Configurer le chiffrement IPsec en vol

ONTAP 9

NetApp
January 10, 2025

Sommaire

Configurer le chiffrement IPsec en vol

Préparez-vous à utiliser la sécurité IP

À partir de ONTAP 9.8, vous avez la possibilité d'utiliser la sécurité IP (IPSec) pour protéger votre trafic réseau. IPSec est l'une des nombreuses options de chiffrement de données en mouvement ou à la volée disponibles avec ONTAP. Vous devez vous préparer à configurer IPsec avant de l'utiliser dans un environnement de production.

Mise en œuvre de la sécurité IP dans ONTAP

IPSec est une norme Internet gérée par l'IETF. Il assure le cryptage et l'intégrité des données ainsi que l'authentification du trafic circulant entre les terminaux réseau au niveau IP.

Avec ONTAP, IPSec sécurise l'ensemble du trafic IP entre ONTAP et les différents clients, notamment les protocoles NFS, SMB et iSCSI. En plus de la confidentialité et de l'intégrité des données, le trafic réseau est protégé contre plusieurs attaques, telles que les attaques par réexécution et les attaques de l'homme du milieu. ONTAP utilise l'implémentation du mode de transport IPsec. Il s'appuie sur le protocole Internet Key Exchange (IKE) version 2 pour négocier le matériel clé entre ONTAP et les clients utilisant IPv4 ou IPv6.

Lorsque la fonctionnalité IPSec est activée sur un cluster, le réseau requiert une ou plusieurs entrées de la base de données SPD (Security Policy Database) de ONTAP correspondant aux différentes caractéristiques de trafic. Ces entrées sont mappées aux détails de protection spécifiques nécessaires au traitement et à l'envoi des données (par exemple, suite de chiffrement et méthode d'authentification). Une entrée SPD correspondante est également nécessaire pour chaque client.

Pour certains types de trafic, une autre option de chiffrement des données en mouvement peut être préférable. Par exemple, pour le chiffrement du trafic NetApp SnapMirror et de peering de cluster, le protocole TLS (transport Layer Security) est généralement recommandé à la place d'IPsec. En effet, TLS offre de meilleures performances dans la plupart des situations.

Informations associées

- "Internet Engineering Task Force"
- "RFC 4301 : Architecture de sécurité pour le protocole Internet"

Évolution de l'implémentation ONTAP IPsec

IPSec a été introduit pour la première fois avec ONTAP 9.8. La mise en œuvre a continué d'évoluer et de s'améliorer comme décrit ci-dessous.

> Sauf mention contraire, lorsqu'une fonctionnalité est introduite à partir d'une version spécifique de ONTAP, elle est également prise en charge dans les versions ultérieures.

ONTAP 9.16.1

Plusieurs opérations cryptographiques, telles que le cryptage et les contrôles d'intégrité, peuvent être déchargées sur une carte NIC prise en charge. Voir Fonctionnalité de déchargement matériel IPsec pour plus d'informations.

ONTAP 9.12.1

La prise en charge du protocole hôte IPSec frontal est disponible dans les configurations MetroCluster IP et

MetroCluster FAS. La prise en charge IPsec fournie avec les clusters MetroCluster est limitée au trafic hôte frontal et n'est pas prise en charge sur les LIF intercluster MetroCluster.

ONTAP 9.10.1

Les certificats peuvent être utilisés pour l'authentification IPsec en plus des clés prépartagées (PSK). Avant ONTAP 9.10.1, seuls les PSK sont pris en charge pour l'authentification.

ONTAP 9.9.1

Les algorithmes de chiffrement utilisés par IPsec sont validés par la norme FIPS 140-2-2. Ces algorithmes sont traités par le module cryptographique NetApp de ONTAP, qui est certifié FIPS 140-2-2.

ONTAP 9.8

La prise en charge d'IPsec devient initialement disponible en fonction de l'implémentation du mode de transport.

Fonctionnalité de déchargement matériel IPsec

Si vous utilisez ONTAP 9.16.1 ou une version ultérieure, vous avez la possibilité de transférer certaines opérations à forte intensité de calcul, telles que le cryptage et les contrôles d'intégrité, vers une carte de contrôleur d'interface réseau (NIC) installée sur le nœud de stockage. L'utilisation de cette option de déchargement matériel peut améliorer considérablement les performances et le débit du trafic réseau protégé par IPsec.

