保护您的网络安全
ONTAP 9

NetApp
April 24, 2024

目录

保护您的网络安全

使用联邦信息处理标准（FIPS）配置网络安全性

对于所有 SSL 连接， ONTAP 均符合联邦信息处理标准（FIPS） 140-2 的要求。您可以在 ONTAP 中打开和关闭 SSL FIPS 模式，全局设置 SSL 协议以及关闭 RC4 等任何弱密码。

默认情况下， ONTAP 上的 SSL 设置为禁用 FIPS 合规性，并启用 SSL 协议，其中包括以下内容：

- TLSv1.3 (从ONTAP 9.11.1开始)
- TLSv1.2
- TLSv1.1
- TLSv1.

启用 SSL FIPS 模式后，从 ONTAP 到外部客户端或 ONTAP 外部服务器组件的 SSL 通信将使用 FIPS 兼容的 SSL 加密。

如果您希望管理员帐户使用 SSH 公有密钥访问 SVM ，则在启用 SSL FIPS 模式之前，必须确保主机密钥算法受支持。

注： ONTAP 9.11.1及更高版本对主机密钥算法的支持已发生更改。

ONTAP 版本	支持的密钥类型	不支持的密钥类型
9.11.1及更高版本	ECDSA-SHA2-nistp256	RSA-SHA2-512 RSA-SHA2-256 SSS-ed25519及更高 SSS-DSS SSS-RSA
9.10.1及更早版本	ECDSA-SHA2-nistp256 SSS-ed25519	SSS-DSS SSS-RSA

在启用 FIPS 之前，必须使用支持的密钥类型重新配置不具有受支持密钥算法的现有 SSH 公有密钥帐户，否则管理员身份验证将失败。

有关详细信息，请参见 "启用 SSH 公有密钥帐户"。

有关SSL FIPS模式配置的详细信息、请参见 `security config modify` 手册页。

启用 FIPS

建议所有安全用户在系统安装或升级后立即调整其安全配置。启用 SSL FIPS 模式后，从 ONTAP 到外部客户端或 ONTAP 外部服务器组件的 SSL 通信将使用 FIPS 兼容的 SSL 加密。

> 启用FIPS后、您不能安装或创建RSA密钥长度为4096的证书。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 启用FIPS：

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

3. 当系统提示您继续时、输入 `y`

4. 如果您运行的是 ONTAP 9.8 或更早版本，请逐个手动重新启动集群中的每个节点。从 ONTAP 9.1.1 开始，不需要重新启动。

示例

如果您运行的是 ONTAP 9.9.1 或更高版本，则不会看到警告消息。

```
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
```

禁用 FIPS

如果您仍在运行较旧的系统配置，并且希望为 ONTAP 配置向后兼容性，则只有在禁用 FIPS 时才能打开 SSLv3。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 通过键入以下命令禁用 FIPS：

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

3. 当系统提示您继续时、输入 `y`。

4. 如果您运行的是 ONTAP 9.8 或更早版本，请手动重新启动集群中的每个节点。从 ONTAP 9.1.1 开始，不需要重新启动。

示例

如果您运行的是 ONTAP 9.9.1 或更高版本，则不会看到警告消息。

```
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
```

查看 FIPS 合规状态

您可以查看整个集群是否正在运行当前安全配置设置。

步骤

1. 逐个重新启动集群中的每个节点。

   请勿同时重新启动所有集群节点。要确保集群中的所有应用程序都运行新的安全配置，并对 FIPS 开关模式，协议和密码进行所有更改，需要重新启动。

2. 查看当前合规状态：

   ```
   security config show
   ```

```
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
```

通过线缆加密配置 IP 安全性（ IP security， IPsec ）

ONTAP在传输模式下使用互联网协议安全性(Internet Protocol Security、IPsec)来确保数据持续安全和加密、即使在传输过程中也是如此。IPsec 为所有 IP 流量提供数据加密，包括 NFS， iSCSI 和 SMB 协议。

从ONTAP 9.12.1开始、MetroCluster IP和MetroCluster 光纤连接配置支持前端主机协议IPsec。MetroCluster 集群中的IPsec支持仅限于前端主机流量、MetroCluster 集群间LIF不支持。

从 ONTAP 9.10.1 开始，您可以使用预共享密钥（ PSK ）或证书通过 IPsec 进行身份验证。以前， IPsec 仅支持 PSK 。

从ONTAP 9.1.1开始、IPsec使用的加密算法已通过FIPS 140-2验证。这些算法由ONTAP 中的NetApp加密模块生成、该模块执行FIPS 140-2验证。

