualsiasi altra rete configurata
- *wan*: rete pubblica, gli host su questa rete possono accedere solo al server stesso

Tutte le interfacce di rete configurate sono elencate nella parte superiore della pagina. Ogni interfaccia viene visualizzata con il proprio nome e la zona firewall assegnata. Questa sezione offre una panoramica immediata delle configurazioni attuali, permettendo di vedere rapidamente quali reti sono già configurate e associate a specifiche zone di sicurezza.

Nella sezione inferiore della pagina sono elencati i dispositivi di rete disponibili ma non configurati. Per configurare un dispositivo, si fa clic sul pulsante *Configura* corrispondente al dispositivo desiderato. I nuovi *dispositivi VLAN* creati sono visibili in questa sezione.

Indirizzi IPv4 per reti private (RFC1918)

Le reti private TCP/IP non direttamente connesse a Internet dovrebbero utilizzare indirizzi speciali selezionati dall'Internet Assigned Numbers Authority (IANA).

Rete privata	Maschera di sottorete	Intervallo di indirizzi IP
10.0.0.0	255.0.0.0	10.0.0.1 - 10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1 - 172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1 - 192.168.255.254

17.1 Interfacce logiche

Le interfacce di rete logiche sono interfacce di rete virtuali che consentono una maggiore flessibilità e funzionalità nelle configurazioni di rete. A differenza delle interfacce di rete fisiche, che corrispondono a porte hardware reali, le interfacce di rete logiche sono basate su software e possono essere configurate e gestite per soddisfare requisiti di rete specifici.

Fare clic sul pulsante *Aggiungi interfaccia logica* per creare un nuovo dispositivo di rete virtuale. Il dispositivo può essere un

- *bridge*: è un'interfaccia di rete logica che collega due o più segmenti di rete differenti, consentendo la comunicazione tra dispositivi presenti in questi segmenti. Un bridge estende di fatto la rete locale, permettendo ai dispositivi di comunicare come se fossero sulla stessa rete fisica.
- *bond*: noto anche come network bonding o NIC bonding, è un metodo che consente di combinare due o più interfacce di rete fisiche in un'unica interfaccia logica. Offre due vantaggi principali: aumento della larghezza di banda e tolleranza ai guasti.

I bond possono essere configurati in modalità multiple.

Modalità che forniscono bilanciamento del carico e tolleranza ai guasti:

- Round Robin bilanciato (consigliato)
- Bilanciamento XOR
- 802.3ad (LACP): richiede il supporto a livello di driver e uno switch con la modalità di aggregazione dinamica dei collegamenti IEEE 802.3ad abilitata
- Bilancia TLB: richiede il supporto a livello di driver
- Bilanciare ALB

Modalità che forniscono solo tolleranza ai guasti:

- Backup attivo (consigliato)
- Politica di trasmissione

Durante la creazione di un bond, l'interfaccia utente mostrerà un indirizzo IP di gestione nella rete privata 127.x.x.1/32. Questo indirizzo IP viene utilizzato esclusivamente per la gestione del bond e non è coinvolto nell'inoltro del traffico. Una volta creato il dispositivo bond, è possibile assegnargli un indirizzo IP e una zona firewall. Si noti che la configurazione del bond non è modificabile dopo la creazione. Se è necessario modificare l'indirizzo IP o la zona del bond, sarà necessario rimuovere la sua configurazione e riconfigurarla nuovamente. Se è necessario modificare i dispositivi del bond, la modalità del bond o l'IP di gestione, sarà necessario rimuovere la configurazione del bond e il dispositivo bond e ricrearlo da zero.

17.2 VLAN

Una VLAN, o Virtual Local Area Network, è una tecnologia di rete che consente agli amministratori di rete di creare reti logicamente segmentate all'interno di un'infrastruttura di rete fisica. Le VLAN permettono la creazione di più domini di broadcast in una rete, anche se sono fisicamente collegati allo stesso switch di rete.

È possibile creare un nuovo dispositivo VLAN facendo clic sul pulsante *Crea dispositivo VLAN*. Selezionare il tipo di dispositivo VLAN:

- VLAN 802.1q è utilizzato principalmente per implementazioni VLAN standard all'interno delle organizzazioni
- 802.1ad (QinQ) viene utilizzato nelle reti dei provider di servizi dove più clienti richiedono la segmentazione VLAN, e queste VLAN segmentate devono essere supportate anche nella rete del provider

Assicurarsi inoltre di scegliere l'ID VLAN corretto. Si ricorda che è necessario configurare lo stesso ID VLAN anche all'interno dello switch di rete.

17.3 Alias IP

Utilizzare l'IP aliasing per assegnare più indirizzi IP alla stessa interfaccia di rete.

L'uso più comune è con un'interfaccia wan: quando l'ISP fornisce un pool di indirizzi IP pubblici (all'interno della stessa subnet), è possibile aggiungerne alcuni (o tutti) alla stessa interfaccia wan e gestirli individualmente (ad esempio nella configurazione dell'inoltro porte).

Per aggiungere un alias, fare clic sul menu con i tre puntini nell'angolo destro dell'interfaccia di rete esistente, quindi selezionare la voce *Crea interfaccia alias*.

17.4 PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) collega il server a Internet tramite un modem DSL. È possibile configurare una nuova connessione PPPoE utilizzando un'interfaccia di rete Ethernet non assegnata oppure creando una nuova interfaccia logica.

All'interno della finestra dell'interfaccia di rete, scegliere la zona wan, quindi selezionare il protocollo `PPPoE`. Successivamente, compilare tutti i campi richiesti come `Nome utente` e `Password`.

17.4.1 PPPoE con DHCPv6-PD

La DHCPv6 Prefix Delegation (DHCPv6-PD) automatizza l'assegnazione dei prefissi IPv6 da parte del proprio provider di servizi Internet (ISP). Elimina la necessità di configurazione manuale o di Network Address Translation (NAT), semplificando la distribuzione di IPv6.

Per prima cosa, assicurarsi che il proprio ISP supporti DHCPv6-PD, quindi seguire questi passaggi:

- Configurare l'interfaccia WAN: impostare la modalità dell'interfaccia WAN su PPPoE e abilitare l'opzione `Abilita IPv6`
- Configurare l'interfaccia LAN: abilitare l'opzione *Enable IPv6* e lasciare vuoto il campo dell'indirizzo IPv6

Abilitando IPv6 sia per le interfacce WAN che LAN senza specificare un indirizzo per la LAN, il router richiederà e riceverà automaticamente un prefisso IPv6 (di solito un /64) dal proprio ISP tramite DHCPv6-PD. Questo prefisso verrà poi utilizzato per assegnare indirizzi IPv6 individuali ai dispositivi sulla rete.

17.5 Adattatori USB-Ethernet

Gli adattatori USB-Ethernet non sono considerati adatti all'uso in un dispositivo firewall critico per la comunicazione di rete; per questo motivo i driver non sono inclusi nell'immagine di NethSecurity. Solo a scopo sperimentale, è possibile installare driver specifici tramite il gestore dei pacchetti per l'utilizzo in un ambiente di test.

Si raccomanda vivamente **di non utilizzare questi adattatori in ambienti di produzione**. Se l'unità dispone di un abbonamento Enterprise o Community, si tenga presente che gli adattatori USB-to-Ethernet **non sono coperti dal supporto Nethesis**.

Avvertimento: I pacchetti aggiuntivi, inclusi i moduli del kernel, non vengono mantenuti durante gli aggiornamenti dell'immagine; pertanto, in caso di aggiornamento, sarà necessario scaricarli e installarli nuovamente se necessario.

17.5.1 Come installare moduli USB-to-Ethernet

Questi pacchetti possono essere installati dalla console della riga di comando, è sufficiente individuare il modulo corretto e installarlo.

- Verificare che l'adattatore ethernet sia collegato alla porta USB utilizzando `lsusb`. Esempio di output:

```
# lsusb
Bus 002 Device 002: ID 0bda:8153 Realtek USB 10/100/1000 LAN
Bus 002 Device 001: ID 1d6b:0003 Linux 5.15.162 xhci-hcd xHCI Host Controller
Bus 001 Device 002: ID 0627:0001 QEMU QEMU USB Tablet
Bus 001 Device 001: ID 1d6b:0002 Linux 5.15.162 xhci-hcd xHCI Host Controller
```

- Cercare il modulo kernel:

```
opkg update
opkg find kmod-usb-net-\*
```

- Esempio di output:

```
kmod-usb-net-aqc111 - 5.15.162-1 - Support for USB-to-Ethernet Aquantia AQtion 5/2.
↪5GbE
kmod-usb-net-asix-ax88179 - 5.15.162-1 - Kernel module for USB-to-Ethernet ASIX␣
↪AX88179 based USB 3.0/2.0 to Gigabit Ethernet adapters.
kmod-usb-net-cdc-ether - 5.15.162-1 - Kernel support for USB CDC Ethernet devices
kmod-usb-net-cdc-ncm - 5.15.162-1 - Kernel support for CDC NCM connections
kmod-usb-net-dm9601-ether - 5.15.162-1 - Kernel support for USB DM9601 devices
kmod-usb-net-lan78xx - 5.15.162-1 - Kernel module for Microchip LAN78XX based USB 2␣
↪& USB 3 10/100/1000 Ethernet adapters.
kmod-usb-net-mcs7830 - 5.15.162-1 - Kernel module for USB-to-Ethernet MCS7830␣
↪convertors
kmod-usb-net-pegasus - 5.15.162-1 - Kernel module for USB-to-Ethernet Pegasus␣
↪convertors
kmod-usb-net-rtl8150 - 5.15.162-1 - Kernel module for USB-to-Ethernet Realtek 8150␣
↪convertors
kmod-usb-net-rtl8152 - 5.15.162-1 - Kernel module for USB-to-Ethernet Realtek 8152␣
↪USB2.0/3.0 convertors
kmod-usb-net-smsc95xx - 5.15.162-1 - Kernel module for SMSC LAN95XX based devices
```

(continues on next page)

(continua dalla pagina precedente)

```
kmod-usb-net-sr9700 - 5.15.162-1 - Kernel module for CoreChip-sz SR9700 based USB 1.
↪1 10/100 ethernet devices
```

- Installare il driver corretto:

```
opkg install kmod-usb-net-rtl8150
```

- Verificare che venga visualizzata una nuova interfaccia ethX utilizzando `ifconfig -a`
- Configurare l'ethernet dall'interfaccia utente

CAPITOLO 18

DNS e DHCP

NethSecurity può fornire servizi DNS e DHCP a tutte le reti locali. Questa sezione è suddivisa in 5 schede:

- DHCP e MAC bindining
- Lease statiche
- Lease dinamici
- DNS
- Record DNS
- Scansione rete

18.1 DHCP e MAC bindining

Questa sezione consente di abilitare e gestire un server DHCP per ogni rete locale configurata nel proprio NethSecurity. Ogni interfaccia locale è dotata di una scheda in cui è possibile abilitare il servizio facendo clic sul pulsante *Modifica*.

Campi disponibili:

- `MAC binding`
  - `Stato`: abilita/disabilita la funzione di binding MAC-IP per questa interfaccia
  - `Tipo`: è possibile scegliere tra due tipi di binding MAC-IP:
    - `Soft binding`: consente agli host senza una reservation, blocca IP/MAC non corrispondenti

      Esempio: Una rete aziendale in cui i dipendenti portano frequentemente i propri dispositivi (BYOD). In questo caso, il Soft binding consente ai dispositivi senza una reservation di accedere alla rete, ma garantisce che qualsiasi dispositivo con un indirizzo IP/MAC non corrispondente venga bloccato. Questo offre flessibilità ai dipendenti mantenendo comunque un certo livello di sicurezza.
    - `Strict binding`: Solo gli host con una prenotazione sono consentiti, gli altri vengono bloccati

Esempio: Una rete aziendale con politiche di sicurezza rigorose. In questo caso, il hard binding garantisce che solo i dispositivi con una reservation preconfigurata possano accedere alla rete. Questo impedisce che i dipendenti rubino un IP con autorizzazioni superiori.

- `DHCP`:
  - `Abilita DHCP` : abilita/disabilita il servizio
  - `Inizio intervallo IP` : primo indirizzo IP dell'intervallo DHCP
  - `Fine intervallo IP` : ultimo indirizzo IP dell'intervallo DHCP
  - `Tempo di lease` : tempo di lease (predefinito 1 ora)

Impostazioni avanzate DHCP

`Forza l'avvio del server DHCP`

All'avvio, il server DHCP verifica se sono presenti altri server DHCP sulla rete. Con questa opzione disabilitata, il server DHCP non verrà attivato se ne viene rilevato un altro sulla rete. Se l'opzione di forzatura è abilitata, il server DHCP verrà avviato anche se sono presenti altri server DHCP all'interno della rete.

`Opzione DHCP`

È possibile dichiarare opzioni DHCP molto specifiche, cercando il campo da configurare (ad esempio, DNS passato ai client, indirizzo IP tftp e così via) e quindi specificando il valore. Il valore può anche essere un elenco di valori separati da una virgola.

Esempio per sovrascrivere il DNS passato ai client con 2 server:

- opzione selezionata: `dns-server`
- valore: `1.1.1.1,8.8.8.8`

Vedere anche *Opzioni personalizzate non standard* per ulteriori informazioni sulle opzioni non standard.

18.2 Lease statici

I lease statici assegnano indirizzi IP stabili e nomi host simbolici ai client DHCP. L'host viene identificato tramite il suo indirizzo MAC, gli viene assegnato un indirizzo IP fisso e viene fornito un nome host simbolico per un facile riconoscimento.

Fare clic sul pulsante *Aggiungi reservation* per aggiungere una nuova reservation per un dispositivo.

Campi disponibili:

- `Nome host` : Nome host associato all'indirizzo IP
- `Indirizzo IP` : Indirizzo IP da assegnare al MAC Address specificato. L'indirizzo IP deve essere compreso nell'intervallo DHCP.
- `Indirizzo MAC` : Indirizzo MAC del dispositivo per cui si desidera effettuare la reservation
- `Nome reservation` : Facoltativo, campo configurabile liberamente

18.3 Lease dinamici

I lease dinamici rappresentano gli indirizzi IP attualmente in uso e assegnati ai dispositivi sulla rete. Questa scheda mostra tutti i lease attualmente attivi.

18.3.1 Configurazione predefinita

Per impostazione predefinita, il server DHCP ha un limite di 1000 lease simultanei per prevenire attacchi DoS. Impostare l'opzione `dhcpleasemax` di dnsmasq per modificare il limite.

Eseguire questi comandi:

```
uci set dhcp.@dnsmasq[0].dhcpleasemax='2500'
uci commit dhcp
reload_config
```

18.3.2 Opzioni personalizzate non standard

Oltre alle opzioni DHCP standard, NethSecurity consente di configurare opzioni personalizzate non standard, come l'opzione 82 (DHCP Relay Agent Information). Queste opzioni possono essere utili per configurazioni avanzate o requisiti di rete specifici.

Per impostare un'opzione personalizzata dalla riga di comando, utilizzare i seguenti comandi:

```
uci add_list dhcp.lan.dhcp_option='82,myvalue'
uci commit dhcp
reload_config
```

Le opzioni personalizzate configurate tramite la riga di comando vengono mantenute anche quando vengono apportate modifiche tramite l'interfaccia utente. Le opzioni personalizzate possono essere rimosse in modo sicuro dall'interfaccia utente.

Tuttavia, si consiglia di evitare di modificare queste opzioni personalizzate direttamente dall'interfaccia utente per prevenire comportamenti imprevisti.

18.4 DNS

Il sistema utilizza Dnsmasq come server DNS cache downstream. Dnsmasq funziona come un nameserver locale con cache, che per impostazione predefinita inoltra le query DNS ai server DNS a monte forniti dal server DHCP delle interfacce WAN. Tuttavia, questo comportamento può essere personalizzato utilizzando le seguenti opzioni di configurazione:

- `Server di DNS forwarding`: Fare clic sul pulsante *Aggiungi server DNS* per specificare il DNS upstream desiderato; è possibile aggiungere più server, ognuno dei quali viene gestito individualmente.
- `DNS Domain` : Inserire il dominio DNS locale, assicurandosi che le query per questo dominio vengano sempre risolte localmente.
- `Log query DNS`: abilitarlo se si desidera che tutte le query DNS vengano registrate dal sistema.

18.4.1 Server di forwarding

È necessario configurare i forwarder solo se le interfacce WAN sono impostate con indirizzi IP statici. Se le interfacce WAN sono configurate tramite DHCP, solitamente fornito dal proprio ISP, il sistema utilizzerà automaticamente i server DNS forniti dalle interfacce WAN. I server DNS upstream configurati automaticamente possono essere trovati nel file */tmp/resolv.conf.d/resolv.conf.auto*.

È possibile configurare quanto segue:

- **Specificare un singolo server DNS upstream:** inserire l'indirizzo IP del server DNS desiderato nel campo designato.
- **Configurare server DNS specifici per dominio:** questo consente di instradare le query per domini specifici verso server diversi.

Per una configurazione DNS orientata alla privacy utilizzando connessioni crittografate, consultare *DNS over HTTPS con filtraggio* per la configurazione di DNS over HTTPS (DoH).

Server DNS specifici per dominio

Per utilizzare un server DNS personalizzato per un dominio specifico, utilizzare la seguente sintassi:

```
/DOMAIN/IP_ADDRESS#PORT
```

dove:

- IP_ADDRESS: specificare l'indirizzo IP del server desiderato
- PORTA: aggiungere la porta desiderata (dopo l'indirizzo IP utilizzando il carattere #).

Il valore `PORT` è opzionale, quindi di solito la configurazione appare semplicemente così:

```
/DOMAIN/IP_ADDRESS
```

Queste sono le principali opzioni supportate:

- Dominio vuoto (`//`): corrisponde a nomi non qualificati (senza punti).
- Dominio specifico (`/google.com/`): corrisponde esattamente al dominio indicato e a tutti i suoi sottodomini (ad esempio, google.com, www.google.com, drive.google.com...).
- Dominio wildcard (`*google.com/`): corrisponde a qualsiasi dominio **contenente** «google.com» (ad esempio, google.com, www.google.com, supergoogle.com).

Esempi:

- Inviare tutte le query per «google.com» e i suoi sottodomini a 1.2.3.4: `/google.com/1.2.3.4`
- Inviare tutti i nomi non qualificati (ad esempio, «localhost») a 10.0.0.1 e tutto il resto ai server standard: `//10.0.0.1`
- Inviare le query per il dominio «ad.nethserver.org» e i suoi sottodomini a 192.168.1.1 e tutto il resto ai server standard: `/ad.nethserver.org/192.168.1.1`

I domini più specifici hanno la precedenza su quelli meno specifici, quindi per una configurazione come questa:

- `/google.com/1.2.3.4`
- `/www.google.com/2.3.4.5`

NethSecurity invierà le richieste per google.com e gmail.google.com a 1.2.3.4, ma www.google.com verrà indirizzato a 2.3.4.5

Questo vale anche per i caratteri jolly: se sono definiti sia domini specifici che domini con caratteri jolly per lo stesso pattern, quello specifico ha la precedenza (ad esempio, avendo `/google.com/` e `/*google.com/` : il primo gestirà google.com e www.google.com, mentre il carattere jolly gestirà supergoogle.com).

18.4.2 Numero massimo di query DNS simultanee

Per impostazione predefinita, dnsmasq ha un limite di 150 query DNS concorrenti per prevenire attacchi DoS. Se questo limite viene raggiunto, dnsmasq registrerà un errore e interromperà l'elaborazione di nuove query DNS fino al completamento di alcune di quelle già in corso.

In questo caso, dnsmasq registrerà un errore simile a:

```
May 12 09:27:23 fw1 dnsmasq[1]: Maximum number of concurrent DNS queries reached (max:␣
↪150)
```

Per aumentare il limite dalla CLI, eseguire i seguenti comandi:

```
uci set dhcp.@dnsmasq[0].dnsforwardmax=5000
uci commit dhcp
reload_config
```

Questa opzione non è esposta nell'interfaccia utente, ma la modifica persisterà attraverso gli aggiornamenti e non verrà sovrascritta dall'interfaccia utente.

18.4.3 Tempistica di aggiornamento del set di domini

Le voci del *Domain set* vengono aggiornate quando dnsmasq esegue una nuova ricerca per il dominio. Quando le risposte vengono servite dalla cache locale invece di eseguire una nuova ricerca, gli indirizzi IP non vengono riaggiunti al set. Questo può causare delle interruzioni intermittenti se l'ipset scade prima che scada il TTL del DNS, oppure se la cache impedisce a dnsmasq di effettuare nuove ricerche. Si noti che Adblock può modificare il comportamento di dnsmasq e influire sull'aggiornamento del domain set.

Un job cron viene eseguito ogni 10 minuti per aggiornare tutti i set di domini, ma dipende anche dal fatto che dnsmasq esegua effettivamente le interrogazioni invece di fornire risultati memorizzati nella cache.

Per risolvere i problemi di aggiornamento del set di domini, regolare le impostazioni del TTL della cache DNS:

```
uci set dhcp.@dnsmasq[0].max_cache_ttl=300
uci set dhcp.@dnsmasq[0].max_ttl=300
uci commit dhcp
reload_config
```

Queste impostazioni garantiscono che le voci memorizzate nella cache scadano rapidamente, consentendo a dnsmasq di eseguire nuove ricerche e aggiornare correttamente i set di domini. Si noti che questa impostazione sovrascriverà il TTL predefinito fornito dai server DNS a monte. Un TTL così basso può aumentare il numero di query inviate ai server DNS a monte, il che può comportare un aumento del traffico di rete e potenziali problemi di prestazioni se i server a monte hanno limiti di frequenza o se ci sono molti client che effettuano richieste DNS frequenti. Utilizzare questa configurazione con cautela e monitorare le prestazioni del sistema dopo averla applicata.

18.4.4 Protezione contro il DNS Rebind

La protezione contro il DNS Rebind è una funzionalità di sicurezza che protegge dagli attacchi di DNS rebinding. Blocca l'utilizzo di intervalli di indirizzi IP privati da parte di domini pubblici, impedendo ai siti web dannosi di manipolare i browser per effettuare richieste non autorizzate ai dispositivi della rete locale.

La protezione contro il DNS Rebind è abilitata di default su NethSecurity e solitamente non comporta ripercussioni operative. In presenza di split DNS, ovvero quando si risolvono domini pubblici con risorse interne, la protezione contro il rebind può causare problemi di risoluzione. In tali scenari, eventuali problemi possono essere individuati nel log (`/var/log/messages`), dove potrebbero comparire righe simili alle seguenti:

```
Sep 21 13:09:36 fw1 dnsmasq[1]: possible DNS-rebind attack detected: ad.nethesis.it
```

Nota: Per garantire la massima compatibilità e prevenire malfunzionamenti nelle installazioni migrate utilizzando lo strumento dedicato di NethServer 7.9, la Protezione DNS Rebind è disabilitata, assicurando lo stesso comportamento della versione precedente.

Come risolvere i problemi di protezione DNS rebind

È possibile risolvere facilmente qualsiasi di questi problemi dalla CLI.

Soluzione 1: Inserire il dominio nella whitelist

Inserire il dominio specifico in una whitelist (consigliato):

```
uci add_list dhcp.@dnsmasq[0].rebind_domain="nethesis.it"
```

quindi eseguire il commit e riavviare:

```
uci commit dhcp
/etc/init.d/dnsmasq restart
```

Soluzione 2: disabilitare la protezione DNS

Disabilitare completamente la protezione contro il DNS rebind utilizzando questi comandi:

```
uci set dhcp.@dnsmasq[0].rebind_protection='0'
uci commit dhcp
/etc/init.d/dnsmasq restart
```

Come abilitare la protezione contro il DNS rebind

Se in precedenza è stata disabilitata la protezione contro il rebind o se la configurazione deriva da una migrazione e si desidera abilitare la protezione contro il rebind, si consiglia di attivare anche il parametro `rebind_localhost`. Questa impostazione ha effetto esclusivamente quando la protezione contro il rebind è abilitata e consente risposte upstream da 127.0.0.0/8, essenziale per i servizi di blacklist basati su DNS. Eseguire questi comandi:

```
uci set dhcp.@dnsmasq[0].rebind_protection='1'
uci set dhcp.@dnsmasq[0].rebind_localhost='1'
uci commit dhcp
/etc/init.d/dnsmasq restart
```

18.5 Record DNS

Il sistema può gestire record DNS locali. Quando il server esegue una ricerca DNS, prima cercherà all'interno dei record DNS locali. Se non viene trovato alcun record locale, verrà effettuata una query DNS esterna.

Nota: I record DNS locali avranno sempre la precedenza sui record provenienti dai server DNS esterni.

Fare clic sul pulsante *Aggiungi record DNS* per aggiungere un nuovo hostname DNS.

Campi disponibili:

- `Nome host` : Nome host DNS
- `Indirizzo IP` : Indirizzo IP associato al nome host
- `Nome` : campo facoltativo
- `Record DNS wildcard`: abilitarlo se si desidera questa risposta per qualsiasi sottodominio non già definito

18.6 Scansione rete

Questa sezione descrive la funzionalità di scansione della rete locale. La pagina consente di eseguire la scansione di tutte le reti locali disponibili, escludendo le reti WAN. La pagina visualizza un elenco delle reti locali rilevate; ogni rete include un pulsante *Scan network*, la selezione di questo pulsante avvia una scansione completa della rete scelta.

18.6.1 Risultati della scansione

Al termine dell'operazione, la pagina mostra una tabella con tutti gli host rilevati. Per ciascun host vengono fornite le seguenti informazioni:

- Indirizzo IP
- Indirizzo MAC
- Nome host (se rilevato)
- Descrizione

È possibile selezionare qualsiasi host dalla tabella e creare una voce di record DNS o una prenotazione DHCP utilizzando il relativo menu a tre puntini.

Nota: Il sistema supporta la scansione solo su reti con una netmask massima di 255.255.240.0 (CIDR /20), che corrisponde a un massimo di 4094 host. Le scansioni su reti più grandi non sono supportate.

18.7 DHCP Relay

Il relay DHCP consente al firewall di inoltrare le richieste DHCP dai client a un server DHCP esterno. Il relay DHCP non è disponibile dall'interfaccia utente, ma è possibile configurarlo dal terminale utilizzando *uci*.

- Sostituire *<INTERFACE_NAME>* con il nome dell'interfaccia su cui il relay DHCP deve ascoltare.
- Sostituire *<LOCAL_ADDR>* con l'indirizzo IP del firewall su quella interfaccia.
- Sostituire *<SERVER_ADDR>* con l'indirizzo IP del server DHCP upstream.

1.Create a new DHCP relay entry

```
uci add dhcp relay
```

2.Set the interface:

```
uci set dhcp.@relay[-1].interface='<INTERFACE_NAME>'
```

3.Set the local address of the firewall:

```
uci set dhcp.@relay[-1].local_addr='<LOCAL_ADDR>'
```

4.Set the upstream DHCP server address:

```
uci set dhcp.@relay[-1].server_addr='<SERVER_ADDR>'
```

5.Commit the configuration:

```
uci commit dhcp
```

6.Reload the system configuration:

```
reload_config
```

18.7.1 Esempio

```
uci add dhcp relay
uci set dhcp.@relay[-1].interface='LAN'
uci set dhcp.@relay[-1].local_addr='192.168.1.1'
uci set dhcp.@relay[-1].server_addr='192.168.10.100'
uci commit dhcp
reload_config
```

18.8 Riferimenti esterni

- Documentazione DNS e DHCP di OpenWrt
- Manuale di Dnsmasq

CAPITOLO 19

Rotte statiche

Il routing statico in Linux consente un controllo preciso su come i pacchetti dati attraversano una rete. A differenza del routing dinamico, che è automatico, il routing statico richiede una configurazione manuale da parte degli amministratori di rete.

Il routing statico è semplice e prevedibile, il che lo rende ideale per reti stabili in cui i percorsi non cambiano frequentemente. Gli amministratori possono definire manualmente le route, fornendo istruzioni specifiche su come i dati devono viaggiare attraverso la rete.

Le rotte statiche possono essere configurate dalla pagina `Rotte`, nella sezione `Rete` del menu a sinistra.

Per aggiungere una nuova rotta, fare clic sul pulsante *Aggiungi rotta*. Per modificare una rotta esistente, fare clic sul pulsante *Modifica* nel record della tabella. Per eliminare una rotta, fare clic sul menu a tre puntini nel record della tabella e premere il pulsante *Elimina*.

CAPITOLO 20

MultiWAN

La configurazione MultiWAN (Wide Area Network) è un'impostazione in cui il firewall utilizza contemporaneamente più connessioni Internet provenienti da diversi provider di servizi Internet (ISP). Questa configurazione ha l'obiettivo di aumentare l'affidabilità della rete, incrementare la larghezza di banda e migliorare la velocità di connessione distribuendo il traffico di rete su più collegamenti. Può offrire protezione da failover, garantendo che, in caso di guasto di una connessione, il traffico di rete venga automaticamente reindirizzato verso la connessione funzionante, riducendo al minimo i tempi di inattività e assicurando un accesso continuo a Internet. Le configurazioni MultiWAN sono spesso utilizzate da aziende e organizzazioni che necessitano di una connessione Internet altamente disponibile e stabile per le proprie operazioni.

La configurazione MultiWAN richiede almeno due interfacce di rete nella zona WAN del sistema. Questo è il requisito fondamentale per implementare una connessione MultiWAN.

La prima volta che si accede alla pagina di configurazione, è obbligatorio creare una policy predefinita. Questa policy è essenziale e non può essere eliminata. La policy predefinita definisce il comportamento di base del sistema MultiWAN. È necessario specificarne il comportamento. Sono disponibili due opzioni principali:

- `Bilanciato`: In questa modalità, le connessioni WAN vengono utilizzate simultaneamente e il traffico viene bilanciato in base al peso assegnato a ciascuna WAN. Il peso della WAN può variare da 1 a 1000.
- `Backup`: In modalità backup, la connessione WAN secondaria entra in funzione solo se la connessione primaria fallisce. Questo garantisce una connettività di riserva in caso di guasto della WAN primaria.

Esiste anche una modalità `Personalizzato` che consente una configurazione più dettagliata, particolarmente utile quando si gestiscono tre o più connessioni WAN. Questa modalità offre una maggiore flessibilità nella gestione del traffico tra le diverse connessioni WAN.

Nella modalità personalizzata della configurazione Multi-WAN, si applicano i seguenti concetti:

- Livelli di priorità indipendenti: ogni livello di priorità funziona in modo indipendente dagli altri. Le interfacce WAN all'interno di un determinato livello di priorità non influenzano e non dipendono dalle interfacce presenti in altri livelli.
- Più interfacce WAN all'interno di un livello di priorità: ogni livello di priorità può contenere due o più interfacce WAN. Queste interfacce sono raggruppate insieme per impostazioni di configurazione specifiche.

- I pesi determinano la distribuzione del traffico: i pesi assegnati alle interfacce WAN all'interno di un livello di priorità determinano come il traffico viene distribuito tra queste interfacce. Pesi più alti indicano una maggiore proporzione di allocazione del traffico.
- La priorità diminuisce con i nuovi livelli: aggiungere un nuovo livello di priorità comporta che le interfacce all'interno di questo livello abbiano una priorità inferiore. Esse vengono utilizzate solo se tutte le interfacce nel livello precedente falliscono.

Si consideri uno scenario in cui le prime due interfacce WAN sono configurate in modalità bilanciamento, e l'ultima interfaccia funge da backup nel caso in cui entrambe le prime due interfacce risultino non disponibili.

1. Selezionare le prime due interfacce WAN e impostarle in modalità bilanciamento assegnando dei pesi a entrambe in base alle prestazioni della connessione Internet.
2. aggiungere un nuovo livello di priorità facendo clic sul pulsante *Aggiungi livello di priorità*
3. selezionare la terza interfaccia WAN e assegnare un peso. Tuttavia, in questo scenario, il peso non influenza la distribuzione del traffico poiché è l'unica interfaccia a questo livello. Funziona come backup, entrando in gioco solo se entrambe le interfacce del livello precedente falliscono.

20.1 Regole di instradamento

Gli utenti possono creare regole di traffico in uscita basate su criteri specifici come IP sorgente, IP di destinazione, porta(e) sorgente, porta(e) di destinazione e tipi di protocollo IP. Questa funzionalità di routing basato su policy consente di personalizzare quali connessioni in uscita utilizzano specifiche interfacce WAN, permettendo una configurazione di rete altamente personalizzata.

Ecco come è possibile creare una regola personalizzata:

1. Creare una nuova policy: per iniziare a personalizzare l'instradamento del traffico, iniziare creando una nuova policy. Fare clic sul pulsante *Crea policy* per avviare il processo.
2. Crea una nuova regola: quindi fare clic sul pulsante *Crea regola*. Questo passaggio consente di definire condizioni specifiche in base alle quali il traffico verrà instradato in modo diverso rispetto alla policy predefinita.
3. Assegnare un nome significativo alla regola: assegnare un nome descrittivo e significativo alla regola. Questo nome dovrebbe riflettere lo scopo o le condizioni della regola di instradamento del traffico per facilitarne l'identificazione.
4. Specificare il tipo di traffico: definire i criteri per il traffico che si desidera personalizzare. Questo può includere l'indirizzo IP sorgente, l'indirizzo IP di destinazione, protocolli specifici, porte o qualsiasi combinazione di questi fattori. Specificando questi parametri, si restringe l'ambito della regola a uno specifico tipo di traffico. Con i campi `Indirizzo sorgente` e `Indirizzo di destinazione`, è possibile scegliere tra le seguenti opzioni:
   - Immettere un indirizzo o un intervallo: specificare un singolo indirizzo IP o un CIDR. È supportato solo IPv4.
   - Qualsiasi indirizzo: selezionare questa opzione per corrispondere a qualsiasi indirizzo.
   - Selezionare un oggetto firewall: scegliere dall'elenco degli oggetti firewall predefiniti.
5. Selezionare la policy creata per questo tipo di traffico: scegliere la policy personalizzata creata nel primo passaggio come preferenza di instradamento per questo specifico tipo di traffico. Associando la regola a una determinata policy, si indica al sistema di instradare il traffico definito secondo le impostazioni specificate all'interno di quella policy.

- Opzione `Sticky`: L'opzione sticky di una regola garantisce che il traffico proveniente dallo stesso IP di origine esca sempre attraverso la stessa WAN per una durata di 10 minuti. Questo può prevenire problemi durante la connessione a siti web di banche, compagnie assicurative, ecc. Questa opzione viene tipicamente utilizzata per il traffico HTTPS (443/TCP).

Le seguenti sono le opzioni disponibili per definire le porte di traffico:

- <port>: Porta singola
- <porta>,<porta>: Elenco di porte
- <port>-<endport>: Intervallo da <port> a <endport>

20.2 Impostazioni generali

NethSecurity monitora ciascuna connessione WAN utilizzando test ICMP ripetuti.

La pagina `Impostazioni generali` consente di specificare i seguenti parametri:

- Elenco degli host da monitorare: è possibile definire un elenco di host (computer, server o dispositivi) che il sistema monitorerà per lo stato di connettività. Questi host vengono controllati per garantire che siano raggiungibili tramite la rete.
- Numero di pacchetti ICMP (ping) da inviare: è possibile impostare il numero di pacchetti ICMP (Internet Control Message Protocol) da inviare durante ciascun test di monitoraggio. Impostando il numero di pacchetti, si può controllare l'intensità del monitoraggio.
- Determinazione dell'irraggiungibilità dopo quanti test falliti: è possibile configurare il sistema per stabilire quando una connessione WAN deve essere considerata irraggiungibile. Questo viene fatto specificando una soglia, ovvero dopo quanti test consecutivi falliti la connessione WAN viene considerata irraggiungibile.

20.3 Reset configurazione

Avvertimento: Questo reimposterà effettivamente la configurazione MultiWAN, con una perdita della connessione Internet se nessuna WAN è configurata.

Se il firewall era stato precedentemente configurato con due o più interfacce WAN e, dopo la riconfigurazione, è presente solo una interfaccia WAN, si consiglia di reimpostare la configurazione MultiWAN. In questo modo si garantirà che il firewall sia configurato correttamente e funzioni come previsto.

```
/usr/libexec/rpcd/ns.mwan call clear_config
uci commit mwan3
reload_config
```

CAPITOLO 21

Hotspot

L'obiettivo principale dell'Hotspot è fornire connettività Internet tramite wi-fi agli utenti occasionali. Gli utenti vengono reindirizzati a un captive portal dal quale possono accedere alla rete autenticandosi tramite social login, sms, email o un codice voucher. Il servizio hotspot consente la regolamentazione, la tracciabilità e la tariffazione dell'accesso a Internet in luoghi pubblici, come piazze, hotel, stazioni e molti altri.

21.1 Funzionalità principali

- Isolamento della rete tra azienda e ospiti
- Pagina del captive portal personalizzabile
- Sono supportate molte modalità di autenticazione (Social Login, SMS, Email o codice Voucher)
- Supporto AutoLogin
- Gestore hotspot con diversi tipi di accesso (admin, cliente, desk)
- Esportazione del report di account e connessioni

21.2 Come funziona?

L'implementazione si basa su 2 componenti:

Una sezione del gestore hotspot in esecuzione su un server cloud, una WebUI dedicata consente di eseguire attività quali:

- creare un'istanza hotspot: di solito ogni istanza fa riferimento a una posizione specifica (ad esempio, Art Cafè, Ritz Hotel e così via)
- modificare la pagina del captive portal
- scegliere quale tipo di accesso utilizzare
- vedere sessione e utenti connessi

Una parte client in esecuzione su NethSecurity (in terminologia nethspot questo client è chiamato «unità»).

- Deve essere fisicamente connesso alla rete degli Access Points
- Assegna indirizzi IP ai dispositivi
- Reindirizza i dispositivi al captive portal

Nota: Questo manuale copre solo la parte client. Se si è interessati alla sezione hotspot manager, fare riferimento al progetto Icaro per creare una propria istanza di Icaro oppure contattare info@nethesis.it se si desidera utilizzare il servizio SaaS fornito da Nethesis e disponibile su my.nethspot.com.

21.3 Stato

Questa sezione mostra tutti gli utenti connessi al sistema, distinguendo tra coloro che si sono autenticati e coloro che hanno semplicemente ricevuto un indirizzo IP; vengono fornite ulteriori informazioni come l'indirizzo MAC, il traffico effettuato e così via. Informazioni più dettagliate sono disponibili nel gestore hotspot.

21.4 Impostazioni

Questa sezione consente di associare un'unità a una specifica istanza di hotspot creata nel gestore degli hotspot.

Nota: Prima di associare l'unità è necessario creare un'istanza nel gestore degli hotspot.

Più unità geograficamente separate (NethSecurity) possono essere collegate alla stessa istanza centralizzata di hotspot, creando una conferenza in cui tutti gli utenti accedono allo stesso captive portal e possono riutilizzare le stesse credenziali di accesso in tutte le unità collegate.

21.4.1 Accedere al proprio gestore hotspot

Questa operazione è obbligatoria per associare l'unità all'istanza hotspot creata; utilizzare lo stesso utente e la stessa password del proprio hotspot manager. Il campo `Nome host` per impostazione predefinita punta a my.nethspot.com.

Una volta effettuato l'accesso, è possibile continuare a compilare i seguenti campi. Questo accesso rimarrà attivo per 24 ore senza la necessità di effettuare nuovamente il login.

21.4.2 Registrare l'unità

`Hotspot parent` : scegliere a quale istanza si desidera collegare l'unità

`Nome unità` : il nome del proprio NethSecurity

`Descrizione unità` : inserire una breve descrizione per identificare più facilmente l'unità

`Dispositivo di rete` : Specificare un dispositivo di rete da utilizzare per il servizio hotspot. Il dispositivo può essere sia fisico che una VLAN; tuttavia, è fondamentale che il dispositivo non sia già configurato. L'interfaccia utente mostrerà tutte le opzioni attualmente disponibili e l'hotspot intercetterà tutte le connessioni su questa interfaccia di rete, imponendo l'autenticazione per i client connessi.

`Indirizzo di rete` : i client riceveranno un indirizzo IP appartenente a questa rete (utilizzare il formato CIDR). Il primo indirizzo della classe di rete viene sempre assegnato all'interfaccia hotspot di NethSecurity. Il numero totale di client che possono essere gestiti contemporaneamente dipende dall'intervallo DHCP specificato. Se è necessario fornire il servizio hotspot per più di 253 dispositivi, considerare l'utilizzo di una netmask più ampia (/23 o /22 o anche superiore) e assicurarsi di avere un intervallo appropriato.

`Limite DHCP` : per impostazione predefinita, il sistema utilizza l'intera gamma della rete. Tuttavia, è possibile definire un intervallo più specifico regolando il numero massimo di lease. Il primo indirizzo dell'intervallo DHCP viene calcolato automaticamente.

Dopo aver compilato il modulo, fare clic sul pulsante *Salva* per registrare l'unità.

Nota: Verificare in Hotspot manager -> Units che l'unità sia stata registrata correttamente. Ogni unità registrata correttamente deve mostrare il proprio indirizzo MAC nel Hotspot manager`. Se l'indirizzo MAC è assente, annullare la registrazione dell'unità e ripetere la procedura di registrazione.

21.4.3 Annullare la registrazione dell'unità

Se è stato commesso un errore durante la registrazione dell'unità (ad esempio, l'unità è stata associata a un'istanza hotspot errata) oppure si desidera rimuovere questo servizio, effettuare l'accesso nella sezione hotspot di NethSecurity e fare clic su *Rimuovi registrazione unità hotspot*. L'unità verrà rimossa sia da NethSecurity sia dal gestore hotspot remoto, l'interfaccia utilizzata in NethSecurity verrà liberata e potrà essere utilizzata per altri scopi.

21.4.4 Modificare le impostazioni DNS

Per impostazione predefinita, il server DNS utilizzato dall'hotspot è quello di OpenDNS; per modificare le impostazioni DNS è necessaria una configurazione manuale. Seguire i passaggi riportati di seguito dal terminale:

1. Modificare il file di configurazione UCI con i seguenti comandi:

```
uci set dedalo.config.dns1='<insert dns 1>'
uci set dedalo.config.dns2='<insert dns 2>'
```

2. Salvare le modifiche con il seguente comando:

```
uci commit dedalo
```

3. Riavviare il servizio dedalo con:

```
service dedalo restart
```

21.4.5 Ripristinare le impostazioni DNS predefinite

Per ripristinare le impostazioni DNS predefinite, utilizzare i seguenti comandi:

```
uci delete dedalo.config.dns1
uci delete dedalo.config.dns2
```

Quindi ripetere i passaggi 2 e 3 della sezione precedente per applicare le modifiche.