Exigences et recommandations

Vous devez tenir compte de plusieurs exigences avant d'utiliser la fonction de déchargement matériel IPsec.

Cartes Ethernet prises en charge

Vous devez installer et utiliser uniquement les cartes Ethernet prises en charge sur les nœuds de stockage. Les cartes Ethernet suivantes sont prises en charge par ONTAP 9.16.1 :

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

Étendue du cluster

La fonction de déchargement matériel IPSec est configurée globalement pour le cluster. Et ainsi, par exemple, la commande `security ipsec config` s'applique à tous les nœuds du cluster.

Configuration cohérente

Les cartes NIC prises en charge doivent être installées sur tous les nœuds du cluster. Si une carte NIC prise en charge n'est disponible que sur certains nœuds, vous pouvez constater une dégradation importante des performances après un basculement si certaines LIF ne sont pas hébergées sur une carte réseau prenant en charge le déchargement.

Désactiver l'anti-relecture

Vous devez désactiver la protection anti-relecture IPSec sur ONTAP (configuration par défaut) et les clients IPsec. Si elle n'est pas désactivée, la fragmentation et le multi-chemin (route redondante) ne sont pas pris en charge.

Limites

Vous devez tenir compte de plusieurs limitations avant d'utiliser la fonction de déchargement matériel IPsec.

IPv6

La version IP 6 n'est pas prise en charge pour la fonction de déchargement matériel IPsec. IPv6 est uniquement pris en charge avec l'implémentation du logiciel IPsec.

Numéros de séquence étendus

Les numéros de séquence étendus IPsec ne sont pas pris en charge avec la fonction de déchargement matériel. Seuls les numéros de séquence 32 bits normaux sont utilisés.

Agrégation de liens

La fonction de déchargement matériel IPSec ne prend pas en charge l'agrégation de liens. Il ne peut donc pas être utilisé avec une interface ou un groupe d'agrégation de liens tel qu'administré par le biais des `network port ifgrp` commandes de l'interface de ligne de commandes de ONTAP.

Prise en charge de la configuration dans l'interface de ligne de commandes ONTAP

Trois commandes CLI existantes sont mises à jour dans ONTAP 9.16.1 pour prendre en charge la fonctionnalité de déchargement matériel IPSec comme décrit ci-dessous. Voir également "Configurer la sécurité IP dans ONTAP"pour plus d'informations.

Commande ONTAP	Mise à jour
`security ipsec config show`	Le paramètre booléen `Offload Enabled` indique l'état actuel du déchargement de la carte réseau.
`security ipsec config modify`	Le paramètre `is-offload-enabled` peut être utilisé pour activer ou désactiver la fonction de déchargement de carte réseau.
`security ipsec config show-ipsecsa`	Quatre nouveaux compteurs ont été ajoutés pour afficher le trafic entrant et sortant en octets et en paquets.

Prise en charge de la configuration dans l'API REST ONTAP

Deux terminaux d'API REST existants sont mis à jour dans ONTAP 9.16.1 pour prendre en charge la fonctionnalité de déchargement matériel IPSec, comme décrit ci-dessous.

Terminal REST	Mise à jour
`/api/security/ipsec`	Le paramètre `offload_enabled` a été ajouté et est disponible avec la méthode PATCH.
`/api/security/ipsec/security_association`	Deux nouvelles valeurs de compteur ont été ajoutées pour suivre le nombre total d'octets et de paquets traités par la fonction de déchargement.

Pour en savoir plus sur l'API REST ONTAP, y compris "Nouveautés de l'API REST ONTAP", consultez la documentation sur l'automatisation ONTAP. Vous devez également consulter la documentation sur l'automatisation ONTAP pour plus de détails sur "Noeuds finaux IPsec".

Configurer la sécurité IP dans ONTAP

Plusieurs tâches sont nécessaires pour configurer et activer le chiffrement à la volée IPsec sur votre cluster ONTAP.

Vérifiez "Préparez-vous à utiliser la sécurité IP" avant de configurer IPsec. Par exemple, vous devrez peut-être décider d'utiliser la fonction de déchargement matériel IPSec disponible à partir de ONTAP 9.16.1.

Activez IPsec sur le cluster

Vous pouvez activer IPsec sur le cluster pour vous assurer que les données sont chiffrées en continu et sécurisées pendant le transit.

Étapes

1. Découvrez si IPSec est déjà activé :

   ```
   security ipsec config show
   ```

   Si le résultat inclut `IPsec Enabled: false`, passez à l'étape suivante.

