Proteja a sua rede

ONTAP 9

NetApp
January 17, 2025

Índice

Proteja a sua rede

Configurar a segurança da rede usando padrões federais de processamento de informações (FIPS)

O ONTAP é compatível com os padrões federais de processamento de informações (FIPS) 140-2 para todas as conexões SSL. Você pode ativar e desativar o modo SSL FIPS, definir protocolos SSL globalmente e desativar quaisquer cifras fracas, como RC4 dentro do ONTAP.

Por padrão, o SSL no ONTAP é definido com conformidade FIPS desativada e o protocolo SSL habilitado com o seguinte:

- TLSv1,3 (começando em ONTAP 9.11,1)
- TLSv1.2
- TLSv1.1
- TLSv1

Quando o modo SSL FIPS está ativado, a comunicação SSL do ONTAP para clientes externos ou componentes de servidor fora do ONTAP usará criptografia compatível com FIPS para SSL.

Se você quiser que as contas de administrador acessem SVMs com uma chave pública SSH, certifique-se de que o algoritmo da chave do host seja suportado antes de ativar o modo SSL FIPS.

Nota: o suporte ao algoritmo da chave do host foi alterado no ONTAP 9.11,1 e versões posteriores.

Lançamento do ONTAP	Tipos de chave suportados	Tipos de chave não suportados
9.11.1 e mais tarde	ecdsa-sha2-nistp256	rsa-sha2-512 mais rsa-sha2-256 mais ssh-ed25519 mais ssh-dss e ssh-rsa
9.10.1 e anteriores	ecdsa-sha2-nistp256 e ssh-ed25519	ssh-dss e ssh-rsa

Contas de chave pública SSH existentes sem os algoritmos de chave suportados devem ser reconfiguradas com um tipo de chave suportado antes de ativar o FIPS, ou a autenticação do administrador falhará.

Para obter mais informações, "Ativar contas de chave pública SSH"consulte .

Para obter mais informações sobre a configuração do modo SSL FIPS, consulte a `security config modify` página de manual.

Ativar FIPS

É recomendável que todos os usuários seguros ajustem sua configuração de segurança imediatamente após a instalação ou atualização do sistema. Quando o modo SSL FIPS está ativado, a comunicação SSL do ONTAP para clientes externos ou componentes de servidor fora do ONTAP usará criptografia compatível com FIPS para SSL.

Quando o FIPS está ativado, não é possível instalar ou criar um certificado com um comprimento de chave RSA de 4096.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Ativar FIPS:

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

3. Quando solicitado a continuar, digite `y`
4. Se você estiver executando o ONTAP 9.8 ou anterior reinicialize manualmente cada nó no cluster um por um. A partir do ONTAP 9.9,1, a reinicialização não é necessária.

Exemplo

Se estiver a executar o ONTAP 9.9,1 ou posterior, não verá a mensagem de aviso.

```
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
```

Desativar FIPS

Se você ainda estiver executando uma configuração de sistema mais antiga e quiser configurar o ONTAP com compatibilidade com versões anteriores, você poderá ativar o SSLv3 somente quando o FIPS estiver desativado.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Desative o FIPS digitando:

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

3. Quando solicitado a continuar, digite `y`.
4. Se você estiver executando o ONTAP 9.8 ou anterior, reinicie manualmente cada nó no cluster. A partir do ONTAP 9.9,1, a reinicialização não é necessária.

Exemplo

Se estiver a executar o ONTAP 9.9,1 ou posterior, não verá a mensagem de aviso.

```
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
```

Visualizar o status de conformidade FIPS

Você pode ver se todo o cluster está executando as configurações de segurança atuais.

Passos

1. Um por um, reinicie cada nó no cluster.

   Não reinicie todos os nós de cluster simultaneamente. É necessário reinicializar para garantir que todos os aplicativos do cluster estejam executando a nova configuração de segurança e todas as alterações no modo de ativação/desativação FIPS, protocolos e cifras.