从ONTAP 9.8开始、ONTAP支持在传输模式下使用IPsec。

配置 IPsec 后，客户端和 ONTAP 之间的网络流量将通过预防措施得到保护，以防止重放和中间人（ MIM ）攻击。

对于 NetApp SnapMirror 和集群对等流量加密，仍然建议使用集群对等加密（ Cluster peering encryption， CPE ）和传输层安全（ Transport Layer Security， TLS ）而不是通过 IPsec 进行，以便通过线缆进行安全传输。这是因为 TLS 的性能优于 IPsec 。

在集群上启用了 IPsec 功能时，网络需要使用安全策略数据库（ SPD ）条目来匹配要保护的流量，并指定保护详细信息（例如密码套件和身份验证方法），然后才能使流量流动。每个客户端上也需要相应的 SPD 条目。

在集群上启用 IPsec

您可以在集群上启用 IPsec ，以确保数据持续安全和加密，即使在传输期间也是如此。

步骤

1. 发现是否已启用 IPsec：

   ```
   security ipsec config show
   ```

   如果结果包括 `IPsec Enabled: false`下，继续下一步。

2. 启用 IPsec：

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

3. 再次运行 discovery 命令：

   ```
   security ipsec config show
   ```

   结果现在包括 `IPsec Enabled: true`。

准备使用证书身份验证创建IPsec策略

如果您仅使用预共享密钥(PSK)进行身份验证、而不使用证书身份验证、则可以跳过此步骤。

在创建使用证书进行身份验证的IPsec策略之前，必须验证是否满足以下前提条件：

- ONTAP和客户端都必须安装另一方的CA证书、以使最终实体(ONTAP或客户端)证书可由双方验证
- 系统会为参与此策略的 ONTAP LIF 安装证书

> ONTAP LIF 可以共享证书。不需要在证书和 LIF 之间进行一对一映射。

步骤

1. 将在相互身份验证期间使用的所有CA证书(包括ONTAP端和客户端CA)安装到ONTAP证书管理中、除非已安装(例如ONTAP自签名根CA)。

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

2. 要确保安装的CA在身份验证期间位于IPsec CA搜索路径内、请使用将ONTAP证书管理CA添加到IPsec模块 `security ipsec ca-certificate add` 命令：

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

3. 创建并安装一个证书以供 ONTAP LIF 使用。此证书的颁发者 CA 必须已安装到 ONTAP 并添加到 IPsec 中。

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

有关ONTAP中证书的详细信息，请参见ONTAP 9文档中的security certificates命令。

定义安全策略数据库（ SPD ）

在允许流量在网络上流动之前， IPsec 需要 SPD 条目。无论您使用的是 PSk 还是证书进行身份验证，都是如此。

步骤

1. 使用 `security ipsec policy create` 命令：
   a. 选择要参与 ONTAP 传输的 IPsec IP 地址或 IP 地址子网。
   b. 选择要连接到 ONTAP IP 地址的客户端 IP 地址。

      > 客户端必须使用预共享密钥（ psk ）支持 Internet 密钥交换版本 2 （ IKEv2 ）。

   c. 可选。选择细化的流量参数、例如上层协议(UDP、TCP、ICMP等))、本地端口号和用于保护流量的远

程端口号。相应的参数为 `protocols`， `local-ports` 和 `remote-ports` 。

跳过此步骤可保护 ONTAP IP 地址和客户端 IP 地址之间的所有流量。默认情况下，保护所有流量。

d. 为输入PSK或公共密钥基础架构(PKI) `auth-method` 所需身份验证方法的参数。

   i. 如果输入PSK、请包含参数、然后按<enter>显示提示、以输入并验证预共享密钥。

   > `local-identity` 和 `remote-identity` 如果主机和客户端均使用strong、并且未为主机或客户端选择通配符策略、则参数为可选参数。

   ii. 如果输入PKI、则还需要输入 `cert-name`， `local-identity`， `remote-identity` parameters 如果远程端证书标识未知、或者如果需要多个客户端标识、请输入特殊标识 `ANYTHING`。

```
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
```

只有在ONTAP和客户端都设置了匹配的IPsec策略并且身份验证凭据(PSK或证书)在两端都到位之后、IP流量才能在客户端和服务器之间流动。有关详细信息、请参见客户端IPsec配置。

