Secure your network

ONTAP 9

NetApp
February 02, 2026

Table of Contents

Secure your network

Configure ONTAP network security using FIPS for all SSL connections

ONTAP is compliant with the Federal Information Processing Standards (FIPS) 140-2 for all SSL connections. You can turn on and off SSL FIPS mode, set SSL protocols globally, and turn off any weak ciphers within ONTAP.

By default, SSL on ONTAP is set with FIPS compliance disabled and with the following TLS protocols enabled:

- TLSv1.3 (beginning with ONTAP 9.11.1)
- TLSv1.2

Previous ONTAP releases had the following TLS protocols enabled by default:

- TLSv1.1 (disabled by default beginning with ONTAP 9.12.1)
- TLSv1 (disabled by default beginning with ONTAP 9.8)

When SSL FIPS mode is enabled, SSL communication from ONTAP to external client or server components outside of ONTAP will use FIPS compliant crypto for SSL.

If you want administrator accounts to access SVMs with an SSH public key, you must ensure that the host key algorithm is supported before enabling SSL FIPS mode.

Note: Host key algorithm support has changed in ONTAP 9.11.1 and later releases.

ONTAP release	Supported key types	Unsupported key types
9.11.1 and later	ecdsa-sha2-nistp256	rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ssh-dss ssh-rsa

Existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type before enabling FIPS, or the administrator authentication will fail.

For more information, see Enable SSH public key accounts.

ONTAP 9.18.1 introduces support for the ML-KEM, ML-DSA, and SLH-DSA post-quantum computing cryptographic algorithms for SSL, providing an additional layer of security against potential future quantum computer attacks. These algorithms are only available when FIPS is disabled. Post-quantum cryptographic algorithms are negotiated when FIPS is disabled and the peer supports them.

Enable FIPS

It is recommended that all secure users adjust their security configuration immediately after system installation or upgrade. When SSL FIPS mode is enabled, SSL communication from ONTAP to external client or server components outside of ONTAP will use FIPS compliant crypto for SSL.

> When FIPS is enabled, you cannot install or create a certificate with an RSA key length of 4096.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Enable FIPS:

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

3. When prompted to continue, enter `y`
4. Beginning with ONTAP 9.9.1, rebooting is not required. If you are running ONTAP 9.8 or earlier, manually reboot each node in the cluster one by one.

Example

If you are running ONTAP 9.9.1 or later, you will not see the warning message.

```
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
```

Learn more about `security config modify` and SSL FIPS mode configuration in the ONTAP command reference.

Disable FIPS

Beginning with ONTAP 9.18.1, SSL in ONTAP supports the ML-KEM, ML-DSA, and SLH-DSA post-quantum computing cryptographic algorithms. These algorithms are only available when FIPS is disabled and the peer supports them.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Disable FIPS by typing:

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

3. When prompted to continue, enter `y`.
4. Beginning with ONTAP 9.9.1, rebooting is not required. If you are running ONTAP 9.8 or earlier, manually reboot each node in the cluster.

If you need to use the SSLv3 protocol, you must disable FIPS with the above procedure. SSLv3 can only be enabled when FIPS is disabled.

You can enable SSLv3 with the following command. If you are running ONTAP 9.9.1 or later, you will not see the warning message.

```
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
```

View FIPS compliance status

You can see whether the entire cluster is running the current security configuration settings.

Steps

1. If you are running ONTAP 9.8 or earlier, manually reboot each node in the cluster one by one.
2. View the current compliance status:

   ```
   security config show
   ```

Example

```
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,
                     ...
```

Learn more about `security config show` in the ONTAP command reference.

Related information

- FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)
- FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA)
- FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)

Configure IPsec in-flight encryption

Prepare to use IP security on the ONTAP network

Beginning with ONTAP 9.8, you have the option to use IP security (IPsec) to protect your network traffic. IPsec is one of several data-in-motion or in-flight encryption options available with ONTAP. You should prepare to configure IPsec before using it in a production environment.

IP security implementation in ONTAP

IPsec is an internet standard maintained by the IETF. It provides data encryption and integrity as well as authentication for the traffic flowing among the network endpoints at an IP level.