2. Exibir o status de conformidade atual:

   ```
   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 a criptografia IPsec em trânsito

Prepare-se para usar a segurança IP

A partir do ONTAP 9.8, você tem a opção de usar a segurança IP (IPsec) para proteger o tráfego de rede. IPsec é uma das várias opções de criptografia de dados em movimento ou em trânsito disponíveis com o ONTAP. Você deve se preparar para configurar o IPsec antes de usá-lo em um ambiente de produção.

Implementação de segurança IP no ONTAP

IPsec é um padrão de Internet mantido pelo IETF. Ele fornece criptografia e integridade de dados, bem como autenticação para o tráfego que flui entre os endpoints da rede em um nível IP.

Com o ONTAP, o IPsec protege todo o tráfego IP entre o ONTAP e os vários clientes, incluindo os protocolos NFS, SMB e iSCSI. Além da privacidade e integridade dos dados, o tráfego de rede é protegido contra vários ataques, como repetição e ataques man-in-the-middle. O ONTAP usa a implementação do modo de transporte IPsec. Ele aproveita o protocolo IKE (Internet Key Exchange) versão 2 para negociar o material chave entre o ONTAP e os clientes usando IPv4 ou IPv6.

Quando o recurso IPsec está ativado em um cluster, a rede requer uma ou mais entradas no banco de dados de diretiva de segurança (SPD) do ONTAP que correspondam às várias caraterísticas de tráfego. Essas entradas mapeiam para os detalhes de proteção específicos necessários para processar e enviar os dados (como, por exemplo, conjunto de codificações e método de autenticação). Uma entrada SPD correspondente também é necessária em cada cliente.

Para certos tipos de tráfego, outra opção de criptografia de dados em movimento pode ser preferível. Por exemplo, para a criptografia do tráfego de peering de cluster e NetApp SnapMirror, o protocolo TLS (Transport Layer Security) geralmente é recomendado em vez de IPsec. Isso ocorre porque o TLS oferece melhor desempenho na maioria das situações.

Informações relacionadas

- "Internet Engineering Task Force"
- "RFC 4301: Arquitetura de segurança para o Protocolo de Internet"

Evolução da implementação IPsec do ONTAP

O IPsec foi introduzido pela primeira vez com o ONTAP 9.8. A implementação continuou a evoluir e melhorar, conforme descrito abaixo.

> Quando um recurso é introduzido a partir de uma versão específica do ONTAP, ele também é suportado em versões subsequentes, a menos que indicado de outra forma.

ONTAP 9.16,1

Várias operações criptográficas, como verificações de criptografia e integridade, podem ser descarregadas para uma placa NIC suportada. Consulte Recurso de descarga de hardware IPsec para obter mais informações.

ONTAP 9.12,1

O suporte ao protocolo de host front-end IPsec está disponível nas configurações de conexão de malha MetroCluster IP e MetroCluster. O suporte IPsec fornecido com clusters MetroCluster é limitado ao tráfego de host front-end e não é compatível com LIFs MetroCluster entre clusters.

ONTAP 9.10,1

Os certificados podem ser usados para autenticação IPsec, além das chaves pré-compartilhadas (PSKs). Antes do ONTAP 9.10,1, apenas PSKs são suportados para autenticação.

ONTAP 9.9,1

Os algoritmos de criptografia usados pelo IPsec são validados pelo FIPS 140-2. Esses algoritmos são processados pelo módulo criptográfico NetApp no ONTAP, que carrega a validação FIPS 140-2.

ONTAP 9,8

O suporte para IPsec torna-se inicialmente disponível com base na implementação do modo de transporte.

Recurso de descarga de hardware IPsec

Se você estiver usando o ONTAP 9.16,1 ou posterior, terá a opção de descarregar determinadas operações computacionalmente intensivas, como verificações de criptografia e integridade, para uma placa de controlador de interface de rede (NIC) instalada no nó de armazenamento. O uso dessa opção de descarga de hardware pode melhorar significativamente o desempenho e a taxa de transferência do tráfego de rede protegido por IPsec.

Requisitos e recomendações