使用 IPsec 身份

对于预共享密钥身份验证方法、如果主机和客户端都使用strong、并且未为主机或客户端选择通配符策略、则本地和远程标识是可选的。

对于 PKI/ 证书身份验证方法，本地和远程身份都是必需的。这些身份用于指定在每一方的证书中进行认证并在验证过程中使用的身份。如果远程身份未知或可能是多个不同的身份、请使用特殊身份 `ANYTHING`。

关于此任务

在 ONTAP 中，标识是通过修改 SPD 条目或在创建 SPD 策略期间指定的。SPD 可以是 IP 地址或字符串格式的标识名称。

步骤

要修改现有SPD标识设置、请使用以下命令：

```
security ipsec policy modify
```

命令示例

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

IPsec 多客户端配置

如果少数客户端需要利用 IPsec ，则为每个客户端使用一个 SPD 条目就足以满足要求。但是，当数百甚至数千个客户端需要利用 IPsec 时， NetApp 建议使用 IPsec 多客户端配置。

关于此任务

ONTAP 支持将多个网络中的多个客户端连接到启用了 IPsec 的单个 SVM IP 地址。您可以使用以下方法之一完成此操作：

- * 子网配置 *

  要允许特定子网上的所有客户端(例如192.168.134.0/24)使用单个SPD策略条目连接到单个SVM IP地址、必须指定 `remote-ip-subnets` 子网形式。此外、您还必须指定 `remote-identity` 具有正确客户端标识的字段。

  > 在子网配置中使用单个策略条目时，该子网中的 IPsec 客户端将共享 IPsec 身份和预共享密钥（ PSk ）。但是，对于证书身份验证，情况并非如此。使用证书时，每个客户端都可以使用自己的唯一证书或共享证书进行身份验证。ONTAP IPsec 会根据安装在其本地信任存储上的 CA 检查证书的有效性。ONTAP 还支持证书撤消列表（ Certificate Revocation List ， CRL ）检查。

- * 允许所有客户端配置 *

  要允许任何客户端(无论其源IP地址如何)连接到已启用SVM IPsec的IP地址、请使用 `0.0.0.0/0` 指定时使用通配符 `remote-ip-subnets` 字段。

  此外、您还必须指定 `remote-identity` 具有正确客户端标识的字段。对于证书身份验证、您可以输入 `ANYTHING`。

  此外、当 `0.0.0.0/0` 如果使用通配符、则必须配置要使用的特定本地或远程端口号。例如： `NFS port 2049`。

  步骤

  a. 使用以下命令之一为多个客户端配置IPsec。

     i. 如果使用*subnetconfiguration (子网配置)*支持多个IPsec客户端：

     ```
     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
     ```

     命令示例

     ```
     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. 如果使用*允许所有客户端配置*支持多个IPsec客户端：

     ```
     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
     ```

命令示例

```
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 统计信息

通过协商，可以在 ONTAP SVM IP 地址和客户端 IP 地址之间建立一个称为 "ike 安全关联（ SA ） " 的安全通道。IPsec SAS 安装在两个端点上，用于执行实际的数据加密和解密工作。

您可以使用 statistics 命令来检查 IPsec SAS 和 ike SAS 的状态。

命令示例

IKESA 命令示例：

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

IPsec SA 命令和输出示例：

```
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 命令和输出示例：

```
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
```

为 LIF 配置防火墙策略

设置防火墙可增强集群的安全性，并有助于防止未经授权访问存储系统。默认情况下，板载防火墙配置为允许远程访问数据，管理和集群间 LIF 的一组特定 IP 服务。

从 ONTAP 9.10.1 开始：

- 防火墙策略已弃用、并由LIF服务策略取代。以前，板载防火墙是使用防火墙策略进行管理的。现在，可以使用 LIF 服务策略来实现此功能。
- 所有防火墙策略均为空，不会打开底层防火墙中的任何端口。而是必须使用 LIF 服务策略打开所有端口。
- 升级到9.10.1或更高版本后、无需执行任何操作即可从防火墙策略过渡到LIF服务策略。系统会根据上一个ONTAP 版本中使用的防火墙策略自动构建LIF服务策略。如果您使用脚本或其他工具创建和管理自定义防火墙策略，则可能需要升级这些脚本以创建自定义服务策略。

要了解更多信息，请参见 "ONTAP 9.6 及更高版本中的 LIF 和服务策略"。

防火墙策略可用于控制对 SSH ， HTTP ， HTTPS ， Telnet ， NTP ， NDMP ， NDMPS ， RSH ， DNS 或 SNMP 。无法为 NFS 或 SMB 等数据协议设置防火墙策略。