With ONTAP, IPsec secures all the IP traffic between ONTAP and the various clients, including the NFS, SMB, and iSCSI protocols. In addition to privacy and data integrity, the network traffic is protected against several attacks such as the replay and man-in-the-middle attacks. ONTAP uses the IPsec transport mode implementation. It leverages the Internet Key Exchange (IKE) protocol version 2 for negotiating the key material between ONTAP and the clients using either IPv4 or IPv6.

When the IPsec capability is enabled on a cluster, the network requires one or more entries in the ONTAP Security Policy Database (SPD) matching the various traffic characteristics. These entries map to the specific protection details needed to process and send the data (such as, cipher suite and authentication method). A corresponding SPD entry is also needed at each client.

For certain types of traffic, another data-in-motion encryption option might be preferable. For example, for the encryption of NetApp SnapMirror and cluster peering traffic, the transport layer security (TLS) protocol is generally recommended instead of IPsec. This is because TLS offers better performance in most situations.

Related information

- Internet Engineering Task Force
- RFC 4301: Security Architecture for the Internet Protocol

Evolution of the ONTAP IPsec implementation

IPsec was first introduced with ONTAP 9.8. The implementation has continued to evolve in subsequent ONTAP releases as described below.

ONTAP 9.18.1

Support for IPsec hardware offload is extended to IPv6 traffic.

ONTAP 9.17.1

Support for IPsec hardware offload is extended to link aggregation groups. Postquantum pre-shared keys (PPKs) are supported for IPsec pre-shared keys (PSK) authentication.

ONTAP 9.16.1

Several of the cryptographic operations, such as encryption and integrity checks, can be offloaded to a supported NIC card. See IPsec hardware offload feature for more information.

ONTAP 9.12.1

IPsec front-end host protocol support is available in MetroCluster IP and MetroCluster fabric-attached configurations. The IPsec support provided with MetroCluster clusters is limited to front-end host traffic and is not supported on MetroCluster intercluster LIFs.

ONTAP 9.10.1

Certificates can be used for IPsec authentication in addition to the PSKs. Prior to ONTAP 9.10.1, only PSKs are supported for authentication.

ONTAP 9.9.1

The encryption algorithms used by IPsec are FIPS 140-2 validated. These algorithms are processed by the NetApp Cryptographic Module in ONTAP which carries the FIPS 140-2 validation.

ONTAP 9.8

Support for IPsec becomes initially available based on the transport mode implementation.

IPsec hardware offload feature

If you are using ONTAP 9.16.1 or later, you have the option of offloading certain computationally intensive operations, such as encryption and integrity checks, to a network interface controller (NIC) card installed at the storage node. The throughput for operations offloaded to the NIC card is approximately 5% or less. This can significantly improve the performance and throughput of the network traffic protected by IPsec.

Requirements and recommendations

There are several requirements you should consider before using the IPsec hardware offload feature.

Supported Ethernet cards

You need to install and use only supported Ethernet cards. The following Ethernet cards are supported beginning with ONTAP 9.16.1:

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

ONTAP 9.17.1 adds support for the following Ethernet cards:

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

The X50131A and X50135A cards are supported on the following platforms:

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

The X60132A and X60135A cards are supported on the following platforms:

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

See the NetApp Hardware Universe for more information about the supported platforms and cards.

Cluster scope

The IPsec hardware offload feature is configured globally for the cluster. And so, for example, the command `security ipsec config` applies to all the nodes in the cluster.

Consistent configuration

Supported NIC cards should be installed at all the nodes in the cluster. If a supported NIC card is only available on some of the nodes, you can see a significant performance degradation after a failover if some of the LIFs are not hosted on an offload capable NIC.

Disable anti-replay

You must disable IPsec anti-replay protection on ONTAP (default configuration) and the IPsec clients. If not disabled, fragmentation and multi-path (redundant route) will not be supported.

If the ONTAP IPsec configuration has been changed from the default to enable anti-replay protection, use this command to disable it:

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

You must ensure that IPsec anti-replay protection is disabled on your client. Refer to the IPsec documentation for your client to disable anti-replay protection.