Há vários requisitos que você deve considerar antes de usar o recurso de descarga de hardware IPsec.

Placas Ethernet suportadas

Você precisa instalar e usar apenas placas Ethernet compatíveis nos nós de storage. As seguintes placas Ethernet são suportadas com o ONTAP 9.16,1:

- X50131A (controlador Ethernet 2P, 40G/100g/200g/400G)
- X60132A (controlador Ethernet 4P, 10G/25G)

Escopo do cluster

O recurso de descarga de hardware IPsec é configurado globalmente para o cluster. E assim, por exemplo, o comando `security ipsec config` se aplica a todos os nós no cluster.

Configuração consistente

As placas NIC suportadas devem ser instaladas em todos os nós do cluster. Se uma placa NIC suportada estiver disponível apenas em alguns dos nós, você poderá ver uma degradação significativa do desempenho após um failover se algumas LIFs não estiverem hospedadas em uma NIC compatível com descarga.

Desativar a anti-repetição

Você deve desativar a proteção anti-replay IPsec no ONTAP (configuração padrão) e nos clientes IPsec. Se não estiver desativado, a fragmentação e o multi-path (rota redundante) não serão suportados.

Limitações

Há várias limitações que você deve considerar antes de usar o recurso de descarga de hardware IPsec.

IPv6

A versão 6 do IP não é suportada para o recurso de descarga de hardware IPsec. O IPv6 só é suportado com a implementação do software IPsec.

Números de sequência alargados

Os números de sequência estendida IPsec não são suportados com o recurso de descarga de hardware. Apenas são utilizados os números normais de sequência de 32 bits.

Agregação de links

O recurso de descarga de hardware IPsec não suporta agregação de links. E assim não pode ser usado com uma interface ou grupo de agregação de links conforme administrado através dos `network port ifgrp` comandos na CLI do ONTAP.

Suporte à configuração na CLI do ONTAP

Três comandos CLI existentes são atualizados no ONTAP 9.16,1 para suportar o recurso de descarga de hardware IPsec, conforme descrito abaixo. Consulte também "Configure a segurança IP no ONTAP"para obter mais informações.

Comando ONTAP	Atualização
`security ipsec config show`	O parâmetro booleano `Offload Enabled` mostra o status atual de descarga da NIC.
`security ipsec config modify`	O parâmetro `is-offload-enabled` pode ser usado para ativar ou desativar o recurso de descarga de NIC.
`security ipsec config show-ipsecsa`	Quatro novos contadores foram adicionados para exibir o tráfego de entrada, bem como de saída em bytes e pacotes.

Suporte à configuração na API REST do ONTAP

Dois endpoints de API REST existentes são atualizados no ONTAP 9.16,1 para oferecer suporte ao recurso de descarga de hardware IPsec, conforme descrito abaixo.

Endpoint da REST	Atualização
`/api/security/ipsec`	O parâmetro `offload_enabled` foi adicionado e está disponível com o método DE PATCH.

Endpoint da REST	Atualização
`/api/security/ipsec/security_association`	Dois novos valores de contador foram adicionados para rastrear o total de bytes e pacotes processados pelo recurso de descarga.

Saiba mais sobre a API REST do ONTAP, incluindo "Novidades com a API REST do ONTAP", na documentação de automação do ONTAP. Você também deve consultar a documentação de automação do ONTAP para obter detalhes sobre "Pontos de extremidade IPsec"o .

Configure a segurança IP no ONTAP

Há várias tarefas que você precisa executar para configurar e ativar a criptografia IPsec em trânsito no cluster do ONTAP.

Certifique-se de revisar "Prepare-se para usar a segurança IP" antes de configurar o IPsec. Por exemplo, talvez seja necessário decidir se deve usar o recurso de descarga de hardware IPsec disponível a partir do ONTAP 9.16,1.

Ative o IPsec no cluster

Você pode habilitar o IPsec no cluster para garantir que os dados estejam criptografados continuamente e seguros enquanto estiverem em trânsito.

Passos

1. Descubra se o IPsec já está habilitado:

   ```
   security ipsec config show
   ```

   Se o resultado incluir `IPsec Enabled: false`, avance para o passo seguinte.

