Schützen Sie Ihr Netzwerk

ONTAP 9

NetApp
October 08, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/networking/configure_network_security_using_federal_information_processing_standards_fips.html on October 08, 2026. Always check docs.netapp.com for the latest.

Inhalt

Schützen Sie Ihr Netzwerk . . . 1
ONTAP Netzwerksicherheit mit FIPS konfigurieren . . . 1
FIPS aktivieren . . . 2
FIPS deaktivieren . . . 3
FIPS-Konformitätsstatus anzeigen . . . 3
IPsec In-Flight-Verschlüsselung konfigurieren . . . 4
Informationen zur IP-Sicherheit im ONTAP Netzwerk . . . 4
IP-Sicherheit für das ONTAP Netzwerk konfigurieren . . . 8
ONTAP Backend Cluster-Netzwerkverschlüsselung konfigurieren . . . 13
Verschlüsselung für die Cluster-Netzwerkkommunikation aktivieren oder deaktivieren . . . 14
Cluster-Netzwerkverschlüsselungszertifikate verwalten . . . 14
ONTAP Firewall-Richtlinien für LIFs konfigurieren . . . 15
Firewall-Richtlinien und LIFs . . . 16
Portmap Service-Konfiguration . . . 17
Eine Firewall-Richtlinie erstellen und einer LIF zuweisen . . . 18
ONTAP TLS-Hardware-Offload konfigurieren . . . 20
TLS-Offload aktivieren oder deaktivieren . . . 22
ONTAP Befehle zur Verwaltung des Firewall-Dienstes und der Richtlinien . . . 23

Schützen Sie Ihr Netzwerk

ONTAP Netzwerksicherheit mit FIPS konfigurieren

ONTAP erfüllt die Federal Information Processing Standards (FIPS) für alle SSL-Verbindungen. Sie können den SSL FIPS Modus aktivieren und deaktivieren, SSL-Protokolle global festlegen und schwache Verschlüsselungsverfahren in ONTAP deaktivieren.

Die unterstützte FIPS Compliance hängt von Ihrer ONTAP Version ab:

Unterstützte FIPS Compliance	ONTAP Release
FIPS 140-3	• 9.19.1P2 und später • 9.18.1P6 und spätere 9.18.1-Patch-Versionen
FIPS 140-2	• 9.19.1 • 9.19.1P1 • 9.18.1P5 und früher

Standardmäßig ist SSL auf ONTAP so konfiguriert, dass die FIPS-Konformität deaktiviert ist und die folgenden TLS-Protokolle aktiviert sind:

- TLSv1.3 (beginnend mit ONTAP 9.11.1)
- TLSv1.2

In früheren ONTAP Versionen waren die folgenden TLS-Protokolle standardmäßig aktiviert:

- TLSv1.1 (standardmäßig deaktiviert ab ONTAP 9.12.1)
- TLSv1 (ab ONTAP 9.8 standardmäßig deaktiviert)

Wenn der SSL-FIPS-Modus aktiviert ist, verwendet die SSL-Kommunikation von ONTAP zu externen Client- oder Serverkomponenten außerhalb von ONTAP FIPS-konforme Verschlüsselung für SSL.

Wenn Administratorkonten mit einem öffentlichen SSH-Schlüssel auf SVMs zugreifen sollen, muss sichergestellt werden, dass der Host-Algorithmus unterstützt wird, bevor der SSL FIPS-Modus aktiviert wird.

Hinweis: Die Unterstützung für Host-Key-Algorithmen hat sich in ONTAP 9.11.1 und späteren Versionen geändert.

ONTAP Release	Unterstützte Schlüsseltypen	Nicht unterstützte Schlüsseltypen
9.11.1 und später	ecdsa-sha2-nistp256	rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 und früher	ecdsa-sha2-nistp256 + ssh-ed25519	ssh-dss + ssh-rsa

Sie müssen bestehende SSH-Public-Key-Konten so umkonfigurieren, dass sie einen unterstützten Schlüsseltyp verwenden, bevor Sie FIPS aktivieren, oder die Administratorauthentifizierung schlägt fehl.

Weitere Informationen finden sich unter "SSH-Zugriff mit öffentlichem Schlüssel für ein ONTAP Administratorkonto wird aktiviert".

