Konfigurieren Sie die IPsec-Verschlüsselung während der Übertragung

ONTAP 9

NetApp
January 17, 2025

Inhalt

Konfigurieren Sie die IPsec-Verschlüsselung während der Übertragung

Bereiten Sie sich auf die Verwendung der IP-Sicherheit vor

Ab ONTAP 9.8 haben Sie die Möglichkeit, IP-Sicherheit (IPsec) zum Schutz Ihres Netzwerkverkehrs zu verwenden. IPsec ist eine von mehreren Data-in-Motion- oder in-Flight-Verschlüsselungsoptionen, die mit ONTAP verfügbar sind. Sie sollten die IPsec-Konfiguration vorbereiten, bevor Sie sie in einer Produktionsumgebung verwenden.

Implementierung der IP-Sicherheit in ONTAP

IPsec ist ein Internetstandard, der von der IETF verwaltet wird. Es bietet Datenverschlüsselung und -Integrität sowie Authentifizierung für den Datenverkehr, der auf IP-Ebene zwischen den Netzwerkendpunkten fließt.

Mit ONTAP sichert IPsec den gesamten IP-Datenverkehr zwischen ONTAP und den verschiedenen Clients, einschließlich der NFS-, SMB- und iSCSI-Protokolle. Neben Datenschutz und Datenintegrität ist der Netzwerkverkehr vor mehreren Angriffen wie Replay- und man-in-the-Middle-Angriffen geschützt. ONTAP verwendet die Implementierung des IPsec-Transportmodus. Er nutzt das IKE-Protokoll (Internet Key Exchange) Version 2 für die Verhandlung des Schlüsselmaterials zwischen ONTAP und den Clients, die entweder IPv4 oder IPv6 verwenden.

Wenn die IPsec-Funktion auf einem Cluster aktiviert ist, erfordert das Netzwerk einen oder mehrere Einträge in der ONTAP-Sicherheitsrichtliniendatenbank (SPD), die den verschiedenen Datenverkehrseigenschaften entsprechen. Diese Einträge werden den spezifischen Schutzdetails zugeordnet, die zum Verarbeiten und Senden der Daten erforderlich sind (z. B. Chiffre Suite und Authentifizierungsmethode). Ein entsprechender SPD-Eintrag ist ebenfalls bei jedem Client erforderlich.

Für bestimmte Arten von Datenverkehr ist möglicherweise eine andere Option zur Verschlüsselung von Daten in Bewegung vorzuziehen. Für die Verschlüsselung von NetApp SnapMirror- und Cluster-Peering-Datenverkehr wird beispielsweise das TLS-Protokoll (Transport Layer Security) anstelle von IPsec empfohlen. Das liegt daran, dass TLS in den meisten Situationen eine bessere Leistung bietet.

Verwandte Informationen

- "Internet Engineering Task Force"
- "RFC 4301: Sicherheitsarchitektur für das Internet Protocol"

Weiterentwicklung der ONTAP IPsec-Implementierung

IPsec wurde erstmals mit ONTAP 9.8 eingeführt. Die Umsetzung hat sich wie unten beschrieben weiterentwickelt und verbessert.

> Wenn eine Funktion, die mit einer bestimmten ONTAP Version eingeführt wird, wird sie auch in nachfolgenden Versionen unterstützt, sofern nicht anders angegeben.

ONTAP 9.16.1

Mehrere kryptografische Vorgänge, wie Verschlüsselungs- und Integritätsprüfungen, können auf eine unterstützte NIC-Karte verlagert werden. Weitere Informationen finden Sie unter IPsec-Hardware-Offload-Funktion .

ONTAP 9.12.1

Die Unterstützung von IPsec-Front-End-Hostprotokollen ist in MetroCluster-IP- und MetroCluster-Fabric-Attached-Konfigurationen verfügbar. Die durch MetroCluster Cluster bereitgestellte IPsec-Unterstützung für Cluster ist auf Front-End-Host-Datenverkehr beschränkt und wird auf MetroCluster LIFs nicht unterstützt.

ONTAP 9.10.1

Zusätzlich zu den vorab freigegebenen Schlüsseln (PSKs) können Zertifikate für die IPsec-Authentifizierung verwendet werden. Vor ONTAP 9.10.1 werden nur PSKs zur Authentifizierung unterstützt.

