配置IPsec传输中加密

ONTAP 9

NetApp
January 17, 2025

目录

配置IPsec传输中加密

准备使用IP安全性

从ONTAP 9 IPsec-8开始，您可以选择使用IP安全性(IPsec)来保护网络通信。IPSEC是ONTAP提供的多种移动数据或传输中数据加密选项之一。在生产环境中使用IPsec之前，应准备好配置它。

ONTAP中的IP安全实施

IPsec是IETF维护的一种Internet标准。它可以为IP级别网络端点之间的流量提供数据加密和完整性以及身份验证。

通过ONTAP、IPsec可保护ONTAP与各种客户端之间的所有IP流量、包括NFS、SMB和iSCSI协议。除了隐私和数据完整性之外、网络流量还可以抵御多种攻击、例如重放攻击和中间人攻击。ONTAP使用IPsec传输模式实现。它利用Internet密钥交换(IKE)协议版本2在ONTAP和使用IPv4或IPv6的客户端之间协商密钥材料。

如果在集群上启用了IPsec功能、则网络需要在ONTAP安全策略数据库(SPD)中有一个或多个与各种流量特征匹配的条目。这些条目映射到处理和发送数据所需的特定保护详细信息(例如密码套件和身份验证方法)。每个客户端还需要相应的SPD条目。

对于某些类型的流量、另一种移动数据加密选项可能更好。例如、对于NetApp SnapMirror和集群对等流量的加密、通常建议使用传输层安全(Transport Layer Security、TLS)协议、而不是IPsec。这是因为在大多数情况下、TLS的性能会更高。

相关信息

- "互联网工程任务小组"
- "RFC 4301：《Internet协议的安全架构》"

ONTAP IPsec实施的演变

IPsec. 8首次推出ONTAP 9。执行工作继续不断发展和改进，如下所述。

从特定ONTAP版本开始引入某项功能时、除非另有说明、否则后续版本也支持该功能。

ONTAP 9.16.1.

加密和完整性检查等多个加密操作可以卸载到受支持的NIC卡。有关详细信息、请参见 IPsec硬件卸载功能 。

ONTAP 9.12.1

MetroCluster IP和MetroCluster光纤连接配置支持IPSec前端主机协议。随MetroCluster集群提供的IPsec支持仅限于前端主机流量、MetroCluster集群间LIS不支持此功能。

ONTAP 9.10.1

除了预共享密钥(PSK)之外、证书还可用于IPsec身份验证。在PSM.10.1之前的版本中、仅支持ONTAP 9进行身份验证。

ONTAP 9.9.1

IPsec使用的加密算法已通过FIPS 140-2验证。这些算法由ONTAP中的NetApp加密模块处理、该模块执行FIPS

140-2验证。

ONTAP 9.8

根据传输模式的实现情况，最初可提供对IPsec的支持。

IPsec硬件卸载功能

如果您使用的是NIC.161或更高版本、则可以选择将某些计算密集型操作(例如加密和完整性检查)卸载到存储节点上安装的网络接口控制器(ONTAP 9)卡。使用此硬件卸载选项可以显著提高受IPsec保护的网络流量的性能和吞吐量。

要求和建议

在使用IPsec硬件卸载功能之前，应考虑几个要求。

支持的以太网卡

您只需要在存储节点上安装和使用受支持的以太网卡。ONTAP 9．16．1支持以下以太网卡：

- X50131A (2p、40G/100G/200g/400G以太网控制器)
- X60132A (4p、10G25G以太网控制器)