2. Activer IPsec :

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

   Vous pouvez activer la fonction de déchargement matériel IPsec à l'aide du paramètre booléen `is-offload-enabled`.

3. Exécutez à nouveau la commande de découverte :

   ```
   security ipsec config show
   ```

   Le résultat inclut maintenant `IPsec Enabled: true`.

Préparez la création de stratégies IPsec avec l'authentification par certificat

Vous pouvez ignorer cette étape si vous utilisez uniquement des clés prépartagées (PSK) pour l'authentification et que vous n'utilisez pas l'authentification par certificat.

Avant de créer une stratégie IPSec qui utilise des certificats pour l'authentification, vous devez vérifier que les conditions préalables suivantes sont remplies :

- ONTAP et le client doivent avoir installé le certificat CA de l'autre partie afin que les certificats de l'entité finale (ONTAP ou le client) soient vérifiables des deux côtés
- Un certificat est installé pour la LIF de ONTAP qui participe à la politique

Les LIF ONTAP peuvent partager des certificats. Un mappage un-à-un entre les certificats et les LIFs n'est pas nécessaire.

Étapes

1. Installez tous les certificats de l'autorité de certification utilisés lors de l'authentification mutuelle, y compris les autorités de certification côté ONTAP et côté client, dans la gestion des certificats ONTAP, sauf s'il est déjà installé (comme c'est le cas pour une autorité de certification racine auto-signée ONTAP).

   Commande exemple

   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   ```

`-cert-name my_ca_cert`

2. Pour vous assurer que l'autorité de certification installée se trouve dans le chemin de recherche de l'autorité de certification IPSec lors de l'authentification, ajoutez les autorités de certification de gestion de certificat ONTAP au module IPSec à l'aide du `security ipsec ca-certificate add` commande.

   Commande exemple
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. Créez et installez un certificat pour une utilisation par le LIF ONTAP. L'autorité de certification de l'émetteur de ce certificat doit déjà être installée sur ONTAP et ajoutée à IPsec.

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

Pour plus d'informations sur les certificats dans ONTAP, consultez les commandes de certificat de sécurité dans la documentation de ONTAP 9.

Définir la base de données de règles de sécurité (SPD)

IPSec requiert une entrée SPD avant d'autoriser le trafic à circuler sur le réseau. Ceci est vrai si vous utilisez un PSK ou un certificat pour l'authentification.

Étapes

1. Utilisez le `security ipsec policy create` commande pour :
   a. Sélectionnez l'adresse IP ONTAP ou le sous-réseau d'adresses IP pour participer au transport IPsec.
   b. Sélectionnez les adresses IP des clients qui se connectent aux adresses IP ONTAP.

      Le client doit prendre en charge Internet Key Exchange version 2 (IKEv2) avec une clé pré-partagée (PSK).

   c. Facultatif. Sélectionnez les paramètres de trafic à granularité fine, tels que les protocoles de couche supérieure (UDP, TCP, ICMP, etc.)), les numéros de port local et les numéros de port distant pour protéger le trafic. Les paramètres correspondants sont `protocols`, `local-ports` et `remote-ports` respectivement.

      Ignorez cette étape pour protéger tout le trafic entre l'adresse IP ONTAP et l'adresse IP du client. La protection de tout le trafic est la valeur par défaut.

   d. Entrez PSK ou PKI (public-Key Infrastructure) pour le `auth-method` paramètre de la méthode d'authentification souhaitée.
      i. Si vous entrez une clé PSK, incluez les paramètres, puis appuyez sur <enter> pour que l'invite vous demande d'entrer et de vérifier la clé pré-partagée.

         Les `local-identity` paramètres et `remote-identity` sont facultatifs si l'hôte et le client utilisent StrongSwan et qu'aucune règle générique n'est sélectionnée pour l'hôte ou le client.