ONTAP 9.18.1 führt die Unterstützung für die Post-Quanten-Kryptografiealgorithmen ML-KEM, ML-DSA und SLH-DSA für SSL ein und bietet damit eine zusätzliche Sicherheitsebene gegen potenzielle zukünftige Quantencomputerangriffe. Diese Algorithmen sind nur verfügbar, wenn FIPS ist deaktiviert. Post-Quanten-Kryptografiealgorithmen werden ausgehandelt, wenn FIPS deaktiviert ist und der Peer sie unterstützt.

FIPS aktivieren

Es wird empfohlen, dass alle sicheren Benutzer ihre Sicherheitskonfiguration unmittelbar nach der Systeminstallation oder -aktualisierung anpassen. Wenn der SSL-FIPS-Modus aktiviert ist, verwendet die SSL-Kommunikation von ONTAP zu externen Client- oder Serverkomponenten außerhalb von ONTAP FIPS-konforme Verschlüsselung für SSL.

Wenn FIPS aktiviert ist, kann kein Zertifikat mit einer RSA-Schlüssellänge von 4096 installiert oder erstellt werden.

Schritte

1. Wechsel zum erweiterten Berechtigungslevel:

   ```
   set -privilege advanced
   ```

2. FIPS aktivieren:

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

3. Wenn Sie zur Fortsetzung aufgefordert werden, geben Sie Folgendes ein: `y`
4. Ab ONTAP 9.9.1 ist kein Neustart mehr erforderlich. Wenn Sie ONTAP 9.8 oder früher verwenden, starten Sie jeden Knoten im Cluster einzeln manuell neu.

Beispiel

Wenn Sie ONTAP 9.9.1 oder eine neuere Version verwenden, wird Ihnen diese Warnmeldung nicht angezeigt.

```
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
```

Weitere Informationen zu `security config modify` und zur Konfiguration des SSL FIPS-Modus finden Sie in der "ONTAP-Befehlsreferenz".

FIPS deaktivieren

Ab ONTAP 9.18.1 unterstützt SSL in ONTAP die Post-Quanten-Computing-Kryptografie-Algorithmen ML-KEM, ML-DSA und SLH-DSA. Diese Algorithmen sind nur verfügbar, wenn FIPS deaktiviert ist und der Peer sie unterstützt.

Schritte

1. Wechsel zum erweiterten Berechtigungslevel:

   ```
   set -privilege advanced
   ```

2. FIPS wird deaktiviert durch Eingabe von:

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

3. Wenn Sie zur Fortsetzung aufgefordert werden, `y` eingeben.
4. Ab ONTAP 9.9.1 ist kein Neustart mehr erforderlich. Wenn ONTAP 9.8 oder eine frühere Version verwendet wird, ist ein manueller Neustart jedes Knotens im Cluster erforderlich.

Wenn Sie das SSLv3-Protokoll verwenden müssen, müssen Sie FIPS mit dem oben beschriebenen Verfahren deaktivieren. SSLv3 kann nur aktiviert werden, wenn FIPS deaktiviert ist.

Sie können SSLv3 mit dem folgenden Befehl aktivieren. Wenn Sie ONTAP 9.9.1 oder später verwenden, wird keine Warnmeldung angezeigt.

```
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
```

FIPS-Konformitätsstatus anzeigen

Es ist ersichtlich, ob der gesamte Cluster mit den aktuellen Sicherheitskonfigurationseinstellungen arbeitet.

