Proteja su red

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Proteja su red

Configuración de la seguridad de red mediante estándares federales de procesamiento de información (FIPS)

ONTAP cumple con los estándares de procesamiento de información federal (FIPS) 140-2 para todas las conexiones SSL. Puede activar y desactivar el modo FIPS de SSL, establecer protocolos SSL a nivel global y desactivar todos los cifrados débiles, como RC4 dentro de ONTAP.

De forma predeterminada, SSL en ONTAP se establece con el cumplimiento FIPS deshabilitado y el protocolo SSL habilitado con lo siguiente:

- TLSv1.3 (a partir de ONTAP 9.11.1)
- TLSv1,2
- TLSv1,1
- TLSv1

Cuando el modo SSL FIPS está activado, la comunicación SSL desde ONTAP a componentes de cliente o servidor externos a ONTAP utilizará cifrado compatible con FIPS para SSL.

Si desea que las cuentas de administrador accedan a SVM con una clave pública SSH, debe asegurarse de que el algoritmo de clave de host sea compatible antes de habilitar el modo SSL FIPS.

Nota: la compatibilidad con el algoritmo de clave de host ha cambiado en ONTAP 9.11.1 y versiones posteriores.

Versión de ONTAP	Tipos de clave admitidos	Tipos de claves no compatibles
9.11.1 y posterior	ecdsa-sha2-nistp256	rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 y anteriores	ecdsa-sha2-nistp256 ssh-ed25519	ssh-dss ssh-rsa

Las cuentas de clave pública SSH existentes sin los algoritmos de clave admitidos deben volver a configurarse con un tipo de clave compatible antes de habilitar FIPS o la autenticación del administrador fallará.

Para obtener más información, consulte "Habilite cuentas de clave pública de SSH".

Para obtener más información acerca de la configuración del modo FIPS de SSL, consulte `security config modify` página de manual.

Habilite FIPS

Se recomienda que todos los usuarios seguros ajusten su configuración de seguridad inmediatamente después de instalar o actualizar el sistema. Cuando el modo SSL FIPS está activado, la comunicación SSL desde ONTAP a componentes de cliente o servidor externos a ONTAP utilizará cifrado compatible con FIPS para SSL.

> Cuando FIPS está habilitada, no se puede instalar ni crear un certificado con una longitud de clave RSA de 4096.

Pasos

1. Cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Habilitar FIPS:

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

3. Cuando se le solicite continuar, introduzca `y`
4. Si ejecuta ONTAP 9.8 o versiones anteriores, reinicie manualmente cada nodo del clúster de uno en uno. A partir de ONTAP 9.9.1, no es necesario reiniciar.

Ejemplo

Si está ejecutando ONTAP 9.9.1 o posterior, no verá el mensaje de advertencia.

```
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
```

Deshabilite FIPS

Si sigue ejecutando una configuración de sistema anterior y desea configurar ONTAP con compatibilidad con versiones anteriores, solo puede activar SSLv3 cuando FIPS esté deshabilitado.

Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Para deshabilitar FIPS, escriba:

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

3. Cuando se le solicite continuar, introduzca `y`.
4. Si utiliza ONTAP 9.8 o una versión anterior, reinicie manualmente cada nodo del clúster. A partir de ONTAP 9.9.1, no es necesario reiniciar.

Ejemplo

Si está ejecutando ONTAP 9.9.1 o posterior, no verá el mensaje de advertencia.

```
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
```

Ver el estado de cumplimiento de normativas FIPS

Puede ver si el clúster completo está ejecutando las opciones de configuración de seguridad actuales.

Pasos

1. De uno a uno, reinicie cada nodo del clúster.

   No reinicie todos los nodos del clúster en simultáneo. Se requiere un reinicio para asegurarse de que todas las aplicaciones del clúster estén ejecutando la nueva configuración de seguridad y para todos los cambios en el modo de encendido/apagado, los protocolos y los cifrados de FIPS.

2. Ver el estado de cumplimiento actual:

```
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
```

Configurar la seguridad IP (IPsec) a través del cifrado de cable

ONTAP utiliza la seguridad del protocolo de Internet (IPsec) en el modo de transporte para garantizar que los datos estén protegidos y cifrados de forma continua, incluso durante el tránsito. IPSec ofrece cifrado de datos para todo el tráfico IP, incluidos los protocolos NFS, iSCSI y SMB.