ii. Si vous entrez une PKI, vous devez également entrer `cert-name`, `local-identity`, `remote-identity` paramètres. Si l'identité du certificat côté distant est inconnue ou si plusieurs identités client sont attendues, entrez l'identité spéciale `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
```

Le trafic IP ne peut pas circuler entre le client et le serveur tant que ONTAP et le client n'ont pas configuré les stratégies IPSec correspondantes et que les informations d'identification d'authentification (PSK ou certificat) ne sont pas en place des deux côtés.

Utiliser les identités IPsec

Pour la méthode d'authentification par clé pré-partagée, les identités locales et distantes sont facultatives si l'hôte et le client utilisent StrongSwan et qu'aucune règle générique n'est sélectionnée pour l'hôte ou le client.

Pour la méthode d'authentification PKI/certificat, les identités locales et distantes sont obligatoires. Les identités spécifient quelle identité est certifiée dans le certificat de chaque côté et sont utilisées dans le processus de vérification. Si l'identité distante est inconnue ou si elle peut être de nombreuses identités différentes, utilisez l'identité spéciale `ANYTHING`.

Description de la tâche

Au sein de ONTAP, les identités sont spécifiées en modifiant l'entrée du démon du processeur de service ou pendant sa création. Le démon du processeur de service peut être un nom d'identité avec une adresse IP ou un format de chaîne.

Étapes

1. Utiliser la commande suivante pour modifier un paramètre d'identité SPD existant :

```
security ipsec policy modify
```

Commande exemple

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

Configuration client multiple IPsec

Lorsqu'un petit nombre de clients doivent utiliser IPsec, l'utilisation d'une seule entrée SPD pour chaque client est suffisante. Toutefois, lorsque des centaines voire des milliers de clients doivent utiliser IPsec, NetApp recommande l'utilisation d'une configuration client multiple IPsec.

Description de la tâche

ONTAP prend en charge la connexion de plusieurs clients sur de nombreux réseaux à une seule adresse IP de SVM avec IPsec activé. Vous pouvez effectuer cette opération en utilisant l'une des méthodes suivantes :

- **Configuration du sous-réseau**

  Pour permettre à tous les clients d'un sous-réseau particulier (192.168.134.0/24 par exemple) de se connecter à une seule adresse IP de SVM à l'aide d'une seule entrée de la politique SPD, vous devez spécifier le `remote-ip-subnets` sous-réseau. De plus, vous devez spécifier le `remote-identity` champ avec l'identité côté client correcte.

  > Lors de l'utilisation d'une seule entrée de stratégie dans une configuration de sous-réseau, les clients IPsec de ce sous-réseau partagent l'identité IPsec et la clé pré-partagée (PSK). Cependant, ceci n'est pas vrai avec l'authentification par certificat. Lors de l'utilisation de certificats, chaque client peut utiliser son propre certificat unique ou un certificat partagé pour s'authentifier. ONTAP IPSec vérifie la validité du certificat en fonction des autorités de certification installées dans son magasin de confiance local. ONTAP prend également en charge la vérification de la liste de révocation de certificats (CRL).

- **Autoriser la configuration de tous les clients**

  Pour permettre à n'importe quel client, quelle que soit son adresse IP source, de se connecter à l'adresse IP du SVM IPsec, utilisez l' `0.0.0.0/0` caractère générique lors de la spécification du `remote-ip-subnets` légale.

  De plus, vous devez spécifier le `remote-identity` champ avec l'identité côté client correcte. Pour l'authentification par certificat, vous pouvez entrer `ANYTHING`.

  Aussi, lorsque le `0.0.0.0/0` le caractère générique est utilisé. vous devez configurer un numéro de port local ou distant spécifique à utiliser. Par exemple : `NFS port 2049`.

  Étapes

  a. Utilisez l'une des commandes suivantes pour configurer IPsec pour plusieurs clients.

     i. Si vous utilisez **subnet configuration** pour prendre en charge plusieurs clients 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
     ```

     Commande exemple

     ```
     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 vous utilisez **Autoriser la configuration de tous les clients** à prendre en charge plusieurs clients 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
     ```

     Commande exemple

```
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
```

Afficher les statistiques IPsec

Lors de la négociation, un canal de sécurité appelé Association de sécurité IKE (sa) peut être établi entre l'adresse IP du SVM ONTAP et l'adresse IP du client. IPSec SAS est installé sur les deux noeuds finaux pour effectuer le cryptage et le décryptage des données. Vous pouvez utiliser les commandes de statistiques pour vérifier l'état des ports SAS IPsec et SAS IKE.

Si vous utilisez la fonction de déchargement matériel IPSec, plusieurs nouveaux compteurs sont affichés avec la commande `security ipsec config show-ipsecsa`.

Exemples de commandes

IKE sa exemple de commande :

`security ipsec show-ikesa -node hosting_node_name_for_svm_ip`

Exemple de commande et de sortie 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
```

Exemple de commande et de sortie 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
```

Informations sur le copyright

Informations sur les marques commerciales