FIREWALL TOOLBOX

Report completo

Dettagli appliance

Numero di serie:	0040103CD830
Nome firewall:	UDS-NSV270
Modello appliance:	SonicWall NSv 270
Tempo di attività:	0 Days, 0 Hours, 22 Minutes, 15 Seconds
Versione firmware:	7.3.0-7012-R8150

Dettagli del report

Creato il:	15.09.2026 16:36:20
File EXP:	C:\Us...ox\Repository\0040103CD830\exp_api_downloaded.exp
Timestamp EXP:	15.09.2026 16:33:48
File TSR:	C:\Us...ox\Repository\0040103CD830\tsr_api_downloaded.wri
Timestamp TSR:	15.09.2026 16:33:49

Informazioni aggiuntive

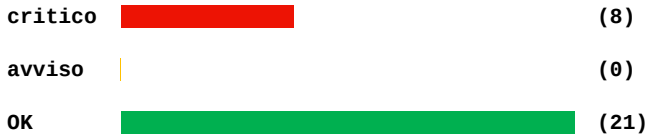
- IPv6 è disattivato. I report relativi a IPv6 non sono inclusi

- Le regole aggiunte automaticamente sono escluse da questo report

Indice

Spiegazione

Allineamento della configurazione alle best practice



Questo report valuta l'attuale configurazione del firewall SonicWall rispetto alle raccomandazioni di best practice consolidate. Il suo scopo è identificare le impostazioni già allineate agli standard operativi e di sicurezza, evidenziando al contempo le aree in cui potrebbero essere consigliabili miglioramenti. La valutazione è intesa a supportare una revisione strutturata della configurazione del dispositivo per quanto riguarda sicurezza, manutenibilità, resilienza e affidabilità complessiva del servizio.

Una configurazione firewall ben allineata aiuta a ridurre il rischio operativo, semplifica l'amministrazione e migliora la trasparenza durante le attività di supporto e audit. Oltre ai controlli di sicurezza tecnici, l'allineamento alle best practice include anche la coerenza della configurazione, un'identificazione chiara del dispositivo e l'eliminazione di impostazioni non necessarie o legacy. Ogni sezione esaminata in questo report è quindi progettata per fornire sia un'indicazione dello stato sia una breve spiegazione del motivo per cui l'elemento valutato è rilevante da una prospettiva operativa o di sicurezza.

Particolare attenzione viene dedicata allo stato del software e del firmware del firewall. Il report verifica se il firmware attualmente installato è aggiornato e se sono state rilevate indicazioni di un downgrade firmware non supportato. Ciò è importante perché un firmware obsoleto può esporre il dispositivo a problemi noti, mentre scenari di downgrade non supportati possono influire su stabilità, compatibilità e supportabilità da parte del fornitore. Uno stato firmware conforme è pertanto un requisito chiave per un funzionamento sicuro e affidabile.

Il report esamina anche se IPv6 è attivato e se il suo utilizzo appare appropriato per l'ambiente. Se IPv6 non è richiesto, dovrebbe generalmente essere disattivato per ridurre la superficie di attacco non necessaria e la complessità amministrativa. Allo stesso modo, il report valuta se l'alta disponibilità è attivata. Laddove l'alta disponibilità non sia in uso, se ne consiglia vivamente l'implementazione, poiché migliora la resilienza e riduce i tempi di inattività in caso di guasto hardware o manutenzione pianificata.

Un'altra area importante è la ridondanza della connettività. La configurazione viene esaminata per determinare se sono disponibili più connessioni WAN. Se è in uso un solo uplink WAN, si consiglia vivamente una connessione WAN aggiuntiva per migliorare la ridondanza e mantenere la connettività Internet durante le interruzioni del provider. Vengono considerate anche le impostazioni di ottimizzazione relative al WAN come l'MTU. Se la WAN MTU appare configurata a un valore insolitamente basso, ciò dovrebbe essere esaminato, poiché valori MTU inutilmente bassi possono ridurre l'efficienza di trasmissione e influire negativamente sulle prestazioni.

Da una prospettiva di sicurezza, il report include controlli relativi alla protezione degli account utente, all'hardening VPN e alle capacità di difesa dalle minacce. Valuta se gli account amministrativi sono protetti dall'autenticazione a due fattori, fortemente consigliata per ridurre il rischio di accesso non autorizzato tramite credenziali deboli, riutilizzate o compromesse. Viene inoltre esaminata la configurazione VPN per la presenza di algoritmi di crittografia obsoleti, cifrari deboli o impostazioni legacy che potrebbero ridurre la sicurezza delle comunicazioni crittografate. Inoltre, il report verifica se le funzioni di rilevamento e prevenzione sono attivate, poiché queste funzioni sono essenziali per identificare attività sospette e bloccare potenziali minacce in una fase iniziale.

La visibilità amministrativa e la disciplina operativa vengono ulteriormente affrontate tramite controlli come il logging di audit interno e lo stato di packet capture. Una funzione di audit interno attivata è importante perché fornisce tracciabilità per le modifiche di configurazione e le azioni amministrative, supportando la risoluzione dei problemi, le indagini di sicurezza e i requisiti di conformità. Il report identifica anche se Packet Capture è ancora in esecuzione. Una cattura di pacchetti continuamente attiva può indicare una risoluzione dei problemi non completata e può creare un sovraccarico non necessario se lasciata attiva senza un valido motivo operativo.

Infine, il report considera lo stato di utilizzo complessivo del firewall. Esaminare l'utilizzo complessivo è importante per determinare se il dispositivo opera entro un intervallo di carico accettabile o si sta avvicinando ai limiti di capacità. Un utilizzo costantemente elevato può indicare rischi per le prestazioni e dovrebbe essere ulteriormente valutato. Nel loro insieme, i riscontri di questo report forniscono una panoramica pratica della qualità della configurazione attuale e aiutano a identificare misure che possono migliorare la postura di sicurezza, la stabilità operativa e la manutenibilità a lungo termine.

Il nome del firewall è stato modificato

Rinominare un firewall SonicWall dal suo numero di serie a un nome dispositivo significativo migliora l'amministrazione, la risoluzione dei problemi e il reporting. Un nome descrittivo facilita l'identificazione a colpo d'occhio della posizione, del ruolo o dell'assegnazione al cliente del firewall, specialmente in ambienti con più dispositivi. Ciò riduce la confusione, velocizza le attività di supporto e abbassa il rischio di errori di configurazione o operativi.

Funzione - Impostazione	Stato	Raccomandazione
Il nome del firewall è stato modificato	Stato	-

Firmware e impostazioni

Questa sezione mostra se la versione firmware attuale è in uso e se è stato rilevato un downgrade firmware non supportato. Ciò consente di valutare rapidamente lo stato del software e identificare potenziali rischi per il funzionamento, la compatibilità e il supporto.

Funzione - Impostazione	Stato	Raccomandazione
La versione firmware è aggiornata	aggiornamento disponibile	Aggiornare il firmware

Downgrade firmware non supportato

Questo è un controllo per verificare se si è verificato un downgrade firmware non supportato

Funzione - Impostazione	Stato	Raccomandazione
Downgrade firmware non supportato	non rilevato	-

Stato IPv6

Se IPv6 non è richiesto nell'ambiente, dovrebbe essere disattivato per ridurre la superficie di attacco non necessaria e la complessità amministrativa.

Funzione - Impostazione	Stato	Raccomandazione
Stato IPv6	disattivato	-

Stato alta disponibilità

Se l'alta disponibilità non è attivata, se ne consiglia vivamente l'uso per migliorare la resilienza e ridurre i tempi di inattività in caso di guasto hardware o manutenzione. Aiuta a garantire la continuità del servizio e aumenta la disponibilità complessiva dell'infrastruttura di sicurezza.

Funzione - Impostazione	Stato	Raccomandazione
Stato alta disponibilità	presente	-

Linee WAN ridondanti

Se è in uso una sola connessione WAN, si consiglia vivamente una linea WAN aggiuntiva per migliorare la ridondanza e mantenere la connettività Internet in caso di interruzione del provider. Più connessioni WAN aumentano anche la disponibilità complessiva e possono supportare failover o bilanciamento del carico.

Funzione - Impostazione	Stato	Raccomandazione
Linee WAN ridondanti	configurato	-

Configurazione VPN

Questa sezione evidenzia potenziali problemi nella configurazione VPN, come algoritmi di crittografia obsoleti, cifrari deboli o impostazioni legacy. Tali riscontri possono ridurre la sicurezza complessiva della connessione VPN e portare a problemi di compatibilità, conformità o supporto. Si consiglia di rivedere e aggiornare la configurazione VPN per allinearla agli standard di sicurezza e alle best practice attuali.

Funzione - Impostazione	Stato	Raccomandazione
Algoritmi VPN non sicuri utilizzati	sì	Riconfigurare i tunnel VPN

Audit interno del firewall

Questa sezione mostra se la funzione di audit interno è attivata sul firewall SonicWall. Una funzione di audit attivata è importante perché registra le modifiche di configurazione e le azioni amministrative, migliorando tracciabilità e responsabilità. Ciò supporta la risoluzione dei problemi, le indagini di sicurezza e i requisiti di conformità.

Funzione - Impostazione	Stato	Raccomandazione
Audit interno del firewall	attivato	-

Account amministratore integrato utilizzato per l'amministrazione

Se l'audit interno è attivo, questa funzione verifica se l'utente Admin generico è stato rilevato nel log di audit. Si consiglia di utilizzare account personalizzati per l'amministrazione

Funzione - Impostazione	Stato	Raccomandazione
Account amministratore integrato utilizzato per l'amministrazione	sì	utilizzare account pe

Funzioni di rilevamento e prevenzione

Questa sezione mostra se le funzioni di rilevamento e prevenzione sono attivate sul firewall SonicWall.

Funzione - Impostazione	Stato	Raccomandazione
Funzioni di rilevamento e prevenzione	attivato	-

Packet Capture attivo

Questa sezione mostra se Packet Capture è attualmente ancora in esecuzione sul firewall SonicWall.
Una cattura di pacchetti continuamente attiva dovrebbe essere esaminata, poiché potrebbe indicare una risoluzione dei problemi non completata e può consumare risorse di sistema o generare dati di cattura non necessari.
Se non è più necessaria, dovrebbe essere interrotta per evitare sovraccarico non necessario e impatto operativo.

Funzione - Impostazione	Stato	Raccomandazione
Packet Capture attivo	no	-

Protezione degli account

Questa sezione mostra se gli account utente sul firewall SonicWall sono protetti con autenticazione a due fattori (2FA).

Funzione - Impostazione	Stato	Raccomandazione
Account Admin protetto con TOTP	no	Attivare servizio o funzione
Account utente protetti con TOTP	no	Attivare servizio o funzione

Utilizzo del firewall

Il monitoraggio dell'utilizzo complessivo è importante per identificare condizioni di carico elevato che potrebbero influire sulle prestazioni, sulla stabilità o sull'efficacia dei servizi di sicurezza.

Funzione - Impostazione	Stato	Raccomandazione
Utilizzo ultimo minuto	0 %	OK
Utilizzo ultima ora	0 %	OK
Utilizzo ultimo giorno	0 %	OK
Utilizzo ultimo giorno	0 %	OK

Servizi di sicurezza licenziati ma non utilizzati

Questo report mostra il numero di servizi di sicurezza concessi in licenza ma non in uso

Funzione - Impostazione	Stato	Raccomandazione
Numero di servizi	1	Attivare servizio o funzione

Servizio di sicurezza non attivato

Attivare un servizio di sicurezza su una zona mentre il servizio stesso è disattivato globalmente non produce alcuna protezione effettiva. Sebbene la configurazione della zona indichi che il servizio è attivo, il motore sottostante non è in esecuzione, quindi non viene eseguita alcuna ispezione o filtraggio. Ciò può creare un falso senso di sicurezza e portare a policy firewall mal configurate.

Funzione - Impostazione	Stato	Raccomandazione
Servizio di sicurezza non attivato	sì	Attivare servizio o funzione

Impostazioni WAN MTU

Una MTU WAN configurata correttamente è importante per garantire una trasmissione efficiente dei pacchetti e una comunicazione di rete stabile. Se il valore MTU è impostato su un valore troppo basso, può ridurre il throughput, aumentare l'overhead e influire negativamente sulle prestazioni delle applicazioni o delle connessioni VPN.

Funzione - Impostazione	Stato	Raccomandazione
Rilevata dimensione MTU WAN bassa	non rilevato	-

Timeout di connessione TCP

La modifica del timeout TCP globale influisce su ogni sessione TCP elaborata dal firewall. In genere si consiglia di lasciare invariato il valore predefinito e di adattare i timeout solo per le singole regole di accesso quando necessario.

Funzione - Impostazione	Stato	Raccomandazione
Il timeout TCP predefinito è stato modificato	non rilevato	-

Regole firewall non utilizzate da molto tempo

Le regole attualmente non in uso non offrono alcun valore operativo. Per mantenere il framework chiaro ed efficiente, queste regole inutilizzate dovrebbero essere rivalutate ed eliminate ove opportuno

Tipo di regola	Numero di occorrenze
Regole firewall mai utilizzate (IP v4)	0
Regole firewall non utilizzate da molto tempo (IP v4)	21

Regole firewall disattivate

Le regole attualmente non in uso non offrono alcun valore operativo. Per mantenere il framework chiaro ed efficiente, queste regole inutilizzate dovrebbero essere rivalutate ed eliminate ove opportuno

Tipo di regola	Numero di occorrenze
Regole firewall disattivate (IP v4)	0

Regole firewall che consentono l'accesso dal WAN alle reti interne

Le regole firewall che consentono l'accesso dal WAN alla rete interna aumentano l'esposizione e dovrebbero essere limitate solo ai servizi essenziali, con verifica regolare della necessità aziendale

Tipo di regola	Numero di occorrenze
Regole firewall che consentono l'accesso dal WAN alle reti interne (IP v4)	0

Regole ANY <> ANY

Le regole che consentono qualsiasi origine verso qualsiasi destinazione su qualsiasi porta creano un'esposizione eccessiva e dovrebbero essere evitate a meno che non vi sia una necessità aziendale chiaramente giustificata e documentata.