Schritte

1. Wenn Sie ONTAP 9.8 oder früher verwenden, starten Sie jeden Knoten im Cluster einzeln manuell neu.

2. Aktueller Compliance-Status:

   `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,
                     ...
```

   Weitere Informationen zu `security config show` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "FIPS 203: Standard für einen Modul-Gitter-basierten Schlüsselkapselungsmechanismus (ML-KEM)"
- "FIPS 204: Modulgitter-basierter digitaler Signaturstandard (ML-DSA)"
- "FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)"
- "TLS-Hardware-Offload konfigurieren"

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"

ONTAP Backend Cluster-Netzwerkverschlüsselung konfigurieren

Ab ONTAP 9.18.1 kann die Transport Layer Security (TLS)-Verschlüsselung für Daten während der Übertragung im Backend-Cluster-Netzwerk konfiguriert werden. Diese Verschlüsselung schützt Kundendaten, die in ONTAP gespeichert sind, wenn sie zwischen ONTAP Knoten im Backend-Cluster-Netzwerk übertragen werden.

Über diese Aufgabe

- Die Backend Cluster Netzwerkverschlüsselung ist standardmäßig deaktiviert.
- Wenn die Verschlüsselung des Backend-Clusternetzwerks aktiviert ist, werden alle in ONTAP gespeicherten Kundendaten bei der Übertragung zwischen ONTAP Knoten im Backend-Clusternetzwerk verschlüsselt. Bestimmte Netzwerkdaten des Clusters, wie Steuerungspfaddaten, werden nicht verschlüsselt.
- Standardmäßig verwendet die Backend-Cluster-Netzwerkverschlüsselung automatisch generierte Zertifikate für jeden Knoten im Cluster. Sie können Cluster-Netzwerkverschlüsselungszertifikate verwalten auf jedem Knoten ein benutzerdefiniertes installiertes Zertifikat verwenden.

Bevor Sie beginnen

- Sie müssen ONTAP Administrator auf der `admin`-Berechtigungsstufe sein, um die folgenden Aufgaben auszuführen.
- Alle Knoten im Cluster müssen ONTAP 9.18.1 oder höher ausführen, damit die Backend Cluster-Netzwerkverschlüsselung aktiviert werden kann.

Verschlüsselung für die Cluster-Netzwerkkommunikation aktivieren oder deaktivieren

Schritte

1. Aktueller Verschlüsselungsstatus des Clusternetzwerks:

   ```
   security cluster-network show
   ```

   Dieser Befehl zeigt den aktuellen Status der Cluster-Netzwerkverschlüsselung an:

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

   Enabled: true

   Mode: tls

   Status: READY
   ```

2. Aktivieren oder Deaktivieren der TLS-Backend-Cluster-Netzwerkverschlüsselung:

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

   Dieser Befehl aktiviert oder deaktiviert die verschlüsselte Kommunikation für Kundendaten während der Übertragung im Backend-Cluster-Netzwerk.

Cluster-Netzwerkverschlüsselungszertifikate verwalten

1. Aktuelle Informationen zum Cluster-Netzwerkverschlüsselungszertifikat:

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

Dieser Befehl zeigt die aktuellen Informationen zum Cluster Netzwerkverschlüsselungszertifikat an:

```
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
```

Die Namen des Zertifikats und der Zertifizierungsstelle (CA) werden für jeden Knoten im Cluster angezeigt.

2. Das Clusternetzwerk-Verschlüsselungszertifikat für einen Knoten ändern:

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

Dieser Befehl ändert das Cluster-Netzwerkverschlüsselungszertifikat für einen bestimmten Knoten. Das Zertifikat muss vor der Ausführung dieses Befehls installiert und von einer installierten Zertifizierungsstelle signiert sein. Weitere Informationen zur Zertifikatsverwaltung finden sich unter "ONTAP Zertifikate mit System Manager verwalten". Wenn `-name` nicht angegeben wird, wird das automatisch generierte Standardzertifikat verwendet.

ONTAP Firewall-Richtlinien für LIFs konfigurieren

Die Einrichtung einer Firewall erhöht die Sicherheit des Clusters und hilft, unbefugten Zugriff auf das Speichersystem zu verhindern. Standardmäßig ist die integrierte Firewall so konfiguriert, dass der Fernzugriff auf eine bestimmte Gruppe von IP-Services für Daten-, Verwaltungs- und Intercluster-LIFs möglich ist.

Ab ONTAP 9.10.1:

- Firewall-Richtlinien sind veraltet und werden durch LIF-Dienstrichtlinien ersetzt. Zuvor wurde die integrierte Firewall mithilfe von Firewall-Richtlinien verwaltet. Diese Funktionalität wird jetzt mit einer LIF-Dienstrichtlinie umgesetzt.
- Alle Firewall-Richtlinien sind leer und öffnen keine Ports in der zugrunde liegenden Firewall. Stattdessen müssen alle Ports über eine LIF-Dienstrichtlinie geöffnet werden.
- Nach einem Upgrade auf Version 9.10.1 oder höher ist kein weiteres Vorgehen erforderlich, um von Firewall-Richtlinien auf LIF-Dienstrichtlinien umzustellen. Das System erstellt automatisch LIF-Dienstrichtlinien, die mit den in der vorherigen ONTAP Version verwendeten Firewall-Richtlinien konsistent

sind. Wenn Skripte oder andere Tools verwendet werden, die benutzerdefinierte Firewall-Richtlinien erstellen und verwalten, kann es erforderlich sein, diese Skripte so anzupassen, dass stattdessen benutzerdefinierte Dienstrichtlinien erstellt werden.