Limitations

There are several limitations you should consider before using the IPsec hardware offload feature.

IPv6

Beginning with ONTAP 9.18.1, IPv6 is supported for the IPsec hardware offload feature. Prior to ONTAP 9.18.1, IPsec hardware offload does not support IPv6.

Extended sequence numbers

The IPsec extended sequence numbers are not supported with the hardware offload feature. Only the normal 32-bit sequence numbers are used.

Link aggregation

Beginning with ONTAP 9.17.1, you can use the IPsec hardware offload feature with a link aggregation group.

Prior to 9.17.1, the IPsec hardware offload feature does not support link aggregation. It cannot be used with an interface or link aggregation group as administered through the `network port ifgrp` commands at the ONTAP CLI.

Configuration support in the ONTAP CLI

Three existing CLI commands are updated in ONTAP 9.16.1 to support the IPsec hardware offload feature as described below. Also see Configure IP security in ONTAP for more information.

ONTAP command	Update
`security ipsec config show`	The boolean parameter `Offload Enabled` shows the current NIC offload status.
`security ipsec config modify`	The parameter `is-offload-enabled` can be used to enable or disable NIC offload feature.
`security ipsec config show-ipsecsa`	Four new counters have been added to display the inbound as well as outbound traffic in bytes and packets.

Configuration support in the ONTAP REST API

Two existing REST API endpoints are updated in ONTAP 9.16.1 to support the IPsec hardware offload feature as described below.

REST endpoint	Update
`/api/security/ipsec`	The parameter `offload_enabled` has been added and is available with the PATCH method.
`/api/security/ipsec/security_association`	Two new counter values have been added to track the total bytes and packets processed by the offload feature.

Learn more about the ONTAP REST API, including what's new with the ONTAP REST API, from the ONTAP automation documentation. You should also review the ONTAP automation documentation for details about IPsec endpoints.

Related information

- security ipsec

Configure IP security for the ONTAP network

There are several tasks you need to perform to configure and activate IPsec in-flight encryption on your ONTAP cluster.

> ⓘ Make sure to review Prepare to use IP security before configuring IPsec. For example, you might need to decide whether to use the IPsec hardware offload feature available beginning with ONTAP 9.16.1.

Enable IPsec on the cluster

You can enable IPsec on the cluster to ensure data is continuously encrypted and secure while in transit.

Steps

1. Discover if IPsec is enabled already:

   ```
   security ipsec config show
   ```

   If the result includes `IPsec Enabled: false`, proceed to the next step.

2. Enable IPsec:

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

   You can enable the IPsec hardware offload feature using the boolean parameter `is-offload-enabled`.

3. Run the discovery command again:

   ```
   security ipsec config show
   ```

   The result now includes `IPsec Enabled: true`.

Prepare for IPsec policy creation with certificate authentication

You can skip this step if you are only using pre-shared keys (PSKs) for authentication and will not use certificate authentication.

Before creating an IPsec policy that uses certificates for authentication, you must verify that the following pre-requisites are met:

- Both ONTAP and the client must have the other party's CA certificate installed so that the end entity (either ONTAP or the client) certificates are verifiable by both sides
- A certificate is installed for the ONTAP LIF that participates in the policy

ONTAP LIFs can share certificates. A one-to-one mapping between certificates and LIFs is not required.

Steps

1. Install all CA certificates used during the mutual authentication, including both ONTAP-side and client-side CAs, to ONTAP certificate management unless it is already installed (as is the case of an ONTAP self-signed root-CA).

   Sample command

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

2. To make sure that the CA installed is within the IPsec CA searching path during authentication, add the ONTAP certificate management CAs to the IPsec module using the `security ipsec ca-certificate add` command.

   Sample command

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

3. Create and install a certificate for use by the ONTAP LIF. The issuer CA of this certificate must already be installed to ONTAP and added to IPsec.

   Sample command

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

For more information about certificates in ONTAP, see the security certificate commands in the ONTAP 9 documentation.

