Proteggere la rete

ONTAP 9

NetApp
February 12, 2026

Sommario

Proteggere la rete

Configurare la protezione di rete ONTAP utilizzando FIPS per tutte le connessioni SSL

ONTAP è conforme agli standard FIPS (Federal Information Processing Standards) 140-2 per tutte le connessioni SSL. È possibile attivare e disattivare la modalità SSL FIPS, impostare i protocolli SSL a livello globale e disattivare eventuali cifrari deboli all'interno ONTAP.

Per impostazione predefinita, SSL su ONTAP è impostato con la conformità FIPS disattivata e con i seguenti protocolli TLS attivati:

- TLSv1,3 (a partire da ONTAP 9.11.1)
- TLSv1.2

Nelle precedenti versioni di ONTAP i seguenti protocolli TLS erano attivati per impostazione predefinita:

- TLSv1,1 (disattivata per impostazione predefinita a partire da ONTAP 9.12.1)
- TLSv1 (disattivata per impostazione predefinita a partire da ONTAP 9,8)

Quando la modalità SSL FIPS è attivata, la comunicazione SSL da ONTAP a componenti client o server esterni a ONTAP utilizzerà la crittografia conforme a FIPS per SSL.

Se si desidera che gli account amministratore accedano alle SVM con una chiave pubblica SSH, assicurarsi che l'algoritmo della chiave host sia supportato prima di attivare la modalità SSL FIPS.

Nota: il supporto dell'algoritmo della chiave host è stato modificato in ONTAP 9.11.1 e versioni successive.

Release di ONTAP	Tipi di chiave supportati	Tipi di chiave non supportati
9.11.1 e versioni successive	ecdsa-sha2-nistp256	rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 e versioni precedenti	ecdsa-sha2-nistp256 + ssh-ed25519	ssh-dss + ssh-rsa

Gli account di chiave pubblica SSH esistenti senza gli algoritmi di chiave supportati devono essere riconfigurati con un tipo di chiave supportato prima di attivare FIPS, altrimenti l'autenticazione dell'amministratore non avrà esito positivo.

Per ulteriori informazioni, vedere "Abilitare gli account a chiave pubblica SSH".

ONTAP 9.18.1 introduce il supporto per gli algoritmi crittografici post-quantum computing ML-KEM, ML-DSA e SLH-DSA per SSL, fornendo un ulteriore livello di sicurezza contro potenziali futuri attacchi ai computer quantistici. Questi algoritmi sono disponibili solo quandoFIPS è disabilitato . Gli algoritmi crittografici post-quantistici vengono negoziati quando FIPS è disabilitato e il peer li supporta.

Abilitare FIPS

Si consiglia a tutti gli utenti sicuri di modificare la propria configurazione di sicurezza subito dopo l'installazione o l'aggiornamento del sistema. Quando la modalità SSL FIPS è attivata, la comunicazione SSL da ONTAP a componenti client o server esterni a ONTAP utilizzerà la crittografia conforme a FIPS per SSL.

Quando FIPS è attivato, non è possibile installare o creare un certificato con una chiave RSA di lunghezza pari a 4096.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Attiva FIPS:

   ```
   security config modify * -is-fips-enabled true
   ```

3. Quando viene richiesto di continuare, immettere `y`
4. A partire da ONTAP 9.9.1, il riavvio non è più necessario. Se si utilizza ONTAP 9.8 o una versione precedente, riavviare manualmente ciascun nodo del cluster, uno alla volta.

Esempio

Se si utilizza ONTAP 9.9.1 o versione successiva, il messaggio di avviso non viene visualizzato.

```
security config modify -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Ulteriori informazioni sulla `security config modify` configurazione della modalità SSL FIPS in "Riferimento al comando ONTAP".

Disattiva FIPS

A partire da ONTAP 9.18.1, SSL in ONTAP supporta gli algoritmi crittografici post-quantum computing ML-KEM, ML-DSA e SLH-DSA. Questi algoritmi sono disponibili solo quando FIPS è disabilitato e il peer li supporta.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Disattivare FIPS digitando:

   ```
   security config modify -is-fips-enabled false
   ```

3. Quando viene richiesto di continuare, immettere `y`.
4. A partire da ONTAP 9.9.1, il riavvio non è più necessario. Se si esegue ONTAP 9.8 o una versione precedente, riavviare manualmente ciascun nodo nel cluster.

Se è necessario utilizzare il protocollo SSLv3, è necessario disabilitare FIPS con la procedura sopra descritta. SSLv3 può essere abilitato solo quando FIPS è disabilitato.

È possibile abilitare SSLv3 con il seguente comando. Se si utilizza ONTAP 9.9.1 o una versione successiva, il messaggio di avviso non verrà visualizzato.

```
security config modify -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Visualizza lo stato di conformità FIPS

È possibile verificare se l'intero cluster esegue le impostazioni di configurazione della protezione correnti.