Weitere Informationen finden sich unter "LIFs und Servicerichtlinien in ONTAP 9.6 und später".

Firewall-Richtlinien können verwendet werden, um den Zugriff auf Management-Service-Protokolle wie SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS oder SNMP zu steuern. Für Datenprotokolle wie NFS oder SMB können keine Firewall-Richtlinien festgelegt werden.

Der Firewall-Service und die zugehörigen Richtlinien lassen sich auf folgende Weise verwalten:

- Aktivieren oder Deaktivieren des Firewall-Service
- Anzeige der aktuellen Firewall-Service-Konfiguration
- Erstellen einer neuen Firewall-Richtlinie mit dem angegebenen Richtliniennamen und Netzwerkservices
- Anwenden einer Firewall-Richtlinie auf eine logische Schnittstelle
- Erstellung einer neuen Firewall-Richtlinie, die eine exakte Kopie einer bestehenden Richtlinie ist

  Dies kann verwendet werden, um eine Richtlinie mit ähnlichen Eigenschaften innerhalb desselben SVM zu erstellen oder die Richtlinie in einen anderen SVM zu kopieren.

- Anzeige von Informationen zu Firewall-Richtlinien
- Ändern der von einer Firewall-Richtlinie verwendeten IP-Adressen und Netzmasken
- Löschen einer Firewall-Richtlinie, die nicht von einer LIF verwendet wird

Firewall-Richtlinien und LIFs

LIF-Firewallrichtlinien werden verwendet, um den Zugriff auf den Cluster über jede LIF einzuschränken. Es ist wichtig zu verstehen, wie sich die Standard-Firewallrichtlinie auf den Systemzugriff über die einzelnen LIF-Typen auswirkt und wie eine Firewallrichtlinie angepasst werden kann, um die Sicherheit über eine LIF zu erhöhen oder zu verringern.

Bei der Konfiguration einer LIF mit dem `network interface create` oder `network interface modify` Befehl legt der für den `-firewall-policy` Parameter angegebene Wert fest, welche Serviceprotokolle und IP-Adressen Zugriff auf die LIF erhalten. Weitere Informationen zu `network interface` finden sich in der "ONTAP-Befehlsreferenz".

In vielen Fällen kann der Standardwert der Firewall-Richtlinie übernommen werden. In anderen Fällen kann es erforderlich sein, den Zugriff auf bestimmte IP-Adressen und bestimmte Management-Service-Protokolle einzuschränken. Zu den verfügbaren Management-Service-Protokollen gehören SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS und SNMP.

Die Firewall-Richtlinie für alle Cluster-LIFs ist standardmäßig auf `""` festgelegt und kann nicht geändert werden.

Die folgende Tabelle beschreibt die Standard-Firewall-Richtlinien, die jedem LIF je nach seiner Rolle (ONTAP 9.5 und früher) oder Service-Policy (ONTAP 9.6 und später) beim Erstellen des LIF zugewiesen werden:

Firewall-Richtlinie	Standard-Serviceprotokolle	Standardzugriff	LIFs angewendet auf

mgmt	DNS, HTTP, HTTPS, NDMP, NDMPS, NTP, SNMP, SSH	Beliebige Adresse (0.0.0.0/0)	Clusterverwaltung, SVM-Verwaltung und Knotenverwaltung LIFs
mgmt-nfs	DNS, HTTP, HTTPS, NDMP, NDMPS, NTP, Portmap, SNMP, SSH	Beliebige Adresse (0.0.0.0/0)	Daten-LIFs, die auch den SVM-Managementzugriff unterstützen
Intercluster	https, ndmp, ndmps	Beliebige Adresse (0.0.0.0/0)	Alle Intercluster-LIFs
Daten	dns, ndmp, ndmps, portmap	Beliebige Adresse (0.0.0.0/0)	Alle Daten-LIFs

Portmap Service-Konfiguration

Der Portmap-Service ordnet RPC-Services den Ports zu, auf denen sie lauschen.

