Configurar a criptografia IPsec em trânsito

ONTAP 9

NetApp
January 17, 2025

Índice

Configurar a criptografia IPsec em trânsito 1
Prepare-se para usar a segurança IP 1
Configure a segurança IP no ONTAP 3

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.
`/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
```

Informações sobre direitos autorais

Informações sobre marcas comerciais