Tipo di regola	Numero di occorrenze
Regole ANY <> ANY (IP v4)	0

Regole che consentono l'accesso di gestione

Le regole che consentono l'accesso di gestione dovrebbero essere rigorosamente limitate a fonti autorizzate e servizi protetti, poiché rappresentano un rischio elevato se esposte troppo ampiamente.

Tipo di regola	Numero di occorrenze
Regole che consentono l'accesso di gestione (IP v4)	4

Policy NAT inutilizzate

Le policy NAT inutilizzate non offrono alcuna funzione attiva e dovrebbero essere riviste regolarmente per determinare se sono ancora necessarie o possono essere rimosse.

Tipo di regola	Numero di occorrenze
Policy NAT inutilizzate (IP v4)	0

Policy NAT disattivate

Le policy NAT inutilizzate non offrono alcuna funzione attiva e dovrebbero essere riviste regolarmente per determinare se sono ancora necessarie o possono essere rimosse.

Tipo di regola	Numero di occorrenze
Policy NAT disattivate (IP v4)	0

Informazioni aggiuntive

- Le regole aggiunte automaticamente sono escluse da questo report

Report di sicurezza

Spiegazione

L'audit di sicurezza si concentra sull'identificazione di potenziali rischi per la sicurezza e debolezze delle policy. Analizza le regole firewall alla ricerca di configurazioni eccessivamente permissive, rileva oggetti inutilizzati o rischiosi e rivede i privilegi utente e i diritti di accesso. L'obiettivo è evidenziare errori di configurazione che potrebbero essere sfruttati o che violano le best practice, fornendo informazioni utili per migliorare la postura di sicurezza complessiva.

Report impostazioni di audit

Spiegazione

Audit interno del firewall
L'audit interno sui firewall è una componente essenziale per mantenere l'integrità operativa, la responsabilità e la sicurezza all'interno di un ambiente di rete. Il firewall rappresenta uno dei punti di controllo più critici in un'organizzazione, e l'audit fornisce visibilità sulle modifiche di configurazione, sugli eventi di accesso e sulle azioni amministrative che influenzano direttamente la postura di sicurezza della rete.

Responsabilità e tracciabilità
I log di audit documentano chi ha effettuato le modifiche, quando sono state effettuate e cosa è stato modificato. Questa tracciabilità garantisce che le responsabilità siano chiaramente assegnate e che qualsiasi errore di configurazione, deviazione dagli standard o modifica non autorizzata possa essere rapidamente identificata e corretta.

Rilevamento di modifiche non autorizzate o rischiose
I firewall influenzano direttamente il controllo degli accessi, la protezione dei dati e il flusso del traffico. L'audit interno consente agli amministratori di rilevare modifiche di configurazione intenzionali o accidentali, aiutando a identificare incidenti di sicurezza, violazioni delle policy o potenziali abusi di privilegi amministrativi.

Supporto alla conformità e alla governance
Molti framework normativi richiedono l'audit di sistemi critici come i firewall. I record di audit interno supportano la conformità a standard rilevanti per settori come finanza, sanità e pubblica amministrazione. Forniscono la prova che le policy vengono seguite e che i meccanismi di protezione sono adeguatamente applicati.

Approfondimento operativo e miglioramento continuo
I log di audit aiutano i team di sicurezza a comprendere la cronologia della configurazione e le tendenze operative. La revisione regolare di questi record consente alle organizzazioni di perfezionare le policy di accesso, identificare problemi ricorrenti e rafforzare le pratiche di gestione delle modifiche.

Indagine sugli incidenti e forense
Quando si verifica un evento di sicurezza, i dati di audit interno sono spesso una delle fonti di prova più preziose. Consentono agli investigatori di ricostruire le azioni intraprese sul firewall, analizzare le cause profonde e determinare se attività dannose o errori umani abbiano contribuito all'incidente.

Conclusione
L'audit interno è necessario per garantire trasparenza, coerenza e responsabilità nelle operazioni del firewall. Migliora la sicurezza, supporta i requisiti normativi, consente una risoluzione dei problemi più rapida e fornisce una base fondamentale per una gestione della rete resiliente.

Report impostazioni di audit

Audit Details

Audit interno:	on
Record di audit trovati nel report TS:	2000
Voce di audit più recente trovata nel report TS:	15.09.2026 16:33:49
Voce di audit più vecchia trovata nel report TS	27.07.2026 08:29:20

Utenti identificati nel log di audit

- UDSAdmin
- admin
- apiuser
- HA Sync

Informazioni aggiuntive

Uso di un account amministratore generico

L'account utente *"admin"* è stato rilevato nei record di audit. Si consiglia di evitare l'uso di account amministratore generici o condivisi per la gestione del firewall. Ogni amministratore dovrebbe invece accedere utilizzando un account personalizzato.

L'uso di identità utente individuali garantisce che le modifiche di configurazione possano essere tracciate

Commento
L'account *HA Sync* è un utente di sistema interno utilizzato esclusivamente per sincronizzare dati di configurazione e operativi tra le appliance in una configurazione ad alta disponibilità (HA). Questo account non è destinato all'accesso manuale o all'uso amministrativo.

Report regole DPI SSL disattivato

Spiegazione

Regole con Deep Packet Inspection disabilitata
La Deep Packet Inspection (DPI) consente al firewall di analizzare il traffico oltre le informazioni di connessione di base, come origine, destinazione e porta. È un importante requisito per l'applicazione dei servizi di sicurezza e il rilevamento delle minacce nel traffico di rete.
Questo report identifica le regole di accesso per le quali la Deep Packet Inspection è disabilitata. Il traffico corrispondente a queste regole può eludere l'ispezione basata sulla DPI e, di conseguenza, potrebbe non beneficiare di tutti i servizi di sicurezza configurati.
La disabilitazione della DPI può essere appropriata per determinati tipi di traffico, ad esempio per motivi di compatibilità, prestazioni o perché il traffico interessato non richiede un'ispezione aggiuntiva. Tuttavia, la DPI dovrebbe normalmente essere disabilitata solo intenzionalmente e per un motivo documentato.
Esaminare le regole elencate in questo report e verificare che la disabilitazione della DPI sia necessaria. Se non esiste un motivo specifico, valutare l'attivazione della DPI per garantire che il traffico sia sottoposto al livello di ispezione di sicurezza previsto.

Regole in cui l'ispezione Client DPI SSL è disattivata

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	DPI Disabled
YES	A	Allow WAN1	LAN	WAN	KlausMeier	any	any	any	True
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	True

- Le regole aggiunte automaticamente sono escluse da questo report

Numero di record: 2

Decrittografia DPI-SSL client

Spiegazione

L'ispezione Client DPI-SSL è una funzione di sicurezza chiave che consente al firewall di ispezionare il traffico HTTPS in uscita crittografato. Senza decrittazione, servizi di sicurezza come Gateway Anti-Virus, Intrusion Prevention, Capture ATP, Content Filtering e Application Control hanno visibilità limitata sulle connessioni crittografate, consentendo potenzialmente alle minacce di eludere l'ispezione.
Questo report verifica se l'ispezione Client DPI-SSL è concessa in licenza e attivata sul firewall. Identifica inoltre le zone su cui l'ispezione client è attiva ed evidenzia eventuali regole di accesso in cui DPI-SSL è stato esplicitamente disattivato. Le eccezioni a livello di regola dovrebbero essere esaminate attentamente, poiché possono creare punti ciechi in cui il traffico crittografato non viene ispezionato e i servizi di sicurezza non possono essere applicati completamente.
Le organizzazioni dovrebbero garantire che l'ispezione Client DPI-SSL sia attivata ove appropriato e che le eccezioni siano limitate ad applicazioni o servizi con requisiti di compatibilità documentati. La revisione regolare della configurazione DPI-SSL aiuta a mantenere la visibilità sul traffico crittografato e riduce il rischio di minacce non rilevate.

Decrittografia DPI-SSL client

```
DPI SSL Licensed:          yes
```

```
La decrittazione SSL per il traffico in uscita è disattivata (!)
```

Decrittografia DPI-SSL client

Zone	DPI SSL Client
LAN	On
WAN	Off
DMZ	Off
VPN	Off
SSLVPN	Off
MULTICAST	Off
DMZ-unsec	Off
DMZ-sec	Off
Test	On
150971-Test	Off
060466	Off

Regole in cui l'ispezione Client DPI SSL è disattivata

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	DPI-SSL Client Disabled
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	True
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	True
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	True

- Le regole aggiunte automaticamente sono escluse da questo report

Numero di record: 3

Funzioni di rilevamento e prevenzione

Spiegazione

Le opzioni Randomize IP ID e Enable Stealth Mode forniscono protezione aggiuntiva contro la ricognizione di rete e alcune classi di attacchi. La randomizzazione del campo IP Identification rende più difficile per gli aggressori eseguire il fingerprinting del sistema operativo o dedurre i pattern di traffico, mentre lo Stealth Mode impedisce al firewall di rispondere a tentativi di connessione non richiesti, riducendo la sua visibilità su reti non attendibili.

Funzioni di rilevamento e prevenzione

Stealth Mode

Stealth Mode attivato	on

Randomize IP ID

Randomize IP ID attivato	on

Regole che consentono qualsiasi destinazione e qualsiasi porta (IPv4)

Spiegazione

Perché le regole firewall che consentono "Any" sono rischiose
Nell'ambito della sicurezza di rete, le regole firewall svolgono un ruolo fondamentale nel controllare il traffico in entrata e in uscita da una rete. Una pratica comune, ma fortemente sconsigliata, è l'implementazione di regole "any to any". Queste regole consentono un flusso di traffico illimitato da qualsiasi origine a qualsiasi destinazione, permettendo essenzialmente a tutti i tipi di pacchetti dati di passare attraverso il firewall senza alcun filtraggio.

Implicazioni per la sicurezza *La preoccupazione principale relativa alle regole "any to any" è il rischio significativo per la sicurezza che comportano. I firewall sono progettati per fungere da gatekeeper, esaminando il traffico in entrata e in uscita per proteggere la rete da accessi non autorizzati, attacchi informatici e altre attività dannose. Impostando regole che consentono indiscriminatamente tutto il traffico, la funzione essenziale del firewall viene aggirata, esponendo la rete a potenziali minacce. Questo gateway aperto può essere sfruttato dagli aggressori per accedere a informazioni sensibili, iniettare malware o lanciare altri exploit dannosi.*

Mancanza di controllo del traffico *Oltre alle vulnerabilità di sicurezza, le regole "any to any" ostacolano la capacità di monitorare e controllare efficacemente il traffico di rete. Una gestione efficace della rete si basa sulla comprensione e sulla gestione del flusso di dati. Le regole illimitate rendono difficile tracciare, analizzare o dare priorità al traffico, causando potenziali problemi di prestazioni di rete, inclusa la congestione della larghezza di banda e una ridotta efficienza.*

Conformità e best practice *In molti settori, i requisiti normativi impongono un controllo e un monitoraggio rigorosi del traffico dati. Le regole "any to any" possono violare gli standard di conformità, portando a ripercussioni legali e reputazionali. Inoltre, le best practice di cybersecurity promuovono un principio del privilegio minimo, in cui è consentito solo il traffico necessario, evidenziando ulteriormente la sconsigliabilità di tali regole permissive.*

Raccomandazione *Invece di adottare regole "any to any", si consiglia di implementare regole firewall specifiche e ben definite basate sul principio del privilegio minimo. Queste regole dovrebbero essere adattate per consentire solo il traffico necessario e legittimo richiesto per le operazioni aziendali, garantendo sia la sicurezza della rete che prestazioni ottimali.*

Regole che consentono qualsiasi destinazione e qualsiasi porta (IPv4)

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	
YES	A	Allow WAN1	DMZ-sec	WAN	any	any	Enhanced TV	any	
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	
YES	A	Allow WAN1	DMZ-unsec	WAN	any	any	Citrix UDP	any	
YES	A	Allow Citrix	any		any	any	Citrix UDP	any	Example any<> any
YES	A	Allow FTP	any		any	any	FTP	any	

- Le regole aggiunte automaticamente sono escluse da questo report

Numero di record: 5

Regole firewall che consentono servizi di gestione da reti non attendibili (IPv4)

Spiegazione

Regole firewall che consentono servizi di gestione da reti non attendibili
Servizi di gestione come SSH (Secure Shell), HTTPS (Hypertext Transfer Protocol Secure) e interfacce di amministrazione simili sono destinati all'accesso privilegiato. Consentirli direttamente da reti non attendibili introduce molteplici problemi di sicurezza.

Perché tali regole sono rischiose:
Esposizione ad attacchi
Consentire l'accesso ai servizi di gestione tramite Internet li espone ad attacchi come tentativi di login a forza bruta, sfruttamento di vulnerabilità software o attacchi denial-of-service mirati al servizio.

Elevazione dei privilegi
Se un aggressore riesce a connettersi a un servizio di gestione, potrebbe ottenere l'accesso a livello di amministratore. Ciò potrebbe consentirgli di modificare le configurazioni del firewall, creare meccanismi di accesso persistenti o interrompere le comunicazioni di rete.

Sniffing e intercettazione
I protocolli di gestione non crittografati possono consentire agli aggressori di intercettare informazioni sensibili. Anche i servizi crittografati possono essere a rischio se le chiavi sono esposte, viene utilizzata una crittografia obsoleta o esistono difetti di implementazione.

Mancanza di monitoraggio
Le interfacce di gestione spesso non vengono monitorate con la stessa attenzione dei sistemi rivolti agli utenti, aumentando la probabilità che l'accesso non autorizzato rimanga inosservato.

Complessità ed errore umano
Maggiore è il numero di servizi esposti esternamente, maggiore è il rischio di errori di configurazione o errori operativi, che possono portare all'esposizione accidentale di sistemi critici.

Best practice consigliate
L'accesso di gestione dovrebbe essere limitato rigorosamente alle reti interne attendibili. Se è necessaria l'amministrazione remota, dovrebbe essere effettuata tramite canali di accesso sicuri come connessioni VPN con crittografia forte. L'autenticazione a più fattori dovrebbe essere implementata ove possibile, i servizi di gestione dovrebbero essere monitorati attivamente per tentativi di accesso non autorizzato e i dispositivi devono essere mantenuti aggiornati con le patch attuali per mitigare le vulnerabilità note.