2. Ativar IPsec:

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

   Você pode ativar o recurso de descarga de hardware IPsec usando o parâmetro booleano `is-offload-enabled` .

3. Execute o comando Discovery novamente:

   ```
   security ipsec config show
   ```

   O resultado agora `IPsec Enabled: true`inclui .

Prepare-se para a criação de diretiva IPsec com autenticação de certificado

Você pode ignorar esta etapa se estiver usando apenas chaves pré-compartilhadas (PSKs) para autenticação e não usar autenticação de certificado.

Antes de criar uma diretiva IPsec que usa certificados para autenticação, você deve verificar se os seguintes pré-requisitos são atendidos:

- Tanto o ONTAP quanto o cliente devem ter o certificado CA da outra parte instalado para que os certificados da entidade final (ONTAP ou cliente) sejam verificáveis por ambos os lados
- Um certificado é instalado para o ONTAP LIF que participa da política

> ONTAP LIFs podem compartilhar certificados. Não é necessário um mapeamento individual entre certificados e LIFs.

Passos

1. Instale todos os certificados de CA usados durante a autenticação mútua, incluindo CAs do lado do ONTAP e do lado do cliente, no gerenciamento de certificados do ONTAP, a menos que ele já esteja instalado (como é o caso de uma CA raiz autoassinada do ONTAP).
   - Exemplo de comando*
     `cluster::> security certificate install -vserver svm_name -type server-ca -cert-name my_ca_cert`
2. Para garantir que a CA instalada esteja dentro do caminho de pesquisa da CA IPsec durante a autenticação, adicione as CAs de gerenciamento de certificados ONTAP ao módulo IPsec usando o `security ipsec ca-certificate add` comando.
   - Exemplo de comando*
     `cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs my_ca_cert`
3. Crie e instale um certificado para uso pelo ONTAP LIF. A CA do emissor deste certificado já deve ser instalada no ONTAP e adicionada ao IPsec.
   - Exemplo de comando*
     `cluster::> security certificate install -vserver svm_name -type server -cert -name my_nfs_server_cert`

Para obter mais informações sobre certificados no ONTAP, consulte os comandos do certificado de segurança na documentação do ONTAP 9.

Definir o banco de dados de políticas de segurança (SPD)

O IPsec requer uma entrada SPD antes de permitir que o tráfego flua na rede. Isso é verdade se você estiver usando um PSK ou um certificado para autenticação.

Passos

1. Use o `security ipsec policy create` comando para:
   a. Selecione o endereço IP do ONTAP ou a sub-rede de endereços IP para participar do transporte IPsec.
   b. Selecione os endereços IP do cliente que se conetarão aos endereços IP do ONTAP.

      > O cliente deve suportar o Internet Key Exchange versão 2 (IKEv2) com uma chave pré-compartilhada (PSK).

   c. Opcional. Selecione os parâmetros de tráfego detalhados, como os protocolos da camada superior (UDP, TCP, ICMP, etc.), os números de porta local e os números de porta remota para proteger o tráfego. Os parâmetros correspondentes são `protocols`, `local-ports` e `remote-ports` respetivamente.

Ignore esta etapa para proteger todo o tráfego entre o endereço IP do ONTAP e o endereço IP do cliente. Proteger todo o tráfego é o padrão.

d. Insira PSK ou infra-estrutura de chave pública (PKI) para `auth-method` o parâmetro para o método de autenticação desejado.

   i. Se você inserir um PSK, inclua os parâmetros e pressione <enter> para que o prompt digite e verifique a chave pré-compartilhada.

   > Os `local-identity` parâmetros e `remote-identity` são opcionais se o host e o cliente usarem strongSwan e nenhuma política de curinga for selecionada para o host ou cliente.

   ii. Se introduzir uma PKI, terá de introduzir também os `cert-name` `local-identity` parâmetros , . `remote-identity` Se a identidade do certificado do lado remoto for desconhecida ou se forem esperadas várias identidades de cliente, insira a identidade `ANYTHING`especial .