ONTAP 9.9.1

Die von IPsec verwendeten Verschlüsselungsalgorithmen sind nach FIPS 140-2 validiert. Diese Algorithmen werden vom NetApp Cryptographic Module in ONTAP verarbeitet, das die FIPS 140-2-2-Validierung führt.

ONTAP 9,8

Die Unterstützung für IPsec wird basierend auf der Implementierung des Transportmodus zunächst verfügbar.

IPsec-Hardware-Offload-Funktion

Wenn Sie ONTAP 9.16.1 oder höher verwenden, haben Sie die Möglichkeit, bestimmte rechenintensive Vorgänge, wie z. B. Verschlüsselungs- und Integritätsprüfungen, auf eine am Storage-Node installierte NIC-Karte (Network Interface Controller) zu übertragen. Durch die Verwendung dieser Hardware-Offload-Option können die Leistung und der Durchsatz des durch IPsec geschützten Netzwerkverkehrs erheblich verbessert werden.

Anforderungen und Empfehlungen

Vor der Verwendung der IPsec-Hardware-Offload-Funktion sollten Sie mehrere Anforderungen beachten.

Unterstützte Ethernet-Karten

Auf den Storage Nodes müssen nur unterstützte Ethernet-Karten installiert und verwendet werden. Die folgenden Ethernet-Karten werden von ONTAP 9.16.1 unterstützt:

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

Umfang des Clusters

Die IPsec-Hardware-Offload-Funktion ist global für den Cluster konfiguriert. Und so wird der Befehl beispielsweise `security ipsec config` auf alle Nodes im Cluster angewendet.

Konsistente Konfiguration

Unterstützte NIC-Karten sollten auf allen Knoten im Cluster installiert werden. Wenn eine unterstützte NIC-Karte nur auf einigen Nodes verfügbar ist, wird nach einem Failover eine deutliche Performance-Verschlechterung angezeigt, wenn einige der LIFs nicht auf einer Offload-fähigen NIC gehostet werden.

Anti-Replay deaktivieren

Sie sollten den IPsec-Anti-Replay-Schutz unter ONTAP (Standardkonfiguration) und den IPsec-Clients deaktivieren. Wenn diese Option nicht deaktiviert ist, werden Fragmentierung und Multi-Path (redundante Route) nicht unterstützt.

Einschränkungen

Vor der Verwendung der IPsec-Hardware-Offload-Funktion sollten Sie mehrere Einschränkungen

berücksichtigen.

IPv6

IP-Version 6 wird für die IPsec-Hardware-Offload-Funktion nicht unterstützt. IPv6 wird nur mit der IPsec-Softwareimplementierung unterstützt.

Erweiterte Sequenznummern

Die erweiterten IPsec-Sequenznummern werden von der Hardware-Offload-Funktion nicht unterstützt. Es werden nur die normalen 32-Bit-Sequenznummern verwendet.

Link-Aggregation

Die IPsec-Hardware-Offload-Funktion unterstützt keine Link-Aggregation. Und so kann es nicht mit einer Schnittstelle oder Link Aggregation Group verwendet werden, wie sie über die Befehle an der ONTAP CLI administriert `network port ifgrp` wird.

Konfigurationsunterstützung in der ONTAP-CLI

In ONTAP 9.16.1 werden drei vorhandene CLI-Befehle aktualisiert, um die IPsec-Hardware-Offload-Funktion wie unten beschrieben zu unterstützen. "Konfigurieren Sie die IP-Sicherheit in ONTAP"Weitere Informationen finden Sie unter.

ONTAP-Befehl	Aktualisieren
`security ipsec config show`	Der boolesche Parameter `Offload Enabled` zeigt den aktuellen NIC-Offload-Status an.
`security ipsec config modify`	Mit dem Parameter `is-offload-enabled` kann die NIC-Offload-Funktion aktiviert oder deaktiviert werden.
`security ipsec config show-ipsecsa`	Vier neue Zähler wurden hinzugefügt, um den ein- und ausgehenden Datenverkehr in Byte und Paketen anzuzeigen.

