Configure firewall policies for LIFs

ONTAP 9

aherbin
April 28, 2021

Table of Contents

Configure firewall policies for LIFs 1
Firewall policies and LIFs 1
Portmap service configuration 2
Create a firewall policy and assigning it to a LIF 3

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
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 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.

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
```