設定 IPsec 在線上加密

ONTAP 9

NetApp
January 17, 2025

目錄

設定 IPsec 在線上加密

準備使用 IP 安全性

從 ONTAP 9 8 開始，您可以選擇使用 IP 安全性（ IPsec ）來保護網路流量。IPsec 是 ONTAP 提供的數種資料傳輸或傳輸中加密選項之一。在正式作業環境中使用 IPsec 之前，您應該做好設定的準備。

ONTAP 中的 IP 安全實作

IPsec 是由 IETF 維護的網際網路標準。它提供資料加密與完整性，以及 IP 層級網路端點之間流量傳輸的驗證。

使用 ONTAP 時， IPsec 可保護 ONTAP 和各種用戶端之間的所有 IP 流量，包括 NFS ， SMB 和 iSCSI 傳輸協定。除了隱私權和資料完整性之外，網路流量還能防範多種攻擊，例如重播和攔截式攻擊。ONTAP 使用 IPsec 傳輸模式實作。它利用網際網路金鑰交換（ IKE） 傳輸協定第 2 版，在 ONTAP 和使用 IPv4 或 IPv6 的用戶端之間協商金鑰資料。

當叢集上啟用 IPsec 功能時，網路需要 ONTAP 安全性原則資料庫（ SPD ）中的一或多個項目，才能符合各種流量特性。這些項目會對應至處理及傳送資料所需的特定保護詳細資料（例如密碼套件和驗證方法）。每個用戶端也需要對應的 SPD 項目。

對於某些類型的流量，最好使用另一個資料傳輸加密選項。例如，對於 NetApp SnapMirror 和叢集對等流量的加密，一般建議使用傳輸層安全性（ TLS ）傳輸協定，而非 IPsec 。這是因為 TLS 在大多數情況下都能提供更好的效能。

相關資訊

- "網際網路工程工作團隊"
- "RFC 4301-Security Architecture for the Internet Protocol （網際網路傳輸協定的安全架構）"

ONTAP IPsec 實作的演進

ONTAP 9 第一次推出 IPsec 。 8實作持續進化並改善，如下所述。

從特定 ONTAP 版本開始引進某項功能時，除非另有說明，否則後續版本也會支援該功能。

ONTAP 9.16.1.

加密和完整性檢查等多項密碼編譯作業可卸載至支援的 NIC 卡。如需詳細資訊、請參閱 IPsec 硬體卸載功能 。

ONTAP 9.12.1

MetroCluster IP 和 MetroCluster 網路附加組態提供 IPsec 前端主機傳輸協定支援。MetroCluster 叢集所提供的 IPsec 支援僅限於前端主機流量， MetroCluster 叢集間的生命體不受支援。

零點9.10.1 ONTAP

除了預先共用金鑰（ PSK ）之外，憑證也可用於 IPsec 驗證。在 ONTAP 9 .10.1 之前，僅支援驗證 PSK 。

部分9.9.1 ONTAP

IPsec 使用的加密演算法已通過 FIPS 140-2 驗證。這些演算法由 ONTAP 中的 NetApp 密碼編譯模組處理，該

模組執行 FIPS 140-2 驗證。

部分**9.8 ONTAP**

根據傳輸模式實作， IPsec 的支援一開始就可用。

IPsec 硬體卸載功能

如果您使用的是 ONTAP 9 。 16.1 或更新版本，您可以選擇將某些運算密集的作業（例如加密和完整性檢查）卸載到儲存節點上安裝的網路介面控制器（ NIC ）卡。使用此硬體卸載選項可大幅改善受 IPsec 保護的網路流量的效能和處理量。

要求與建議

在使用 IPsec 硬體卸載功能之前，您應該考量幾項需求。

支援的乙太網路卡

您只需要在儲存節點上安裝及使用支援的乙太網路卡。ONTAP 9 支援下列乙太網路卡：

- X50131A （ 2p ， 40G/100g/200g/400G 乙太網路控制器）
- X60132A （ 4p ， 10G/25G 乙太網路控制器）

叢集範圍

IPsec 硬體卸載功能是針對叢集進行全域設定。例如，此命令會 `security ipsec config`套用至叢集中的所有節點。

一致的組態

支援的 NIC 卡應安裝在叢集中的所有節點上。如果支援的 NIC 卡只能在某些節點上使用，則當容錯移轉後，如果部分生命負載未裝載於具有卸載功能的 NIC 上，您就會發現效能大幅降低。

停用反重播

您應該在 ONTAP （預設組態）和 IPsec 用戶端停用 IPsec 反重新執行保護。如果未停用，將不支援分割和多重路徑（備援路由）。

限制

在使用 IPsec 硬體卸載功能之前，您應該考慮幾項限制。

IPv6

IPsec 硬體卸載功能不支援 IP 版本 6 。只有 IPsec 軟體實作支援 IPv6 。

延伸序號

硬體卸載功能不支援 IPsec 延伸序列號。僅使用正常的 32 位元序列號。

連結集合體

IPsec 硬體卸載功能不支援連結集合。因此，它無法與透過 ONTAP CLI 命令所管理的介面或連結集合群組搭配使用 `network port ifgrp`。