Fasi

1. Se si utilizza ONTAP 9.8 o una versione precedente, riavviare manualmente ciascun nodo del cluster, uno alla volta.
2. Visualizza lo stato di conformità corrente:

   ```
   security config show
   ```

```
cluster1::> security config show
Cluster    Supported
FIPS Mode  Protocols Supported Cipher Suites
---------- ---------
-----------------------------------------------------------
false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
TLS_RSA_WITH_AES_128_CCM_8,
           TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                     TLS_RSA_WITH_AES_128_CBC_SHA,
                     TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CCM,
                     TLS_RSA_WITH_AES_256_CCM_8,
                     ...
```

Ulteriori informazioni su `security config show` nella "Riferimento al comando ONTAP".

Informazioni correlate

- "FIPS 203: Standard del meccanismo di incapsulamento delle chiavi basato su reticolo modulare (ML-KEM)"
- "FIPS 204: Standard di firma digitale basato su modulo-reticolo (ML-DSA)"
- "FIPS 205: Standard di firma digitale basato su hash senza stato (SLH-DSA)"

Configurare la crittografia IPSec in-flight

Preparare l'utilizzo della protezione IP sulla rete ONTAP

A partire da ONTAP 9.8, è possibile utilizzare la protezione IP (IPsec) per proteggere il traffico di rete. IPSec è una delle diverse opzioni di crittografia data-in-motion o in-flight disponibili con ONTAP. È necessario prepararsi a configurare IPsec prima di utilizzarlo in un ambiente di produzione.

Implementazione della protezione IP in ONTAP

IPSec è uno standard Internet gestito da IETF. Fornisce crittografia e integrità dei dati nonché autenticazione per il traffico che fluisce tra gli endpoint di rete a livello IP.

Con ONTAP, IPSec protegge tutto il traffico IP tra ONTAP e i vari client, inclusi i protocolli NFS, SMB e iSCSI. Oltre alla privacy e all'integrità dei dati, il traffico di rete è protetto da diversi attacchi, come il replay e gli attacchi man-in-the-middle. ONTAP utilizza l'implementazione della modalità di trasporto IPSec. Utilizza il protocollo IKE (Internet Key Exchange) versione 2 per negoziare il materiale chiave tra ONTAP e i client utilizzando IPv4 o IPv6.

Quando la funzionalità IPsec è attivata su un cluster, la rete richiede una o più voci nel database dei criteri di protezione ONTAP (SPD) corrispondenti alle varie caratteristiche del traffico. Queste voci vengono associate ai dettagli di protezione specifici necessari per elaborare e inviare i dati (ad esempio, la suite di crittografia e il metodo di autenticazione). È inoltre necessaria una voce SPD corrispondente in ogni client.

Per alcuni tipi di traffico, potrebbe essere preferibile un'altra opzione di crittografia dati in movimento. Ad esempio, per la crittografia del traffico NetApp SnapMirror e di peering dei cluster, si consiglia di utilizzare il protocollo TLS (Transport Layer Security) invece di IPSec. Ciò è dovuto al fatto che TLS offre prestazioni migliori nella maggior parte delle situazioni.

Informazioni correlate

- "Internet Engineering Task Force"
- "RFC 4301: Architettura di sicurezza per il protocollo Internet"

Evoluzione dell'implementazione di ONTAP IPSec

IPsec è stato introdotto per la prima volta con ONTAP 9.8. L'implementazione ha continuato a evolversi nelle successive versioni ONTAP , come descritto di seguito.

ONTAP 9.18.1

Il supporto per l'offload hardware IPsec è esteso al traffico IPv6.

ONTAP 9.17.1

Il supporto per l'offload hardware IPsec è esteso a "gruppi di aggregazione di link" . "Chiavi pre-condivise postquantistiche (PPK)" sono supportati per l'autenticazione con chiavi pre-condivise IPsec (PSK).

ONTAP 9.16.1

Molte delle operazioni crittografiche, come la crittografia e i controlli di integrità, possono essere scaricate su una scheda NIC supportata. Per ulteriori informazioni, vedere Funzione di offload dell'hardware IPSec .

ONTAP 9.12.1

Il supporto del protocollo host front-end IPSec è disponibile nelle configurazioni fabric-attached MetroCluster IP e MetroCluster. Il supporto IPSec fornito con i cluster MetroCluster è limitato al traffico host front-end e non è supportato nelle LIF intercluster MetroCluster.

ONTAP 9.10.1

Oltre alle PSK, è possibile utilizzare i certificati per l'autenticazione IPsec. Prima di ONTAP 9.10.1, solo le PSK erano supportate per l'autenticazione.

ONTAP 9.9.1

Gli algoritmi di crittografia utilizzati da IPSec sono validati con FIPS 140-2-2. Questi algoritmi vengono elaborati dal modulo crittografico di NetApp in ONTAP che esegue la convalida FIPS 140-2.

ONTAP 9.8

Il supporto per IPsec diventa inizialmente disponibile in base all'implementazione della modalità di trasporto.

Funzione di offload dell'hardware IPSec

Se si utilizza ONTAP 9.16,1 o versioni successive, è possibile eseguire l'offload di alcune operazioni a elaborazione intensiva, come la crittografia e i controlli di integrità, a una scheda NIC (Network Interface Controller) installata nel nodo di storage. La velocità di trasmissione per le operazioni scaricate sulla scheda NIC è di circa il 5% o inferiore. Ciò può migliorare significativamente le prestazioni e la velocità effettiva del traffico di rete protetto da IPsec.