Define the security policy database (SPD)

IPsec requires an SPD entry before allowing traffic to flow on the network. This is true whether you are using a PSK or a certificate for authentication.

Steps

1. Use the `security ipsec policy create` command to:

   a. Select the ONTAP IP address or subnet of IP addresses to participate in the IPsec transport.

   b. Select the client IP addresses that will connect to the ONTAP IP addresses.

      The client must support Internet Key Exchange version 2 (IKEv2) with a pre-shared key (PSK).

   c. Optionally select the fine-grained traffic parameters, such as the upper layer protocols (UDP, TCP, ICMP, etc.), the local port numbers, and the remote port numbers to protect traffic. The corresponding parameters are `protocols`, `local-ports` and `remote-ports` respectively.

      Skip this step to protect all traffic between the ONTAP IP address and client IP address. Protecting all traffic is the default.

   d. Either enter PSK or public-key infrastructure (PKI) for the `auth-method` parameter for the desired authentication method.

  i. If you enter a PSK, include the parameters, then press <enter> for the prompt to enter and verify the pre-shared key.

     > The `local-identity` and `remote-identity` parameters are optional if both host and client use strongSwan and no wildcard policy is selected for the host or client.

  ii. If you enter a PKI, you need to also enter the `cert-name`, `local-identity`, `remote-identity` parameters. If the remote-side certificate identity is unknown or if multiple client identities are expected, enter the special identity `ANYTHING`.

e. Beginning with ONTAP 9.17.1, optionally enter a postquantum pre-shared key (PPK) identity with the `ppk-identity` parameter. PPKs offer an additional layer of security against potential future quantum computer attacks. When you enter a PPK identity, you will be prompted to enter the PPK secret. PPKs are only supported for PSK authentication.

Learn more about `security ipsec policy create` in the ONTAP command reference.

Sample command for PSK authentication

```
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_:
```

Sample command for PKI/certificate authentication

```
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
```

IP traffic cannot flow between the client and server until both ONTAP and the client have set up the matching IPsec policies, and authentication credentials (either PSK or certificate) are in place on both sides.

Use IPsec identities

For the pre-shared key authentication method, local and remote identities are optional if both host and client use strongSwan and no wildcard policy is selected for the host or client.

For the PKI/certificate authentication method, both local and remote identities are mandatory. The identities specify what identity is certified within each side's certificate and are used in the verification process. If the remote-identity is unknown or if it could be many different identities, use the special identity `ANYTHING`.

About this task

Within ONTAP, identities are specified by modifying the SPD entry or during SPD policy creation. The SPD can be an IP address or string format identity name.

Steps

1. Use the following command to modify an existing SPD identity setting:

```
security ipsec policy modify
```

Sample command

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

IPsec multiple client configuration

When a small number of clients need to leverage IPsec, using a single SPD entry for each client is sufficient. However, when hundreds or even thousands of clients need to leverage IPsec, NetApp recommends using an IPsec multiple client configuration.

About this task

ONTAP supports connecting multiple clients across many networks to a single SVM IP address with IPsec enabled. You can accomplish this using one of the following methods:

- **Subnet configuration**

  To allow all clients on a particular subnet (192.168.134.0/24 for example) to connect to a single SVM IP address using a single SPD policy entry, you must specify the `remote-ip-subnets` in subnet form. Additionally, you must specify the `remote-identity` field with the correct client-side identity.

  > When using a single policy entry in a subnet configuration, IPsec clients in that subnet share the IPsec identity and pre-shared key (PSK). However, this is not true with certificate authentication. When using certificates each client can use either their own unique certificate or a shared certificate to authenticate. ONTAP IPsec checks the validity of the certificate based on the CAs installed on its local trust store. ONTAP also supports certificate revocation list (CRL) checking.

- **Allow all clients configuration**

  To allow any client, regardless of their source IP address, to connect to the SVM IPsec-enabled IP address, use the `0.0.0.0/0` wildcard when specifying the `remote-ip-subnets` field.

  Additionally, you must specify the `remote-identity` field with the correct client-side identity. For certificate authentication, you can enter `ANYTHING`.