```
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
```

O tráfego IP não pode fluir entre o cliente e o servidor até que o ONTAP e o cliente tenham configurado as diretivas IPsec correspondentes e as credenciais de autenticação (PSK ou certificado) estejam no lugar em ambos os lados.

Use identidades IPsec

Para o método de autenticação de chave pré-compartilhada, identidades locais e remotas são opcionais se o host e o cliente usarem strongSwan e nenhuma política de curinga for selecionada para o host ou cliente.

Para o método de autenticação PKI/certificado, as identidades locais e remotas são obrigatórias. As identidades especificam qual identidade é certificada no certificado de cada lado e são usadas no processo de verificação. Se a identidade remota for desconhecida ou se puder ser muitas identidades diferentes, use a identidade `ANYTHING`especial .

Sobre esta tarefa

Dentro do ONTAP, as identidades são especificadas modificando a entrada SPD ou durante a criação da política SPD. O SPD pode ser um endereço IP ou um nome de identidade de formato de cadeia de carateres.

Passos

1. Use o seguinte comando para modificar uma configuração de identidade SPD existente:

```
security ipsec policy modify
```

Exemplo de comando

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

Configuração de vários clientes IPsec

Quando um pequeno número de clientes precisa aproveitar o IPsec, usar uma única entrada SPD para cada cliente é suficiente. No entanto, quando centenas ou mesmo milhares de clientes precisam utilizar o IPsec, o NetApp recomenda o uso de uma configuração de vários clientes IPsec.

Sobre esta tarefa

O ONTAP é compatível com a conexão de vários clientes em várias redes a um único endereço IP SVM com IPsec ativado. Você pode fazer isso usando um dos seguintes métodos:

- **Configuração de sub-rede**

  Para permitir que todos os clientes em uma sub-rede específica (por exemplo, 192.168.134.0/24) se conetem a um único endereço IP SVM usando uma única entrada de política SPD, você deve especificar o `remote-ip-subnets` formulário de sub-rede in. Além disso, você deve especificar o `remote-identity` campo com a identidade do lado do cliente correta.

  > Ao usar uma única entrada de diretiva em uma configuração de sub-rede, os clientes IPsec nessa sub-rede compartilham a identidade IPsec e a chave pré-compartilhada (PSK). No entanto, isso não é verdade com a autenticação de certificado. Ao usar certificados, cada cliente pode usar seu próprio certificado exclusivo ou um certificado compartilhado para autenticar. O IPsec do ONTAP verifica a validade do certificado com base nas CAs instaladas em seu armazenamento de confiança local. O ONTAP também suporta verificação de lista de revogação de certificados (CRL).

- **Permitir a configuração de todos os clientes**

  Para permitir que qualquer cliente, independentemente do endereço IP de origem, se conete ao endereço IP habilitado para IPsec SVM, use o `0.0.0.0/0` caractere curinga ao especificar o `remote-ip-subnets` campo.

  Além disso, você deve especificar o `remote-identity` campo com a identidade do lado do cliente correta. Para autenticação de certificado, pode introduzir `ANYTHING`.

  Além disso, quando o `0.0.0.0/0` caractere curinga é usado, você deve configurar um número de porta local ou remota específico para usar. Por exemplo, `NFS port 2049`.

  Passos

  a. Use um dos comandos a seguir para configurar o IPsec para vários clientes.

     i. Se você estiver usando **configuração de sub-rede** para oferecer suporte a vários 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
     ```

  Exemplo de comando

  ```
  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. Se você estiver usando **permitir que a configuração de todos os clientes** ofereça suporte a vários 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
```

Exemplo de comando