Requisiti e raccomandazioni

Prima di utilizzare la funzione di offload dell'hardware IPsec, è necessario prendere in considerazione diversi requisiti.

Schede Ethernet supportate

È necessario installare e utilizzare solo schede Ethernet supportate. Le seguenti schede Ethernet sono supportate a partire da ONTAP 9.16.1:

- X50131A (controller Ethernet 2P, 40G/100g/200G/400G)
- X60132A (controller Ethernet 4P, 10G/25g)

ONTAP 9.17.1 aggiunge il supporto per le seguenti schede Ethernet:

- X50135A (controller Ethernet 2p, 40G/100G)
- X60135A (controller Ethernet 2p, 40G/100G)

Le schede X50131A e X50135A sono supportate sulle seguenti piattaforme:

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K
- AFF A90
- AFF A70

Le schede X60132A e X60135A sono supportate sulle seguenti piattaforme:

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20

Vedi il "NetApp Hardware Universe" per maggiori informazioni sulle piattaforme e sulle schede supportate.

Ambito del cluster

La funzione di offload dell'hardware IPSec è configurata globalmente per il cluster. Così, ad esempio, il comando `security ipsec config` si applica a tutti i nodi nel cluster.

Configurazione coerente

Le schede NIC supportate devono essere installate in tutti i nodi del cluster. Se una scheda NIC supportata è disponibile solo su alcuni dei nodi, è possibile riscontrare un peggioramento significativo delle prestazioni dopo un failover se alcune LIF non sono ospitate su una NIC con funzionalità offload.

Disattiva l'anti-ripetizione

È necessario disattivare la protezione anti-replay IPsec su ONTAP (configurazione predefinita) e sui client IPsec. Se non è disattivata, la frammentazione e il percorso multiplo (percorso ridondante) non saranno supportati.

Se la configurazione IPsec di ONTAP è stata modificata rispetto all'impostazione predefinita per attivare la protezione anti-replay, utilizzare questo comando per disattivarla:

```
security ipsec config modify -replay-window 0
```

È necessario verificare che la protezione anti-riproduzione IPsec sia disattivata sul client. Per disattivare la protezione anti-riproduzione, consultare la documentazione IPsec relativa al client.

Limitazioni

Prima di utilizzare la funzione di offload dell'hardware IPsec, è necessario prendere in considerazione diverse limitazioni.

IPv6

A partire da ONTAP 9.18.1, IPv6 è supportato per la funzionalità di offload hardware IPsec. Prima di ONTAP 9.18.1, l'offload hardware IPsec non supporta IPv6.

Numeri di sequenza estesi

I numeri di sequenza estesi IPsec non sono supportati con la funzione di offload hardware. Vengono utilizzati solo i normali numeri di sequenza a 32 bit.

Aggregazione dei collegamenti

A partire da ONTAP 9.17.1, è possibile utilizzare la funzionalità di offload hardware IPsec con un "gruppo di aggregazione di link" .

Prima della versione 9.17.1, la funzionalità di offload hardware IPsec non supporta l'aggregazione di link. Non può essere utilizzata con un'interfaccia o un gruppo di aggregazione di link amministrato tramite `network port ifgrp` comandi nella CLI ONTAP .

Supporto di configurazione nell'interfaccia a riga di comando di ONTAP

Tre comandi CLI esistenti vengono aggiornati in ONTAP 9.16,1 per supportare la funzione di offload dell'hardware IPsec come descritto di seguito. Per ulteriori informazioni, vedere anche"Configurare la protezione IP in ONTAP".

Comando ONTAP	Aggiornare
`security ipsec config show`	Il parametro booleano `Offload Enabled` mostra lo stato attuale di offload NIC.
`security ipsec config modify`	Il parametro `is-offload-enabled` può essere utilizzato per attivare o disattivare la funzione di offload NIC.
`security ipsec config show-ipsecsa`	Sono stati aggiunti quattro nuovi contatori per visualizzare il traffico in entrata e in uscita in byte e pacchetti.

Supporto della configurazione nell'API REST ONTAP

Due endpoint REST API esistenti vengono aggiornati in ONTAP 9.16,1 per supportare la funzione di offload hardware IPsec come descritto di seguito.

Endpoint REST	Aggiornare
`/api/security/ipsec`	Il parametro `offload_enabled` è stato aggiunto ed è disponibile con il metodo PATCH.

Endpoint REST	Aggiornare
`/api/security/ipsec/security_association`	Sono stati aggiunti due nuovi valori del contatore per tenere traccia dei byte totali e dei pacchetti elaborati dalla funzione di offload.

Ulteriori informazioni sull'API REST di ONTAP, incluso "Novità dell'API REST di ONTAP", nella documentazione di automazione di ONTAP. Per ulteriori informazioni su, consultare anche la documentazione relativa all'automazione di ONTAP "Endpoint IPSec" .

Informazioni correlate

- "sicurezza ipsec"

Configurare la protezione IP per la rete ONTAP

È necessario eseguire diverse attività per configurare e attivare la crittografia in-flight IPSec sul cluster ONTAP.

Assicurarsi di controllare "Prepararsi all'utilizzo della protezione IP" prima di configurare IPsec. Ad esempio, potrebbe essere necessario decidere se utilizzare la funzione di offload dell'hardware IPsec disponibile a partire da ONTAP 9.16,1.