Konfigurationsunterstützung in der ONTAP-REST-API

Zwei vorhandene REST-API-Endpunkte werden in ONTAP 9.16.1 aktualisiert, um die IPsec-Hardware-Offload-Funktion wie unten beschrieben zu unterstützen.

REST-Endpunkt	Aktualisieren
`/api/security/ipsec`	Der Parameter `offload_enabled` wurde hinzugefügt und ist mit der PATCH-Methode verfügbar.
`/api/security/ipsec/security_association`	Zwei neue Zählerwerte wurden hinzugefügt, um die Gesamtzahl der von der Offload-Funktion verarbeiteten Bytes und Pakete zu verfolgen.

Weitere Informationen zur ONTAP REST-API einschließlich "Neuerungen an der ONTAP REST-API"finden Sie in der Dokumentation zur ONTAP Automatisierung. Weitere Informationen zu finden Sie auch in der Dokumentation zur ONTAP-Automatisierung "IPsec-Endpunkte".

Konfigurieren Sie die IP-Sicherheit in ONTAP

Zum Konfigurieren und Aktivieren der IPsec-Verschlüsselung während der Übertragung

auf Ihrem ONTAP-Cluster sind mehrere Aufgaben erforderlich.

Überprüfen Sie die "Bereiten Sie sich auf die Verwendung der IP-Sicherheit vor"Einstellungen, bevor Sie IPsec konfigurieren. Sie müssen beispielsweise entscheiden, ob Sie die ab ONTAP 9.16.1 verfügbare IPsec-Hardware-Offload-Funktion verwenden möchten.

Aktivieren Sie IPsec auf dem Cluster

Sie können IPsec auf dem Cluster aktivieren, um sicherzustellen, dass Daten während der Übertragung kontinuierlich verschlüsselt und sicher sind.

Schritte

1. Ermitteln, ob IPsec bereits aktiviert ist:

   ```
   security ipsec config show
   ```

   Wenn das Ergebnis enthält `IPsec Enabled: false`, fahren Sie mit dem nächsten Schritt fort.

2. IPsec aktivieren:

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

   Sie können die IPsec-Hardware-Offload-Funktion mit dem booleschen Parameter aktivieren `is-offload-enabled`.

3. Führen Sie den Ermittlungsbefehl erneut aus:

   ```
   security ipsec config show
   ```

   Das Ergebnis enthält nun `IPsec Enabled: true` .

Bereiten Sie die IPsec-Richtlinienerstellung mit Zertifikatauthentifizierung vor

Sie können diesen Schritt überspringen, wenn Sie nur PSKs (Pre-Shared Keys) zur Authentifizierung verwenden und keine Zertifikatauthentifizierung verwenden.

Bevor Sie eine IPsec-Richtlinie erstellen, die Zertifikate für die Authentifizierung verwendet, müssen Sie überprüfen, ob die folgenden Voraussetzungen erfüllt sind:

- Sowohl ONTAP als auch der Client müssen das CA-Zertifikat der anderen Partei installiert haben, damit die Zertifikate der Endeinheit (entweder ONTAP oder der Client) von beiden Seiten verifiziert werden können
- Für die ONTAP LIF, die an der Richtlinie teilnimmt, wird ein Zertifikat installiert

ONTAP LIFs können Zertifikate gemeinsam nutzen. Es ist keine 1:1-Zuordnung zwischen Zertifikaten und LIFs erforderlich.

Schritte

1. Installieren Sie alle während der gegenseitigen Authentifizierung verwendeten CA-Zertifikate, einschließlich ONTAP- und Client-seitiger CAS, in das ONTAP-Zertifikatsmanagement, sofern sie nicht bereits installiert ist (wie bei einer selbstsignierten ONTAP-Root-CA).

Beispielbefehl

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

2. Um sicherzustellen, dass sich die installierte CA während der Authentifizierung im IPsec-CA-Suchpfad befindet, fügen Sie mithilfe des `security ipsec ca-certificate add` Befehls die ONTAP-Zertifizierungsstelle für die Zertifikatsverwaltung zum IPsec-Modul hinzu.

