



# Secure your network

## ONTAP 9

NetApp  
May 08, 2021

This PDF was generated from [https://docs.netapp.com/us-en/ontap/networking/configure\\_network\\_security\\_using\\_federal\\_information\\_processing\\_standards\\_@fips@.html](https://docs.netapp.com/us-en/ontap/networking/configure_network_security_using_federal_information_processing_standards_@fips@.html) on May 08, 2021. Always check docs.netapp.com for the latest.

# Table of Contents

- Secure your network ..... 1
  - Configure network security using federal information processing standards (FIPS) ..... 1
  - Configure IP security (IPsec) over wire encryption ..... 3
  - Configure firewall policies for LIFs ..... 7
  - Commands for managing firewall service and policies ..... 12

# Secure your network

## Configure network security using federal information processing standards (FIPS)

ONTAP is compliant in 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 such as RC4 within ONTAP.

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

- TLSv1.2
- TLSv1.1
- TLSv1

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.

### 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.

#### About this task

The following settings are recommended to enable FIPS:

- `FIPS: on`
- `SSL protocol = {TLSv1.2}`
- `SSL ciphers = {ALL:!LOW:!aNULL:!EXP:!eNULL:!RC4}`

#### Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Enable FIPS:

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

3. When prompted to continue, enter `y`
4. One by one, manually reboot each node in the cluster.

## Example

```
security config modify -interface SSL -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

## Disable FIPS

If you are still running an older system configuration and want to configure ONTAP with backward compatibility, you can turn on SSLv3 only when FIPS is disabled.

### About this task

The following settings are recommended to disable FIPS:

- `FIPS = false`
- `SSL protocol = {SSLv3}`
- `SSL ciphers = {ALL:!LOW:!aNULL:!EXP:!eNULL}`

### Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Disable FIPS by typing:

```
security config modify -interface SSL -supported-protocols SSLv3
```

3. When prompted to continue, enter `y`.
4. Manually reboot each node in the cluster.

## Example

```
security config modify -interface SSL -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. One by one, reboot each node in the cluster.

Do not reboot all cluster nodes simultaneously. A reboot is required to make sure that all applications in the cluster are running the new security configuration, and for all changes to FIPS on/off mode, Protocols, and Ciphers.

2. View the current compliance status:

```
security config show
```

## Example

```
security config show
```

	Cluster		Cluster
Security			
Interface	FIPS Mode	Supported Protocols	Supported Ciphers Config
Ready			
-----		-----	-----
-----			
SSL	false	TLSv1_2, TLSv1_1, TLSv1	ALL:!LOW:!aNULL: yes !EXP:!eNULL

## Configure IP security (IPsec) over wire encryption

Starting with ONTAP 9.8, ONTAP uses the IPsec protocol in transport mode to ensure

data is continuously secure and encrypted, even while in transit. IPsec offers data encryption for all IP traffic including the NFS, iSCSI, and SMB/CIFS protocols. IPsec provides the only encryption in flight option for iSCSI traffic.

While IPsec capability is enabled on the cluster, the network requires a Security Policy Database (SPD) entry and a preshared secret on the client before traffic can flow.

After IPsec is configured, network traffic between the client and ONTAP is protected with preventive measures to combat replay and man-in-the-middle (MITM) attacks.

For NetApp SnapMirror and cluster peering traffic encryption, cluster peering encryption (CPE) is still recommended over IPsec for secure in-transit over the wire. This is because CPE has better performance than IPsec. You do not require a license for IPsec and there are no import or export restrictions.

## Enable IPsec on the cluster

You can enable Internet Protocol security (IPsec) on the cluster to ensure data is continuously secure and encrypted, even 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
```

3. Run the discovery command again:

```
security ipsec config show
```

The result now includes `IPsec Enabled: true`.

## Define the security policy database (SPD)

IPsec requires an SPD entry before allowing traffic to flow on the network.

### Step

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. Optional. Select the upper layer protocols (UDP, TCP, ICMP, etc. ), the local port numbers, and the remote port numbers to protect. 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. Enter the pre-shared key to use between the client and ONTAP.

#### Sample command

```
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_:
```



IP traffic cannot flow between the client and server until the client pre-shared key is set on the IPsec client.

## Use IPsec identities

Some IPsec clients, such as Libreswan, require the use of identities in addition to pre-shared keys to authenticate the IPsec connection.

#### 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.

#### Step

To add an identity to an existing SPD, use the following command:

```
security ipsec policy modify
```

#### Sample command

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

- **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` wild card when specifying the `remote-ip-subnets` field.

Additionally, you must specify the `remote-identity` field with the correct client side identity.

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

### Step

1. Use one of the following commands to configure IPsec for multiple clients:
  - a. If you are using a **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 an **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
```

## 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.

### Sample commands

IKE SA sample command:

```
security ipsec show-ikesasa -node hosting_node_name_for_svm_ip
```

IPsec SA sample command:

```
security ipsec show-ipseca -node hosting_node_name_for_svm_ip
```



# Configure firewall policies for LIFs

Setting up a firewall enhances the security of the cluster and helps prevent unauthorized access to the storage system. By default, the firewall service allows remote systems access to a specific set of default services for data, management, and intercluster LIFs.

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/CIFS.

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.

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

Firewall policy	Default service protocols	Default access	LIFs applied to
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 starting in 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.
- Starting in 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 previous ONTAP versions, 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 -policy
mgmt|intercluster|data|custom -service portmap
```

You can use the network interface modify command to apply the firewall policy to an existing LIF. For complete command syntax, see [ONTAP 9 commands](#).

## Create a firewall policy and assigning 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 modify or remove services, 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` and `mgmt` firewall policies include `::/0`, the IPv6 wildcard, in their list of accepted addresses.

- When using ONTAP 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) 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.

- Starting 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 vs1 -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 vs1 -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.

### Example of creating a firewall policy and applying 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

# Commands for managing 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.

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

For more information, see the man pages for the `system services firewall`, `system services firewall policy`, and `network interface modify` commands in [ONTAP 9 commands](#).

## Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.