CAPITOLO 22

Certificati e reverse proxy

22.1 Reverse proxy

NethSecurity fornisce un reverse proxy utilizzando nginx. Un reverse proxy, talvolta chiamato anche proxy pass, è un server che si trova davanti a uno o più web server e inoltra le richieste verso di essi. Può essere utilizzato per migliorare le prestazioni, la sicurezza e l'affidabilità.

In termini più semplici, un reverse proxy è come un vigile del traffico per i server web. Instrada le richieste in arrivo al server appropriato e restituisce le risposte.

I reverse proxy sono spesso utilizzati per migliorare le prestazioni memorizzando nella cache i contenuti statici e distribuendo il traffico su più server. Possono anche essere utilizzati per aumentare la sicurezza implementando l'endpoint TLS.

Nota: Il reverse proxy è disponibile solo sulla porta 443 (HTTPS) e *non* sulla porta 80 (HTTP).

Questa pagina consente di configurare le impostazioni di proxy pass, specificando se la regola si applica a un dominio o a un percorso. Per le configurazioni di dominio, è possibile selezionare un certificato. L'URL di destinazione determina dove vengono inoltrate le richieste in ingresso e il campo rete consentita offre la possibilità di limitare l'accesso a specifiche reti in formato CIDR. È possibile aggiungere una descrizione per maggiore chiarezza.

Per configurare un nuovo proxy pass, fare clic su *Aggiungi reverse proxy* e personalizzare le seguenti opzioni:

- `Tipo`: scegliere tra Dominio o Percorso. Se il tipo è `Percorso`, inserire il percorso della risorsa iniziando con una "/" per le regole di corrispondenza (ad esempio, `/resource-path`). Se il tipo è `Dominio`, inserire il nome di dominio completo per le regole di corrispondenza del sito web. Selezionare anche un *certificato* associato.
- `URL di destinazione`: specificare la posizione di inoltro per le richieste in arrivo (ad esempio, `http://destination-server:port/path`).
- `Reti permesse`: definire le reti IPv4/IPv6 consentite in formato CIDR. Per impostazione predefinita, accessibile da qualsiasi luogo.
- `Descrizione`: facoltativamente, aggiungere una descrizione per maggiore chiarezza.

Informazioni aggiuntive:

- Header verso il server di destinazione: X-Forwarded-Proto, X-Forwarded-For, X-Real-IP sono sempre inviati.
- Validazione del certificato: se la destinazione utilizza HTTPS, il certificato non viene validato per evitare errori su server configurati in modo errato.
- Supporto WebSocket: tutti i reverse proxy supportano automaticamente i WebSocket.

22.1.1 Proxy sulla porta 80 (HTTP)

NethSecurity 8 ascolta solo su HTTPS (porta 443) per le regole di reverse proxy. Questo differisce da NethSecurity 7, dove il reverse proxy ascoltava sia su HTTP (porta 80).

Durante la migrazione da NethSecurity 7, alcuni servizi o segnalibri utente potrebbero ancora utilizzare HTTP. Poiché NethSecurity 8 non ascolta sulla porta 80 per impostazione predefinita, tali collegamenti HTTP non raggiungeranno più il reverse proxy e potrebbero risultare non funzionanti per gli utenti.

Abilitare la porta 80 può esporre i servizi, inclusa la web UI, su canali non crittografati. Per questo motivo, l'approccio raccomandato è mantenere il reverse proxy in ascolto solo su un canale sicuro e fornire un reindirizzamento permanente (301) da HTTP a HTTPS.

Per creare un reindirizzamento globale da HTTP a HTTPS, accedere al terminale e inserire i seguenti comandi:

```
uci set nginx._cleartext=server
uci add_list nginx._cleartext.listen='80 default_server'
uci add_list nginx._cleartext.listen='[::]:80 default_server'
uci set nginx._cleartext.return='301 https://$host$request_uri'
uci set nginx._cleartext.server_name='_'
uci commit nginx
/etc/init.d/nginx reload
```

Dopo aver abilitato il reindirizzamento, accedere alla pagina delle regole del firewall e assicurarsi che la porta 80 sia aperta sul lato WAN per consentire le connessioni in ingresso.

22.1.2 Nascondere la versione del server web

Per impostazione predefinita, il reverse proxy nginx include il proprio numero di versione negli header di risposta HTTP. Molte valutazioni delle vulnerabilità si basano sull'identificazione della versione del software, il che può generare falsi positivi quando le correzioni vengono retroportate senza modificare la versione riportata. Sebbene nascondere le informazioni sulla versione non migliori la sicurezza di per sé, può contribuire a limitare l'esposizione di vulnerabilità note e specifiche della versione agli strumenti di scansione automatizzati.

Per disabilitare la visualizzazione della versione di nginx negli header HTTP del reverse proxy, è necessario configurare la direttiva `server_tokens` nelle configurazioni del server nginx.

Per prima cosa, identificare le configurazioni del server nginx:

```
uci show nginx | grep "=server"
```

Questo mostrerà i blocchi server configurati nel sistema (ad esempio, `nginx._lan=server`, `nginx.ns_88e3b6fd=server`).

Quindi, per ciascun blocco server che si desidera configurare, impostare `server_tokens` su `off`. Ad esempio, per configurare il server `_lan`:

```
uci set nginx._lan.server_tokens='off'
uci commit nginx
reload_config
```

Se sono presenti ulteriori blocchi server personalizzati (come `ns_88e3b6fd` nell'esempio), applicare la stessa configurazione:

```
uci set nginx.ns_88e3b6fd.server_tokens='off'
uci commit nginx
reload_config
```

Per applicare questa impostazione globalmente a tutti i server reverse proxy contemporaneamente, è possibile utilizzare uno script:

```
for server in $(uci show nginx | grep "=server$" | cut -d. -f2 | cut -d= -f1); do
  uci set nginx.$server.server_tokens='off'
done
uci commit nginx
reload_config
```

22.2 Certificati

La pagina `Certificati` centralizza le funzionalità di gestione dei certificati, facilitando la gestione dei certificati sul firewall. Al primo avvio del firewall, viene generato automaticamente un certificato autofirmato. Questo certificato funge da opzione sicura predefinita.

La pagina di gestione dei certificati consente di caricare certificati personalizzati, richiedere certificati da Let's Encrypt e gestire i certificati esistenti.

La pagina elenca tutti i certificati, evidenziando il certificato predefinito. Per impostare un certificato come certificato predefinito, fare clic sul pulsante *Imposta come predefinito*. Il certificato predefinito è quello servito automaticamente quando si accede all'"*interfaccia web utente*, sia sulla porta 443, sia sulla *9090 o su una porta personalizzata*.

22.2.1 Let's Encrypt

Let's Encrypt è una Certificate Authority (CA) gratuita, automatizzata e aperta che fornisce certificati SSL/TLS per la protezione dei siti web. Questi certificati garantiscono una comunicazione crittografata tra i server web e i browser degli utenti, migliorando la sicurezza e la privacy su Internet. A differenza delle CA tradizionali, Let's Encrypt offre certificati SSL tramite un sistema automatizzato, rendendoli accessibili ai proprietari e agli amministratori di siti web senza costi significativi o particolari competenze tecniche.

La pagina del certificato consente di richiedere certificati da Let's Encrypt. Il processo è semplice e richiede una configurazione minima. È possibile specificare un nome significativo per il certificato e uno o più domini. Il certificato viene rinnovato automaticamente ogni 60 giorni.

Il processo di richiesta del certificato Let's Encrypt prevede i seguenti passaggi:

- fare clic sul pulsante *Aggiungi certificato Let's Encrypt*;
- specificare un nome significativo per il certificato;
- specificare uno o più domini per il certificato;
- fare clic sul pulsante *Salva*.

Il processo di validazione può essere eseguito in due modi:

- Modalità standalone (validazione HTTP): la modalità standalone prevede l'arresto temporaneo del server web per consentire allo strumento client ACME di collegarsi direttamente alle porte richieste. Serve le challenge di autenticazione per dimostrare la proprietà del dominio, ottenendo e installando il certificato.
- Validazione DNS: la validazione DNS richiede l'aggiunta di uno specifico record DNS TXT alla configurazione DNS del dominio. Il client ACME verifica la presenza di questo record per confermare la proprietà del dominio. Questo metodo è utile in situazioni in cui modificare la configurazione del server web risulta difficile o non è desiderato.

Quando viene selezionata la modalità standalone, assicurarsi che siano soddisfatti i seguenti requisiti:

1. Il firewall deve essere raggiungibile dall'esterno sulla porta 80. Il client acme:
   - associare temporaneamente alla porta 80 per servire le sfide di autenticazione
   - apri temporaneamente la porta 80 verso Internet pubblico per eseguire la convalida.

   Una volta completata la convalida, la porta 80 viene chiusa automaticamente. Si noti che, se la porta 80 è inoltrata a un altro server, la convalida non andrà a buon fine.
2. I domini per cui si desidera il certificato devono essere nomi di dominio pubblici associati all'indirizzo IP pubblico del server. Assicurarsi di avere un nome DNS pubblico che punti al proprio server (è possibile verificare con siti come VDNS).

Selezionare la convalida DNS se il proprio provider DNS supporta l'accesso tramite API. Scegliere il provider DNS dal menu a discesa e inserire la chiave API e il segreto. Consultare la documentazione dei provider DNS di acme.sh per sapere quale chiave API e quale segreto sono richiesti dal proprio provider DNS. La convalida DNS è l'unica supportata per i certificati wildcard.

Il processo di generazione del certificato può richiedere alcuni minuti. Durante questo periodo, lo stato del certificato è `In attesa`.

Debug Let's Encrypt

Se la richiesta del certificato Let's Encrypt fallisce, è possibile eseguire il debug del processo inserendo i seguenti comandi nel terminale:

```
uci set acme.@acme[0].debug=1
/etc/init.d/acme start
```

I messaggi di debug verranno stampati sull'output standard. Dopo che il problema è stato risolto, è possibile disabilitare il debug inserendo il seguente comando nel terminale:

```
uci revert acme
```

22.2.2 Certificato personalizzato

L'utente può caricare un certificato personalizzato nel firewall.

Il processo prevede i seguenti passaggi:

- fare clic sul pulsante *Importa certificato*
- specificare un nome significativo per il certificato
- trascinare e rilasciare il certificato, la chiave privata e, facoltativamente, il certificato della catena; assicurarsi che tutti i file caricati rispettino gli standard del formato PEM

- fare clic sul pulsante *Salva*

CAPITOLO 23

Quality of Service (QoS)

NethSecurity QoS fornisce funzionalità di Active Queue Management (AQM) e Flow Queuing (FQ) per garantire che le risorse di rete vengano utilizzate in modo efficiente ed equo.

23.1 Principi di funzionamento

NethSecurity QoS è progettato per sfruttare al meglio la banda disponibile, senza imporre limiti rigidi o shaping del traffico come impostazione predefinita. Funziona secondo i seguenti principi:

- *Utilizzo della larghezza di banda*: QoS si impegna a sfruttare al massimo la banda disponibile. Per impostazione predefinita, non impone limiti rigorosi alla larghezza di banda della rete. Invece, si adatta dinamicamente alle condizioni della rete, garantendo che la banda non utilizzata venga sfruttata in modo efficiente.
- *Gestione dei flussi*: QoS gestisce attivamente i flussi di rete per evitare che un singolo client o applicazione monopolizzi la banda disponibile. Questo garantisce un accesso equo e imparziale alle risorse di rete per tutti gli utenti.

23.2 Configurazione

La gestione della banda viene gestita in modo dinamico e automatico dal sistema. La configurazione è semplice e consiste nell'impostare i valori di larghezza di banda in upload e download per ciascuna interfaccia sotto QoS.

Sebbene il QoS possa essere configurato su qualsiasi interfaccia, generalmente funziona in modo ottimale sulle interfacce di tipo WAN, impostando le velocità di upload e download ai valori della connessione dati a Internet.

Per garantire la resilienza contro le fluttuazioni del servizio, è consigliabile mantenere un margine di sicurezza configurando questi parametri al 10% in meno rispetto ai valori misurati.

23.3 Configurazione avanzata

QoS si basa su un classificatore eBPF (Extended Berkeley Packet Filter) per impostare i campi Differentiated Services Code Point (DSCP) nei pacchetti. Questa classificazione aiuta a dare priorità e a gestire il traffico di rete in modo efficiente. Per massimizzare l'efficienza, QoS opera nello spazio kernel utilizzando la tecnologia eBPF. Questo garantisce un overhead minimo e un impatto minimo sulle prestazioni del sistema. Oltre alle regole basate su IP e porta, QoS consente di definire regole di traffico basate su nomi DNS, offrendo un controllo granulare su come il traffico viene classificato e gestito.

Sebbene Qosify funzioni efficacemente senza una configurazione approfondita, può essere ulteriormente ottimizzato impostando limiti di banda e regole. Una regolazione fine dei parametri QoS può portare a prestazioni di rete ancora migliori.

Le modifiche al comportamento standard, tuttavia, possono essere utili solo in scenari molto limitati, per i quali, attualmente, è possibile intervenire esclusivamente tramite la riga di comando.

23.3.1 Classi di priorità

QoS utilizza quattro classi di priorità, ciascuna delle quali può utilizzare una percentuale massima di banda definita dalla propria soglia.

- **Bulk (CS1, LE nel kernel v5.9+):** Questa classe è progettata per il traffico a bassa priorità, con una soglia del 6,25%.
- **Best Effort (Generale):** Questa classe ha una soglia del 100% ed è utilizzata per il traffico tipico, non prioritario.
- **Video (AF4x, AF3x, CS3, AF2x, CS2, TOS4, TOS1):** Il traffico video rientra in questa classe, con una soglia del 50%.
- **Voce (CS7, CS6, EF, VA, CS5, CS4):** Il traffico voce riceve la massima priorità, con una soglia del 25%.

QoS può temporaneamente ridurre la priorità di un flusso se questo genera una quantità significativa di traffico, parametro che è configurabile. Ad esempio, un flusso potrebbe essere temporaneamente spostato alla priorità `Bulk` se invia un numero elevato di pacchetti in un breve periodo di tempo. QoS può anche dare priorità ai pacchetti di piccole dimensioni per garantire una trasmissione a bassa latenza dei dati sensibili al tempo.

Oltre alle regole basate su IP e porta, QoS consente di definire regole di traffico basate su nomi DNS, offrendo un controllo granulare su come il traffico viene classificato e gestito.

Per eseguire l'override della classificazione DSCP, creare un file `/etc/qosify/10-custom.conf` con le mappature: ogni riga contiene due campi separati da uno spazio, match e dscp.

La corrispondenza è una delle seguenti:

- `tcp:<porta>[-<porta-finale>]`
  Porta TCP singola, o intervallo da <port> a <endport>
- `udp:<porta>[-<portafine>]`
  Porta UDP singola, o intervallo da <port> a <endport>
- `<ipaddr>`
  Indirizzo IPv4, ad esempio 1.1.1.1
- `<ipv6addr>`
  Indirizzo IPv6, ad es. ff01::1
- `dns:<pattern>`
  Modello fnmatch() che supporta * e ? come caratteri jolly

- **dns:/<regex>**
  Espressione regolare estesa POSIX.2 per la corrispondenza dei nomi host. Funziona solo se le ricerche DNS vengono passate a qosify tramite la chiamata ubus add_dns_host.
- **dns_c:...**
  Come dns, ma corrisponde solo alle voci cname

Il dscp può essere un valore grezzo oppure un codepoint come CS0. Aggiungendo un + davanti al valore si indica a qosify di sovrascrivere il valore DSCP solo se è zero.

Esempio:

```
tcp:80                +voice
216.58.204.238        video
dns:nethesis.it       +CS7
```

23.4 Risoluzione dei problemi

Ispezionare lo stato di qosify con `qosify-status`, verificare i pacchetti nelle 4 classi.

CAPITOLO 24

Database utenti

NethSecurity introduce il supporto per due tipi di database utenti: un database locale e un database LDAP remoto, migliorando le capacità di gestione degli utenti. Gli utenti presenti nei database possono essere utilizzati per le connessioni VPN, inclusa la *OpenVPN Road Warrior*.

Solo gli utenti con una password possono connettersi alla VPN autenticandosi con nome utente e password. Gli utenti senza password possono connettersi alla VPN autenticandosi tramite certificato o altri metodi di autenticazione.

24.1 Database locale

Il database utenti locale è una componente intrinseca del firewall, è disponibile di default e non richiede alcuna configurazione aggiuntiva. Funziona come un sistema di gestione utenti integrato, consentendo agli amministratori di creare e gestire utenti direttamente sul firewall. Si integra inoltre perfettamente con i servizi VPN, in particolare con il server OpenVPN Road Warrior.

Per creare un nuovo utente, fare clic sul pulsante *Aggiungi utente* per avviare la procedura. Durante la configurazione di un utente locale, è necessario compilare tutti i seguenti campi:

- `Nome utente`: specifica il nome utente desiderato.
- `Nome visualizzato`: specifica il nome visualizzato dell'utente. Questo campo è facoltativo.
- `Password utente`: specifica la password dell'utente. Questo è richiesto solo se la VPN è configurata per utilizzare l'autenticazione tramite password.
- `Conferma password`: specifica la password dell'utente; assicurarsi che la password corrisponda a quella inserita nel campo precedente.

Il database utenti locale è implementato come file di configurazione UCI. Le password degli utenti locali sono memorizzate nel formato Unix passwd, garantendo compatibilità e sicurezza nel database utenti locale.

Agli utenti presenti nel database locale possono essere concessi *privilegi amministrativi* sull'interfaccia web abilitando l'opzione `Utente amministratore`. L'utente deve avere una password impostata.

24.2 Database remoti

Subscription richiesta

Questa funzionalità è disponibile solo se il firewall dispone di una subscription valida.

L'amministratore può estendere le funzionalità del firewall aggiungendo nuovi database remoti. I database remoti consentono al firewall di autenticare gli utenti tramite un server LDAP esterno, come Active Directory o OpenLDAP.

A differenza degli utenti locali, gli utenti presenti in database remoti devono essere gestiti direttamente sul server LDAP di origine. Qualsiasi aggiunta, eliminazione o modifica degli account utente deve essere eseguita sul server LDAP stesso, poiché queste modifiche saranno riflesse nella pagina di configurazione del firewall ma non potranno essere effettuate dall'interfaccia del firewall.

Si noti inoltre che, se il database remoto è offline, l'autenticazione VPN non andrà a buon fine. È fondamentale assicurarsi che il database remoto sia online e accessibile per garantire una corretta autenticazione degli utenti tramite il servizio VPN.

Quando si configura un database remoto, fare clic sul pulsante *Aggiungi database remoto* e compilare tutti i seguenti campi:

- `LDAP URI`: specifica l'Uniform Resource Identifier (URI) LDAP, includendo l'indirizzo del server e la porta (ad esempio, `ldap://example.com:389`).
- `Tipo`: specifica il tipo di server LDAP. Le opzioni disponibili sono `Active Directory` e `OpenLDAP`. Se viene selezionato OpenLDAP, il server remoto deve rispettare lo schema RFC 2307.
- `Base DN`: specifica il Base Distinguished Name (DN) di LDAP, che rappresenta il punto di partenza per le ricerche nella directory LDAP (ad es. `dc=example,dc=com`).
- `Utente DN`: specifica il Distinguished Name (DN) dell'utente LDAP. Se non presente, il valore predefinito è uguale a base_dn (ad es. `cn=users,dc=example,dc=com`).
- `Campo d'attributo utente`: specifica l'attributo utente utilizzato per identificare l'utente; questa opzione viene utilizzata dal server OpenVPN road warrior per comporre il bind DN dell'utente. Dovrebbe essere `cn` per Active Directory oppure `uid` per OpenLDAP.

  Questo campo viene utilizzato per autenticare gli utenti nel server OpenVPN road warrior. Il processo di autenticazione si basa su un'operazione di bind LDAP che utilizza il campo attributo utente per comporre il bind DN dell'utente con il DN dell'utente. Esempio: dato un utente chiamato `jdoe` nella directory OpenLDAP, il bind DN dell'utente viene composto come `uid=jdoe,ou=People,dc=directory,dc=nh`.
- `Nome utente`: specifica l'attributo utente che contiene il nome completo dell'utente, come *John Doe*. Di solito è `cn` per OpenLDAP e `displayName` per Active Directory.
- `User bind DN personalizzato`: se questo campo è impostato, sovrascrive il user bind DN calcolato utilizzato per autenticare gli utenti nel server OpenVPN road warrior. Il campo può contenere un segnaposto `%u` che viene sostituito con il nome utente durante il processo di autenticazione. Utilizzare questa impostazione se non si sa se il campo CN dell'utente contiene il nome completo dell'utente, come `John Doe`, o il nome utente, come `jdoe`. Se il server remoto è un server Active Directory, è possibile utilizzare uno dei seguenti valori:
  - `%u@domain.local`: dove *domain.local* è il nome di dominio del server Active Directory; all'interno del client OpenVPN, per autenticare l'utente utilizzare solo il nome utente come `jdoe`
  - `DOMAIN\%u`: dove *DOMAIN* è il realm del server Active Directory; all'interno del client OpenVPN, per autenticare l'utente utilizzare solo il nome utente come `jdoe`

  Se il server remoto è un OpenLDAP è possibile lasciare questo campo vuoto oppure specificarlo come `uid=%u,dc=directory,dc=nh`.

- `Bind DN`: specifica il Distinguished Name (DN) di Bind LDAP, che rappresenta l'utente utilizzato per effettuare il bind al server LDAP. Per un server OpenLDAP, di solito è qualcosa come `uid=ldapservice,dc=directory,dc=nh`, mentre per un server Active Directory, di solito è qualcosa come `ldapservice@example.com` oppure `cn=ldapservice,cn=Users,dc=example,dc=com`.
- `Password di bind`: specifica la password dell'utente utilizzato per effettuare il bind al server LDAP.
- `StartTLS`: abilita StartTLS per la comunicazione sicura con il server LDAP; dovrebbe essere disabilitato se l'URI LDAP utilizza già lo schema `ldaps://`.
- `Verifica certificato TLS`: determina se abilitare o disabilitare la validazione del certificato; deve essere disabilitata se il server LDAP utilizza un certificato autofirmato.

24.3 Configurazioni consigliate

Le seguenti configurazioni sono suggerite per i server LDAP più comuni. Durante la configurazione del database remoto:

- assicurarsi che il server LDAP sia raggiungibile dal firewall. Se l'URI LDAP contiene un nome host, verificare che il nome host sia risolvibile
- sostituire i valori di esempio con i valori effettivi del server LDAP
- per Active Directory, si consiglia di utilizzare `User bind DN personalizzato` per specificare come il server OpenVPN deve autenticare l'utente

24.3.1 OpenLDAP (RFC 2307)

È possibile accedere a NethServer 7 OpenLDAP senza autenticazione:

- URI LDAP: `ldap://ns7ldap.nethserver.org`
- Tipo: `OpenLDAP`
- Base DN: `dc=directory,dc=nh`
- DN utente: `ou=People,dc=directory,dc=nh`
- Campo attributo utente: `uid`
- Campo nome visualizzato utente: `cn`

Se si desidera utilizzare l'autenticazione inserendo Bind DN e Bind Password, ricordarsi di abilitare StartTLS.

24.3.2 Active Directory

Per accedere a NethServer 7 Samba Active Directory o Windows Server 2012 Active Directory, utilizzare la seguente configurazione:

- URI LDAP: `ldap://dcserver.ad.example.com`
- Tipo: `Active Directory`
- Base DN: `dc=example,dc=com`
- DN utente: `cn=Users,dc=example,dc=com`
- Campo attributo utente: `sAMAccountName`
- Campo nome visualizzato utente: `displayName`

- DN di binding utente personalizzato: `%u@example.com`
- Bind DN: `<user>@exampl.com` oppure `cn=<user>,cn=Users,dc=example,dc=com`, dove `<user>` è il nome utente dell'utente utilizzato per effettuare il bind al server LDAP
- Password di Bind: `<password>`, dove `<password>` è la password dell'utente inserito nel campo Bind DN

L'opzione `StartTLS` dovrebbe essere abilitata per NethServer 7 Samba Active Directory, mentre di solito dovrebbe essere disabilitata per Windows Server 2012 Active Directory.

CAPITOLO 25

Oggetti firewall

Gli oggetti firewall sono insiemi predefiniti di indirizzi di rete che possono essere utilizzati per semplificare e ottimizzare la configurazione del firewall. Questi oggetti consentono di raggruppare indirizzi IP, reti o nomi di dominio correlati in unità riutilizzabili, facilitando la creazione e la gestione di regole firewall, port forwarding e altre policy di rete.

I vantaggi dell'utilizzo degli oggetti firewall includono:

- organizzazione e leggibilità migliorate della configurazione del firewall
- probabilità ridotta di errori durante l'inserimento manuale di indirizzi IP o reti
- manutenzione più semplice - l'aggiornamento di un oggetto aggiorna automaticamente tutte le regole associate
- gestione delle regole più efficiente, soprattutto per reti complesse

Gli oggetti firewall sono particolarmente utili quando sono presenti più regole che fanno riferimento allo stesso insieme di indirizzi o quando è necessario modificare frequentemente gruppi di indirizzi. Tuttavia, per configurazioni semplici con solo alcune regole statiche, l'utilizzo degli oggetti potrebbe non essere necessario e potrebbe aggiungere complessità non necessaria.

Il sistema fornisce diversi tipi di oggetti firewall:

- Lease statici (DHCP Reservation): assegnazioni IP statiche per dispositivi specifici
- Record DNS: nomi di dominio associati a indirizzi IP specifici
- Utenti VPN: utenti con indirizzi IP riservati da OpenVPN Road Warrior
- Sost set: gruppi di indirizzi IP, reti o intervalli
- Domain set: raccolte di nomi di dominio che si risolvono in indirizzi IP

25.1 Lease statici

Lease statici, note anche come DHCP reservations, permettono di assegnare indirizzi IP fissi a dispositivi specifici sulla rete. Questa funzionalità unisce la comodità del DHCP con la stabilità dell'assegnazione statica degli indirizzi IP.

Vantaggi principali:

- garantisce che i dispositivi ricevano sempre lo stesso indirizzo IP
- consente di associare nomi host facili da ricordare ai dispositivi
- semplifica la gestione e la risoluzione dei problemi della rete

Un lease statico consiste in:

- hostname: Un nome riconoscibile per il dispositivo
- Indirizzo IP: L'IP fisso che si desidera assegnare (deve essere all'interno dell'intervallo DHCP)
- Indirizzo MAC: L'identificatore hardware univoco del dispositivo

25.2 Record DNS

Record DNS consentono di creare associazioni locali tra nomi host e indirizzi IP. Questi record locali hanno la precedenza sulle query DNS esterne, offrendo un maggiore controllo sulla risoluzione dei nomi nella rete.

Un record DNS include:

- hostname: Il nome di dominio che si desidera risolvere localmente
- Indirizzo IP: L'indirizzo IP corrispondente per il nome host

Casi d'uso per i record DNS locali:

- creare collegamenti rapidi a risorse interne (ad esempio, `intranet.mycompany.local`)
- ignorare il DNS esterno per scopi di test o di sicurezza
- impostare nomi di dominio personalizzati per i servizi locali

Utilizzando lease statici e record DNS locali, è possibile creare un ambiente di rete più organizzato e facilmente gestibile. Queste funzionalità funzionano perfettamente con altri oggetti del firewall come gli host set, offrendo strumenti potenti per l'amministrazione della rete.

Per istruzioni dettagliate su come creare e gestire lease statici e record DNS, fare riferimento ai *capitoli di configurazione DHCP e DNS*.

25.3 Utenti VPN

Gli utenti *OpenVPN* con riserva di IP possono essere utilizzati come oggetti firewall, consentendo il controllo dell'accesso alla rete specifico per utente. Questa funzionalità si applica sia agli utenti locali che remoti (LDAP) configurati per l'accesso OpenVPN.

Punti chiave:

- a ciascun utente può essere assegnato un indirizzo IP OpenVPN specifico
- questi utenti possono essere referenziati nelle regole del firewall come origine o destinazione
- si applica sia agli utenti locali che a quelli remoti (LDAP)

- consente la creazione di politiche di accesso specifiche per l'utente

Casi d'uso:

- limitare gli utenti OpenVPN a specifiche risorse di rete
- creare elenchi di autorizzazione/negazione basati sull'utente
- implementare politiche di accesso basate sul tempo per utenti remoti
- monitorare e controllare l'utilizzo della banda per utente

Requisiti:

- l'utente ha l'accesso OpenVPN abilitato
- un indirizzo IP specifico è riservato per l'utente

Utilizzando gli utenti OpenVPN come oggetti firewall, è possibile creare un ambiente di rete più sicuro con politiche di accesso direttamente collegate alle identità degli utenti.

25.4 Host set

I set host sono oggetti firewall versatili che consentono di raggruppare più indirizzi IP, reti o intervalli in un'unica unità facilmente gestibile. Questi set possono essere utilizzati in diverse regole firewall, semplificando il processo di controllo del traffico per più destinazioni o sorgenti.

Caratteristiche principali dei host set:

1. Supporto versione IP:
    - disponibile sia per indirizzi IPv4 che IPv6
    - ogni host set è specifico per una versione IP
2. Contenuto flessibile, i host set possono includere:
    - indirizzi IP individuali
    - intervalli di rete in notazione CIDR
    - Intervalli IP
    - Prenotazioni DHCP
    - Nomi dei record DNS
    - Utenti VPN (solo per IPv4)
3. Gestione semplice:
    - creare, modificare o eliminare host set senza modificare direttamente le regole del firewall
    - le modifiche a un host set si applicano automaticamente a tutte le regole che utilizzano quel set
4. Casi d'uso:
    - raggruppare i server aziendali per il controllo degli accessi
    - creare elenchi di autorizzazione o negazione per segmenti di rete specifici
    - gestire l'accesso remoto per più utenti VPN

Nota: Gli host set sono pienamente supportati nella loro completezza espressiva (IP, CIDR, intervallo, raggruppamenti) all'interno delle regole del firewall. Altre pagine potrebbero supportare solo un sottoinsieme ridotto; ad esempio, MultiWAN supporta solo indirizzi IP singoli e CIDR. In questi casi, nei menu a discesa verranno visualizzati solo gli host set compatibili quando si utilizza l'oggetto all'interno della regola.

25.4.1 Gestione degli host set

Accedere alla pagina `Oggetti` nella sezione `Utenti e oggetti` dal menu laterale sinistro, quindi navigare nella scheda `Host set`.

La pagina visualizzerà un elenco degli host set esistenti, inclusi i loro nomi, le versioni IP e il numero di record in ciascun set.

All'interno dell'elenco, è possibile trovare anche oggetti host provenienti da altre sezioni come:

- Lease statici
- Record DNS
- Utenti VPN

Questi oggetti possono essere utilizzati negli host set per creare regole più complesse, ma non possono essere modificati direttamente dalla pagina degli host set.

Quando un oggetto non viene utilizzato in alcun set host né in alcuna regola del firewall, verrà contrassegnato come `non utilizzato` nell'elenco.

Per vedere dove viene utilizzato un oggetto, fare clic sul collegamento `Mostra utilizzi` accanto all'oggetto.

Si noti che gli oggetti utilizzati non possono essere eliminati finché non vengono rimossi da tutti gli host set e dalle regole del firewall.

Aggiungere un Host Set

1. Accedere alla pagina `Oggetti` nella sezione `Uteenti ed oggetti` dal menu laterale sinistro.
   - Passare alla scheda `Host set`
   - Fare clic sul pulsante *Aggiungi host set*
2. Immettere il nome dell'Host Set
   - Nel campo `Nome`, inserire un nome descrittivo per il host set
   - Utilizzare solo lettere e numeri; spazi e caratteri speciali non sono consentiti
   - Scegliere un nome che identifichi chiaramente lo scopo del gruppo di host
3. Selezionare la versione IP
   - In `Versione IP`, scegliere tra IPv4 e IPv6
   - Selezionare IPv4 per gli indirizzi standard del protocollo Internet
   - Scegliere IPv6 se si utilizza il formato di indirizzo più recente ed esteso
4. Aggiungere record
   - Nel campo `Record`, è possibile aggiungere gli host per questo set
   - Fare clic sul menu a discesa per scegliere tra le opzioni predefinite oppure inserire un valore personalizzato.

- È possibile aggiungere i seguenti tipi di record:
  - Indirizzi IP individuali (ad es., `192.168.1.10`)
  - Notazione CIDR per le reti (ad es., `10.10.0.0/24`)
  - Intervalli IP (ad es., `10.10.1.1-10.10.1.5`)
  - Oggetti creati in precedenza
- Dopo aver inserito ciascun record, fare clic su *Aggiungi record* per includerlo nell'insieme
- Ripetere questo processo per aggiungere più record secondo necessità

5. Finalizzare gli Host set
   - Verificare che tutte le informazioni inserite siano corrette
   - Se è necessario rimuovere un record, utilizzare l'icona di eliminazione (cestino) accanto ad esso
   - Una volta soddisfatti della configurazione dell'host set, fare clic su *Aggiungi host set* per crearlo.
   - Se è necessario ricominciare da capo o annullare il processo, fare clic su *Annulla*

25.5 Domain set

I domain set sono oggetti del firewall che consentono di raggruppare più nomi di dominio in un'unica unità gestibile. Questi set sono particolarmente utili per creare regole basate sugli indirizzi web anziché sugli indirizzi IP, che possono cambiare frequentemente per molti siti web.

Caratteristiche principali dei domain set:

1. Risoluzione DNS:
   - i nomi di dominio presenti nell'insieme vengono automaticamente risolti in indirizzi IP
   - la risoluzione viene aggiornata periodicamente per garantire l'accuratezza
2. Supporto versione IP:
   - può essere configurato sia per IPv4 che per IPv6
   - ogni domain set è specifico per una versione IP
3. Contenuto flessibile, i domain set possono includere:
   - nomi di dominio completamente qualificati (ad es., `www.example.com`)
   - domini wildcard (ad esempio, `example.com`, corrisponderà a tutti i sottodomini)
4. Timeout automatico:
   - I record DNS nel set vengono memorizzati nella cache per una durata specificata
   - un processo di aggiornamento automatico aggiorna periodicamente la risoluzione
5. Gestione semplice:
   - creare, modificare o eliminare insiemi di domini senza modificare direttamente le regole del firewall
   - le modifiche apportate a un domain set vengono applicate automaticamente a tutte le regole che utilizzano quel set

Casi d'uso per i domain set:

- controllo delle applicazioni: gestire l'accesso ai servizi cloud o alle piattaforme di social media

- sicurezza: creare regole di autorizzazione per domini attendibili
- prevenzione malware: creare regole di negazione per domini noti come dannosi

Vantaggi dell'utilizzo dei domain set:

- semplificare la gestione delle regole basate sugli indirizzi web
- gestire automaticamente le modifiche degli indirizzi IP dei siti web
- ridurre la necessità di aggiornamenti manuali alle regole del firewall
- fornire un modo più intuitivo per controllare l'accesso ai servizi basati sul web

Quando utilizzare i domain set:

- quando è necessario controllare l'accesso a siti web che potrebbero cambiare indirizzo IP
- per l'implementazione di politiche di filtraggio dei contenuti
- quando si gestisce l'accesso ai servizi cloud o alle applicazioni web
- per la creazione di criteri di sicurezza basati sulla reputazione del dominio

25.5.1 Temporizzazione della cache DNS

Le voci del set di domini vengono aggiornate quando dnsmasq esegue una nuova ricerca per il dominio. Se la risposta viene fornita dalla cache locale, l'IP non viene aggiunto nuovamente al set.

Consultare *Tempistica di aggiornamento del set di domini* per informazioni su come la temporizzazione della cache influisce sull'aggiornamento dei set di domini.

25.5.2 Gestire i domain set

Accedere alla pagina `Oggetti` nella sezione `Utenti e oggetti` dal menu laterale sinistro, quindi navigare nella scheda `Domain set`.

La pagina visualizzerà un elenco dei domain set esistenti, inclusi i loro nomi, le versioni IP e il numero di domini in ciascun set.

Se un insieme di domini non viene utilizzato in nessuna regola del firewall, verrà contrassegnato come `non utilizzato` nell'elenco. Per vedere dove viene utilizzato un insieme di domini, fare clic sul link `Mostra utilizzi` accanto all'insieme.

Aggiungere un Domain Set

1. Accedere all'interfaccia Aggiungi insieme di domini
   - Accedere alla pagina `Oggetti` nella sezione `Utenti e oggetti` dal menu laterale sinistro
   - Passare alla scheda `Domain set`
   - Fare clic sul pulsante *Aggiungi domain set*
2. Inserire il nome del Domain Set:
   - Nel campo `Nome`, inserire un nome descrittivo per il domain set
   - Utilizzare solo lettere e numeri; spazi e caratteri speciali non sono consentiti
   - Scegliere un nome che identifichi chiaramente lo scopo del gruppo di domini

3. Selezionare la versione IP:
    - In `Versione IP`, scegliere tra IPv4 e IPv6
    - I domini inseriti verranno risolti in IPv4 o IPv6 in base alla versione IP selezionata.
    - Se è necessario creare un domain set per entrambe le versioni IP, sarà necessario creare set separati per ciascuna.
4. Aggiungere domini:
    - Nel campo `Domini`, è possibile aggiungere i domini per questo set
    - Inserire i nomi di dominio nel campo fornito
    - Dopo aver inserito ciascun dominio, fare clic su *Aggiungi dominio* per includerlo nell'insieme.
    - Ripetere questo processo per aggiungere più domini secondo necessità
5. Finalizzare il Domain Set:
    - Verificare che tutte le informazioni inserite siano corrette
    - Se è necessario rimuovere un dominio, utilizzare l'icona di eliminazione (cestino) accanto ad esso
    - Una volta soddisfatti della configurazione del domain set, fare clic su *Aggiungi domain set* per crearlo
    - Se è necessario ricominciare da capo o annullare il processo, fare clic su *Annulla*

CAPITOLO 26

Port forward

Il firewall impedisce che le richieste provenienti da reti pubbliche accedano a quelle private. Ad esempio, se è presente un server web che opera all'interno della LAN, solo i computer della rete locale possono accedere a questo servizio. Qualsiasi tentativo effettuato da utenti esterni, al di fuori della rete locale, viene negato.

Un port forward, noto anche come port redirect o port forwarding, è una tecnica di rete utilizzata nei firewall per reindirizzare traffico di rete specifico da una combinazione di indirizzo IP e numero di porta a un'altra. Viene tipicamente impiegata per consentire agli utenti esterni di accedere a servizi o applicazioni ospitati su dispositivi all'interno di una rete locale privata.

Per i server web, le porte di ascolto comuni includono la porta 80 (HTTP) e la porta 443 (HTTPS). Quando si crea un port forwarding, è necessario specificare determinati parametri:

- `Nome`: assegnare un nome a una regola di port forwarding è utile per riferimenti e gestione futuri. Fornendo un nome descrittivo e significativo, gli amministratori di rete possono identificare facilmente lo scopo e il contesto di ogni port forwarding.
- `Tipo di traffico`: Specifica a quale traffico si applica la regola.
  - `Seleziona protocolli`: la regola si applica solo ai protocolli selezionati. I protocolli devono essere selezionati nel campo seguente.
  - `Tutto il traffico`: la regola si applica a tutto il traffico in ingresso indipendentemente dal protocollo, che viene inoltrato all'indirizzo IP di destinazione configurato senza ulteriori filtri. Quando questa opzione è selezionata, il modulo viene ridotto e deve essere configurato solo l'indirizzo IP di destinazione. Utilizzare questa impostazione con cautela, poiché potrebbe esporre il sistema a traffico indesiderato o potenzialmente dannoso.
- `Protocolli`: specifica il protocollo come `TCP`, `UDP`, `UDPLITE`, `ICMP`, `ESP`, `AH`, `SCTP`, `GRE`. È necessario specificare almeno un protocollo.
- `Porta sorgente`: la porta da cui ha origine la richiesta. Si noti che non tutti i protocolli richiedono una porta. Ad esempio, protocolli come `GRE` non utilizzano porte.
- `Indirizzo di destinazione`: specifica l'host interno verso cui il traffico deve essere reindirizzato. Questo può essere:
  - un indirizzo IP specifico

  - un oggetto firewall: un host definito da un insieme di host (eccetto insiemi di host che contengono intervalli IP o oggetti annidati), una prenotazione DHCP, un record DNS o un account OpenVPN con prenotazione IP
  - il firewall stesso

- `Porta di destinazione`: la porta a cui è diretto il traffico; questa può differire dalla porta di origine.

Per impostazione predefinita, tutti i port forwarding sono accessibili solo dagli host all'interno della WAN. Fare riferimento alla *Hairpin NAT* per le istruzioni su come modificare questo comportamento predefinito.

Per ogni inoltro di porta è inoltre possibile configurare i seguenti aspetti:

- **Associazione a un IP pubblico specifico**: gli inoltri di porta possono essere associati a un indirizzo IP pubblico specifico utilizzando il campo `IP WAN`. Questo significa che, se il router/firewall dispone di più indirizzi IP pubblici, è possibile assegnare un inoltro di porta a un determinato IP. Questa funzionalità è utile in presenza di configurazioni di rete complesse, garantendo che il traffico indirizzato a uno specifico IP pubblico venga inoltrato correttamente al server interno.
- **Restrizione di accesso**: Gli inoltri di porta possono essere limitati a sorgenti specifiche per aumentare la sicurezza. Questo può essere fatto utilizzando il campo `Limita accesso a`. Il campo accetta indirizzi IP, blocchi CIDR o un oggetto. Sono supportati tutti gli oggetti, tranne i set di host che contengono intervalli di IP o oggetti annidati.
- **Abilitazione del logging**: i port forward possono essere configurati per registrare il traffico in ingresso per ogni regola. Abilitando l'opzione `Log`, l'amministratore di rete può tenere traccia del traffico che passa attraverso il port forward, consentendo il monitoraggio e l'analisi. Per impostazione predefinita, la registrazione è limitata a 1 voce al secondo. Per modificare questo limite, consultare la sezione *Limiti di logging*.

26.1 Hairpin NAT

Hairpin NAT, noto anche come NAT loopback o NAT reflection, è una tecnica utilizzata nel networking in cui host interni accedono a un server situato all'interno della stessa rete locale utilizzando l'indirizzo IP esterno del router o del firewall. In altre parole, quando dispositivi interni tentano di connettersi a un server utilizzando l'indirizzo IP pubblico, hairpin NAT garantisce che il traffico venga instradato internamente senza uscire su internet e poi rientrare nella rete locale.