  Also, when the `0.0.0.0/0` wildcard is used, you must configure a specific local or remote port number to use. For example, `NFS port 2049`.

  Steps

  1. Use one of the following commands to configure IPsec for multiple clients.
     a. If you are using **subnet configuration** to support multiple IPsec clients:

        ```
        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
        ```

        Sample command

        ```
        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
        ```

b. If you are using **allow all clients configuration** to support multiple IPsec clients:

```
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
```

Sample command

```
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
```

Display IPsec statistics

Through negotiation, a security channel called an IKE Security Association (SA) can be established between the ONTAP SVM IP address and the client IP address. IPsec SAs are installed on both endpoints to do the actual data encryption and decryption work. You can use statistics commands to check the status of both IPsec SAs and IKE SAs.

> If you are using the IPsec hardware offload feature, several new counters are displayed with the command `security ipsec config show-ipsecsa`.

Sample commands

IKE SA sample command:

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

IPsec SA sample command and output:

```
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 sample command and output:

```
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
```

Related information

- security certificate install
- security ipsec

Configure ONTAP backend cluster network encryption

Beginning with ONTAP 9.18.1, you can configure Transport Layer Security (TLS) encryption for data-in-flight on the backend cluster network. This encryption protects customer data stored in ONTAP when it is transmitted between ONTAP nodes on the backend cluster network.

About this task

- Backend cluster network encryption is disabled by default.
- When backend cluster network encryption is enabled, all customer data stored in ONTAP is encrypted when transmitted between ONTAP nodes on the backend cluster network. Some cluster network traffic, such as control path data, is not encrypted.
- By default, backend cluster network encryption will use auto-generated certificates for each node in the cluster. You can Manage cluster network encryption certificates on each node to use a custom installed certificate.

Before you begin

- You must be an ONTAP administrator at the `admin` privilege level to perform the following tasks.
- All nodes in the cluster must be running ONTAP 9.18.1 or later to enable backend cluster network encryption.

Enable or disable encryption for cluster network communication

Steps

1. View the current cluster network encryption status:

   ```
   security cluster-network show
   ```

This command shows the current status of cluster network encryption:

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

Enabled: true

Mode: tls

Status: READY
```

2. Enable or disable TLS backend cluster network encryption:

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

This command enables or disables encrypted communication for customer data-in-flight on the backend cluster network.

Manage cluster network encryption certificates

1. View the current cluster network encryption certificate information:

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

This command shows the current cluster network encryption certificate information:

```
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
```

The certificate and certificate authority (CA) names are shown for each node in the cluster.

2. Modify the cluster network encryption certificate for a node:

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

This command modifies the cluster network encryption certificate for a specific node. The certificate must be installed and signed by an installed CA prior to running this command. For more information on certificate management, refer to Manage ONTAP certificates with System Manager. If `-name` is not specified, the auto-generated default certificate is used.

Configure firewall policies for LIFs in the ONTAP network

Setting up a firewall enhances the security of the cluster and helps prevent unauthorized access to the storage system. By default, the onboard firewall is configured to allow remote access to a specific set of IP services for data, management, and intercluster LIFs.

Beginning with ONTAP 9.10.1:

- Firewall policies are deprecated and are replaced by LIF service policies. Previously, the onboard firewall was managed using firewall policies. This functionality is now accomplished using a LIF service policy.
- All firewall policies are empty and do not open any ports in the underlying firewall. Instead, all ports must be opened using a LIF service policy.
- No action is required after an upgrade to 9.10.1 or later to transition from firewall policies to LIF service policies. The system automatically constructs LIF service policies consistent with the firewall policies in use in the previous ONTAP release. If you use scripts or other tools that create and manage custom firewall policies, you might need to upgrade those scripts to create custom service policies instead.

To learn more, see LIFs and service policies in ONTAP 9.6 and later.

Firewall policies can be used to control access to management service protocols such as SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS, or SNMP. Firewall policies cannot be set for data protocols such as NFS or SMB.