Regole firewall che consentono servizi di gestione da reti non attendibili (IPv4)

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	
YES	A	Test 24	WAN	060466	any	any	any	OSPF	
YES	A	Test 25	WAN	060466	any	any	any	POP3 (Retrieve E-Mail)	
YES	A	Test 23	WAN	060466	any	any	any	MSN	
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Temp, Rule to allow M...

- Le regole aggiunte automaticamente sono escluse da questo report

Numero di record: 4

Opzioni di accesso alla gestione

Spiegazione

Opzioni di accesso alla gestione e considerazioni sulla sicurezza

Sono disponibili diversi metodi per accedere alla gestione del firewall, ciascuno con vantaggi di usabilità e implicazioni di sicurezza diverse. Poiché le interfacce di gestione del firewall forniscono il controllo amministrativo su infrastrutture di rete critiche, un'esposizione impropria di questi metodi di accesso può introdurre rischi significativi.

L'accesso non autorizzato alla gestione del firewall può comportare la manipolazione della configurazione, la divulgazione di parametri di sicurezza sensibili o persino la completa compromissione dell'ambiente di rete. Per questo motivo, è essenziale rivedere regolarmente quali meccanismi di accesso di gestione sono abilitati e garantire che rimangano accessibili solo metodi sicuri, giustificati e adeguatamente protetti.

Limitare l'accesso di gestione a reti attendibili, applicare un'autenticazione forte e monitorare l'attività amministrativa sono pratiche chiave per mantenere un panorama di configurazione sicuro e controllato.

Opzioni di accesso alla gestione

Central Management

Central Management (NSM / GMS):	off
NSM ZeroTouch:	enabled

SSL-VPN

SSL VPN Web Management:	on
SSL VPN SSH Management:	off

API

API access:	enabled

Opzioni di accesso alla gestione: Gestione interfacce

Interface	Zone	HTTP	HTTPS	PING	SSH	SNMP	API
X0	LAN	off	on	on	on	on	on
X1	WAN	off	on	on	on	off	on
X2	DMZ-unsec	off	on	on	off	off	on
X3	DMZ-sec	off	on	on	off	off	on
X4	HA Data & Control	off	off	off	off	off	off
X5	WAN	off	off	on	off	off	off
X6	LAN	off	on	on	off	off	on
X7	DMZ-sec	off	off	off	off	off	off
X6:V100	LAN	off	off	off	off	off	off

Opzioni di accesso alla gestione: IPSec (VPN)

Tunnel-Name	Enabled	HTTP	HTTPS	SSH	SNMP
WAN GroupVPN	False	off	off	off	off
SNWL Policy Mode	False	off	on	on	on
Test	False	off	off	off	off
Bad Tunnel	False	off	off	off	off
To TZ570	True	off	off	off	off
Remote Site1	True	off	off	off	off
New York	True	off	off	off	off

Servizi di sicurezza - Panoramica attivati e disattivati

Spiegazione

Servizi di sicurezza attivi
Questo report mostra quali servizi di sicurezza sono attualmente attivati sul dispositivo. Tuttavia, l'attivazione a livello di sistema indica solo che la funzionalità del servizio è disponibile, non garantisce che il traffico venga effettivamente ispezionato.

Per analizzare efficacemente il traffico, i servizi di sicurezza devono anche essere esplicitamente assegnati alle zone o applicati a regole firewall specifiche. Senza questo passaggio di configurazione, le tecnologie attivate potrebbero rimanere inattive per i flussi di rete rilevanti, con conseguente riduzione della copertura di protezione.

Stato servizio di sicurezza

Deep Packet Inspection for SSL (DPI-SSL)	Off
Gateway AV	On
Anti-Spyware	On
Intrusion Prevention	On
App Control	On
Content Filtering Service	On
GeoIP Filtering	On

Informazioni aggiuntive

Nessun tunnel VPN Route-All configurato

Non è attualmente configurato e attivo alcun tunnel VPN route-all. Si tratta di uno scenario comune in ambienti in cui tutto il traffico viene inoltrato a un dispositivo di sicurezza upstream, responsabile dell'ispezione del traffico, dell'applicazione delle policy e dell'elaborazione di sicurezza aggiuntiva.

In tali configurazioni, il firewall funziona principalmente come dispositivo di routing o segmentazione, mentre l'ispezione più approfondita è gestita da una soluzione di sicurezza centralizzata, come un secure web gateway, un servizio di sicurezza cloud o una piattaforma di ispezione dedicata.

Servizi di sicurezza - Assegnazione per zona

Spiegazione

Servizi di sicurezza
Questo report mostra quali servizi di sicurezza sono attivati su ciascuna zona. Sebbene l'attivazione globale di un servizio ne renda disponibile la funzionalità, la protezione effettiva viene applicata solo se il servizio è assegnato attivamente a livello di zona.

I servizi di sicurezza associati alle zone determinano quali segmenti di rete ricevono l'ispezione per minacce come malware, tentativi di intrusione o contenuti indesiderati. Le zone senza le corrispondenti assegnazioni di servizio potrebbero rimanere insufficientemente protette, anche se la funzione è attivata sul sistema.

Questa panoramica aiuta a identificare le lacune di copertura, verificare che le zone critiche (come LAN o aree di accesso VPN) siano adeguatamente protette e garantire che le policy di ispezione siano allineate con i requisiti di sicurezza organizzativi.

Informazioni aggiuntive

I servizi di sicurezza contrassegnati con (!) sono attivati sulla zona ma disattivati globalmente.

Servizi di sicurezza - Assegnazione per zona

Zone	ClientAV	GatewayAV	IPS	AntiSpyware	DPI SSL Client	DPI SSL Server	SSLControl
LAN	Off	On	On	On	On (!)	Off	Off
WAN	Off	On	On	On	Off	On (!)	Off
DMZ	Off	Off	Off	Off	Off	Off	Off
VPN	Off	Off	Off	Off	Off	Off	Off
SSLVPN	Off	Off	Off	Off	Off	Off	Off
MULTICAST	Off	Off	Off	Off	Off	Off	Off
DMZ-unsec	Off	Off	Off	Off	Off	Off	Off
DMZ-sec	Off	Off	Off	Off	Off	Off	Off
Test	Off	On	On	On	On (!)	Off	Off
150971-Test	Off	Off	Off	Off	Off	Off	Off
060466	Off	On	On	On	Off	Off	Off

Protezione degli account utente

Spiegazione

Panoramica protezione account utente
Questo report elenca tutti gli account utente e indica come sono protetti, inclusa l'informazione se l'autenticazione a due fattori (2FA) è attivata. Ciò aiuta a verificare la solidità dei meccanismi di autenticazione e a identificare gli account che potrebbero richiedere protezione aggiuntiva.

Protezione degli account utente

Nome utente	TOTP attivato
admin	**NO**
All LDAP Users	NO
apiuser	NO
Isabel	NO
LocalAdmin	YES
mschmitz	NO
Robert	NO
Sylvia	NO
Udo	NO
Uwe	NO
Webadmin	NO

Metodi di autenticazione esterna degli utenti

Spiegazione

Panoramica configurazione autenticazione esterna
Questo report elenca quali sistemi di autenticazione esterna sono configurati, se sono attivati, ed evidenzia eventuali potenziali problemi di sicurezza relativi alla loro configurazione. L'autenticazione esterna può rafforzare significativamente la gestione dell'identità utente se implementata correttamente, ma una configurazione errata può introdurre rischi operativi e di sicurezza.

LDAP (Lightweight Directory Access Protocol)
Quando viene utilizzato LDAP, le richieste di autenticazione vengono inoltrate a una directory esterna come Microsoft Active Directory. L'uso di LDAP centralizza l'identità utente e la gestione delle password, riducendo la dipendenza dagli account locali. Tuttavia, l'autenticazione LDAP dovrebbe sempre essere protetta tramite TLS (LDAPS). La comunicazione LDAP non crittografata espone nomi utente, password e informazioni sull'appartenenza ai gruppi all'intercettazione, aumentando il rischio di furto di credenziali.

Autenticazione RADIUS
RADIUS è comunemente utilizzato per l'accesso VPN e i servizi di autenticazione centralizzati. Supporta metodi challenge-response, logging centralizzato e applicazione standardizzata delle policy di autenticazione. I rischi per la sicurezza sorgono quando i segreti condivisi sono deboli o riutilizzati su più sistemi. Inoltre, se i server RADIUS diventano non disponibili, l'accesso potrebbe essere interrotto a meno che non siano configurati adeguati meccanismi di fallback.

Autenticazione TACACS+
TACACS+ è tipicamente utilizzato per l'autenticazione amministrativa, specialmente in ambienti aziendali. Separa le funzioni di autenticazione, autorizzazione e accounting (AAA), garantendo attività amministrativa tracciabile e controllo granulare dei privilegi. Sebbene sicuro per design, TACACS+ richiede una configurazione corretta di canali crittografati e chiavi univoche. Interruzioni centrali di TACACS+ possono bloccare l'accesso amministrativo a meno che non sia presente ridondanza.

Configurare e proteggere correttamente i sistemi di autenticazione esterna aiuta a migliorare la responsabilità, ridurre la complessità di gestione e rafforzare la sicurezza complessiva degli accessi. La revisione regolare della disponibilità, delle impostazioni di crittografia, della mappatura delle policy di autenticazione e del comportamento di fallback garantisce processi di autenticazione affidabili e sicuri in tutto l'ambiente.

LDAP

Server	Enabled	TLS	UserName
udsserver.uds.local	on	on	UDSReadDir

Radius

Server	Enabled	VPN
10.10.33.11	off	off(!)

Tacacs

Server	Enabled	VPN
1.2.3.4	off	off(!)

Panoramica utenti amministrativi

Spiegazione

Utente amministrativo
Questo report elenca tutti gli utenti che dispongono di privilegi amministrativi. Gli account con diritti amministrativi hanno accesso elevato alle impostazioni di configurazione, alle modifiche delle policy, alle informazioni sensibili e alle funzioni di gestione del sistema.
La revisione di questi utenti garantisce che solo il personale autorizzato mantenga l'accesso privilegiato e supporta la conformità, la responsabilità e le pratiche di controllo degli accessi sicure.

Users with Full Admin Rights

UDSAdmin

mschmitz

Webadmin

LocalAdmin

Uwe

apiuser

UDS-SNWL-Admins@uds.local

Users with Limited Admin Rights

- no entries -

Users with Read-Only Admin Rights

Udo

Users with Guest Admin Rights

Robert

Sylvia

Informazioni aggiuntive

Avviso importante riguardante le assegnazioni ai gruppi LDAP
Se i diritti amministrativi sono assegnati a gruppi LDAP, tutti i membri di tali gruppi ereditano automaticamente i privilegi di amministratore. Ciò significa che qualsiasi modifica all'appartenenza LDAP - come l'aggiunta di nuovi utenti o la sincronizzazione di strutture di directory esterne - potrebbe concedere involontariamente un accesso elevato.

La revisione regolare delle assegnazioni ai gruppi e dell'appartenenza è essenziale per garantire che solo il personale autorizzato riceva privilegi amministrativi e che il controllo degli accessi rimanga allineato con le policy di sicurezza organizzative.

Best practice per la sicurezza VPN

Spiegazione

Sicurezza VPN
Le reti private virtuali (VPN) sono essenziali per proteggere i dati attraverso reti non attendibili. Per rimanere efficaci, le loro impostazioni crittografiche devono essere riviste e aggiornate regolarmente. Metodi obsoleti indeboliscono la sicurezza, riducono la conformità ed espongono le organizzazioni a rischi inutili.

Perché i controlli regolari sono importanti:

- Sicurezza:
Le minacce informatiche evolvono rapidamente. Metodi di crittografia o autenticazione obsoleti possono essere compromessi con la potenza di calcolo moderna.
- Conformità:
Molti settori richiedono una crittografia forte per soddisfare i requisiti normativi.
- Controllo degli accessi:
Un'autenticazione forte impedisce l'uso non autorizzato della VPN.
- Protezione dei dati:
Una crittografia aggiornata garantisce riservatezza e integrità delle informazioni sensibili.
- Prestazioni e prontezza futura:
Gli standard più recenti aumentano non solo la sicurezza, ma anche l'efficienza e la scalabilità.

Elementi non sicuri da evitare:
- Cifrari simmetrici:
DES e 3DES sono obsoleti e vulnerabili.
- Gruppi Diffie-Hellman (DH):
I gruppi 1 (768 bit), 2 (1024 bit) e 5 (1536 bit) sono troppo deboli.
- Versioni IKE:
IKEv1 è obsoleto; si consiglia IKEv2.
- Funzioni hash:
MD5 e SHA-1 sono considerati compromessi e non più sicuri.
- Gestione delle chiavi:
Le chiavi precondivise (PSK) deboli o statiche sono facili da indovinare o violare con la forza bruta.

Opzioni sicure consigliate

- Crittografia:
- AES-128 o AES-256.
- Scambio di chiavi:
- Gruppi DH ≥ 2048 bit o Elliptic Curve Diffie-Hellman (P-256/P-384).
- Protocollo:
- IKEv2 per configurazioni VPN moderne.
- Integrità:
- SHA-256 o superiore.
- Autenticazione:
Preferire i certificati; se si usano PSK, utilizzare chiavi forti e casuali.

Conclusione
Le VPN sono sicure quanto le loro fondamenta crittografiche. Evitando algoritmi deboli e adottando standard moderni, si proteggono i dati sensibili, si soddisfano i requisiti di conformità e si prepara la rete alle sfide future. Rivedere e aggiornare regolarmente la configurazione VPN per rimanere sicuri.

