IPsec In-Flight-Verschlüsselung konfigurieren

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/networking/ipsec-prepare.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

IPsec In-Flight-Verschlüsselung konfigurieren . . . 1
Informationen zur IP-Sicherheit im ONTAP Netzwerk . . . 1
IP-Security-Implementierung in ONTAP . . . 1
Evolution der ONTAP IPsec Implementierung . . . 1
IPsec Hardware Offload Funktion . . . 2
IP-Sicherheit für das ONTAP Netzwerk konfigurieren . . . 5
IPsec im Cluster aktivieren . . . 5
Vorbereitung der Erstellung der IPsec-Richtlinie mit Zertifikatsauthentifizierung . . . 5
Die Sicherheitsrichtliniendatenbank (SPD) definieren . . . 6
IPsec Identitäten nutzen . . . 7
IPsec Konfiguration für mehrere Clients . . . 8
IPsec-Statistiken anzeigen . . . 9

IPsec In-Flight-Verschlüsselung konfigurieren

Informationen zur IP-Sicherheit im ONTAP Netzwerk

Ab ONTAP 9.8 besteht die Möglichkeit, IP-Sicherheit (IPsec) zum Schutz des Netzwerkverkehrs zu verwenden. IPsec ist eine von mehreren Verschlüsselungsoptionen für Daten während der Übertragung, die mit ONTAP verfügbar sind. Vor der Nutzung von IPsec in einer Produktionsumgebung empfiehlt sich eine entsprechende Konfiguration.

IP-Security-Implementierung in ONTAP

IPsec ist ein vom IETF gepflegter Internetstandard. Es werden Datenverschlüsselung und -integrität sowie Authentifizierung für den Datenverkehr zwischen den Netzwerkendpunkten auf IP-Ebene bereitgestellt.

Mit ONTAP sichert IPsec den gesamten IP-Verkehr zwischen ONTAP und den verschiedenen Clients, einschließlich der Protokolle NFS, SMB und iSCSI. Neben Datenschutz und Datenintegrität ist der Netzwerkverkehr vor verschiedenen Angriffen wie Replay- und Man-in-the-Middle-Angriffen geschützt. ONTAP verwendet die IPsec Transportmodus-Implementierung. Dabei wird das Internet Key Exchange (IKE) Protokollversion 2 zur Aushandlung des Schlüsselmaterials zwischen ONTAP und den Clients über IPv4 oder IPv6 eingesetzt.

Wenn die IPsec-Funktion auf einem Cluster aktiviert ist, benötigt das Netzwerk einen oder mehrere Einträge in der ONTAP Security Policy Database (SPD), die den verschiedenen Verkehrseigenschaften entsprechen. Diese Einträge ordnen die spezifischen Schutzdetails zu, die für die Verarbeitung und Übertragung der Daten erforderlich sind (wie zum Beispiel Cipher Suite und Authentifizierungsverfahren). Ein entsprechender SPD-Eintrag ist auch auf jedem Client erforderlich.

Für bestimmte Arten von Datenverkehr kann eine andere Verschlüsselungsoption für Daten in Bewegung vorzuziehen sein. Beispielsweise wird für die Verschlüsselung von NetApp SnapMirror und Cluster-Peering-Datenverkehr im Allgemeinen das Transport Layer Security (TLS) Protokoll anstelle von IPsec empfohlen. Dies ist darauf zurückzuführen, dass TLS in den meisten Situationen eine bessere Leistung bietet.

Verwandte Informationen

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

Evolution der ONTAP IPsec Implementierung

IPsec wurde erstmals mit ONTAP 9.8 eingeführt. Die Implementierung hat sich in den nachfolgenden ONTAP Versionen wie unten beschrieben weiterentwickelt.

ONTAP 9.18.1

Die Unterstützung für IPsec-Hardware-Offload wurde auf IPv6-Datenverkehr ausgeweitet.

ONTAP 9.17.1

Die Unterstützung für IPsec Hardware-Offload wurde auf "Link-Aggregation-Gruppen" erweitert. "Postquantum Pre-Shared Keys (PPKs)" werden für die IPsec Pre-Shared-Key (PSK) Authentifizierung unterstützt.