You can manage firewall service and policies in the following ways:

- Enabling or disabling firewall service
- Displaying the current firewall service configuration
- Creating a new firewall policy with the specified policy name and network services
- Applying a firewall policy to a logical interface
- Creating a new firewall policy that is an exact copy of an existing policy

  You can use this to make a policy with similar characteristics within the same SVM, or to copy the policy to a different SVM.

- Displaying information about firewall policies
- Modifying the IP addresses and netmasks that are used by a firewall policy
- Deleting a firewall policy that is not being used by a LIF

Firewall policies and LIFs

LIF firewall policies are used to restrict access to the cluster over each LIF. You need to understand how the default firewall policy affects system access over each type of LIF, and how you can customize a firewall policy to increase or decrease security over a LIF.

When configuring a LIF using the `network interface create` or `network interface modify` command, the value specified for the `-firewall-policy` parameter determines the service protocols and IP addresses that are allowed access to the LIF. Learn more about `network interface` in the ONTAP command reference.

In many cases you can accept the default firewall policy value. In other cases, you might need to restrict access to certain IP addresses and certain management service protocols. The available management service protocols include SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS, and SNMP.

The firewall policy for all cluster LIFs defaults to `""` and cannot be modified.

The following table describes the default firewall policies that are assigned to each LIF, depending on their role (ONTAP 9.5 and earlier) or service policy (ONTAP 9.6 and later), when you create the LIF:

Firewall policy	Default service protocols	Default access	LIFs applied to
mgmt	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Any address (0.0.0.0/0)	Cluster management, SVM management, and node management LIFs
mgmt-nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Any address (0.0.0.0/0)	Data LIFs that also support SVM management access
intercluster	https, ndmp, ndmps	Any address (0.0.0.0/0)	All intercluster LIFs
data	dns, ndmp, ndmps, portmap	Any address (0.0.0.0/0)	All data LIFs

Portmap service configuration

The portmap service maps RPC services to the ports on which they listen.

The portmap service was always accessible in ONTAP 9.3 and earlier, became configurable in ONTAP 9.4 through ONTAP 9.6, and is managed automatically beginning with ONTAP 9.7.

- In ONTAP 9.3 and earlier, the portmap service (rpcbind) was always accessible on port 111 in network configurations that relied on the built-in ONTAP firewall rather than a third-party firewall.
- From ONTAP 9.4 through ONTAP 9.6, you can modify firewall policies to control whether the portmap service is accessible on particular LIFs.
- Beginning with ONTAP 9.7, the portmap firewall service is eliminated. Instead, the portmap port is opened automatically for all LIFs that support the NFS service.

Portmap service is configurable in the firewall in ONTAP 9.4 through ONTAP 9.6.

The remainder of this topic discusses how to configure the portmap firewall service for ONTAP 9.4 through ONTAP 9.6 releases.

Depending on your configuration, you may be able to disallow access to the service on specific types of LIFs, typically management and intercluster LIFs. In some circumstances, you might even be able to disallow access on data LIFs.

What behavior you can expect

The ONTAP 9.4 through ONTAP 9.6 behavior is designed to provide a seamless transition on upgrade. If the portmap service is already being accessed over specific types of LIFs, it will continue to be accessible over those types of LIFs. As in ONTAP 9.3 and earlier, you can specify the services accessible within the firewall in the firewall policy for the LIF type.

All nodes in the cluster must be running ONTAP 9.4 through ONTAP 9.6 for the behavior to take effect. Only inbound traffic is affected.

The new rules are as follows:

- On upgrade to release 9.4 through 9.6, ONTAP adds the portmap service to all existing firewall policies, default or custom.
- When you create a new cluster or new IPspace, ONTAP adds the portmap service only to the default data policy, not to the default management or intercluster policies.
- You can add the portmap service to default or custom policies as needed, and remove the service as needed.

How to add or remove the portmap service

To add the portmap service to an SVM or cluster firewall policy (make it accessible within the firewall), enter:

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

To remove the portmap service from an SVM or cluster firewall policy (make it inaccessible within the firewall), enter:

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

You can use the network interface modify command to apply the firewall policy to an existing LIF.
Learn more about the commands described in this procedure in the ONTAP command reference.