Spiegazione

(!) = non sicuro © = attenzione

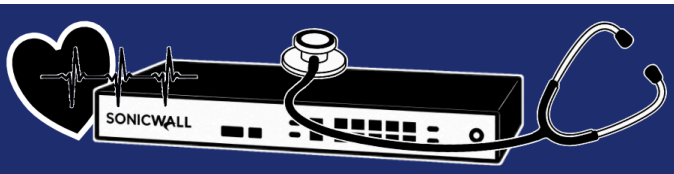
Best practice per la sicurezza VPN

Ena	Name	Phase1 Exchange Mode	Phase1 DH-Group	Phase 1 Encr	Phase1 Auth	Phase2 Protcl	Phase2 Encr	Phase2 Auth	Phase 2 PFS	Phase 2 DH-Group
yes	New York	Main (!)	224-Bit R ECP Group	AES-128 (C)	MD5 (!)	ESP	DES (!)	AES-XCBC (C)	off (!)	Group 2 (!)
yes	Remote Site1	IKEv2	Group 2 (!)	AESCGM16-256 (C)	SHA-1 (!)	ESP	AESGMAC-128	n/a	off (!)	Group 2 (!)
yes	To TZ570	IKEv2	Group 1 (!)	AES-256	SHA-1 (!)	ESP	AES-256	n/a	on	n/a

Impostazioni crittografiche policy VPN – Algoritmi non sicuri utilizzati

Unsafe		
Category	**Type**	**Comment**
DH Group	192-Bit R ECP Group	Too small ECC group
Encryption	DES	Broken unsafe
IKE	Aggressive	Leads to info leaks insecure
Integrity	MD5	Broken collisions possible
Integrity	SHA-1	Deprecated collision attacks
Misc	None	No encryption integrity

Not recommended		
Category	**Type**	**Comment**
DH Group	224-Bit R ECP Group	Borderline ECC group aging out
Encryption	3DES	Legacy slow 112-bit effective strength
Encryption	AES-XCBC	Niche less common not widely supported
IKE	Main	Standard for IKEv1 secure but older
Protocol	AH	Rarely used integrity only no encryption



Report sullo stato di salute

Spiegazione

Il report di manutenzione aiuta a identificare gli elementi di configurazione che dovrebbero essere rivisti regolarmente per mantenere il firewall pulito, efficiente e facile da gestire. Nel tempo, le configurazioni firewall crescono naturalmente man mano che vengono aggiunte nuove regole, oggetti, VPN e servizi. Senza una manutenzione periodica, le voci obsolete o inutilizzate possono accumularsi, aumentando il carico amministrativo e rendendo la risoluzione dei problemi più difficile.
Questo report evidenzia gli elementi di configurazione che potrebbero richiedere attenzione, come regole firewall disattivate o inutilizzate, policy NAT inattive, oggetti indirizzo e servizio inutilizzati, servizi di sicurezza scaduti e altri elementi di configurazione non più attivamente utilizzati. Identifica anche le impostazioni che potrebbero beneficiare di ottimizzazione o pulizia.
Lo scopo di questo report non è raccomandare la rimozione automatica di ogni elemento elencato. Fornisce invece agli amministratori una panoramica strutturata dei componenti di configurazione che dovrebbero essere verificati prima di apportare qualsiasi modifica. Alcuni oggetti o regole potrebbero comunque essere necessari per progetti futuri, ambienti temporanei, procedure di disaster recovery o servizi utilizzati raramente.
La manutenzione regolare offre diversi vantaggi importanti:
- Riduce la complessità della configurazione e migliora la leggibilità.
- Rende la risoluzione dei problemi e l'audit significativamente più semplici.
- Aiuta a identificare elementi di configurazione obsoleti o dimenticati.
- Riduce il rischio di errori di configurazione accidentali.
- Migliora la gestibilità a lungo termine del firewall.
- Supporta un ambiente di sicurezza ben documentato e mantenuto professionalmente.
Un firewall ben mantenuto è più facile da amministrare, più facile da sottoporre ad audit e fornisce una base più solida per future modifiche di configurazione e miglioramenti della sicurezza.

Analisi dell'utilizzo del firewall

Spiegazione

Analisi dell'utilizzo del firewall
Questi grafici illustrano il livello di utilizzo del firewall nel periodo precedente l'esportazione dei dati. Un utilizzo elevato può portare a un degrado delle prestazioni, inclusi ritardi nell'elaborazione del traffico o pacchetti persi. Per ottenere informazioni significative, il Technical Support Report utilizzato come fonte di dati dovrebbe idealmente essere generato durante un periodo di elevato carico di sistema.

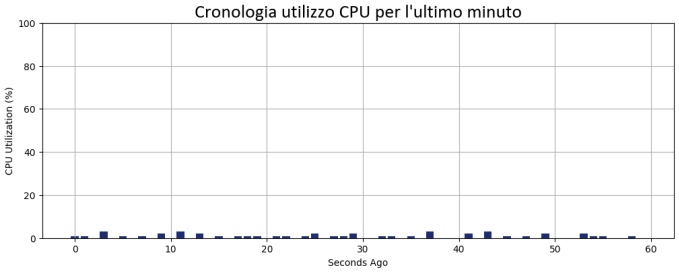
Fonti di dati consigliate
Statistiche di utilizzo più accurate si ottengono in genere da sistemi di monitoraggio esterni basati su NetFlow o SNMP. Per il reporting basato su NetFlow, SonicWall fornisce una soluzione dedicata denominata *Analytics*, che si integra perfettamente con i firewall SonicWall.

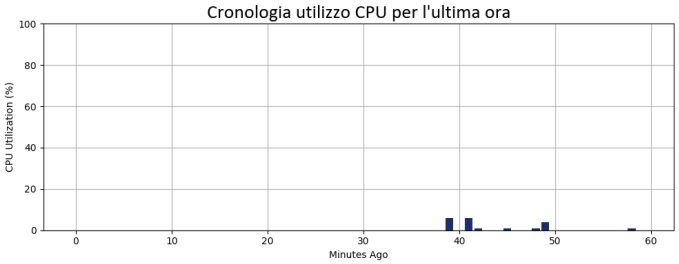
Considerazioni importanti per gli ambienti HA
Se i valori di utilizzo mancano per l'intervallo di tempo selezionato, verificare se il firewall opera in un cluster ad alta disponibilità (HA). Quando l'unità in standby diventa attiva durante il periodo di reporting, i dati di utilizzo potrebbero non essere acquisiti sul dispositivo previsto, con conseguenti informazioni grafiche incomplete o mancanti.

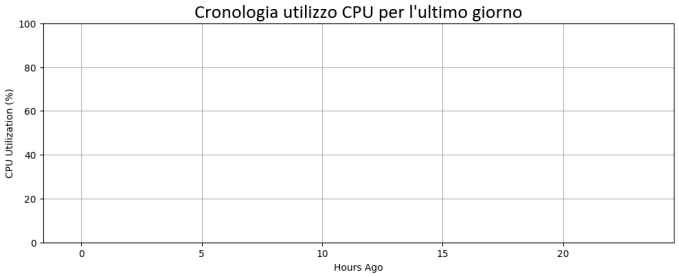
Analisi dell'utilizzo del firewall

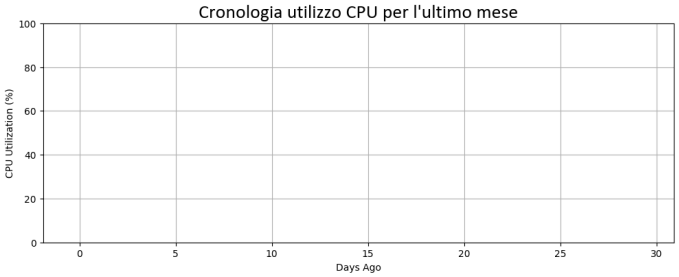
Intervallo di tempo	Media	Stato
Minuto:	0 %	OK
Ora:	0 %	OK
Giorno:	0 %	OK
Mese:	0 %	OK

Grafici di utilizzo delle prestazioni









Firmware Version Check

Spiegazione

Confronto versione firmware
Questa sezione confronta la versione firmware attualmente installata con l'ultima versione disponibile su MySonicWall. Ciò aiuta a determinare se il dispositivo è aggiornato, richiede un upgrade consigliato o esegue una build software obsoleta che potrebbe non disporre di miglioramenti, correzioni di bug o miglioramenti della sicurezza.

Firmware Version Check:

```
Firmware Installed on Firewall:  7.3.0-7012-R8150
Latest Firmware on MySonicWall:  7.3.3-7015
Firmware Release Date:           26.06.2026
Release Note URL:
https://software.sonicwall.com/Firmware/Documentation/232-006386-00_RevJ_SonicOS_7.3_ReleaseNotes.pdf
```

Informazioni aggiuntive

Il firmware 7.3.3-7015 è disponibile su MySonicWall.com, si consiglia di eseguire l'upgrade a quella versione

Panoramica cronologia configurazione e firmware

Spiegazione

Panoramica cronologia configurazione e firmware
La tabella seguente fornisce una panoramica degli stati di configurazione passati e delle versioni firmware implementate sul dispositivo. Evidenzia la frequenza con cui le impostazioni sono state migrate e se si sono verificati downgrade del firmware non supportati.

Downgrade non supportati
Un downgrade del firmware è considerato non supportato se non è stata successivamente importata alcuna configurazione dalla versione firmware declassata. In tali casi, la compatibilità del sistema non può essere garantita e possono verificarsi problemi operativi.

Impatto di configurazioni obsolete o migrate frequentemente
Le configurazioni migrate ripetutamente o utilizzate su più dispositivi possono accumulare gradualmente incoerenze o parametri obsoleti. Ciò può portare a comportamenti imprevisti, prestazioni degradate o errori di elaborazione della configurazione durante future migrazioni o aggiornamenti.

Firmware	TimeStamp	Action	Comment
7.0.1-5145-2363	24.01.2024 01:33:01	Settings import	
7.1.1-7040-5387	24.01.2024 08:25:53	Firmware applied	
7.1.1-7047-5557	01.03.2024 07:37:45	Firmware applied	
7.1.1-7047-5557	27.11.2024 18:21:03	Settings import	
7.1.1-7058-6162	03.12.2024 20:01:06	Firmware applied	
7.1.1-7058-6162	05.02.2025 21:58:08	Settings import	
7.1.1-7058-6162	21.03.2025 16:23:00	Settings import	
7.1.3-7015-6965	31.03.2025 21:24:27	Firmware applied	
7.3.0-7012-8150	08.09.2025 18:29:24	Firmware applied	
7.3.0-7012-8150	10.03.2026 14:38:34	Settings import	
7.3.0-7012-8150	10.03.2026 16:27:54	Settings import	
7.3.0-7012-8150	11.03.2026 02:01:27	Settings import	
7.3.0-7012-8150	11.03.2026 09:10:26	Settings import	
7.3.0-7012-8150	11.03.2026 11:03:15	Settings import	
7.3.0-7012-8150	21.05.2026 21:28:13	Settings import	

Informazioni aggiuntive

Nessun downgrade firmware non supportato rilevato

Panoramica cronologia configurazione e firmware

Spiegazione

Panoramica conversione configurazione
Questo report indica se le impostazioni di configurazione sono state convertite utilizzando il Conversion Tool di SonicWall. Ciò aiuta a identificare le configurazioni migrate e fornisce informazioni su se le impostazioni provengono da piattaforme precedenti o deployment precedenti.

Details

```
Le impostazioni sono state convertite in passato: No
```

Affidabilità - Alta disponibilità

Spiegazione

Importanza dell'alta disponibilità nei sistemi firewall

1. Applicazione continua della sicurezza
L'alta disponibilità (HA) garantisce il funzionamento ininterrotto dei sistemi firewall, mantenendo controlli di sicurezza continui anche durante problemi hardware, aggiornamenti o manutenzione pianificata. Ciò previene lacune nel rilevamento delle minacce, nella convalida degli accessi e nell'applicazione delle policy.

2. Riduzione dei tempi di inattività
In una configurazione HA, un firewall secondario subentra automaticamente se l'unità primaria diventa non disponibile. Questo failover senza interruzioni riduce al minimo i tempi di inattività, garantendo un accesso ininterrotto ad applicazioni e servizi critici.

3. Maggiore affidabilità del sistema
Avere più firewall che operano in una coppia ridondante aumenta la resilienza contro guasti hardware, corruzione della configurazione o interruzioni impreviste. L'affidabilità dell'infrastruttura di sicurezza di rete è significativamente migliorata.

4. Supporto alla continuità operativa
Le organizzazioni che dipendono da connettività in tempo reale, accesso cloud e servizi online non possono tollerare interruzioni di rete prolungate. L'HA protegge le operazioni aziendali mantenendo attiva l'applicazione della sicurezza durante eventi operativi e scenari di guasto.

5. Vantaggi prestazionali con la distribuzione del carico
Alcuni ambienti HA supportano la distribuzione del carico, migliorando il throughput bilanciando sessioni o percorsi di traffico su più appliance. Ciò evita colli di bottiglia nell'elaborazione e aumenta le prestazioni complessive della rete.

6. Capacità di disaster recovery
L'HA svolge un ruolo cruciale nella pianificazione del disaster recovery. Quando un dispositivo primario si guasta, l'unità secondaria mantiene attive le policy, il routing, i tunnel VPN e i servizi di sicurezza, riducendo l'impatto operativo durante le attività di recovery.

7. Allineamento normativo e di conformità
Molti settori richiedono una disponibilità garantita dei controlli di sicurezza e meccanismi di failover tracciabili. L'implementazione dell'HA supporta le iniziative di conformità, la preparazione agli audit e gli impegni sui livelli di servizio.

8. Migliore esperienza utente e cliente
Con un accesso di rete ininterrotto, gli utenti sperimentano meno interruzioni del servizio e un ripristino più rapido dopo i guasti. Ciò contribuisce direttamente a livelli di soddisfazione più elevati e a un'erogazione del servizio più stabile.

Riepilogo
L'alta disponibilità nei sistemi firewall è una base fondamentale per la resilienza aziendale. Garantisce protezione continua, riduce al minimo i tempi di inattività operativi, supporta il disaster recovery, migliora le prestazioni e consente la conformità. Riducendo le interruzioni del servizio e mantenendo una connettività sicura, l'HA migliora significativamente sia l'efficacia operativa che quella di sicurezza.

Affidabilità - Alta disponibilità

High Availability Settings

High Availability:	Enabled
HA Primary Serial-Number:	0040103CD830
HA Secondary Serial-Number:	0040103F5B1C
HA Stateful Sync:	Enabled
HA Preempt Mode:	Disabled
HA Control Interface:	X4
HA Data Interface:	X4
HA Role:	Primary
HA Firmware mismatch with peer:	No
HA Active Time:	0 Days 00:21:47

High Availability Status

HA Firewall Status:	Active
HA Peer State:	Peer not found / not active
HA Peer in sync:	No

Informazioni sul ciclo di vita del prodotto

Spiegazione

Informazioni sul ciclo di vita del prodotto
Questa sezione fornisce informazioni sullo stato attuale del ciclo di vita del prodotto. Aiuta a determinare se un dispositivo è completamente supportato, si sta avvicinando alla fine del supporto o si trova già oltre il suo periodo di manutenzione ufficiale.