集群范围

IPsec硬件卸载功能是为集群全局配置的。因此、例如、命令 `security ipsec config`将应用于集群中的所有节点。

一致的配置

应在集群中的所有节点上安装受支持的NIC卡。如果支持的NIC卡仅在某些节点上可用、而某些IF未托管在支持卸载的NIC上、则在故障转移后、性能可能会显著下降。

禁用反重放

您应在ONTAP (默认配置)和IPsec客户端上禁用IPsec反重放保护。如果未禁用、则不支持分段和多路径(冗余路由)。

限制

在使用IPsec硬件卸载功能之前，应考虑一些限制。

IPv6

IPsec硬件卸载功能不支持IP版本6。只有IPsec软件实施才支持IPv6。

扩展序列号

硬件卸载功能不支持IPsec扩展序列号。仅使用正常的32位序列号。

链路聚合

IPsec硬件卸载功能不支持链路聚合。因此、它不能与通过ONTAP命令行界面上的命令管理的接口或链路聚合组结合使用 `network port ifgrp`。

ONTAP命令行界面中的配置支持

IPsec.161中更新了三个现有命令行界面命令、以支持如下所述的ONTAP 9硬件卸载功能。有关详细信息、另请参见"在ONTAP中配置IP安全性"。

ONTAP 命令	更新
`security ipsec config show`	布尔值参数 `Offload Enabled`显示当前NIC卸载状态。
`security ipsec config modify`	参数 `is-offload-enabled`可用于启用或禁用NIC卸载功能。
`security ipsec config show-ipsecsa`	添加了四个新计数器、用于显示入站和出站流量(以字节和数据包为单位)。

ONTAP REST API中的配置支持

IPsec.161中更新了两个现有的REST API端点、以支持如下所述的ONTAP 9硬件卸载功能。

REST端点	更新
`/api/security/ipsec`	已添加参数、此参数 `offload_enabled`可用于修补方法。
`/api/security/ipsec/security_association`	添加了两个新的计数器值、用于跟踪由卸载功能处理的总字节数和数据包数。

从ONTAP自动化文档中了解有关ONTAP REST API的更多信息，包括 "ONTAP REST API的新增功能"。有关的详细信息，您还应查看ONTAP自动化文档 "IPsec端点"。

在ONTAP中配置IP安全性

要在ONTAP集群上配置和激活IPsec传输中加密、需要执行多项任务。

请确保在配置IPsec之前进行查看"准备使用IP安全性"。例如，您可能需要决定是否使用从IPsec.16.1开始提供的ONTAP 9硬件卸载功能。

在集群上启用 IPsec

您可以在集群上启用IPsec、以确保数据在传输过程中持续加密和安全。

步骤

1. 发现是否已启用 IPsec：

   ```
   security ipsec config show
   ```

   如果结果包括 `IPsec Enabled: false`下，继续下一步。

2. 启用 IPsec：

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

   可以使用布尔参数启用IPsec硬件卸载功能 `is-offload-enabled`。

3. 再次运行 discovery 命令：

   `security ipsec config show`

   结果现在包括 `IPsec Enabled: true`。

准备使用证书身份验证创建IPsec策略

如果您仅使用预共享密钥(PSK)进行身份验证、而不使用证书身份验证、则可以跳过此步骤。

在创建使用证书进行身份验证的IPsec策略之前，必须验证是否满足以下前提条件：

- ONTAP和客户端都必须安装另一方的CA证书、以使最终实体(ONTAP或客户端)证书可由双方验证
- 系统会为参与此策略的 ONTAP LIF 安装证书

ONTAP LIF 可以共享证书。不需要在证书和 LIF 之间进行一对一映射。

步骤

1. 将在相互身份验证期间使用的所有CA证书(包括ONTAP端和客户端CA)安装到ONTAP证书管理中、除非已安装(例如ONTAP自签名根CA)。

   命令示例
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. 要确保安装的CA在身份验证期间位于IPsec CA搜索路径内、请使用将ONTAP证书管理CA添加到IPsec模块 `security ipsec ca-certificate add` 命令：

   命令示例
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. 创建并安装一个证书以供 ONTAP LIF 使用。此证书的颁发者 CA 必须已安装到 ONTAP 并添加到 IPsec 中。

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

有关 ONTAP 中证书的详细信息，请参见 ONTAP 9 文档中的 security certificate 命令。

定义安全策略数据库（ SPD ）

在允许流量在网络上流动之前， IPsec 需要 SPD 条目。无论您使用的是 PSk 还是证书进行身份验证，都是如此。

步骤

1. 使用 `security ipsec policy create` 命令：

a. 选择要参与 ONTAP 传输的 IPsec IP 地址或 IP 地址子网。

b. 选择要连接到 ONTAP IP 地址的客户端 IP 地址。

> 客户端必须使用预共享密钥（ psk ）支持 Internet 密钥交换版本 2 （ IKEv2 ）。

c. 可选。选择细化的流量参数、例如上层协议(UDP、TCP、ICMP等))、本地端口号和用于保护流量的远程端口号。相应的参数为 `protocols`， `local-ports` 和 `remote-ports` 。