Per abilitare l'hairpin, attivare l'opzione `Hairpin NAT` e selezionare una o più zone in cui il NAT loopback deve essere abilitato.

26.1.1 Hairpin NAT per le zone VPN

Per utilizzare Hairpin NAT con zone VPN come `ipsec`, `openvpn` e `rwopenvpn`, è necessaria una configurazione aggiuntiva. È necessario dichiarare esplicitamente la subnet utilizzata dalla VPN; in caso contrario, Hairpin NAT non funzionerà per i client connessi tramite VPN.

Questa configurazione può essere eseguita tramite la riga di comando. Per prima cosa, identificare il riferimento interno per la zona, quindi aggiungere la rete desiderata, confermare le modifiche e riavviare il servizio.

Assicurarsi che le subnet siano assegnate alle zone corrette:

- `ipsec`: tunnel IPsec
- `openvpn`: tunnel OpenVPN
- `rwopenvpn`: OpenVPN Road Warrior

Se sono presenti più tunnel o reti, tutti devono essere inclusi nelle rispettive zone.

Come dichiarare una subnet per una zona VPN

Per dichiarare la rete OpenVPN Road Warrior, è possibile utilizzare la seguente sequenza di comandi di esempio:

1. Identificare il riferimento interno per la zona **rwopenvpn**:

   ```
   uci show firewall | grep ".name='rwopenvpn'"
   ```

   Esempio di output:

   ```
   firewall.ns_49d9f400.name='rwopenvpn'
   ```

2. Impostare la rete desiderata (in questo caso, **10.88.88.0/24**) per la zona **rwopenvpn**:

   ```
   uci add_list firewall.ns_49d9f400.subnet=10.88.88.0/24
   ```

3. Eseguire il commit delle modifiche e riavviare il servizio firewall:

   ```
   uci commit firewall
   /etc/init.d/firewall restart
   ```

Assicurarsi di sostituire la **subnet** di rete con quella corretta per la propria configurazione VPN specifica.

4. Verificare la rete aggiunta:

   ```
   uci show firewall | grep subnet
   ```

   Esempio di output:

   ```
   firewall.ns_49d9f400.subnet='10.88.88.0/24'
   ```

Aggiungere o rimuovere più subnet alla zona VPN

Se è già stata impostata una subnet per una zona VPN e si desidera **aggiungere** un'altra subnet (ad esempio 10.33.33.0/24), utilizzare il seguente comando (stesso riferimento interno dell'esempio precedente):

```
uci add_list firewall.ns_49d9f400.subnet=10.33.33.0/24
```

Se sono già state impostate più subnet per una zona VPN e si desidera **rimuovere** una subnet (ad esempio 10.33.33/24), utilizzare il seguente comando (stesso riferimento interno dell'esempio precedente):

```
uci del_list firewall.ns_49d9f400.subnet=10.33.33.0/24
```

Assicurarsi di eseguire il commit e riavviare il servizio firewall dopo le modifiche.

CAPITOLO 27

NAT

Il Network Address Translation (NAT) viene utilizzata per modificare le informazioni sugli indirizzi di rete negli header dei pacchetti durante il transito. Il NAT consente principalmente la traduzione degli indirizzi IP privati utilizzati all'interno di una rete locale in un indirizzo IP pubblico, permettendo a più dispositivi all'interno della rete locale di condividere un unico IP pubblico quando accedono a Internet. Per impostazione predefinita, tutti gli host all'interno della rete locale che accedono alla WAN tramite il firewall utilizzano il masquerade. Il masquerade è una forma di NAT che assegna automaticamente l'indirizzo IP di origine dei pacchetti in uscita all'indirizzo IP WAN del firewall. Questo garantisce che gli host interni che accedono a Internet appaiano ai server esterni come se provenissero dall'indirizzo IP pubblico del firewall.

Accedere alla pagina `NAT` nella sezione `Firewall`; questa pagina è organizzata in due schede: `Regole e NETMAP` e `NAT helper`.

La scheda `Regole e NETMAP` consente di configurare i seguenti tipi di regole NAT:

- *Source NAT*
- *Masquerade*
- *Accetta (disabilita NAT)*
- *Netmap*

Si noti che queste regole NAT vengono applicate a tutti i protocolli di rete.

È possibile configurare anche le regole di NAT di destinazione (DNAT), solitamente chiamate port forward o port redirects, dalla pagina *port forward*.

La scheda `NAT helper` consente di abilitare o disabilitare i NAT helper:

- *NAT helper*

27.1 SNAT

Il Source NAT, spesso indicato come SNAT, modifica l'indirizzo IP di origine dei pacchetti in uscita. Viene comunemente utilizzato nelle reti in cui gli indirizzi IP privati vengono tradotti in un singolo indirizzo IP pubblico durante la comunicazione con reti esterne. SNAT garantisce che le risposte dai server esterni vengano instradate correttamente al dispositivo interno appropriato modificando l'indirizzo IP di origine dei pacchetti in uscita con l'indirizzo IP pubblico. Questo consente a più dispositivi interni di accedere a Internet utilizzando un indirizzo IP pubblico condiviso, migliorando la sicurezza e la scalabilità.

Esempio Si dispone di una piccola azienda con due indirizzi IP pubblici forniti dal proprio provider di servizi Internet (ISP). Si desidera utilizzare uno di questi IP (1.2.3.4) specificamente per il server di posta interno (192.168.1.33) al fine di migliorarne la reputazione e l'autenticazione del mittente. L'altro indirizzo IP verrà utilizzato per l'accesso generale a Internet.

Problema Per impostazione predefinita, tutto il traffico in uscita dalla rete utilizza lo stesso IP WAN, incluso il mail server. Questo può influire negativamente sulla reputazione del mail server, poiché gli spammer spesso utilizzano IP condivisi. Inoltre, potrebbero essere necessarie configurazioni specifiche per il mail server diverse da quelle per il resto del traffico internet.

Soluzione Configurare l'IP alias (1.2.3.4) sull'interfaccia WAN, quindi creare una regola SNAT (Static Network Address Translation) nel firewall per indirizzare tutto il traffico in uscita dal mail server verso l'indirizzo IP pubblico dedicato. La regola deve contenere l'indirizzo IP interno del mail server (192.168.1.33) come sorgente e l'indirizzo IP pubblico dedicato (1.2.3.4) come indirizzo di traduzione; la zona di uscita deve essere impostata su WAN; selezionare SNAT come azione.

Risultato Tutto il traffico in uscita proveniente dal server di posta verrà ora tradotto sull'indirizzo IP pubblico dedicato. Questo migliora la reputazione del server di posta e consente configurazioni specifiche adattate alle sue esigenze. Il traffico internet generale continuerà a utilizzare l'altro indirizzo IP pubblico.

27.1.1 Source NAT in uno scenario MultiWAN

Se sono presenti più WAN e la regola SNAT riscrive su uno degli IP pubblici WAN, è necessario creare una regola MultiWAN oltre alla regola SNAT. Questa regola instraderà il traffico dall'indirizzo IP sorgente attraverso la WAN corretta con l'indirizzo IP pubblico.

Se non è stato ancora configurato, aggiungere una policy personalizzata che includa solo la WAN pertinente. Successivamente, creare una regola per applicare questa policy personalizzata al traffico proveniente dall'indirizzo IP interno (indirizzo sorgente) verso qualsiasi destinazione e protocollo.

27.2 MASQUERADE

La regola di masquerade maschera tutto il traffico in uscita con l'indirizzo IP dell'interfaccia di uscita del firewall. Il traffico proveniente dagli host interni verso Internet viene automaticamente mascherato dal firewall. Masquerade può anche essere utilizzato per mascherare il traffico proveniente da una rete remota (ad esempio, VPN) con l'IP del firewall per evitare eventuali problemi di routing.

Esempio È necessario raggiungere un host sulla rete locale (instradata) dalla rete VPN (ad es. 192.168.7.0/24), ma l'host non ha un gateway configurato oppure ha un gateway diverso dal firewall.

Problema L'host non può raggiungere il dispositivo locale a causa dell'assenza di un gateway.

Soluzione Creare una regola NAT con azione di mascheramento per il traffico proveniente dalla VPN Network. Questo maschera il traffico dalla VPN network (192.168.7.0/24) verso la rete locale utilizzando l'indirizzo IP del firewall

dell'interfaccia di destinazione. La regola deve contenere la VPN network (192.168.7.0/24) come sorgente e la rete interna degli host (192.168.1.0/24) come indirizzo di destinazione; la zona di uscita può essere lasciata vuota; selezionare MASQUERADE come azione.

Risultato L'host può raggiungere il dispositivo locale (ad esempio 192.168.1.78) come se la connessione provenisse dal firewall.

27.3 ACCEPT (disabilita NAT)

Una regola ACCEPT disabilita il NAT (no-NAT) e consente di bypassare il processo NAT per traffico specifico. Questo è particolarmente utile quando si desidera evitare il masquerading WAN per destinazioni specifiche.

Esempio Il firewall è collegato a un router che, oltre a consentire l'accesso a Internet, permette anche di raggiungere reti private tramite connessioni CDN o tunnel IPsec. Per poter raggiungere le reti private remote, il traffico proveniente dalla rete locale deve uscire con il proprio indirizzo IP originale (senza riscrittura tramite masquerade).

Problema Le policy dei tunnel del router consentono il traffico solo tra la rete locale di NethSecurity e le reti di destinazione, ma tutto il traffico esce dal firewall con l'IP mascherato (IP WAN di NethSecurity). A causa del masquerading, la comunicazione diretta tra la LAN di NethSecurity e la rete remota non è possibile.

Soluzione: Creare una regola NAT (Network Address Translation) con ACCEPT nel firewall. Questa regola evita il masquerading per tutto il traffico verso la rete CDN, mantenendo invariato l'indirizzo IP sorgente locale. La regola dovrebbe includere la rete interna (192.168.1.0/24) come sorgente e la rete CDN (192.168.50.0/24) come indirizzo di destinazione.

27.4 Netmap

Netmap è una tecnica NAT che offre una traduzione 1:1 a livello di rete senza modificare gli indirizzi dei singoli host. Questo significa che può mappare un'intera rete privata (ad esempio, 192.168.1.0/24) su un'altra rete (ad esempio, 10.5.6.0/24) in un'unica operazione, eliminando la necessità di configurare manualmente regole NAT individuali per ogni dispositivo.

Esempio 2 firewall, FW-A e FW-B, mantengono un tunnel VPN tra le reti A e B; le reti locali e remote si sovrappongono (192.168.1.0/24), il che rende impossibile instradare il traffico tra di esse. Tradurre le reti A e B su due reti alternative può risolvere il problema, evitando così la sovrapposizione delle reti.

Utilizziamo questo schema di traduzione.

- Rete A: 192.168.1.0/24 -> viene tradotta in -> Rete ALT_A: 10.1.1.0/24
- Rete B: 192.168.1.0/24 -> viene tradotta in -> Rete ALT_B: 10.2.2.0/24

Un host nella rete A che tenta di raggiungere un host nella rete B non deve contattare il vero IP, ma il suo indirizzo di rete tradotto (solo l'ultimo ottetto rimane invariato). Ad esempio, l'host 192.168.1.10 della rete A che vuole raggiungere 192.168.0.20 nella rete B deve invece contattare l'IP 10.2.2.20. Prima che la richiesta esca dal firewall FW-A, la sorgente del pacchetto verrà riscritta da FW-A come ALT_IP 10.1.1.10 per eliminare qualsiasi problema di routing nella rete B. Il processo inverso avverrà per i pacchetti di ritorno.

Soluzione Il problema può essere risolto utilizzando netmap per tradurre il traffico verso una rete privata diversa. Questo consente al traffico di essere instradato correttamente.

Come fare

Per consentire alla rete A di accedere a una risorsa nella rete B, sono necessarie due regole: una per il netmap di origine e una per il netmap di destinazione.

- La prima regola, che agisce come una source netmap, specifica che tutto il traffico diretto verso la rete 10.2.2.0/24 (rete di destinazione) e proveniente dalla rete 192.168.1.0/24 (rete sorgente) verrà mappato sulla rete 10.1.1.0/24 (rete sorgente mappata).
- La seconda regola funziona come una destination netmap, svolgendo un ruolo cruciale nel ricevere correttamente le risposte. È necessario che il traffico proveniente dalla rete 10.2.2.0/24 (rete sorgente) e destinato alla rete 10.1.1.0/24 (rete di destinazione) venga mappato sulla rete 192.168.1.0/24 (rete di destinazione mappata).

Risultato Tutte le richieste di traffico (e le relative risposte) dalla rete A alla rete B verranno instradate correttamente.

Nota: Se è necessario consentire le richieste dalla rete B verso la rete A, è necessario fare lo stesso nel firewall B.

27.4.1 Netmap sorgente

La «source netmap» consente di determinare come deve cambiare la sorgente quando il traffico è diretto verso una destinazione specifica. Ad esempio, rete di destinazione 10.2.2.0/24, rete sorgente: 192.168.0.0/24, rete sorgente nattata: 10.1.1.0/24.

È possibile creare una regola di source netmap dall'interfaccia web all'interno della pagina `NAT`. Nella parte inferiore della pagina, fare clic sul pulsante *Aggiungi NETMAP sorgente* per creare una nuova regola. All'interno del drawer, compilare i campi come segue:

- **Nome**: un nome per la regola
- **Rete di destinazione**: la rete di destinazione in notazione CIDR, ad esempio 10.2.2.0/24 per l'esempio sopra
- **Rete di origine**: la rete di origine, ad esempio 192.168.1.0/24
- **Rete mappata**: la rete di origine tradotta, ad esempio 10.1.1.0/24

Nella sezione `Impostazioni avanzate`, è possibile specificare i dispositivi di input e output per la regola. Se il dispositivo non viene specificato, la regola verrà applicata a tutti i dispositivi.

27.4.2 Netmap destinazione

La «destination netmap» consente di determinare come deve cambiare l'IP di destinazione quando il traffico proviene da una rete specifica. Ad esempio, rete sorgente 10.2.2.0/24, rete di destinazione: 10.1.1.0/24, rete di destinazione natted: 192.168.0.0/24.

È possibile creare una regola di destination netmap dall'interfaccia web all'interno della pagina `NAT`. Nella parte inferiore della pagina, fare clic sul pulsante *Aggiungi NETMAP destinazione* per creare una nuova regola. All'interno del drawer, compilare i campi come segue:

- **Nome**: un nome per la regola
- **Rete di origine**: la rete di origine in notazione CIDR, ad esempio 10.2.2.0/24
- **Rete di destinazione**: la rete di destinazione, ad esempio 10.1.1.0/24
- **Rete mappata**: la rete di destinazione tradotta, ad esempio 192.168.1.0/24

Nella sezione `Impostazioni avanzate`, è possibile specificare i dispositivi di input e output per la regola. Se il dispositivo non viene specificato, la regola verrà applicata a tutti i dispositivi.

27.4.3 Comandi CLI

Per creare una regola netmap SOURCE dalla CLI

```
uci set netmap.r1=rule
uci set netmap.r1.name=source_nat
uci set netmap.r1.dest=10.2.2.0/24
uci set netmap.r1.map_from=192.168.1.0/24
uci set netmap.r1.map_to=10.1.1.0/24
```

è anche possibile specificare dispositivi di input/output opzionali in questo modo:

```
uci  add_list netmap.r1.device_in='eth0'
uci  add_list netmap.r1.device_out='tunrw1'
```

Quindi eseguire il commit e applicare:

```
uci commit netmap
ns-netmap
```

Per creare una regola netmap DESTINATION dalla CLI

```
uci set netmap.r2=rule
uci set netmap.r2.name=dest_nat
uci set netmap.r2.src=10.2.2.0/24
uci set netmap.r2.map_from=10.1.1.0/24
uci set netmap.r2.map_to=192.168.1.0/24
```

è anche possibile specificare dispositivi di input/output opzionali in questo modo:

```
uci  add_list netmap.r2.device_in='tunrw1'
uci  add_list netmap.r2.device_out='eth01'
```

Quindi eseguire il commit e applicare:

```
uci commit netmap
ns-netmap
/etc/init.d/firewall reload
```

27.5 Helper NAT

I NAT helper sono meccanismi progettati per facilitare la comunicazione di alcuni protocolli che possono incontrare problemi quando utilizzati con il NAT di base. Alcuni protocolli comuni, come FTP, SIP o H.323, inseriscono indirizzi IP o numeri di porta all'interno del payload dei dati, il che può creare problemi con il NAT standard.

I NAT helper, noti anche come Application Layer Gateway (ALG), operano a livello applicativo. Il loro ruolo principale è modificare i dati specifici del protocollo, come indirizzi IP o porte incorporati nei pacchetti, garantendo che questi protocolli funzionino correttamente durante il transito attraverso il NAT.

Ad esempio, in FTP, i NAT helper modificano gli indirizzi IP e le porte all'interno dei pacchetti di controllo e dati FTP, consentendo una corretta attraversamento NAT per le connessioni FTP. Allo stesso modo, i NAT helper per SIP e altri protocolli garantiscono che i dispositivi che utilizzano questi protocolli possano stabilire connessioni attraverso i confini NAT senza problemi.

NethSecurity fornisce diversi tipi di NAT helper, tutti disabilitati per impostazione predefinita. Se necessario, è possibile abilitare specifici helper tramite l'interfaccia web.

Durante la configurazione dell'helper, l'interfaccia può mostrare alcuni parametri tipici del protocollo coinvolto. Questi parametri sono precompilati con i valori predefiniti più comunemente utilizzati. Poiché i parametri dipendono dal tipo di protocollo, variano sia per numero che per tipologia a seconda dell'helper (alcuni helper non mostrano alcun parametro).

Dopo qualsiasi modifica, il firewall notificherà se è necessario un riavvio. Questo avviene tipicamente quando un helper viene disabilitato o modificato (se è già attivo).

Quando alcuni helper sono abilitati, gli helper correlati vengono caricati automaticamente nel kernel come dipendenze. Ad esempio, se `nf_nat_ftp` è abilitato, l'helper correlato `nf_conntrack_ftp` verrà caricato automaticamente nel kernel. Per quell'helper, l'interfaccia web mostrerà `Caricato` con un'icona informativa per notificare l'utente.

CAPITOLO 28

Regole

Le regole del firewall definiscono come il traffico di rete viene segmentato e controllato tra le diverse zone. I firewall agiscono come barriere tra reti interne affidabili e reti esterne non affidabili, come Internet. Queste regole specificano quale traffico è consentito, negato o monitorato in base a politiche di sicurezza predefinite.

L'ordine delle regole è importante; viene applicata la prima regola corrispondente, determinando il destino del pacchetto di rete.

La pagina è organizzata in tre schede, ciascuna con una funzione specifica:

- Scheda `Regole di forward`: questa scheda è dedicata alla configurazione delle regole per i pacchetti di dati che si spostano tra diverse zone nella rete.
- Scheda `Regole di input`: questa scheda è dedicata alla configurazione delle regole per i pacchetti in ingresso destinati al firewall stesso.
- Scheda `Regole di output`: questa scheda è dedicata alla configurazione delle regole per i pacchetti emessi dal firewall.

Individuare il pulsante per aggiungere una nuova regola e fare clic su di esso per avviare il processo di creazione della regola. Compilare i seguenti campi per la nuova regola:

- `Stato`: abilitare o disabilitare la regola in base alle proprie esigenze. Per impostazione predefinita, la regola è abilitata durante la creazione.
- `Nome regola`: assegnare un nome descrittivo per identificare la regola.
- `Indirizzo sorgente`: selezionare l'indirizzo sorgente tra tre diverse opzioni:
  - inserire uno o più indirizzi/reti IPv4/IPv6 o intervalli di IP
  - selezionare un oggetto firewall tra quelli disponibili
  - qualsiasi indirizzo sorgente

  Questo campo non è presente per `Regole di output`, poiché l'indirizzo sorgente è sempre il firewall stesso.
- `Zona sorgente`: specificare la zona di origine del traffico. Scegliere una zona specifica oppure selezionare `Qualsiasi` per includere il traffico proveniente da qualsiasi zona.
- `Indirizzo di destinazione`: selezionare l'indirizzo di destinazione tra tre diverse opzioni:

  - inserire uno o più indirizzi/reti IPv4/IPv6 o intervalli di IP
  - selezionare un oggetto firewall tra quelli disponibili
  - qualsiasi indirizzo di destinazione

  Questo campo non è presente per `Regole di input`, poiché l'indirizzo di destinazione è sempre il firewall stesso.

- `Zona di destinazione`: specificare la zona di destinazione del traffico. Scegliere una zona specifica. Tenere presente che le zone di origine e di destinazione non possono essere uguali.
- `Servizio di destinazione`: selezionare dall'elenco oppure scegliere `Personalizzato` per inserire porte specifiche e selezionare i protocolli.
- `Azione`: definire l'azione quando le condizioni della regola sono soddisfatte:
  - `Accept`: accetta il traffico di rete.
  - `Rifiuta`: blocca il traffico e notifica l'host mittente.
  - `Drop`: blocca il traffico, i pacchetti vengono scartati e nessuna notifica viene inviata all'host mittente.
- `Posizione della regola`: consente di decidere se aggiungere la regola in fondo o all'inizio dell'elenco delle regole.
- `Log`: indica se il traffico che corrisponde a questa regola deve essere registrato nei log. La voce di log includerà il nome della regola come prefisso. Per impostazione predefinita, la registrazione nei log è limitata a 1 voce al secondo. Consultare la sezione *Limiti di logging* per le istruzioni su come modificare questo limite.
- `Tag`: facoltativamente, aggiungere tag per scopi organizzativi. Si noti che il tag "automated" è riservato all'uso di sistema.

28.1 Limiti di logging

La registrazione può essere abilitata sui seguenti oggetti:

- zone
- regole del firewall
- regole di reindirizzamento (port-forwarding)

Quando la registrazione è abilitata, il firewall aggiungerà dei limiti di registrazione a varie regole. Questo garantisce che la registrazione non sovraccarichi il sistema impostando un limite al tasso di registrazione.

Per impostazione predefinita, vengono applicati i seguenti limiti di registrazione:

- 1 voce di log al secondo per le regole del firewall
- 5 voci di log al secondo per zone
- 1 voce di log al secondo per le regole di reindirizzamento

28.1.1 Modifica dei limiti predefiniti di logging

Avvertimento: La modifica dei limiti predefiniti di logging può influire sulle prestazioni del sistema. Prestare attenzione quando si modificano questi limiti.

I limiti predefiniti sono salvati nella sezione *ns_defaults* della configurazione del firewall:

- `zone_log_limit`: il limite predefinito per le zone
- `rule_log_limit`: il limite predefinito per le regole del firewall
- `redirect_log_limit`: il limite predefinito per le regole di reindirizzamento

1. Impostare il limite di log desiderato per le regole del firewall utilizzando il comando *uci*:

```
uci set firewall.ns_defaults.zone_log_limit="10/s"
uci commit firewall
```

2. Eseguire lo script *firewall-apply-default-logging* per applicare il nuovo limite di log:

```
firewall-apply-default-logging
```

CAPITOLO 29

Connessioni

Il connection tracking (Conntrack) è una funzionalità di rete utilizzata in firewall e router per monitorare e gestire lo stato delle connessioni di rete attive. Tiene traccia dello stato di ciascuna connessione, come nuova, stabilita, correlata o scaduta, e mantiene queste informazioni in una tabella di connection tracking. Questo consente un'ispezione stateful dei pacchetti, in cui i pacchetti vengono analizzati in base al contesto della connessione, permettendo regole di filtraggio più precise e sicure. Conntrack supporta inoltre la Network Address Translation (NAT) tracciando le associazioni tra indirizzi IP interni ed esterni e ottimizza le prestazioni scartando rapidamente i pacchetti provenienti da connessioni non valide o scadute.

Le connessioni possono essere filtrate tramite:

- `Protocollo`
- `Stato`
- `IP`
- `Porta`

L'elenco delle connessioni non viene aggiornato in tempo reale. Per elencare le nuove connessioni, fare clic sul pulsante *Aggiorna pagina*.

L'amministratore può eliminare una singola connessione o svuotare l'intera tabella di tracciamento delle connessioni utilizzando il pulsante *Elimina tutte le connessioni*.

29.1 Buone pratiche per la terminazione delle sessioni

Quando terminare una connessione:

- la connessione è scaduta o è rimasta inattiva per un periodo prolungato
- ci sono prove di attività dannosa associate alla sessione
- la connessione sembra essere inattiva o bloccata, impedendo nuove connessioni
- la terminazione è necessaria per la risoluzione dei problemi di rete o per la diagnostica

Quando evitare di terminare una sessione:

- la connessione è attiva e sembra funzionare normalmente
- la connessione è fondamentale per il funzionamento continuo dell'applicazione
- eventuali problemi con la connessione sembrano essere temporanei e potrebbero risolversi da soli

In una configurazione MultiWAN, il traffico specifico come i trunk VoIP viene instradato e NATtato attraverso interfacce designate verso provider distinti. Quando un'interfaccia o una rotta diventa non disponibile, è essenziale interrompere tutte le connessioni che utilizzano tale interfaccia e instradare il traffico successivo attraverso la connessione funzionante, altrimenti il trunk non sarà in grado di registrarsi presso il provider.

Per risolvere questo problema, è possibile rimuovere le voci conntrack specifiche associate al vecchio indirizzo esterno tramite l'interfaccia utente.

CAPITOLO 30

Zone e policy

Le zone del firewall categorizzano le interfacce di rete, definendo i confini sicuri, mentre le regole del firewall determinano la gestione del traffico tra le zone. Le zone organizzano i segmenti di rete e le regole applicano le politiche di sicurezza specificando le condizioni per le azioni consentite o negate. Insieme, consentono di definire e applicare regole per il traffico di rete all'interno del firewall.

In un sistema firewall, le zone e le policy sono concetti fondamentali che aiutano a gestire la sicurezza della rete controllando il flusso del traffico tra diversi segmenti della rete. Una zona in un firewall rappresenta uno specifico segmento di rete con il proprio livello di affidabilità. Ad esempio, una configurazione comune può includere zone come WAN (Wide Area Network), che rappresenta la rete esterna e non affidabile (di solito Internet), e LAN (Local Area Network), che rappresenta la rete interna e affidabile (i dispositivi all'interno di una rete privata domestica o aziendale). Ogni zona ha il proprio insieme di regole di sicurezza e policy che determinano come il traffico può fluire da e verso quella zona.

Le policy in un firewall definiscono le regole e le azioni che determinano come il traffico viene gestito tra le diverse zone. Queste regole specificano quale tipo di traffico è consentito, negato o monitorato in base a criteri di sicurezza predefiniti.

Zone predefinite:

- **WAN (Wide Area Network):** rappresenta la rete esterna e non affidabile (ad esempio, Internet).
- **LAN (Local Area Network):** rappresenta la rete interna e affidabile (ad esempio, dispositivi all'interno di una casa privata o di un'organizzazione).

Traffico accettato:

- **da LAN a WAN:** il traffico dai dispositivi all'interno della zona LAN verso la zona WAN è consentito, permettendo ai dispositivi interni di accedere a Internet.
- **da LAN al firewall stesso:** il traffico dai dispositivi LAN verso il firewall stesso è consentito, facilitando la comunicazione per vari scopi.
- **Da LAN a LAN stessa:** il traffico tra dispositivi all'interno della zona LAN è consentito, permettendo ai dispositivi interni di comunicare tra loro.

Traffico negato:

- **Dal WAN al firewall stesso:** il traffico dalla zona WAN verso il firewall stesso è negato, impedendo tentativi di accesso esterni non autorizzati.
- **Da WAN a WAN stessa:** la comunicazione diretta tra reti esterne (da WAN a WAN) è negata, isolando le diverse entità esterne per una maggiore sicurezza.

In questa configurazione, il firewall regola il traffico tra le zone WAN e LAN, consentendo ai dispositivi interni di accedere a Internet e di comunicare internamente, mantenendo la sicurezza tramite il blocco dell'accesso diretto esterno al firewall e impedendo la comunicazione tra reti esterne.

Le zone predefinite non possono essere eliminate, ma l'amministratore di rete può modificare le policy esistenti o creare nuove zone.

Il logging può essere abilitata per le zone utilizzando l'opzione *Log* all'interno della pagina `Zone e policy`. Abilitando il logging, l'amministratore di rete può monitorare l'attività di rete, identificare potenziali minacce e analizzare i modelli di traffico. Il logging è limitata a 5 voci al secondo per impostazione predefinita. Per modificare questo limite, consultare la sezione *Limiti di logging*.

30.1 Zone guest e DMZ

Oltre alle zone predefinite, il firewall può essere configurato con zone aggiuntive per soddisfare requisiti di rete specifici. Due esempi comuni sono le zone Guest e DMZ (Demilitarized Zone). Talvolta la zona Guest è anche conosciuta come zona blu, mentre la DMZ è anche chiamata arancione.

30.1.1 Zona guest (blu)

La zona Guest rappresenta un segmento di rete per dispositivi degli ospiti, come visitatori o utenti temporanei. Questa zona è tipicamente isolata dalla zona LAN per prevenire accessi non autorizzati alle risorse interne. Tuttavia, è consentito l'accesso alla zona WAN.

Per creare una zona Guest, seguire questi passaggi:

- accedere alla sezione `Zones & policies`
- fare clic sul pulsante `Aggiungi zona`
- inserire **guest** nel campo `Nome`, in questo caso la zona verrà evidenziata in blu
- lascia vuoto il campo `Consenti traffico verso`
- selezionare `LAN` all'interno del campo `Consenti traffico da`
- abilitare l'opzione `Traffico verso WAN`
- selezionare `Drop` sia per i campi `Traffico verso firewall` che `Traffico verso la stessa zona`
- fare clic sul pulsante `Salva` e applicare le modifiche

Nota: Se il firewall è destinato a fornire i servizi `DHCP` e `DNS`, creare una `regola di input` del firewall che consenta il traffico sulle porte `53 TCP/UDP (DNS)` e `67 UDP (DHCP)` per la zona `Guest`. Se questi servizi non sono necessari o sono forniti da un altro dispositivo in questa rete, le porte corrispondenti possono rimanere bloccate.

30.1.2 Zona DMZ (arancione)

La DMZ rappresenta un segmento di rete per server e servizi che devono essere accessibili da internet ma isolati dalla rete interna.

Per creare una DMZ, seguire questi passaggi:

- accedere alla sezione `Zones & policies`
- fare clic sul pulsante `Aggiungi zona`
- inserire **dmz** nel campo `Nome`, in questo caso la zona verrà evidenziata in arancione
- lasciare vuoti sia i campi `Consenti traffico verso` che `Consenti traffico da`
- abilitare l'opzione `Traffico verso WAN`
- selezionare `Drop` sia per i campi `Traffico verso firewall` che `Traffico verso la stessa zona`
- fare clic sul pulsante `Salva` e applicare le modifiche

CAPITOLO 31

Filtro contenuti

Il filtraggio dei contenuti è un aspetto cruciale della sicurezza di rete e svolge due scopi principali:

1. Blocco di malware e prevenzione di attacchi dannosi
2. Filtraggio di siti indesiderati, come quelli che contengono contenuti per adulti

NethSecurity offre quattro distinti meccanismi di filtraggio per soddisfare queste esigenze:

- **Threat Shield IP**: sistema di blocco basato su IP che prende di mira le minacce malware
- **Threat Shield DNS**: sistema di blocco basato su DNS per malware e filtraggio di contenuti di base
- **Filtro Deep Packet Inspection (DPI)**: Filtraggio specifico per applicazione e protocollo utilizzando netifyd
- **FlashStart DNS filter**: Soluzione commerciale di filtraggio DNS con funzionalità complete di controllo dei contenuti

31.1 Threat Shield IP

Threat Shield IP è un sistema di blocco basato su IP progettato specificamente per contrastare le minacce malware. Funziona bloccando le connessioni verso o da indirizzi IP noti come dannosi.

Ambito: Prende di mira il malware e offre funzionalità limitate di rimozione della privacy e della pubblicità (ads)

Elenchi:

- Liste della community, gratuite, che mirano a malware generico, pubblicità e tracker
- Liste Enterprise, a pagamento, focalizzate sulla protezione da malware di alto valore

Vantaggi:

- Elaborazione veloce in quanto funziona a livello IP
- Efficace contro intere reti dannose

Limitazioni:

- Impossibile filtrare in base al tipo di contenuto
- Può occasionalmente bloccare servizi legittimi che condividono un IP con quelli dannosi

Per configurare Threat Shield IP, consultare la sezione *Threat shield IP*.

31.2 Threat Shield DNS

Threat Shield DNS fornisce il blocco basato su DNS, offrendo protezione contro malware e funzionalità di filtraggio dei contenuti di base.

Ambito: Copre malware e categorie di contenuti limitate (ad esempio, contenuti per adulti, gioco d'azzardo)

Elenchi:

- Liste della community, gratuite, focalizzate su malware generico e filtraggio semplice dei contenuti
- Liste Enterprise, a pagamento, focalizzate sulla protezione da malware di alto valore

Vantaggi:

- Può bloccare domini specifici indipendentemente dall'indirizzo IP
- Offre una categorizzazione di base dei contenuti (ad esempio, contenuti per adulti, gioco d'azzardo)

Limitazioni:

- Potrebbe essere aggirato utilizzando server DNS alternativi, ma può essere mitigato con il filtraggio DPI e abilitando categorie di blocco speciali.
- Meno granulare rispetto al filtraggio completo degli URL

Per configurare Threat Shield DNS, consultare la sezione *Threat shield DNS*.

31.3 Filtro DNS FlashStart

FlashStart è una soluzione commerciale di filtraggio basata su DNS che offre funzionalità complete di controllo dei contenuti e di reportistica.

Ambito: contenuti completo che va oltre il solo malware e i contenuti per adulti

Liste: Liste commerciali gestite da FlashStart

Vantaggi:

- Liste di blocco di alta qualità
- Report personalizzabili
- Configurazione basata su cloud, non è necessario l'accesso diretto al firewall
- Categorie di contenuti estese
- Facile da gestire
- Scalabile per organizzazioni di diverse dimensioni

Per configurare il filtro DNS di FlashStart, consultare la sezione *Filtro DNS FlashStart*.

31.4 Filtro Deep Packet Inspection (DPI)

NethSecurity utilizza tecniche di Deep Packet Inspection (DPI) per filtrare il traffico di rete tramite Netify Agent.

Ambito: Filtro specifico per applicazione e protocollo

Elenchi:

- Firme della community, gratuite ma limitate nel numero e nella frequenza di aggiornamento
- Firme Enterprise, incluse in qualsiasi abbonamento, offrono una copertura più completa

Vantaggi:

- Fornisce un controllo granulare sul traffico di rete
- Può identificare e filtrare in base ad applicazioni o protocolli specifici
- Consente la gestione dinamica del traffico basata sull'analisi in tempo reale

Considerazioni:

- Potrebbe richiedere una maggiore potenza di elaborazione rispetto al filtraggio basato su IP o DNS
- Richiede una configurazione accurata per bilanciare sicurezza e prestazioni
- L'amministratore deve creare regole DPI per ciascuna interfaccia

Per configurare il filtraggio DPI, consultare la sezione *Filtro Deep Packet Inspection (DPI)*.

31.5 Confronto delle opzioni di filtraggio

Funzionalità	Threat Shield IP	Threat Shield DNS	Filtro DNS Flashstart	Filtro DPI
Metodo di blocco	Basato su IP	Basato su DNS	Basato su DNS	Ispezione dei pacchetti
Focus principale	Malware	Malware + contenuto di base	Contenuto completo	Specifico per applicazione/protocollo
Tipi di elenco	Community, Enterprise	Community, Enterprise	Commerciale	N/D (analisi in tempo reale)
Configurazione	Firewall	Firewall	Cloud	Firewall (per interfaccia)
Reportistica	Nessuno	Nessuno	Avanzato, personalizzabile	Limitato

Strategie di implementazione

Per una sicurezza ottimale, si consiglia di adottare un approccio a più livelli:

1. Utilizzare Threat Shield IP come prima linea di difesa contro le reti dannose conosciute.
2. Implementare un filtro DNS, utilizzare una delle seguenti opzioni:
   - Threat Shield DNS per rilevare minacce basate su dominio e fornire un filtro dei contenuti di base
   - Flashstart DNS Filtering per un controllo completo dei contenuti, particolarmente indicato in ambienti che richiedono una gestione dettagliata delle policy e reportistica avanzata.

3. Utilizzare il filtraggio DPI per un controllo granulare su applicazioni e protocolli specifici, e per gestire il traffico in base all'analisi in tempo reale.

Questa combinazione offre una difesa stratificata, affrontando diversi vettori di minaccia ed esigenze di filtraggio dei contenuti.

CAPITOLO 32

Threat shield IP

NethSecurity è dotato di diversi strumenti e integrazioni utili per contrastare le minacce provenienti da Internet. Uno di questi strumenti è Threat Shield IP, che blocca qualsiasi traffico proveniente da indirizzi IP compromessi o a essi destinato, così come qualsiasi richiesta indirizzata a nomi host che potrebbero essere dannosi.

Il servizio può caricare blocklist mantenute dalla comunità oppure può fare affidamento su blocklist di alta qualità, aggiornate e mantenute molto frequentemente da Nethesis e Yoroi, un'azienda leader nel settore della CyberSecurity e membro della Cyber Threat Alliance. Le blacklist di Yoroi garantiscono grande efficacia e un elevato livello di affidabilità, riducendo al minimo la possibilità di falsi positivi.

Si noti che, per accedere alle blocklist di Nethesis e Yoroi, la macchina deve disporre di un abbonamento addizionale valido per questo servizio.

32.1 Configurazione

Il servizio è disabilitato per impostazione predefinita; per abilitarlo, navigare alla pagina `Threat shield IP` nella sezione `Sicurezza`. Accedere alla scheda `Impostazioni` e attivare l'interruttore `Stato`.

Quando il servizio è abilitato, la scheda `Blocklist feed` mostrerà tutte le blocklist disponibili. È possibile abilitare o disabilitare ciascuna blocklist utilizzando l'interruttore sul lato destro dell'elenco. Le blocklist abilitate verranno aggiornate automaticamente a intervalli regolari. NethSecurity 8 consente l'utilizzo di blocklist Community ed Enterprise.

32.1.1 Blocklist della community

Le blocklist della community sono fornite da contributori della community e coprono diverse aree: blocco delle pubblicità, blocco di malware, blocco dello spam, blocco dei tracker e così via. NethSecurity le rende disponibili così come sono.

Le liste della community non forniscono un parametro standardizzato di «Confidence», pertanto l'interfaccia utente mostra la loro affidabilità come «Sconosciuta». Come euristica pratica, quando il nome della lista contiene un indicatore di severità o affidabilità (ad esempio, «lvl 1», «level 1»), generalmente indica il tasso più basso di falsi positivi e la massima affidabilità; al contrario, livelli più alti indicati (ad esempio, «lvl 2», «lvl 3», «lvl 4») tipicamente implicano una minore affidabilità e un rischio maggiore di inserimenti aggressivi o errati. Tuttavia, le convenzioni di denominazione variano e non tutti i provider della community includono tali indicatori, quindi è sempre consigliabile esaminare il contenuto e lo scopo di una lista della community prima di abilitarla in produzione. Il tipo di licenza d'uso può variare a seconda del provider, quindi se l'utilizzo non è personale, potrebbe essere necessario contattare il provider.

Manutenzione delle liste della community

Ogni blocklist è gestita dal relativo provider specifico. NethSecurity include già gli URL per il download dei feed, validi al momento del rilascio. Tuttavia, poiché questi URL sono integrati nel software, se il provider li modifica, alcune blocklist potrebbero non essere più scaricabili.

32.1.2 Blocklist Enterprise

Abbonamento richiesto

Questa funzionalità è disponibile solo se il firewall dispone di un abbonamento *Community o Enterprise* valido.

Le blocklist Enterprise sono specificamente orientate alla sicurezza e offrono diversi vantaggi rispetto alle blocklist mantenute dalla comunità:

1. **Qualità e accuratezza**: Le blocklist Enterprise, come quelle fornite da Nethesis e Yoroi, sono curate e mantenute da aziende di cybersecurity affidabili. Queste aziende dispongono di team dedicati che monitorano e aggiornano continuamente le blocklist per garantire che siano accurate ed efficaci nel bloccare il traffico dannoso. Questo si traduce in un livello superiore di qualità e accuratezza rispetto alle blocklist mantenute dalla comunità, che potrebbero non ricevere la stessa attenzione e frequenza di aggiornamenti.
2. **Tempestività**: Le blocklist Enterprise vengono aggiornate frequentemente per includere le minacce più recenti e gli indirizzi IP dannosi. Aziende di cybersecurity come Nethesis e Yoroi monitorano attivamente le minacce emergenti e le aggiungono tempestivamente alle loro blocklist. Questo garantisce che il sistema sia protetto contro le minacce più recenti e in evoluzione.
3. **Riduzione dei falsi positivi**: I falsi positivi si verificano quando il traffico legittimo viene bloccato per errore. Le blocklist Enterprise sono progettate per ridurre al minimo i falsi positivi attraverso una selezione e una verifica accurata degli indirizzi IP e dei nomi host elencati. Le aziende che gestiscono le blocklist Enterprise adottano processi rigorosi per garantire che solo entità malevole vengano incluse nelle blocklist. Questo riduce la probabilità che il traffico legittimo venga bloccato, minimizzando le interruzioni alla rete o ai servizi.
4. **Supporto Enterprise**: Le blocklist Enterprise spesso includono supporto aggiuntivo e servizi specifici per ambienti aziendali. Questo comprende l'accesso al supporto tecnico, alla documentazione e all'assistenza per l'integrazione. In caso di problemi o domande durante l'utilizzo delle blocklist Enterprise, è possibile fare affidamento sul supporto fornito dalle aziende di cybersecurity per affrontarli in modo efficace.

32.1.3 Affidabilità

Le blocklist Enterprise includono un punteggio di «Confidence» che viene mostrato nell'interfaccia utente. Il punteggio è espresso come un valore da 1 a 10 e rappresenta la valutazione del provider sulla qualità della lista: valori più alti indicano una maggiore affidabilità e una minore probabilità di falsi positivi. Questa metrica di «Confidence» è disponibile solo per le liste Enterprise; le liste Community vengono presentate «così come sono» e mostrano «Unknown» per la confidence.