A partir de ONTAP 9.12.1, está disponible la compatibilidad con IPsec del protocolo de host de interfaz de usuario en las configuraciones con conexión a la estructura de MetroCluster IP y MetroCluster.
La compatibilidad con IPSec en clústeres de MetroCluster se limita al tráfico de host de front-end y no se admite en las LIF de interconexión de clústeres de MetroCluster.

A partir de ONTAP 9.10.1, puede utilizar claves precompartidas (PSK) o certificados para la autenticación con IPsec. Anteriormente, sólo PSK eran compatibles con IPsec.

A partir de ONTAP 9.9.1, los algoritmos de cifrado utilizados por IPsec están validados con FIPS 140-2-2. Los algoritmos los genera el módulo de criptografía de NetApp en ONTAP, que conlleva la validación FIPS 140-2-2.

A partir de ONTAP 9,8, ONTAP admite IPsec en modo de transporte.

Una vez configurado IPsec, el tráfico de red entre el cliente y ONTAP está protegido con medidas preventivas para combatir los ataques de repetición y de hombre en el medio (MITM).

Para el cifrado de tráfico de paridad de clústeres y SnapMirror de NetApp, se recomienda el cifrado de paridad de clústeres (CPE) y la seguridad de la capa de transporte (TLS) a través de IPsec para garantizar la seguridad en tránsito por el cable. Esto se debe a que TLS tiene mejor rendimiento que IPsec.

Aunque la capacidad IPsec está habilitada en el clúster, la red requiere una entrada de base de datos de directivas de seguridad (SPD) para que coincida con el tráfico a proteger y para especificar detalles de protección (como la suite de cifrado y el método de autenticación) antes de que pueda fluir el tráfico. También se necesita una entrada SPD correspondiente en cada cliente.

Habilite IPsec en el clúster

Puede habilitar IPsec en el clúster para asegurarse de que los datos están protegidos y cifrados de forma continua, incluso mientras están en tránsito.

Pasos

1. Detectar si IPsec está activada:

   ```
   security ipsec config show
   ```

   Si el resultado incluye `IPsec Enabled: false`, continúe con el próximo paso.

2. Habilitar IPsec:

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

3. Vuelva a ejecutar el comando Discovery:

   ```
   security ipsec config show
   ```

   El resultado ahora incluye `IPsec Enabled: true`.

Prepárese para la creación de directivas IPsec con autenticación de certificados

Puede omitir este paso si solo utiliza claves precompartidas (PSKs) para la autenticación y no utilizará la autenticación de certificados.

Antes de crear una política IPsec que utilice certificados para la autenticación, debe verificar que se cumplan los siguientes requisitos previos:

- Tanto ONTAP como el cliente deben tener instalado el certificado CA de la otra parte para que los certificados de la entidad final (ya sea ONTAP o el cliente) sean verificables por ambas partes
- Se instala un certificado para el LIF de ONTAP que participa en la política

> Las LIF de ONTAP pueden compartir certificados. No es necesario realizar una asignación de uno a uno entre certificados y LIF.

Pasos

1. Instale todos los certificados de CA utilizados durante la autenticación mutua, incluidas las CA de ONTAP y del lado del cliente, en la gestión de certificados de ONTAP a menos que ya esté instalado (como es el caso de una CA raíz autofirmado de ONTAP).

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

2. Para asegurarse de que la CA instalada se encuentra dentro de la ruta de búsqueda de la CA IPsec durante la autenticación, agregue las CA de gestión de certificados ONTAP al módulo IPsec mediante `security ipsec ca-certificate add` comando.

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

3. Cree e instale un certificado para que lo utilice la LIF de ONTAP. La entidad emisora de certificados de este certificado ya debe estar instalada en ONTAP y agregada a IPsec.

Comando de ejemplo

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

Para obtener más información sobre los certificados de ONTAP, consulte los comandos de certificado de seguridad en la documentación de ONTAP 9 .

Definir la base de datos de directivas de seguridad (SPD)

IPSec requiere una entrada SPD antes de permitir que el tráfico fluya por la red. Esto es cierto tanto si está utilizando un PSK como un certificado para la autenticación.