ONTAP 9.16.1

Einige kryptografische Operationen, wie Verschlüsselung und Integritätsprüfungen, können auf eine unterstützte Netzwerkkarte ausgelagert werden. Siehe IPsec Hardware Offload Funktion für weitere

Informationen.

ONTAP 9.12.1

IPsec Frontend-Hostprotokollunterstützung ist in MetroCluster IP- und MetroCluster fabric-attached Konfigurationen verfügbar. Die mit MetroCluster Clustern bereitgestellte IPsec-Unterstützung ist auf Frontend-Host-Datenverkehr beschränkt und wird auf MetroCluster Intercluster-LIFs nicht unterstützt.

ONTAP 9.10.1

Zertifikate können für die IPsec-Authentifizierung zusätzlich zu den PSKs verwendet werden. Vor ONTAP 9.10.1 wurden für die Authentifizierung nur PSKs unterstützt.

ONTAP 9.9.1

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

ONTAP 9.8

Die Unterstützung für IPsec ist zunächst auf Basis der Implementierung des Transportmodus verfügbar.

IPsec Hardware Offload Funktion

Bei Verwendung von ONTAP 9.16.1 oder höher besteht die Möglichkeit, bestimmte rechenintensive Operationen wie Verschlüsselung und Integritätsprüfungen auf eine Netzwerkschnittstellenkarte (NIC), die im Speicherknoten installiert ist, auszulagern. Die Auswirkungen auf die Netzwerkdurchsatzleistung durch die Auslagerung der IPsec-Verschlüsselungsoperationen auf die NIC-Karte betragen im Vergleich zu Klartextoperationen ohne aktivierte IPsec-Verschlüsselung etwa 5 % oder weniger. Dadurch können die Leistung und der Durchsatz des durch IPsec geschützten Netzwerkverkehrs erheblich verbessert werden.

Anforderungen und Empfehlungen

Es gibt einige Voraussetzungen, die Sie beachten sollten, bevor Sie die IPsec Hardware-Offload-Funktion verwenden.

Unterstützte Ethernet Karten

Es dürfen nur unterstützte Ethernet-Karten installiert und verwendet werden. Die folgenden Ethernet-Karten werden ab ONTAP 9.16.1 unterstützt:

- X50131A (IO Modul, 2PT, 100/200GbE)
- X50131B (E/A-Modul, 2PT, 200/400GbE,B)
- X60132A (4p, 10G/25G-Ethernet-Controller)

ONTAP 9.17.1 bietet Unterstützung für die folgenden Ethernet Karten:

- X50135A (IO Modul, 2PT, 100GbE, Verschlüsselung)
- X60135A (2p, 40G/100G Ethernet-Controller)

Die Karten X50131A, X50131B und X50135A werden auf den folgenden Plattformen unterstützt:

- ASA A1K
- ASA A90
- ASA A70

- AFF A1K
- AFF A90
- AFF A70
- AFF C80
- FAS90
- FAS70

Die Karten X60132A und X60135A werden auf den folgenden Plattformen unterstützt:

- ASA A50
- ASA A30
- ASA A20
- ASA C30
- AFF A50
- AFF A30
- AFF A20
- AFF C60
- AFF C30
- FAS50

Weitere Informationen zu den unterstützten Plattformen und Karten enthält die "NetApp Hardware Universe".

Clusterbereich

Die IPsec-Hardware-Offload-Funktion ist global für den Cluster konfiguriert. Daher gilt beispielsweise der Befehl `security ipsec config` für alle Knoten im Cluster.

Konsistente Konfiguration

Unterstützte Netzwerkkarten sollten auf allen Knoten im Cluster installiert sein. Steht eine unterstützte Netzwerkkarte nur auf einigen Knoten zur Verfügung, kann es nach einem Failover zu erheblichen Leistungseinbußen kommen, wenn einige der LIFs nicht auf einer Offload-fähigen Netzwerkkarte gehostet sind.

Anti-Replay deaktivieren

IPsec-Anti-Replay-Schutz muss auf ONTAP (Standardkonfiguration) und den IPsec-Clients deaktiviert werden. Wenn dies nicht deaktiviert ist, werden Fragmentierung und Multi-Path (redundanter Pfad) nicht unterstützt.