Le blocklist Yoroi e Nethesis sono blocklist Enterprise. Queste liste saranno visualizzate solo se la macchina dispone di un *abbonamento Enterprise o Community valido* e di un abbonamento valido per il servizio Threat Shield IP.

32.1.4 Log

La funzionalità Threat Shield IP include capacità avanzate di registrazione per monitorare e tracciare potenziali minacce. La sezione di registrazione consente di configurare quali tipi di pacchetti bloccati vengono registrati:

1. Log dei pacchetti bloccati nella chain di pre-routing: quando abilitata, questa opzione registra i pacchetti che vengono bloccati nella catena di pre-routing, che elabora i pacchetti prima che entrino nella tabella di routing.
2. Log dei pacchetti bloccati nella chain di input: questa opzione, quando attivata, registra i pacchetti bloccati nella catena di input, che gestisce i pacchetti destinati direttamente al firewall stesso. Si noti che questa opzione può generare un numero elevato di log se il firewall è sottoposto a traffico intenso.
3. Log dei pacchetti bloccati nella chain di forward: Abilitando questa opzione vengono registrati i pacchetti bloccati nella catena di forward, che elabora i pacchetti instradati attraverso il firewall.
4. Log dei pacchetti bloccati inoltrati dalla LAN: Questa opzione registra i pacchetti che vengono bloccati quando vengono inoltrati dalla rete locale (LAN).

Queste opzioni di logging offrono un controllo granulare su quali pacchetti bloccati vengono registrati, permettendo di esporre metriche all'interno delle sezioni *monitoraggio in tempo reale* e *monitoraggio storico*.

32.1.5 Allowlist locale

A volte può essere necessario consentire l'accesso a determinati indirizzi IP; per farlo è possibile utilizzare la scheda `Allowlist locale`. Utilizzare il pulsante *Aggiungi indirizzo* per aggiungere un nuovo indirizzo all'elenco. L'indirizzo può essere un indirizzo IPv4/IPv6 valido con notazione CIDR opzionale, un indirizzo MAC oppure un hostname completo di dominio (FQDN).

Ad esempio, l'indirizzo può essere:

- Indirizzo IPv4: 192.168.0.1
- Indirizzo IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Indirizzo IPv4 con notazione CIDR: 192.168.0.0/24
- Indirizzo MAC: 00:0a:95:9d:68:16
- FQDN: example.com

È possibile associare un commento a ciascun indirizzo per facilitarne la gestione.

È possibile aggiungere un commento per fornire informazioni aggiuntive sull'indirizzo, come ad esempio il suo scopo o il proprietario. Questo può aiutare a organizzare e gestire la allowlist in modo efficace.

32.1.6 Blocklist locale

Threat Shield IP include una funzionalità di blocklist locale, che consente di specificare manualmente gli indirizzi che devono essere sempre bloccati. Questo offre un ulteriore livello di personalizzazione alla configurazione della sicurezza.

Per accedere e personalizzare la blocklist, navigare nella scheda `Blocklist locale` nell'interfaccia Threat Shield IP. Utilizzare il pulsante *Aggiungi indirizzo* per includere nuove voci. Ogni voce è composta da un indirizzo e una descrizione. La sintassi valida per l'indirizzo è la stessa utilizzata per la *Allowlist locale*.

Quando si aggiungono indirizzi alla blocklist locale, assicurarsi di inserirli correttamente per evitare di bloccare accidentalmente traffico legittimo. È inoltre buona pratica includere un commento descrittivo per ogni voce, in modo da facilitare la gestione e la verifica futura della propria blocklist.

32.2 Bloccare gli attacchi brute force

Quando Threat Shield IP è abilitato, il sistema avvia automaticamente il controllo dei tentativi di attacco brute force sui servizi del firewall. Per impostazione predefinita, i servizi monitorati includono l'accesso SSH e il login all'interfaccia utente di NethSecurity. Il sistema rileva i tentativi di accesso e blocca automaticamente gli IP che non sono riusciti a inserire le credenziali corrette.

Per abilitare o disabilitare la protezione contro gli attacchi brute force, accedere alla sezione `Blocca attacchi brute force` nell'interfaccia Threat Shield IP, sotto la scheda `Impostazioni` e utilizzare l'interruttore per attivare o disattivare la funzionalità.

La funzionalità può essere personalizzata modificando le seguenti impostazioni:

- `Ban dopo N accessi falliti`: questa impostazione determina il numero di tentativi di accesso falliti consentiti prima che un indirizzo IP venga bannato. Il valore predefinito è solitamente 3, ma può essere modificato secondo necessità. Un valore più basso aumenta la sicurezza ma può anche aumentare il rischio di falsi positivi, ad esempio bloccando utenti legittimi che inseriscono erroneamente le proprie credenziali.
- `Pattern per rilevare gli attacchi`: questo campo consente di specificare i pattern che il sistema utilizza per identificare potenziali attacchi di forza bruta. I pattern comuni includono:
  - *Exit before auth from*: rileva tentativi di autenticazione non riusciti al servizio SSH
  - *authentication failed for user*: identifica i tentativi di autenticazione non riusciti all'interfaccia web di NethSecurity
  - *TLS Auth Error*, *TLS handshake failed*, *AUTH_FAILED*: rileva tentativi di autenticazione non riusciti al servizio OpenVPN

  È possibile aggiungere ulteriori pattern utilizzando il pulsante *Aggiungi pattern* per personalizzare il meccanismo di rilevamento. Ogni pattern può essere una valida espressione regolare *grep*.
- `Tempo di ban`: questa impostazione determina la durata per cui un indirizzo IP rimane bannato dopo aver superato il numero consentito di tentativi falliti. Il valore predefinito è spesso impostato a 30 minuti, ma può essere modificato in base alle proprie esigenze di sicurezza.

È possibile eseguire ulteriori azioni utilizzando la riga di comando; questi sono i comandi supportati:

- Visualizzare tutti gli indirizzi IP attualmente presenti nella blocklist: `/etc/init.d/banip survey blocklistv4`
- Cercare un IP specifico nella blocklist: `/etc/init.d/banip search IP_ADDRESS`
- Rimuovere il ban da un indirizzo IP: `nft delete element inet banIP blocklistv4 { IP_ADDRESS }`

Tenere presente che è necessario specificare la blocklist corretta nei comandi quando richiesto (`blocklistv4` per IPv4, `blocklistv6` per IPv6).

32.2.1 Bloccare DoS

Threat Shield IP include anche la protezione contro vari tipi di attacchi Denial of Service (DoS). La protezione DoS limita il traffico eccessivo di protocolli specifici, bloccando quel tipo di traffico fino a quando la situazione non si normalizza. Monitora tutto il traffico WAN in ingresso per rilevare e bloccare attacchi DoS provenienti dalla WAN.

- `Blocca DoS ICMP`: quando abilitata, questa opzione protegge dagli attacchi DoS che utilizzano il protocollo Internet Control Message Protocol (ICMP). Il limite è impostato a 100 pacchetti al secondo.
- `Blocca DoS TCP SYN`: questa opzione, quando attivata, protegge da attacchi DoS basati su TCP limitando il numero di nuove connessioni per secondo. Un pacchetto può essere considerato non valido se non fa parte di una connessione stabilita o se appartiene a una connessione che è stata chiusa. Il limite è impostato a 10 connessioni per secondo.
- `Blocca DoS UDP`: L'abilitazione di questa opzione protegge da attacchi DoS basati su User Datagram Protocol (UDP). Il limite è impostato a 100 pacchetti al secondo.

CAPITOLO 33

Threat shield DNS

Threat shield DNS utilizza Adblock, che blocca qualsiasi richiesta verso domini considerati dannosi. Il servizio può caricare liste di blocco mantenute dalla comunità oppure utilizzare feed Enterprise forniti da Nethesis e Yoroi, un'azienda leader focalizzata sulla CyberSecurity e membro della Cyber Threat Alliance.

Si noti che, per accedere alle blocklist di Nethesis e Yoroi, l'unità deve disporre di un abbonamento extra valido per questo servizio.

33.1 Configurazione

Nota: Utilizzare Threat shield DNS solo se non si sta già utilizzando il servizio FlashStart. Entrambi i servizi operano a livello DNS e non possono essere utilizzati insieme. L'interfaccia utente impedisce di abilitarli contemporaneamente per evitare conflitti.

Il servizio è disattivato per impostazione predefinita; per abilitarlo, navigare alla pagina `Threat shield DNS` nella sezione `Sicurezza`. Accedere alla scheda `Impostazioni` e attivare l'interruttore `Stato`.

Quando il servizio è abilitato, la scheda `Sorgenti blocklist` mostrerà tutte le blocklist disponibili. È possibile abilitare o disabilitare ciascuna blocklist utilizzando l'interruttore sul lato destro dell'elenco. Le blocklist abilitate verranno aggiornate automaticamente a intervalli regolari.

Per specificare su quali zone il servizio deve essere attivo, selezionarle nella combobox `Forza la redirezione DNS in queste zone`.

`Porte redirezionate` consente di specificare quali porte devono essere reindirizzate al servizio DNS di Threat shield.

33.1.1 Blocklist della community

Le blocklist della community sono fornite da contributori della community e bloccano vari domini relativi a: pubblicità, malware, spam, tracker, contenuti sessuali espliciti, pirateria e così via. NethSecurity le rende disponibili così come sono.

Le liste della community non forniscono un parametro «Confidence» standardizzato, pertanto l'interfaccia utente mostra la loro affidabilità come «Sconosciuta». Come euristica pratica, quando il nome della lista contiene un indicatore di severità o affidabilità (ad esempio, «lvl 1», «level 1»), generalmente indica il tasso di falsi positivi più basso e la massima affidabilità; al contrario, livelli più alti indicati (ad esempio, «lvl 2», «lvl 3», «lvl 4») tipicamente implicano una minore affidabilità e un rischio maggiore di voci aggressive o errate. Le convenzioni di denominazione variano e non tutti i fornitori della community includono tali indicatori, quindi è sempre consigliabile esaminare il contenuto e lo scopo di una lista della community prima di abilitarla in produzione. Il tipo di licenza d'uso può variare a seconda del fornitore, quindi se l'utilizzo non è personale, potrebbe essere necessario informarsi presso il fornitore.

Manutenzione delle liste della community

Ogni blocklist è gestita dal relativo provider specifico. NethSecurity include già gli URL per il download dei feed, che sono validi al momento del rilascio. Tuttavia, poiché questi URL sono codificati all'interno del sistema, se il provider li modifica, alcune blocklist potrebbero non essere più scaricabili.

33.1.2 Blocklist Enterprise

Subscription richiesta

Questa funzionalità è disponibile solo se l'unità dispone di un valido *abbonamento Community o Enterprise*.

Le blocklist enterprise sono specificamente focalizzate sulla sicurezza e offrono diversi vantaggi rispetto alle blocklist mantenute dalla comunità:

1. **Qualità e accuratezza**: Le blocklist aziendali, come quelle fornite da Nethesis e Yoroi, sono curate e mantenute da aziende di cybersecurity affidabili. Queste aziende dispongono di team dedicati che monitorano e aggiornano continuamente le blocklist per garantire che siano accurate ed efficaci nel bloccare il traffico dannoso. Questo si traduce in un livello superiore di qualità e accuratezza rispetto alle blocklist mantenute dalla comunità, che potrebbero non ricevere la stessa attenzione e frequenza di aggiornamenti.
2. **Tempestività**: Le blocklist aziendali vengono aggiornate frequentemente per includere le minacce più recenti e gli indirizzi IP dannosi. Aziende di cybersecurity come Nethesis e Yoroi monitorano attivamente le minacce emergenti e le aggiungono tempestivamente alle loro blocklist. Questo garantisce che il sistema sia protetto contro le minacce più recenti e in evoluzione.
3. **Falsi positivi ridotti**: I falsi positivi si verificano quando il traffico legittimo viene bloccato per errore. Le blocklist Enterprise sono progettate per ridurre al minimo i falsi positivi attraverso una selezione e una verifica accurata degli indirizzi IP e dei nomi host elencati. Le aziende che gestiscono le blocklist Enterprise dispongono di processi solidi per garantire che solo entità malevole vengano incluse nelle blocklist. Questo riduce la possibilità che il traffico legittimo venga bloccato, minimizzando le interruzioni alla rete o ai servizi.
4. **Supporto Enterprise**: Le blocklist Enterprise spesso includono supporto aggiuntivo e servizi pensati per ambienti aziendali. Questo comprende l'accesso al supporto tecnico, alla documentazione e all'assistenza per l'integrazione. In caso di problemi o domande durante l'utilizzo delle blocklist Enterprise, è possibile fare affidamento sul supporto fornito dalle aziende di cybersecurity per affrontarli in modo efficace.

33.1.3 Affidabilità

Le blocklist Enterprise includono un punteggio di «Affidabilità» che viene mostrato nell'interfaccia utente. Il punteggio è espresso come un valore da 1 a 10 e rappresenta la valutazione del provider sulla qualità della lista: valori più alti indicano una maggiore affidabilità e una minore probabilità di falsi positivi. Questa metrica di «Affidabilità» è disponibile solo per le liste Enterprise; le liste Community vengono presentate «così come sono» e mostrano «Sconosciuto» per l'affidabilità.

Le blocklist Yoroi e Nethesis sono blocklist Enterprise. Queste liste saranno visualizzate solo se l'unità dispone di un valido *abbonamento Enterprise o Community* e di un diritto valido per il servizio Threat Shield.

33.2 Bypass del filtro

Alcuni host o subnet potrebbero dover bypassare il filtro DNS di Threat shield. Per configurare il bypass del filtro, navigare nella scheda `Bypass filtro` di Threat shield DNS. Utilizzare il pulsante *Aggiungi bypass* per aggiungere un nuovo indirizzo all'elenco. L'indirizzo può essere un indirizzo IPv4/IPv6 valido con notazione CIDR opzionale.

33.3 Allowlist locale

Per consentire domini specifici che potrebbero essere inclusi nelle blocklist, è possibile navigare nella scheda `Allowlist locale` di Threat shield DNS. Utilizzare il pulsante *Aggiungi dominio* per aggiungere un dominio all'elenco; è possibile aggiungere una descrizione al dominio per ricordare il motivo per cui è stato aggiunto.

I domini presenti nella allowlist hanno priorità rispetto alle `Blocklists` e alla `Blocklist locale`.

33.4 Blocklist locale

Per bloccare domini specifici non inclusi nelle blocklist, è possibile navigare nella scheda `Blocklist locale` di Threat shield DNS. Utilizzare il pulsante *Aggiungi dominio* per aggiungere un dominio all'elenco; è possibile aggiungere una descrizione al dominio per ricordare il motivo per cui è stato aggiunto.

Avvertimento: La risoluzione DNS per i nomi elencati nella blocklist influenzerà anche l'unità stessa

33.5 Verificare se un dominio è bloccato

Se si riscontrano problemi con la risoluzione dei domini e si desidera verificare se un dominio specifico è bloccato, è possibile eseguire una query direttamente dal terminale locale.

Utilizzare il seguente comando per verificare un dominio:

```
/etc/init.d/adblock query <domain>
```

Ad esempio:

```
root@nethsecurity8:~# /etc/init.d/adblock query baddomain.com
```

L'output potrebbe apparire così:

```
:::
::: domain 'baddomain.com' in active blocklist
:::
  + baddomain.com

:::
::: domain 'baddomain.com' in backups and black-/whitelist
:::
  + adb_list.adult.gz             baddomain.com
```

Questa schermata mostra se il dominio è attualmente bloccato da una qualsiasi delle blocklist attive. In questo esempio specifico, il dominio *baddomain.com* fa parte della categoria **adult**, come indicato da `adb_list.adult.gz`. Questo aiuta a identificare quale categoria o lista ha causato il blocco del dominio.

33.6 Configurazione avanzata

Quando Threat shield DNS è abilitato:

- Un nuovo file sorgente di categoria viene generato in base alla registrazione dell'unità e ai diritti.
- Tutte le query DNS vengono reindirizzate alla macchina locale.
- Adblock è configurato per utilizzare il nuovo file di origine delle categorie e verrà avviato automaticamente.

Anche se non è raccomandato, è possibile utilizzare Adblock senza Threat shield DNS. Per opzioni di configurazione più dettagliate, consultare il manuale per sviluppatori.

CAPITOLO 34

Filtro Deep Packet Inspection (DPI)

NethSecurity utilizza Netify Agent per impiegare tecniche di Deep Packet Inspection (DPI) per il filtraggio del traffico di rete.

Il Netify Agent funziona come un server di deep-packet inspection, sfruttando nDPI (precedentemente OpenDPI) per identificare protocolli e applicazioni di rete. Le informazioni rilevate possono essere memorizzate localmente, accessibili tramite socket UNIX o TCP, oppure inviate tramite HTTP POST a un server remoto di terze parti. Dettagli come i metadati dei flussi, le statistiche di rete e le classificazioni di rilevamento possono essere utilizzati per prendere decisioni sul flusso.

Ecco come funziona:

- il plugin delle azioni di flusso Netify assegna etichette alle connessioni corrispondenti
- Le regole nft possono quindi bloccare o regolare la priorità (DSCP) delle connessioni in base a queste etichette.

L'amministratore può creare regole di Deep Packet Inspection (DPI) per ciascuna interfaccia.

34.1 Configurazione

Per configurare queste regole, l'amministratore avvia il processo selezionando l'interfaccia di rete specifica sulla quale la regola deve operare. Questo passaggio garantisce che la regola venga applicata con precisione al segmento di rete designato, consentendo una gestione mirata ed efficace del traffico di rete.

Dopo la selezione dell'interfaccia, all'amministratore viene richiesto di specificare le applicazioni che devono essere bloccate o regolate. Questo passaggio essenziale prevede la scelta da un elenco completo di applicazioni accessibile tramite l'interfaccia del sistema.

L'interfaccia, come funzionalità predefinita, presenta un catalogo di applicazioni comunemente utilizzate. Tuttavia, offre una funzionalità di ricerca avanzata che consente all'amministratore di esplorare e individuare applicazioni specifiche e categorie di applicazioni che richiedono particolare attenzione.

34.1.1 Firme delle applicazioni Premium

Subscription richiesta

Questa funzionalità è disponibile solo se il firewall dispone di una subscription *Community o Enterprise* valida.

In assenza di una subscription, il sistema riconosce intrinsecamente una base di circa 400 applicazioni. Tuttavia, con una subscription attivo, questa capacità si espande significativamente, includendo oltre 2300 applicazioni. In questo scenario, l'elenco delle applicazioni riconosciute viene aggiornato quotidianamente, garantendo che il sistema rimanga al passo con il panorama in continua evoluzione delle applicazioni e dei servizi digitali.

34.1.2 Elenco di applicazioni e protocolli

L'elenco completo di tutte le applicazioni e i protocolli supportati dalla versione Enterprise è disponibile qui:

- Applicazioni
- Protocolli

34.1.3 Eccezioni

L'esclusione DPI consente di escludere indirizzi di rete specifici, come il gateway o altre infrastrutture critiche, impedendo che vengano bloccati.

Per aggiungere una nuova eccezione, fare clic sul pulsante `Aggiungi eccezione`. Inserire l'`Indirizzo IP address o CIDR` che deve essere escluso dal filtro. È possibile includere una descrizione che spieghi il motivo dell'esclusione.

Ogni eccezione può essere abilitata o disabilitata secondo necessità.

34.1.4 Netify traffic bypass

By default, Netifyd processes all traffic passing from, to and out of the firewall. In some cases it may be desiderable to completely ignore traffic analysis on some specific hosts or subnets. The exclusions is configured using the *bypassv4* and *bypassv6* options that take a list of IP addresses or CIDR subnets. Bypasses can have a description to explain the reason for the bypass, separated by a | pipe character after the IP.

To add a new bypass entry, use the following command:

```
uci add_list netifyd.config.bypassv4='10.45.23.0/24|Remote network'
uci add_list netifyd.config.bypassv4='192.168.5.164|Critical host'
uci commit netifyd
reload_config
```

To edit and manage uci entries, refer to the *UCI list management* section.

You can visualize the applied bypass entries and netifyd capture configuration using the following command:

```
nft list table inet netifyd
```

CAPITOLO 35

Filtro DNS FlashStart

Il filtro DNS si integra con software di filtraggio dei contenuti basato su DNS di terze parti; il filtro dei contenuti supportato di default è quello fornito da FlashStart.

Collega fondamentalmente 2 componenti: la configurazione dei filtri e la configurazione di rete.

1. La configurazione del filtro dei contenuti avviene interamente sulla piattaforma di terze parti; tipicamente è possibile bloccare singoli siti web, nonché categorie di siti (ad esempio, per adulti), gestire eccezioni, visualizzare report e così via.
2. La configurazione della rete è completamente automatizzata ed è gestita da NethSecurity, che si occupa di:

- collegare il firewall all'istanza specifica di terze parti
- reindirizzare tutte le richieste DNS al servizio esterno
- aggiornare automaticamente gli indirizzi IP di tutte le connettività

Richiesta subscription

Questa funzionalità è disponibile solo se il firewall dispone di una subscription valida.

Nota: Prima di configurare NethSecurity è necessario creare un account su FlashStart e configurare il servizio. FlashStart è un servizio a pagamento che consente di utilizzare licenze di prova. Fare riferimento alla documentazione del fornitore doc.

Avvertimento: Non specificare manualmente gli indirizzi IP dei server DNS di FlashStart, poiché vengono gestiti automaticamente dall'integrazione.

Una volta che l'account è stato creato e il servizio configurato, è possibile configurare NethSecurity.

35.1 Raccomandazioni prima di configurare FlashStart DNS Filter

Prima di abilitare il filtro DNS di FlashStart, si prega di considerare le seguenti raccomandazioni importanti:

1. **Comportamento di reindirizzamento DNS** Quando il filtraggio dei contenuti è abilitato, tutto il traffico DNS proveniente dai client verrà automaticamente reindirizzato al servizio di filtraggio esterno FlashStart, indipendentemente dalla loro configurazione. **Non apportare modifiche ai server DNS configurati in NethSecurity o nei client di rete.**
2. **Bloccare i protocolli DNS alternativi** Per preservare l'efficacia del filtro dei contenuti, si raccomanda vivamente di bloccare i protocolli DNS alternativi come DoT e DoH. L'approccio più efficace consiste nell'utilizzare la blocklist IP di Threat Shield "public DoH-Provider" per bloccare i provider DoH noti e nel rifiutare tutte le connessioni TCP in uscita sulla porta 853 per bloccare il traffico DoT.
3. **Evitare conflitti con Threat Shield DNS** Utilizzare FlashStart solo se **non si sta già utilizzando il servizio Threat Shield DNS**, poiché l'uso simultaneo di entrambi potrebbe causare conflitti.

35.2 Configurazione

35.2.1 Configurazione della piattaforma FlashStart

Prima di configurare FlashStart sul firewall, è necessario prima acquistare e configurare il servizio **Pro** o **Pro Plus** sulla piattaforma FlashStart. Una volta acquistato il servizio, sarà necessario configurare le reti sul portale FlashStart.

Durante il processo di configurazione, il sistema guiderà l'utente attraverso la procedura di impostazione; seguire le istruzioni e selezionare le seguenti opzioni:

Collega il router della tua rete → Ho un IP dinamico → Sincronizza con DNS dinamico Nethesis → NethSecurity → Scegliere PRO o PRO PLUS.

Nota: A partire dal 2 luglio 2025, la piattaforma FlashStart richiede la creazione di un nuovo nome utente e una nuova password durante questa fase di configurazione. Si noti che non è più possibile utilizzare l'accesso tramite email precedentemente associato all'account. Una volta create le nuove credenziali, queste dovranno essere utilizzate per l'autenticazione lato firewall.

Le reti precedentemente configurate utilizzando l'accesso basato su email continueranno a funzionare normalmente finché non vengono rimosse. Se una rete viene rimossa, il sistema richiederà una nuova coppia di nome utente e password, e le relative credenziali dovranno essere aggiornate anche sul lato NethSecurity.

35.2.2 Configurazione di NethSecurity

- `Stato` : È possibile abilitare o disabilitare il filtro DNS utilizzando l'interruttore `Stato`.
- `Tipo di servizio` : Selezionare il tipo di servizio acquistato: **Pro** oppure **Pro Plus**
- `Nome utente` : Inserire lo stesso nome utente utilizzato per il proprio account FlashStart
- `Password` : Inserire la stessa password utilizzata per l'account FlashStart
- `Zone da filtrare` : Selezionare le zone di rete che si desidera proteggere con il filtro DNS. Solo le zone selezionate saranno interessate dal filtro DNS di FlashStart.

- `Bypass Source IPs or Networks` : È possibile specificare un elenco di indirizzi IP o reti (formato CIDR) che devono bypassare il filtro DNS. Il traffico proveniente da queste sorgenti non sarà soggetto ad alcuna regola di filtraggio.
- `Server DNS personalizzati` : Se è necessario definire **resolver DNS personalizzati per domini specifici**, è possibile configurarli qui. La sintassi è la stessa utilizzata nella sezione DNS di NethSecurity. Per riferimento, consultare la documentazione ufficiale: Server DNS specifici per dominio

Una volta che il servizio FlashStart è stato configurato sul firewall, tutta la configurazione e la gestione successive devono essere effettuate esclusivamente tramite il portale web di FlashStart. Non sono necessarie ulteriori modifiche sul firewall stesso.

35.2.3 Configurazione del server DNS

I server DNS utilizzati da FlashStart vengono configurati automaticamente da NethSecurity quando il servizio viene abilitato. È possibile personalizzare alcune opzioni:

- **Registrazione delle query**: È possibile abilitare la registrazione delle query eseguendo il seguente comando:

  ```
  uci set flashstart.global.logqueries='1'
  uci commit flashstart
  reload_config
  ```

  Questo registrerà le query DNS nel registro di sistema del firewall, il che può essere utile per scopi di monitoraggio e risoluzione dei problemi.

- **Protezione contro il DNS Rebind**

La protezione contro il DNS Rebind è disabilitata per impostazione predefinita per i client FlashStart, al fine di evitare blocchi indesiderati quando i server DNS interni risolvono domini privati o interni che altrimenti potrebbero essere segnalati dal meccanismo di protezione DNS Rebind del firewall. Se necessario, questa protezione può essere abilitata manualmente utilizzando la seguente configurazione:

```
uci set flashstart.global.rebind_protection='1'
uci commit flashstart
reload_config
```

35.3 Presenza di un controller Active Directory (AD)

Se è presente un controller AD, è possibile abilitare il profiling basato sull'utente. Per fare ciò, è necessario prima installare il connettore specifico di FlashStart (fare riferimento alla documentazione ufficiale di FlashStart per le istruzioni di installazione), **attualmente disponibile solo per Microsoft Windows Server**.

35.3.1 Gestione DNS nella rete

Tutti i client sulla rete devono instradare le loro richieste DNS attraverso NethSecurity invece di interrogare direttamente il controller AD; questo impedisce ai client di ereditare la policy di profilazione del controller AD.

Dettagli di configurazione

- Il controller AD utilizza un resolver DNS esterno.
- Nell'interfaccia utente di FlashStart DNS su NethSecurity, aggiungere il dominio locale del controller AD per la risoluzione, specificando l'indirizzo IP del controller AD per la risoluzione di questi nomi locali (ad esempio, `/ad.mydomain.local/192.168.55.1`).
- Configurare i client affinché utilizzino un server DNS esterno oppure il firewall stesso come loro resolver DNS.

Note importanti

È necessario impedire ai client di interrogare il controller AD per la risoluzione di domini non locali; questo può essere ottenuto tramite:

- Blocco della porta 53 UDP/TCP in ingresso sul controller AD
- disabilitare la ricorsione DNS per i client sul server AD, in modo che il server risponda solo alle query per la propria zona locale.

35.4 FlashStart Pro vs FlashStart Pro Plus

FlashStart fornisce soluzioni di filtraggio dei contenuti basate su cloud integrate con NethSecurity. I due principali tipi di servizio, FlashStart Pro e FlashStart Pro Plus, offrono capacità differenti in termini di granularità del filtraggio e gestione dei profili. Di seguito è riportato un breve confronto che evidenzia le principali differenze.

35.4.1 FlashStart Pro

FlashStart Pro consente il filtraggio dei contenuti utilizzando un unico profilo di filtro, applicato all'intera rete o a zone di rete selezionate.

- **Filtraggio con profilo singolo:** Tutti gli IP filtrati seguono le stesse regole e i blocchi di categoria definiti sulla piattaforma FlashStart.
- **Applicazione basata su zone:** Gli amministratori possono scegliere quali zone di rete sono soggette al filtraggio.
- **Gestione dei profili basata su IP:** FlashStart Pro su NethSecurity supporta implicitamente tre profili di traffico, basati su IP:
  - IP filtrati : Soggetti al singolo profilo di filtro definito in FlashStart.
  - IP non filtrati : Nessun filtro applicato (vedere Esclusioni di seguito)
  - IP bloccati : Accesso negato a livello di firewall utilizzando regole del firewall.
- **Esclusioni:** È possibile configurare delle eccezioni utilizzando indirizzi IP o blocchi CIDR.

35.4.2 FlashStart Pro Plus (Beta)

FlashStart Pro Plus estende la funzionalità con il supporto per più profili di filtraggio indipendenti, consentendo una maggiore flessibilità e l'applicazione delle policy a livello utente.

- **Supporto multi-profilo:** Possono essere definiti fino a 5 profili indipendenti, ciascuno con la propria configurazione di filtraggio.
- **Configurazione indipendente del profilo:** Ogni profilo può essere personalizzato individualmente (categorie, Safe Search, restrizioni YouTube, ecc.).
- **Opzioni dei criteri di filtraggio:** I profili possono essere assegnati utilizzando:
  - **Oggetti firewall (host set):** Dal pannello di configurazione di FlashStart, gli amministratori possono associare insiemi specifici di host (definiti nel firewall) a un profilo.
  - **Utenti Active Directory:** Se il connettore FlashStart AD è installato, i profili possono essere assegnati direttamente agli utenti AD, eliminando la necessità di fare affidamento sugli indirizzi IP.

Nota: A causa delle limitazioni della piattaforma, il sistema può gestire insiemi di host con un numero limitato di elementi.

Se l'insieme contiene solo host, può includere fino a 16 voci. Se contiene solo reti CIDR, può includere fino a 13 voci. Se l'insieme di host contiene dati misti (sia host che reti), è consigliabile fare riferimento al limite inferiore (13).

35.4.3 Funzionalità comuni (Pro e Pro Plus)

- **Stesse capacità di filtraggio:**
  - Filtraggio basato su categorie di URL (liste nere)
  - Filtraggio dei motori di ricerca (Safe Search)
  - Modalità con restrizioni di YouTube
  - Protezione dalle minacce
- **Configurazione gestita dal cloud:** Tutte le regole di filtraggio e i profili sono gestiti tramite l'interfaccia web di FlashStart.

Funzionalità	FlashStart Pro	FlashStart Pro Plus
Filtraggio basato su zone	Sì	Sì
Esclusioni del profilo (IP/CIDR)	Sì	Sì
Numero di profili filtro	1	Fino a 5
Blocco IP	No	Sì
Blocco app	No	Sì
Agente remoto per Win/Mac/Android/iOS	No	Sì
Filtraggio per utente AD	No	Sì
Integrazione degli oggetti firewall	No	Sì
Gestione dei conflitti (utente vs oggetto)	N/A	L'oggetto Firewall ha la priorità

Nota: Sebbene al momento non siano stati segnalati bug noti, la funzionalità Pro Plus è attualmente rilasciata come **Beta**. Si consiglia di testarla in un ambiente non critico prima di implementarla in produzione.

35.5 Risoluzione dei problemi

35.5.1 1. Il mio IP pubblico non è elencato nelle reti FlashStart

Se l'indirizzo IP pubblico non compare nella dashboard di FlashStart sotto le reti registrate, attendere fino a 15 minuti. Questo ritardo può essere causato da meccanismi di protezione sulla piattaforma FlashStart progettati per mitigare tentativi di registrazione ripetuti o automatizzati.

35.5.2 2. Il filtro DNS sembra non funzionare

Se il filtraggio non è efficace immediatamente dopo la configurazione:

- Si tenga presente che FlashStart potrebbe richiedere alcuni minuti per propagare le impostazioni applicate attraverso la propria infrastruttura.
- Considerare anche l'impatto della cache DNS del browser, che potrebbe ritardare gli effetti visibili.

Per verificare se il filtraggio è effettivamente attivo e funzionante, è possibile eseguire una query DNS manuale **sul client locale** utilizzando il comando *dig*:

```
dig @8.8.8.8 www.mydomain.com
```

Sostituire `www.mydomain.com` con il dominio effettivo che si sta testando.

Se il dominio viene ancora risolto e dovrebbe essere bloccato, verificare nuovamente il profilo attivo e le impostazioni di blocco sulla dashboard di FlashStart.

Nota: Questo test `dig` deve essere sempre eseguito dal **client** e **mai dal firewall**. Il firewall **non** viene **mai** filtrato dai server DNS di FlashStart, poiché ciò potrebbe potenzialmente entrare in conflitto con alcuni dei servizi che fornisce.

35.5.3 3. Verifica del filtraggio DNS con dig direttamente dal firewall

Se si desidera eseguire dei test utilizzando `dig` direttamente dal firewall, è possibile farlo specificando la porta. Ogni porta corrisponde a un diverso profilo di filtraggio.

FlashStart Pro

Se si utilizza **FlashStart Pro**, la porta è sempre **5300**. È possibile verificare se la richiesta viene filtrata correttamente con il seguente comando:

```
dig @127.0.0.1 -p 5300 mydomain.com
```

FlashStart Pro Plus

Se si utilizza **FlashStart Pro Plus**, ogni profilo è associato a una porta diversa. È possibile inviare una richiesta per ciascun profilo per verificare che il filtraggio si comporti come previsto.

Per prima cosa, è necessario identificare la porta corretta per ciascun profilo. Utilizzare il seguente comando per visualizzare la configurazione:

```
uci show dhcp
```

Si vedranno più voci come questa:

```
dhcp.ns_56e6071cbd=dnsmasq
dhcp.ns_56e6071cbd.ns_flashstart='1'
dhcp.ns_56e6071cbd.ns_tag='automated'
dhcp.ns_56e6071cbd.ns_flashstart_profile='Guests'
dhcp.ns_56e6071cbd.ns_flashstart_dns_code='143'
dhcp.ns_56e6071cbd.port='5301'
dhcp.ns_56e6071cbd.noresolv='1'
dhcp.ns_56e6071cbd.max_ttl='60'
dhcp.ns_56e6071cbd.max_cache_ttl='60'
dhcp.ns_56e6071cbd.server='185.236.104.124' '185.236.105.125'
```

In questo esempio, il profilo **«Guests»** è associato alla porta **5301**, quindi si dovrebbe eseguire:

```
dig @127.0.0.1 -p 5301 mydomain.com
```

CAPITOLO 36

Intrusion Prevention System (Snort)

Snort 3 è un sistema open-source di prevenzione delle intrusioni di rete (Intrusion Prevention System) in grado di eseguire l'analisi del traffico in tempo reale e la registrazione dei pacchetti sulle reti IP. Può effettuare l'analisi dei protocolli, la ricerca/corrispondenza di contenuti e può essere utilizzato per rilevare una varietà di attacchi e sonde, come buffer overflow, scansioni di porte stealth, attacchi CGI, sonde SMB, tentativi di fingerprinting del sistema operativo e molto altro.

36.1 Abilitare IPS

IPS è disabilitato per impostazione predefinita; per abilitarlo, navigare alla pagina `IPS` nella sezione `Sicurezza`. L'interfaccia segnalerà che il servizio è disabilitato e fornirà un collegamento rapido per accedere direttamente alla scheda `Impostazioni`.

Una volta attivato l'interruttore *Stato*, sarà possibile configurare il servizio.

36.1.1 Politica delle regole

Le regole sono raggruppate in policy, ciascuna policy è un insieme di regole ottimizzate per un caso d'uso specifico; le policy sono:

- **connettività**: dà priorità alle prestazioni rispetto alla sicurezza, riducendo al minimo i falsi positivi e garantendo elevate prestazioni del dispositivo, pur rilevando le minacce comuni.
- **bilanciato**: consigliato per le implementazioni iniziali, bilancia sicurezza e prestazioni, offrendo un livello di prestazioni relativamente elevato con strumenti di valutazione e test.
- **sicurezza**: per ambienti ad alta sicurezza con larghezza di banda ridotta e una maggiore tolleranza ai falsi positivi. Fornisce la massima protezione riducendo al minimo il rischio di interrompere la rete.

36.1.2 Reti domestiche

Le reti domestiche definiscono le reti interne protette e specificano gli indirizzi IP o le subnet che IPS dovrebbe considerare come reti locali, permettendo di distinguere il traffico interno da quello esterno e riducendo i falsi positivi nel rilevamento delle minacce.

Selezionare una policy, definire le proprie reti domestiche e quindi fare clic sul pulsante *Salva* per salvare le modifiche.

Nota: I valori delle Reti Domestiche non vengono aggiornati automaticamente. Se l'indirizzo IP di un'interfaccia locale viene modificato e questo comporta una rete diversa, la configurazione della rete domestica dell'IPS deve essere aggiornata manualmente per riflettere la nuova rete.

36.1.3 Abilitare Hyperscan

Hyperscan è un motore avanzato di pattern matching che può migliorare le prestazioni di Snort3 sull'hardware supportato. Richiede che la CPU supporti specifici flag del processore.

Prima di abilitare Hyperscan, verificare che il processore supporti i flag CPU richiesti:

```
grep --color=auto -E 'sse3|ssse3|sse4_1|sse4_2|avx|avx2' /proc/cpuinfo
```

Se il comando restituisce dei risultati, il processore è compatibile con Hyperscan.

Per abilitare Hyperscan, creare innanzitutto il file di configurazione in `/etc/snort/hyperscan.config`:

```
cat > /etc/snort/hyperscan.config << 'EOF'
search_engine = { search_method = hyperscan }
detection = { hyperscan_literals = true, pcre_to_regex = true }
EOF
```

Quindi abilitarlo con i seguenti comandi:

```
uci set snort.snort.include=/etc/snort/hyperscan.config
uci commit snort
reload_config
```

Per disabilitare Hyperscan:

```
uci del snort.snort.include
uci commit snort
reload_config
```

Nota: Hyperscan è una funzionalità opzionale per il miglioramento delle prestazioni. Attivarla solo se la CPU supporta i flag del processore richiesti e si desidera migliorare le prestazioni dell'IPS a fronte di requisiti più elevati per le funzionalità della CPU.

36.2 Accesso alle regole Snort tramite Oinkcode

NethSecurity supporta l'utilizzo di un abbonamento Snort per ottenere regole `Registered` e `Subscriber` tramite l'Oinkcode. L'*Oinkcode* è un codice univoco assegnato agli utenti registrati su Snort.org; questo codice è necessario per autenticare il download delle regole Snort.

36.2.1 Categorie di regole disponibili

- **Regole della Community (Regole gratuite)**: Disponibili per tutti gli utenti registrati senza restrizioni. Mantenute dalla community di Snort. Forniscono una protezione di base ma ricevono aggiornamenti meno frequenti rispetto alle regole ufficiali. Non è necessario alcun Oinkcode per accedere a queste regole.
- **Regole Registrate (Regole gratuite con ritardo)**: Regole ufficiali aggiornate dal team Snort. Disponibili gratuitamente per gli utenti registrati, ma con un ritardo di 30 giorni rispetto alla versione più recente. È necessario un Oinkcode per accedere a queste regole.
- **Regole per abbonati (regole a pagamento, aggiornamenti in tempo reale)**: Accesso immediato alle regole più aggiornate senza alcun ritardo. Disponibile solo per gli utenti con un abbonamento Snort Subscriber Rule Set. È necessario un Oinkcode per accedere a queste regole.

36.2.2 Come ottenere e utilizzare l'Oinkcode

- Registrarsi su Snort.org
- Recuperare il proprio Oinkcode dalla sezione del profilo account
- Su NethSecurity, incollare il proprio codice personale nel campo *Oinkcode*. È possibile verificare se il codice è valido facendo clic sul pulsante *Verifica codice*.

36.3 Elenco eventi di oggi

L'IPS controlla automaticamente il traffico all'interno della rete e genera avvisi o blocca il traffico in base al set di regole. Un elenco consultabile è disponibile nella scheda `Eventi di oggi`. Durante la consultazione dell'elenco, è possibile vedere le regole che hanno generato l'avviso, gli indirizzi IP di origine e destinazione, il protocollo e l'azione intrapresa dal sistema.

Questo elenco può essere filtrato utilizzando la casella di filtro nella parte superiore della pagina. Inoltre, per ogni record visualizzato, è possibile accedere direttamente alla documentazione della regola facendo clic sull'ID della regola.

Facendo clic sull'icona del menu sul lato destro del record, è possibile aprire un modulo precompilato per sopprimere o disabilitare la regola che ha generato l'avviso.

36.4 Bypass del filtro

Tutto il traffico che passa attraverso il firewall viene analizzato dall'IPS. Il sistema supporta regole di bypass per indirizzi IPv4 e IPv6 specifici. Qualsiasi indirizzo IP aggiunto a una regola di bypass verrà valutato sia per il traffico in ingresso che in uscita.

Per farlo, accedere alla scheda *Filter bypass* e premere il pulsante *Aggiungi bypass*. Viene fornito un modulo per aggiungere una regola di bypass per un indirizzo IP specifico; la regola si applica al traffico in entrambe le direzioni e include i seguenti campi:

- `Tipo di indirizzo`: se l'IP fornito è IPv4 o IPv6
- `Indirizzo IP`: l'indirizzo IP o CIDR da bypassare
- `Descrizione`: una descrizione della regola di bypass; è opzionale e può essere omessa

36.5 Disabilitare regole

In alcuni ambienti, le regole possono essere troppo restrittive o generare troppi falsi positivi. Per evitare ciò, è possibile disabilitare alcune regole. Una regola disabilitata è una regola che non viene inclusa nel set di regole di Snort.

Passare alla scheda *Regole disabilitate* e premere il pulsante *Disabilita regola*. Il sistema richiederà i seguenti campi:

- `GID`: il GID della regola, è un numero e di solito è sempre *1*
- `SID`: il SID della regola, è un numero
- `Descrizione`: una descrizione della regola disabilitata; è opzionale e può essere omessa

36.6 Allarmi silenziati

Una regola di soppressione è una regola che viene ignorata da Snort per un indirizzo IP o CIDR specifico. La regola viene comunque valutata per tutti gli altri indirizzi IP.