Der Portmap-Service war in ONTAP 9.3 und früher immer zugänglich, wurde in ONTAP 9.4 bis ONTAP 9.6 konfigurierbar und wird ab ONTAP 9.7 automatisch verwaltet.

- In ONTAP 9.3 und früher war der Portmap-Service (rpcbind) in Netzwerkkonfigurationen, die auf die integrierte ONTAP Firewall und nicht auf eine Firewall eines Drittanbieters angewiesen waren, immer auf Port 111 zugänglich.
- Von ONTAP 9.4 bis ONTAP 9.6 besteht die Möglichkeit, Firewall-Richtlinien zu ändern, um zu steuern, ob der Portmap-Dienst auf bestimmten LIFs zugänglich ist.
- Ab ONTAP 9.7 entfällt der portmap Firewall-Service. Stattdessen wird der portmap Port automatisch für alle LIFs geöffnet, die den NFS-Service unterstützen.

Der Portmap-Service ist in der Firewall in ONTAP 9.4 bis ONTAP 9.6 konfigurierbar.

Im weiteren Verlauf dieses Themas wird beschrieben, wie der Portmap-Firewall-Service für ONTAP 9.4 bis ONTAP 9.6 konfiguriert wird.

Je nach Konfiguration können Sie den Zugriff auf den Service auf bestimmten Typen von LIFs, typischerweise Management- und Intercluster-LIFs, untersagen. Unter bestimmten Umständen kann der Zugriff sogar auf Daten-LIFs untersagt werden.

Welches Verhalten Sie erwarten können

Das Verhalten von ONTAP 9.4 bis ONTAP 9.6 ist darauf ausgelegt, einen nahtlosen Übergang beim Upgrade zu ermöglichen. Wenn der portmap-Service bereits über bestimmte Typen von logischen Schnittstellen (LIFs) genutzt wird, bleibt der Zugriff über diese Typen von LIFs weiterhin möglich. Wie bei ONTAP 9.3 und früher kann in der Firewall-Richtlinie für den LIF-Typ festgelegt werden, welche Dienste innerhalb der Firewall zugänglich sind.

Alle Knoten im Cluster müssen ONTAP 9.4 bis ONTAP 9.6 ausführen, damit das Verhalten wirksam wird. Nur der eingehende Datenverkehr ist betroffen.

Die neuen Regeln lauten wie folgt:

- Beim Upgrade auf Version 9.4 bis 9.6 fügt ONTAP den Portmap-Service zu allen bestehenden Firewall-Richtlinien hinzu, sowohl zu Standard- als auch zu benutzerdefinierten.
- Wenn ein neuer Cluster oder ein neuer IPspace erstellt wird, fügt ONTAP den Portmap-Dienst nur der Standard-Datenrichtlinie hinzu, nicht jedoch den Standard-Management- oder Intercluster-Richtlinien.

- Der Portmap-Dienst kann nach Bedarf zu Standard- oder benutzerdefinierten Richtlinien hinzugefügt und bei Bedarf entfernt werden.

Hinzufügen oder Entfernen des Portmap-Dienstes

Um den Portmap-Dienst zu einer SVM- oder Cluster-Firewall-Richtlinie hinzuzufügen (damit er innerhalb der Firewall zugänglich ist), ist Folgendes einzugeben:

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

Um den Portmap-Dienst aus einer SVM- oder Cluster-Firewall-Richtlinie zu entfernen (damit er innerhalb der Firewall nicht zugänglich ist), eingeben:

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

Sie können den Befehl „network interface modify“ verwenden, um die Firewall-Richtlinie auf eine bestehende LIF anzuwenden. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Eine Firewall-Richtlinie erstellen und einer LIF zuweisen

Standardmäßige Firewall-Richtlinien werden jedem LIF zugewiesen, wenn das LIF erstellt wird. In vielen Fällen funktionieren die standardmäßigen Firewall-Einstellungen gut und müssen nicht geändert werden. Wenn die Netzwerkservices oder IP-Adressen geändert werden sollen, die auf ein LIF zugreifen können, kann eine benutzerdefinierte Firewall-Richtlinie erstellt und dem LIF zugewiesen werden.

Über diese Aufgabe

- Es kann keine Firewall-Richtlinie mit dem `policy` Namen `data`, `intercluster`, `cluster` oder `mgmt` erstellt werden.