```
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
```

Exibir estatísticas IPsec

Por meio da negociação, um canal de segurança chamado Associação de Segurança IKE (SA) pode ser estabelecido entre o endereço IP do ONTAP SVM e o endereço IP do cliente. As SAS IPsec são instaladas em ambos os endpoints para fazer o trabalho real de criptografia e descriptografia de dados. Você pode usar comandos de estatísticas para verificar o status de SAS IPsec e SAS IKE.

Se você estiver usando o recurso de descarga de hardware IPsec, vários novos contadores serão exibidos com o comando `security ipsec config show-ipsecsa`.

Comandos de exemplo

Comando de exemplo IKE SA:

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

Comando e saída de amostra IPsec SA:

```
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
```

Comando e saída de amostra IPsec SA:

```
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 LIFs

A configuração de um firewall aumenta a segurança do cluster e ajuda a impedir o acesso não autorizado ao sistema de armazenamento. Por padrão, o firewall integrado é configurado para permitir acesso remoto a um conjunto específico de serviços IP para dados, gerenciamento e LIFs entre clusters.

Começando com ONTAP 9.10,1:

- As políticas de firewall são obsoletas e são substituídas por políticas de serviço LIF. Anteriormente, o firewall integrado era gerenciado usando políticas de firewall. Essa funcionalidade agora é realizada usando uma política de serviço LIF.
- Todas as políticas de firewall estão vazias e não abrem nenhuma porta no firewall subjacente. Em vez disso, todas as portas devem ser abertas usando uma política de serviço LIF.
- Nenhuma ação é necessária após uma atualização para 9.10.1 ou posterior para a transição de políticas de firewall para políticas de serviço LIF. O sistema constrói automaticamente políticas de serviço LIF consistentes com as políticas de firewall em uso na versão anterior do ONTAP. Se você usar scripts ou outras ferramentas que criam e gerenciam políticas de firewall personalizadas, talvez seja necessário atualizar esses scripts para criar políticas de serviço personalizadas.

Para saber mais, "LIFs e políticas de serviço no ONTAP 9.6 e posteriores"consulte .

As políticas de firewall podem ser usadas para controlar o acesso a protocolos de serviço de gerenciamento, como SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS ou SNMP. Não é possível definir políticas de firewall para protocolos de dados como NFS ou SMB.

Você pode gerenciar o serviço de firewall e as políticas das seguintes maneiras:

- Ativar ou desativar o serviço de firewall
- Exibindo a configuração atual do serviço de firewall
- Criar uma nova política de firewall com o nome da política e os serviços de rede especificados
- Aplicar uma política de firewall a uma interface lógica
- Criar uma nova política de firewall que seja uma cópia exata de uma política existente

  Use isso para criar uma política com características semelhantes no mesmo SVM ou para copiar a política

para um SVM diferente.

- Exibindo informações sobre políticas de firewall
- Modificar os endereços IP e as máscaras de rede que são usadas por uma política de firewall
- Eliminar uma política de firewall que não está a ser utilizada por um LIF

Políticas de firewall e LIFs

As políticas de firewall LIF são usadas para restringir o acesso ao cluster em cada LIF. Você precisa entender como a política de firewall padrão afeta o acesso do sistema sobre cada tipo de LIF e como você pode personalizar uma política de firewall para aumentar ou diminuir a segurança sobre um LIF.

Ao configurar um LIF usando o `network interface create` comando ou `network interface modify`, o valor especificado para o `-firewall-policy` parâmetro determina os protocolos de serviço e os endereços IP que têm acesso permitido ao LIF.

Em muitos casos, você pode aceitar o valor padrão da política de firewall. Em outros casos, talvez seja necessário restringir o acesso a determinados endereços IP e a determinados protocolos de serviço de gerenciamento. Os protocolos de serviço de gerenciamento disponíveis incluem SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS e SNMP.

A política de firewall para todas as LIFs de cluster é padrão `""` e não pode ser modificada.