跳过此步骤可保护 ONTAP IP 地址和客户端 IP 地址之间的所有流量。默认情况下，保护所有流量。

d. 为输入PSK或公共密钥基础架构(PKI) `auth-method` 所需身份验证方法的参数。

i. 如果输入PSK、请包含参数、然后按<enter>显示提示、以输入并验证预共享密钥。

> `local-identity`如果主机和客户端均使用strong、并且未为主机或客户端选择通配符策略、则和 `remote-identity`参数是可选的。

ii. 如果输入PKI、则还需要输入 `cert-name`， `local-identity`， `remote-identity` parameters 如果远程端证书标识未知、或者如果需要多个客户端标识、请输入特殊标识 `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
```

只有在ONTAP和客户端都设置了匹配的IPsec策略并且身份验证凭据(PSK或证书)在两端都到位之后、IP流量才能在客户端和服务器之间流动。

使用 IPsec 身份

对于预共享密钥身份验证方法、如果主机和客户端都使用strong、并且未为主机或客户端选择通配符策略、则本地和远程标识是可选的。

对于 PKI/ 证书身份验证方法，本地和远程身份都是必需的。这些身份用于指定在每一方的证书中进行认证并在验证过程中使用的身份。如果远程身份未知或可能是多个不同的身份、请使用特殊身份 `ANYTHING`。

关于此任务

在 ONTAP 中，标识是通过修改 SPD 条目或在创建 SPD 策略期间指定的。SPD 可以是 IP 地址或字符串格式的标识名称。

步骤

1. 使用以下命令修改现有SPD标识设置：

```
security ipsec policy modify
```

命令示例

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

IPsec 多客户端配置

如果少数客户端需要利用 IPsec ，则为每个客户端使用一个 SPD 条目就足以满足要求。但是，当数百甚至数千个客户端需要利用 IPsec 时， NetApp 建议使用 IPsec 多客户端配置。

关于此任务

ONTAP 支持将多个网络中的多个客户端连接到启用了 IPsec 的单个 SVM IP 地址。您可以使用以下方法之一完成此操作：

- * 子网配置 *

  要允许特定子网上的所有客户端(例如192.168.134.0/24)使用单个SPD策略条目连接到单个SVM IP地址、必须指定 `remote-ip-subnets` 子网形式。此外、您还必须指定 `remote-identity` 具有正确客户端标识的字段。

  > 在子网配置中使用单个策略条目时，该子网中的 IPsec 客户端将共享 IPsec 身份和预共享密钥（ PSk ）。但是，对于证书身份验证，情况并非如此。使用证书时，每个客户端都可以使用自己的唯一证书或共享证书进行身份验证。ONTAP IPsec 会根据安装在其本地信任存储上的 CA 检查证书的有效性。ONTAP 还支持证书撤消列表（ Certificate Revocation List ， CRL ）检查。

- * 允许所有客户端配置 *

  要允许任何客户端(无论其源IP地址如何)连接到已启用SVM IPsec的IP地址、请使用 `0.0.0.0/0` 指定时使用通配符 `remote-ip-subnets` 字段。

  此外、您还必须指定 `remote-identity` 具有正确客户端标识的字段。对于证书身份验证、您可以输入 `ANYTHING`。

  此外、当 `0.0.0.0/0` 如果使用通配符、则必须配置要使用的特定本地或远程端口号。例如： `NFS port 2049`。

  步骤

  a. 使用以下命令之一为多个客户端配置IPsec。

     i. 如果使用*subnetconfiguration (子网配置)*支持多个IPsec客户端：

     ```
     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
     ```

  命令示例

  ```
  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. 如果使用*允许所有客户端配置*支持多个IPsec客户端：

```
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
```

命令示例

```
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
```

显示IPsec统计信息

通过协商，可以在 ONTAP SVM IP 地址和客户端 IP 地址之间建立一个称为 "ike 安全关联（ SA ） " 的安全通道。IPsec SAS 安装在两个端点上，用于执行实际的数据加密和解密工作。您可以使用 statistics 命令来检查 IPsec SAS 和 ike SAS 的状态。

如果使用IPsec硬件卸载功能，则命令会显示几个新计数器 `security ipsec config show-ipsecsa`。

命令示例

IKESA 命令示例：

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

IPsec SA 命令和输出示例：

```
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 命令和输出示例：

```
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
```