Wenn die ONTAP IPsec Konfiguration von der Standardeinstellung geändert wurde, um den Anti-Replay-Schutz zu aktivieren, kann dieser Befehl verwendet werden, um ihn zu deaktivieren:

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

Sie müssen sicherstellen, dass der IPsec-Anti-Replay-Schutz auf Ihrem Client deaktiviert ist. In der IPsec-Dokumentation Ihres Clients finden sich Hinweise zum Deaktivieren des Anti-Replay-Schutzes.

Einschränkungen

Es gibt einige Einschränkungen, die vor der Verwendung der IPsec Hardware Offload-Funktion berücksichtigt werden sollten.

IPv6

Ab ONTAP 9.18.1 wird IPv6 für die IPsec Hardware Offload-Funktion unterstützt. Vor ONTAP 9.18.1 unterstützt die IPsec Hardware Offload-Funktion kein IPv6.

Erweiterte Sequenznummern

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

Link-Aggregation

Ab ONTAP 9.17.1 kann die IPsec Hardware-Offload-Funktion mit einem "Link-Aggregation-Gruppe" verwendet werden.

Vor Version 9.17.1 unterstützt die IPsec-Hardware-Offload-Funktion keine Link-Aggregation. Sie kann nicht mit einer Schnittstelle oder einer Link-Aggregation-Gruppe verwendet werden, wie sie über die `network port ifgrp` Befehle an der ONTAP CLI verwaltet wird.

Konfigurationsunterstützung in der ONTAP CLI

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

ONTAP Befehl	Aktualisieren
`security ipsec config show`	Der boolesche Parameter `Offload Enabled` zeigt den aktuellen NIC-Offload-Status an.
`security ipsec config modify`	Der Parameter `is-offload-enabled` kann verwendet werden, um die NIC-Offload-Funktion zu aktivieren oder zu deaktivieren.
`security ipsec config show-ipsecsa`	Vier neue Zähler wurden hinzugefügt, um den eingehenden sowie ausgehenden Datenverkehr in Bytes und Paketen anzuzeigen.

Konfigurationsunterstützung in der ONTAP REST API

Zwei bestehende 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 erfassen.

Weitere Informationen zur ONTAP REST API, einschließlich "Was ist neu bei der ONTAP REST API"aus der ONTAP Automation-Dokumentation. Auch die ONTAP Automatisierungsdokumentation enthält Details zu

"IPsec Endpunkte".

Verwandte Informationen

- "IPsec-Sicherheit"

IP-Sicherheit für das ONTAP Netzwerk konfigurieren

Es gibt mehrere Aufgaben, die zur Konfiguration und Aktivierung der IPsec-Verschlüsselung während der Übertragung auf Ihrem ONTAP Cluster erforderlich sind.

Stellen Sie sicher, dass "Vorbereitung auf die Nutzung von IP-Sicherheit" vor der Konfiguration von IPsec überprüft wird. Beispielsweise kann es erforderlich sein zu entscheiden, ob die ab ONTAP 9.16.1 verfügbare IPsec Hardware-Offload-Funktion verwendet werden soll.

IPsec im Cluster aktivieren

IPsec kann auf dem Cluster aktiviert werden, sodass die Daten während der Übertragung kontinuierlich verschlüsselt und geschützt sind.

Schritte

1. Es kann festgestellt werden, ob IPsec bereits aktiviert ist:

   ```
   security ipsec config show
   ```

   Falls das Ergebnis `IPsec Enabled: false` enthält, erfolgt der nächste Schritt.

2. IPsec aktivieren:

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

   Die IPsec Hardware Offload Funktion kann mit dem booleschen Parameter `is-offload-enabled` aktiviert werden.

3. Führen Sie den Erkennungsbefehl erneut aus:

   ```
   security ipsec config show
   ```

   Das Ergebnis umfasst nun `IPsec Enabled: true`.

Vorbereitung der Erstellung der IPsec-Richtlinie mit Zertifikatsauthentifizierung

Dieser Schritt kann übersprungen werden, wenn ausschließlich Pre-Shared Keys (PSKs) für die Authentifizierung verwendet werden und keine Zertifikatsauthentifizierung erfolgt.