Abilitare IPSec sul cluster

È possibile abilitare IPsec sul cluster per garantire che i dati vengano crittografati e protetti in modo continuo durante il trasferimento.

Fasi

1. Scopri se IPsec è già attivato:

   ```
   security ipsec config show
   ```

   Se il risultato include `IPsec Enabled: false`, passare alla fase successiva.

2. Attiva IPSec:

   ```
   security ipsec config modify -is-enabled true
   ```

   È possibile attivare la funzione di offload dell'hardware IPsec utilizzando il parametro booleano `is-offload-enabled` .

3. Eseguire nuovamente il comando di rilevamento:

   ```
   security ipsec config show
   ```

   Il risultato ora include `IPsec Enabled: true`.

Preparare la creazione del criterio IPsec con l'autenticazione del certificato

È possibile saltare questo passaggio se si utilizzano solo chiavi pre-condivise (PSK) per l'autenticazione e non si utilizza l'autenticazione del certificato.

Prima di creare un criterio IPsec che utilizza i certificati per l'autenticazione, è necessario verificare che siano soddisfatti i seguenti prerequisiti:

- Sia ONTAP che il client devono avere installato il certificato CA dell'altra parte in modo che i certificati dell'entità finale (ONTAP o client) siano verificabili da entrambe le parti
- Viene installato un certificato per il LIF ONTAP che partecipa al criterio

> Le LIF ONTAP possono condividere i certificati. Non è richiesta una mappatura uno-a-uno tra certificati e LIF.

Fasi

1. Installare tutti i certificati CA utilizzati durante l'autenticazione reciproca, incluse le CA lato ONTAP e lato client, nella gestione dei certificati ONTAP, a meno che non sia già installato (come nel caso di una CA root autofirmata di ONTAP).

   Comando di esempio
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. Per assicurarsi che la CA installata rientri nel percorso di ricerca della CA IPSec durante l'autenticazione, aggiungere le CA di gestione dei certificati ONTAP al modulo IPSec utilizzando `security ipsec ca-certificate add` comando.

   Comando di esempio
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. Creare e installare un certificato per l'utilizzo da parte della LIF ONTAP. La CA emittente di questo certificato deve essere già installata in ONTAP e aggiunta a IPSec.

   Comando di esempio
   ```
   cluster::> security certificate install -vserver svm_name -type server -cert
   -name my_nfs_server_cert
   ```

Per ulteriori informazioni sui certificati in ONTAP, vedere i comandi dei certificati di protezione nella documentazione di ONTAP 9.

Definizione del database dei criteri di protezione (SPD)

IPSec richiede una voce SPD prima di consentire il flusso del traffico sulla rete. Ciò vale sia che si utilizzi un PSK o un certificato per l'autenticazione.

Fasi

1. Utilizzare `security ipsec policy create` comando a:
   a. Selezionare l'indirizzo IP ONTAP o la subnet degli indirizzi IP per partecipare al trasporto IPSec.
   b. Selezionare gli indirizzi IP del client che si connetteranno agli indirizzi IP ONTAP.

      > Il client deve supportare Internet Key Exchange versione 2 (IKEv2) con una chiave precondivisa (PSK).

c. Facoltativamente, selezionare i parametri di traffico a grana fine, come i protocolli di livello superiore (UDP, TCP, ICMP, ecc.), i numeri di porta locali e i numeri di porta remota per proteggere il traffico. I parametri corrispondenti sono `protocols` , `local-ports` E `remote-ports` rispettivamente.

   Ignorare questo passaggio per proteggere tutto il traffico tra l'indirizzo IP ONTAP e l'indirizzo IP del client. La protezione di tutto il traffico è l'impostazione predefinita.

d. Immettere PSK o Public-Key Infrastructure (PKI) per `auth-method` parametro per il metodo di autenticazione desiderato.

   i. Se si immette una PSK, includere i parametri, quindi premere <enter> per visualizzare la richiesta di immissione e verifica della chiave precondivisa.

   > I `local-identity` parametri e `remote-identity` sono facoltativi se sia l'host che il client utilizzano lo standard "Swan" e non è stato selezionato alcun criterio wildcard per l'host o il client.

   ii. Se si inserisce un'infrastruttura PKI, è necessario immettere anche il `cert-name`, `local-identity`, `remote-identity` parametri. Se l'identità del certificato lato remoto non è nota o se sono previste più identità client, inserire l'identità speciale `ANYTHING`.

e. A partire da ONTAP 9.17.1, è possibile immettere facoltativamente un'identità PPK (pre-shared key) postquantistica con `ppk-identity` parametro. Le PPK offrono un ulteriore livello di sicurezza contro potenziali futuri attacchi ai computer quantistici. Quando si inserisce un'identità PPK, verrà richiesto di inserire il segreto PPK. Le PPK sono supportate solo per l'autenticazione PSK.

Scopri di più su `security ipsec policy create` nel "Riferimento al comando ONTAP" .

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

Il traffico IP non può passare tra il client e il server finché ONTAP e il client non hanno impostato i criteri IPSec corrispondenti e le credenziali di autenticazione (PSK o certificato) non sono installate su entrambi i lati.