  Diese Werte sind für die systemdefinierten Firewall-Richtlinien reserviert.

- Für Cluster-LIFs kann keine Firewall-Richtlinie festgelegt oder geändert werden.

  Die Firewall-Richtlinie für Cluster-LIFs ist für alle Service-Typen auf 0.0.0.0/0 eingestellt.

- Wenn ein Dienst aus einer Richtlinie entfernt werden soll, ist die bestehende Firewall-Richtlinie zu löschen und eine neue Richtlinie zu erstellen.
- Wenn IPv6 auf dem Cluster aktiviert ist, ist das Erstellen von Firewall-Richtlinien mit IPv6-Adressen möglich.

  Nach der Aktivierung von IPv6 `data`, `intercluster` und `mgmt` enthalten die Firewall-Richtlinien ::/0, den IPv6-Wildcard-Eintrag, in ihrer Liste der akzeptierten Adressen.

- Bei der Verwendung von System Manager zur Konfiguration der Datensicherungsfunktionen über Cluster hinweg muss sichergestellt werden, dass die Intercluster-LIF-IP-Adressen in der Zulassungsliste enthalten sind und dass der HTTPS-Service sowohl auf den Intercluster-LIFs als auch auf den firmeneigenen Firewalls Ihres Unternehmens erlaubt ist.

  Standardmäßig erlaubt die `intercluster`Firewall-Richtlinie den Zugriff von allen IP-Adressen (0.0.0.0/0 bzw. ::/0 für IPv6) und aktiviert die Dienste HTTPS, NDMP und NDMPS. Bei einer Änderung dieser Standardrichtlinie oder beim Erstellen einer eigenen Firewall-Richtlinie für Intercluster-LIFs ist es erforderlich, jede Intercluster-LIF-IP-Adresse zur Liste der zulässigen Adressen hinzuzufügen und den

HTTPS-Service zu aktivieren.

- Ab ONTAP 9.6 werden die HTTPS- und SSH-Firewall-Services nicht unterstützt.

  In ONTAP 9.6 sind die `management-https`- und `management-ssh`-LIF-Services für den HTTPS- und SSH-Verwaltungszugriff verfügbar.

Schritte

1. Eine Firewall-Richtlinie erstellen, die den LIFs auf einer bestimmten SVM zur Verfügung steht:

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

   Sie können diesen Befehl mehrmals verwenden, um mehr als einen Netzwerkservice und eine Liste zulässiger IP-Adressen für jeden Netzwerkservice in der Firewall-Richtlinie hinzuzufügen.

2. Es kann mithilfe des `system services firewall policy show` Befehls überprüft werden, ob die Richtlinie korrekt hinzugefügt wurde.
3. Die Firewall-Richtlinie auf eine LIF anwenden:

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

4. Es kann mithilfe des `network interface show -fields firewall-policy` Befehls überprüft werden, ob die Richtlinie korrekt zum LIF hinzugefügt wurde.

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiel für die Erstellung einer Firewall-Richtlinie und deren Zuweisung zu einem LIF

Der folgende Befehl erstellt eine Firewall-Richtlinie namens data_http, die den Zugriff auf HTTP- und HTTPS-Protokolle von IP-Adressen im Subnetz 10.10 ermöglicht, wendet diese Richtlinie auf die LIF namens data1 auf SVM vs1 an und zeigt anschließend alle Firewall-Richtlinien im Cluster an:

```
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
```

ONTAP TLS-Hardware-Offload konfigurieren

Ab ONTAP 9.19.1 kann die TLS Offload-Funktion konfiguriert werden, um die TLS-Post-Handshake-Leistung durch Nutzung von Ressourcen auf unterstützten Ethernet-Karten zu verbessern. Diese Funktion lagert Verschlüsselung und Entschlüsselung aus, reduziert die CPU-Last und verbessert die Leistung.

TLS-Offload kann nur für Datenverkehr aktiviert werden, der KTLS verwendet. Diese Einstellung gilt nicht für den gesamten TLS-aktivierten Datenverkehr. Verwaltungsdatenverkehr wie HTTPS- und REST-API-Datenverkehr ist von dieser Einstellung nicht betroffen. HA-Datenverkehr wird nicht unterstützt.