Per aggiungere una regola di soppressione, accedere alla scheda *Allarmi silenziati* e premere il pulsante *Silenzia allarme*. Compilare i campi con le seguenti informazioni:

- `GID`: il GID della regola, è un numero e di solito è sempre *1*
- `SID`: il SID della regola, è un numero
- `Direzione`: se la soppressione riguarda l'indirizzo IP di origine o di destinazione
- `Indirizzo IP`: l'indirizzo IP per cui sopprimere l'avviso; può essere un intervallo CIDR
- `Descrizione`: una descrizione della regola di soppressione; è facoltativa e può essere omessa

CAPITOLO 37

OpenVPN Road Warrior

Road Warrior si riferisce a una configurazione specifica di OpenVPN VPN pensata per utenti remoti, che consente loro di accedere in modo sicuro a una rete privata da qualsiasi luogo su Internet. Questa configurazione è particolarmente utile per aziende e organizzazioni con dipendenti o collaboratori distribuiti in diverse sedi, garantendo comunicazioni cifrate e la privacy dei dati.

OpenVPN è un protocollo supportato dalle piattaforme più diffuse, con *client gratuiti* disponibili per sistemi Windows, MacOS, Linux, Android e iOS.

Nota: Prima di configurare OpenVPN Road Warrior, assicurarsi di aver letto il capitolo relativo al *database utenti*.

37.1 Configurazione del server

Un server OpenVPN è in esecuzione su NethSecurity in attesa che i client remoti lo contattino e stabiliscano una connessione. Deve essere raggiungibile da internet sulla sua porta specifica (predefinita: `1194/UDP`). Più client possono connettersi al server, autenticarsi e ottenere l'accesso alla rete privata; non è necessario che i client siano raggiungibili da internet. Ogni client che si connette, dopo l'autenticazione, riceve un indirizzo IP con cui si presenterà alla rete remota.

Un server OpenVPN su NethSecurity è strettamente collegato a un database utenti, che può essere locale o remoto. L'associazione con il database viene definita durante la creazione del server e non può essere modificata successivamente.

La configurazione del server è semplificata perché NethSecurity imposta automaticamente la maggior parte dei campi su valori predefiniti adeguati, che di solito richiedono solo una verifica.

Per configurare un nuovo server OpenVPN, fare clic sul pulsante *Crea server* e configurare i campi proposti:

- `Nome del server`: assegnare un nome a questo server OpenVPN
- `Database utenti`: scegliere il database utenti da utilizzare per l'autenticazione; può essere un database locale oppure uno remoto (ad esempio LDAP o Active Directory)

- `Crea un account per ogni utente`: questo è un campo speciale e non verrà mostrato nuovamente in futuro; consente di creare automaticamente un account VPN per ogni utente presente nel database. Tutti gli account creati avranno un certificato valido per 3650 giorni.
- `Modalità`: bridged o routed; la modalità routed è quella predefinita e la più comune, consente di creare una rete virtuale in cui i client sono connessi al server e possono comunicare tra loro. La modalità bridged è meno comune e permette di collegare i client al server come se fossero connessi alla stessa LAN; questa modalità è utile quando i client devono accedere a risorse che non sono direttamente accessibili dal server. In caso di dubbio, selezionare la modalità routed.
- `Modalità di autenticazione`: sono supportate diverse modalità di autenticazione:
  - `Utente e password`: il client che si connette deve fornire un nome utente e una password validi; solo gli utenti con una password impostata possono utilizzare questa modalità
  - `Certificato`: il client che si connette deve disporre di un proprio certificato per autenticarsi; questa è la modalità consigliata nella maggior parte dei casi
  - `Utente, password e certificato`: il client che si connette deve fornire un nome utente, una password e un certificato validi
  - `Nome utente, certificato e OTP`: il client che si connette deve fornire un nome utente valido, un certificato e anche un codice OTP utilizzato come password. Questa modalità richiede una configurazione aggiuntiva nel client per ricevere il codice OTP.
- `Rete VPN`: la rete virtuale utilizzata dai client; a ogni client verrà assegnato un indirizzo IP prelevato da questa rete. NethSecurity suggerisce già una rete poco comune per evitare sovrapposizioni con altre reti utilizzate dal firewall.
- `Inizio intervallo IP dinamico`: il primo indirizzo IP che verrà assegnato ai client che si connettono al server; l'indirizzo deve far parte della rete VPN. Quando si aggiunge una prenotazione IP a un client, assicurarsi che l'indirizzo IP sia al di fuori dell'intervallo dinamico.
- `Fine intervallo IP dinamico`: l'ultimo indirizzo IP che verrà assegnato ai client che si connettono al server
- `Indirizzo IP/hostname pubblico di questa unità`: NethSecurity compila automaticamente questo campo con l'indirizzo IP pubblico di ciascuna interfaccia WAN configurata. Questi IP/hostname verranno inseriti nella configurazione del client. L'ordine degli elementi è fondamentale perché il client che si connette inizierà a contattare gli IP/hostname partendo dal primo nella lista e proseguendo con i successivi in caso di indisponibilità.

Fare clic sul pulsante *Crea* per creare il server. Successivamente, i dettagli principali del server verranno mostrati nell'interfaccia Web.

37.1.1 Impostazioni avanzate

Se necessario, è anche possibile personalizzare alcune opzioni avanzate:

- `Protocollo`: UDP (predefinito), TCP
- `Porta`: 1194 (predefinita)
- `Instrada tutto il traffico attraverso la VPN`: se abilitata, tutto il traffico proveniente dal client verrà instradato all'interno del tunnel VPN, incluso il traffico internet standard. Può essere utilizzata per scopi di monitoraggio e controllo, ma solitamente è disabilitata perché introduce una maggiore latenza e consuma larghezza di banda.
- `Instrada queste reti sulla VPN`: un elenco di reti che il client deve instradare nel tunnel VPN; le reti LAN vengono aggiunte automaticamente, ma possono anche essere rimosse e altre reti possono essere aggiunte allo stesso modo

- `Consenti il traffico tra i client`: consente a tutti i client connessi di scambiarsi traffico tra loro; si consiglia di lasciarlo disabilitato.
- `Compressione`: comprime il traffico del tunnel OpenVPN per risparmiare larghezza di banda. Tuttavia, attualmente questa opzione è meno utile e, in alcuni casi, può essere dannosa. Si raccomanda vivamente di lasciarla disabilitata. Quando questa opzione viene modificata, è necessario scaricare nuovamente la configurazione del client.
- `Digest`: il digest autentica i pacchetti del canale dati (SHA 256 predefinito)
- `Cipher`: cifrario di crittografia utilizzato (predefinito AES-256-GCM)
- `Imporre una versione minima di TLS`: consente la connessione solo ai client che utilizzano una versione di TLS uguale o superiore a quella specificata.
- `Opzioni DHCP personalizzate`: consente di passare opzioni DHCP specifiche al client (ad esempio DOMAIN, DNS, WINS e così via)

Opzioni DHCP

Le opzioni DHCP vengono utilizzate per trasmettere parametri di configurazione specifici al client. Le opzioni DHCP disponibili sono:

1. `DNS [addr]`: imposta gli indirizzi del server DNS primario e secondario (IPv4 o IPv6). Ripetere l'opzione per impostare più indirizzi.
2. `WINS [addr]`: imposta gli indirizzi del server Windows Internet Name Service primario e secondario (server dei nomi NetBIOS su TCP/IP). Ripetere l'opzione per impostare più indirizzi.
3. `NBDD [addr]`: imposta gli indirizzi del server di distribuzione datagrammi NetBIOS primario e secondario (NetBIOS over TCP/IP Datagram Distribution Server). Ripetere l'opzione per impostare più indirizzi.
4. `NTP [addr]`: imposta gli indirizzi dei server Network Time Protocol primario e secondario. Ripetere l'opzione per impostare più indirizzi.
5. `NBT [type]`: imposta il tipo di modalità NetBIOS over TCP/IP
    - `1`: Trasmissione
    - `2`: Punto-a-punto (usa WINS)
    - `4`: Misto (broadcast, poi query al name server)
    - `8`: Ibrido (interroga il name server, poi trasmette in broadcast)
6. `NBS [scope-id]`: imposta l'ID di ambito NetBIOS per isolare il traffico NetBIOS e consentire nomi di computer univoci tra ambiti diversi.
7. `DISABLE-NBT [1]`: Disattiva NetBIOS su TCP/IP. Il parametro è semplicemente `1` per abilitare l'opzione.

37.2 Account VPN

Ora che il server è stato configurato, è necessario creare gli account per i client che si connetteranno. Per fare ciò, fare clic su *Aggiungi account VPN* e compilare il modulo:

- `Utente`: ogni account è associato a un solo utente dal database selezionato; selezionare l'utente per questo account
- `IP riservato`: specificare un indirizzo IP che faccia parte della rete VPN definita ma che sia al di fuori dell'intervallo dinamico. L'indirizzo IP inserito verrà sempre assegnato a questo specifico account; ciò può essere molto utile per creare regole firewall. Lasciare vuoto per assegnare un indirizzo IP casuale a ogni connessione.

- `Scadenza certificato (giorni)`: specificare una durata del certificato (predefinito 3650 giorni)

Una volta creato l'account, è necessario esportare la configurazione e caricarla nel client che deve connettersi. Per fare ciò, è sufficiente cliccare sul menu dell'account specifico e scegliere `Scarica configurazione`. Questa azione scarica il file pronto all'uso, semplicemente da caricare nel client. Questo file viene generato dinamicamente in base alla configurazione attuale del server OpenVPN e contiene già tutte le informazioni necessarie, inclusi i dettagli di configurazione (indirizzi del server, porta, ecc.) e i certificati richiesti. Nel caso in cui venga modificata la modalità operativa del server (ad esempio, se viene cambiata la modalità di autenticazione), è necessario scaricare nuovamente il file.

Altre azioni disponibili sono:

- `Disabilita`: disabilita l'account; l'account può essere riabilitato in qualsiasi momento.

Nota: Se un client è già connesso al server roadwarrior, l'azione `Disabilita` sull'account corrispondente provoca una disconnessione immediata dal server, interrompendo la comunicazione.

- `Rigenera certificato`: ricrea il certificato personale per l'account; se il certificato attuale non è scaduto, verrà revocato e sarà necessario utilizzare quello nuovo. Dopo aver ricreato il certificato, è necessario aggiornarlo sul client scaricando nuovamente l'intera configurazione oppure solo il certificato.
- `Elimina`: elimina l'account e il relativo certificato; questa operazione è irreversibile e il certificato non è recuperabile.

37.2.1 Comportamento del client

Alcune informazioni sul comportamento dei client:

- I client connessi alla VPN Road Warrior vengono assegnati alla zona `rwopenvpn`, che è considerata intrinsecamente attendibile. Per impostazione predefinita, questa zona dispone di accesso privilegiato sia alle zone LAN che WAN all'interno dell'infrastruttura di rete.
- Backup della connessione: in caso di più WAN, i client si connetteranno utilizzando il primo IP/nome host della configurazione del server; se questo non è disponibile, verrà utilizzato il secondo IP/nome host e così via.
- Per motivi di sicurezza, non è possibile connettere più client con lo stesso account. Ogni account può essere utilizzato da un solo client alla volta. Se un nuovo client tenta di connettersi con un account già connesso al sistema, il primo account verrà disconnesso.

37.2.2 Client software

Tutte le principali piattaforme sono supportate. Ecco alcuni riferimenti per scaricare il software necessario:

- Sistemi Windows: OpenVPN WebSite
- Sistemi MacOS: TunnelBlick oppure il Client Ufficiale
- Sistemi Linux: di solito già disponibile nella maggior parte delle sezioni software delle distribuzioni, i sorgenti sono disponibili su OpenVPN WebSite
- Sistemi Android: OpenVPN Connect su Play Store
- Sistemi iOS: OpenVPN Connect su App Store

37.3 Gestione della scadenza dei certificati

Un'istanza OpenVPN Road Warrior utilizza certificati TLS per l'autenticazione. Per evitare problemi di connettività, è fondamentale monitorare le date di scadenza dei certificati utilizzati in tutta l'infrastruttura.

Quando viene creato un nuovo server OpenVPN Road Warrior, il sistema genera una nuova `PKI (Public Key Infrastructure)`, che è composta da:

- un certificato **CA** (**Certificate Authority**)
- un certificato **server**

I certificati client vengono generati per ogni utente nel database selezionato durante la configurazione del server o quando un utente viene aggiunto successivamente.

Ciascuno di questi elementi (client, server e CA) possiede il proprio certificato con una specifica data di scadenza, e tutti devono essere validi per consentire la connessione.

È possibile verificare le date di scadenza direttamente nell'interfaccia utente. Le date della CA e del server (che appartengono all'istanza OpenVPN) sono visualizzate nella sezione dei dettagli del server, mentre quelle dei client (che appartengono agli account utente creati per quell'istanza) sono mostrate nella tabella dei client.

Accanto a ciascuna data possono essere visualizzate due icone diverse:

- un'icona a triangolo giallo con punto esclamativo, che indica che il certificato scadrà entro 30 giorni
- un'icona a cerchio rosso con punto esclamativo, che indica che il certificato è già scaduto.

Per impostazione predefinita, tutti i certificati vengono generati con una validità di 3650 giorni (10 anni).

Una connessione tra il server OpenVPN Road Warrior e i suoi client verrà interrotta quando almeno un certificato scade, quindi è importante monitorare le date di scadenza e rinnovare i certificati prima che scadano. In particolare, questi sono gli scenari possibili:

- il certificato CA è scaduto
- il certificato del server è scaduto
- il certificato client è scaduto

Di seguito sono riportati i passaggi per rinnovare i certificati in ciascuno scenario e ripristinare la connessione.

37.3.1 Certificato client scaduto

In questo scenario, il certificato client deve essere rigenerato utilizzando l'opzione *Rigenera certificato* sul lato server (come menzionato sopra). Successivamente, la nuova configurazione/certificato client deve essere scaricata e importata sul lato client.

37.3.2 Certificato del server scaduto

In questo scenario, il certificato del server deve essere rinnovato lato server.

Il certificato server può essere rinnovato utilizzando l'opzione dedicata *Rinnova certificato server*, disponibile nel menu a destra della sezione dei dettagli del server.

Questa operazione revocherà il certificato server esistente, ne creerà uno nuovo senza influire sul certificato CA e quindi riavvierà il servizio *openvpn* per applicare le modifiche. In questo scenario, se i certificati client sono ancora validi, è possibile continuare a utilizzare la configurazione client esistente.

Avvertimento: Quando si rigenera il certificato del server, i certificati dei client rimangono validi (se non scaduti). Se il rinnovo del certificato viene effettuato mentre i client sono connessi, è necessario che il client si disconnetta e poi si riconnetta al server per ripristinare la connessione. Se il rinnovo del certificato viene effettuato mentre **i client sono disconnessi (modalità consigliata)**, la connessione verrà ripristinata automaticamente quando tenteranno nuovamente di connettersi.

37.3.3 Certificato CA scaduto

In questo scenario, la rigenerazione del certificato non è possibile perché il certificato CA è quello che firma sia i certificati del server che quelli del client. Pertanto, è necessario generare una nuova PKI completa.

Per generare una nuova PKI, l'opzione *Rigenera tutti i certificati* è disponibile nel menu a destra della sezione dei dettagli del server. È quindi necessario digitare il nome del server per confermare l'operazione.

Questa operazione genererà un nuovo certificato CA, oltre a nuovi certificati server e client firmati dalla nuova CA. In questo scenario, è **obbligatorio** scaricare e importare la nuova configurazione client sul lato client per ripristinare la connessione, quindi assicurarsi di eseguire questa operazione il prima possibile per ridurre al minimo i tempi di inattività.

Avvertimento: Quando il certificato CA è scaduto, l'unico modo per ripristinare la connessione è generare una nuova PKI e importare la nuova configurazione client sul lato client. Se i certificati client e server sono ancora validi (ad esempio, è stato rigenerato il certificato client utilizzando l'opzione *Rigenera certificato* e rinnovato il certificato server utilizzando l'opzione *Rinnova certificato server* sopra), ma il certificato CA è scaduto, la connessione non verrà ripristinata finché non verrà generato un nuovo certificato CA e importata la nuova configurazione client sul lato client. Pertanto, se il client non riesce più a connettersi al server a causa della scadenza di un certificato, assicurarsi di verificare quale certificato è scaduto e seguire la procedura corretta per ripristinare la connessione.

37.4 Problema MTU e Frammentazione dei Pacchetti

Per impostazione predefinita, le istanze server OpenVPN Road Warrior create su NethSecurity vengono inizializzate con i seguenti valori:

- Unità Massima di Trasmissione - `tun_mtu` = `1500`
- Dimensione massima del segmento - `mssfix` = `1450`.

Questi sono i valori predefiniti di OpenVPN, generalmente adatti alla maggior parte degli ambienti di rete, che dovrebbero essere modificati solo in caso di problemi di connettività dovuti alla frammentazione dei pacchetti.

Gli utenti VPN possono riscontrare problemi di connettività a causa della frammentazione dei pacchetti. L'interfaccia LAN ha un MTU di 1500 per impostazione predefinita, ma quando i pacchetti vengono criptati per la trasmissione tramite VPN, la dimensione aumenta, causando la perdita di pacchetti. Per risolvere questo problema, è necessario abbassare l'MTU e l'MSS sul server OpenVPN RW. Non sono richieste modifiche lato client.

I valori di MTU e MSS possono essere regolati direttamente tramite l'interfaccia utente, sia durante la creazione iniziale del server OpenVPN RW sia successivamente modificandolo tramite il pulsante `Modifica`, nella sezione `Opzioni avanzate` del drawer. In alternativa, è possibile regolare i due valori di configurazione utilizzando l'interfaccia a riga di comando sul firewall:

```
uci set openvpn.ns_<name>.tun_mtu='1300'
uci set openvpn.ns_<name>.mssfix='1250'
```

(continues on next page)

(continua dalla pagina precedente)

```
uci commit openvpn.ns_<name>
/etc/init.d/openvpn restart ns_<name>
```

I valori di *tun_mtu* e *mssfix* potrebbero dover essere regolati in base al proprio ambiente di rete specifico. Un MTU più basso garantisce che i pacchetti rientrino nei limiti del tunnel OpenVPN senza frammentazione. A seconda di fattori come la latenza di rete o l'overhead, si potrebbe riscontrare che valori leggermente diversi funzionano meglio per la propria configurazione.

Per informazioni più specifiche, consultare la documentazione ufficiale di OpenVPN.

37.5 Cronologia delle connessioni

Ogni volta che un client si connette o si disconnette dal server, l'evento viene salvato all'interno di un database SQLite. La cronologia di tali eventi può essere visualizzata facendo clic sulla scheda `Connection History` disponibile nella parte superiore della pagina.

Per impostazione predefinita, la pagina visualizzerà tutte le connessioni del giorno corrente, ma è possibile filtrare i risultati per data e ora e per nome account.

Per scaricare tutta la cronologia in formato CSV, fare clic sul pulsante *Scarica la cronologia del server*. L'intestazione del file CSV spiega il significato di ciascuna colonna, incluse le unità di misura.

La cronologia viene letta da un database SQLite che può essere memorizzato in:

- **RAM**: memorizzato in RAM (non persistente); andrà perso al riavvio del firewall.
- **Archiviazione**: archiviato su storage persistente; sopravviverà a un riavvio.

Per impostazione predefinita, se uno storage persistente è disponibile e configurato, gli eventi di connessione vengono memorizzati nel database di storage, altrimenti vengono memorizzati nel database RAM.

Se un server RoadWarrior è già configurato e viene collegato un nuovo dispositivo di storage, la cronologia viene automaticamente spostata dalla RAM allo storage, diventando persistente e in grado di sopravvivere ai riavvii. Al contrario, se lo storage viene rimosso, i nuovi eventi di connessione saranno memorizzati nel database RAM e saranno visibili nella sezione *Connections History*. Se successivamente lo storage viene ricollegato, le cronologie presenti in RAM e nello storage vengono unite senza perdita di dati.

Se il server è connesso a un *Controller*, la cronologia viene inviata al controller e può essere visualizzata all'interno della sezione *Storico monitoraggio*.

CAPITOLO 38

Tunnel OpenVPN

I tunnel net-to-net di OpenVPN stabiliscono connessioni sicure tra due reti separate, come ad esempio le filiali di un'azienda, tramite internet. Queste connessioni utilizzano i protocolli SSL/TLS per la cifratura e l'autenticazione, garantendo la riservatezza e l'integrità dei dati.

La connessione è gestita da 2 firewall NethSecurity, ciascuno con un ruolo specifico. Quando si crea una connessione OpenVPN net2net, un firewall avrà il ruolo di server mentre l'altro NethSecurity si collegherà come client. Un NethSecurity può essere contemporaneamente server e client per tunnel differenti; tutti i tunnel utilizzano la modalità routed di OpenVPN.

L'interfaccia dei tunnel OpenVPN è stata progettata per una connessione semplice tra due dispositivi NethSecurity. Per questo motivo, è volutamente limitata e non espone tutti i parametri che possono essere configurati con OpenVPN per collegarsi a un dispositivo di terze parti. Per connettersi a un dispositivo di terze parti, si consiglia di utilizzare il protocollo IPsec.

38.1 Configurazione

Per collegare due firewall tramite un tunnel OpenVPN, è necessario prima configurare il firewall server e successivamente quello client. Il server deve disporre di almeno un indirizzo IP pubblico per essere raggiungibile dal client, mentre il client può anche non avere indirizzi IP pubblici. La configurazione del firewall server richiede solo pochissimi parametri; ove possibile, tutti i parametri sono già compilati automaticamente per evitare errori e velocizzare il processo. Una volta configurato il firewall server, sarà possibile scaricare la configurazione client da importare sull'altro firewall.

38.1.1 Procedere come segue:

Accedere alla pagina dei tunnel OpenVPN, spostarsi sulla scheda `Tunnel server` e fare clic su *Aggiungi tunnel server*.

Inserire tutti i campi obbligatori, ma si noti:

- `Endpoint pubblici` è un elenco di indirizzi IP o nomi host che i client possono utilizzare per raggiungere il server tunnel OpenVPN
- `Reti locali` è un elenco di reti locali che saranno accessibili dal server remoto. Se la topologia è impostata su p2p, lo stesso elenco verrà riportato nel campo `Reti remote` del client.
- `Reti remote`, è un elenco di reti dietro il server remoto che saranno accessibili dagli host nella rete locale
- Dopo che la configurazione è stata salvata, fare clic sull'azione *Scarica* e selezionare `Client configuration`
- Accedere al firewall client, al tunnel OpenVPN, spostarsi nella scheda `Tunnel client`, fare clic su *Importa configurazione*

38.2 Topologia

I tunnel possono avere due tipi di topologie: `subnet` e `p2p` (Point to Point).

38.2.1 Subnet

`Subnet` è la topologia predefinita e quella consigliata: nella topologia `subnet`, il server accetterà le connessioni e agirà come server DHCP per ogni client connesso.

In questo scenario il server autenticherà i client utilizzando certificati TLS e invierà le route locali al client remoto.

38.2.2 P2P

In una topologia `p2p`, l'amministratore deve configurare un server per ciascun client; in questo scenario, l'unico metodo di autenticazione supportato è il PSK (Pre-Shared Key).

- assicurarsi di scambiare il PSK utilizzando un canale sicuro (come SSH o HTTPS)
- l'amministratore deve selezionare un IP per entrambi gli endpoint
- le route verso le reti remote devono essere configurate su ciascun endpoint

38.3 Funzionalità avanzate

L'interfaccia web consente la configurazione di funzionalità avanzate come:

- `Host remoto multipli`: è possibile specificare più indirizzi di server remoti per la ridondanza; il client OpenVPN tenterà di connettersi a ciascun host nell'ordine indicato
- `Protocollo`: OpenVPN è progettato per funzionare in modo ottimale su UDP, ma la compatibilità con TCP è prevista per situazioni in cui UDP non può essere utilizzato.
- `Compressione`: se abilitata, i dati inviati attraverso il tunnel VPN verranno compressi. Questa opzione è disabilitata per impostazione predefinita anche per motivi di sicurezza. La compressione è raramente essenziale al giorno d'oggi, poiché il traffico internet è generalmente già altamente compresso e ottimizzato.

- `Digest`: l'algoritmo di digest utilizzato per trasformare un blocco di dati di dimensione arbitraria in un output di dimensione fissa. Se non viene selezionato esplicitamente, il server e il client tenteranno di negoziare il miglior digest disponibile su entrambi i lati.
- `Cipher`: l'algoritmo crittografico utilizzato per cifrare tutto il traffico. Se non viene selezionato esplicitamente, il server e il client tenteranno di negoziare il miglior cipher disponibile su entrambi i lati.
- `Imporre una versione minima di TLS`: Consente di scegliere una versione minima di TLS; in tal caso, saranno consentite solo le connessioni provenienti da dispositivi che utilizzano una versione uguale o superiore a quella selezionata.

38.4 Multiple OpenVPN tunnels

If a NethSecurity must act as the VPN server for multiple remote firewalls, create a dedicated OpenVPN tunnel for each remote peer. The UI-supported and recommended model is one server/client pair per site-to-site connection, for example, a central firewall connected to three remote firewalls should have three separate OpenVPN server tunnels, each with its own client configuration imported on the corresponding remote firewall.

This approach allows each tunnel to be managed independently, with separate configuration, certificates, routes, status, monitoring, and troubleshooting. It also prevents issues on one remote connection from affecting the operational management of the others.

Do not use a single OpenVPN server tunnel shared by multiple remote clients for site-to-site configurations managed from the UI.

38.5 Problema MTU e Frammentazione dei Pacchetti

Per impostazione predefinita, le istanze del tunnel OpenVPN create su NethSecurity vengono inizializzate con i seguenti valori:

- Unità Massima di Trasmissione - `tun_mtu` = `1500`
- Dimensione massima del segmento - `mssfix` = `1450`.

Questi sono i valori predefiniti di OpenVPN, generalmente adatti alla maggior parte degli ambienti di rete, che dovrebbero essere modificati solo in caso di problemi di connettività dovuti alla frammentazione dei pacchetti.

Gli utenti VPN possono riscontrare problemi di connettività a causa della frammentazione dei pacchetti. L'interfaccia LAN ha un MTU di 1500 per impostazione predefinita, ma quando i pacchetti vengono criptati per la trasmissione tramite VPN, la dimensione aumenta, causando la perdita di pacchetti. Per risolvere questo problema, è necessario abbassare l'MTU e l'MSS sul tunnel OpenVPN. Non sono richieste modifiche lato client.

I valori di MTU e MSS possono essere regolati direttamente nell'interfaccia utente, sia durante la creazione iniziale del tunnel sia successivamente modificandolo tramite il pulsante `Modifica`, nella sezione `Opzioni avanzate` del drawer. In alternativa, è possibile regolare i due valori di configurazione utilizzando l'interfaccia a riga di comando sul firewall:

```
uci set openvpn.ns_<name>.tun_mtu='1300'
uci set openvpn.ns_<name>.mssfix='1250'
uci commit openvpn.ns_<name>
/etc/init.d/openvpn restart ns_<name>
```

I valori di *tun_mtu* e *mssfix* potrebbero dover essere regolati in base al proprio ambiente di rete specifico. Un MTU più basso garantisce che i pacchetti rientrino nei limiti del tunnel OpenVPN senza frammentazione. A seconda di fattori

come la latenza di rete o l'overhead, potrebbe risultare che valori leggermente diversi funzionino meglio per la propria configurazione.

Per informazioni più specifiche, consultare la documentazione ufficiale di OpenVPN.

38.6 Gestione della scadenza dei certificati

Come menzionato nella sezione *Gestione della scadenza dei certificati*, i tunnel OpenVPN si basano anch'essi su certificati ed è fondamentale monitorare le loro date di scadenza per evitare problemi di connettività.

Quando viene creato un nuovo tunnel OpenVPN, il sistema genera una nuova `PKI (Public Key Infrastructure)`, composta dalla **CA**, dal **server** e da un **singolo certificato client** (a differenza delle connessioni Road Warrior, che prevedono un certificato per ogni utente).

Tutte le informazioni sulle date di scadenza dei certificati sono disponibili nella tabella **OpenVPN Tunnels**, dove per ogni tunnel viene mostrata un'icona a forma di lente d'ingrandimento. Facendo clic su di essa si apre una finestra modale con tutti i dettagli sulla configurazione del tunnel, inclusi i certificati e le rispettive date di scadenza.

Sul **lato server**, la finestra modale mostra le informazioni sui certificati per la CA, il server e i certificati client. Sul **lato client**, mostra solo i certificati CA e client.

Nella tabella dei tunnel, viene mostrata un'icona di avviso quando almeno uno di questi certificati scadrà entro 30 giorni o è già scaduto. Aprendo la finestra modale dei dettagli del tunnel, è possibile vedere quale certificato sta per scadere e la sua data di scadenza.

Per impostazione predefinita, tutti i certificati vengono generati con una validità di 3650 giorni (10 anni).

Una connessione tra i due firewall verrà interrotta quando almeno un certificato scade, secondo i tre possibili scenari descritti nella sezione OpenVPN Road Warrior.

Per verificare se il tunnel OpenVPN è disconnesso a causa della scadenza del certificato, è possibile ispezionare i **log del firewall** e cercare messaggi relativi a OpenVPN, situati nel file `/var/log/messages`.

Esempio:

```
grep 'VERIFY ERROR:' /var/log/messages
```

La ricerca restituisce messaggi come il seguente:

```
Feb  9 13:02:07 NethSec openvpn(ns_roadwarrior1)[8031]: VERIFY ERROR: depth=1,␣
↪error=certificate has expired
Feb  9 13:02:07 NethSec openvpn(ns_roadwarrior1)[8031]: VERIFY ERROR: depth=0,␣
↪error=certificate has expired
```

Queste righe indicano che la connessione non funziona a causa della scadenza del certificato. Il problema può essere relativo al certificato CA (`depth=1`), al certificato del server (`depth=0`), o a entrambi.

Per verificare la validità dei certificati, è possibile utilizzare i seguenti comandi `openssl`.

```
# client
openssl x509 -in /etc/openvpn/{vpn-instance}/pki/issued/client.crt -text -noout | grep
↪'Not After'
# server
openssl x509 -in /etc/openvpn/{vpn-instance}/pki/issued/server.crt -text -noout | grep
↪'Not After'
# CA
```

(continues on next page)

(continua dalla pagina precedente)

```
openssl x509 -in /etc/openvpn/{vpn-instance}/pki/ca.crt -noout -dates -subject -issuer -
↪serial
```

Il segnaposto `{vpn-instance}` deve essere sostituito con il nome della propria istanza OpenVPN (ad esempio `ns_roadwarrior1`).

Di seguito sono riportati i passaggi per rinnovare i certificati in ciascuno scenario e ripristinare la connessione.

38.6.1 Certificato client scaduto

In questo scenario, il certificato client deve essere rinnovato lato server e poi scaricato e importato nuovamente lato client.

1. Accedere al firewall del server e navigare alla sezione **Tunnel OpenVPN**.
2. Fare clic sul menu a destra del tunnel e selezionare *Rigenera certificati*.
3. Scaricare il nuovo certificato client e importarlo sul lato client.

Queste operazioni creeranno nuovi certificati server e client senza influire sul certificato CA (che si presume sia ancora valido in questo caso). In questo scenario, l'utilizzo del nuovo certificato client sul firewall client è **obbligatorio** per ripristinare la connessione, quindi è necessario scaricarlo e importarlo sul lato client il prima possibile per ridurre al minimo i tempi di inattività.

38.6.2 Certificato del server scaduto

In questo scenario, il certificato del server deve essere rinnovato lato server. Utilizzare la stessa azione *Rigenera certificati* descritta nello scenario precedente. È possibile continuare a utilizzare il certificato client esistente (se ancora valido) e scaricare/importare quello appena generato in un secondo momento. Il nuovo certificato client scadrà lo stesso giorno del nuovo certificato server.

Per quanto riguarda il rinnovo del certificato server Road Warrior, la considerazione sul comportamento del client è la stessa: se il rinnovo del certificato viene effettuato mentre i client sono connessi, è necessario che il client si disconnetta e poi si riconnetta al server per ripristinare la connessione, mentre se il rinnovo del certificato viene effettuato mentre **i client sono disconnessi (modalità consigliata)**, la connessione verrà automaticamente ripristinata quando tenteranno nuovamente di connettersi.

38.6.3 Certificato CA scaduto

In questo scenario, è necessario procedere con la generazione di una nuova PKI completa.

1. Accedere al terminale del firewall del server.
2. Eseguire i seguenti comandi:

```
ns-openvpn-renew-ca {vpn-instance}
service openvpn restart
```

Questi comandi genereranno un nuovo certificato CA, oltre a nuovi certificati server e client firmati dalla nuova CA. In questo scenario, è **obbligatorio** scaricare e importare la nuova configurazione client sul lato client per ripristinare la connessione, quindi assicurarsi di eseguire questa operazione il prima possibile per ridurre al minimo i tempi di inattività.

Tutte le considerazioni rimangono le stesse delle connessioni Road Warrior. Se il certificato scaduto è il certificato CA, è necessario generare una nuova PKI completa, mentre se il certificato scaduto è quello del server o del client, è possibile rigenerarlo utilizzando l'azione dedicata.

CAPITOLO 39

Tunnel IPsec

I tunnel IPsec sono una componente cruciale della sicurezza delle reti moderne. Questi tunnel forniscono un percorso di comunicazione sicuro e cifrato attraverso Internet o qualsiasi rete non affidabile, garantendo la riservatezza e l'integrità dei dati in transito.

Il protocollo IPsec (IP Security) è lo standard 'de facto' nei tunnel VPN, viene tipicamente utilizzato per creare tunnel net-to-net ed è supportato da tutti i produttori. Questo protocollo può essere utilizzato per creare tunnel VPN tra un NethSecurity e un dispositivo di un altro produttore, così come tunnel VPN tra due NethSecurity.

NethSecurity per impostazione predefinita utilizza VPN basate su routing (Route-Based VPN), quindi ogni tunnel utilizza un proprio device tun specifico.

39.1 Configurazione

La configurazione di un tunnel IPsec include 2 peer che chiameremo A e B, i quali possono essere:

- 1 Nethsecurity e 1 firewall di terze parti
- 2 Nethsecurity

I dispositivi A e B devono essere configurati con parametri che, a seconda della sezione specifica, saranno identici o speculari.

I parametri che devono essere configurati in modo speculare tra i 2 dispositivi sono tipicamente quelli legati alla rete:

- l'interfaccia WAN utilizzata dal tunnel
- le 2 (o più) reti che si desidera connettere (rete locale, rete remota)
- gli identificatori locali e remoti (tipicamente gli IP pubblici delle WAN dei 2 firewall, ma possono essere utilizzati anche altri)

Pertanto:

- L'indirizzo IP WAN del firewall A deve coincidere con l'indirizzo IP remoto del firewall B
- la rete locale del firewall A deve coincidere con la rete remota del firewall B

- l'ID locale del firewall A deve coincidere con l'ID remoto del firewall B

Tutti gli altri parametri, tuttavia, devono essere identici su entrambi i firewall per consentire una comunicazione corretta (chiave di cifratura, configurazione IKE ed ESP, ecc.). NethSecurity utilizza una chiave condivisa come unico metodo per cifrare i dati.

39.1.1 Come creare un nuovo tunnel IPsec

Fare clic sul pulsante *Aggiungi tunnel IPsec* per configurare un nuovo tunnel. Assegnare un nome a questo tunnel e poi configurarlo; la configurazione è suddivisa in 3 passaggi. Il primo passaggio contiene solo i parametri relativi alla rete, mentre gli altri contengono tutti i restanti parametri che devono essere identici su entrambi i firewall per consentire una comunicazione corretta.

Una volta completata la configurazione, un nuovo tunnel verrà visualizzato nella pagina IPSec.

Nota: Se un endpoint si trova dietro NAT, si consiglia di impostare i valori dei campi Identificatore locale e Identificatore remoto su nomi univoci personalizzati con una sintassi simile a quella di un indirizzo email, ad esempio nsec@site-a e otherdevice@site-b.

Gestione di più reti

Un singolo tunnel IPsec può gestire più reti locali e remote. In questo caso, NethSecurity crea sempre più child SA per garantire un'ampia compatibilità con i dispositivi remoti. Il comportamento rimane invariato sia per IKEv1 che per IKEv2.

Facendo clic sull'icona della lente di ingrandimento nell'elenco dei tunnel IPsec, è possibile visualizzare i dettagli del tunnel, inclusi lo stato dei child SA e le reti associate a ciascun SA. Dopo aver aggiunto o rimosso una rete, se i child tunnel non si aggiornano automaticamente, potrebbe essere necessario riavviare il servizio. Per riavviare il servizio, fare clic sul pulsante `Riavvia` nell'angolo in alto a destra della pagina dei tunnel IPsec.

39.2 Tunnel IPsec in uno scenario MultiWAN

In uno scenario multi-WAN, è fondamentale garantire che ciascun endpoint remoto del tunnel venga raggiunto attraverso la stessa interfaccia WAN configurata per il tunnel IPsec.

Per imporre questo comportamento, è necessario creare una rotta statica affinché il traffico verso l'IP remoto venga instradato attraverso il gateway dell'interfaccia WAN specifica assegnata al tunnel.

Ad esempio, se il tunnel è su WAN1 e l'endpoint remoto è `11.22.33.44`, la rotta statica specificherà che il traffico verso `11.22.33.44` utilizza il gateway WAN1.

CAPITOLO 40

WireGuard VPN

WireGuard è una tecnologia VPN (Virtual Private Network) moderna che utilizza crittografia all'avanguardia. È progettata per essere più veloce, semplice e funzionale rispetto a IPsec e OpenVPN. WireGuard è una soluzione VPN sicura, veloce e facile da configurare che utilizza crittografia di ultima generazione. È progettata per essere più semplice da configurare rispetto a OpenVPN e per offrire una superficie di attacco ridotta.

NethSecurity fornisce un server e un client WireGuard che possono essere configurati dall'interfaccia web.

Funzionalità:

- È possibile eseguire simultaneamente più istanze del server WireGuard
- Ogni istanza opera nella propria zona di rete isolata
- Assegnazione di indirizzo IP statico per ogni peer (account client)
- Configurazione client disponibile come file di testo o codice QR
- Connessioni site-to-site (net2net) supportate
- Sicurezza avanzata con chiavi pre-condivise opzionali
- Funzionalità di importazione dei file di configurazione standard WireGuard

40.1 Configurazione del server

È possibile creare più istanze del server WireGuard, ciascuna con la propria zona di rete isolata. NethSecurity aprirà automaticamente le porte firewall necessarie per consentire le connessioni in ingresso al server WireGuard e creerà una zona VPN per permettere la gestione di come il traffico viene instradato tra le zone.

Al contrario del server OpenVPN, non ci sono legami con il database utenti; gli account (peer) vengono creati e gestiti direttamente all'interno dell'interfaccia WireGuard.

Per creare un server WireGuard, fare clic su *Aggiungi server*, quindi compilare il modulo con la configurazione desiderata. I campi sono i seguenti:

- *Stato*: abilitare o disabilitare l'istanza del server WireGuard

- *Nome*: il nome dell'istanza del server WireGuard; questo non è il nome dell'interfaccia di rete, che verrà creata automaticamente come *wgX*, dove *X* è un numero
- *Rete VPN*: il CIDR di rete che verrà utilizzato dal server WireGuard; il server otterrà automaticamente il primo IP della rete. Assicurarsi che questa rete non si sovrapponga a nessuna rete esistente.
- *Porta UDP*: la porta su cui il server WireGuard ascolta le connessioni in ingresso
- *Public endpoint*: l'indirizzo IP pubblico o FQDN del server

Nelle impostazioni avanzate, è possibile configurare opzioni aggiuntive:

- *MTU*: per impostare manualmente l'MTU dell'interfaccia WireGuard
- *Server DNS*: per impostare server DNS personalizzati che verranno inviati ai client, utile per evitare perdite DNS

Dopo aver creato il server, è possibile aggiungere nuovi client (peer) direttamente dall'interfaccia di WireGuard, facendo clic su *Aggiungi peer* e compilando il modulo come segue:

- *Stato*: abilitare o disabilitare il peer
- *Name*: il nome del peer
- *Reserved IP*: l'indirizzo IP statico che verrà assegnato al peer; deve essere all'interno della rete VPN e verrà precompilato con il prossimo IP disponibile
- *Chiave pre-condivisa*: se abilitato, una chiave pre-condivisa verrà creata automaticamente per aumentare la sicurezza
- *Instrada tutto il traffico*: se abilitato, quando il client si connette, invierà tutto il traffico al server
- *Reti del server*: a quali reti il peer può accedere; tutte le reti LAN saranno aggiunte automaticamente
- *Peer networks*: reti raggiungibili dal lato peer. Compilare sempre questo campo quando si desidera creare un tunnel net2net.

Nota: È possibile creare una connessione client-to-site (Road Warrior) lasciando vuoti i campi *Peer networks*. In questo modo il client potrà accedere alle reti del server.

Una volta che il peer è stato salvato, è possibile scaricare il file di configurazione in formato testo oppure come codice QR utilizzando il menu sul lato destro della voce del peer.

La configurazione del server e dei peer può essere modificata tramite il menu contestuale situato sul lato destro di ciascuna voce.

Avvertimento: Dopo aver modificato il server WireGuard o i peer, ricordare che tali modifiche devono essere applicate al peer riscaricando il file di configurazione.

40.2 Configurazione del tunnel

Nethsecurity può essere configurato come client (peer) WireGuard per connettersi a un altro server WireGuard. Nella scheda *Peer tunnels*, è possibile aggiungere manualmente un nuovo tunnel facendo clic su *Aggiungi tunnel peer* oppure importare un file di configurazione WireGuard generico utilizzando *Importa tunnel peer*.