Per descrizioni dettagliate del ciclo di vita, tappe importanti e programmi di supporto attuali, fare riferimento alla documentazione ufficiale sul ciclo di vita del prodotto SonicWall disponibile tramite le risorse di supporto SonicWall.

Description	Value
Model:	SonicWall NSA NSV 270
Last Order Date:	15.04.2022
ARM Begin:	16.04.2022
LRM Begin:	16.04.2024
1 Year LOD:	15.04.2025
End of Support:	16.04.2026

Informazioni aggiuntive

Verificare nuovamente queste informazioni sul sito web ufficiale di SonicWall!

Servizi di sicurezza - Panoramica stato licenza

Spiegazione

Licenze dei servizi di sicurezza
Questo report mostra quali servizi dispongono attualmente di una licenza attiva. I servizi con licenza sono completamente funzionali e in grado di fornire la protezione o il set di funzionalità previsti. I servizi senza una licenza valida potrebbero avere funzionalità limitate o essere completamente inattivi.

Questa vista aiuta a verificare se le funzionalità di sicurezza e basate su abbonamento richieste rimangono operative e assiste nella pianificazione dei rinnovi per evitare interruzioni del servizio.

Servizi di sicurezza - Panoramica stato licenza

Nome servizio	Stato licenza	Conteggio	Scadenza
Node Upgrade	None		Unlimited
Active/Active Clustering Service	None		Unlimited
NSM Essential (Retired)	Not Licensed		Unlimited
NSM Advanced (Retired)	Disabled		05.02.2026
Capture Client Basic	Not Licensed		Unlimited
Content Filtering Client	None		Unlimited
Capture Client Advanced	Not Licensed		Unlimited
Capture Client Premier	Not Licensed		Unlimited
Deep Packet Inspection for SSL (DPI-SSL)	Licensed		Unlimited
Deep Packet Inspection for SSH (DPI-SSH)	None		Unlimited
Virtual Assist	None		Unlimited
SSL VPN	Licensed	2 Max: 100	Unlimited
Global VPN Client	Licensed	50 Max: 1000	Unlimited
Global VPN Client Enterprise	None		Unlimited
WAN Acceleration Client	None		Unlimited
WAN Acceleration Software	None		Unlimited
Botnet Block	None		Unlimited
Stateful High Availability	Licensed		Unlimited
Comprehensive Anti-Spam Service	None		Unlimited
External IDS Support	None		Unlimited
CSC Analytics (includes Reporting)	None		Unlimited
CSC Management	None		Unlimited
CSC Management Lite	None		Unlimited
CSC Management and Reporting	None		Unlimited
CSC Management and 7-day Reporting	None		Unlimited
Syslog Analytics	Expired		03.02.2024
Comprehensive/Advanced Gateway Security Suite	None		Unlimited
Gateway AV	None		Unlimited
Anti-Spyware	None		Unlimited
Intrusion Prevention	None		Unlimited
App Control	None		Unlimited
App Visualization	None		Unlimited
Content Filtering: Premium Edition	None		Unlimited
Analyzer	None		Unlimited
Capture Advanced Threat Protection	Licensed		14.02.2027
Standard Support	Not Licensed		Unlimited
24x7 Support	Licensed		14.02.2027
SonicOS Expanded	None		Unlimited
Software and Firmware Updates	None		Unlimited
Hardware Warranty	None		Unlimited
Remote Implementation Service	None		Unlimited
Gateway Anti-malware/Intrusion Prevention/App Control	Licensed		14.02.2027
Content Filtering Service	Licensed		14.02.2027
Secure Connect Lite	None		Unlimited
Secure Connect	None		Unlimited
Advanced Reporting & Analytics (7 days)	Licensed		14.02.2027
DNS Filtering	Licensed		14.02.2027

Servizi di sicurezza - Panoramica stato licenza

Nome servizio	Stato licenza	Conteggio	Scadenza
Advanced Protection Security Suite	Licensed		14.02.2027
Managed Protection Security Suite	Not Licensed		Unlimited
Web and Chat Only Support	None		Unlimited
Basic Reporting (7 days)	Not Licensed		Unlimited
Essential Protection Service Suite	Disabled		05.02.2026
Advanced Reporting & Analytics	None		Unlimited
Threat Protection Service Suite	None		Unlimited
Model Upgrade	Not Licensed		Unlimited
GeoIP Filtering	None		Unlimited

Affidabilità - Failover WAN

Spiegazione

Importanza del failover WAN nei sistemi firewall

1. Connettività Internet ininterrotta
Il failover WAN garantisce un accesso continuo a Internet passando automaticamente a una connessione di backup se il collegamento WAN primario si guasta. Ciò è fondamentale per mantenere le operazioni aziendali che dipendono dalla connettività Internet.

2. Maggiore affidabilità e disponibilità
Fornendo una connessione secondaria, il failover WAN migliora l'affidabilità e la disponibilità dei servizi di rete. Ciò riduce i tempi di inattività e aumenta la produttività complessiva.

3. Continuità operativa
Le interruzioni di rete possono causare perdite finanziarie, riduzione della soddisfazione dei clienti e ritardi operativi. Il failover WAN supporta la continuità operativa riducendo al minimo le interruzioni e mantenendo l'accesso ad applicazioni e servizi critici.

4. Bilanciamento del carico e prestazioni migliorate
Alcune piattaforme firewall supportano sia il failover che il bilanciamento del carico. Ciò consente di distribuire il traffico su più collegamenti WAN, ottimizzando la larghezza di banda e migliorando le prestazioni per gli utenti finali.

5. Supporto al disaster recovery
Durante interruzioni impreviste o guasti dell'infrastruttura, il failover garantisce che i processi di recovery rimangano accessibili e ininterrotti, preservando la disponibilità del servizio e l'integrità dei dati.

6. Mantenimento della postura di sicurezza
I firewall con capacità di failover garantiscono che tutto il traffico - durante il normale funzionamento e durante gli eventi di failover - continui a passare attraverso le ispezioni di sicurezza. Ciò impedisce di aggirare le misure di protezione durante le interruzioni.

7. Efficienza dei costi
Sebbene l'implementazione di linee WAN secondarie comporti costi associati, prevenire le interruzioni del servizio aiuta a evitare perdite finanziarie, riduzioni di produttività e insoddisfazione dei clienti, con conseguenti risparmi a lungo termine.

Riepilogo
Il failover WAN è una capacità cruciale nei sistemi firewall. Mantiene l'accesso continuo a Internet, supporta il disaster recovery, migliora l'affidabilità, rafforza la coerenza della sicurezza e protegge la continuità operativa. Riducendo i tempi di inattività e migliorando le prestazioni, il failover WAN aiuta le organizzazioni a mantenere la qualità del servizio e l'efficienza operativa.

Affidabilità - Failover WAN

WAN Interface Summary

Number of WAN Interfaces configured & enabled: 2

Interface	Type	Comment	PacketsIn	PacketsOut
X1	WAN	Default WAN	9268	9071
X5	WAN		1215	328

WAN Load Balancing is: enabled

Interface	Probing	Type	Prim Dest	Protocol	Alt Dest	Protocol
X1	Logical	At least one target should reply	204.212.170.23	TCP	8.8.8.8	ICMP
X5	Physical	None	None	None	None	None

Report di configurazione

Spiegazione

L'audit di configurazione esamina l'impostazione tecnica e la prontezza operativa dell'ambiente firewall. Valuta funzionalità di sistema come l'alta disponibilità (HA), il WAN Failover e lo stato dei servizi di sicurezza. Inoltre, verifica se i componenti chiave sono configurati correttamente e allineati agli standard di deployment consigliati.

Timeout di connessione TCP

Spiegazione

Il timeout di connessione TCP determina per quanto tempo il firewall mantiene una sessione TCP inattiva nella sua tabella di connessione prima che venga rimossa. Il valore predefinito globale di 15 minuti è un'impostazione ragionevole per la maggior parte degli ambienti e fornisce un buon equilibrio tra il supporto al traffico di rete legittimo e la conservazione delle risorse del firewall.
La modifica del timeout TCP globale influisce su ogni connessione TCP che passa attraverso il firewall. Aumentare questo valore inutilmente può portare a sessioni obsolete che rimangono in memoria per periodi prolungati, consumando voci della tabella di connessione e potenzialmente riducendo la capacità complessiva dell'appliance. In ambienti grandi o intensamente utilizzati, ciò può avere un impatto notevole sulle prestazioni del firewall e sull'utilizzo delle risorse.
Alcune applicazioni, tuttavia, richiedono periodi di inattività più lunghi per mantenere connessioni persistenti. Esempi possono includere determinate applicazioni database, software client/server legacy o sistemi di controllo industriale specializzati. In questi casi, è considerata best practice lasciare il timeout globale al suo valore predefinito e configurare invece un timeout TCP personalizzato solo sulle specifiche regole di accesso che lo richiedono.
Applicare timeout estesi a livello di regola offre diversi vantaggi:
Minimizza l'impatto sul firewall complessivo.
Limita l'aumento del consumo di risorse alle applicazioni interessate.
Riduce il numero di sessioni obsolete nella tabella di connessione.
Rende visibili e più facili da documentare i requisiti applicativi speciali.
Semplifica futuri audit e risoluzione dei problemi.
Questo report mostra l'attuale impostazione del timeout TCP globale ed elenca tutte le regole di accesso che utilizzano un valore di timeout TCP personalizzato. Le regole con impostazioni non predefinite dovrebbero essere riviste periodicamente per garantire che l'eccezione sia ancora necessaria e adeguatamente documentata.
Come raccomandazione generale, il timeout TCP globale dovrebbe rimanere al valore predefinito ove possibile, mentre i requisiti specifici delle applicazioni dovrebbero essere gestiti utilizzando override del timeout per singola regola.

General TCP Setting

Timeout di connessione TCP globale: 69

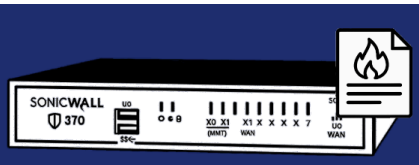
Informazioni aggiuntive

Il timeout di connessione TCP predefinito è stato modificato. Si consiglia di mantenere l'impostazione generale a 15 minuti. Se un determinato servizio richiede valori diversi, modificare il timeout TCP su una regola specifica

Regole in cui il timeout TCP predefinito è stato modificato

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	TCP Timeout
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	66
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	10
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	30

Numero di record: 3



Report di documentazione

Spiegazione

Il report di documentazione fornisce una panoramica strutturata dell'ambiente firewall e dei suoi elementi di configurazione chiave. Raccoglie e presenta informazioni di sistema rilevanti, tra cui impostazioni di rete, assegnazioni di interfacce, configurazioni di zona e policy applicate.
Il report è pensato per fungere da riferimento completo per gli amministratori, supportando sia le attività operative che il trasferimento di conoscenze. Garantisce che i dettagli di configurazione importanti siano chiaramente documentati e facilmente accessibili, riducendo la dipendenza dall'ispezione manuale del sistema.
Inoltre, la documentazione aiuta a mantenere trasparenza e coerenza in tutto l'ambiente, facilitando la risoluzione dei problemi, gli audit e le modifiche future.

Tutti i record di audit

Spiegazione

Audit interno del firewall
L'audit interno sui firewall è una componente essenziale per mantenere l'integrità operativa, la responsabilità e la sicurezza all'interno di un ambiente di rete. Il firewall rappresenta uno dei punti di controllo più critici in un'organizzazione, e l'audit fornisce visibilità sulle modifiche di configurazione, sugli eventi di accesso e sulle azioni amministrative che influenzano direttamente la postura di sicurezza della rete.

Responsabilità e tracciabilità
I log di audit documentano chi ha effettuato le modifiche, quando sono state effettuate e cosa è stato modificato. Questa tracciabilità garantisce che le responsabilità siano chiaramente assegnate e che qualsiasi errore di configurazione, deviazione dagli standard o modifica non autorizzata possa essere rapidamente identificata e corretta.

Rilevamento di modifiche non autorizzate o rischiose
I firewall influenzano direttamente il controllo degli accessi, la protezione dei dati e il flusso del traffico. L'audit interno consente agli amministratori di rilevare modifiche di configurazione intenzionali o accidentali, aiutando a identificare incidenti di sicurezza, violazioni delle policy o potenziali abusi di privilegi amministrativi.

Supporto alla conformità e alla governance
Molti framework normativi richiedono l'audit di sistemi critici come i firewall. I record di audit interno supportano la conformità a standard rilevanti per settori come finanza, sanità e pubblica amministrazione. Forniscono la prova che le policy vengono seguite e che i meccanismi di protezione sono adeguatamente applicati.

Approfondimento operativo e miglioramento continuo
I log di audit aiutano i team di sicurezza a comprendere la cronologia della configurazione e le tendenze operative. La revisione regolare di questi record consente alle organizzazioni di perfezionare le policy di accesso, identificare problemi ricorrenti e rafforzare le pratiche di gestione delle modifiche.

Indagine sugli incidenti e forense
Quando si verifica un evento di sicurezza, i dati di audit interno sono spesso una delle fonti di prova più preziose. Consentono agli investigatori di ricostruire le azioni intraprese sul firewall, analizzare le cause profonde e determinare se attività dannose o errori umani abbiano contribuito all'incidente.

Conclusione
L'audit interno è necessario per garantire trasparenza, coerenza e responsabilità nelle operazioni del firewall. Migliora la sicurezza, supporta i requisiti normativi, consente una risoluzione dei problemi più rapida e fornisce una base fondamentale per una gestione della rete resiliente.

Informazioni aggiuntive

Panoramica eventi di audit
Questa sezione elenca tutti gli eventi di audit estratti dal Technical Support Report (TSR). Fornisce visibilità sulle modifiche di configurazione apportate al firewall e identifica gli utenti responsabili di tali azioni.

Nota importante
I log di audit non vengono sincronizzati tra le appliance quando l'alta disponibilità (HA) è attivata. Di conseguenza, le modifiche eseguite sull'unità secondaria (attiva) durante i periodi di failover potrebbero non apparire nel percorso di audit dell'appliance primaria. Versioni future di FirewallToolbox potrebbero risolvere questo problema!