A tabela a seguir descreve as políticas de firewall padrão que são atribuídas a cada LIF, dependendo de sua função (ONTAP 9.5 e anterior) ou diretiva de serviço (ONTAP 9.6 e posterior), quando você cria o LIF:

Política de firewall	Protocolos de serviço padrão	Acesso predefinido	LIFs aplicadas a
gestão	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Qualquer endereço (0,0.0,0/0)	Gerenciamento de clusters, gerenciamento de SVM e LIFs de gerenciamento de nós
gerenciamento nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Qualquer endereço (0,0.0,0/0)	LIFs de dados que também são compatíveis com o acesso de gerenciamento da SVM
entre clusters	https, ndmp, ndmps	Qualquer endereço (0,0.0,0/0)	Todos os LIFs entre clusters
dados	dns, ndmp, ndmps, portmap	Qualquer endereço (0,0.0,0/0)	Todos os dados LIFs

Configuração do serviço portmap

O serviço portmap mapeia os serviços RPC para as portas nas quais eles escutam.

O serviço portmap estava sempre acessível no ONTAP 9.3 e anterior, tornou-se configurável no ONTAP 9.4 através do ONTAP 9.6 e é gerenciado automaticamente a partir do ONTAP 9.7.

- No ONTAP 9.3 e anteriores, o serviço portmap (rpcbind) estava sempre acessível na porta 111 em configurações de rede que dependiam do firewall ONTAP integrado em vez de um firewall de terceiros.
- Do ONTAP 9.4 ao ONTAP 9.6, você pode modificar políticas de firewall para controlar se o serviço portmap está acessível em LIFs específicos.
- A partir do ONTAP 9.7, o serviço de firewall portmap é eliminado. Em vez disso, a porta portmap é aberta automaticamente para todos os LIFs que suportam o serviço NFS.

O serviço portmap é configurável no firewall no ONTAP 9.4 através do ONTAP 9.6.

O restante deste tópico discute como configurar o serviço de firewall do portmap para as versões do ONTAP 9.4 através do ONTAP 9.6.

Dependendo da sua configuração, você poderá desativar o acesso ao serviço em tipos específicos de LIFs, geralmente de gerenciamento e LIFs entre clusters. Em algumas circunstâncias, você pode até mesmo ser capaz de proibir o acesso em LIFs de dados.

Que comportamento você pode esperar

O comportamento do ONTAP 9.4 até o ONTAP 9.6 foi projetado para fornecer uma transição perfeita na atualização. Se o serviço portmap já estiver sendo acessado sobre tipos específicos de LIFs, ele continuará acessível sobre esses tipos de LIFs. Como no ONTAP 9.3 e anteriores, você pode especificar os serviços acessíveis no firewall na política de firewall para o tipo LIF.

Todos os nós no cluster devem estar executando o ONTAP 9.4 a ONTAP 9.6 para que o comportamento entre em vigor. Apenas o tráfego de entrada é afetado.

As novas regras são as seguintes:

- Ao atualizar para a versão 9,4 até 9,6, o ONTAP adiciona o serviço portmap a todas as políticas de firewall existentes, padrão ou personalizado.
- Quando você cria um novo cluster ou um novo espaço de IPspace, o ONTAP adiciona o serviço de portmap apenas à política de dados padrão, não ao gerenciamento padrão ou às políticas entre clusters.
- Você pode adicionar o serviço portmap a políticas padrão ou personalizadas conforme necessário e remover o serviço conforme necessário.

Como adicionar ou remover o serviço portmap

Para adicionar o serviço portmap a uma diretiva de firewall de cluster ou SVM (torná-lo acessível dentro do firewall), digite:

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

Para remover o serviço portmap de uma diretiva de firewall de cluster ou SVM (torná-lo inacessível no firewall), digite:

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

Você pode usar o comando Network Interface Modify para aplicar a política de firewall a um LIF existente. Para obter a sintaxe de comando completa, consulte "Referência do comando ONTAP" .

Crie uma política de firewall e atribua-a a um LIF

As políticas de firewall padrão são atribuídas a cada LIF quando você cria o LIF. Em muitos casos, as configurações padrão do firewall funcionam bem e você não precisa alterá-las. Se você quiser alterar os serviços de rede ou endereços IP que podem acessar um LIF, você pode criar uma política de firewall personalizada e atribuí-la ao LIF.