Utilizzare le identità IPsec

Per il metodo di autenticazione con chiave pre-condivisa, le identità locali e remote sono facoltative se host e client utilizzano il metodo di autenticazione con chiave strongSwan e non è stato selezionato alcun criterio con caratteri jolly per l'host o il client.

Per il metodo di autenticazione PKI/certificato, le identità locali e remote sono obbligatorie. Le identità specificano l'identità certificata all'interno del certificato di ciascun lato e vengono utilizzate nel processo di verifica. Se l'identità remota è sconosciuta o se può essere costituita da diverse identità, utilizzare l'identità speciale `ANYTHING`.

A proposito di questa attività

All'interno di ONTAP, le identità vengono specificate modificando la voce SPD o durante la creazione del criterio SPD. Il nome SPD può essere un indirizzo IP o un nome di identità in formato stringa.

Fasi

1. Utilizzare il seguente comando per modificare un'impostazione di identità SPD esistente:

```
security ipsec policy modify
```

Comando di esempio

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

Configurazione di più client IPSec

Quando un numero limitato di client deve sfruttare IPSec, è sufficiente utilizzare una singola voce SPD per ciascun client. Tuttavia, quando centinaia o addirittura migliaia di client devono sfruttare IPSec, NetApp consiglia di utilizzare una configurazione con più client IPSec.

A proposito di questa attività

ONTAP supporta la connessione di più client su molte reti a un singolo indirizzo IP SVM con IPSec attivato. È possibile eseguire questa operazione utilizzando uno dei seguenti metodi:

- **Configurazione subnet**

  Per consentire a tutti i client di una determinata subnet (ad esempio 192.168.134.0/24) di connettersi a un singolo indirizzo IP SVM utilizzando una singola voce di policy SPD, è necessario specificare `remote-ip-subnets` sotto forma di subnet. Inoltre, è necessario specificare `remote-identity` campo con l'identità lato client corretta.

  > Quando si utilizza una singola voce di criterio in una configurazione di subnet, i client IPSec in tale subnet condividono l'identità IPSec e la chiave precondivisa (PSK). Tuttavia, questo non è vero con l'autenticazione del certificato. Quando si utilizzano i certificati, ciascun client può utilizzare il proprio certificato univoco o un certificato condiviso per l'autenticazione. IPSec ONTAP verifica la validità del certificato in base alle CA installate nel relativo archivio di attendibilità locale. ONTAP supporta anche il controllo dell'elenco di revoche di certificati (CRL).

- **Consenti configurazione di tutti i client**

  Per consentire a qualsiasi client, indipendentemente dall'indirizzo IP di origine, di connettersi all'indirizzo IP SVM abilitato a IPSec, utilizzare `0.0.0.0/0` carattere jolly quando si specifica `remote-ip-subnets` campo.

  Inoltre, è necessario specificare `remote-identity` campo con l'identità lato client corretta. Per l'autenticazione del certificato, è possibile immettere `ANYTHING`.

  Inoltre, quando `0.0.0.0/0` se si utilizza il carattere jolly, è necessario configurare un numero di porta locale o remota specifico da utilizzare. Ad esempio, `NFS port 2049`.

  Fasi

  a. Utilizzare uno dei seguenti comandi per configurare IPSec per più client.

i. Se si utilizza la **configurazione della subnet** per supportare più client IPsec:

```
security ipsec policy create -vserver vserver_name -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
IP_address/subnet -local-identity local_id -remote-identity remote_id
```

Comando di esempio

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
ontap_side_identity -remote-identity client_side_identity
```

i. Se si utilizza l'opzione **Allow all clients Configuration** (Consenti configurazione di tutti i client) per supportare più client IPsec:

```
security ipsec policy create -vserver vserver_name -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
-ports port_number -local-identity local_id -remote-identity remote_id
```

Comando di esempio

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

Visualizza le statistiche IPsec

Attraverso la negoziazione, è possibile stabilire un canale di sicurezza denominato SA (IKE Security Association) tra l'indirizzo IP di ONTAP SVM e l'indirizzo IP del client. I SAS IPSec vengono installati su entrambi gli endpoint per eseguire le operazioni di crittografia e decrittografia dei dati. È possibile utilizzare i comandi delle statistiche per controllare lo stato di IPSec SAS e IKE SAS.

Se si utilizza la funzione di offload dell'hardware IPsec, vengono visualizzati diversi nuovi contatori con il comando `security ipsec config show-ipsecsa`.

Comandi di esempio

Comando di esempio IKE SA:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

Comando e output di esempio SA IPSec:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

Comando e output di esempio SA IPSec:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

Informazioni correlate

- "installazione del certificato di sicurezza"
- "sicurezza ipsec"

Configurare la crittografia di rete del cluster backend ONTAP

A partire da ONTAP 9.18.1, è possibile configurare la crittografia Transport Layer Security (TLS) per i dati in transito sulla rete del cluster back-end. Questa crittografia protegge i dati dei clienti memorizzati in ONTAP quando vengono trasmessi tra i nodi ONTAP sulla rete del cluster back-end.

A proposito di questa attività

- Per impostazione predefinita, la crittografia della rete del cluster backend è disabilitata.
- Quando è abilitata la crittografia della rete del cluster backend, tutti i dati dei clienti archiviati in ONTAP vengono crittografati quando vengono trasmessi tra i nodi ONTAP sulla rete del cluster backend. Una parte del traffico di rete del cluster, come i dati del percorso di controllo, non è crittografata.
- Per impostazione predefinita, la crittografia della rete del cluster backend utilizzerà certificati generati automaticamente per ciascun nodo del cluster. PuoiGestire i certificati di crittografia della rete del cluster su ogni nodo per utilizzare un certificato installato personalizzato.

Prima di iniziare

- Devi essere un amministratore ONTAP presso `admin` livello di privilegio per eseguire le seguenti attività.
- Tutti i nodi del cluster devono eseguire ONTAP 9.18.1 o versione successiva per abilitare la crittografia della rete del cluster backend.

Abilita o disabilita la crittografia per la comunicazione di rete del cluster

Fasi

1. Visualizza lo stato attuale della crittografia della rete del cluster:

   ```
   security cluster-network show
   ```

   Questo comando mostra lo stato attuale della crittografia della rete del cluster:

   ```
   Cluster-1::*> security cluster-network show