Questo report aiuta a convalidare l'attività amministrativa, supporta la responsabilità e assiste nell'identificazione di modifiche di configurazione indesiderate o non autorizzate.

Informazioni aggiuntive

uesto report mostra solo le 10 voci più recenti. Eseguire il report individuale per visualizzare tutti i risultati.

Firewall Internal Admin Audit Records

ID: 3749 Timestamp: 15.09.2026 16:33:49
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19526)

ID: 3749 Timestamp: 15.09.2026 16:33:49
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19526)

ID: 3748 Timestamp: 15.09.2026 16:33:49
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19525)

ID: 3748 Timestamp: 15.09.2026 16:33:49
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19525)

ID: 3747 Timestamp: 15.09.2026 16:31:36
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46610)

ID: 3747 Timestamp: 15.09.2026 16:31:36
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46610)

ID: 3746 Timestamp: 15.09.2026 16:31:36
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46608)

ID: 3746 Timestamp: 15.09.2026 16:31:36
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46608)

Firewall Internal Admin Audit Records

```
ID:          3745      Timestamp:   15.09.2026 16:18:33
Description: End Configuration Mode
Old:
New:
Status:
User:        UDSAdmin
Session:     GMS
Source:      127.0.0.1 (50325)
```


```
ID:          3745      Timestamp:   15.09.2026 16:18:33
Description: End Configuration Mode
Old:
New:
Status:
User:        UDSAdmin
Session:     GMS
Source:      127.0.0.1 (50325)
```

Tutte le regole (IPv4)

Spiegazione

Questo report fornisce un inventario completo di tutte le regole di accesso IPv4 configurate sul firewall, escludendo le regole di accesso predefinite integrate. Per ogni regola, il report elenca lo stato di attivazione, l'azione (Consenti/Nega), il nome della regola, le zone di origine e destinazione, gli oggetti di rete di origine e destinazione, gli oggetti di servizio, i commenti dell'amministratore e l'UUID univoco della regola.
Mantenere un inventario aggiornato delle regole firewall è una parte essenziale dell'amministrazione del firewall e dell'audit di sicurezza. Consente agli amministratori di rivedere la policy di sicurezza implementata, verificare che le regole seguano il principio del privilegio minimo, identificare regole obsolete o ridondanti e garantire che la documentazione delle regole sia completa e significativa. La revisione regolare della base delle regole aiuta a ridurre la complessità della configurazione, migliora la risoluzione dei problemi e riduce al minimo il rischio di accesso non intenzionale causato da regole firewall obsolete o eccessivamente permissive.

Tutte le regole (IPv4)

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	
YES	A	My Rule	DMZ-sec	DMZ-unsec	any	any	any	FTP Data	
YES	A	Test 17	DMZ-sec	DMZ-unsec	any	any	any	HTTPS	
YES	A	Test 20	DMZ-sec	DMZ-unsec	any	any	any	Kazaa / FastTrack	
YES	A	Test 21	DMZ-sec	DMZ-unsec	any	any	any	Lotus Notes	
YES	A	Test 19	DMZ-sec	DMZ-unsec	any	any	any	IKE	
YES	A	Test 18	DMZ-sec	DMZ-unsec	any	any	any	ICMP	
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	
YES	A	Rule10	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	Direct Connect	any	
YES	A	Allow WAN1	DMZ-sec	WAN	any	any	Enhanced TV	any	
YES	A	Test 22	DMZ-unsec	DMZ-sec	any	any	any	MSN	
YES	A	Allow syslog	DMZ-unsec	DMZ-unsec	any	any	SSH Management	any	
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	
YES	A	Allow WAN1	DMZ-unsec	WAN	any	any	Citrix UDP	any	
YES	A	Allow WAN1	LAN	WAN	KlausMeier	any	any	any	
YES	A	Allow management via ...	SSLVPN	LAN	SSLVPN-NetExtender Range	any	any	HTTPS Management	
YES	A	Test 24	WAN	060466	any	any	any	OSPF	
YES	A	Test 25	WAN	060466	any	any	any	POP3 (Retrieve E-Mail)	
YES	A	Test 23	WAN	060466	any	any	any	MSN	
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Temp, Rule to allow M...
YES	A	Allow Citrix	any		any	any	Citrix UDP	any	Example any<> any
YES	A	Allow FTP	any		any	any	FTP	any	

- Le regole aggiunte automaticamente sono escluse da questo report

Numero di record: 21

Regole di gestione (IPv4)

Spiegazione

Regole firewall che consentono l'accesso di gestione sui firewall SonicWall (SSH / HTTPS)

I firewall SonicWall forniscono servizi di gestione come SSH e HTTPS per consentire agli amministratori di configurare, monitorare e mantenere il dispositivo. Questi servizi concedono accesso privilegiato al firewall e ai suoi controlli di sicurezza. Le regole firewall che consentono l'accesso di gestione devono pertanto essere gestite con estrema attenzione, poiché un'esposizione impropria può introdurre gravi rischi operativi e di sicurezza.

Rischi per la sicurezza
Consentire l'accesso di gestione tramite regole firewall aumenta la superficie di attacco dell'appliance SonicWall. Le interfacce di gestione sono un obiettivo comune per gli aggressori poiché un accesso riuscito fornisce il controllo amministrativo diretto. I servizi SSH o HTTPS esposti possono essere soggetti a tentativi di login a forza bruta, attacchi di credential stuffing o sfruttamento di vulnerabilità nel piano di gestione SonicWall o nel firmware sottostante.

Se un aggressore ottiene l'accesso amministrativo, potrebbe modificare le regole del firewall, disattivare i servizi di sicurezza, alterare le configurazioni VPN o creare backdoor persistenti. Tali azioni possono provocare l'intercettazione del traffico, la perdita dell'integrità della rete o la completa compromissione dell'ambiente protetto.

Esposizione ad attacchi basati sulla rete
Quando i servizi di gestione SonicWall sono raggiungibili da reti non attendibili (come il WAN o zone definite in modo ampio), diventano visibili a scansioni automatizzate, attività di ricognizione e attacchi denial-of-service. Anche quando vengono utilizzati protocolli crittografati come HTTPS o SSH, i rischi permangono se il firmware è obsoleto, sono abilitate impostazioni crittografiche deboli o l'accesso non è sufficientemente limitato.

Inoltre, regole di accesso di gestione mal configurate possono esporre involontariamente porte amministrative su più interfacce o zone, aumentando la probabilità di accesso accidentale o non autorizzato.

Impatto operativo e di conformità
Regole di accesso di gestione troppo permissive complicano il monitoraggio e il rilevamento degli incidenti sui firewall SonicWall. I tentativi di accesso non autorizzato possono essere difficili da distinguere dall'attività amministrativa legittima, specialmente se logging e alerting non sono configurati in modo rigoroso. Dal punto di vista della conformità, l'accesso di gestione illimitato o non documentato spesso viola le policy di sicurezza interne e i requisiti normativi che impongono un controllo rigoroso sull'accesso privilegiato e sulle interfacce amministrative.

Best practice consigliate per i firewall SonicWall
L'accesso di gestione sui dispositivi SonicWall dovrebbe essere limitato a reti interne attendibili o zone di gestione dedicate. L'accesso diretto di gestione dalle interfacce WAN dovrebbe essere evitato ove possibile. Se è necessaria l'amministrazione remota, dovrebbe essere effettuata tramite connessioni VPN sicure con autenticazione e crittografia forti.

Ulteriori controlli consigliati includono la limitazione dell'accesso per indirizzo IP di origine, l'attivazione dell'autenticazione a più fattori per gli utenti amministrativi, il mantenimento del firmware SonicWall aggiornato e la revisione regolare delle regole di accesso di gestione e dei log di audit. Queste misure aiutano a garantire che l'accesso amministrativo rimanga controllato, verificabile e allineato alle best practice di sicurezza SonicWall.

Regole di gestione (IPv4)

Spiegazione

Oggetti e gruppi di servizi di gestione
Gli elementi elencati di seguito rappresentano gli oggetti e i gruppi di servizio classificati come servizi di gestione. In genere includono protocolli e porte utilizzati per l'accesso amministrativo, la configurazione dei dispositivi e le funzioni di monitoraggio.

L'identificazione di questi servizi aiuta a determinare dove è consentito l'accesso di gestione e garantisce che le interfacce amministrative siano applicate solo ad aree attendibili e controllate della rete.

Service Objects
Citrix TCP
Citrix TCP (Session Reliability)
Citrix UDP
GMS HTTPS
HTTP
HTTP Management
HTTPS
HTTPS Management
IKE (Key Exchange)
IKE (Traversal)
Kerberos TCP
Ping
SSH
SSH Management
Syslog

Service-Groups
Citrix
Idle HF
Management Services
IKE
Kerberos
Interface Management Services

Regole di gestione (IPv4)

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	
YES	A	Test 17	DMZ-sec	DMZ-unsec	any	any	any	HTTPS	
YES	A	Test 19	DMZ-sec	DMZ-unsec	any	any	any	IKE	
YES	A	Allow management via ...	SSLVPN	LAN	SSLVPN-NetExtender Range	any	any	HTTPS Management	
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Temp, Rule to allow M...

Numero di record: 4

Interfaces (IPv4)

Spiegazione

Panoramica configurazione interfacce
Questo report mostra tutte le interfacce configurate insieme alle relative impostazioni assegnate. Fornisce visibilità sui ruoli delle interfacce, sulle informazioni di indirizzamento e sui parametri operativi, aiutando a valutare connettività, segmentazione e struttura generale della rete.

Interfaces (IPv4)

Name	Zone	Comment	Assignment	IP	Subnet Mask	Gateway
X0	LAN	Default LAN	Static LAN	10.100.10.254	255.255.255.0	0.0.0.0
X1	WAN	Default WAN	Static	10.10.15.1	255.255.255.0	10.10.15.254
X2	DMZ-unsec		Static LAN	10.100.30.254	255.255.255.0	0.0.0.0
X3	DMZ-sec		Static LAN	10.100.40.254	255.255.255.0	0.0.0.0
X4	HA Data & Control		n/a	n/a	n/a	n/a
X5	WAN		Static	10.10.16.1	255.255.255.0	172.16.1.254
X6	LAN		Static LAN	192.168.1.254	255.255.255.0	0.0.0.0
X6:V100	LAN		Static LAN	192.168.2.254	255.255.255.0	0.0.0.0
X7	DMZ-sec		Static LAN	192.169.1.1	255.255.255.0	0.0.0.0

Numero di record: 9

Panoramica appartenenza utenti e gruppi

Spiegazione

Utenti e appartenenze ai gruppi
Questo report fornisce un elenco dettagliato di tutti gli utenti insieme alle relative appartenenze ai gruppi. Sulla base di queste affiliazioni, evidenzia i diritti di accesso VPN effettivi che gli utenti ereditano tramite i gruppi assegnati.
Ciò aiuta a identificare chi ha accesso alle risorse VPN, verificare i diritti corretti e rilevare potenziali account con privilegi eccessivi derivanti da autorizzazioni basate su gruppi.

Panoramica appartenenza utenti e gruppi

All LDAP Users
-è membro del gruppo: Trusted Users
-è membro del gruppo: SSLVPN Services
-è membro del gruppo: LAN Access66
- Concede diritti di accesso a:WAN Primary IP
- Concede diritti di accesso a:LAN Primary Subnet
- Concede diritti di accesso a:WAN-GoogleDNS-8.8.8.8

Isabel
-è membro del gruppo: Trusted Users
-è membro del gruppo: Content Filtering Bypass
-è membro del gruppo: Limited Administrators

LocalAdmin
-è membro del gruppo: Trusted Users
-è membro del gruppo: SonicWALL Administrators

Robert
-è membro del gruppo: Trusted Users
-è membro del gruppo: Guest Administrators

Sylvia
-è membro del gruppo: Trusted Users
-è membro del gruppo: Guest Administrators

UDS-SNWL-Admins@uds.local
-è membro del gruppo: SonicWALL Administrators

Udo
-è membro del gruppo: Trusted Users
-è membro del gruppo: SonicWALL Read-Only Admins

Uwe
-è membro del gruppo: Trusted Users
-è membro del gruppo: SonicWALL Administrators
-è membro del gruppo: SSLVPN Services
-è membro del gruppo: LAN Access66
- Concede diritti di accesso a:WAN Primary IP
- Concede diritti di accesso a:LAN Primary Subnet
- Concede diritti di accesso a:WAN-GoogleDNS-8.8.8.8

Webadmin
-è membro del gruppo: Trusted Users
-è membro del gruppo: SonicWALL Administrators
-è membro del gruppo: SSLVPN Services

apiuser
-è membro del gruppo: Trusted Users
-è membro del gruppo: SonicWALL Administrators

mschmitz
-è membro del gruppo: Trusted Users
-è membro del gruppo: SonicWALL Administrators
-è membro del gruppo: SSLVPN Services
-è membro del gruppo: LAN Access66
- Concede diritti di accesso a:WAN Primary IP
- Concede diritti di accesso a:LAN Primary Subnet

mschmitz (continua)

- Concede diritti di accesso a:WAN-GoogleDNS-8.8.8.8

Directory utenti esterne

Informazioni aggiuntive

Quando il numero di account utente locali su un firewall supera una piccola soglia (in genere circa 10 utenti), la gestione delle identità direttamente sul firewall diventa inefficiente, soggetta a errori e difficile da scalare. In tali ambienti, si consiglia vivamente di integrare una directory utenti esterna come LDAP, RADIUS o TACACS+.

1. Gestione centralizzata degli utenti
Le directory utenti esterne forniscono un'unica fonte autorevole per le identità utente.
- Gli account utente vengono creati, modificati ed eliminati in un unico sistema centrale.
- Modifiche come aggiornamenti delle password o disattivazione degli account si applicano immediatamente a tutti i sistemi collegati.
- Lo sforzo amministrativo è significativamente ridotto rispetto al mantenimento individuale degli utenti su ciascun firewall.

Ciò diventa sempre più importante man mano che il numero di utenti cresce e i cambiamenti del personale si verificano più frequentemente.

