Configure IP security (IPsec) over wire encryption

ONTAP System Manager

NetApp
December 14, 2020

Table of Contents

Configure IP security (IPsec) over wire encryption

To ensure data is continuously secure and encrypted, even while in transit, ONTAP uses the IPsec protocol in transport mode. IPsec offers data encryption for all IP traffic including the NFS, iSCSI, and SMB/CIFS protocols. IPsec provides the only encryption in flight option for iSCSI traffic.

While IPsec capability is enabled on the cluster, the network requires a Security Policy Database (SPD) entry and a preshared secret on the client before traffic can flow.

After IPsec is configured, network traffic between the client and ONTAP is protected with preventive measures to combat replay and man-in-the-middle (MITM) attacks.

For NetApp SnapMirror and cluster peering traffic encryption, cluster peering encryption (CPE) is still recommended over IPsec for secure in-transit over the wire. This is because CPE has better performance than IPsec. You do not require a license for IPsec and there are no import or export restrictions.

Enable IPsec on the cluster

You can enable Internet Protocol security (IPsec) on the cluster to ensure data is continuously secure and encrypted, even while in transit.

Steps

1. Discover if IPsec is enabled already:

   ```
   security ipsec config show
   ```

   If the result includes `IPsec Enabled: false`, proceed to the next step.

2. Enable IPsec:

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

3. Run the discovery command again:

   ```
   security ipsec config show
   ```

   The result now includes `IPsec Enabled: true`.

Define the security policy database (SPD)

IPsec requires an SPD entry before allowing traffic to flow on the network.

Step

1. Use the `security ipsec policy create` command to:
   a. Select the ONTAP IP address or subnet of IP addresses to participate in the IPsec transport.
   b. Select the client IP addresses that will connect to the ONTAP IP addresses.

The client must support Internet Key Exchange version 2 (IKEv2) with a pre-shared key (PSK).

c. Optional. Select the upper layer protocols (UDP, TCP, ICMP, etc.), the local port numbers, and the remote port numbers to protect. The corresponding parameters are `protocols`, `local-ports` and `remote-ports` respectively.

   Skip this step to protect all traffic between the ONTAP IP address and client IP address. Protecting all traffic is the default.

d. Enter the pre-shared key to use between the client and ONTAP.

Sample command

```
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_:
```

IP traffic cannot flow between the client and server until the client pre-shared key is set on the IPsec client.

Use IPsec identities

Some IPsec clients, such as Libreswan, require the use of identities in addition to pre-shared keys to authenticate the IPsec connection.

About this task

Within ONTAP, identities are specified by modifying the SPD entry or during SPD policy creation. The SPD can be an IP address or string format identity name.

Step

To add an identity to an existing SPD, use the following command:

`security ipsec policy modify`

Sample command

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

IPsec multiple client configuration

When a small number of clients need to leverage IPsec, using a single SPD entry for each client is sufficient. However, when hundreds or even thousands of clients need to leverage IPsec, NetApp recommends using an IPsec multiple client configuration.

About this task

ONTAP supports connecting multiple clients across many networks to a single SVM IP address with IPsec

enabled. You can accomplish this using one of the following methods:

- **Subnet configuration**

  To allow all clients on a particular subnet (192.168.134.0/24 for example) to connect to a single SVM IP address using a single SPD policy entry, you must specify the `remote-ip-subnets` in subnet form. Additionally, you must specify the `remote-identity` field with the correct client side identity.

  

  When using a single policy entry in a subnet configuration, IPsec clients in that subnet share the IPsec identity and pre-shared key (PSK).

- **Allow all clients configuration**

  To allow any client, regardless of their source IP address, to connect to the SVM IPsec-enabled IP address, use the `0.0.0.0/0` wild card when specifying the `remote-ip-subnets` field.

  Additionally, you must specify the `remote-identity` field with the correct client side identity.

  Also, when the `0.0.0.0/0` wild card is used, you must configure a specific local or remote port number to use. For example, `NFS port 2049`.

  Step

  1. Use one of the following commands to configure IPsec for multiple clients:
     a. If you are using a **subnet configuration** to support multiple IPsec clients:

     ```
     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
     ```

     Sample command

     ```
     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
     ```

     b. If you are using an **allow all clients configuration** to support multiple IPsec clients:

     ```
     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
     ```

     Sample command

     ```
     security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
     IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
     -identity ontap_side_identity -remote-identity client_side_identity
     ```

IPsec statistics

Through negotiation, a security channel called an IKE Security Association (SA) can be established between the ONTAP SVM IP address and the client IP address. IPsec SAs are installed on both endpoints to do the

actual data encryption and decryption work.

You can use statistics commands to check the status of both IPsec SAs and IKE SAs.

Sample commands:

IKE SA sample command:

```
security ipsec show-ikesasa -node hosting_node_name_for_svm_ip
```

IPsec SA sample command:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```