您可以通过以下方式管理防火墙服务和策略：

- 启用或禁用防火墙服务
- 显示当前防火墙服务配置
- 使用指定的策略名称和网络服务创建新的防火墙策略
- 将防火墙策略应用于逻辑接口
- 创建与现有策略完全相同的新防火墙策略

  您可以使用此选项在同一 SVM 中创建具有类似特征的策略，或者将此策略复制到其他 SVM 。

- 显示有关防火墙策略的信息
- 修改防火墙策略使用的 IP 地址和网络掩码
- 删除 LIF 未使用的防火墙策略

防火墙策略和 LIF

LIF 防火墙策略用于限制通过每个 LIF 对集群的访问。您需要了解默认防火墙策略如何影响通过每种类型的 LIF 进行的系统访问，以及如何自定义防火墙策略以通过 LIF 提高或降低安全性。

使用配置LIF时 `network interface create` 或 `network interface modify` 命令、即为指定的值 `-firewall-policy` 参数用于确定允许访问LIF的服务协议和IP地址。

在许多情况下，您可以接受默认防火墙策略值。在其他情况下，您可能需要限制对某些 IP 地址和某些管理服务协议的访问。可用的管理服务协议包括 SSH ， HTTP ， HTTPS ， Telnet ， NTP ， NDMP ， NDMPS ， RSH ， DNS 和 SNMP 。

所有集群SIFs的防火墙策略默认为 `""` 并且无法修改。

下表介绍了在创建 LIF 时分配给每个 LIF 的默认防火墙策略，具体取决于其角色（ ONTAP 9.5 及更早版本）或服务策略（ ONTAP 9.6 及更高版本）：

防火墙策略	默认服务协议	默认访问	应用于的 LIF
管理	DNS ， http ， https ， NDMP ， NDMPS ， NTP ， SNMP ， ssh	任何地址（ 0.0.0.0/0 ）	集群管理， SVM 管理和节点管理 LIF
MGMT-NFS	DNS ， http ， https ， NDMP ， NDMPS ， NTP ，端口映射， SNMP ， ssh	任何地址（ 0.0.0.0/0 ）	也支持 SVM 管理访问的数据 LIF
集群间	HTTPS ， NDMP ， NDMPS	任何地址（ 0.0.0.0/0 ）	所有集群间 LIF
数据	DNS ， NDMP ， NDMPS ， portmap	任何地址（ 0.0.0.0/0 ）	所有数据 LIF

portmap 服务配置

portmap 服务会将 RPC 服务映射到它们侦听的端口。

portmap 服务在 ONTAP 9.3 及更早版本中始终可访问，在 ONTAP 9.4 至 ONTAP 9.6 中可配置，并从 ONTAP 9.7 开始自动进行管理。

- 在 ONTAP 9.3 及更早版本中， portmap 服务（ rpcbind ）始终可通过网络配置中的端口 111 访问，该端口依赖于内置的 ONTAP 防火墙，而不是第三方防火墙。
- 从 ONTAP 9.4 到 ONTAP 9.6 ，您可以修改防火墙策略，以控制是否可通过特定 LIF 访问 portmap 服务。
- 从 ONTAP 9.7 开始，不再使用 portmap 防火墙服务。而是会自动为支持 NFS 服务的所有 LIF 打开 portmap 端口。
- 在 ONTAP 9.4 到 ONTAP 9.6* 中，可以在防火墙中配置端口映射服务

本主题的其余部分将讨论如何为 ONTAP 9.4 到 ONTAP 9.6 版配置 portmap 防火墙服务。

根据您的配置，您可能会禁止对特定类型的 LIF （通常为管理 LIF 和集群间 LIF ）访问服务。在某些情况下，您甚至可以禁止对数据 LIF 进行访问。

您可以预期的行为

ONTAP 9.4 到 ONTAP 9.6 的行为旨在在升级时实现无缝过渡。如果 portmap 服务已通过特定类型的 LIF 进行访问，则它将继续通过这些类型的 LIF 进行访问。与ONTAP 9.3及更早版本一样、您可以在防火墙策略中为LIF类型指定可在防火墙内访问的服务。