2. Maggiore sicurezza e rischio ridotto
Gestire un numero crescente di utenti locali del firewall aumenta nel tempo il rischio di lacune di sicurezza.
- Gli account orfani possono rimanere attivi dopo che i dipendenti lasciano l'organizzazione.
- Le policy delle password potrebbero essere incoerenti o non applicate in modo uniforme.
- L'amministrazione manuale degli utenti aumenta la probabilità di errori di configurazione.

I sistemi di autenticazione esterna applicano policy di sicurezza coerenti, tra cui complessità delle password, rotazione delle password, regole di blocco degli account e, dove supportata, l'autenticazione a più fattori.

3. Migliore scalabilità e manutenibilità a lungo termine
I firewall sono progettati principalmente per l'ispezione del traffico e l'applicazione delle policy, non per la gestione del ciclo di vita delle identità.
- Gestire un piccolo numero di utenti locali può essere accettabile.
- Oltre circa 10 utenti, il carico amministrativo cresce in modo sproporzionato.
- Le directory esterne scalano fino a decine, centinaia o migliaia di utenti senza aumentare la complessità sul firewall.

Il firewall diventa un consumatore di servizi di identità piuttosto che il proprietario dei dati utente.

4. Controllo degli accessi basato sui ruoli (RBAC)
Le directory utenti esterne consentono di assegnare i diritti di accesso utilizzando gruppi invece di singoli account utente.
- Gli utenti sono assegnati a gruppi di directory come utenti VPN o amministratori del firewall.
- Le regole firewall fanno riferimento a questi gruppi anziché a utenti specifici.
- Le modifiche di accesso possono essere implementate senza modificare la configurazione del firewall.

Questa separazione tra gestione delle identità e autorizzazione migliora chiarezza, coerenza ed efficienza operativa.

5. Audit e conformità più semplici
Gli standard di sicurezza e le policy interne spesso richiedono una chiara tracciabilità dell'accesso degli utenti.
I sistemi di autenticazione esterna forniscono log di autenticazione centralizzati, eventi di login tracciabili e una chiara responsabilità per ogni utente.

Ciò semplifica notevolmente gli audit e supporta la conformità con framework come ISO 27001, NIST o requisiti di governance interni.

6. Integrazione perfetta con l'infrastruttura esistente
La maggior parte delle organizzazioni gestisce già sistemi di identità centralizzati.
- LDAP o Active Directory per le identità utente
- RADIUS per l'accesso VPN e di rete
- TACACS+ per il controllo dell'accesso amministrativo

L'integrazione del firewall in questi sistemi evita database utente duplicati e allinea l'accesso al firewall ai processi IT consolidati.

7. Riduzione degli errori operativi
La gestione manuale degli utenti sui firewall porta frequentemente a problemi operativi.
- Rimozioni di account dimenticate
- Permessi incoerenti
- Configuration drift nel tempo

Delegare l'autenticazione a un sistema esterno produce configurazioni firewall più pulite e riduce il rischio di errore umano.

Conclusione
Sebbene gli utenti locali del firewall possano essere sufficienti per ambienti molto piccoli, non scalano efficacemente.
Una volta che il numero di utenti supera circa 10, l'uso di una directory utenti esterna offre chiari vantaggi in termini di sicurezza, scalabilità, efficienza amministrativa e verificabilità.

Per ambienti medi e grandi, l'integrazione di LDAP, RADIUS o TACACS+ è considerata una best practice e un requisito fondamentale per operazioni firewall sostenibili e sicure.

Report zone

Spiegazione

Questo report mostra i dettagli sulle zone

Report zone

Zone	Type	Member Interfaces	Trust	Active Security Services	SSLVPN	SSO
060466	1	None	Blocked	GAV, IPS, ASPY	No	No
150971-Test	1	None	Blocked	None	No	No
DMZ	2	None	Allowed	None	No	Yes
DMZ-sec	2	X3, X7	Blocked	None	No	Yes
DMZ-unsec	2	X2	Blocked	None	No	No
LAN	1	X0, X6, X6:V100	Allowed	GAV, IPS, ASPY, DPI-SSL-C	No	Yes
MULTICAST	6	None	Blocked	None	No	No
SSLVPN	8	None	Blocked	None	Yes	No
Test	1	None	Blocked	GAV, IPS, ASPY, DPI-SSL-C	No	Yes
VPN	5	None	Blocked	None	No	No
WAN	0	X1, X5	Blocked	GAV, IPS, ASPY, DPI-SSL-S, GVPN	Yes	No

Numero di record: 11

Report di manutenzione

Spiegazione

Il report di manutenzione aiuta a identificare gli elementi di configurazione che dovrebbero essere rivisti regolarmente per mantenere il firewall pulito, efficiente e facile da gestire. Nel tempo, le configurazioni firewall crescono naturalmente man mano che vengono aggiunte nuove regole, oggetti, VPN e servizi. Senza una manutenzione periodica, le voci obsolete o inutilizzate possono accumularsi, aumentando il carico amministrativo e rendendo la risoluzione dei problemi più difficile.
Questo report evidenzia gli elementi di configurazione che potrebbero richiedere attenzione, come regole firewall disattivate o inutilizzate, policy NAT inattive, oggetti indirizzo e servizio inutilizzati, servizi di sicurezza scaduti e altri elementi di configurazione non più attivamente utilizzati. Identifica anche le impostazioni che potrebbero beneficiare di ottimizzazione o pulizia.
Lo scopo di questo report non è raccomandare la rimozione automatica di ogni elemento elencato. Fornisce invece agli amministratori una panoramica strutturata dei componenti di configurazione che dovrebbero essere verificati prima di apportare qualsiasi modifica. Alcuni oggetti o regole potrebbero comunque essere necessari per progetti futuri, ambienti temporanei, procedure di disaster recovery o servizi utilizzati raramente.
La manutenzione regolare offre diversi vantaggi importanti:
- Riduce la complessità della configurazione e migliora la leggibilità.
- Rende la risoluzione dei problemi e l'audit significativamente più semplici.
- Aiuta a identificare elementi di configurazione obsoleti o dimenticati.
- Riduce il rischio di errori di configurazione accidentali.
- Migliora la gestibilità a lungo termine del firewall.
- Supporta un ambiente di sicurezza ben documentato e mantenuto professionalmente.
Un firewall ben mantenuto è più facile da amministrare, più facile da sottoporre ad audit e fornisce una base più solida per future modifiche di configurazione e miglioramenti della sicurezza.

Convenzioni di denominazione degli oggetti indirizzo

Spiegazione

Importanza di convenzioni di denominazione comuni per gli oggetti indirizzo
Una gestione efficace degli oggetti indirizzo del firewall è essenziale per mantenere un ambiente di rete sicuro e ben organizzato. Un fattore chiave che contribuisce a questa efficacia è l'uso di convenzioni di denominazione coerenti e significative.

Chiarezza e amministrazione più rapida
Quando gli oggetti indirizzo seguono standard di denominazione uniformi, gli amministratori possono riconoscere immediatamente il loro scopo, posizione o servizio correlato senza dover esaminare dati di configurazione dettagliati. Ciò riduce il tempo dedicato alla risoluzione dei problemi, all'aggiornamento delle regole o alle modifiche delle policy, e minimizza la possibilità di modificare l'oggetto sbagliato.

Coerenza e accuratezza nella configurazione
Formati di denominazione standardizzati stabiliscono uniformità in tutte le configurazioni. Ciò previene duplicazioni, evita confusione e riduce gli errori di configurazione che potrebbero portare a permessi di accesso indesiderati o flussi di comunicazione bloccati. Nomi prevedibili consentono agli amministratori di interpretare le policy firewall in modo più efficiente e accurato.

Migliore collaborazione e trasferimento di conoscenze
Convenzioni di denominazione coerenti consentono ai team di lavorare con una comprensione condivisa. Gli amministratori che non hanno familiarità con una configurazione possono comunque interpretare immediatamente l'uso degli oggetti e le dipendenze. Ciò migliora la collaborazione, semplifica l'inserimento di nuovo personale e garantisce continuità nel tempo, anche quando le responsabilità cambiano.

Conclusione
Le convenzioni di denominazione comuni rafforzano la manutenibilità, l'accuratezza e la trasparenza delle configurazioni firewall. Migliorando la chiarezza, riducendo la complessità della configurazione e favorendo la collaborazione, contribuiscono in modo significativo a un'amministrazione di rete sicura e sostenibile.

Convenzioni di denominazione degli oggetti indirizzo

Address Object Name old	Address Object Name new
SSLVPN-NetExtender Range	AO-SSLVPN-NetExtender Range-192.168.168.100
WAN-GoogleDNS-8.8.8.8	AO-WAN-GoogleDNS-8.8.8.8
WAN-TZ570-10.10.10.254	AO-WAN-TZ570-10.10.10.254
LAN-UDS-Analytics-10.100.10.50	AO-LAN-UDSAnalytics-10.100.10.50
WAN-GoogleDNS-8.8.8.8-2	AO-WAN-GoogleDNS2-8.8.8.8
TZ570 LAN	AO-VPN-TZ570 LAN-10.10.10.0
Server	AO-LAN-Server-10.99.10.223
MartinSchmitz	AO-LAN-MartinSchmitz-1.1.1.1
KlausMeier	AO-LAN-KlausMeier-1.1.2.2
FTP Server Private	AO-LAN-FTP Server Private-172.20.20.101
FTP Server Public1	AO-WAN-FTP Server Public1-10.10.20.2
Test	AO-LAN-Test-10.100.10.99
Test1	AO-LAN-Test1-10.100.10.99
Test4	AO-LAN-Test4-10.100.10.99
x0 und x6 subnet	AO--x0 und x6 subnet-0.0.0.0
Test12	AO-LAN-Test12-10.100.10.99
Test_111	AO-LAN-Test_111-10.100.10.111
Test_112	AO-LAN-Test_112-10.100.10.112
Test_113	AO-LAN-Test_113-10.100.10.113
Test_114	AO-LAN-Test_114-10.100.10.114
Test_115	AO-LAN-Test_115-10.100.10.115
Test_116	AO-LAN-Test_116-10.100.10.116
Test_117	AO-LAN-Test_117-10.100.10.117
Test_118	AO-LAN-Test_118-10.100.10.118
Test13	AO-LAN-Test13-10.100.10.13
Syslog Synology	AO-WAN-Syslog Synology-10.10.40.50
Test Group	AO--Test Group-0.0.0.0

Oggetti indirizzo duplicati

Spiegazione

Analisi degli oggetti indirizzo duplicati
Gli oggetti indirizzo duplicati, in cui nomi diversi si riferiscono allo stesso indirizzo IP o rete, possono introdurre molteplici sfide operative e di sicurezza sui firewall.
1. Maggiore complessità e rischio di errori di configurazione
Quando più oggetti fanno riferimento alla stessa destinazione, gli amministratori potrebbero non sapere quale utilizzare. Ciò complica la creazione delle policy, aumenta la probabilità di utilizzare l'oggetto sbagliato e rallenta gli audit, la risoluzione dei problemi e i processi di modifica.
2. Policy in conflitto o sovrapposte
Oggetti diversi che rappresentano lo stesso IP potrebbero essere utilizzati in modo incoerente tra le regole. Una regola potrebbe consentire il traffico mentre un'altra lo blocca, con conseguente comportamento imprevedibile e difficile analisi delle policy.
3. Applicazione incoerente della sicurezza
Quando team o amministratori diversi creano oggetti separati per la stessa risorsa, l'applicazione delle policy diventa frammentata. Ciò può portare ad accessi non intenzionali o a una copertura parziale delle policy, indebolendo la postura di sicurezza complessiva.
4. Maggiore sforzo di manutenzione
Qualsiasi modifica che interessa un oggetto duplicato deve essere aggiornata in tutti i riferimenti delle policy. Trascurare una posizione può portare a regole obsolete, lacune nelle restrizioni di accesso o configuration drift.
Best practice consigliate
– *Consolidare gli oggetti indirizzo:* identificare le voci duplicate e sostituirle con un singolo oggetto che rappresenti ciascun IP, subnet o risorsa.
– *Utilizzare convenzioni di denominazione chiare:* i nomi dovrebbero riflettere lo scopo o l'identità della risorsa, migliorando coerenza e leggibilità.
– *Eseguire audit regolari:* la pulizia periodica riduce la ridondanza e migliora la qualità delle policy.
– *Documentare l'utilizzo e la proprietà:* una documentazione adeguata aiuta durante la manutenzione ed evita la ricreazione di oggetti non necessari.

La pulizia degli oggetti indirizzo duplicati migliora la chiarezza delle regole, semplifica l'amministrazione delle policy, riduce gli errori operativi e contribuisce a una configurazione di sicurezza più solida e prevedibile.

Duplicate Address Objects

IP	Name
- nessun record trovato -	

Logging esterno

Spiegazione

Il logging/telemetria esterna su un firewall (ad es. Syslog, IPFIX/NetFlow, trap SNMP) è importante perché il firewall è uno dei pochi dispositivi in grado di osservare in modo affidabile chi ha comunicato con chi, quando, come e cosa è stato bloccato o consentito. Senza esportare questi segnali, si opera essenzialmente alla cieca: si potrebbe essere ancora protetti dalla policy, ma si perde la capacità di rilevare, indagare e dimostrare cosa sia accaduto.
Da una prospettiva di sicurezza, i log esterni sono la base per il rilevamento e la risposta agli incidenti. Gli attacchi raramente si annunciano con un singolo allarme evidente. Si manifestano come pattern - ripetuti fallimenti di login, anomalie VPN, hit di policy, connessioni in uscita impreviste, movimento laterale o traffico verso destinazioni sospette. Un SIEM o una piattaforma di log può correlare questi pattern tra fonti diverse (firewall + endpoint + identità + server). Gli eventi del firewall spesso forniscono il primo indicatore di alta qualità che qualcosa non va, e la telemetria dei flussi (NetFlow/IPFIX) fornisce la "narrazione di rete" necessaria per comprendere portata e impatto.
La raccolta esterna è anche fondamentale per la forense e la responsabilità. I firewall hanno una conservazione locale dei log limitata e possono perdere dati durante riavvii, aggiornamenti o rotazione dello storage. Il logging centralizzato preserva le prove per periodi più lunghi, supporta i requisiti legali/normativi e consente un reporting affidabile. In pratica, molte indagini iniziano giorni o settimane dopo la compromissione iniziale. Se i log fossero conservati solo localmente, l'intervallo di tempo chiave potrebbe già essere andato perso.
Dal punto di vista operativo, la telemetria migliora la stabilità e la risoluzione dei problemi. Il monitoraggio SNMP e le trap forniscono avvisi anticipati su pressione CPU/memoria, errori di interfaccia, instabilità dei tunnel o saturazione delle risorse - problemi che possono sembrare "interruzioni casuali" a meno che non si disponga di dati di serie temporali. I record di flusso aiutano a convalidare l'utilizzo della larghezza di banda, identificare i principali generatori di traffico, rilevare errori di configurazione (ad es. routing asimmetrico) e confermare se una modifica della policy ha effettivamente avuto l'effetto previsto.
Infine, il logging/telemetria esterna supporta il miglioramento continuo. Consente di misurare l'efficacia delle policy, ottimizzare le regole troppo permissive o troppo rumorose e identificare shadow IT o servizi rischiosi. In breve: esportare log e telemetria del firewall trasforma il firewall da una scatola che "blocca il traffico" in un controllo che è possibile verificare, sottoporre ad audit e rendere operativo, il che rappresenta la differenza tra avere controlli di sicurezza e avere garanzia di sicurezza.