   Enabled: true

   Mode: tls

   Status: READY
   ```

2. Abilita o disabilita la crittografia di rete del cluster backend TLS:

   ```
   security cluster-network modify -enabled <true|false>
   ```

   Questo comando abilita o disabilita la comunicazione crittografata per i dati dei clienti in transito sulla rete del cluster back-end.

Gestire i certificati di crittografia della rete del cluster

1. Visualizza le informazioni correnti sul certificato di crittografia della rete del cluster:

   ```
   security cluster-network certificate show
   ```

   Questo comando mostra le informazioni correnti sul certificato di crittografia della rete del cluster:

```
security cluster-network certificate show
Node                  Certificate Name                       CA
--------------------- -------------------------------------
--------------
node1                 -                                      Cluster-
1_Root_CA
node2                 -                                      Cluster-
1_Root_CA
node3                 google_issued_cert1                    Google_CA1
node4                 google_issued_cert2                    Google_CA1
```

Per ogni nodo del cluster vengono visualizzati i nomi dei certificati e delle autorità di certificazione (CA).

2. Modificare il certificato di crittografia della rete del cluster per un nodo:

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

Questo comando modifica il certificato di crittografia della rete del cluster per un nodo specifico. Prima di eseguire questo comando, il certificato deve essere installato e firmato da una CA installata. Per ulteriori informazioni sulla gestione dei certificati, fare riferimento a"Gestione dei certificati ONTAP con Gestione sistema" . Se `-name` Se non è specificato, viene utilizzato il certificato predefinito generato automaticamente.

Configurare i criteri del firewall per le LIF nella rete ONTAP

La configurazione di un firewall migliora la sicurezza del cluster e impedisce l'accesso non autorizzato al sistema di storage. Per impostazione predefinita, il firewall integrato è configurato in modo da consentire l'accesso remoto a un set specifico di servizi IP per le LIF di dati, gestione e intercluster.

A partire da ONTAP 9.10.1:

- Le policy firewall sono obsolete e vengono sostituite dalle policy di servizio LIF. In precedenza, il firewall integrato era gestito tramite policy firewall. Questa funzionalità viene ora eseguita utilizzando una policy di servizio LIF.
- Tutti i criteri firewall sono vuoti e non aprono porte nel firewall sottostante. Tutte le porte devono invece essere aperte utilizzando una policy di servizio LIF.
- Non è richiesta alcuna azione dopo un aggiornamento alla versione 9.10.1 o successiva per passare dalle policy firewall alle policy di servizio LIF. Il sistema crea automaticamente policy di servizio LIF coerenti con le policy firewall in uso nella release precedente di ONTAP. Se si utilizzano script o altri strumenti che creano e gestiscono policy firewall personalizzate, potrebbe essere necessario aggiornare tali script per creare policy di servizio personalizzate.

Per ulteriori informazioni, vedere "LIF e policy di servizio in ONTAP 9.6 e versioni successive".

Le policy firewall possono essere utilizzate per controllare l'accesso ai protocolli dei servizi di gestione come SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS O SNMP. Non è possibile impostare policy firewall per protocolli dati come NFS o SMB.

È possibile gestire il servizio firewall e le policy nei seguenti modi:

- Attivazione o disattivazione del servizio firewall
- Visualizzazione della configurazione corrente del servizio firewall
- Creazione di un nuovo criterio firewall con il nome del criterio e i servizi di rete specificati
- Applicazione di un criterio firewall a un'interfaccia logica
- Creazione di una nuova policy firewall che sia una copia esatta di una policy esistente

  È possibile utilizzare questa opzione per creare una policy con caratteristiche simili all'interno della stessa SVM o per copiare la policy su una SVM diversa.

- Visualizzazione di informazioni sui criteri firewall
- Modifica degli indirizzi IP e delle netmask utilizzati da una policy firewall
- Eliminazione di una policy firewall non utilizzata da una LIF

Policy firewall e LIF

I criteri firewall LIF vengono utilizzati per limitare l'accesso al cluster su ogni LIF. È necessario comprendere in che modo la policy firewall predefinita influenza l'accesso al sistema su ciascun tipo di LIF e come è possibile personalizzare una policy firewall per aumentare o ridurre la sicurezza su una LIF.

Quando si configura una LIF usando il `network interface create` comando OR `network interface modify`, il valore specificato per `-firewall-policy` il parametro determina i protocolli di servizio e gli indirizzi IP a cui è consentito l'accesso alla LIF. Ulteriori informazioni su `network interface` nella "Riferimento al comando ONTAP".