Bevor eine IPsec-Richtlinie erstellt wird, die Zertifikate zur Authentifizierung verwendet, muss sichergestellt sein, dass die folgenden Voraussetzungen erfüllt sind:

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

ONTAP LIFs können Zertifikate gemeinsam nutzen. Eine Eins-zu-eins-Zuordnung zwischen Zertifikaten und LIFs ist nicht erforderlich.

Schritte

1. Alle während der gegenseitigen Authentifizierung verwendeten CA-Zertifikate, einschließlich sowohl der ONTAP-seitigen als auch der Client-seitigen CAs, in die ONTAP Zertifikatsverwaltung installieren, sofern sie nicht bereits installiert sind (wie im Fall einer ONTAP self-signed Root-CA).

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

2. Um sicherzustellen, dass die installierte Zertifizierungsstelle sich während der Authentifizierung im IPsec-CA-Suchpfad befindet, werden die ONTAP Zertifikatverwaltungs-Zertifizierungsstellen mithilfe des `security ipsec ca-certificate add` Befehls dem IPsec-Modul hinzugefügt.

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

3. Ein Zertifikat zur Verwendung durch den ONTAP LIF erstellen und installieren. Die ausstellende Zertifizierungsstelle dieses Zertifikats muss bereits auf ONTAP installiert und zu IPsec hinzugefügt sein.

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

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

Die Sicherheitsrichtliniendatenbank (SPD) definieren

IPsec erfordert einen SPD-Eintrag, bevor Datenverkehr im Netzwerk zugelassen wird. Dies gilt unabhängig davon, ob ein PSK oder ein Zertifikat für die Authentifizierung verwendet wird.

Schritte

1. Mit dem `security ipsec policy create`Befehl können Sie:
   a. Wählen Sie die ONTAP IP-Adresse oder das Subnetz von IP-Adressen aus, die am IPsec-Transport teilnehmen sollen.
   b. Wählen Sie die Client-IP-Adressen aus, die sich mit den ONTAP IP-Adressen verbinden.

      Der Client muss Internet Key Exchange Version 2 (IKEv2) mit einem Pre-Shared Key (PSK) unterstützen.

   c. Optional können die fein abgestuften Verkehrsparameter ausgewählt werden, wie die Protokolle der höheren Schichten (UDP, TCP, ICMP usw.), die lokalen Portnummern und die Remote-Portnummern zum Schutz des Datenverkehrs. Die entsprechenden Parameter sind `protocols`, `local-ports` und `remote-ports` jeweils.

      Diesen Schritt überspringen, 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-Infrastructure (PKI) für den `auth-method` Parameter des gewünschten Authentifizierungsverfahrens ein.

   i. Wenn Sie einen PSK eingeben, geben Sie die Parameter an und drücken Sie dann <enter> bei der Aufforderung, um den vorab vereinbarten Schlüssel einzugeben und zu überprüfen.

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

   ii. Wenn eine PKI eingegeben wird, müssen auch die `cert-name`, `local-identity`, `remote-identity` Parameter angegeben werden. Falls die Identität des Remote-Zertifikats unbekannt ist oder mehrere Client-Identitäten erwartet werden, ist die spezielle Identität `ANYTHING` einzugeben.

e. Ab ONTAP 9.17.1 kann optional eine Postquantum-Pre-Shared-Key-(PPK)-Identität mit dem `ppk-identity` Parameter eingegeben werden. PPKs bieten eine zusätzliche Sicherheitsebene gegen potenzielle zukünftige Angriffe durch Quantencomputer. Bei Eingabe einer PPK-Identität erfolgt eine Aufforderung zur Eingabe des PPK-Geheimnisses. PPKs werden nur für PSK-Authentifizierung unterstützt.

