Configure IPsec in-flight encryption

ONTAP 9

NetApp
December 21, 2024

Table of Contents

Configure IPsec in-flight encryption

Prepare to use IP security

Beginning with ONTAP 9.8, you have the option to use IP security (IPsec) to protect your network traffic. IPsec is one of several data-in-motion or in-flight encryption options available with ONTAP. You should prepare to configure IPsec before using it in a production environment.

IP security implementation in ONTAP

IPsec is an internet standard maintained by the IETF. It provides data encryption and integrity as well as authentication for the traffic flowing among the network endpoints at an IP level.

With ONTAP, IPsec secures all the IP traffic between ONTAP and the various clients, including the NFS, SMB, and iSCSI protocols. In addition to privacy and data integrity, the network traffic is protected against several attacks such as the replay and man-in-the-middle attacks. ONTAP uses the IPsec transport mode implementation. It leverages the Internet Key Exchange (IKE) protocol version 2 for negotiating the key material between ONTAP and the clients using either IPv4 or IPv6.

When the IPsec capability is enabled on a cluster, the network requires one or more entries in the ONTAP Security Policy Database (SPD) matching the various traffic characteristics. These entries map to the specific protection details needed to process and send the data (such as, cipher suite and authentication method). A corresponding SPD entry is also needed at each client.

For certain types of traffic, another data-in-motion encryption option might be preferable. For example, for the encryption of NetApp SnapMirror and cluster peering traffic, the transport layer security (TLS) protocol is generally recommended instead of IPsec. This is because TLS offers better performance in most situations.

Related information

- Internet Engineering Task Force
- RFC 4301: Security Architecture for the Internet Protocol

Evolution of the ONTAP IPsec implementation

IPsec was first introduced with ONTAP 9.8. The implementation has continued to evolve and improve as described below.

> When a feature is introduced beginning with a specific ONTAP release, it is also supported in subsequent releases unless otherwise noted.

ONTAP 9.16.1

Several of the cryptographic operations, such as encryption and integrity checks, can be offloaded to a supported NIC card. See IPsec hardware offload feature for more information.

ONTAP 9.12.1

IPsec front-end host protocol support is available in MetroCluster IP and MetroCluster fabric-attached configurations. The IPsec support provided with MetroCluster clusters is limited to front-end host traffic and is not supported on MetroCluster intercluster LIFs.

ONTAP 9.10.1

Certificates can be used for IPsec authentication in addition to the pre-shared keys (PSKs). Prior to ONTAP 9.10.1, only PSKs are supported for authentication.

ONTAP 9.9.1

The encryption algorithms used by IPsec are FIPS 140-2 validated. These algorithms are processed by the NetApp Cryptographic Module in ONTAP which carries the FIPS 140-2 validation.

ONTAP 9.8

Support for IPsec becomes initially available based on the transport mode implementation.

IPsec hardware offload feature

If you are using ONTAP 9.16.1 or later, you have the option of offloading certain computationally intensive operations, such as encryption and integrity checks, to a network interface controller (NIC) card installed at the storage node. Using this hardware offload option can significantly improve the performance and throughput of the network traffic protected by IPsec.

Requirements and recommendations

There are several requirements you should consider before using the IPsec hardware offload feature.

Supported Ethernet cards

You need to install and use only supported Ethernet cards on the storage nodes. The following Ethernet cards are supported with ONTAP 9.16.1:

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

Cluster scope

The IPsec hardware offload feature is configured globally for the cluster. And so, for example, the command `security ipsec config` applies to all the nodes in the cluster.

Consistent configuration

Supported NIC cards should be installed at all the nodes in the cluster. If a supported NIC card is only available on some of the nodes, you can see a significant performance degradation after a failover if some of the LIFs are not hosted on an offload capable NIC.

Disable anti-replay

You should disable IPsec anti-replay protection at ONTAP (default configuration) and the IPsec clients. If not disabled, fragmentation and multi-path (redundant route) will not be supported.

Limitations

There are several limitations you should consider before using the IPsec hardware offload feature.

IPv6

IP version 6 is not supported for the IPsec hardware offload feature. IPv6 is only supported with the IPsec software implementation.

Extended sequence numbers

The IPsec extended sequence numbers are not supported with the hardware offload feature. Only the normal

32-bit sequence numbers are used.

Link aggregation

The IPsec hardware offload feature does not support link aggregation. And so it cannot be used with an interface or link aggregation group as administered through the `network port ifgrp` commands at the ONTAP CLI.

Configuration support in the ONTAP CLI

Three existing CLI commands are updated in ONTAP 9.16.1 to support the IPsec hardware offload feature as described below. Also see Configure IP security in ONTAP for more information.

ONTAP command	Update
`security ipsec config show`	The boolean parameter `Offload Enabled` shows the current NIC offload status.
`security ipsec config modify`	The parameter `is-offload-enabled` can be used to enable or disable NIC offload feature.
`security ipsec config show-ipsecsa`	Four new counters have been added to display the inbound as well as outbound traffic in bytes and packets.