Create a firewall policy and assign it to a LIF

Default firewall policies are assigned to each LIF when you create the LIF. In many cases, the default firewall settings work well and you do not need to change them. If you want to change the network services or IP addresses that can access a LIF, you can create a custom firewall policy and assign it to the LIF.

About this task

- You cannot create a firewall policy with the `policy` name `data`, `intercluster`, `cluster`, or `mgmt`.

  These values are reserved for the system-defined firewall policies.

- You cannot set or modify a firewall policy for cluster LIFs.

  The firewall policy for cluster LIFs is set to 0.0.0.0/0 for all services types.

- If you need to remove a service from a policy, you must delete the existing firewall policy and create a new policy.

- If IPv6 is enabled on the cluster, you can create firewall policies with IPv6 addresses.

  After IPv6 is enabled, `data`, `intercluster`, and `mgmt` firewall policies include ::/0, the IPv6 wildcard, in their list of accepted addresses.

- When using System Manager to configure data protection functionality across clusters, you must ensure that the intercluster LIF IP addresses are included in the allowed list, and that HTTPS service is allowed on both the intercluster LIFs and on your company-owned firewalls.

  By default, the `intercluster` firewall policy allows access from all IP addresses (0.0.0.0/0, or ::/0 for IPv6) and enables HTTPS, NDMP, and NDMPS services. If you modify this default policy, or if you create your own firewall policy for intercluster LIFs, you must add each intercluster LIF IP address to the allowed list and enable HTTPS service.

- Beginning with ONTAP 9.6, the HTTPS and SSH firewall services are not supported.

  In ONTAP 9.6, the `management-https` and `management-ssh` LIF services are available for HTTPS and SSH management access.

Steps

1. Create a firewall policy that will be available to the LIFs on a specific SVM:

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

   You can use this command multiple times to add more than one network service and list of allowed IP addresses for each service in the firewall policy.

2. Verify that the policy was added correctly by using the `system services firewall policy show` command.
3. Apply the firewall policy to a LIF:

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

4. Verify that the policy was added correctly to the LIF by using the `network interface show -fields firewall-policy` command.

   Learn more about `network interface show` in the ONTAP command reference.

Example of creating a firewall policy and assigning it to a LIF

The following command creates a firewall policy named data_http that enables HTTP and HTTPS protocol access from IP addresses on the 10.10 subnet, applies that policy to the LIF named data1 on SVM vs1, and then shows all of the firewall policies on the cluster:

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

```
system services firewall policy show

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

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

network interface show -fields firewall-policy

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

ONTAP commands to manage firewall service and policies

You can use the `system services firewall` commands to manage firewall service, the `system services firewall policy` commands to manage firewall policies, and the `network interface modify` command to manage firewall settings for LIFs.

Beginning with ONTAP 9.10.1:

- Firewall policies are deprecated and are replaced by LIF service policies. Previously, the onboard firewall was managed using firewall policies. This functionality is now accomplished using a LIF service policy.
- All firewall policies are empty and do not open any ports in the underlying firewall. Instead, all ports must be opened using a LIF service policy.
- No action is required after an upgrade to 9.10.1 or later to transition from firewall policies to LIF service policies. The system automatically constructs LIF service policies consistent with the firewall policies in use in the previous ONTAP release. If you use scripts or other tools that create and manage custom firewall policies, you might need to upgrade those scripts to create custom service policies instead.

To learn more, see LIFs and service policies in ONTAP 9.6 and later.

If you want to…	Use this command…
Enable or disable firewall service	`system services firewall modify`
Display the current configuration for firewall service	`system services firewall show`
Create a firewall policy or add a service to an existing firewall policy	`system services firewall policy create`
Apply a firewall policy to a LIF	`network interface modify -lif lifname -firewall-policy`
Modify the IP addresses and netmasks associated with a firewall policy	`system services firewall policy modify`
Display information about firewall policies	`system services firewall policy show`
Create a new firewall policy that is an exact copy of an existing policy	`system services firewall policy clone`
Delete a firewall policy that is not used by a LIF	`system services firewall policy delete`

Related information

- system services firewall
- network interface modify

Copyright information

Trademark information