   Beispielbefehl

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

3. Erstellen und installieren Sie ein Zertifikat zur Verwendung durch die LIF von ONTAP. Die Emittent-CA dieses Zertifikats muss bereits in ONTAP installiert und zu IPsec hinzugefügt werden.

   Beispielbefehl

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

Weitere Informationen zu Zertifikaten in ONTAP finden Sie in den Befehlen für Sicherheitszertifikate in der Dokumentation zu ONTAP 9.

Security Policy Database (SPD) definieren

IPsec erfordert einen SPD-Eintrag, bevor der Datenverkehr im Netzwerk fließen kann. Dies gilt unabhängig davon, ob Sie ein PSK oder ein Zertifikat zur Authentifizierung verwenden.

Schritte

1. Mit dem `security ipsec policy create` Befehl können Sie:
   a. Wählen Sie die ONTAP-IP-Adresse oder das Subnetz der IP-Adressen aus, die am IPsec-Transport beteiligt werden sollen.
   b. Wählen Sie die Client-IP-Adressen aus, die eine Verbindung zu den ONTAP-IP-Adressen herstellen.

      Der Client muss Internet Key Exchange Version 2 (IKEv2) mit einem vorab freigegebenen Schlüssel (PSK) unterstützen.

   c. Optional Wählen Sie die feingranularen Datenverkehrsparameter aus, z. B. die Protokolle der oberen Schicht (UDP, TCP, ICMP usw.), die lokalen Portnummern und die Remote-Portnummern zum Schutz des Datenverkehrs. Die entsprechenden Parameter sind `protocols`, `local-ports` `remote-ports` bzw. und.

      Überspringen Sie diesen Schritt, um den gesamten Datenverkehr zwischen der ONTAP-IP-Adresse und der Client-IP-Adresse zu schützen. Der Schutz des gesamten Datenverkehrs ist die Standardeinstellung.

   d. Geben Sie entweder PSK oder Public-Key-Infrastruktur (PKI) für den `auth-method` Parameter für die gewünschte Authentifizierungsmethode ein.
      i. Wenn Sie eine PSK eingeben, fügen Sie die Parameter ein, und drücken Sie dann <enter>, um die Aufforderung zur Eingabe und Überprüfung der zuvor freigegebenen Taste zu drücken.

Die `local-identity` Parameter und `remote-identity` sind optional, wenn sowohl Host als auch Client strongSwan verwenden und keine Platzhalterrichtlinie für den Host oder Client ausgewählt ist.

ii. Wenn Sie eine PKI eingeben, müssen Sie auch die `cert-name` `local-identity` `remote-identity` Parameter , , eingeben. Wenn die Identität des externen Zertifikats unbekannt ist oder mehrere Client-Identitäten erwartet werden, geben Sie die spezielle Identität ein `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
```

Der IP-Verkehr kann erst zwischen Client und Server übertragen werden, wenn sowohl ONTAP als auch der Client die entsprechenden IPsec-Richtlinien eingerichtet haben und die Authentifizierungsdaten (entweder PSK oder Zertifikat) auf beiden Seiten vorhanden sind.

Verwenden Sie IPsec-Identitäten

Bei der Authentifizierungsmethode für vorinstallierte Schlüssel sind lokale und Remote-Identitäten optional, wenn sowohl Host als auch Client strongSwan verwenden und keine Platzhalterrichtlinie für den Host oder Client ausgewählt ist.

Für die PKI/Zertifikat-Authentifizierungsmethode sind sowohl lokale als auch Remote-Identitäten zwingend erforderlich. Die Identitäten geben an, welche Identität innerhalb des Zertifikats jeder Seite zertifiziert ist und für den Überprüfungsprozess verwendet wird. Wenn die Remote-Identität unbekannt ist oder wenn es viele verschiedene Identitäten sein könnte, verwenden Sie die spezielle Identität `ANYTHING`.

Über diese Aufgabe

Innerhalb von ONTAP werden Identitäten durch Ändern des SPD-Eintrags oder während der Erstellung der SPD-Richtlinie festgelegt. Beim SPD kann es sich um einen Identitätsnamen im IP-Adressenformat oder String-Format handelt.

Schritte

1. Verwenden Sie den folgenden Befehl, um eine vorhandene SPD-Identitätseinstellung zu ändern:

```
security ipsec policy modify
```

Beispielbefehl

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

IPsec Konfiguration für mehrere Clients

Wenn eine kleine Anzahl von Clients IPsec nutzen muss, reicht die Verwendung eines einzelnen SPD-Eintrags für jeden Client aus. Wenn jedoch Hunderte oder gar Tausende von Clients IPsec nutzen müssen, empfiehlt NetApp die Verwendung einer IPsec Konfiguration für mehrere Clients.

Über diese Aufgabe

ONTAP unterstützt die Verbindung mehrerer Clients über mehrere Netzwerke mit einer einzelnen SVM-IP-Adresse, wobei IPsec aktiviert ist. Dies lässt sich mit einer der folgenden Methoden erreichen:

- **Subnetz-Konfiguration**

  Damit alle Clients in einem bestimmten Subnetz (z. B. 192.168.134.0/24) über einen einzigen SPD-Richtlinieneintrag eine Verbindung zu einer einzelnen SVM-IP-Adresse herstellen `remote-ip-subnets` können, müssen Sie das im Subnetz-Formular angeben. Außerdem müssen Sie das `remote-identity` Feld mit der korrekten clientseitigen Identität angeben.

  > Bei der Verwendung eines einzelnen Richtlinieneintrags in einer Subnetzkonfiguration teilen IPsec-Clients in diesem Subnetz die IPsec-Identität und den vorab gemeinsam genutzten Schlüssel (PSK). Dies gilt jedoch nicht für die Zertifikatauthentifizierung. Bei der Verwendung von Zertifikaten kann jeder Client sein eigenes eindeutiges Zertifikat oder ein freigegebenes Zertifikat zur Authentifizierung verwenden. ONTAP IPsec überprüft die Gültigkeit des Zertifikats auf der Grundlage des CAS, das auf seinem lokalen Vertrauensspeicher installiert ist. ONTAP unterstützt auch die Überprüfung der Zertifikatsperrliste (Certificate Revocation List, CRL).

- **Alle Clients konfigurieren** zulassen

  Damit jeder Client unabhängig von seiner Quell-IP-Adresse eine Verbindung zur IPsec-fähigen SVM-IP-Adresse `0.0.0.0/0` herstellen kann, verwenden Sie bei der Angabe des `remote-ip-subnets` Felds den Platzhalter.

  Außerdem müssen Sie das `remote-identity` Feld mit der korrekten clientseitigen Identität angeben. Für die Zertifikatauthentifizierung können Sie eingeben `ANYTHING`.

  Wenn der `0.0.0.0/0` Platzhalter verwendet wird, müssen Sie außerdem eine bestimmte lokale oder Remote-Portnummer konfigurieren, die verwendet werden soll. `NFS port 2049`Beispiel: .

  Schritte

  a. Verwenden Sie einen der folgenden Befehle, um IPsec für mehrere Clients zu konfigurieren.

     i. Wenn Sie **Subnetz-Konfiguration** zur Unterstützung mehrerer IPsec-Clients verwenden:

     ```
     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
     ```

     Beispielbefehl

     ```
     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. Wenn Sie **allow all Clients Configuration** verwenden, um mehrere IPsec-Clients zu unterstützen:

```
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
```

Beispielbefehl

```
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
```

Zeigt IPsec-Statistiken an

Während der Verhandlung kann ein Sicherheitskanal, der als IKE-Sicherheitszuordnung (SA) bezeichnet wird, zwischen der ONTAP SVM-IP-Adresse und der Client-IP-Adresse eingerichtet werden. IPsec SAS werden auf beiden Endpunkten installiert, um die eigentliche Datenverschlüsselung und -Entschlüsselung zu ermöglichen. Sie können Statistikbefehle verwenden, um den Status von IPsec SAS und IKE SAS zu überprüfen.

Wenn Sie die IPsec-Hardware-Offload-Funktion verwenden, werden mit dem Befehl mehrere neue Zähler angezeigt `security ipsec config show-ipsecsa`.

Beispielbefehle

IKE SA-Beispielbefehl:

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

IPsec SA-Beispielbefehl und -Ausgabe:

```
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
```

IPsec SA-Beispielbefehl und -Ausgabe:

```
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
```