Pasos

1. Utilice la `security ipsec policy create` comando para:
   a. Seleccione la dirección IP de ONTAP o la subred de direcciones IP para participar en el transporte IPsec.
   b. Seleccione las direcciones IP del cliente que se conectarán a las direcciones IP de ONTAP.

      El cliente debe admitir la versión 2 de Exchange de claves de Internet (IKEv2) con una clave compartida previamente (PSK).

   c. Opcional. Seleccione los parámetros de tráfico detallados, como los protocolos de capa superior (UDP, TCP, ICMP, etc.)), los números de puerto locales y los números de puerto remotos para proteger el tráfico. Los parámetros correspondientes son `protocols`, `local-ports` y.. `remote-ports` respectivamente.

      Omita este paso para proteger todo el tráfico entre la dirección IP de ONTAP y la dirección IP del cliente. La protección de todo el tráfico es la opción predeterminada.

   d. Introduzca PSK o la infraestructura de clave pública (PKI) para el `auth-method` parámetro del método de autenticación deseado.
      i. Si introduce un PSK, incluya los parámetros y, a continuación, pulse <enter> para que el mensaje introduzca y verifique la clave precompartida.

         `local-identity` y.. `remote-identity` Los parámetros son opcionales si tanto el host como el cliente utilizan strongSwan y no se ha seleccionado ninguna política de comodín para el host o el cliente.

      ii. Si introduce una PKI, deberá introducir también la `cert-name`, `local-identity`, `remote-identity` parámetros. Si la identidad del certificado del lado remoto es desconocida o si se esperan varias identidades de cliente, introduzca la identidad especial `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
```

El tráfico IP no puede fluir entre el cliente y el servidor hasta que ONTAP y el cliente hayan configurado las directivas IPsec coincidentes y las credenciales de autenticación (PSK o certificado) estén en su lugar en ambos lados. Para obtener más información, consulte la configuración de IPsec del lado del cliente.

Usar identidades IPsec

Para el método de autenticación de clave precompartida, las identidades locales y remotas son opcionales si tanto el host como el cliente utilizan strongSwan y no se selecciona ninguna política de comodín para el host o el cliente.

Para el método de autenticación PKI/certificado, las identidades locales y remotas son obligatorias. Las identidades especifican qué identidad está certificada dentro del certificado de cada lado y se utilizan en el proceso de verificación. Si la identidad remota es desconocida o si podría ser una identidad muy distinta, utilice la identidad especial `ANYTHING`.

Acerca de esta tarea

En ONTAP, las identidades se especifican modificando la entrada SPD o durante la creación de la política SPD. El SPD puede ser una dirección IP o un nombre de identidad con formato de cadena.

Paso

Para modificar una configuración de identidad SPD existente, utilice el siguiente comando:

```
security ipsec policy modify
```

Comando de ejemplo

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

Configuración de varios clientes IPSec

Cuando un pequeño número de clientes necesitan aprovechar IPsec, es suficiente utilizar una sola entrada SPD para cada cliente. Sin embargo, cuando cientos o incluso miles de clientes necesitan aprovechar IPsec, NetApp recomienda el uso de una configuración de varios clientes IPsec.

Acerca de esta tarea

ONTAP admite la conexión de varios clientes a través de varias redes a una única dirección IP de SVM con IPsec habilitada. Para ello, utilice uno de los siguientes métodos:

- **Configuración de subred**

  Para permitir que todos los clientes de una subred determinada (por ejemplo, 192.168.134.0/24) se conecten a una única dirección IP de SVM mediante una única entrada de directiva SPD, debe especificar el `remote-ip-subnets` en formato de subred. Además, debe especificar el `remote-identity` campo con la identidad del cliente correcta.

> Al utilizar una sola entrada de directiva en una configuración de subred, los clientes IPsec de esa subred comparten la identidad IPsec y la clave precompartida (PSK). Sin embargo, esto no es cierto con la autenticación de certificado. Cuando se utilizan certificados, cada cliente puede utilizar su propio certificado único o un certificado compartido para autenticarse. IPsec de ONTAP comprueba la validez del certificado en función de las CA instaladas en el almacén de confianza local. ONTAP también admite la comprobación de la lista de revocación de certificados (CRL).

- **Permitir la configuración de todos los clientes**

  Para permitir que cualquier cliente, independientemente de su dirección IP de origen, se conecte a la dirección IP habilitada para IPsec de SVM, utilice `0.0.0.0/0` comodín al especificar `remote-ip-subnets` campo.

  Además, debe especificar el `remote-identity` campo con la identidad del cliente correcta. Para la autenticación del certificado, puede introducir `ANYTHING`.

  Además, cuando la `0.0.0.0/0` se utiliza el comodín, debe configurar un número de puerto local o remoto específico para utilizarlo. Por ejemplo: `NFS port 2049`.

  Pasos

  a. Utilice uno de los siguientes comandos para configurar IPsec para varios clientes.

     i. Si está utilizando **configuración de subred** para admitir varios clientes IPsec:

     ```
     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
     ```

     Comando de ejemplo

     ```
     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. Si está utilizando **Permitir que todos los clientes configuren** para admitir múltiples clientes IPsec:

     ```
     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
     ```

     Comando de ejemplo

     ```
     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
     ```

Estadísticas IPSec

A través de la negociación, se puede establecer un canal de seguridad denominado Asociación de seguridad IKE (SA) entre la dirección IP de la SVM de ONTAP y la dirección IP del cliente. Las unidades SAS IPSec se instalan en ambos extremos para que funcionen el cifrado y descifrado de datos.

Puede utilizar comandos de estadísticas para comprobar el estado de las unidades SAS IPsec y SAS IKE.

Comandos de ejemplo

Comando de ejemplo IKE SA:

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

Ejemplo de comando SA IPSec y salida:

```
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
```

Ejemplo de comando SA IPSec y salida:

```
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
```

Configurar políticas de firewall para LIF

La configuración de un firewall mejora la seguridad del clúster y ayuda a evitar el acceso no autorizado al sistema de almacenamiento. De forma predeterminada, el firewall incorporado está configurado para permitir el acceso remoto a un conjunto específico de servicios IP para LIF de datos, gestión e interconexión de clústeres.

A partir de ONTAP 9.10.1:

- Las políticas de firewall quedan obsoletas y se reemplazan por las políticas de servicio de LIF. Anteriormente, el firewall incorporado se gestionaba mediante directivas de firewall. Esta funcionalidad ahora se logra usando una política de servicio de LIF.

- Todas las políticas de firewall están vacías y no abren ningún puerto en el firewall subyacente. En su lugar, se deben abrir todos los puertos con una política de servicio de LIF.
- No es necesario realizar ninguna acción después de una actualización a la versión 9.10.1 o posterior para pasar de políticas de firewall a políticas de servicio de LIF. El sistema crea automáticamente políticas de servicio de LIF coherentes con las políticas de firewall que se están usando en la versión anterior de ONTAP. Si utiliza scripts u otras herramientas que crean y gestionan políticas de firewall personalizadas, es posible que deba actualizar dichas secuencias de comandos para crear políticas de servicio personalizadas en su lugar.

Para obtener más información, consulte "LIF y políticas de servicio en ONTAP 9.6 y posteriores".

Las políticas de firewall se pueden utilizar para controlar el acceso a protocolos de servicio de gestión como SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS O SNMP. No se pueden establecer políticas de firewall para protocolos de datos como NFS o SMB.

Puede administrar el servicio y las políticas de firewall de las siguientes maneras:

- Activación o desactivación del servicio de firewall
- Mostrar la configuración actual del servicio de firewall
- Creación de una nueva directiva de firewall con el nombre de directiva y los servicios de red especificados
- Aplicar una política de firewall a una interfaz lógica
- Crear una nueva directiva de firewall que sea una copia exacta de una directiva existente

  Puede usar esto para realizar una política con características similares dentro de la misma SVM o para copiar la política en una SVM diferente.

- Mostrar información acerca de las directivas de firewall
- Modificar las direcciones IP y las máscaras de red que utiliza una directiva de firewall
- Eliminar una política de firewall que no esté en uso en una LIF

Políticas de firewall y LIF

Las políticas de firewall de LIF se utilizan para restringir el acceso al clúster en cada LIF. Debe entender cómo afecta la política de firewall predeterminada al acceso del sistema sobre cada tipo de LIF y cómo puede personalizar una política de firewall para aumentar o reducir la seguridad de una LIF.

Al configurar una LIF con la `network interface create` o. `network interface modify` comando, el valor especificado para `-firewall-policy` El parámetro determina los protocolos de servicio y las direcciones IP a los que se permite el acceso a la LIF.

En muchos casos puede aceptar el valor predeterminado de la política de firewall. En otros casos, es posible que deba restringir el acceso a determinadas direcciones IP y ciertos protocolos de servicio de gestión. Los protocolos de servicio de gestión disponibles incluyen SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS Y SNMP.

De forma predeterminada, la política de firewall para todas las LIF del clúster es `""` y no se puede modificar.

En la siguiente tabla se describen las políticas de firewall predeterminadas que se asignan a cada LIF, en función de su rol (ONTAP 9.5 y versiones anteriores) o política de servicio (ONTAP 9.6 y versiones posteriores), al crear la LIF:

Política de firewall	Protocolos de servicio predeterminados	Acceso predeterminado	LIF aplicadas a.