In molti casi è possibile accettare il valore predefinito del criterio firewall. In altri casi, potrebbe essere necessario limitare l'accesso a determinati indirizzi IP e a determinati protocolli dei servizi di gestione. I protocolli dei servizi di gestione disponibili includono SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS E SNMP.

Per impostazione predefinita, il criterio firewall per tutte le LIF del cluster è `""` e non possono essere modificati.

La tabella seguente descrive i criteri firewall predefiniti assegnati a ciascun LIF, in base al ruolo (ONTAP 9.5 e versioni precedenti) o ai criteri di servizio (ONTAP 9.6 e versioni successive), quando si crea il LIF:

Policy del firewall	Protocolli di servizio predefiniti	Accesso predefinito	LIF applicati a.
gestione	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Qualsiasi indirizzo (0.0.0.0/0)	Gestione del cluster, gestione SVM e LIF di gestione dei nodi

mgmt-nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Qualsiasi indirizzo (0.0.0.0/0)	Le LIF dei dati che supportano anche l'accesso alla gestione SVM
intercluster	https, ndmp, ndmps	Qualsiasi indirizzo (0.0.0.0/0)	Tutti i LIF intercluster
dati	dns, ndmp, ndmps, portmap	Qualsiasi indirizzo (0.0.0.0/0)	Tutti i dati LIF

Configurazione del servizio portmap

Il servizio portmap associa i servizi RPC alle porte su cui sono in ascolto.

Il servizio portmap era sempre accessibile in ONTAP 9.3 e versioni precedenti, è diventato configurabile in ONTAP 9.4 fino a ONTAP 9.6 e viene gestito automaticamente a partire da ONTAP 9.7.

- In ONTAP 9.3 e versioni precedenti, il servizio portmap (rpcbind) era sempre accessibile sulla porta 111 nelle configurazioni di rete che si basavano sul firewall ONTAP integrato anziché su un firewall di terze parti.
- Da ONTAP 9.4 a ONTAP 9.6, è possibile modificare i criteri del firewall per controllare se il servizio portmap è accessibile su specifiche LIF.
- A partire da ONTAP 9.7, il servizio firewall portmap viene eliminato. La porta portmap viene invece aperta automaticamente per tutti i LIF che supportano il servizio NFS.

Il servizio Portmap è configurabile nel firewall in ONTAP 9.4 fino a ONTAP 9.6.

Il resto di questo argomento illustra come configurare il servizio firewall portmap per le versioni da ONTAP 9.4 a ONTAP 9.6.

A seconda della configurazione, potrebbe essere possibile non consentire l'accesso al servizio su specifici tipi di LIF, in genere LIF di gestione e di intercluster. In alcuni casi, potresti persino essere in grado di impedire l'accesso alle LIF dei dati.

Quale comportamento ci si può aspettare

Il comportamento da ONTAP 9.4 a ONTAP 9.6 è progettato per fornire una transizione perfetta all'aggiornamento. Se si accede già al servizio portmap su specifici tipi di LIF, questo continuerà ad essere accessibile attraverso questi tipi di LIF. Come in ONTAP 9,3 e versioni precedenti, nella policy di firewall per il tipo di LIF è possibile specificare i servizi a cui accedere.

Tutti i nodi del cluster devono eseguire ONTAP 9.4 fino a ONTAP 9.6 per rendere effettivo il comportamento. Viene influenzato solo il traffico in entrata.

Le nuove regole sono le seguenti:

- All'aggiornamento alla versione 9.4 fino alla 9.6, ONTAP aggiunge il servizio portmap a tutte le policy firewall esistenti, predefinite o personalizzate.
- Quando si crea un nuovo cluster o un nuovo IPSpace, ONTAP aggiunge il servizio portmap solo al criterio dati predefinito, non ai criteri di gestione predefiniti o di intercluster.

- È possibile aggiungere il servizio portmap alle policy predefinite o personalizzate in base alle necessità e rimuovere il servizio in base alle necessità.

Come aggiungere o rimuovere il servizio portmap

Per aggiungere il servizio portmap a una policy SVM o del firewall del cluster (renderlo accessibile all'interno del firewall), immettere:

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Per rimuovere il servizio portmap da una policy SVM o del firewall del cluster (rendendolo inaccessibile all'interno del firewall), immettere:

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

È possibile utilizzare il comando di modifica dell'interfaccia di rete per applicare il criterio firewall a una LIF esistente. Per ulteriori informazioni sui comandi descritti in questa procedura, consultare la "Riferimento al comando ONTAP".

Creare una policy firewall e assegnarla a una LIF

I criteri firewall predefiniti vengono assegnati a ciascun LIF quando si crea il LIF. In molti casi, le impostazioni predefinite del firewall funzionano correttamente e non è necessario modificarle. Se si desidera modificare i servizi di rete o gli indirizzi IP che possono accedere a una LIF, è possibile creare una policy firewall personalizzata e assegnarla alla LIF.

A proposito di questa attività

- Non è possibile creare un criterio firewall con `policy` nome `data`, `intercluster`, `cluster`, o. `mgmt`.

  Questi valori sono riservati ai criteri firewall definiti dal sistema.

- Non è possibile impostare o modificare un criterio firewall per le LIF del cluster.