Über diese Aufgabe

- TLS-Offload ist standardmäßig deaktiviert.
- Lediglich AES-GCM-Verschlüsselungssuiten (TLSv1.2/TLSv1.3, 128/256-Bit) werden ausgelagert.
- Die TLS-Handschlagphase wird nicht ausgelagert. Nur die Datenphase nach dem Handschlag wird ausgelagert.
- Die Migration der logischen Netzwerkschnittstelle (LIF) auf Ports, die nicht für Offloading geeignet sind, führt zu einem automatischen Software-Fallback.

  Bei TLS-offloaded-Verbindungen umgehen die kryptografischen Operationen von TLS üblicherweise die Software und werden von einer Offload-fähigen NIC ausgeführt. Wenn die mit dieser Verbindung verknüpfte LIF auf einen Netzwerkport ohne TLS-Offload-Funktion migriert, greifen die kryptografischen Operationen auf die Software zurück und werden vom Systemkernel verarbeitet.

- Die Management-Schnittstellen (HTTPS, REST API) sind von dieser Einstellung nicht betroffen.
- Die TLS Hardwareauslagerung ist eine clusterweite Einstellung.
- HA-Datenverkehr wird für TLS Hardware-Offload nicht unterstützt.

Unterstützte Netzwerkkarten und Plattformen

Für die Hardware-Auslagerung von TLS ist eine unterstützte Netzwerkkarte erforderlich. Die folgende Tabelle listet die unterstützten Netzwerkkarten nach Plattform auf.

Plattformfamilie	Plattformen	Unterstützte Netzwerkkarten
AFF und FAS	AFF A20, AFF A30, AFF A50, AFF C30, AFF C60, FAS50	• 4-Port CX7 10/25 GbE • 2-Port CX6-DX 40/100 GbE • 2-Port CX7 40/100 GbE
AFF und FAS	AFF A70, AFF A90, AFF C80, FAS70, FAS90, AFF A1K	• 2-Port CX6-DX 40/100 GbE • 2-Port CX7 40/100 GbE • 2-Port CX7 40/100/200/400 GbE
ASA	ASA A20, ASA A30, ASA A50, ASA C30	• 4-Port CX7 10/25 GbE • 2-Port CX6-DX 40/100 GbE • 2-Port CX7 40/100 GbE
ASA	ASA A70, ASA A90, ASA A1K	• 2-Port CX6-DX 40/100 GbE • 2-Port CX7 40/100 GbE • 2-Port CX7 40/100/200/400 GbE
AFX	AFX 1K	• 2-Port CX6-DX 40/100 GbE • 2-Port CX7 40/100 GbE • 2-Port CX7 40/100/200/400 GbE
AFX	AFX 2K	• 2-Port CX7 40/100/200/400 GbE

Unterstützte Verkehrstypen

Die folgende Tabelle zeigt, ob TLS-Hardware-Offloading für jeden Verkehrstyp unterstützt wird.

Verkehrsart	Unterstützt	Hinweise
NVMe/TCP	Ja	Unterstützt auf Plattformen und Netzwerkkarten, die TLS Offload unterstützen.
Cluster-Peering-Verschlüsselung	Ja	Unterstützt für Cluster-Netzwerkverkehr. Dies schließt HA-Verkehr nicht ein.
FabricPool	Ja	Unterstützt auf Plattformen und Netzwerkkarten, die TLS Offload unterstützen.
S3	Ja	Unterstützt auf Plattformen und Netzwerkkarten, die TLS Offload unterstützen.
NFS über TLS	Ja, ab ONTAP 9.19.1	Unterstützt für ONTAP NFS over TLS Datenverkehr, bei dem KTLS verwendet wird.
KMIP	Nein	Nicht unterstützt.
System Manager	Nein	Die Management-Schnittstellen sind von dieser Einstellung nicht betroffen.
REST API	Nein	Die Management-Schnittstellen sind von dieser Einstellung nicht betroffen.
HA Verkehr	Nein	Die TLS-Hardwareauslagerung gilt nicht für HA-Datenverkehr.

Auf ASA-Systemen gilt die TLS-Hardwareauslagerung nur für NVMe/TCP-Datenverkehr. NFS über TLS, FabricPool und S3 werden auf ASA-Plattformen nicht unterstützt.

Auf AFX-Plattformen unterstützt die TLS-Hardwareauslagerung NFS über TLS und S3 Frontend-Datenverkehrstypen. NVMe/TCP wird auf AFX-Plattformen nicht unterstützt, da AFX keine SAN/Block-Protokolle unterstützt.

