Configurare la crittografia IPSec in-flight

ONTAP 9

NetApp
January 08, 2025

Sommario

Configurare la crittografia IPSec in-flight

Prepararsi all'utilizzo della protezione IP

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 ad evolversi e migliorare come descritto di seguito.

> Quando una funzionalità viene introdotta a partire da una specifica release di ONTAP, è supportata anche nelle versioni successive, se non diversamente specificato.

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

I certificati possono essere utilizzati per l'autenticazione IPsec oltre alle chiavi precondivise (PSK). Prima di ONTAP 9.10,1, per l'autenticazione sono supportati solo i PSK.

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. L'utilizzo di questa opzione di offload hardware può migliorare significativamente le prestazioni e il throughput 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 sui nodi di archiviazione. Con ONTAP 9.16,1 sono supportate le seguenti schede Ethernet:

- X50131A (controller Ethernet CX7 2P, 40G/100g/200G/400G)
- X60243A (4P, controller Ethernet 10G/25g CX7)

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.

Limitazioni

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

IPv6

La versione IP 6 non è supportata per la funzione di offload dell'hardware IPsec. IPv6 è supportato solo con l'implementazione del software IPsec.

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

La funzione di offload hardware IPsec non supporta l'aggregazione dei collegamenti. Pertanto, non può essere utilizzato con un'interfaccia o un gruppo di aggregazione dei collegamenti amministrato tramite i comandi all'interfaccia `network port ifgrp` CLI di 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.
`/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" .

Configurare la protezione IP in 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. Opzionale. Selezionare i parametri di traffico a grana fine, ad esempio i protocolli di livello superiore (UDP, TCP, ICMP, ecc.)), i numeri delle porte locali e i numeri delle porte remote 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`.

```
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 sul copyright

Informazioni sul marchio commerciale