要使此行为生效，集群中的所有节点都必须运行 ONTAP 9.4 到 ONTAP 9.6 。仅影响入站流量。

新规则如下：

- 升级到 9.4 到 9.6 版后， ONTAP 会将 portmap 服务添加到所有现有防火墙策略中，默认或自定义。

- 在创建新集群或新 IP 空间时， ONTAP 仅会将 portmap 服务添加到默认数据策略中，而不会添加到默认管理或集群间策略中。
- 您可以根据需要将 portmap 服务添加到默认策略或自定义策略中，并根据需要删除此服务。

如何添加或删除**portmap**服务

要将 portmap 服务添加到 SVM 或集群防火墙策略中（使其可在防火墙内访问），请输入：

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

要从 SVM 或集群防火墙策略中删除 portmap 服务（使其无法在防火墙内访问），请输入：

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

您可以使用 network interface modify 命令将防火墙策略应用于现有 LIF 。有关完整的命令语法，请参见 "ONTAP 9 命令"。

创建防火墙策略并将其分配给 LIF

创建 LIF 时，系统会为每个 LIF 分配默认防火墙策略。在许多情况下，默认防火墙设置运行良好，您无需更改它们。如果要更改可访问 LIF 的网络服务或 IP 地址，可以创建自定义防火墙策略并将其分配给 LIF 。

关于此任务

- 您不能使用创建防火墙策略 `policy` name `data`， `intercluster`， `cluster`或 `mgmt`。

  这些值是为系统定义的防火墙策略保留的。

- 您不能为集群 LIF 设置或修改防火墙策略。

  对于所有服务类型，集群 LIF 的防火墙策略均设置为 0.0.0.0/0 。

- 如果需要从策略中删除服务，则必须删除现有防火墙策略并创建新策略。
- 如果集群上启用了 IPv6 ，则可以使用 IPv6 地址创建防火墙策略。

  启用IPv6后、 `data`， `intercluster`，和 `mgmt` 防火墙策略的可接受地址列表中包括：：： /0 (IPv6通配符)。

- 在使用 System Manager 跨集群配置数据保护功能时，您必须确保允许列表中包含集群间 LIF IP 地址，并且允许在集群间 LIF 和公司拥有的防火墙上使用 HTTPS 服务。

  默认情况下、 `intercluster` 防火墙策略允许从所有IP地址(0.0.0.0/0或：：： /0表示IPv6)进行访问、并启用HTTPS、NDMP和NDMP服务。如果修改此默认策略，或者为集群间 LIF 创建自己的防火墙策略，则必须将每个集群间 LIF IP 地址添加到允许列表中并启用 HTTPS 服务。

- 从 ONTAP 9.6 开始，不支持 HTTPS 和 SSH 防火墙服务。

  在ONTAP 9.6中、 `management-https` 和 `management-ssh` LIF服务可用于HTTPS和SSH管理访问。

步骤

1. 创建可供特定 SVM 上的 LIF 使用的防火墙策略：

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

   您可以多次使用此命令为防火墙策略中的每个服务添加多个网络服务和允许的 IP 地址列表。

2. 使用验证是否已正确添加此策略 `system services firewall policy show` 命令：
3. 将防火墙策略应用于 LIF ：

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

4. 使用验证是否已将此策略正确添加到LIF `network interface show -fields firewall-policy` 命令：

创建防火墙策略并将其应用于**LIF**的示例

以下命令将创建一个名为 data_http 的防火墙策略，用于从 10.10 子网上的 IP 地址访问 HTTP 和 HTTPS 协议，并将该策略应用于 SVM vs1 上名为 data1 的 LIF ，然后显示集群上的所有防火墙策略：

```
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
```

用于管理防火墙服务和策略的命令

您可以使用 `system services firewall` 用于管理防火墙服务的命令 `system services firewall policy` 用于管理防火墙策略的命令、以及 `network interface modify` 用于管理LIFs的防火墙设置的命令。

如果您要 ...	使用此命令 ...
启用或禁用防火墙服务	`system services firewall modify`
显示防火墙服务的当前配置	`system services firewall show`
创建防火墙策略或向现有防火墙策略添加服务	`system services firewall policy create`
将防火墙策略应用于 LIF	`network interface modify -lif lifname -firewall-policy`
修改与防火墙策略关联的 IP 地址和网络掩码	`system services firewall policy modify`
显示有关防火墙策略的信息	`system services firewall policy show`
创建一个与现有策略完全相同的新防火墙策略	`system services firewall policy clone`
删除 LIF 未使用的防火墙策略	`system services firewall policy delete`

有关详细信息、请参见的手册页 `system services firewall`， `system services firewall policy` ，和 `network interface modify` 中的命令 "ONTAP 9 命令"。