  Il criterio del firewall per le LIF del cluster è impostato su 0.0.0.0/0 per tutti i tipi di servizi.

- Se è necessario rimuovere un servizio da un criterio, è necessario eliminare il criterio firewall esistente e crearne uno nuovo.
- Se IPv6 è attivato nel cluster, è possibile creare policy firewall con indirizzi IPv6.

  Dopo aver attivato IPv6, `data`, `intercluster`, e. `mgmt` I criteri firewall includono ::/0, il carattere jolly IPv6, nell'elenco degli indirizzi accettati.

- Quando si utilizza System Manager per configurare la funzionalità di protezione dei dati tra cluster, è necessario assicurarsi che gli indirizzi IP LIF tra cluster siano inclusi nell'elenco consentito e che il servizio HTTPS sia consentito sia per le LIF tra cluster che per i firewall di proprietà dell'azienda.

  Per impostazione predefinita, il `intercluster` La policy firewall consente l'accesso da tutti gli indirizzi IP (0.0.0.0/0, o ::/0 per IPv6) e abilita i servizi HTTPS, NDMP e NDMPS. Se si modifica questo criterio predefinito o si crea un criterio firewall personalizzato per le LIF tra cluster, è necessario aggiungere ciascun indirizzo IP LIF tra cluster all'elenco consentito e attivare il servizio HTTPS.

- A partire da ONTAP 9.6, i servizi firewall HTTPS e SSH non sono supportati.

In ONTAP 9.6, il `management-https` e. `management-ssh` I servizi LIF sono disponibili per l'accesso alla gestione HTTPS e SSH.

Fasi

1. Creare una policy firewall che sarà disponibile per i LIF su una SVM specifica:

   `system services firewall policy create -vserver` *`vserver_name`* `-policy` *`policy_name`* `-service` *`network_service`* `-allow-list` *`ip_address/mask`*

   È possibile utilizzare questo comando più volte per aggiungere più di un servizio di rete e un elenco di indirizzi IP consentiti per ciascun servizio nella policy del firewall.

2. Verificare che il criterio sia stato aggiunto correttamente utilizzando `system services firewall policy show` comando.
3. Applicare il criterio firewall a una LIF:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. Verificare che il criterio sia stato aggiunto correttamente alla LIF utilizzando `network interface show -fields firewall-policy` comando.

   Ulteriori informazioni su `network interface show` nella "Riferimento al comando ONTAP".

Esempio di creazione di una policy firewall e di assegnazione a una LIF

Il seguente comando crea una policy firewall denominata data_http che abilita l'accesso ai protocolli HTTP e HTTPS dagli indirizzi IP sulla subnet 10.10, applica tale policy alla LIF denominata data1 su SVM vs1, quindi mostra tutte le policy firewall sul cluster:

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

Comandi ONTAP per la gestione dei criteri e del servizio firewall

È possibile utilizzare `system services firewall` comandi per la gestione del servizio firewall, il `system services firewall policy` comandi per la gestione delle policy firewall e di `network interface modify` Comando per gestire le impostazioni del firewall per le LIF.

A partire da ONTAP 9.10.1:

- Le policy firewall sono obsolete e vengono sostituite dalle policy di servizio LIF. In precedenza, il firewall integrato era gestito tramite policy firewall. Questa funzionalità viene ora eseguita utilizzando una policy di servizio LIF.
- Tutti i criteri firewall sono vuoti e non aprono porte nel firewall sottostante. Tutte le porte devono invece essere aperte utilizzando una policy di servizio LIF.
- Non è richiesta alcuna azione dopo un aggiornamento alla versione 9.10.1 o successiva per passare dalle policy firewall alle policy di servizio LIF. Il sistema crea automaticamente policy di servizio LIF coerenti con le policy firewall in uso nella release precedente di ONTAP. Se si utilizzano script o altri strumenti che creano e gestiscono policy firewall personalizzate, potrebbe essere necessario aggiornare tali script per creare policy di servizio personalizzate.

Per ulteriori informazioni, vedere "LIF e policy di servizio in ONTAP 9.6 e versioni successive".

Se si desidera…	Utilizzare questo comando…
Attiva o disattiva il servizio firewall	`system services firewall modify`
Visualizza la configurazione corrente per il servizio firewall	`system services firewall show`
Creare una policy firewall o aggiungere un servizio a una policy firewall esistente	`system services firewall policy create`
Applicare un criterio firewall a una LIF	`network interface modify -lif lifname -firewall-policy`
Modificare gli indirizzi IP e le netmask associate a un criterio firewall	`system services firewall policy modify`
Visualizza informazioni sui criteri firewall	`system services firewall policy show`
Creare una nuova policy firewall che sia una copia esatta di una policy esistente	`system services firewall policy clone`
Eliminare una policy firewall non utilizzata da una LIF	`system services firewall policy delete`

Informazioni correlate

- "firewall dei servizi di sistema"
- "modifica dell’interfaccia di rete"