gestión	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Cualquier dirección (0.0.0.0/0)	Gestión de clústeres, gestión de SVM y LIF de gestión de nodos
gestión de nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Cualquier dirección (0.0.0.0/0)	LIF de datos que también admiten el acceso a la gestión de la SVM
interconexión de clústeres	https, ndmp, ndmps	Cualquier dirección (0.0.0.0/0)	Todas las LIF de interconexión de clústeres
sql server	dns, ndmp, ndmps, portmap	Cualquier dirección (0.0.0.0/0)	Todos los LIF de datos

Configuración del servicio portmap

El servicio portmap asigna los servicios RPC a los puertos en los que escuchan.

El servicio portmap siempre se pudo acceder en ONTAP 9.3 y versiones anteriores, se pasó a configurar en ONTAP 9.4 a través de ONTAP 9.6 y se gestiona automáticamente empezando por ONTAP 9.7.

- En ONTAP 9.3 y anteriores, siempre se pudo acceder al servicio portmap (rpcbind) en el puerto 111 en configuraciones de red que dependían del firewall integrado de ONTAP en lugar de un firewall de terceros.
- Desde ONTAP 9.4 a ONTAP 9.6, puede modificar las políticas de firewall para controlar si el servicio portmap es accesible en determinadas LIF.
- A partir de ONTAP 9.7, se elimina el servicio de firewall de portmap. En su lugar, el puerto portmap se abre automáticamente para todos los LIF que admiten el servicio NFS.

El servicio Portmap se puede configurar en el firewall de ONTAP 9.4 a ONTAP 9.6.

En el resto de este tema se describe cómo configurar el servicio de firewall de portmap para versiones de ONTAP 9.4 a ONTAP 9.6.

En función de la configuración, es posible que no permita el acceso al servicio en tipos específicos de LIF, que suelen ser de gestión y LIF entre clústeres. En algunas circunstancias, puede que incluso no permita el acceso en las LIF de datos.

Qué comportamiento se puede esperar

El comportamiento de ONTAP 9.4 a ONTAP 9.6 está diseñado para proporcionar una transición fluida durante la actualización. Si ya se está accediendo al servicio portmap a través de tipos específicos de LIF, continuará siendo accesible mediante estos tipos de LIF. Al igual que en ONTAP 9,3 y versiones anteriores, puede especificar los servicios a los que se puede acceder dentro del firewall en la política de firewall para el tipo de LIF.

Para que el comportamiento surta efecto, todos los nodos del clúster deben ejecutar de ONTAP 9.4 a ONTAP 9.6. Sólo se ve afectado el tráfico entrante.

Las nuevas reglas son las siguientes:

- Tras la actualización al lanzamiento del 9.4 al 9.6, ONTAP agrega el servicio portmap a todas las políticas de firewall existentes, predeterminadas o personalizadas.
- Cuando crea un nuevo clúster o un nuevo espacio IP, ONTAP agrega el servicio portmap solo a la política de datos predeterminada, no a las políticas de gestión o interconexión de clústeres predeterminadas.
- Puede agregar el servicio portmap a las políticas predeterminadas o personalizadas según sea necesario y eliminar el servicio según sea necesario.

Cómo agregar o quitar el servicio portmap

Para agregar el servicio portmap a una política de firewall de SVM o clúster (hacer que sea accesible dentro del firewall), introduzca:

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

Para quitar el servicio portmap de una política de firewall de SVM o clúster (hacer que sea inaccesible dentro del firewall), introduzca:

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

Puede usar el comando network interface modify para aplicar la política del firewall a una LIF existente. Para obtener una sintaxis completa del comando, consulte "Comandos de ONTAP 9".

Cree una política de firewall y asígnela a una LIF

Las políticas de firewall predeterminadas se asignan a cada LIF al crear la LIF. En muchos casos, la configuración predeterminada del firewall funciona bien y no es necesario modificarla. Si desea cambiar los servicios de red o las direcciones IP que pueden acceder a una LIF, puede crear una política de firewall personalizada y asignarla a la LIF.

Acerca de esta tarea

- No puede crear una directiva de firewall con `policy` nombre `data`, `intercluster`, `cluster`, o. `mgmt`.

