Configurar el cifrado en tiempo real de IPsec

ONTAP 9

NetApp
December 20, 2024

Tabla de contenidos

Configurar el cifrado en tiempo real de IPsec

Prepárese para usar la seguridad IP

A partir de ONTAP 9.8, tiene la opción de usar la seguridad IP (IPsec) para proteger el tráfico de red. IPSec es una de las diversas opciones de cifrado de datos en movimiento o en tránsito disponibles con ONTAP. Debe prepararse para configurar IPsec antes de utilizarlo en un entorno de producción.

Implementación de seguridad IP en ONTAP

IPSec es un estándar de Internet mantenido por el IETF. Proporciona cifrado e integridad de datos, así como autenticación para el tráfico que fluye entre los extremos de red a nivel de IP.

Con ONTAP, IPsec protege todo el tráfico IP entre ONTAP y los distintos clientes, incluidos los protocolos NFS, SMB e iSCSI. Además de la privacidad y la integridad de los datos, el tráfico de red está protegido contra varios ataques, como los ataques de repetición y de intermediario. ONTAP utiliza la implantación del modo de transporte IPsec. Aprovecha la versión 2 del protocolo de intercambio de claves de Internet (IKE) para negociar el material clave entre ONTAP y los clientes utilizando IPv4 o IPv6.

Cuando la funcionalidad IPsec está habilitada en un cluster, la red necesita una o más entradas en la base de datos de políticas de seguridad de ONTAP (SPD) que coincidan con las distintas características del tráfico. Estas entradas se asignan a los detalles de protección específicos necesarios para procesar y enviar los datos (por ejemplo, conjunto de cifrado y método de autenticación). También es necesario introducir el SPD correspondiente en cada cliente.

Para ciertos tipos de tráfico, es preferible otra opción de cifrado de datos en movimiento. Por ejemplo, para el cifrado del tráfico de interconexión de clústeres y NetApp SnapMirror, por lo general se recomienda el protocolo de seguridad de la capa de transporte (TLS) en lugar de IPsec. Esto se debe a que TLS ofrece un mejor rendimiento en la mayoría de las situaciones.

Información relacionada

- "Grupo de trabajo de ingeniería de Internet (IETF)"
- "RFC 4301: Arquitectura de seguridad para el protocolo de Internet"

Evolución de la implementación de ONTAP IPsec

IPSec se introdujo por primera vez con ONTAP 9.8. La implementación ha seguido evolucionando y mejorando como se describe a continuación.

> Cuando se introduce una función a partir de una versión de ONTAP específica, también se admite en versiones posteriores, a menos que se indique lo contrario.

ONTAP 9.16.1

Varias de las operaciones criptográficas, como el cifrado y las comprobaciones de integridad, se pueden descargar en una tarjeta NIC admitida. Consulte Función de descarga de hardware IPSec para obtener más información.

ONTAP 9.12.1

La compatibilidad con el protocolo de host de interfaz IPSec está disponible en configuraciones FAS

MetroCluster y MetroCluster IP. La compatibilidad de IPsec que se proporciona con los clústeres de MetroCluster se limita al tráfico del host de interfaz de usuario y no es compatible con las LIF de interconexión de clústeres de MetroCluster.

ONTAP 9.10.1

Los certificados se pueden utilizar para la autenticación IPsec, además de las claves precompartidas (PSKs). Antes de ONTAP 9.10,1, sólo se admiten los PSKs para la autenticación.

ONTAP 9.9.1

Los algoritmos de cifrado utilizados por IPsec son validados por FIPS 140-2. Estos algoritmos son procesados por el módulo criptográfico de NetApp en ONTAP, que lleva la validación FIPS 140-2.

ONTAP 9,8

La compatibilidad con IPsec está disponible inicialmente en función de la implementación del modo de transporte.

Función de descarga de hardware IPSec

Si utiliza ONTAP 9.16,1 o posterior, tiene la opción de descargar ciertas operaciones de uso intensivo computacional, como el cifrado y las comprobaciones de integridad, a una tarjeta de controladora de interfaz de red (NIC) instalada en el nodo de almacenamiento. El uso de esta opción de descarga de hardware puede mejorar significativamente el rendimiento y el rendimiento del tráfico de red protegido por IPsec.

Requisitos y recomendaciones

Hay varios requisitos que debe tener en cuenta antes de utilizar la función de descarga de hardware IPsec.