Quando si aggiunge manualmente un nuovo tunnel, sono disponibili i seguenti campi:

- *Status*: abilita o disabilita il tunnel

- *Nome*: il nome del tunnel; questo non è il nome dell'interfaccia di rete, che verrà creata automaticamente come *wgX*, dove *X* è un numero
- *Reserved IP*: l'indirizzo IP statico che verrà utilizzato dal tunnel
- *Server public key*: la chiave pubblica del server WireGuard
- *Peer private key*: la chiave privata del tunnel
- *Pre-shared key*: la chiave pre-condivisa, se utilizzata; il campo è facoltativo
- *Instrada tutto il traffico*: se abilitato, tutto il traffico verrà instradato attraverso il tunnel
- *Route di rete*: reti rese disponibili tramite il tunnel
- *Endpoint*: l'indirizzo IP pubblico o FQDN del server WireGuard
- *Porta UDP*: la porta su cui il tunnel WireGuard si connetterà
- *Server DNS*: server DNS personalizzati da utilizzare quando il tunnel è attivo

40.3 Debug

Per impostazione predefinita, WireGuard non registra alcun log. Per abilitare la registrazione su */var/log/messages*, utilizzare i seguenti comandi:

```
echo module wireguard +p > /sys/kernel/debug/dynamic_debug/control
```

Per disabilitare la registrazione, utilizzare:

```
echo module wireguard -p > /sys/kernel/debug/dynamic_debug/control
```

CAPITOLO 41

Panoramica, Funzionalità, Limitazioni

L'Alta Disponibilità (HA) di NethSecurity garantisce la continuità operativa della rete fornendo ridondanza tramite un cluster di due firewall. Se il firewall primario si guasta a causa di problemi hardware, problemi software o manutenzione, un firewall di backup assume automaticamente la gestione di tutti i servizi di rete e del traffico, riducendo al minimo i tempi di inattività.

Questo è fondamentale per aziende o organizzazioni in cui l'accesso a Internet senza interruzioni, la connettività VPN e i servizi di sicurezza sono essenziali per le operazioni quotidiane, prevenendo la perdita di produttività o di ricavi durante un'interruzione.

41.1 Concetti chiave

Alcuni concetti chiave da comprendere prima di configurare HA:

- **Nodo Primario**: Il firewall che gestisce attivamente il traffico e i servizi.
- **Nodo secondario (o di backup)**: Il firewall che subentra automaticamente in caso di guasto del nodo primario.
- **Virtual IP (VIP)**: Un indirizzo IP condiviso utilizzato da entrambi i nodi per ciascuna interfaccia configurata, al fine di garantire un accesso ininterrotto ai servizi da parte dei client. I client sulla rete dovrebbero *sempre* utilizzare l'indirizzo VIP (ad esempio, come gateway, server DNS o endpoint VPN) per garantire un failover senza interruzioni.

41.1.1 Ruoli HA

- **Principale**
  - Il nodo che attualmente ha tutte le interfacce attive ed elabora tutto il traffico di rete
  - In condizioni normali, il Nodo Primario opera in questo stato.
- **Backup**
  - Il nodo che non elabora il traffico di rete.

  - In condizioni normali, il Nodo Secondario opera in questo stato.

Le modifiche alla configurazione devono essere **sempre** effettuate sul **nodo primario**. Il nodo secondario deve essere considerato in sola lettura. L'unica eccezione riguarda la configurazione di rete delle interfacce LAN che fanno parte del cluster HA.

Tutte le altre configurazioni rilevanti, come le regole del firewall, le impostazioni VPN o le regole di Threat Shield, vengono sincronizzate automaticamente dal nodo primario al nodo secondario.

Ecco come funziona il sistema HA:

- **Heartbeat**: I firewall primario e secondario controllano continuamente lo stato l'uno dell'altro utilizzando il protocollo VRRP. Se il primario si guasta, il secondario subentra. Il protocollo VRRP viene trasportato tramite un'interfaccia LAN dedicata chiamata **interfaccia HA**; ulteriori informazioni saranno fornite in una sezione successiva.
- **Sincronizzazione delle impostazioni**: Il firewall primario invia in modo sicuro le proprie impostazioni, inclusi i dettagli sulle connessioni attive come VPN e route di rete, al firewall secondario.
- Il sistema regola automaticamente il comportamento di ciascun firewall in base al fatto che sia l'unità attiva (primaria) o di standby (secondaria):
  - **Il secondario riceve aggiornamenti di configurazione**: Quando il firewall secondario riceve nuove impostazioni, le salva ma mantiene i servizi correlati (come le VPN) disattivati. Il firewall secondario conserva una copia completa della configurazione del primario, ma mantiene inattivi la maggior parte dei processi in background. Questo include attività come la verifica degli aggiornamenti software, l'esecuzione di backup remoti o l'invio di report. In questo modo, solo il firewall primario attivo gestisce queste attività, prevenendo conflitti.
  - **Il firewall diventa attivo**: Quando un firewall assume il ruolo di primario (sia durante un avvio normale che durante un failover), attiva tutti i servizi e le connessioni necessari.
  - **Il firewall diventa standby**: Quando un firewall è in modalità di backup (sia all'avvio che quando il primario torna online), disattiva la maggior parte dei servizi e delle connessioni.

Sebbene il sistema HA sia progettato per essere il più automatico possibile, alcune configurazioni richiedono un intervento manuale. Ad esempio, se si aggiunge una nuova interfaccia di rete LAN o si modifica una esistente, è necessario informare il sistema HA di queste modifiche.

41.2 Funzionalità supportate e limitazioni

Il cluster HA supporta la sincronizzazione per un'ampia gamma di funzionalità, tra cui:

- Regole del firewall, port forwarding, DHCP, DNS
- Configurazioni VPN (OpenVPN, IPsec, WireGuard)
- QoS, Multi-WAN, regole DPI
- Reverse proxy, certificati ACME e altro.
- Route statiche
- Configurazione informatica di Netifyd
- Protezione dalle minacce IP (banip)
- Threat shield DNS (adblock)
- Database di utenti e oggetti
- Netmap

- Flashstart
- Server SNMP (snmpd)
- Helper NAT
- DNS dinamico (ddns)
- Client SMTP (msmtp)
- Password di cifratura del backup
- Connessione e sottoscrizione del controller (ns-plug)
- Monitoraggio delle connessioni attive (conntrackd)
- Hotspot (dedalo) solo su interfacce fisiche

41.2.1 Tipi e configurazioni di interfacce WAN

- Indirizzi IPv4 statici e indirizzi IPv6 statici
- IPv4 tramite DHCP
- Interfacce Ethernet fisiche
- Interfacce bond (aggregazione di link) composte da interfacce fisiche
- Interfacce bridge su interfacce fisiche
- VLAN su interfacce fisiche, interfacce bond o interfacce bridge
- PPPoE su interfacce fisiche o su interfacce VLAN

41.2.2 Limitazioni delle interfacce

- Solo IPv4 è supportato sulle interfacce LAN
- L'interfaccia HA deve essere un'interfaccia fisica
- I bond e i bridge sono supportati solo per interfacce LAN aggiuntive e WAN, non per l'interfaccia HA
- L'Hotspot è supportato solo su interfacce fisiche
- Se è stata effettuata una migrazione da NethServer 7, i dispositivi bond con nomi lunghi (come `bond-bond0`) non sono compatibili con HA. Consultare la sezione *correzione dei nomi dei bond* per le istruzioni su come rinominarli.

41.2.3 Limitazioni generali

- I pacchetti aggiuntivi non inclusi nell'immagine non sono supportati (ad es. NUT, etherwake, ecc.)
- La configurazione del demone Syslog (rsyslog) non è sincronizzata: se è necessario inviare i log a un server remoto, occorre utilizzare il controller.
- Dopo la prima sincronizzazione, il nodo secondario avrà lo stesso hostname del nodo primario. L'interfaccia utente web mostrerà l'hostname del nodo primario, ma la dashboard indicherà il ruolo del nodo (primario o secondario). Inoltre, quando si accede alla console SSH, il prompt cambierà per indicare il ruolo del nodo. Consultare la sezione *Risoluzione dei problemi* per ulteriori dettagli.

41.2.4 Sincronizzazione e conservazione dei log

HA sincronizza la configurazione, le sessioni attive e lo stato di runtime tra i nodi del cluster per garantire la continuità del servizio durante il failover. I log e i dati di reportistica, come i log di sistema o i database della cronologia di OpenVPN Road Warrior, **non** vengono sincronizzati tra i nodi HA. Per la conservazione centralizzata e la reportistica unificata, utilizzare il controller.

CAPITOLO 42

Configurazione e gestione

42.1 Requisiti

Prima di configurare HA, assicurarsi che siano soddisfatti i seguenti requisiti:

- Due firewall con dispositivi di rete identici. Ogni dispositivo deve avere esattamente lo stesso nome e la stessa numerazione (ad esempio, eth0, eth1, eth2, eth3)
- Entrambi i nodi devono essere collegati alla stessa LAN; collegare le interfacce LAN allo stesso dominio di broadcast (di solito allo stesso switch).
- Indirizzi IP statici per tutte le interfacce LAN che ospiteranno un IP virtuale.

42.2 Configurazione e impostazione

Il processo di configurazione HA prevede diversi passaggi. Se si desidera solo visualizzare i comandi, è possibile passare direttamente alla sezione *Configuration example*, ma si consiglia di leggere l'intera sezione per comprendere il processo e i requisiti.

Il processo di configurazione è il seguente:

1. **Installare la stessa versione di NethSecurity** su due macchine identiche (fisiche o virtuali). Consultare *Installazione* per istruzioni dettagliate sull'installazione.
2. **Collegare correttamente i cavi di rete** per garantire la ridondanza. Consultare la sezione *Network cabling* di seguito per le linee guida corrette sul cablaggio.
3. **Configurare l'interfaccia HA** su entrambi i nodi con indirizzi IP statici. Creare una LAN sul nodo primario e su quello secondario che sarà necessaria per il cluster prima di procedere con la configurazione di HA. Consultare la sezione *HA interface* qui sotto per istruzioni dettagliate.
4. **Inizializzare il cluster** utilizzando i comandi *ns-ha-config* per stabilire la base del cluster HA. Il processo di inizializzazione configura i servizi necessari e prepara entrambi i nodi per la sincronizzazione. Durante la prima configurazione, tutte le interfacce di rete che verranno utilizzate nel cluster HA devono avere il cavo collegato

su entrambi i nodi, altrimenti il nodo potrebbe entrare in stato di errore e il cluster HA potrebbe non funzionare correttamente. Consultare la sezione *Cluster initialization* qui sotto per istruzioni dettagliate.

5. **Configurare l'interfaccia WAN nel nodo primario** utilizzando la pagina `Interfacce e dispositivi` nell'interfaccia web. Le interfacce WAN verranno configurate automaticamente all'interno del cluster e sincronizzate con il nodo secondario. Consultare la sezione *WAN Interfaces* di seguito per ulteriori informazioni.
6. **Verificare la configurazione** per assicurarsi che tutto sia impostato correttamente. Utilizzare i comandi *ns-ha-config* per controllare lo stato e la configurazione del cluster HA. Consultare la sezione *Verificare la configurazione* di seguito per istruzioni dettagliate.
7. **Configurare interfacce LAN aggiuntive (opzionale)** per il cluster. Questo passaggio è opzionale e dipende dalla configurazione della rete. È possibile aggiungere qualsiasi interfaccia LAN aggiuntiva che richieda il supporto HA. Consultare la sezione *Interfacce LAN aggiuntive* di seguito per istruzioni dettagliate. Se è necessario configurare un hotspot, consultare la sezione *Supporto hotspot* di seguito per i requisiti specifici.
8. **Aggiungere IP virtuali extra (opzionale)** al nodo primario sulle interfacce LAN rilevanti. Questo passaggio è opzionale e consente di aggiungere indirizzi IP aggiuntivi al nodo primario per i servizi che richiedono più IP. Consultare la sezione *IP virtuali extra* di seguito per istruzioni dettagliate.

I passaggi dettagliati per ciascuno di questi punti sono trattati nelle sezioni seguenti.

A volte può essere necessario rimuovere interfacce o alias dalla configurazione HA. Questo può essere fatto utilizzando il comando `ns-ha-config`. Consultare la sezione *Remove interfaces and virtual IPs* di seguito per istruzioni dettagliate.

42.2.1 Cablaggio di rete

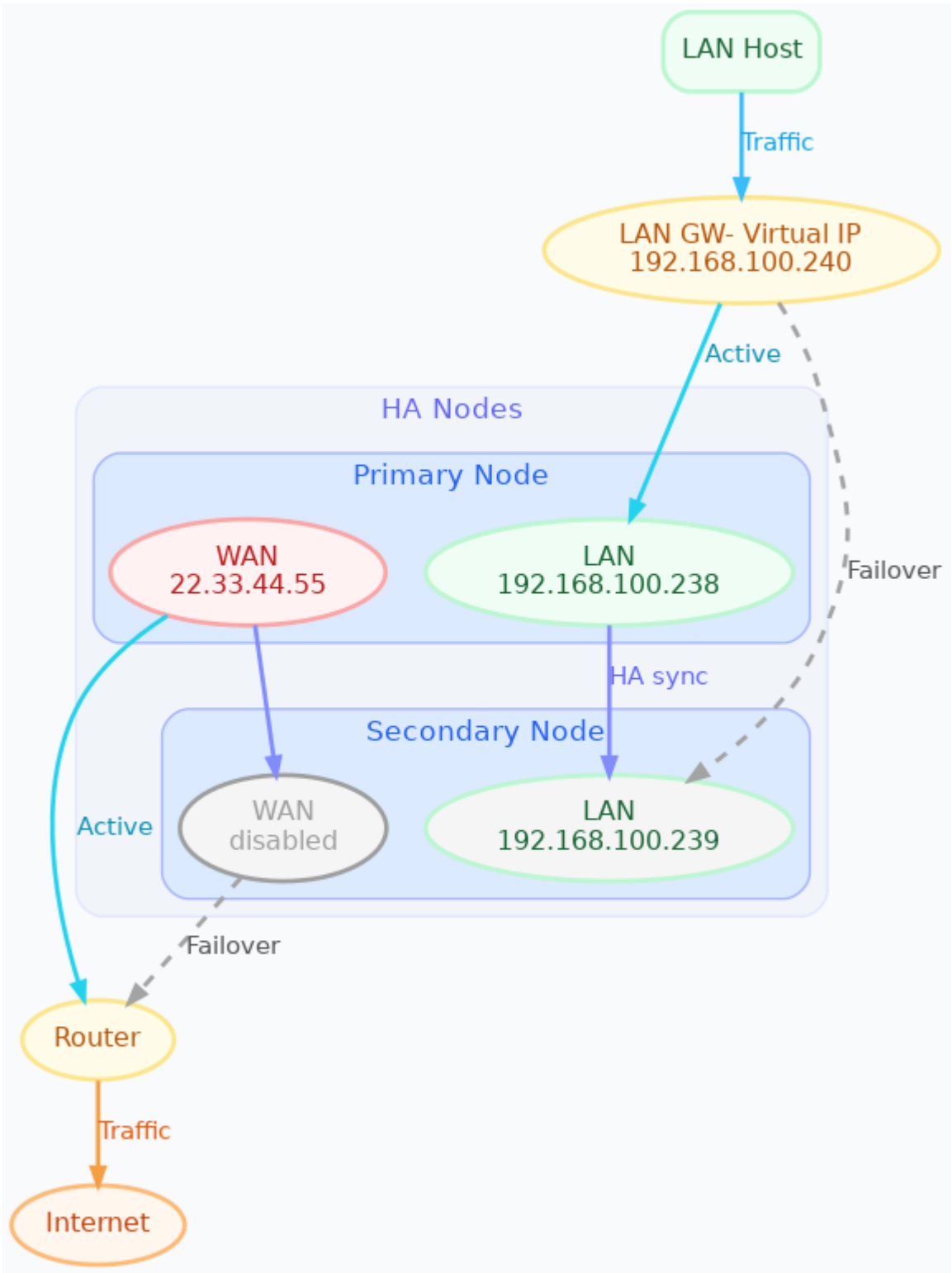
Un cablaggio di rete adeguato è essenziale per garantire un'elevata disponibilità e un failover senza interruzioni tra il firewall primario e quello secondario.

1. **Raccomandazioni generali**:
   - Per ogni zona di rete (LAN, WAN, DMZ, ecc.), utilizzare uno switch dedicato o una VLAN per collegare le interfacce di entrambi i firewall.
   - Evitare di collegare i firewall direttamente tra loro; utilizzare sempre uno switch o un segmento di rete intermedio.
   - Etichettare tutti i cavi e gli switch per maggiore chiarezza e facilitare la risoluzione dei problemi.
2. **Connessioni LAN**:
   - Collegare le interfacce LAN sia del nodo primario che di quello secondario allo stesso segmento di rete.
   - Idealmente, utilizzare **due switch separati** per la ridondanza. Collegare la porta LAN di ciascun firewall a entrambi gli switch (se supportato), oppure almeno assicurarsi che ciascun firewall sia collegato a uno switch diverso. In questo modo si evita un singolo punto di guasto nel caso in cui uno switch si guasti.
   - Se si utilizzano due switch separati per la ridondanza, è necessario che siano correttamente interconnessi e che supportino lo Spanning Tree Protocol (STP) per prevenire loop di rete. Gli switch non gestiti senza supporto STP possono causare broadcast storm quando sono interconnessi.
   - Se è disponibile solo uno switch, utilizzare la segmentazione VLAN per separare logicamente ciascuna zona di rete e minimizzare i domini di broadcast.
   - Ripetere questo processo per **ogni interfaccia di rete** configurata per HA (ad esempio, LAN, GUEST, DMZ). Ogni interfaccia deve essere collegata al relativo segmento di rete, preferibilmente tramite switch ridondanti.
3. **Connessioni WAN**:

- Collegare le interfacce WAN di entrambi i nodi all'ISP o al router upstream.
- Per la massima ridondanza, utilizzare lo stesso approccio adottato per le connessioni LAN.
- Se è disponibile solo uno switch/router WAN, entrambi i firewall dovrebbero collegarsi ad esso, ma questo introduce un singolo punto di guasto.
- Se il proprio ISP fornisce un router con funzionalità HA (ad esempio, VRRP o HSRP), è possibile collegare direttamente le porte WAN di entrambi i firewall ai router ridondanti dell'ISP.
- In alternativa, è possibile configurare MultiWAN direttamente in NethSecurity per gestire più uplink WAN e il failover.

Questa configurazione garantisce che, in caso di guasto di un singolo firewall o switch, la connettività di rete venga mantenuta tramite il nodo secondario e lo switch rimanente.

Il diagramma seguente illustra la configurazione di rete ridondante consigliata; gli switch sono omessi per chiarezza.


LAN Host
Traffic
LAN GW- Virtual IP
192.168.100.240
Active
Failover
HA Nodes
Primary Node
WAN
22.33.44.55
LAN
192.168.100.238
HA sync
Secondary Node
Active
WAN
disabled
LAN
192.168.100.239
Failover
Router
Traffic
Internet

42.2.2 Gestione delle interfacce

Le interfacce possono essere classificate come segue:

1. **Interfaccia HA**:

Questa è l'interfaccia utilizzata per la comunicazione VRRP. Deve essere configurata sia sul nodo primario che su quello secondario, quindi deve essere aggiunta alla configurazione HA durante l'inizializzazione. Questa interfaccia richiede tre indirizzi IP distinti: uno sul nodo primario, uno sul nodo secondario e un VIP (Virtual IP) che si sposta tra le unità quando i loro ruoli cambiano (Master/Backup). *HA interface*

Nota: Questa interfaccia può avere qualsiasi nome; tuttavia, la prassi consigliata è di chiamare l'interfaccia HA `lan`. In un ambiente HA, solo l'interfaccia HA può essere chiamata `lan`, tutte le altre interfacce devono utilizzare un nome diverso.

---

2. **Interfacce LAN aggiuntive**:

Qualsiasi interfaccia che non sia una WAN, come un'altra LAN, una rete guest o una DMZ. Anche queste vengono gestite utilizzando la logica a tre indirizzi (IP primario, IP secondario e VIP), devono essere configurate sia sul nodo primario che su quello secondario, quindi devono essere aggiunte alla configurazione HA dopo l'inizializzazione. Un guasto su una di queste interfacce attiva un failover tra le unità. Vengono configurate aggiungendole come interfacce LAN. *Interfacce LAN aggiuntive*.

Si ricorda che tutte le interfacce aggiuntive devono utilizzare un nome diverso da `lan`.

3. **Interfacce WAN**:

Queste interfacce vengono gestite come casi speciali. I problemi di connettività WAN sono generalmente più probabili rispetto a un guasto fisico di uno switch, di un cavo o di una scheda di rete. Attivare un failover HA quando una singola WAN va giù di solito non apporterebbe alcun reale beneficio: il firewall secondario sarebbe interessato dallo stesso problema di connettività a monte, mentre il failover stesso potrebbe introdurre interruzioni non necessarie.

Per questo motivo, i guasti WAN non provocano il passaggio dal firewall primario a quello secondario. La disponibilità della WAN dovrebbe essere gestita da MultiWAN, che è progettato per gestire la perdita di connettività, il failover dei collegamenti e l'instradamento del traffico su più uplink. Questo previene anche conflitti tra i meccanismi di HA e la gestione MultiWAN, specialmente in installazioni complesse o di alto valore. Le interfacce WAN devono essere configurate solo sul nodo primario; vengono replicate automaticamente sul nodo secondario. Ulteriori dettagli sono forniti nella sezione dedicata di seguito.

42.2.3 Interfaccia HA

Il cluster HA richiede indirizzi IP statici per tutte le interfacce LAN che ospiteranno un IP virtuale. Seguire questi passaggi:

- Accendere il nodo secondario, accedere all'interfaccia web e configurare un'interfaccia fisica con un indirizzo IP LAN statico (ad esempio, `192.168.100.239`).
- Accendere il nodo primario, accedere all'interfaccia web e configurare un'interfaccia fisica con un indirizzo IP LAN statico (ad esempio, `192.168.100.238`).

Questi indirizzi IP statici vengono utilizzati per accedere direttamente ai nodi, anche se il cluster HA è disabilitato. Considerarli come *indirizzi IP di gestione*.

42.2.4 Inizializzazione del cluster

Il processo di configurazione imposta *keepalived* per il failover, *rsync* su SSH per la sincronizzazione della configurazione e *conntrackd* per sincronizzare la tabella di connection tracking. Tutti questi dati passano attraverso l'interfaccia HA, che viene configurata durante la fase di inizializzazione. Utilizzare lo script `ns-ha-config` per semplificare il processo.

Prima di procedere con la configurazione effettiva, è importante assicurarsi che entrambi i nodi siano configurati correttamente e soddisfino i requisiti necessari.

Accedere alla console o connettersi tramite SSH al nodo primario ed eseguire i seguenti comandi.

Verificare i requisiti

Per il nodo primario:

```
ns-ha-config check-primary-node <lan_interface>
```

Questo controlla:

- L'interfaccia HA esiste ed ha un IP statico.
- Se il server DHCP è in esecuzione:
  - L'opzione DHCP `3: router` è impostata (dovrebbe essere l'IP virtuale).
  - L'opzione DHCP `6: DNS server` è impostata.

Per il nodo secondario:

```
ns-ha-config check-backup-node <backup_node_ip> <lan_interface>
```

Questo controlla:

- L'interfaccia HA esiste ed ha un IP statico.
- Il nodo secondario è raggiungibile tramite SSH sulla porta 22 con l'utente root.

Lo script richiederà la password di root per il nodo secondario. È anche possibile passare la password tramite pipe:

```
echo "password" | ns-ha-config check-backup-node <backup_node_ip> <lan_interface>
```

Assicurarsi che il nodo secondario sia raggiungibile tramite SSH dal nodo primario sulla porta standard 22.

Inizializzare i nodi

Inizializzare il nodo primario:

```
ns-ha-config init-primary-node <primary_node_ip> <backup_node_ip> <virtual_ip_cidr> <lan_
↪interface>
```

Dove `primary_node_ip` è l'indirizzo IP statico del nodo primario già configurato per l'interfaccia HA, e `backup_node_ip` è l'indirizzo IP LAN statico del nodo secondario. Il `virtual_ip` è l'indirizzo IP virtuale per l'interfaccia HA a cui tutti gli host LAN devono puntare; deve essere specificato in notazione CIDR.

Questo script:

- Inizializzare *keepalived* con l'IP virtuale per l'interfaccia LAN.
- Configurare *conntrackd*.

- Generare una password casuale e una chiave pubblica per la sincronizzazione.
- Configurare *dropbear* (server SSH) per ascoltare sulla porta *65022* e consentire solo l'autenticazione tramite chiave per la sincronizzazione.

Inizializzare il nodo secondario, eseguire sempre il comando sul nodo primario:

```
ns-ha-config init-backup-node <lan_interface>
```

Lo script richiederà la password di root del nodo secondario. È anche possibile passare la password tramite pipe:

```
echo '<password>' | ns-ha-config init-backup-node <lan_interface>
```

A questo punto, i nodi sono configurati per comunicare tramite LAN e l'indirizzo IP virtuale della LAN effettuerà il failover.

42.2.5 Interfacce WAN

Il sistema non richiede alcuna configurazione speciale per le interfacce WAN. È sufficiente configurarle all'interno della pagina `Interfacce e dispositivi` sul nodo primario e saranno gestite automaticamente dagli script HA.

Gli alias WAN possono essere aggiunti dalla stessa pagina di configurazione della rete e verranno sincronizzati automaticamente con il nodo secondario.

Le interfacce WAN vengono attivate sul nodo primario e mantenute inattive sul nodo secondario. Si noti che l'interfaccia web sul nodo secondario potrebbe non essere coerente: potrebbe mostrare l'interfaccia come «attiva» anche se è inattiva. Questa è una limitazione nota e verrà risolta in una versione futura.

42.2.6 Verificare la configurazione

Il cluster è ora pronto per essere utilizzato. È possibile verificare lo stato del cluster e accertarsi che la configurazione sia corretta.

Verificare la configurazione attuale:

```
ns-ha-config show-config
```

Verificare lo stato del cluster HA. La prima sincronizzazione può richiedere fino a 5 minuti.

```
ns-ha-config status
```

Lo stato iniziale potrebbe mostrare `Last Sync Status: SSH Connection Failed`. Dopo la sincronizzazione, dovrebbe mostrare `Last Sync Status: Up to Date`.

42.2.7 Interfacce LAN aggiuntive

È possibile aggiungere ulteriori interfacce LAN al cluster HA dopo la configurazione iniziale. Prima di aggiungere un'interfaccia, assicurarsi che l'interfaccia sia configurata con un indirizzo IP statico sia sul nodo primario che su quello secondario, analogamente a quanto fatto per l'interfaccia HA durante la configurazione iniziale. Le interfacce possono essere ethernet, bridge, VLAN o bond, ma è necessario che il nodo secondario disponga della stessa interfaccia con lo stesso nome e con la stessa gerarchia dei dispositivi (ad esempio, se l'interfaccia è una VLAN, anche l'interfaccia padre deve essere presente sul nodo secondario).

È possibile utilizzare questo comando per aggiungere qualsiasi interfaccia non-WAN, come una seconda LAN, DMZ o un'interfaccia GUEST al cluster HA.

Aggiungere interfacce aggiuntive secondo necessità:

```
ns-ha-config add-lan-interface <primary_node_ip> <backup_node_ip> <virtual_ip_address>
```

Vengono eseguiti i seguenti controlli:

- l'indirizzo IP virtuale deve essere in notazione CIDR (ad esempio, `192.168.100.1/24`)
- assicurarsi che un dispositivo con l'indirizzo IP statico specificato esista sul nodo
- Se il server DHCP è in esecuzione, il seguente
  - L'opzione DHCP `3: router` è impostata (dovrebbe essere l'IP virtuale).
  - L'opzione DHCP `6: DNS server` è impostata.

Esempio:

```
ns-ha-config add-lan-interface 192.168.200.1 192.168.200.2 192.168.200.253/24
```

42.2.8 Supporto hotspot

La funzionalità hotspot è supportata nei cluster HA, ma ci sono requisiti importanti:

- Deve essere configurato solo sulle interfacce di rete fisiche; le interfacce VLAN non sono supportate.
- Il nodo secondario deve avere esattamente gli stessi dispositivi di rete del nodo primario.
- Per mantenere la funzionalità hotspot durante il failover, l'indirizzo MAC dell'interfaccia che esegue l'hotspot sul nodo primario viene automaticamente copiato sull'interfaccia corrispondente del nodo secondario quando si verifica uno switchover. Questo comportamento impedisce l'utilizzo di interfacce VLAN per l'hotspot.

Si noti che le sessioni attive sono memorizzate nella RAM e andranno perse durante uno switchover; i client dovranno autenticarsi nuovamente a meno che l'accesso automatico non sia abilitato.

42.2.9 IP virtuali extra

Un IP Virtuale (VIP) è un indirizzo IP aggiuntivo assegnato a un'interfaccia di rete che verrà migrato al nodo secondario in caso di failover. È possibile aggiungere IP Virtuali al nodo primario sulle interfacce rilevanti.

Questo è utile per i servizi che richiedono più indirizzi IP sulla stessa interfaccia, come i server virtuali o il bilanciamento del carico.

Utilizzare il comando `ns-ha-config` per registrare l'IP virtuale nella configurazione del cluster HA.

Gli IP virtuali devono essere impostati esplicitamente sul nodo primario.

```
ns-ha-config add-vip <interface> <vip_ip_cidr>
```

Nota: l'IP virtuale apparirà come un indirizzo IP aggiuntivo sull'interfaccia di rete all'interno della pagina `Interfacce e dispositivi` dell'interfaccia web, ma non sarà elencato nella sezione degli alias.

42.2.10 Rimuovere interfacce e IP virtuali

Rimuovere un'interfaccia dalla configurazione HA:

```
ns-ha-config remove-interface <interface>
```

Esempio:

```
ns-ha-config remove-interface guest
```

Questo rimuove l'interfaccia da *keepalived*, quindi verrà esclusa dalla configurazione HA. Inoltre, l'indirizzo IP virtuale associato all'interfaccia verrà spostato sull'interfaccia di rete del nodo primario.

Rimuovere un IP virtuale dalla configurazione HA:

```
ns-ha-config remove-vip <interface> <vip_ip_cidr>
```

Esempio:

```
ns-ha-config remove-vip lan2 192.168.122.66/24
```

42.2.11 Esempio di configurazione

Supponendo:

- IP LAN del nodo primario: `192.168.100.238`
- IP LAN nodo secondario: `192.168.100.239`
- LAN Virtual IP: `192.168.100.240/24`
- Nome interfaccia LAN: `lan`
- Password di root del nodo secondario: `backup_root_password`

Eseguire i seguenti comandi sul **nodo primario**:

1. Verificare i requisiti:

   ```
   # Check requirements first
   ns-ha-config check-primary-node lan
   echo "backup_root_password" | ns-ha-config check-backup-node 192.168.100.239 lan
   ```

2. Configurare il cluster:

   ```
   # Initialize primary
   ns-ha-config init-primary-node 192.168.100.238 192.168.100.239 192.168.100.240/24␣
   ↪lan

   # Initialize secondary (run from primary node)
   echo "backup_root_password" | ns-ha-config init-backup-node lan
   ```

CAPITOLO 43

Manutenzione e Risoluzione dei Problemi

43.1 Avvisi

Abbonamento richiesto

Questa funzionalità è disponibile solo se il firewall dispone di un abbonamento valido.

Il cluster HA fornisce monitoraggio e notifiche automatiche per aiutare gli amministratori a rispondere rapidamente a eventi di failover o problemi di sincronizzazione.

I seguenti avvisi sono disponibili:

- **ha:sync:failed**: Attivato quando la sincronizzazione della configurazione tra nodo primario e secondario non riesce. Questo di solito indica che il nodo secondario non è raggiungibile a causa di problemi di rete, guasto hardware o interruzione del servizio.
- **ha:primary:failed**: Attivato durante eventi di failover quando il nodo primario diventa non disponibile.

43.2 Manutenzione

Il cluster HA è progettato per essere altamente disponibile e richiede una manutenzione minima. Tuttavia, ci sono situazioni in cui potrebbe essere necessario eseguire operazioni di manutenzione sul nodo primario o secondario.

43.2.1 Nodo secondario

Il nodo secondario può essere spento per la manutenzione senza influire sul nodo primario.

1. Arrestare *keepalived* sul **nodo secondario**:

```
/etc/init.d/keepalived stop
```

2. Eseguire la manutenzione.
3. Avviare *keepalived* sul **nodo secondario**:

```
/etc/init.d/keepalived start
```

43.2.2 Nodo primario

Il nodo primario può essere spento per la manutenzione; il nodo secondario assumerà gli indirizzi IP virtuali e tutti i servizi.

1. Arrestare *keepalived* sul **nodo primario**:

```
/etc/init.d/keepalived stop
```

2. Eseguire la manutenzione.
3. Avviare *keepalived* sul **nodo primario**:

```
/etc/init.d/keepalived start
```

43.2.3 Accesso remoto

Il nodo primario è accessibile sia dalle interfacce LAN che WAN. Pertanto, il nodo secondario è accessibile solo dall'interfaccia LAN. Quando ci si connette al nodo secondario da una rete remota, è necessario accedere prima al nodo primario e poi collegarsi al nodo secondario utilizzando SSH.

Dopo essersi connessi al nodo primario, utilizzare il seguente comando per accedere al nodo secondario:

```
ns-ha-config ssh-remote
```

Questo comando stabilirà una connessione SSH al nodo secondario utilizzando la chiave SSH generata durante la configurazione HA.

43.2.4 Aggiornamento

Il nodo secondario non riceve aggiornamenti di sistema automaticamente perché non ha accesso diretto a Internet. Per aggiornare il nodo secondario, è necessario connettersi al nodo primario ed eseguire il comando di aggiornamento sul nodo secondario:

```
ns-ha-config upgrade-remote
```

Questo comando scaricherà l'immagine più recente, la caricherà sul nodo secondario e la installerà. Come per un aggiornamento normale, il nodo secondario verrà riavviato dopo l'installazione.

43.3 Risoluzione dei problemi

La risoluzione dei problemi della configurazione HA può essere complessa, soprattutto se il nodo secondario non è raggiungibile o se il nodo primario non risponde come previsto.

Ricordare che il nodo secondario non ha accesso diretto a Internet nel suo normale stato di standby. Pertanto:

- Non è in grado di risolvere nomi DNS esterni.
- Non è possibile raggiungere il Controller o altri portali esterni.
- Non riceverà aggiornamenti di sistema.

Le seguenti istruzioni possono aiutare a identificare e risolvere i problemi comuni. Per iniziare la risoluzione dei problemi, è necessario accedere alla console SSH di entrambi i nodi.

43.3.1 Identificazione dei nodi

Poiché il nome host del nodo secondario si sincronizza con quello primario, il prompt di bash cambia per indicare il ruolo del nodo:

- Prompt del nodo primario: `root@NethSec [P]:~#`
- Prompt del nodo secondario: `root@NethSec [S]:~#`

43.3.2 Stato di Keepalived

Eseguire `ns-ha-config status` per verificare le statistiche di Keepalived. Estrarre dal risultato:

```
Keepalived Statistics:
  advert_rcvd: 249
  advert_sent: 0
  become_master: 1
  release_master: 0
  packet_len_err: 0
  advert_interval_err: 0
  ip_ttl_err: 0
  invalid_type_rcvd: 0
  addr_list_err: 0
  invalid_authtype: 0
  authtype_mismatch: 0
  auth_failure: 0
  pri_zero_rcvd: 1
  pri_zero_sent: 0
```

Su un nodo primario, il valore di *master.become_master* dovrebbe essere *1* o superiore, indicando che ha assunto con successo il ruolo di master. Inoltre, *master.advert.sent* dovrebbe essere maggiore di *0*, indicando che sta inviando attivamente annunci al nodo secondario.

Su un nodo secondario, il valore di *master.advert_rcvd* dovrebbe essere maggiore di *0*, indicando che sta ricevendo annunci dal nodo primario. Se *master.become_master* è *0*, significa che il nodo non è subentrato come master, il che è previsto per un nodo secondario.

43.3.3 Traffico VRRP

Il nodo primario invia annunci VRRP al nodo secondario ogni secondo. È possibile verificare il traffico VRRP utilizzando il seguente comando sul nodo primario:

```
tcpdump -vnnpi <lan_interface> vrrp
```

Sostituire *<lan_interface>* con il nome dell'interfaccia LAN (ad esempio, `eth0`).

L'output dovrebbe mostrare i pacchetti VRRP inviati dal nodo primario al nodo secondario. Un esempio di output:

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
 13:54:16.629467 IP (tos 0xc0, ttl 255, id 19404, offset 0, flags [none], proto VRRP␣
↪(112), length 44)
 192.168.100.238 > 192.168.100.239: VRRPv2, Advertisement, vrid 100, prio 200, authtype␣
↪simple, intvl 1s, length 24, addrs(2): 192.168.122.49,192.168.100.240 auth "1655e3d3"
```

Se lo stesso comando viene eseguito sul nodo secondario, dovrebbe mostrare i pacchetti VRRP ricevuti dal nodo primario.

43.3.4 Log

Tutti i log sono memorizzati in `/var/log/messages` su entrambi i nodi.

È possibile esaminare componenti specifici del sistema HA nei log:

- Controllare i log di sincronizzazione di rsync:

  ```
  grep ns-rsync.sh /var/log/messages
  ```

- Esaminare le attività di connessione SSH per la sincronizzazione:

  ```
  grep dropbear /var/log/messages
  ```

- Visualizzare le modifiche di stato e gli eventi di keepalived:

  ```
  grep Keepalived /var/log/messages
  ```

- Traccia le importazioni della configurazione di rete sul nodo secondario:

  ```
  grep "ns-ha: Importing network configuration" /var/log/messages
  ```

43.3.5 Debugging

Quando i file di log non sono sufficienti, è possibile abilitare la registrazione di debug per componenti specifici:

Eseguire il debug dello script *ns-ha-config*:

```
bash -x ns-ha-config <action> [<options>]
```

Visualizzare la configurazione attiva di `keepalived`:

```
cat /tmp/keepalived.conf
```

Abilitare la registrazione di debug di *keepalived* (sul primario):

```
uci set keepalived.primary.debug=1
uci commit keepalived
reload_config
```

Quindi, cercare `Keepalived_vrrp` nel file `/var/log/messages`.

43.3.6 Reimpostare la configurazione

Il comando di reset ripristina la configurazione del cluster allo stato predefinito. Tipicamente, dopo il reset, il nodo primario può continuare a funzionare normalmente, mentre il nodo secondario, non più utilizzato nel cluster, dovrebbe essere riportato alle impostazioni predefinite per evitare eventuali conflitti. Dopo il reset, rimane attiva solo l'interfaccia HA, quindi è necessario un riavvio per completare il processo. Il reset deve essere eseguito localmente sul nodo primario.

Il comando di reset:

- Arrestare e disabilitare `keepalived` e `conntrackd`.
- Rimuovere i file di configurazione HA.
- Pulire la configurazione di *dropbear*, inclusi le chiavi SSH.

Alla fine, è necessario un riavvio per applicare le modifiche. È sufficiente eseguire:

```
ns-ha-config reset
reboot
```

CAPITOLO 44

Migrazione da NethSecurity 7.9 con HA

Questo documento descrive la procedura per migrare un sistema **NethSecurity 7.9** configurato con **High Availability (HA)** a **NethSecurity 8**, mantenendo attiva la configurazione HA. Sono possibili diversi approcci per questa migrazione; questa guida illustra un metodo consigliato.

Il processo di migrazione consiste in due fasi principali:

- aggiornamento del sistema NethSecurity 7.9 alla versione 8,
- riconfigurazione del servizio High Availability tra i due firewall che eseguono NethSecurity 8.

Durante la migrazione, i due firewall vengono trattati come sistemi indipendenti. Un dispositivo verrà aggiornato a NethSecurity 8 tramite la migrazione della sua configurazione, mentre l'altro verrà ripristinato alle impostazioni di fabbrica e riconfigurato come nodo secondario HA.

Una volta completata la migrazione e la validazione del nodo primario, il servizio di High Availability verrà nuovamente abilitato tra i due firewall NethSecurity 8.

44.1 Prerequisiti

- Prendere nota degli indirizzi IP utilizzati per l'interfaccia HA: primario, secondario e VIP.
- Esaminare la configurazione di rete, in particolare per le **interfacce locali (non-WAN)**. Ognuna di queste interfacce richiede ora **tre indirizzi IP**: in precedenza ne veniva utilizzato solo uno, ma in NethSecurity 8 anche le interfacce LAN aggiuntive sono gestite tramite **VIP**, garantendo il failover in caso di problemi che interessano tali interfacce.
- Prendere nota di tutti gli indirizzi IP necessari per le interfacce aggiuntive non-WAN.
- Eseguire un backup di entrambi i firewall come precauzione.
- Verificare la **compatibilità hardware** con NethSecurity 8.

44.2 Procedura di migrazione

1. **Spegnere il firewall secondario**

   Prima di iniziare la migrazione, spegnere il firewall secondario per evitare conflitti durante l'aggiornamento del nodo primario.

2. **Scegliere il metodo di migrazione**

   Accedere allo strumento *Firewall Migration* su NethSecurity 7.9. È possibile:

   - Scaricare un'immagine migrata per creare una chiavetta USB da utilizzare per testare e verificare le configurazioni prima di eseguire la migrazione effettiva, oppure
   - Eseguire una **migrazione in-place** direttamente sul sistema.

   Scegliere l'opzione che meglio si adatta alle proprie esigenze: la prima è più sicura, mentre la seconda è più veloce. In caso di problemi, è sufficiente accendere il firewall secondario con la versione 7.9, che mantiene ancora la configurazione originale.

3. **Eseguire la migrazione**

   - Se si utilizza la migrazione in-place, una volta completato il processo, verificare che il firewall stia ora eseguendo NethSecurity 8 e che tutte le funzionalità funzionino come previsto.
   - Se si utilizza l'immagine USB, crearla e avviare il firewall primario da essa. Verificare che tutte le funzionalità siano operative. Successivamente, scrivere lo storage dell'appliance utilizzando il comando *ns-install*, quindi riavviare l'hardware senza la chiave USB.

4. **Configurare l'indirizzo VIP**

   Aggiungere il VIP (IP alias HA) per consentire agli host LAN di accedere correttamente alla rete. Questo garantisce che tutti i client LAN possano raggiungere Internet mentre si procede con il processo di ripristino, senza interrompere la connettività degli utenti. Ricordarsi di fare lo stesso per ogni altra interfaccia non-WAN.

5. **Ripristinare e riconfigurare il nodo secondario**

   Dopo aver confermato che il firewall primario funziona come previsto:

   - Scollegare tutti i cavi di rete dal firewall secondario per evitare conflitti con quello primario.
   - Ripristinare il firewall secondario alle impostazioni di fabbrica.
   - Ricreare la configurazione di rete, assicurandosi che anche le interfacce LAN aggiuntive siano gestite utilizzando i VIP.
   - Riconfigurare l'Alta Affidabilità tra i due sistemi NethSecurity 8.

CAPITOLO 45

DNS dinamico

Il Dynamic DNS (DDNS) aggiorna automaticamente il record DNS del proprio nome di dominio con l'indirizzo IP attuale, anche se questo cambia dinamicamente. Questo consente di accedere al firewall da remoto utilizzando un nome di dominio costante invece di dover ricordare un indirizzo IP che potrebbe cambiare.

45.1 Provider supportati

NethSecurity supporta i seguenti provider DDNS:

- Cloudflare
- DigitalOcean
- DNSpod
- Freedns
- Gandi
- GCP (Google Cloud Platform)
- GoDaddy
- Luadns
- No-IP
- NS1
- One.com
- Pdns
- Route53
- TransIP

Prerequisiti:

- Un firewall NethSecurity con accesso a Internet.
- Un account presso il provider DDNS scelto.
- Un nome di dominio registrato presso il proprio provider DDNS.

45.2 Passaggi generali di configurazione

1. Aprire una finestra del terminale sul firewall.
2. Selezionare il provider DDNS desiderato dall'elenco dei provider supportati. Per ottenere l'elenco dei provider supportati, eseguire il seguente comando:

   ```
   ddns service update
   ddns service list-available
   ```

3. Inserire i dettagli di configurazione DDNS, inclusi le credenziali del provider nei campi designati. Questi possono includere:
   - Il nome del servizio del provider DDNS, dall'elenco sopra: utilizzare il campo `service_name`.
   - Nome utente o ID client: utilizzare il campo `username`.
   - Password o chiave API: utilizzare il campo `password`.
   - Nome di dominio da associare al proprio indirizzo IP dinamico: utilizzare il campo `domain`, è anche possibile utilizzare il campo `lookup_host`.
   - Interfaccia da monitorare per le modifiche dell'indirizzo IP (ad esempio, «wan»): utilizzare il campo `interface`.

Sebbene i passaggi generali siano simili, i dettagli specifici della configurazione possono variare leggermente a seconda del provider scelto. Si consiglia di consultare la documentazione del provider per istruzioni dettagliate e per eventuali impostazioni aggiuntive richieste.

A causa della varietà di provider supportati, inclusi le loro interfacce uniche e i metodi di autenticazione specifici, non è possibile fornire in questa guida istruzioni di configurazione dettagliate per ciascun provider.

Se il proprio provider non è elencato, è comunque possibile configurarlo utilizzando una *configurazione personalizzata*.

45.3 Utilizzo della riga di comando UCI

Utilizzare i comandi uci per impostare e confermare le opzioni di configurazione:

```
uci set ddns.myddns.service_name="ddnsprovider.com"
uci set ddns.myddns.domain="host.yourdomain.net"
uci set ddns.myddns.username="your_user_name"
uci set ddns.myddns.password="p@ssw0rd"
uci set ddns.myddns.interface="wan"
uci set ddns.myddns.enabled="1"
uci commit ddns
```

Ricordarsi di sostituire i segnaposto con i propri valori.

Quindi, riavviare il servizio DDNS:

```
/etc/init.d/ddns restart
```

Consultare la documentazione UCI per un elenco completo delle impostazioni supportate.

Note aggiuntive:

- Assicurarsi che il piano del provider DDNS scelto supporti l'accesso API e gli aggiornamenti dinamici.
- Verificare attentamente tutte le credenziali inserite per garantirne l'accuratezza ed evitare errori durante l'aggiornamento.
- Considerare l'abilitazione della registrazione (logging) per il servizio DDNS per monitorare gli aggiornamenti e risolvere eventuali problemi.
- Alcuni provider possono offrire funzionalità avanzate come i caratteri jolly e l'aggiornamento dei sottodomini. Esplorare queste opzioni in base alle proprie esigenze specifiche.

45.3.1 Example: DigitalOcean (DO)

The following example uses the fictional `firewall.example.net` setup on NethSecurity. The DigitalOcean API token is intentionally redacted; replace it with your own token.