  Estos valores se reservan para las políticas de firewall definidas por el sistema.

- No puede establecer ni modificar una política de firewall para las LIF del clúster.

  La política de firewall para las LIF del clúster se establece en 0.0.0.0/0 para todos los tipos de servicios.

- Si necesita quitar un servicio de una política, debe eliminar la política de firewall existente y crear una nueva.
- Si IPv6 está habilitado en el clúster, puede crear políticas de firewall con direcciones IPv6.

  Una vez que IPv6 está habilitado, `data`, `intercluster`, y. `mgmt` Las políticas de firewall incluyen ::/0, el comodín IPv6, en su lista de direcciones aceptadas.

- Cuando se usa System Manager para configurar la funcionalidad de protección de datos en todos los clústeres, se debe asegurarse de que las direcciones IP de LIF entre clústeres estén incluidas en la lista permitida y que el servicio HTTPS esté en las LIF entre clústeres y en los firewalls de propiedad de la empresa.

  De forma predeterminada, la `intercluster` La directiva de firewall permite el acceso desde todas las

direcciones IP (0.0.0.0/0, o ::/0 para IPv6) y habilita los servicios HTTPS, NDMP y NDMPS. Si modifica esta política predeterminada o crea su propia política de firewall para las LIF de interconexión de clústeres, debe añadir cada dirección IP de la LIF entre clústeres a la lista permitida y habilitar el servicio HTTPS.

- A partir de ONTAP 9.6, los servicios de firewall HTTPS y SSH no son compatibles.

  En ONTAP 9.6, el `management-https` y.. `management-ssh` Los servicios LIF están disponibles para el acceso de gestión HTTPS y SSH.

Pasos

1. Cree una política de firewall que estará disponible para las LIF en una SVM específica:

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

   Puede usar este comando varias veces para agregar más de un servicio de red y una lista de direcciones IP permitidas para cada servicio de la directiva de firewall.

2. Compruebe que la directiva se ha agregado correctamente utilizando `system services firewall policy show` comando.
3. Aplique la política de firewall a una LIF:

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

4. Compruebe que la política se ha añadido correctamente a la LIF mediante el `network interface show -fields firewall-policy` comando.

Ejemplo de creación de una política de firewall y su aplicación a una LIF

El siguiente comando crea una política de firewall llamada data_http que permite el acceso al protocolo HTTP y HTTPS desde direcciones IP de la subred 10.10, aplica esa política a la LIF llamada data1 en la SVM vs1 y, a continuación, muestra todas las políticas de firewall del clúster:

```
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
```

Comandos para administrar el servicio y las políticas de firewall

Puede utilizar el `system services firewall` comandos para administrar el servicio de firewall, el `system services firewall policy` comandos para administrar las directivas de firewall y la `network interface modify` Comando para administrar la configuración del firewall de las LIF.

Si desea…	Se usa este comando…
Active o desactive el servicio de firewall	`system services firewall modify`
Muestra la configuración actual del servicio de firewall	`system services firewall show`
Cree una política de firewall o agregue un servicio a una política de firewall existente	`system services firewall policy create`
Aplique una política de firewall a una LIF	`network interface modify -lif lifname -firewall-policy`
Modifique las direcciones IP y las máscaras de red asociadas a una directiva de firewall	`system services firewall policy modify`
Mostrar información acerca de las políticas de firewall	`system services firewall policy show`
Cree una nueva directiva de firewall que sea una copia exacta de una directiva existente	`system services firewall policy clone`
Eliminar una política de firewall que no esté usando una LIF	`system services firewall policy delete`

Para obtener más información, consulte las páginas de manual de `system services firewall`, `system services firewall policy`, y. `network interface modify` comandos de "Comandos de ONTAP 9".