Weitere Informationen zu `security ipsec policy create` finden sich in der "ONTAP-Befehlsreferenz".

```
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-Datenverkehr kann zwischen Client und Server erst fließen, wenn sowohl ONTAP als auch der Client die passenden IPsec-Richtlinien eingerichtet haben und Authentifizierungsdaten (entweder PSK oder Zertifikat) auf beiden Seiten vorhanden sind.

IPsec Identitäten nutzen

Für das Authentifizierungsverfahren mit vorab gemeinsam genutztem Schlüssel sind lokale und Remote-Identitäten optional, wenn sowohl Host als auch Client strongSwan verwenden und keine Wildcard-Richtlinie für Host oder Client ausgewählt ist.

Für das PKI-/Zertifikat-Authentifizierungsverfahren sind sowohl lokale als auch Remote-Identitäten erforderlich. Die Identitäten geben an, welche Identität im jeweiligen Zertifikat zertifiziert ist und werden im Verifizierungsprozess verwendet. Ist die Remote-Identität unbekannt oder könnten mehrere verschiedene Identitäten vorliegen, sollte die spezielle Identität `ANYTHING` verwendet werden.

Über diese Aufgabe

In ONTAP werden Identitäten durch Ändern des SPD-Eintrags oder während der Erstellung der SPD-Richtlinie

festgelegt. Die SPD kann eine IP-Adresse oder ein Identitätsname im Zeichenkettenformat sein.

Schritte

1. Mit dem folgenden Befehl lässt sich eine bestehende SPD-Identitätseinstellung 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 nur wenige Clients IPsec nutzen müssen, genügt ein einzelner SPD-Eintrag pro Client. Wenn jedoch Hunderte oder sogar Tausende von Clients IPsec nutzen müssen, empfiehlt NetApp die Verwendung einer IPsec Multiple Client-Konfiguration.

Über diese Aufgabe

ONTAP unterstützt die Verbindung mehrerer Clients über verschiedene Netzwerke hinweg mit einer einzigen SVM-IP-Adresse, sofern IPsec aktiviert ist. Dies kann mit einer der folgenden Methoden erreicht werden:

- **Subnetzkonfiguration**

  Um allen Clients in einem bestimmten Subnetz (192.168.134.0/24 zum Beispiel) die Verbindung zu einer einzelnen SVM IP-Adresse mithilfe eines einzelnen SPD-Richtlinieneintrags zu ermöglichen, muss das `remote-ip-subnets` im Subnetz-Format angegeben werden. Zusätzlich muss das `remote-identity` Feld mit der korrekten Client-seitigen Identität angegeben werden.

  > Bei Verwendung eines einzelnen Richtlinieneintrags in einer Subnetzkonfiguration teilen sich IPsec-Clients in diesem Subnetz die IPsec-Identität und den vorab geteilten Schlüssel (PSK). Dies gilt jedoch nicht bei der Authentifizierung mit Zertifikaten. Bei Verwendung von Zertifikaten kann jeder Client entweder sein eigenes, eindeutiges Zertifikat oder ein gemeinsam genutztes Zertifikat zur Authentifizierung verwenden. ONTAP IPsec prüft die Gültigkeit des Zertifikats anhand der im lokalen Vertrauensspeicher installierten Zertifizierungsstellen (CAs). ONTAP unterstützt außerdem die Prüfung von Zertifikatssperrlisten (CRL).

- **Alle Clients Konfiguration zulassen**

  Um jedem Client, unabhängig von seiner Quell-IP-Adresse, die Verbindung mit der IPsec-aktivierten IP-Adresse der SVM zu ermöglichen, wird der Platzhalter `0.0.0.0/0` bei der Angabe des Felds `remote-ip-subnets` verwendet.

  Zusätzlich muss das `remote-identity` Feld mit der korrekten Client-seitigen Identität angegeben werden. Für die Zertifikatsauthentifizierung kann `ANYTHING` eingegeben werden.

  Außerdem muss bei Verwendung des `0.0.0.0/0` Wildcards eine bestimmte lokale oder Remote-Portnummer konfiguriert werden. Zum Beispiel `NFS port 2049`.

  Schritte

  a. Einer der folgenden Befehle dient zur Konfiguration von IPsec für mehrere Clients.

     i. Wenn Sie eine **Subnetzkonfiguration** 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
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 die Konfiguration **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
```

IPsec-Statistiken anzeigen

Durch Aushandlung kann ein Sicherheitskanal, eine sogenannte IKE Security Association (SA), 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 durchzuführen. Mit Statistikbefehlen lässt sich der Status sowohl der IPsec SAs als auch der IKE SAs überprüfen.

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

Beispielbefehle

IKE SA Beispielbefehl:

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

Beispielbefehl und Ausgabe für IPsec SA:

```
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
```

Beispielbefehl und Ausgabe für IPsec SA:

```
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
```

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "IPsec-Sicherheit"

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.