```
uci set ddns.do=service
uci set ddns.do.service_name='digitalocean.com-v2'
uci set ddns.do.lookup_host='firewall.example.net'
uci set ddns.do.domain='example.net'
uci set ddns.do.username='firewall'
uci set ddns.do.password='REDACTED_DIGITALOCEAN_API_TOKEN'
uci set ddns.do.param_opt='21694203'
uci set ddns.do.enabled='1'
uci set ddns.do.interface='wan'
uci set ddns.do.ip_source='network'
uci set ddns.do.ip_network='wan'
uci commit ddns
/etc/init.d/ddns restart
```

The relevant DigitalOcean fields are:

- `domain`: the domain managed in DigitalOcean
- `username`: the hostname label to update
- `password`: the personal access token
- `param_opt`: the DNS record ID for that hostname

To list the records and find the ID, run:

```
curl -X GET -H 'Content-Type: application/json' \
      -H "Authorization: Bearer TOKEN" \
      "https://api.digitalocean.com/v2/domains/DOMAIN/records"
```

Replace `TOKEN` and `DOMAIN` with your own values.

45.3.2 Esempio: afraid.org (FreeDNS)

Configurare un dominio con FreeDNS (afraid.org) utilizzando la riga di comando UCI. Il dominio si chiama «sanchio.crabdance.com» e il nome utente e la password sono «myuser» e «mypass», rispettivamente.

```
uci set ddns.afraid=service
uci set ddns.afraid.service_name='afraid.org-v2-basic'
uci set ddns.afraid.lookup_host='sanchio.crabdance.com'
uci set ddns.afraid.enabled='1'
uci set ddns.afraid.use_ipv6='0'
uci set ddns.afraid.domain='sanchio.crabdance.com'
uci set ddns.afraid.username='myuser'
uci set ddns.afraid.password='mypass'
uci set ddns.afraid.ip_source='network'
uci set ddns.afraid.ip_network='wan'
uci set ddns.afraid.interface='wan'
uci set ddns.afraid.use_syslog='1'
uci set ddns.afraid.check_unit='minutes'
uci set ddns.afraid.force_unit='minutes'
uci set ddns.afraid.retry_unit='seconds'
uci commit ddns
/etc/init.d/ddns restart
```

45.3.3 Esempio personalizzato: dyndns.it (DynDNS)

È inoltre possibile configurare alcuni provider DDNS personalizzati utilizzando la riga di comando UCI. Configurare un dominio con DynDNS utilizzando la riga di comando UCI. Il dominio si chiama «nstest1.freeddns.it» e il nome utente e la password sono rispettivamente «nstest1» e «nstest».

```
uci set ddns.dyndns_it=service
uci set ddns.dyndns_it.enabled='1'
uci set ddns.dyndns_it.lookup_host='nstest1.freeddns.it'
uci set ddns.dyndns_it.domain='nstest1.freeddns.it'
uci set ddns.dyndns_it.username='nstest1'
uci set ddns.dyndns_it.password='nstest'
uci set ddns.dyndns_it.interface='wan'
uci set ddns.dyndns_it.ip_source='network'
uci set ddns.dyndns_it.ip_network='wan'
uci set ddns.dyndns_it.force_interval='24'
uci set ddns.dyndns_it.force_unit='hours'
uci set ddns.dyndns_it.check_interval='10'
uci set ddns.dyndns_it.check_unit='minutes'
uci set ddns.dyndns_it.update_url='http://update.dyndns.it/nic/update?hostname=[DOMAIN]&
↪user=[USERNAME]&password=[PASSWORD]'
uci commit ddns
/etc/init.d/ddns restart
```

45.4 Split DNS

Some deployments publish the same hostname inside the LAN and on the public internet. If `lookup_host` resolves to a private address on the firewall itself, DDNS can compare the public WAN IP against the internal answer and keep retrying even when the provider update succeeded.

The recommended fix is to make DDNS query an external resolver for the lookup instead of the local split-DNS answer. For example:

```
uci set ddns.do.dns_server='1.1.1.1'
uci commit ddns
/etc/init.d/ddns restart
```

This keeps split DNS for LAN clients while the DDNS client validates the public record.

45.5 Utilizzo di Luci

L'interfaccia web *Luci* offre un modo semplificato per configurare DDNS su NethSecurity. Consultare la documentazione ufficiale per istruzioni dettagliate sull'utilizzo di Luci per configurare DDNS.

CAPITOLO 46

DNS over HTTPS con filtraggio

DNS over HTTPS (DoH) è un protocollo per la cifratura delle query DNS tramite HTTPS, migliorando la privacy impedendo l'intercettazione del traffico DNS. Questa funzionalità consente di configurare server DNS upstream che supportano il protocollo DoH. Il pacchetto `https-dns-proxy` fornisce un proxy DNS-to-HTTPS locale che inoltra le query DNS a un provider DoH remoto.

Questo documento fornisce istruzioni per l'installazione e la configurazione dei server upstream DoH che offrono filtraggio e sono basati nell'UE, ma è possibile utilizzare qualsiasi provider DoH che soddisfi le proprie esigenze. Questa configurazione si applica solo ai server upstream del firewall: i client continueranno a inviare richieste DNS al firewall in chiaro sulla porta 53.

Un elenco di provider DoH che supportano località europee e il filtraggio è disponibile sul sito European Alternatives.

Alcune alternative popolari includono:

- DNS4EU, servizio DNS europeo con funzionalità di risoluzione protetta e blocco degli annunci
- Quad9, orientato alla privacy con blocco dei malware
- Mullvad, include il blocco di malware, il blocco di pubblicità e il filtraggio di base (Pornografia, Gioco d'azzardo, ecc.)
- Cloudflare, provider DoH veloce e ampiamente utilizzato con blocco malware (1.1.1.1 for families)

46.1 Installazione

Il pacchetto `https-dns-proxy` non è incluso nelle immagini predefinite di NethSecurity, quindi sarà necessario installarlo manualmente:

```
opkg update
opkg install https-dns-proxy
```

46.2 Configurazione

Per impostazione predefinita, il pacchetto include due provider (Cloudflare e Google). Per utilizzare un provider DoH personalizzato, è necessario:

1. Rimuovere i provider predefiniti (opzionale)
2. Aggiungere la configurazione del provider DoH preferito
3. Eseguire il commit e applicare la configurazione

46.2.1 Passaggi di configurazione

In questo esempio verrà configurato il provider DoH DNS4EU (joindns4.eu).

1. Rimuovere i provider predefiniti (se si desidera utilizzare solo DNS4EU):

```
uci del https-dns-proxy.@https-dns-proxy[1]
uci del https-dns-proxy.@https-dns-proxy[0]
```

2. Aggiungere il provider DNS4EU DoH:

```
uci set https-dns-proxy.joindns4=https-dns-proxy
uci set https-dns-proxy.joindns4.resolver_url='https://noads.joindns4.eu/dns-query'
uci set https-dns-proxy.joindns4.bootstrap_dns='86.54.11.13,86.54.11.213,
↪2a13:1001::86:54:11:13,2a13:1001::86:54:11:213'
uci set https-dns-proxy.joindns4.listen_addr='127.0.0.1'
uci set https-dns-proxy.joindns4.listen_port='5053'
uci commit https-dns-proxy
```

Il parametro `bootstrap_dns` è facoltativo; se non viene fornito, il sistema utilizzerà i DNS di Google e Cloudflare per il bootstrap.

3. Applicare la configurazione, https-dns-proxy utilizzerà automaticamente il proxy DoH locale come DNS upstream:

```
reload_config
```

Verifica

Per verificare che il proxy DoH stia funzionando correttamente, controllare lo stato del servizio:

```
/etc/init.d/https-dns-proxy status
```

È anche possibile testare la risoluzione DNS:

```
dig google.com @127.0.0.1 -p 5053
```

46.3 Risoluzione dei problemi

46.3.1 Reindirizzamento DNS

Per impostazione predefinita, tutte le query DNS verso qualsiasi server vengono forzate attraverso il proxy DoH locale per garantire che tutto il traffico DNS sia crittografato, ma ciò potrebbe causare problemi con alcuni dispositivi o applicazioni.

Se viene visualizzato un errore «Impossibile accedere al server DNS privato» sul dispositivo Android, è possibile risolverlo disabilitando il forcing DNS nella configurazione di `https-dns-proxy`.

Eseguire i seguenti comandi tramite SSH o terminale:

```
uci set https-dns-proxy.config.force_dns='0'
uci commit https-dns-proxy
service https-dns-proxy restart
```

46.3.2 Aggiornamento dell'immagine

Il pacchetto `https-dns-proxy` sovrascrive la configurazione DNS predefinita, quindi se si aggiorna l'immagine di NethSecurity, il sistema non sarà in grado di connettersi a Internet e ripristinare il pacchetto.

Per superare questo problema, è possibile interrompere temporaneamente il proxy DoH prima di aggiornare l'immagine:

```
service https-dns-proxy stop
```

Questo ripristinerà la configurazione DNS predefinita e consentirà al sistema di connettersi a Internet dopo l'aggiornamento dell'immagine. Una volta completato l'aggiornamento, è possibile riavviare il proxy DoH:

```
service https-dns-proxy restart
```

46.3.3 Blocco di altri provider DoH

Per bloccare le richieste DoH dai client verso qualsiasi altro server consentendo però le richieste provenienti dal firewall, sono disponibili due opzioni:

1. Abilitare la categoria `public DoH-Providers` all'interno di Threat Shield IP e inserire nella allowlist il server upstream scelto come provider DoH
2. Utilizzare DPI (Deep Packet Inspection) per bloccare DoH, che opera solo sul traffico inoltrato, consentendo al firewall di utilizzare DoH mentre si impedisce ai client di utilizzarlo direttamente

CAPITOLO 47

Notifiche e-mail (SMTP)

Avvertimento: Questa funzionalità è ancora in fase di sviluppo e non dispone ancora di un'interfaccia utente. Attualmente può essere configurata solo tramite la riga di comando.

Questa sezione fornisce istruzioni per la configurazione del client SMTP (msmtp) sul firewall NethSecurity per l'invio di notifiche email. Il client SMTP viene utilizzato esclusivamente per l'invio di email di notifica e si appoggia a un server SMTP esterno per la consegna.

Il client SMTP msmtp offre funzionalità avanzate per migliorare la sicurezza e l'affidabilità:

- **Supporto TLS/SSL:** msmtp supporta la crittografia TLS/SSL per una comunicazione sicura tra il firewall e il server SMTP esterno
- **Autenticazione:** alcuni server SMTP richiedono l'autenticazione per identificare l'utente che invia l'email

Consultare il manuale per sviluppatori per i comandi su come configurarlo dalla riga di comando.

CAPITOLO 48

Server SNMP

Il Simple Network Management Protocol (SNMP) fornisce un metodo standardizzato per monitorare e gestire dispositivi di rete come il firewall da remoto. Consente agli utenti autorizzati di recuperare informazioni essenziali come lo stato del dispositivo, metriche sulle prestazioni e impostazioni di configurazione.

Il server SNMP è **disabilitato per impostazione predefinita** sul firewall, consentendo l'accesso dalla rete locale (LAN) su tutti gli indirizzi IPv4 e IPv6.

Nota: Se il sistema è stato aggiornato dalla versione v1.4.1 o precedente, il server SNMP sarà **abilitato per impostazione predefinita**. Per disabilitarlo, seguire i passaggi nella sezione *Disabilitazione del server SNMP*.

48.1 Configurazione del server SNMP

È fondamentale configurare le informazioni essenziali che identificano il dispositivo. Ecco come farlo tramite la riga di comando:

1. Aprire una finestra del terminale sul firewall.
2. Utilizzare i seguenti comandi per impostare i valori desiderati per `sysLocation`, `sysContact` e `sysName`:

```
uci set snmpd.general.enabled=1
uci set snmpd.@system[0].sysLocation='<string>'
uci set snmpd.@system[0].sysContact='<string>'
uci set snmpd.@system[0].sysName='<string>'
```

Sostituire <*string*> con le informazioni pertinenti. Ad esempio:

```
uci set snmpd.general.enabled=1
uci set snmpd.@system[0].sysLocation='MyOffice'
uci set snmpd.@system[0].sysContact='admin@nethsecurity.org'
uci set snmpd.@system[0].sysName='firewall.nethsecurity.org'
```

3. Dopo aver apportato le modifiche, applicarle utilizzando:

```
uci commit snmpd
reload_config
```

La configurazione del server SNMP è memorizzata nel file */etc/config/snmpd*.

È possibile testare la configurazione utilizzando un client SNMP come `snmpwalk` o `snmpget` da una macchina remota. Ad esempio:

```
snmpwalk -v 2c -c public 127.0.0.1
```

48.2 Disabilitazione del server SNMP

Se non è necessario l'accesso remoto al server SNMP, è possibile disabilitarlo per una maggiore sicurezza. Seguire questi passaggi:

1. Aprire una finestra del terminale sul firewall.
2. Utilizzare i seguenti comandi per disabilitare il server:

```
uci set snmpd.general.enabled=0
uci commit snmpd
reload_config
```

Nota: La disattivazione del server SNMP potrebbe influire sugli strumenti di monitoraggio o sulle applicazioni che ne fanno affidamento.

48.3 Abilitazione dell'accesso remoto

Se è necessario accedere al server SNMP dall'esterno della propria LAN, creare una regola firewall che consenta il traffico UDP in ingresso sulla porta `161` verso il firewall stesso. Ricordare che l'apertura di questa porta aumenta il rischio, quindi procedere con cautela e assicurarsi di limitare l'accesso solo da indirizzi IP selezionati.

48.4 Considerazioni sulla sicurezza

Dare priorità alla sicurezza prima di abilitare l'accesso remoto:

- **Stringa di community robusta:** Sostituire la stringa di community predefinita «public» con una complessa e unica.
- **Controllo accessi:** Implementare le Access Control List (ACL) per limitare l'accesso esclusivamente agli indirizzi IP autorizzati.

CAPITOLO 49

Tunnel OpenVPN personalizzato

Questa guida spiega come configurare un client OpenVPN su NethSecurity utilizzando un file di configurazione (`myvpn.ovpn`) fornito da un provider di servizi VPN. La configurazione garantisce che la VPN si avvii automaticamente all'avvio del firewall.

49.1 Prerequisiti

- Un file di configurazione OpenVPN valido (*myvpn.ovpn*) fornito dal proprio provider VPN.
- Accesso al terminale NethSecurity tramite SSH.
- Familiarità di base con il sistema UCI (Unified Configuration Interface) in OpenWrt/NethSecurity.

49.1.1 Note aggiuntive sulla configurazione della CLI

- Questa procedura non include alcuna validazione dei dati inseriti. Pertanto, è destinata a essere eseguita da utenti avanzati che hanno familiarità con l'ambiente NethSecurity e le configurazioni di OpenVPN.
- La VPN creata utilizzando questo metodo non apparirà nell'interfaccia web di NethSecurity e potrà essere gestita solo tramite l'interfaccia a riga di comando (CLI).
- È fondamentale evitare di utilizzare lo stesso nome per una VPN creata tramite CLI e una configurata attraverso l'interfaccia web di NethSecurity. Poiché non sono presenti meccanismi di protezione per prevenire conflitti di denominazione, tale sovrapposizione potrebbe causare problemi di configurazione.

Per questi motivi, si raccomanda vivamente cautela e attenzione ai dettagli durante l'esecuzione di questa procedura.

49.2 Configurare la VPN

49.2.1 1. Posizionare il file di configurazione nella directory corretta

1. Copiare il file `myvpn.ovpn` nella directory `/etc/openvpn/`. Utilizzare SCP o uno strumento simile per trasferire il file:

```
scp myvpn.ovpn root@<NethSecurity_IP>:/etc/openvpn/
```

2. Assicurarsi di impostare i permessi corretti per il file:

```
chmod 644 /etc/openvpn/myvpn.ovpn
chown root:root /etc/openvpn/myvpn.ovpn
```

49.2.2 2. Creare una nuova configurazione client OpenVPN in UCI

1. Aggiungere una nuova sezione OpenVPN nel database UCI chiamata `myvpn`, collegare il file di configurazione a questa sezione e abilitare la VPN

```
uci add openvpn openvpn
uci rename openvpn.@openvpn[-1]='myvpn'
uci set openvpn.myvpn.enabled='1'
uci set openvpn.myvpn.config='/etc/openvpn/myvpn.ovpn'
```

2. Eseguire il commit delle modifiche per salvare la configurazione:

```
uci commit openvpn
```

49.2.3 3. Avviare immediatamente il client VPN

Per avviare il client VPN senza riavviare il sistema, eseguire:

```
/etc/init.d/openvpn restart
```

Questo riavvierà tutti i tunnel OpenVPN configurati.

49.2.4 4. Verificare che la VPN sia in esecuzione

Per assicurarsi che OpenVPN stia utilizzando il file di configurazione corretto e stia funzionando come previsto, verificare i processi attivi:

```
ps -ef | grep myvpn
```

L'output dovrebbe essere simile al seguente (nome di configurazione di esempio `myvpn`):

```
4913 ?        S      0:00 /usr/sbin/openvpn --syslog openvpn(myvpn) --status /var/run/
↪openvpn.myvpn.status --cd /etc/openvpn --config myvpn.ovpn --up /usr/libexec/openvpn-
↪hotplug up myvpn --down /usr/libexec/openvpn-hotplug down myvpn --route-up /usr/
↪libexec/openvpn-hotplug route-up myvpn --route-pre-down /usr/libexec/openvpn-hotplug␣
↪route-pre-down myvpn --script-security 2
```

Confermare che il parametro `--config` punti al file di configurazione corretto (ad esempio, `myvpn.ovpn`). Assicurarsi che tutti i riferimenti (ad esempio, `myvpn`) corrispondano alla configurazione VPN desiderata.

Controllare i log di OpenVPN per confermare la connessione:

```
tail -f /var/log/messages | grep openvpn
```

Dovrebbero comparire voci di log che indicano una connessione riuscita.

Nota:

- **Coerenza del nome del file:** Il nome della configurazione `myvpn` deve corrispondere al nome della sezione OpenVPN in UCI e alla posizione del file di configurazione. Se si modifica il nome, assicurarsi che tutti i riferimenti a `myvpn` nei comandi e nei nomi dei file siano aggiornati.
- **Avvio automatico:** Impostando `enabled='1'`, il client VPN si avvierà automaticamente ogni volta che il firewall viene avviato.

49.3 Configurare le credenziali di autenticazione (opzionale)

Se la VPN richiede un nome utente e una password, creare un file di autenticazione.

1. Creare un file denominato `/etc/openvpn/myvpn.auth` (sostituire `myvpn` con il nome della VPN se diverso):

   ```
   vi /etc/openvpn/myvpn.auth
   ```

2. Aggiungere il seguente contenuto, sostituendo `frank` e `frank_password` con il proprio nome utente e la propria password:

   ```
   frank
   frank_password
   ```

3. Salvare e impostare i permessi corretti:

   ```
   chmod 600 /etc/openvpn/myvpn.auth
   chown root:root /etc/openvpn/myvpn.auth
   ```

4. Aggiornare il file di configurazione OpenVPN (`myvpn.ovpn`) per fare riferimento al file di autenticazione.

   ```
   echo "auth-user-pass /etc/openvpn/myvpn.auth" >>  /etc/openvpn/myvpn.ovpn
   ```

Nota: File di autenticazione: quando si utilizza un file di autenticazione, assicurarsi che abbia permessi restrittivi (`600`) per proteggere le informazioni sensibili.

49.4 Configurare il firewall per consentire il traffico per la VPN

Per abilitare il traffico attraverso la VPN, è necessario configurare il firewall su NethSecurity. La pratica consigliata è assegnare un nome dispositivo fisso alla VPN, creare una zona dedicata per la VPN personalizzata e associare il dispositivo VPN a quella zona.

49.4.1 1. Correggere il nome del dispositivo VPN

Per garantire che il nome del dispositivo VPN rimanga coerente ed evitare l'assegnazione automatica, è fondamentale fissare il nome nel file di configurazione di OpenVPN. Modificare il file (`/etc/openvpn/myvpn.ovpn`) per cambiare `dev tun` in `dev tunmyvpn` e aggiungere la seguente riga (questo esempio è realizzato con una VPN *routed*):

```
dev-type tun
```

Avvertimento: Si ricorda che il nome dell'interfaccia (indicato come `tunmyvpn` nell'esempio) non deve superare i 13 caratteri.

49.4.2 2. Creare una zona firewall

Dall'interfaccia utente di NethSecurity, creare una nuova zona firewall denominata `myzone`. Configurare questa zona per consentire l'accesso alle risorse necessarie.

49.4.3 3. Associare il dispositivo VPN alla zona

Per associare il dispositivo VPN alla zona firewall `myzone`, eseguire i seguenti passaggi dalla riga di comando:

1. Aggiungere il dispositivo VPN (`tunmyvpn`) alla zona del firewall:

   ```
   uci add_list firewall.ns_myzone.device=tunmyvpn
   uci commit firewall
   ```

2. Riavviare il firewall per applicare le modifiche:

   ```
   /etc/init.d/firewall restart
   ```

Queste modifiche garantiscono che il dispositivo VPN venga sempre denominato `tunmyvpn`, prevenendo potenziali problemi con l'associazione alla zona del firewall.

49.5 Disabilitare il tunnel

Se si desidera impedire l'avvio automatico della VPN all'avvio del firewall, è possibile disabilitarla utilizzando i seguenti comandi.

1. Disabilitare la VPN in UCI:

   ```
   uci set openvpn.myvpn.enabled='0'
   uci commit openvpn
   ```

2. Riavvia tutti i tunnel VPN attivi. Questo comando interromperà tutti i tunnel e riavvierà completamente solo quelli con il valore enabled impostato a 1:

```
/etc/init.d/openvpn restart
```

CAPITOLO 50

Log

I log vengono inizialmente scritti in una directory temporanea in memoria per prevenire potenziali errori sul file system root in caso di un guasto.

1. **Archiviazione locale**: I log possono essere scritti direttamente nell'archiviazione. Questa opzione può essere configurata dall'interfaccia utente, vedere la sezione *Storage*.
2. **Controller remoto**: I log possono essere inoltrati automaticamente a un *controller remoto*.
3. **Syslog Forwarder personalizzato**: I log possono essere inviati a un server syslog remoto.
4. **Cloud Log Manager**: I log possono essere inoltrati al servizio Nethesis Cloud Log Manager (CLM).

I prossimi paragrafi spiegheranno come configurare queste ultime opzioni.

50.1 Inoltro a un server remoto

È sufficiente configurare il database UCI con le opzioni desiderate, quindi confermare le modifiche e infine riavviare il servizio. I log temporanei continueranno a essere visibili in `/var/log/messages` e saranno anche inviati al server remoto.

La maggior parte dei server syslog sono configurati per ascoltare sulla porta UDP 514 per impostazione predefinita.

Esempio di configurazione per l'invio dei log al server syslog con IP 192.168.1.88 sulla porta UDP 514. La configurazione è denominata `clm` (custom log manager):

```
uci set rsyslog.clm=forwarder
uci set rsyslog.clm.source=*.*
uci set rsyslog.clm.protocol=udp
uci set rsyslog.clm.port=514
uci set rsyslog.clm.target=192.168.1.88
```

Una volta configurato, è sufficiente confermare le modifiche con il comando:

```
uci commit rsyslog
```

E infine, riavviare il servizio:

```
/etc/init.d/rsyslog restart
```

Per impostazione predefinita, il forwarder utilizza il TraditionalFileFormat (RFC 3164) per i log. È anche possibile configurare RFC 5424 utilizzando la stessa sintassi:

```
uci set rsyslog.clm.rfc=5424
```

È possibile configurare più forwarder ripetendo l'operazione utilizzando un nome di configurazione diverso come `clm2`.

50.2 Inoltro a Nethesis Cloud Log Manager

Autorizzazione al servizio richiesta

È necessario acquistare un abbonamento per il servizio CLM da Nethesis e ottenere l'identificativo del tenant. Il servizio è attualmente riservato ai clienti Enterprise. Per ulteriori informazioni, contattare il reparto vendite di Nethesis.

Il pacchetto `ns-clm` inoltra i messaggi syslog al servizio Nethesis Cloud Log Manager (CLM). Fornisce il demone `ns-clm-forwarder`, che monitora `/var/log/messages` e tiene traccia della posizione di lettura in `/var/run/ns-clm/last_offset`. Le nuove righe syslog vengono analizzate, raggruppate e inviate come JSON tramite HTTP POST all'endpoint CLM. Il demone controlla la presenza di nuove righe ogni 10 secondi, rileva automaticamente la rotazione dei log e salva la posizione raggiunta allo spegnimento, in modo da poter riprendere dopo un riavvio.

Il pacchetto non è incluso di default su NethSecurity 8.7.2 o versioni precedenti, ma è disponibile nel repository dei pacchetti e può essere installato manualmente. Installarlo con:

```
opkg update
opkg install ns-clm
```

La configurazione UCI è memorizzata in `/etc/config/ns-clm`:

Opzione	Predefinito	Descrizione
`abilitato`	`0`	Abilitare (`1`) o disabilitare (`0`) il forwarder
`uuid`	Nessun testo da tradurre.	Identificatore univoco per il dispositivo, generato con `uuidgen` e preceduto da «L» per garantire che inizi con una lettera. Questo è necessario affinché il servizio CLM possa identificare la fonte dei log. Esempio: `L3d50ca11-4415-4e46-9ee9-b1da0f62c337`
`indirizzo`	`https://nar.nethesis.it`	Indirizzo server CLM
`tenant`	Nessun testo da tradurre.	Identificatore tenant CLM, disponibile all'interno del portale CLM, sotto `Utenti e Aziende` -> `Aziende`
`debug`	`0`	Abilita l'output di debug su stderr (`1`)

Per abilitare il forwarder e impostare l'identificatore del tenant, eseguire:

```
uci set ns-clm.config.uuid="L$(uuidgen)"
uci set ns-clm.config.enabled=1
uci set ns-clm.config.tenant=<tenant_id>
uci commit ns-clm
reload_config
```

È possibile trovare l'identificatore del tenant nel portale CLM, sotto `Utenti e Aziende` -> `Aziende`.

Per abilitare anche il servizio all'avvio:

```
/etc/init.d/ns-clm enable && /etc/init.d/ns-clm start
```

Per arrestare e disabilitare il forwarder:

```
/etc/init.d/ns-clm stop && /etc/init.d/ns-clm disable
```

50.3 Rotazione dei log

I log vengono ruotati per gestire lo spazio su disco e garantire che i file di log non crescano indefinitamente.

50.3.1 Rotazione dei log in memoria

Il file di log `/var/log/messages` è memorizzato in RAM e viene ruotato in base alle dimensioni. Una volta raggiunto un limite di dimensione predefinito, il log viene ruotato e compresso per risparmiare spazio. Il log ruotato viene salvato come `/var/log/messages.1.gz` in formato gzip. Il sistema mantiene solo due versioni del log: il file di log attivo e l'ultimo file ruotato e compresso. A partire dalla versione 1.4.0, per impostazione predefinita, la soglia di rotazione del log è impostata al 10% del filesystem tmpfs montato su `/tmp`.

Lo script `ns-log-size` gestisce la dimensione di rotazione dei log per il servizio Rsyslog. Consente di **ottenere** e **impostare** la dimensione di rotazione dei log, definita in byte, per il file di log situato in `/var/log/messages`.

- **Ottieni dimensione attuale**: Recupera la dimensione attuale della rotazione del log in byte.
- **Imposta nuova dimensione**: Modificare la dimensione di rotazione dei log a un valore specificato, assicurandosi che la nuova dimensione sia un intero positivo e non inferiore a 52428800 byte (50 MB).
- **Sicurezza della configurazione**: Se la dimensione specificata è inferiore alla soglia minima, lo script avvisa l'utente e non apporta alcuna modifica alla configurazione.

Utilizzo

Per utilizzare lo script, eseguirlo con la seguente sintassi:

```
ns-log-size {get|set <size>}
```

- **get**: Restituisce la dimensione attuale della rotazione dei log in byte.
- **set <size>**: Imposta la dimensione di rotazione del log al valore specificato (in byte).

Esempio

Per ottenere la dimensione attuale della rotazione dei log:

```
ns-log-size get
```

Per impostare una nuova dimensione di rotazione dei log a 104857600 byte (100 MB):

```
ns-log-size set 104857600
```

Il servizio rsyslog viene riavviato automaticamente dopo che la dimensione è stata impostata.

Tutte le modifiche alla dimensione della rotazione dei log vengono scritte direttamente nel file di configurazione di Rsyslog `/etc/rsyslog.conf`.

50.3.2 Rotazione dei log di storage

Quando si utilizza lo storage persistente, la rotazione dei log è gestita dall'utilità `logrotate`, che è configurata per ruotare i log settimanalmente e conservare un massimo di 52 settimane (1 anno) di log. Dopo la rotazione, i log vengono compressi utilizzando gzip e archiviati nella stessa directory con una convenzione di denominazione che include la data della rotazione (ad esempio, `/mnt/data/log/messages-20260315.gz`).

Il file di configurazione per logrotate si trova in `/etc/logrotate.d/data.conf` e può essere modificato per cambiare la frequenza di rotazione e il periodo di conservazione secondo necessità. Il file di configurazione viene aggiunto automaticamente al backup e mantenuto durante gli aggiornamenti, quindi tutte le impostazioni personalizzate vengono preservate.

CAPITOLO 51

Speedtest

Lo strumento Speedtest è un'applicazione ampiamente utilizzata per misurare la velocità e le prestazioni di una connessione Internet. Fornisce informazioni dettagliate sulle velocità di download e upload, oltre che su ping e jitter. Questo strumento è essenziale per diagnosticare problemi di rete, verificare le affermazioni dei fornitori di servizi e garantire prestazioni ottimali per varie attività online.

In NethSecurity lo strumento Speedtest è disponibile come funzionalità integrata accessibile solo dalla riga di comando.

51.1 Utilizzo

Poiché il test può essere influenzato dalle impostazioni QoS, è preferibile disabilitarle prima di eseguire il test:

```
/etc/init.d/qosify stop
```

Speedtest seleziona automaticamente il server migliore in base alla posizione dell'utente. Per eseguire un test di velocità, è sufficiente digitare il seguente comando nel terminale:

```
speedtest
```

Questo comando eseguirà un test completo, includendo test di latenza, velocità di download e upload. La selezione del server si basa sulla posizione dell'utente e sulla disponibilità del server. A volte, la selezione del server potrebbe non essere ottimale, con conseguenti risultati inaccurati del test di velocità.

Per superare questo problema, è possibile forzare la selezione del server utilizzando l'opzione `--force-by-latency-test`:

```
speedtest --force-by-latency-test
```

Ricordarsi di riabilitare QoS dopo aver eseguito il test:

```
/etc/init.d/qosify start
```

51.2 MultiWAN

Lo strumento speedtest seleziona casualmente un server per eseguire il test. In un ambiente MultiWAN, la selezione del server può essere influenzata dall'interfaccia WAN utilizzata per raggiungere il server.

È possibile forzare la selezione dell'interfaccia WAN utilizzando il wrapper mwan3.

Dato un dispositivo WAN chiamato `wan1`, il seguente comando eseguirà lo speedtest utilizzando l'interfaccia selezionata:

```
mwan3 use wan1 speedtest --force-by-latency-test
```

CAPITOLO 52

UPS (NUT)

Un gruppo di continuità (UPS, Uninterruptible Power Supply) è un dispositivo che fornisce alimentazione di riserva quando la fonte di alimentazione principale viene meno. Viene utilizzato per proteggere hardware come computer, apparecchiature di telecomunicazione o altri dispositivi elettrici in cui un'interruzione improvvisa dell'alimentazione potrebbe causare interruzioni operative o perdita di dati.

Network UPS Tools (NUT) è una raccolta di programmi che fornisce un'interfaccia comune per il monitoraggio e l'amministrazione dell'hardware UPS.

Questa guida spiega come configurare un UPS collegato via USB con NUT su NethSecurity. Al termine della guida, l'UPS dovrebbe essere monitorato e il sistema dovrebbe spegnersi quando la batteria è scarica.

NUT non è installato di default. Fa parte dei pacchetti extra di NethSecurity e può essere installato dalla riga di comando. La suite NUT è composta da diversi pacchetti, ma i più importanti sono:

- `nut-server`: Il demone NUT server si connette direttamente all'UPS, fornendo i dati al client.
- `nut-upsc`: Uno strumento da riga di comando per interrogare lo stato dell'UPS.
- `nut-upsmon`: Il demone di monitoraggio NUT UPS comunica con nut-server e avvia lo spegnimento del sistema quando la batteria dell'UPS è scarica.
- `nut-upscmd`: Uno strumento da riga di comando per inviare comandi all'UPS (supportato solo da alcuni modelli di UPS).

Nota: La configurazione di NUT non è supportata sulle macchine con una subscription NethSecurity. La funzionalità è destinata a utenti avanzati e non è coperta dal servizio di supporto.

52.1 Configurare un UPS locale

Prima di configurare l'UPS, assicurarsi che l'UPS sia collegato al firewall (un cavo è solitamente fornito con l'UPS). Quindi, seguire questi passaggi:

1. Installare i pacchetti NUT.
2. Individuare il modello di UPS, quindi installare e configurare il driver appropriato.
3. Configurare i demoni del server UPS.
4. Abilitare il monitor UPS.

52.1.1 Passaggio 1: installare i pacchetti richiesti

Installare i pacchetti richiesti:

```
opkg update
opkg install nut-server nut-upsc nut-upsmon nut-upscmd
```

Nota: A partire dalla versione 8.7.2, i pacchetti extra vengono reinstallati automaticamente dopo l'aggiornamento del sistema. Per le versioni precedenti e per ulteriori informazioni, consultare questa documentazione: *Ripristinare pacchetti aggiuntivi*.

52.1.2 Passaggio 2: configurare il driver appropriato

1. Usare `lsusb` per elencare i dispositivi USB:

   ```
   Bus 002 Device 002: ID 0463:ffff EATON 5E
   Bus 002 Device 001: ID 1d6b:0002 Linux 5.15.150 xhci-hcd xHCI Host Controller
   Bus 001 Device 002: ID 8087:8001
   ```

   In questo esempio, l'UPS è un modello EATON 5E collegato alla seconda porta USB del secondo bus USB.

2. Selezionare il driver dalla pagina dei driver NUT.

3. Tutti i pacchetti driver iniziano con il prefisso `nut-driver-`. Alcuni modelli di UPS possono richiedere un driver specifico, ma la maggior parte di essi funziona con il driver `usbhid-ups`. Installare il pacchetto driver selezionato, in questo caso il driver `usbhid-ups`:

   ```
   opkg install nut-driver-usbhid-ups
   ```

4. Configurare il driver all'interno del server `upsd` (nut-server). Il nut-server si collegherà all'UPS utilizzando il driver e la porta specificati. Monitorerà l'UPS a intervalli regolari e fornirà le informazioni ai client come `upsmon`. Eseguire:

   ```
   uci set nut_server.eaton5e=driver
   uci set nut_server.eaton5e.driver=usbhid-ups
   uci set nut_server.eaton5e.port=auto
   uci set nut_server.upsd=upsd
   uci commit nut_server
   ```

   Ricordare il nome dell'UPS, in questo caso `eaton5e`, poiché verrà utilizzato nei passaggi successivi.

52.1.3 Passaggio 3: configurare il monitoraggio

Il monitor UPS (upsmon) è un demone che monitora l'UPS e avvia l'arresto del sistema quando la batteria dell'UPS è scarica. Si connette al server UPS (upsd) e interroga lo stato dell'UPS.

In questo scenario il monitor UPS è in esecuzione sulla stessa macchina del server UPS, quindi si connetterà a localhost.

1. Configurare l'utente per il monitoraggio all'interno di `upsd`. Si noti che la password è semplice perché non viene inviata attraverso la rete:

```
uci set nut_server.upsuser=user
uci set nut_server.upsuser.username=upsuser
uci set nut_server.upsuser.password=password
uci set nut_server.upsuser.upsmon=master
```

2. Configurare il monitor:

```
uci set nut_monitor.upsmon=upsmon
uci set nut_monitor.master=master
uci set nut_monitor.master.upsname=eaton5e
uci set nut_monitor.master.hostname=localhost
uci set nut_monitor.master.username=upsuser
uci set nut_monitor.master.password=password
```

3. Eseguire il commit e riavviare i servizi:

```
uci commit nut_server
uci commit nut_monitor
/etc/init.d/nut-server restart
/etc/init.d/nut-monitor restart
```

52.1.4 Passaggio 4: verificare lo stato dell'UPS

Controllare lo stato dell'UPS:

```
upsc eaton5e
```

L'output dovrebbe apparire così:

```
battery.charge: 100
battery.runtime: 2637
battery.type: PbAc
device.mfr: EATON
device.model: 5E 850i
...
```

Se l'output è vuoto o viene visualizzato un errore, verificare il contenuto di `/var/log/messages`.

Un log corretto del server per un UPS collegato:

```
Nov 29 09:23:08 NethSec upsd[7111]: Connected to UPS [eaton5e]: usbhid-ups-eaton5e
```

Un log corretto per upsmon:

```
Nov 29 09:23:11 NethSec upsmon[7189]: Communications with UPS eaton5e@localhost␣
↪established
```

Se viene visualizzato un errore, consultare *Risoluzione dei problemi*.

Se tutto funziona correttamente, l'UPS dovrebbe essere monitorato e il sistema dovrebbe spegnersi quando la batteria si trova in uno stato critico, solitamente al di sotto del 20%.

52.2 Consentire il monitoraggio remoto

È possibile collegare più dispositivi hardware a un UPS e il server NUT può condividere lo stato dell'UPS con più client. Ad esempio, un altro sistema alimentato dallo stesso UPS può ispezionare lo stato dell'UPS collegandosi al server NUT e spegnersi quando la batteria è scarica.

Per impostazione predefinita, il server NUT è configurato per ascoltare solo su localhost. Per consentire il monitoraggio remoto, il server deve essere configurato per ascoltare su un indirizzo IP specifico o su tutte le interfacce.

1. Ascolto su tutte le interfacce:

```
uci set nut_server.listen=listen_address
uci set nut_server.listen.address=0.0.0.0
```

2. Aggiungere un utente per il monitoraggio remoto. Assicurarsi di selezionare una password sicura:

```
uci set nut_server.remoteuser=user
uci set nut_server.remoteuser.username=remoteuser
uci set nut_server.remoteuser.password=password
uci commit nut_server
/etc/init.d/nut-server restart
```

2. Verificare lo stato del server:

```
netstat -tuln | grep 3493
```

3. Creare una regola firewall per consentire il monitoraggio remoto dalla LAN, il servizio ascolta sulla porta TCP 3493:

```
uci set firewall.ns_allow_https.name='Allow-NUT-from-LAN'
uci set firewall.ns_allow_https.proto='tcp'
uci set firewall.ns_allow_https.src='lan'
uci set firewall.ns_allow_https.dest_port='3493'
uci set firewall.ns_allow_https.target='ACCEPT'
uci commit firewall
/etc/init.d/firewall restart
```

Ora è possibile connettersi al server NUT da un client upsmon remoto. Una volta configurato il client, esso si collegherà al server NUT e monitorerà lo stato dell'UPS. Se la batteria è scarica, il client avvierà lo spegnimento del sistema.

52.3 Connettersi a server NUT remoto

Questo è il caso in cui un firewall secondario è collegato allo stesso UPS e il server NUT è in esecuzione sul firewall primario. Il firewall secondario si collegherà al firewall primario e monitorerà lo stato dell'UPS.

1. Per prima cosa, installare i servizi NUT sulla macchina client:

   ```
   opkg update
   opkg install nut-upsc nut-upsmon
   ```

   Questi pacchetti non vengono conservati durante un aggiornamento del sistema. Per ulteriori informazioni, consultare *Ripristinare pacchetti aggiuntivi*.

2. Quindi, configurare il client per connettersi al server remoto:

   ```
   uci set nut_monitor.upsmon=upsmon
   uci set nut_monitor.slave=slave
   uci set nut_monitor.slave.upsname=eaton5e
   uci set nut_monitor.slave.hostname=192.168.1.8
   uci set nut_monitor.slave.username=remoteuser
   uci set nut_monitor.slave.password=password
   uci commit nut_monitor
   /etc/init.d/nut-monitor restart
   ```

3. Verificare se il client è connesso al server remoto:

   ```
   upsc eaton5e@192.168.1.8
   ```

   L'output dovrebbe essere lo stesso del server locale.

Ora il client è connesso al server remoto e monitorerà lo stato dell'UPS. Se la batteria è scarica, il client avvierà lo spegnimento del sistema.

52.4 Impostazioni UPS extra

Alcuni modelli di UPS dispongono di impostazioni aggiuntive che possono essere configurate utilizzando il comando `upscmd`. Per eseguire il comando, l'utente deve disporre delle autorizzazioni appropriate.

1. Concedere i permessi all'utente:

   ```
   uci add_list nut_server.upsuser.instcmd=all
   uci add_list nut_server.upsuser.actions=set
   uci commit nut_server
   /etc/init.d/nut-server restart
   ```

2. Controllare i comandi disponibili:

   ```
   upscmd -l eaton5e
   ```

3. Esempio per disabilitare il beep:

   ```
   upscmd -u upsuser -p password eaton5e beeper.disable
   ```

52.5 Risoluzione dei problemi

Un errore comune è il permesso negato durante l'accesso al dispositivo UPS; ad esempio, è possibile vedere questo errore all'interno di `/var/log/messages`:

```
Can't open /etc/nut/ups.conf: Can't open /etc/nut/ups.conf: Permission denied openwrt
```

Un altro errore comune è che upsd non riesce a connettersi all'UPS; ad esempio, è possibile vedere questo errore all'interno di `/var/log/messages`:

```
Nov 29 10:34:51 NethSec upsd[7055]: [D1] mainloop: UPS [eaton5e] is not currently␣
↪connected
Nov 29 10:34:51 NethSec upsd[7055]: [D1] mainloop: UPS [eaton5e] is now connected as FD -
↪1
```

Di solito, questo accade quando nut-server si connette al dispositivo UPS prima che il dispositivo sia pronto. Per risolvere il problema, la soluzione più semplice è riavviare il firewall:

```
reboot
```

Se non è possibile riavviare il firewall, è possibile provare a fermare il nut-server:

```
/etc/init.d/nut-server stop
```

Quindi verificare se il driver riesce a connettersi al dispositivo UPS:

```
/lib/nut/usbhid-ups -a eaton5e
```

Output previsto:

```
Network UPS Tools - Generic HID driver 0.47 (2.8.0)
USB communication driver (libusb 1.0) 0.43
Using subdriver: MGE HID 1.46
```

In caso di errore, potrebbe essere visualizzato un messaggio simile al seguente:

```
Can't claim USB device [0463:ffff]@0/0: Entity not found
```

Si potrebbe quindi provare a reimpostare il dispositivo USB:

```
usbreset 002/003
```

Dove `002/003` è l'ID del dispositivo USB trovato con `lsusb`, `002` è il numero del bus e `003` è il numero del dispositivo.

CAPITOLO 53

Wake-on-LAN (EtherWake)

Wake-on-LAN (WoL) è una tecnologia che consente di accendere da remoto un dispositivo spento o in sospensione inviando un messaggio di rete speciale chiamato *Magic Packet* alla sua interfaccia di rete. Il pacchetto EtherWake fornisce un semplice strumento da riga di comando per inviare questi Magic Packet e riattivare dispositivi nella rete locale. Su NethSecurity, EtherWake è disponibile nei repository ufficiali ma non è installato di default.

Nota: Il dispositivo di destinazione deve supportare Wake-on-LAN (WoL) e avere la funzionalità abilitata nel BIOS/UEFI e nelle impostazioni della scheda di rete. In caso contrario, non risponderà ai Magic Packet.

53.1 Installazione

Installare il pacchetto con:

```
opkg update
opkg install etherwake
```

Nota: A partire dalla versione 8.7.2, i pacchetti extra vengono reinstallati automaticamente dopo l'aggiornamento del sistema. Per le versioni precedenti e per ulteriori informazioni, consultare questa documentazione: *Ripristinare pacchetti aggiuntivi*.

53.2 Utilizzo

Per riattivare un dispositivo nella LAN, è necessario conoscere:

- l'`Indirizzo MAC` del dispositivo da accendere
- l'`interfaccia di rete NethSecurity` a cui il dispositivo è collegato (ad es. `eth0`)

Il comando di base è:

```
etherwake -i <interface> <MAC>
```

Esempio:

```
etherwake -i eth0 00:11:22:33:44:55
```

CAPITOLO 54

Checkmk

Checkmk è una piattaforma di monitoraggio utilizzata per supervisionare server, dispositivi di rete e appliance. Il firewall può essere monitorato con Checkmk installando i pacchetti extra di NethSecurity descritti in questo capitolo.

54.1 Pacchetti NethSecurity

L'integrazione di Checkmk per NethSecurity è suddivisa in due pacchetti:

- `checkmk-agent` è il pacchetto agente standard di Checkmk.
- `ns-checkmk-utils` aggiunge script di monitoraggio specifici per NethSecurity ed è opzionale.

L'installazione di `ns-checkmk-utils` include anche `checkmk-agent` come dipendenza. Se è necessario solo l'agent upstream, installare esclusivamente `checkmk-agent`.

54.2 Installa i pacchetti

Installare l'agente e i controlli opzionali di NethSecurity dalla riga di comando:

```
opkg update
opkg install ns-checkmk-utils
```

Dopo l'installazione, il servizio dell'agente è gestito da `/etc/init.d/check_mk_agent` ed è avviato e abilitato all'avvio per impostazione predefinita.

Utilizzare il seguente comando per verificare lo stato:

```
/etc/init.d/check_mk_agent status
```

Verificare l'output localmente con:

```
check_mk_agent
```

54.3 Consenti il monitoraggio remoto

L'agente ascolta sulla porta TCP 6556. Per impostazione predefinita, il traffico proveniente dalla LAN è consentito, ma se si dispone di una configurazione firewall più restrittiva, potrebbe essere necessario consentire l'accesso a questa porta dal server di monitoraggio Checkmk.

È possibile aggiungere una regola del firewall per consentire l'accesso direttamente dall'interfaccia utente web, vedere *Regole*, oppure utilizzare l'interfaccia a riga di comando per aggiungere una regola.

Ad esempio, per consentire l'accesso da un host di monitoraggio nella LAN:

```
uci add firewall rule
uci set firewall.@rule[-1].name='Allow-Checkmk'
uci set firewall.@rule[-1].src='lan'
uci set firewall.@rule[-1].proto='tcp'
uci set firewall.@rule[-1].dest_port='6556'
uci set firewall.@rule[-1].target='ACCEPT'
uci commit firewall
/etc/init.d/firewall restart
```

Tenere presente che, se il server di monitoraggio si trova in una zona diversa, sarà necessario regolare di conseguenza la zona di origine e l'indirizzo.

Quando la regola è attiva, il server di monitoraggio può connettersi al firewall e leggere l'output dell'agente, inclusi i controlli opzionali di NethSecurity.

CAPITOLO 55

UCI (Unified Configuration Interface)

UCI (Unified Configuration Interface) è un sistema centralizzato di gestione della configurazione utilizzato in NethSecurity. Fornisce un approccio unificato alla configurazione del sistema tramite un'interfaccia a riga di comando e file di configurazione standardizzati.

55.1 Caratteristiche principali

- **Configurazione centralizzata**: Tutte le configurazioni di sistema sono memorizzate in un'unica posizione (`/etc/config/`)
- **Basato su database**: Le configurazioni sono memorizzate in file di database strutturati
- **Nessuna validazione integrata**: UCI esegue i comandi senza controlli di sicurezza - è richiesta conoscenza del sistema
- **Flusso di lavoro in tre fasi**: Modifica → Commit → Riavvia/Ricarica
- **Supporto per eventi multipli**: Le interfacce utente possono attivare più eventi di configurazione simultaneamente

55.2 Archiviazione della configurazione

Tutte le configurazioni UCI sono memorizzate come file di database in `/etc/config/`. Ogni file rappresenta un diverso componente o servizio di sistema; di seguito è fornito un elenco esemplificativo non esaustivo.

55.2.1 Struttura dei file di configurazione

```
/etc/config/
├── acme           # SSL certificate management
├── adblock        # Advertisement blocking
├── banip          # IP banning service
├── chilli         # Captive portal
├── dedalo         # Network access control
├── dhcp           # DHCP server configuration
├── dpi            # Deep packet inspection
├── dropbear       # SSH server
├── firewall       # Firewall rules and zones
├── flashstart     # Web filtering
├── fstab          # Filesystem table
├── ipsec          # IPsec VPN
├── luci           # luci Web interface
├── mwan3          # Multi-WAN configuration
├── network        # Network interfaces and routing
├── nginx          # Web server
├── ns-ui          # NethSecurity user interface
├── objects        # Object definitions
├── openssl        # SSL/TLS configuration
├── openvpn        # OpenVPN configuration
├── qosify         # Quality of Service
├── rpcd           # RPC daemon
├── rsyslog        # System logging
├── socat          # Socket utilities
├── system         # System-wide settings
├── templates      # Configuration templates
├── ucitrack       # UCI change tracking
├── uhttpd         # HTTP server
└── users          # User management
```

55.3 Visualizzazione della configurazione

55.3.1 Mostra tutta la configurazione per un servizio specifico

```
uci show <service>
```

Esempio:

```
uci show network
```

Output:

```
network.loopback=interface
network.loopback.device='lo'
network.loopback.proto='static'
network.loopback.ipaddr='127.0.0.1'
network.loopback.netmask='255.0.0.0'
network.@device[0]=device
```

(continues on next page)

(continua dalla pagina precedente)

```
network.@device[0].name='br-lan'
network.@device[0].type='bridge'
network.@device[0].ports='eth0'
network.lan=interface
network.lan.device='br-lan'
network.lan.proto='static'
network.lan.ipaddr='192.168.100.101'
network.lan.netmask='255.255.255.0'
network.wan=interface
network.wan.device='eth1'
network.wan.proto='dhcp'
```

55.3.2 Mostra opzione di configurazione specifica

```
uci show <service>.<section>.<option>
```

Esempio:

```
uci show network.lan.ipaddr
```

55.4 Flusso di lavoro completo di configurazione

55.4.1 Processo standard in tre fasi

1. **MODIFICA** - Apportare modifiche alla configurazione
2. **COMMIT** - Salva le modifiche nel database di configurazione
3. **RELOAD** - Applica le modifiche al sistema in esecuzione

55.4.2 Esempio pratico: modifica dell'indirizzo IP LAN

```
# Step 1: Modify the configuration
uci set network.lan.ipaddr='192.168.100.151'

# Step 2: Commit the changes
uci commit network

# Step 3: Restart the network service
/etc/init.d/network restart
```

55.5 SET - Modifica della configurazione

Il comando `uci set` viene utilizzato per modificare i valori di configurazione. Le modifiche vengono memorizzate temporaneamente e devono essere confermate per diventare permanenti.

55.5.1 Impostare un valore di configurazione

```
uci set <service>.<section>.<option>='<value>'
```

Esempi:

```
# Change IP address
uci set network.lan.ipaddr='192.168.100.151'

# Change netmask
uci set network.lan.netmask='255.255.255.0'

# Change DHCP protocol to static
uci set network.wan.proto='static'
```

55.5.2 Aggiungere una nuova sezione

```
uci add <service> <section_type>
```

55.5.3 Operazioni di eliminazione

```
# Delete a configuration option
uci delete <service>.<section>.<option>

# Delete an entire section
uci delete <service>.<section>
```

55.6 LISTS - Editing List Options

Lists are a special type of option that can contain multiple values.

55.6.1 Add a value to a list

Use the `uci add_list` command to add values to a list, the command creates the list if it does not already exist.

```
uci add_list <service>.<section>.<list_option>='<value>'
```

55.6.2 Remove a value from a list

To remove the last value from a list, use the `uci del_list`, you must specify the value to be removed.

```
uci del_list <service>.<section>.<list_option>='<value>'
```

To remove all values from a list, use the `uci delete` command as explained in the previous section.

55.7 COMMIT - Salvataggio delle modifiche

Le modifiche apportate con `uci set` non vengono applicate immediatamente al sistema. Devono essere prima confermate per renderle persistenti.

55.7.1 Servizio specifico del commit

```
uci commit <service>
```

Esempio:

```
uci commit network
```

55.7.2 Confermare tutte le modifiche in sospeso

```
uci commit
```

55.7.3 Controllare le modifiche in sospeso

Prima di eseguire il commit, è possibile esaminare quali modifiche verranno applicate:

```
uci changes
```

55.7.4 Annullare le modifiche non confermate

Se si desidera scartare le modifiche non confermate:

```
uci revert <service>
```

55.8 RELOAD - Applicazione delle modifiche

Dopo aver effettuato il commit, è possibile applicare la nuova configurazione al sistema in esecuzione con un unico comando. Questo ricaricherà automaticamente i servizi interessati senza la necessità di riavviarli manualmente uno per uno.

55.8.1 Ricarica configurazione

```
reload_config
```

55.9 Formato del file di configurazione

I file di configurazione UCI utilizzano un formato strutturato con sezioni e opzioni:

```
config <section_type> '<section_name>'
    option <option_name> '<value>'
    list <list_name> '<value1>'
    list <list_name> '<value2>'
```

55.9.1 Esempio: File di configurazione di rete

File di configurazione di rete (`/etc/config/network`):

```
config interface 'loopback'
    option device 'lo'
    option proto 'static'
    option ipaddr '127.0.0.1'
    option netmask '255.0.0.0'

config device
    option name 'br-lan'
    option type 'bridge'
    list ports 'eth0'

config interface 'lan'
    option device 'br-lan'
    option proto 'static'
    option ipaddr '192.168.100.101'
    option netmask '255.255.255.0'

config interface 'wan'
    option device 'eth1'
    option proto 'dhcp'
```

55.10 Migliori pratiche

55.10.1 Considerazioni sulla sicurezza

1. **Eseguire sempre il backup delle configurazioni** prima di apportare modifiche
2. **Testare le modifiche in modo incrementale** invece di apportare più modifiche contemporaneamente
3. **Comprendere le dipendenze dei servizi** prima di riavviare i servizi
4. **Utilizzare** `uci changes` **per esaminare** le modifiche in sospeso

5. **Avere accesso alla console** disponibile durante la modifica delle impostazioni di rete

55.10.2 Problemi comuni

- **Dimenticare di eseguire il commit**: le modifiche non sono persistenti fino a quando non viene effettuato il commit
- **Nessun riavvio dei servizi**: le modifiche confermate potrebbero non essere attive fino al riavvio del servizio
- **Interruzione della connettività di rete**: Assicurarsi sempre di disporre di metodi di accesso alternativi
- **Errori di sintassi**: Una sintassi UCI non valida può causare la corruzione della configurazione

55.11 Risoluzione dei problemi

55.11.1 Comandi comuni per il debug

Visualizza modifiche in sospeso

```
uci changes
```

Ripristina allo stato dell'ultimo commit

```
uci revert <service>
```

Controllare la sintassi UCI

```
uci show | head -1
```

Nota: Assicurarsi sempre di disporre di un accesso alternativo al sistema quando si apportano modifiche critiche alla configurazione, in particolare per quanto riguarda le modifiche relative alla rete.

Avvertimento: I comandi UCI vengono eseguiti senza validazione. Configurazioni errate possono rendere il sistema inaccessibile.

CAPITOLO 56

Migrazione NethServer 7

La migrazione è il processo per convertire una macchina NethServer 7 (*sorgente*) in una NethSecurity (*destinazione*).

La migrazione della configurazione del firewall da NethServer 7 a NethSecurity è un processo cruciale per garantire la continuità e la sicurezza dei servizi di rete.

Requisiti per la migrazione:

- garantire l'accesso a Cockpit su NethServer 7
- installare l'applicazione `Firewall Migration` su NethServer 7. Dopo l'installazione, l'applicazione sarà disponibile nell'elenco delle applicazioni di Cockpit

Scenari di migrazione:

Sistema di origine	Metodo supportato	Note
NethServer 7 con solo il ruolo firewall	In-place o esportazione/importazione	È possibile riutilizzare l'hardware esistente se NethSecurity 8 rileva tutti i dischi e le schede di rete necessari.
NethServer 7 con ruoli aggiuntivi come NethService, NethVoice o mail	Esporta/importa solo	La migrazione in-place non è supportata. Installare NethSecurity 8 su una macchina dedicata e importare solo la configurazione del firewall.
NethServer 6.x	Non supportato	Eseguire prima l'aggiornamento a NethServer 7.

Nota: Se si utilizza l'Alta Affidabilità (HA) con NethServer 7, consultare anche la *guida alla migrazione HA* per istruzioni dettagliate sulla migrazione mantenendo la funzionalità HA.

56.1 Compatibilità hardware

Prima di riutilizzare l'hardware esistente, avviare l'immagine live USB o una nuova installazione di NethSecurity 8 e verificare che tutti i dischi e le schede di rete vengano rilevati. Non è necessario alcun passaggio di migrazione speciale per gli adattatori SFP/SFP+ 10 Gb supportati: se la scheda viene rilevata, è possibile procedere normalmente con la migrazione. Se non viene rilevata, utilizzare un hardware diverso o una scheda di rete già supportata da NethSecurity 8.

Gli adattatori USB-to-Ethernet non sono supportati in produzione su NethSecurity 8. Consultare la *sezione sugli adattatori USB-to-Ethernet* per maggiori dettagli.

56.2 Test della migrazione

Questo metodo consente di effettuare test approfonditi senza influire sull'installazione esistente. Un sistema di test verrà avviato da una chiavetta USB lasciando l'installazione attuale invariata.

Per eseguire una migrazione di prova, seguire questi passaggi:

1. Accedere alla pagina `Firewall Migration` su NethServer 7 Cockpit: la pagina elencherà tutte le configurazioni migrate
2. Scaricare l'immagine live USB: fare clic su *Scarica* nella sezione `Download live USB image`
3. Preparare l'unità USB: scrivere l'immagine scaricata utilizzando il metodo preferito su un'unità USB, vedere la *sezione di installazione* per ulteriori informazioni su come copiare l'immagine su un disco.
4. Avvio da unità USB: spegnere il firewall, collegare l'unità USB e riavviarlo, assicurandosi che l'avvio avvenga dall'unità USB. Questo viene generalmente effettuato tramite le impostazioni del BIOS/UEFI.
5. Avvio di migrazione: durante il processo di avvio, il sistema viene caricato dall'unità USB invece che dal disco rigido interno
6. Ambiente di test: il sistema ora opera utilizzando il sistema migrato memorizzato sulla USB. Eventuali modifiche o test effettuati avvengono all'interno di questo ambiente isolato.

Ricordare che, dopo il test, è sufficiente rimuovere la chiavetta USB, riavviare normalmente il firewall e questo riprenderà a utilizzare la configurazione originale, lasciando l'installazione esistente invariata.

56.3 Migrazione in-place

Se la configurazione iniziale di NethServer 7 include solo il modulo firewall, è possibile migrare e riutilizzare l'hardware attuale senza interruzioni. Questo approccio semplifica la migrazione, eliminando la necessità di hardware aggiuntivo.

Per eseguire la migrazione in-place da NethServer 7 a NethSecurity, seguire questi passaggi:

1. Eseguire il backup dei dati: la migrazione in-place è un processo distruttivo. Si consiglia vivamente di creare un backup completo della macchina prima di procedere. Questo passaggio è fondamentale per garantire la sicurezza dei dati in caso di eventuali problemi durante la migrazione.
2. Accedere alla pagina `Firewall Migration` su NethServer 7 Cockpit: la pagina elencherà tutte le configurazioni migrate
3. Scaricare l'archivio di configurazione come precauzione: come misura precauzionale, scaricare l'archivio contenente la configurazione esportata facendo clic su *Scarica* nella sezione `Download exported archive`. Conservare questo archivio in un luogo sicuro; potrebbe essere utile nel caso in cui la migrazione in-place fallisca.

4. Avviare la migrazione: quando si è pronti, fare clic sul pulsante *Migra* per avviare il processo di migrazione. Questo segnala al sistema di iniziare la migrazione da NethServer 7 a NethSecurity.
5. Selezionare il disco di destinazione: scegliere il disco su cui verrà installato NethSecurity. Si noti che NethSecurity non supporta RAID. Se il server NethServer 7 originale dispone di più di un disco, gli altri dischi rimarranno invariati e inutilizzati durante il processo di migrazione.
6. Confermare e avviare il processo: dopo aver selezionato il disco, fare clic su *Migra* per confermare. Il sistema scaricherà l'immagine di NethSecurity e la scriverà sul disco selezionato. Successivamente, il sistema si riavvierà automaticamente.
7. Completare la migrazione al primo avvio: al primo avvio di NethSecurity, la configurazione da NethServer 7 verrà migrata automaticamente. Assicurarsi di verificare attentamente tutte le impostazioni e i servizi per confermare che siano stati migrati correttamente.

Dopo aver completato la migrazione, seguire i *passaggi post-migrazione* per assicurarsi che il sistema sia configurato correttamente.

56.4 Migrazione con altri moduli installati

Questo scenario prevede l'esportazione di un archivio di configurazione speciale da NethServer 7 e l'importazione dello stesso in NethSecurity.

Questo metodo è consigliato quando la configurazione originale di NethServer 7 include moduli aggiuntivi, come il mail server, il groupware WebTop o il modulo PBX NethVoice. Per eseguire questa migrazione, è necessario installare NethSecurity su un nuovo hardware e poi importare la configurazione nel sistema NethSecurity appena installato.

Per eseguire la migrazione da NethServer 7 a NethSecurity, seguire questi passaggi:

1. Installare NethSecurity su una nuova macchina: seguire le *istruzioni di installazione*
2. Accedere alla pagina `Firewall Migration` su NethServer 7 Cockpit: la pagina elencherà tutte le configurazioni migrate
3. Scaricare l'archivio con la configurazione esportata: fare clic su *Scarica* nella sezione `Download export archive`
4. Accedere alla pagina `Backup & Restore` su NethSecurity e andare nella scheda `Migrazione`, quindi fare clic su *Carica file di migrazione* e selezionare l'archivio scaricato nel passaggio precedente.
5. Quando si importa la configurazione su un nuovo hardware, gli indirizzi MAC delle interfacce di rete cambiano, rendendo necessaria una decisione su come rimappare queste interfacce. L'interfaccia utente mostra le interfacce della macchina di origine a sinistra e quelle della macchina di destinazione a destra. Se la macchina di origine aveva VLAN configurate, è necessario rimappare l'interfaccia fisica e il sistema ricreerà automaticamente la VLAN sull'interfaccia sottostante.
6. Fare clic su *Migra* per avviare il processo di migrazione

Dopo aver completato la migrazione, seguire i *passaggi post-migrazione* per assicurarsi che il sistema sia configurato correttamente.

56.5 Passaggi post-migrazione

Il processo di migrazione in-place viene eseguito quando il sistema è offline. Poiché il processo di registrazione richiede una connessione Internet attiva, la subscription non viene migrata durante la migrazione in-place. Se è stata eseguita una migrazione in-place, è necessario *registrare nuovamente il sistema*. Questo passaggio non è necessario se è stata eseguita una migrazione utilizzando il metodo dell'archivio esportato.

Quando si utilizza un server LDAP remoto o Active Directory per autenticare i client OpenVPN Road Warrior, assicurarsi che il server remoto sia raggiungibile dalla nuova macchina NethSecurity verificando anche la risoluzione dei nomi DNS. Se necessario, aggiornare la configurazione DNS sulla nuova macchina. Inoltre, consultare la *pagina del database utenti remoto* per verificare che tutti gli utenti siano stati importati correttamente.

Si noti che il server web di NethSecurity ascolta solo su HTTPS (porta 443) per le regole di reverse proxy. Se erano state configurate delle regole di reverse proxy su NethServer 7 utilizzando HTTP (porta 80), sarà necessario aggiornarle per utilizzare HTTPS. Consultare la *documentazione sul reverse proxy* per ulteriori dettagli.

Quindi, verificare che tutti i servizi funzionino correttamente. In caso di problemi, consultare la *sezione di risoluzione dei problemi*.

Il processo di migrazione viene registrato in un file di log speciale situato in `/root/migration.log`. Questo file contiene tutte le azioni eseguite durante il processo di migrazione. Si noti che il file di log viene eliminato dopo un aggiornamento dell'immagine.

56.5.1 Correzione della denominazione di bond e VLAN per l'Alta Disponibilità

Se si è effettuata una migrazione da NethServer 7, si potrebbe notare che i dispositivi di rete aggregati hanno nomi lunghi come `bond-bond0` invece del formato più breve `bond0` utilizzato nelle nuove installazioni di NethSecurity 8. Anche se ciò non influisce sulle funzionalità di base, questi nomi più lunghi possono impedire la configurazione dell'*Alta Affidabilità (HA)* e potrebbero apparire incoerenti nell'interfaccia utente.

Se si prevede di utilizzare l'Alta Disponibilità o si preferisce semplicemente avere nomi di dispositivi più chiari, è possibile rinominarli utilizzando uno script semplice.

Prima di iniziare, effettuare una copia di backup della configurazione di rete:

```
cp /etc/config/network /root/network.ori
```

Quindi, eseguire questo comando per rinominare i dispositivi:

```
sed -i \
  -e "/option[[:space:]]\+ifname/s/'bond-bond\([0-9]\+\)'/'bond-b\1'/" \
  -e "/option[[:space:]]\+device/s/'bond-bond\([0-9]\+\)'/'bond-b\1'/" \
  -e "/option[[:space:]]\+name/s/'bond-bond\([0-9]\+\)\(\.[0-9]\+\)'/'b\1\2'/" \
  -e "/option[[:space:]]\+name/s/'bond-bond\([0-9]\+\)'/'bond-b\1'/" \
  -e "s/^\([[:space:]]*option[[:space:]]\+name[[:space:]]\+\)'b\([0-9]\+\)'\
↪([[:space:]]*\)$/\1'bond-b\2'\3/" \
  /etc/config/network
```

Dopo aver eseguito lo script, riavviare la rete per applicare le modifiche:

```
/etc/init.d/network restart
```

In alternativa, è possibile riavviare l'intero sistema per assicurarsi che tutte le modifiche abbiano effetto correttamente.

Una volta verificato che tutto funziona correttamente, è possibile eliminare in sicurezza il backup:

```
rm -f /root/network.ori
```

Dopo le modifiche, i dispositivi utilizzeranno la convenzione di denominazione più breve (ad esempio, `b0`, `b0.20`), che è compatibile con High Availability e corrisponde alle nuove installazioni.

56.6 Matrice di copertura della migrazione

La tabella seguente mostra ciò che viene migrato da NethServer 7 e ciò che richiede ancora un intervento manuale.

Area	Risultato	Note
Password di root	Migrato	La stessa password può essere utilizzata per SSH e per l'interfaccia web.
Interfacce di rete e VLAN	Migrato con limitazioni	La configurazione di rete viene migrata. I bridge su bond non sono supportati. Su nuovo hardware, le VLAN vengono ricreate automaticamente sull'interfaccia fisica scelta durante la rimappatura. Se si è migrato da NethServer 7 e si ha la necessità di normalizzare i nomi di bond e VLAN per HA, consultare *Correzione della denominazione di bond e VLAN per l'Alta Disponibilità*.
Etichette delle interfacce di rete	Migrato	Le etichette di origine vengono mantenute come nomi delle interfacce, ad eccezione delle interfacce WAN che mantengono i loro nomi originali.
Data e fuso orario	Migrato	
Server DHCP e prenotazioni	Migrato con limitazioni	I server DHCP sulle interfacce bond non sono supportati.
Configurazione DNS e host locali	Migrato con limitazioni	Le opzioni TFTP vengono migrate, ma il contenuto TFTP no. Per riabilitarlo, configurare manualmente `tftp_root`.
Route IPv4 statiche	Migrato	
Reindirizzamenti di porta	Migrato	
Zone del firewall	Migrato	Le zone verdi diventano `lan`, quelle rosse diventano `wan`, quelle arancioni diventano `dmz` e quelle blu diventano `guest`. Se esisteva una zona blu, le regole di accettazione per DNS e DHCP vengono aggiunte automaticamente.
Regole del firewall	Migrato con conversione	Le regole che utilizzano i servizi NDPI non sono supportate. Gli oggetti di origine e destinazione, incluse le zone personalizzate, vengono convertiti in valori IP/CIDR all'interno delle regole migrate. I NAT helper vengono caricati automaticamente con i parametri standard del kernel.
Oggetti firewall	Non ricreato	Al momento, gli oggetti firewall non possono essere reimportati automaticamente nel nuovo sistema. Le regole che utilizzavano oggetti come origine o destinazione vengono convertite nei corrispondenti valori IP/CIDR.
MultiWAN	Parziale	I provider vengono mantenuti. Le regole di deviazione (policy routing) non vengono migrate.
QoS	Parziale	Le classi con larghezza di banda riservata e le relative regole non sono supportate.
OpenVPN Road Warrior	Parziale	Le impostazioni vengono migrate. Il database di contabilità non viene migrato e la notifica tramite email non è supportata. Se il server si autentica tramite un Active Directory remoto, consultare anche *Database remoti*.
Tunnel OpenVPN	Migrato	
Tunnel IPSec	Migrato	
Threat Shield IP	Parziale	Solo le liste enterprise vengono migrate. Le liste community devono essere configurate nuovamente manualmente.
Abbonamento	Condizionale	Viene migrato solo quando si utilizza il metodo di esportazione dell'archivio.
Hotspot	Condizionale	Su nuovo hardware l'indirizzo MAC cambia, quindi l'hotspot deve essere registrato nuovamente sul remote manager.
Let's Encrypt e certificati reverse proxy	Rigenerato	La configurazione viene migrata, ma i certificati vengono generati nuovamente dopo la migrazione.
Filtro DNS Cloud FlashStart	Migrato	

56.6.1 Esempi di rimappatura

I seguenti esempi mostrano come alcune configurazioni vengono migrate quando le interfacce di rete delle macchine di origine e destinazione non corrispondono:

- Rimappatura VLAN: se la VLAN 20 era configurata su `eth1` nel firewall di origine e `eth1` viene mappata su `eth2` nel firewall di destinazione, la VLAN 20 viene ricreata automaticamente su `eth2`.
- Conversione degli oggetti firewall: se una regola utilizzava un set di host chiamato `BranchOffice` con valore `10.20.30.0/24`, la regola migrata mantiene direttamente `10.20.30.0/24` invece di ricreare l'oggetto.

56.6.2 Funzionalità non migrate

Le seguenti funzionalità non sono migrate su NethSecurity:

- Proxy web (Squid) e filtro (ufdbGuard), sostituiti da *Content Filtering* e *Filtro Deep Packet Inspection (DPI)*
- IPS (Suricata) e avvisi IPS (EveBox), sostituiti da *Intrusion Prevention System (Snort)*
- Monitoraggio UPS (NUT), disponibile solo da riga di comando con *UPS (NUT)*
- Statistiche di sistema (Collectd), sostituite da Netdata in *Monitoraggio in tempo reale*
- Report (Dante), sostituiti dalle metriche del controller in *Metriche*
- Monitoraggio della larghezza di banda (ntopng), il monitoraggio integrato della larghezza di banda è disponibile in *Monitoraggio in tempo reale* e tramite *Metriche*
- Fail2ban, viene sostituito da Threat shield *funzionalità di blocco dei tentativi di forza bruta*
- Threat shield DNS deve essere riconfigurato manualmente *Threat shield DNS*

56.7 Zone personalizzate

Le zone personalizzate sono raramente utilizzate in NethServer 7 e tipicamente per compiti molto specifici. Sono necessarie per definire un segmento di rete con regole firewall differenti da quelle dell'interfaccia primaria o, più comunemente, per gestire correttamente il traffico proveniente da una rete diversa da quella a cui l'interfaccia è collegata. Queste zone permettono di definire un comportamento specifico per quel segmento di rete e garantiscono un corretto instradamento in ambienti complessi (ad esempio, una regola di port forwarding con destinazione host remoto tramite MPLS o tunnel VPN).

In NethSecurity, le zone funzionano in modo diverso rispetto a NethServer 7, offrendo in questi casi una gestione molto più semplice. Tipicamente, in NethSecurity, tutte le precedenti configurazioni effettuate con zone personalizzate possono essere gestite facilmente **senza la necessità di ricreare alcuna zona personalizzata**, grazie al seguente comportamento predefinito.

1. Ereditarietà delle policy per il traffico in ingresso

Tutto il traffico in ingresso da un'interfaccia NethSecurity eredita automaticamente le stesse policy dell'interfaccia a cui è collegata, indipendentemente dalla rete di origine. Questo include il masquerading automatico quando il traffico è destinato a Internet.

Vediamo un esempio:

Un'interfaccia locale denominata `office` opera sul segmento di rete 192.168.1.0/24 ed è assegnata alla zona `lan`. Un gateway con IP 192.168.1.220 è collegato allo stesso switch dell'interfaccia `office`, fornendo accesso alla rete remota 10.10.10.0/24. La rete remota 10.10.10.0/24 deve utilizzare NethSecurity per accedere a Internet.

In NethSecurity, non è necessaria alcuna configurazione aggiuntiva: tutti i pacchetti inviati all'interfaccia `office` vengono instradati correttamente, anche se provengono da un segmento di rete diverso. Il masquerading viene inoltre applicato a tutti i pacchetti in uscita.

2. Non è necessario creare nuove zone per segmenti diversi

Proprio come le policy, le regole standard possono essere applicate a questo traffico senza la necessità di creare una nuova zona. Se si desidera applicare policy diverse per questo segmento, è sufficiente creare regole firewall standard. Per comodità, è possibile utilizzare un set di host con la rete CIDR negli oggetti firewall.

3. Il routing funziona senza problemi senza regole aggiuntive

Il routing per questo specifico segmento di rete funziona correttamente senza la necessità di regole o zone aggiuntive. In NethServer 7, era obbligatorio creare una zona per garantire il corretto instradamento dei pacchetti in ingresso, come menzionato nell'esempio iniziale di port forwarding.

56.8 Adattatori USB-Ethernet

Può raramente accadere che il NethServer 7 in fase di migrazione abbia collegato un adattatore USB a Ethernet per aggiungere un dispositivo di rete. Questi adattatori non dovrebbero essere utilizzati in un firewall e **non sono supportati su NethSecurity 8**. Tuttavia, è possibile installare alcuni driver specifici per scopi sperimentali, non per ambienti di produzione. Questi driver possono essere utili per gestire temporaneamente il firewall migrato in attesa di hardware dotato di tutte le schede di rete necessarie. Maggiori informazioni sono disponibili nella *sezione di rete*.

Avvertimento: Se si utilizzano questi adattatori, ricordare che non funzioneranno fino a quando non sarà installato il driver corretto. Tenere presente che NethSecurity 8 potrebbe non disporre del driver corretto per l'adattatore utilizzato su NethServer 7. In questo caso, sarà necessario utilizzare un adattatore diverso.

Nota: Se si utilizza un adattatore da USB a Ethernet per un'interfaccia RED/WAN, è importante sapere che non sarà possibile scaricare i moduli necessari per farlo funzionare correttamente su NethSecurity 8 a meno che non siano presenti altre interfacce RED/WAN che utilizzano schede di rete collegate direttamente alla scheda madre.

CAPITOLO 57

Risoluzione dei problemi

NethSecurity è un sistema firewall sofisticato con numerosi componenti interconnessi. Sebbene il sistema automatizzi molte configurazioni in modo trasparente, possono occasionalmente verificarsi dei malfunzionamenti.

È possibile creare una richiesta di supporto e segnalare problemi al team di supporto Nethesis o al forum della community NethServer.

Per le versioni stabili, è possibile aprire un ticket sul portale helpdesk di Nethesis se la macchina dispone di una sottoscrizione.

Per le release instabili, è possibile aprire una nuova discussione sul forum della community NethServer solo in inglese nella categoria NethSecurity. Se si è partner Nethesis, è possibile aprire una nuova discussione in italiano sulla community partner Nethesis nella categoria NethSecurity.

Quando si apre una richiesta di supporto o si segnala un problema, è necessario seguire queste linee guida per garantire una risoluzione rapida ed efficace:

- Assegnare titoli chiari e descrittivi a ciascun ticket o discussione.
- Fornire informazioni complete e dettagliate in ogni richiesta.
- Includere screenshot, log e qualsiasi altra informazione rilevante per facilitare la risoluzione dei problemi.
- Collaborare con il team di supporto fornendo feedback e rispondendo alle loro richieste.

1. Raccogliere informazioni

Prima di creare una richiesta di supporto, è fondamentale raccogliere quante più informazioni possibili sul problema riscontrato. Questo aiuta il team di supporto a identificare e risolvere il problema rapidamente.

La richiesta di assistenza dovrebbe includere quanto segue:

- **Configurazione del sistema:** Questa include la versione di NethSecurity in uso; l'informazione è disponibile all'interno della pagina Dashboard. Si prega di riportare la versione completa, ad esempio `8 23.05.2-ns.0.0.1-beta1-96-ga759afb`
- **Il problema riscontrato:** Descrivere il problema in dettaglio, includendo i passaggi eseguiti per riprodurlo.

- **Eventuali messaggi di errore:** Se vengono visualizzati messaggi di errore, includerli nella richiesta. È possibile utilizzare l'*interfaccia utente* per raccogliere queste informazioni, oppure accedere alla riga di comando e utilizzare `less /var/log/messages` per trovare i log rilevanti.
- **Eventuali modifiche apportate:** Se sono state apportate modifiche alla configurazione del sistema, elencarle nella richiesta.
- **Risultato desiderato:** Qual è l'obiettivo che si intende raggiungere contattando il supporto?

2. Descrivere il problema in modo oggettivo

Quando si descrive il problema, concentrarsi su sintomi oggettivi. Evitare affermazioni soggettive come «non funziona» o «è lento». Invece, descrivere cosa accade quando si eseguono azioni specifiche.

Esempio: invece di dire «Il firewall non funziona», si potrebbe dire «Quando si tenta di accedere a un sito web, viene visualizzato questo messaggio di errore.»

3. Rispondere alle richieste di informazioni

Se il team di supporto richiede di eseguire dei test o di fornire ulteriori dettagli, è necessario farlo tempestivamente e in modo accurato. Più informazioni vengono fornite, più sarà semplice per loro risolvere il problema.

4. Comunicare l'esito della soluzione

Una volta che il team di supporto propone una soluzione, è necessario testarla e comunicare l'esito. Se il problema è stato risolto, informare il team. In caso contrario, fornire ulteriori informazioni affinché possano proseguire con l'indagine.

5. Non riavviare se il problema è bloccante

Evitare di riavviare il sistema se il problema è bloccante. Il riavvio può talvolta peggiorare la situazione. Invece, contattare il supporto e collaborare con esso per risolvere il problema.

6. Ticket o discussioni multiple per lo stesso problema

Si consiglia di aprire «n» ticket o discussioni per «n» richieste diverse, anche se queste sono correlate allo stesso problema di base. Anche se può sembrare rigido e scomodo, questo approccio offre vantaggi significativi:

- **Parallelizzazione migliorata del carico di lavoro:** Consente al team di supporto di lavorare su più aspetti del problema simultaneamente.
- **Risoluzione più rapida da parte degli specialisti:** Diverse richieste possono essere assegnate a specialisti differenti con competenze specifiche, accelerando la risoluzione.
- **Risoluzione dei problemi più efficace:** Consente di concentrarsi su ogni singola richiesta, evitando confusione e disorientamento.
- **Gestione avanzata delle priorità:** Consente di assegnare priorità diverse a ciascuna richiesta in base all'urgenza e all'impatto.
- **Comunicazione migliorata:** Facilita una comunicazione chiara tra il team di supporto e l'utente, garantendo una discussione dedicata per ciascun problema.

57.1 Raccolta di informazioni dall'interfaccia utente

Quando si verificano problemi, l'interfaccia utente (UI) visualizza un messaggio di errore che descrive la natura del problema.

Il messaggio di errore fornisce informazioni preziose, presentando i dettagli della richiesta e l'errore riscontrato in formato JSON. Per facilitare la diagnosi e la risoluzione del problema, è possibile utilizzare il pulsante `Copia comando`. Facendo clic su questo pulsante, si può recuperare il comando che ha generato l'errore. Basta incollare questo comando copiato in una shell per ottenere informazioni più dettagliate.

Quando si segnala un errore al team di supporto, è fondamentale fornire le seguenti informazioni essenziali:

1. **Comando copiato:** Incollare il comando copiato utilizzando il pulsante `Copia comando`.
2. **Output dell'esecuzione:** Per ulteriore assistenza, eseguire il comando copiato e riportare l'output.

Se le informazioni fornite non sono sufficienti, in casi estremi potrebbe essere necessario condividere il contenuto della console JavaScript se l'errore è presente. Seguire le istruzioni del proprio browser (di solito accessibili premendo `F12`), copiare l'intero contenuto della console e incollarlo per un'analisi più approfondita. La collaborazione nel fornire informazioni accurate e dettagliate garantisce una risoluzione più efficace e tempestiva di eventuali problemi riscontrati con NethSecurity.