Configuration support in the ONTAP REST API

Two existing REST API endpoints are updated in ONTAP 9.16.1 to support the IPsec hardware offload feature as described below.

REST endpoint	Update
`/api/security/ipsec`	The parameter `offload_enabled` has been added and is available with the PATCH method.
`/api/security/ipsec/security_association`	Two new counter values have been added to track the total bytes and packets processed by the offload feature.

Learn more about the ONTAP REST API, including what's new with the ONTAP REST API, from the ONTAP automation documentation. You should also review the ONTAP automation documentation for details about IPsec endpoints.

Configure IP security in ONTAP

There are several tasks you need to perform to configure and activate IPsec in-flight encryption on your ONTAP cluster.

> Make sure to review Prepare to use IP security before configuring IPsec. For example, you might need to decide whether to use the IPsec hardware offload feature available beginning with ONTAP 9.16.1.

Enable IPsec on the cluster

You can enable IPsec on the cluster to ensure data is continuously encrypted and secure 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`

   You can enable the IPsec hardware offload feature using the boolean parameter `is-offload-enabled`.

3. Run the discovery command again:

   `security ipsec config show`

   The result now includes `IPsec Enabled: true`.

Prepare for IPsec policy creation with certificate authentication

You can skip this step if you are only using pre-shared keys (PSKs) for authentication and will not use certificate authentication.

Before creating an IPsec policy that uses certificates for authentication, you must verify that the following pre-requisites are met:

- Both ONTAP and the client must have the other party's CA certificate installed so that the end entity (either ONTAP or the client) certificates are verifiable by both sides
- A certificate is installed for the ONTAP LIF that participates in the policy

ONTAP LIFs can share certificates. A one-to-one mapping between certificates and LIFs is not required.

Steps

1. Install all CA certificates used during the mutual authentication, including both ONTAP-side and client-side CAs, to ONTAP certificate management unless it is already installed (as is the case of an ONTAP self-signed root-CA).

   Sample command
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. To make sure that the CA installed is within the IPsec CA searching path during authentication, add the ONTAP certificate management CAs to the IPsec module using the `security ipsec ca-certificate add` command.

   Sample command
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. Create and install a certificate for use by the ONTAP LIF. The issuer CA of this certificate must already be installed to ONTAP and added to IPsec.

   Sample command

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

For more information about certificates in ONTAP, see the security certificate commands in the ONTAP 9 documentation.

Define the security policy database (SPD)

IPsec requires an SPD entry before allowing traffic to flow on the network. This is true whether you are using a PSK or a certificate for authentication.

Steps

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 fine-grained traffic parameters, such as the upper layer protocols (UDP, TCP, ICMP, etc.), the local port numbers, and the remote port numbers to protect traffic. 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. Either enter PSK or public-key infrastructure (PKI) for the `auth-method` parameter for the desired authentication method.
      i. If you enter a PSK, include the parameters, then press <enter> for the prompt to enter and verify the pre-shared key.

         The `local-identity` and `remote-identity` parameters are optional if both host and client use strongSwan and no wildcard policy is selected for the host or client.

      ii. If you enter a PKI, you need to also enter the `cert-name`, `local-identity`, `remote-identity` parameters. If the remote-side certificate identity is unknown or if multiple client identities are expected, enter the special identity `ANYTHING`.

Sample command for PSK authentication

```
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_:
```

Sample command for PKI/certificate authentication

```
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
```

IP traffic cannot flow between the client and server until both ONTAP and the client have set up the matching IPsec policies, and authentication credentials (either PSK or certificate) are in place on both sides.

Use IPsec identities

For the pre-shared key authentication method, local and remote identities are optional if both host and client use strongSwan and no wildcard policy is selected for the host or client.

For the PKI/certificate authentication method, both local and remote identities are mandatory. The identities specify what identity is certified within each side's certificate and are used in the verification process. If the remote-identity is unknown or if it could be many different identities, use the special identity `ANYTHING`.

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.

Steps

1. Use the following command to modify an existing SPD identity setting:

```
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). However, this is not true with certificate authentication. When using certificates each client can use either their own unique certificate or a shared certificate to authenticate. ONTAP IPsec checks the validity of the certificate based on the CAs installed on its local trust store. ONTAP also supports certificate revocation list (CRL) checking.

- **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` wildcard when specifying the `remote-ip-subnets` field.

  Additionally, you must specify the `remote-identity` field with the correct client-side identity. For certificate authentication, you can enter `ANYTHING`.

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

  Steps

  1. Use one of the following commands to configure IPsec for multiple clients.

     a. If you are using **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 **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
     ```

Display 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.

If you are using the IPsec hardware offload feature, several new counters are displayed with the command `security ipsec config show-ipsecsa`.

Sample commands

IKE SA sample command:

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

IPsec SA sample command and output:

```
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
```

IPsec SA sample command and output:

```
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
```

Copyright information

Trademark information