Sobre esta tarefa

- Não é possível criar uma política de firewall com o `policy` nome `data`, `intercluster`, `cluster`, ou `mgmt`.

  Esses valores são reservados para as políticas de firewall definidas pelo sistema.

- Não é possível definir ou modificar uma política de firewall para LIFs de cluster.

  A política de firewall para LIFs de cluster está definida como 0,0.0.0/0 para todos os tipos de serviços.

- Se você precisar remover um serviço de uma política, exclua a política de firewall existente e crie uma nova política.
- Se o IPv6 estiver ativado no cluster, você poderá criar políticas de firewall com endereços IPv6.

  Depois que o IPv6 estiver ativado, `data` `intercluster`, e `mgmt` as políticas de firewall incluem ::/0, o curinga IPv6, em sua lista de endereços aceitos.

- Ao usar o System Manager para configurar a funcionalidade de proteção de dados entre clusters, você deve garantir que os endereços IP LIF sejam incluídos na lista permitida e que o serviço HTTPS seja permitido tanto nas LIFs entre clusters quanto nas firewalls de propriedade da empresa.

  Por padrão, a `intercluster` política de firewall permite o acesso de todos os endereços IP (0,0.0,0/0, ou ::/0 para IPv6) e habilita os serviços HTTPS, NDMP e NDMPS. Se você modificar essa política padrão ou criar sua própria política de firewall para LIFs entre clusters, adicione cada endereço IP LIF entre clusters à lista permitida e ative o serviço HTTPS.

- A partir do ONTAP 9.6, os serviços de firewall HTTPS e SSH não são suportados.

  No ONTAP 9.6, os `management-https` serviços e `management-ssh` LIF estão disponíveis para acesso de gerenciamento HTTPS e SSH.

Passos

1. Crie uma política de firewall que estará disponível para os LIFs em um SVM específico:

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

   Você pode usar este comando várias vezes para adicionar mais de um serviço de rede e lista de endereços IP permitidos para cada serviço na política de firewall.

2. Verifique se a política foi adicionada corretamente usando o `system services firewall policy show` comando.
3. Aplique a política de firewall a um LIF:

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

4. Verifique se a política foi adicionada corretamente ao LIF usando o `network interface show -fields firewall-policy` comando.

Exemplo de criar uma política de firewall e atribuí-la a um LIF

O comando a seguir cria uma política de firewall chamada data_http que habilita o acesso de protocolos HTTP e HTTPS a partir de endereços IP na sub-rede 10,10, aplica essa política ao LIF chamado data1 na SVM VS1 e, em seguida, mostra todas as políticas de firewall no 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
```

Comandos para gerenciar o serviço e as políticas de firewall

Você pode usar os `system services firewall` comandos para gerenciar o serviço de firewall, os `system services firewall policy` comandos para gerenciar políticas de firewall e o `network interface modify` comando para gerenciar configurações de firewall para LIFs.

Se você quiser…	Use este comando…
Ativar ou desativar o serviço de firewall	`system services firewall modify`
Exibir a configuração atual do serviço de firewall	`system services firewall show`
Crie uma política de firewall ou adicione um serviço a uma política de firewall existente	`system services firewall policy create`
Aplique uma política de firewall a um LIF	`network interface modify -lif lifname -firewall-policy`
Modifique os endereços IP e as máscaras de rede associadas a uma política de firewall	`system services firewall policy modify`
Exibir informações sobre políticas de firewall	`system services firewall policy show`
Crie uma nova política de firewall que seja uma cópia exata de uma política existente	`system services firewall policy clone`
Exclua uma política de firewall que não seja usada por um LIF	`system services firewall policy delete`

Para obter mais informações, consulte as páginas de manual dos `system services firewall` comandos , `system services firewall policy` e `network interface modify`"A referência do comando ONTAP 9" em .

Informações sobre direitos autorais

Informações sobre marcas comerciais