ONTAP CLI 中的組態支援

ONTAP 9 。 16.1 中更新了三個現有的 CLI 命令，以支援以下所述的 IPsec 硬體卸載功能。如需詳細資訊，請參閱"在 ONTAP 中設定 IP 安全性"。

指令**ONTAP**	更新
`security ipsec config show`	布林參數 `Offload Enabled`顯示目前的 NIC 卸載狀態。
`security ipsec config modify`	此參數 `is-offload-enabled`可用於啟用或停用 NIC 卸載功能。
`security ipsec config show-ipsecsa`	新增了四個新的計數器，以位元組和封包顯示傳入和傳出流量。

ONTAP REST API 中的組態支援

ONTAP 9 中更新了兩個現有的 REST API 端點。 16.1 可支援 IPsec 硬體卸載功能，如下所述。

REST端點	更新
`/api/security/ipsec`	此參數 `offload_enabled`已新增，可透過修補方法使用。
`/api/security/ipsec/security_association`	新增兩個計數器值，以追蹤卸載功能處理的總位元組和封包數。

從 ONTAP 自動化文件中深入瞭解 ONTAP REST API ，包括 "ONTAP REST API 的新功能"。您也應該檢閱 ONTAP 自動化文件，以取得有關的詳細資訊 "IPsec 端點"。

在 ONTAP 中設定 IP 安全性

在 ONTAP 叢集上設定及啟動 IPsec 進行中加密需要執行數項工作。

設定 IPsec 之前，請務必先檢閱"準備使用 IP 安全性"。例如，您可能需要決定是否使用以 ONTAP 9 開頭的可用 IPsec 硬體卸載功能。 16.1

在叢集上啟用**IPsec**

您可以在叢集上啟用 IPsec ，以確保資料在傳輸過程中持續加密且安全。

步驟

1. 探索是否已啟用IPsec：

   ```
   security ipsec config show
   ```

   如果結果包括 `IPsec Enabled: false`，繼續下一步。

2. 啟用IPsec：

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

   您可以使用布爾參數來啟用 IPsec 硬體卸載功能 `is-offload-enabled`。

3. 再次執行探索命令：

   `security ipsec config show`

   現在的結果包括 `IPsec Enabled: true`。

準備使用憑證驗證建立 **IPsec** 原則

如果您只使用預先共用金鑰（ PSK ）進行驗證、而且不會使用憑證驗證、則可以略過此步驟。

在建立使用憑證進行驗證的 IPsec 原則之前、您必須確認符合下列先決條件：

- ONTAP 和用戶端都必須安裝另一方的 CA 憑證、以便雙方可驗證終端實體（ ONTAP 或用戶端）憑證
- 系統會為ONTAP 參與該原則的Sfor the Sfor the Sfor the Sfor the Sfor the Sfor the Sfor the Sfor the

可共享證書的產品。ONTAP不需要在憑證與lifs之間建立一對一對應關係。

步驟

1. 除非已安裝 ONTAP 憑證管理（例如 ONTAP 自我簽署的根 CA ）、否則請將在相互驗證期間使用的所有 CA 憑證（包括 ONTAP 端和用戶端 CA ）安裝到憑證管理。
   - 命令範例 *
     ```
     cluster::> security certificate install -vserver svm_name -type server-ca
     -cert-name my_ca_cert
     ```
2. 若要確保在驗證期間安裝的 CA 位於 IPsec CA 搜尋路徑內、請使用將 ONTAP 憑證管理 CA 新增至 IPsec 模組 `security ipsec ca-certificate add` 命令。
   - 命令範例 *
     ```
     cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
     my_ca_cert
     ```
3. 建立並安裝認證以供ONTAP 《Sfor the Suse LIF（供《Sfor the Suse：此憑證的發卡行CA必須已安裝ONTAP 至ESA並新增至IPsec。
   - 命令範例 *
     ```
     cluster::> security certificate install -vserver svm_name -type server -cert
     -name my_nfs_server_cert
     ```

如需ONTAP 更多有關資訊、請參閱ONTAP 《》介紹文件中的安全認證命令。

定義安全性原則資料庫（**SPD**）

在允許流量在網路上傳輸之前、IPsec需要SPD項目。無論您使用的是用於驗證的PSK或憑證、都是如此。

步驟

1. 使用 `security ipsec policy create` 命令至：
   a. 選取ONTAP 要參與IPsec傳輸的IP位址或子網路。
   b. 選取要連線ONTAP 至「靜態IP位址」的用戶端IP位址。