Bevor Sie beginnen

- Sie müssen ONTAP Administrator auf der `admin`-Berechtigungsstufe sein, um die folgenden Aufgaben auszuführen.
- Auf allen Knoten muss ONTAP 9.19.1 oder höher laufen.

TLS-Offload aktivieren oder deaktivieren

Schritte

1. Den aktuellen TLS-Offload-Status anzeigen:

```
security config show
```

Dieser Befehl zeigt die clusterweite TLS-Offload-Einstellung an:

```
cluster1::*> security config show
Cluster    Supported Offload
FIPS Mode  Protocols Enabled Supported Cipher Suites
```

```
---------- --------- -------
------------------------------------------------
false      TLSv1.3,  false   TLS_RSA_WITH_AES_128_CCM,
           TLSv1.2           TLS_RSA_WITH_AES_128_CCM_8,
                             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,
[...]
```

2. TLS-Offload aktivieren oder deaktivieren:

```
security config modify * -is-offload-enabled {true|false}
```

Dieser Befehl aktiviert oder deaktiviert die Hardware-Auslagerung für die TLS-Datenphase bei neuen Verbindungen. Bestehende Verbindungen, die vor der Aktivierung der TLS-Auslagerungsfunktion erstellt wurden, werden erst dann ausgelagert, wenn diese Verbindungen entfernt und neu erstellt werden.

Verwandte Informationen

- "security config show"
- "Sicherheitskonfiguration ändern"

ONTAP Befehle zur Verwaltung des Firewall-Dienstes und der Richtlinien

Die `system services firewall` Befehle dienen zur Verwaltung des Firewall-Dienstes, die `system services firewall policy` Befehle zur Verwaltung von Firewall-Richtlinien und der `network interface modify` Befehl zur Verwaltung der Firewall-Einstellungen für LIFs.

Ab ONTAP 9.10.1:

- Firewall-Richtlinien sind veraltet und werden durch LIF-Dienstrichtlinien ersetzt. Zuvor wurde die integrierte Firewall mithilfe von Firewall-Richtlinien verwaltet. Diese Funktionalität wird jetzt mit einer LIF-Dienstrichtlinie umgesetzt.
- Alle Firewall-Richtlinien sind leer und öffnen keine Ports in der zugrunde liegenden Firewall. Stattdessen müssen alle Ports über eine LIF-Dienstrichtlinie geöffnet werden.
- Nach einem Upgrade auf Version 9.10.1 oder höher ist kein weiteres Vorgehen erforderlich, um von Firewall-Richtlinien auf LIF-Dienstrichtlinien umzustellen. Das System erstellt automatisch LIF-Dienstrichtlinien, die mit den in der vorherigen ONTAP Version verwendeten Firewall-Richtlinien konsistent sind. Wenn Skripte oder andere Tools verwendet werden, die benutzerdefinierte Firewall-Richtlinien erstellen und verwalten, kann es erforderlich sein, diese Skripte so anzupassen, dass stattdessen benutzerdefinierte Dienstrichtlinien erstellt werden.

Weitere Informationen finden sich unter "LIFs und Servicerichtlinien in ONTAP 9.6 und später".

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Firewall-Service aktivieren oder deaktivieren	`system services firewall modify`
Aktuelle Konfiguration des Firewall-Dienstes anzeigen	`system services firewall show`
Eine Firewall-Richtlinie erstellen oder einen Dienst zu einer vorhandenen Firewall-Richtlinie hinzufügen	`system services firewall policy create`
Eine Firewall-Richtlinie auf eine LIF anwenden	`network interface modify -lif lifname -firewall-policy`
Ändern der mit einer Firewall-Richtlinie verknüpften IP-Adressen und Netzmasken	`system services firewall policy modify`
Informationen zu Firewall-Richtlinien	`system services firewall policy show`
Eine neue Firewall-Richtlinie erstellen, die eine exakte Kopie einer vorhandenen Richtlinie ist	`system services firewall policy clone`
Eine Firewall-Richtlinie löschen, die von einem LIF nicht verwendet wird	`system services firewall policy delete`

Verwandte Informationen

- "Systemdienste Firewall"
- "Netzwerkschnittstelle ändern"

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.