Logging esterno

Central Management	
Central Management (NSM / GMS):	off
NSM ZeroTouch:	enabled

Syslog	
Syslog Server Name:	n/a
Syslog Standby Server Name:	n/a
Syslog Server Port:	n/a

Netflow	
Netflow Internal:	n/a
Netflow External:	n/a
Netflow External Address:	n/a

Log to FTP Server	
Log to FTP Server:	
FTP Server IP Address:	n/a

Regole firewall disattivate

Spiegazione

Importanza delle regole firewall disattivate
Le regole firewall disattivate, sebbene non applichino attivamente controlli di sicurezza, mantengono comunque rilevanza all'interno della configurazione del firewall e della strategia di sicurezza complessiva.
Backup operativo e riattivazione rapida
Le regole disattivate spesso fungono da alternative di configurazione predefinite. Gli amministratori possono disattivare temporaneamente una regola durante manutenzione, risoluzione dei problemi o modifiche pianificate e successivamente riattivarla senza dover riprogettare o ricreare la policy. Ciò garantisce un rapido ripristino dei controlli di sicurezza previsti.
Documentazione di configurazione e audit
Le regole inattive forniscono informazioni sui set di regole storici e sulle decisioni di sicurezza precedenti. Mantenerle visibili supporta gli audit, la verifica della conformità e l'analisi forense, preservando l'intento della configurazione e la cronologia delle modifiche.
Flessibilità per requisiti futuri
Man mano che gli ambienti di rete cambiano, le regole precedentemente disattivate possono tornare rilevanti. Mantenerle consente una rapida riattivazione o modifica senza dover ricreare da zero policy di accesso complesse o oggetti indirizzo.
Conclusione
Sebbene le regole firewall disattivate non filtrino attivamente il traffico, rimangono comunque utili punti di riferimento per il ripristino operativo, la documentazione delle configurazioni precedenti e il rapido adattamento ai futuri requisiti di sicurezza. Dovrebbero essere riviste periodicamente per garantire che rimangano valide, intenzionali e allineate agli obiettivi di sicurezza attuali.

Regole firewall disattivate

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc

- nessun record trovato -

Numero di record: 0

Regole firewall non utilizzate da molto tempo (IPv4)

Spiegazione

Regole firewall non utilizzate per un periodo prolungato
Le regole firewall non utilizzate per un lungo periodo di tempo spesso indicano percorsi di accesso obsoleti, servizi dismessi o configurazioni legacy non più rilevanti. Mantenere in vigore regole inutilizzate aumenta il carico amministrativo e può creare esposizione di sicurezza non necessaria.

Le regole inattive possono essere erroneamente riattivate o modificate, concedendo potenzialmente accessi non intenzionali o indebolendo l'applicazione delle policy. Rimuovere o disattivare queste regole aiuta a mantenere una base di regole pulita, migliora la gestibilità e riduce la superficie di attacco complessiva dell'ambiente.

La revisione regolare delle regole inutilizzate garantisce che rimangano solo i percorsi di accesso necessari e attivamente utilizzati, supportando sia l'efficienza operativa che le best practice di sicurezza.

Il seguente report mostra le regole non utilizzate da più di 365 giorni.

Regole firewall non utilizzate da molto tempo (IPv4)

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	Last time hit
YES	A	Allow WAN1	LAN	WAN	KlausMeier	any	any	any	Regole firewall non u...
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Regole firewall non u...
YES	A	Test 24	WAN	060466	any	any	any	OSPF	Regole firewall non u...
YES	A	Test 25	WAN	060466	any	any	any	POP3 (Retrieve E-Mail)	Regole firewall non u...
YES	A	Test 23	WAN	060466	any	any	any	MSN	Regole firewall non u...
YES	A	Allow WAN1	DMZ-unsec	WAN	any	any	Citrix UDP	any	Regole firewall non u...
YES	A	Allow syslog	DMZ-unsec	DMZ-unsec	any	any	SSH Management	any	Regole firewall non u...
YES	A	Test 22	DMZ-unsec	DMZ-sec	any	any	any	MSN	Regole firewall non u...
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	Regole firewall non u...
YES	A	Allow WAN1	DMZ-sec	WAN	any	any	Enhanced TV	any	Regole firewall non u...
YES	A	My Rule	DMZ-sec	DMZ-unsec	any	any	any	FTP Data	Regole firewall non u...
YES	A	Test 17	DMZ-sec	DMZ-unsec	any	any	any	HTTPS	Regole firewall non u...
YES	A	Test 20	DMZ-sec	DMZ-unsec	any	any	any	Kazaa / FastTrack	Regole firewall non u...
YES	A	Test 21	DMZ-sec	DMZ-unsec	any	any	any	Lotus Notes	Regole firewall non u...
YES	A	Test 19	DMZ-sec	DMZ-unsec	any	any	any	IKE	Regole firewall non u...
YES	A	Test 18	DMZ-sec	DMZ-unsec	any	any	any	ICMP	Regole firewall non u...
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	Regole firewall non u...
YES	A	Rule10	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	Direct Connect	any	Regole firewall non u...
YES	A	Allow Citrix	any		any	any	Citrix UDP	any	Regole firewall non u...
YES	A	Allow FTP	any		any	any	FTP	any	Regole firewall non u...
YES	A	Allow management via ...	SSLVPN	LAN	SSLVPN-NetExtender Range	any	any	HTTPS Management	2025-03-31 11:40:59

- Le regole aggiunte automaticamente sono escluse da questo report

Numero di record: 21

Policy NAT (Network Address Translation) disattivate (IPv4)

Spiegazione

Policy NAT disattivate e loro impatto
Le policy NAT (Network Address Translation) disattivate sui firewall possono introdurre problemi operativi e di sicurezza significativi all'interno di una rete. Di seguito una panoramica dei principali rischi e implicazioni tecniche associate a regole NAT inattive o rimosse.

1. Perdita di segmentazione della rete
Le policy NAT supportano la separazione logica tra reti interne ed esterne traducendo gli indirizzi IP interni prima che il traffico lasci la rete.
Rischi potenziali:
– *Esposizione degli IP interni:* senza NAT, gli schemi di indirizzamento interni potrebbero essere visibili esternamente, rendendo raggiungibili dispositivi precedentemente isolati.
– *Isolamento ridotto tra zone:* il NAT supporta l'isolamento tra segmenti LAN, DMZ e WAN. Il NAT disattivato può involontariamente offuscare i confini di sicurezza.

2. Maggiori rischi per la sicurezza
Il NAT fornisce indirettamente un livello di sicurezza impedendo connessioni in ingresso non richieste verso host interni.
Possibili conseguenze:
– Gli aggressori possono colpire direttamente i dispositivi interni
– Le restrizioni basate sul firewall possono essere aggirate
– Le risorse interne diventano più facili da enumerare o scansionare

3. Interruzioni della comunicazione
Molti flussi di comunicazione di rete presuppongono che il NAT sia attivo per la traduzione e il routing.
Quando il NAT è disattivato:
– I dispositivi potrebbero perdere l'accesso ai servizi esterni
– Gli utenti potrebbero riscontrare connettività incoerente
– La risoluzione dei problemi diventa più complessa a causa di guasti di routing o servizi irraggiungibili

4. Problemi con connettività multi-rete e VPN
VPN, routing e tecnologie di accesso remoto spesso dipendono dal NAT per allineare gli spazi di indirizzi interni ed esterni.
Rischi chiave:
– Le sessioni di accesso remoto potrebbero non riuscire
– Potrebbero verificarsi sovrapposizioni di rete quando gli spazi IP entrano in conflitto
– I sistemi esterni non possono instradare correttamente il traffico di ritorno

5. Sfide nell'applicazione delle policy e nel monitoraggio
La logica di controllo degli accessi spesso sfrutta il NAT per tracciare e classificare i flussi.
Conseguenze del NAT disattivato:
– Capacità ridotta di monitorare o correlare il traffico
– Difficoltà nell'attribuire l'attività a dispositivi/utenti specifici
– Lacune nell'accuratezza del logging

6. Maggiore consumo di spazio IP pubblico
Il NAT consente a molti dispositivi interni di condividere uno o un piccolo pool di indirizzi IP pubblici.
Senza NAT:
– Ogni sistema potrebbe richiedere il proprio IP instradabile
– L'esaurimento IPv4 diventa una reale preoccupazione operativa

Conclusione
Le policy NAT disattivate possono causare guasti di routing imprevisti, confini di protezione indeboliti e maggiore esposizione alla sicurezza. Nella maggior parte degli ambienti, il NAT serve non solo per la traduzione degli indirizzi ma anche come metodo per applicare l'isolamento, la visibilità del logging e un comportamento di routing prevedibile. Per operazioni stabili e sicure, le policy NAT dovrebbero essere riviste con attenzione, mantenute correttamente e disattivate solo in scenari di progettazione intenzionali e ben controllati.

- Le regole aggiunte automaticamente sono escluse da questo report

Policy NAT (Network Address Translation) disattivate (IPv4)

Ena	Name	Original Source	Translated Source	Original Destination	Translated Destination	Original Service	Translated Service
NO	Test disabled NAT	DMZ-sec Subnets	Original	Any	Server	Citrix UDP	Original
NO	My Rule	DMZ-unsec Subnets	Original	All WAN IP	DEAG_Test	Any	Original
NO	Deact 3	FTP Server Private	FTP Server Public1	Any	Original	Any	Original

Policy NAT attive e senza hit (IPv4)

Spiegazione

Policy NAT senza traffico
Questo report evidenzia le policy NAT (Network Address Translation) attualmente attivate ma non utilizzate nell'intervallo di tempo monitorato. Una policy NAT senza hit registrati indica in genere che la regola non corrisponde più a flussi di traffico attivi o è associata a servizi, reti o dispositivi non più in uso.

Possibili cause per policy NAT inutilizzate
– Il servizio corrispondente non è più attivo
– Un riferimento a dispositivo o rete è cambiato
– Il routing è stato riprogettato, rendendo obsoleta questa traduzione NAT
– Una regola temporanea o relativa a una migrazione non è mai stata rimossa

Perché le policy NAT inutilizzate sono importanti
1. Maggiore complessità delle policy
Le voci NAT inutilizzate rendono la configurazione più difficile da comprendere e mantenere. Gli amministratori potrebbero dedicare tempo aggiuntivo a valutare regole non più rilevanti, rallentando la risoluzione dei problemi e la gestione delle modifiche.

2. Rischio di attivazione accidentale
Una policy NAT dormiente potrebbe diventare attiva se le condizioni di rete cambiano o il routing si modifica. Ciò potrebbe esporre inavvertitamente dispositivi interni, alterare i mapping degli indirizzi o aggirare le policy di accesso previste.

3. Potenziale esposizione alla sicurezza
Anche se inutilizzata, una regola NAT definisce comunque un possibile percorso di traduzione. Se attivata involontariamente, può:
– rivelare l'indirizzamento interno
– abilitare connessioni in entrata o in uscita indesiderate
– aggirare i punti di filtraggio o ispezione previsti

4. Ridotta efficienza operativa
Ampi set di regole NAT aumentano il carico di lavoro amministrativo e riducono la chiarezza della configurazione. La rimozione delle voci obsolete produce un set di policy più pulito e prevedibile e riduce il rischio operativo.

Pratiche di manutenzione consigliate
– Verificare periodicamente se le regole NAT sono ancora necessarie
– Documentare la proprietà e lo scopo previsto delle regole
– Rimuovere i mapping inutilizzati o disattivarli temporaneamente per la convalida
– Rivedere le policy NAT dopo riprogettazioni di rete, migrazioni o attività di dismissione

Conclusione
Le policy NAT attivate senza attività di traffico spesso indicano oggetti di configurazione obsoleti o non necessari. La pulizia delle regole inutilizzate riduce la complessità, previene percorsi di esposizione non intenzionali e migliora la manutenibilità e la postura di sicurezza. La revisione regolare garantisce che la policy del firewall rifletta accuratamente il comportamento di rete richiesto e attivo.

- Le regole aggiunte automaticamente sono escluse da questo report

Policy NAT attive e senza hit (IPv4)

Ena	Name	Original Source	Translated Source	Original Destination	Translated Destination	Original Service	Translated Service
NO	Test disabled NAT	DMZ-sec Subnets	Original	Any	Server	Citrix UDP	Original
YES	Test 1	DMZ-sec Subnets	Original	Any	CSE_Access_Tier_AIP_1	Citrix TCP	Original
NO	My Rule	DMZ-unsec Subnets	Original	All WAN IP	DEAG_Test	Any	Original
NO	Deact 3	FTP Server Private	FTP Server Public1	Any	Original	Any	Original
YES	Default NAT Policy	Any	Any	Any	Any	Any	Original

Impostazioni WAN MTU

Spiegazione

Questa sezione verifica se l'impostazione WAN MTU sul firewall SonicWall è configurata a un valore insolitamente basso.
Un valore MTU troppo basso può ridurre l'efficienza di trasmissione e influire negativamente sulle prestazioni di rete.
Se viene rilevata tale impostazione, dovrebbe essere esaminata per confermare che sia tecnicamente necessaria e non il risultato di una limitazione di configurazione non necessaria.

X1	WAN	1500	ok	-
X5	WAN	1500	ok	-