Tarjetas Ethernet compatibles

Debe instalar y utilizar solo tarjetas Ethernet compatibles en los nodos de almacenamiento. ONTAP 9.16,1 admite las siguientes tarjetas Ethernet:

- X50131A (controladora Ethernet 2P, 40G/100g/200g/400G CX7)
- X60243A (4p, 10G/25G Ethernet Controller CX7)

Ámbito del clúster

La función de descarga de hardware IPsec se configura globalmente para el cluster. Así que, por ejemplo, el comando `security ipsec config` se aplica a todos los nodos del clúster.

Configuración consistente

Las tarjetas NIC admitidas deben instalarse en todos los nodos del clúster. Si solo hay disponible una tarjeta NIC compatible en algunos de los nodos, puede ver una degradación del rendimiento significativa tras una conmutación al nodo de respaldo si algunas de las LIF no están alojadas en una NIC compatible con la descarga.

Desactive la reproducción anti-repetición

Debe desactivar la protección antireproducción IPsec en ONTAP (configuración predeterminada) y los clientes IPsec. Si no está desactivada, la fragmentación y la multiruta (ruta redundante) no serán compatibles.

Limitaciones

Hay varias limitaciones que debe considerar antes de usar la función de descarga de hardware IPsec.

IPv6

La versión IP 6 no es compatible con la función de descarga de hardware IPsec. IPv6 solo es compatible con la implementación del software IPsec.

Núm.s de secuencia ampliados

Los números de secuencia extendida IPsec no son compatibles con la función de descarga de hardware. Solo se utilizan los números de secuencia normales de 32 bits.

Agregación de enlaces

La función de descarga de hardware IPsec no admite la agregación de enlaces. Por lo tanto, no se puede usar con una interfaz o un grupo de agregación de enlaces como se administra a través de `network port ifgrp` los comandos de la CLI de ONTAP.

Compatibilidad con la configuración de la interfaz de línea de comandos de ONTAP

Tres comandos CLI existentes se actualizan en ONTAP 9.16,1 para admitir la función de descarga de hardware IPsec como se describe a continuación. Consulte también "Configure la seguridad IP en ONTAP"para obtener más información.

Comando ONTAP	Actualizar
`security ipsec config show`	El parámetro booleano `Offload Enabled` muestra el estado actual de descarga de NIC.
`security ipsec config modify`	El parámetro `is-offload-enabled` se puede utilizar para activar o desactivar la función de descarga de NIC.
`security ipsec config show-ipsecsa`	Se han agregado cuatro contadores nuevos para mostrar el tráfico entrante y saliente en bytes y paquetes.

Soporte de configuración en la API de REST DE ONTAP

Dos extremos de API REST existentes se actualizan en ONTAP 9.16,1 para admitir la función de descarga de hardware IPsec como se describe a continuación.

Extremo de REST	Actualizar
`/api/security/ipsec`	El parámetro `offload_enabled` se ha agregado y está disponible con el método de PARCHE.
`/api/security/ipsec/security_association`	Se han agregado dos nuevos valores de contador para realizar un seguimiento del total de bytes y paquetes procesados por la función de descarga.

Obtenga más información sobre la API de REST DE ONTAP, incluida "Novedades de la API de REST DE ONTAP", en la documentación de automatización de ONTAP. También debe revisar la documentación de automatización de ONTAP para obtener detalles sobre "Puntos finales IPSec".

Configure la seguridad IP en ONTAP

Hay varias tareas que debe realizar para configurar y activar el cifrado en tiempo real de IPsec en el clúster de ONTAP.

Asegúrese de revisar "Prepárese para usar la seguridad IP" antes de configurar IPsec. Por ejemplo, es posible que deba decidir si desea utilizar la función de descarga de hardware IPsec disponible a partir de ONTAP 9.16,1.

Habilite IPsec en el clúster

Puede habilitar IPsec en el clúster para garantizar que los datos se cifran continuamente y estén seguros 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
   ```

   Puede activar la función de descarga de hardware IPsec mediante el parámetro booleano `is-offload-enabled`.

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 acerca de los certificados en 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.

         Los `local-identity` parámetros y `remote-identity` 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.

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.

Pasos

1. Utilice el siguiente comando para modificar una configuración de identidad SPD existente:

```
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
```

Mostrar estadísticas de 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.

Si está utilizando la función de descarga de hardware IPsec, se muestran varios contadores nuevos con el comando `security ipsec config show-ipsecsa`.

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
```