用戶端必須使用預先共用金鑰（PSK）來支援網際網路金鑰交換版本2（IKEv2）。

c. 選用。選取精細的流量參數、例如上層傳輸協定（ UDP 、 TCP 、 ICMP 等）、本機連接埠號碼和遠端連接埠號碼、以保護流量。對應的參數為 `protocols`、 `local-ports` 和 `remote-ports` 分別。

跳過此步驟以保護ONTAP 所有介於整個過程中的資訊流量、例如：靜態IP位址和用戶端IP位址。保護所有流量是預設設定。

d. 輸入的 PSK 或公開金鑰基礎架構（ PKI ） `auth-method` 所需驗證方法的參數。

i. 如果您輸入一個 PSK 、請包含參數、然後按 <enter> 鍵提示您輸入並驗證預先共用金鑰。

`local-identity`如果主機和用戶端都使用強化天鵝，而且沒有為主機或用戶端選取萬用字元原則，則和 `remote-identity`參數是選用的。

ii. 如果您輸入 PKI 、也需要輸入 `cert-name`、 `local-identity`、 `remote-identity` 參數。如果遠端端憑證身分不明、或是需要多個用戶端身分識別、請輸入特殊身分識別 `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
```

除非 ONTAP 和用戶端都設定了相符的 IPsec 原則、而且雙方都有驗證認證（可以是 PSK 或憑證）、否則 IP 流量無法在用戶端和伺服器之間傳輸。

使用IPsec身分識別

對於預先共用金鑰驗證方法、如果主機和用戶端都使用強化天鵝、而且沒有為主機或用戶端選取萬用字元原則、則本機和遠端身分識別是選用的。

對於公開密碼匙基礎建設/憑證驗證方法、本機和遠端身分識別都是必要的。身分識別會指定在每一方憑證中認證的身分識別、並用於驗證程序。如果遠端身分識別不明、或是可能有許多不同的身分識別、請使用特殊身分識別 `ANYTHING`。

關於這項工作

在不受限的情況下、可透過修改SPD項目或在SPD原則建立期間來指定身分識別。ONTAPSPD可以是IP位址或字串格式身分識別名稱。

步驟

1. 使用下列命令修改現有的 SPD 身分識別設定：

```
security ipsec policy modify
```

命令範例

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

IPsec多個用戶端組態

當少數用戶端需要使用IPsec時、每個用戶端只需使用一個SPD項目就足夠了。但是、當數百甚至數千個用戶端需要使用IPsec時、NetApp建議使用IPsec多重用戶端組態。

關於這項工作

支援將多個網路上的多個用戶端連線至單一SVM IP位址、並啟用IPsec。ONTAP您可以使用下列其中一種方法來達成此目的：

- 子網路組態

  若要允許特定子網路上的所有用戶端（例如 192.168.134.0/24 ）使用單一 SPD 原則項目連線到單一 SVM IP 位址、您必須指定 `remote-ip-subnets` 子網路形式。此外、您必須指定 `remote-identity` 具有正確用戶端身分識別的欄位。

  > 在子網路組態中使用單一原則項目時、該子網路中的IPsec用戶端會共用IPsec身分識別和預先共用金鑰（PSK）。不過、憑證驗證並不符合此要求。使用憑證時、每個用戶端都可以使用自己的唯一憑證或共用憑證進行驗證。IPsec會根據安裝在本機信任存放區上的CA來檢查憑證的有效性。ONTAP支援憑證撤銷清單（CRL）檢查。ONTAP

- 允許所有用戶端組態

  若要允許任何用戶端連線至 SVM IPsec 啟用的 IP 位址、無論其來源 IP 位址為何、請使用 `0.0.0.0/0` 指定時使用萬用字元 `remote-ip-subnets` 欄位。

  此外、您必須指定 `remote-identity` 具有正確用戶端身分識別的欄位。對於憑證驗證、您可以輸入 `ANYTHING`。

  此外、當 `0.0.0.0/0` 使用萬用字元時、您必須設定要使用的特定本機或遠端連接埠號碼。例如、 `NFS port 2049`。

  步驟

  a. 使用下列其中一個命令來設定多個用戶端的 IPsec 。

     i. 如果您使用 * 子網路組態 * 來支援多個 IPsec 用戶端：

     ```
     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
     ```

     命令範例

     ```
     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. 如果您使用 * 允許所有用戶端組態 * 來支援多個 IPsec 用戶端：

```
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
```

命令範例

```
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
```

顯示 IPsec 統計資料

透過協商、ONTAP 可在「穩定SVM IP位址」和「用戶端IP位址」之間建立稱為「IKE安全性關聯」（SA）的安全通道。兩個端點都安裝了IPsec SAS、以執行實際的資料加密與解密工作。您可以使用統計資料命令來檢查IPsec SAS和IKE SAS的狀態。

如果您使用 IPsec 硬體卸載功能，則會使用命令顯示數個新的計數器 `security ipsec config show-ipsecsa`。

命令範例

IKE SA命令範例：

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

IPsec SA命令和輸出範例：

```
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命令和輸出範例：

```
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
```

版權資訊

商標資訊