使用具有證書身份驗證的IKEv2配置DMVPN第3階段

目錄

簡介

本文描述有關如何使用IKEv2配置使用證書驗證的動態多點VPN(DMVPN)第3階段的資訊。

必要條件

需求

思科建議瞭解以下主題：

- DMVPN基礎知識。
- EIGRP基礎知識。
- 公開金鑰基礎架構(PKI)的基本知識。

採用元件

本檔案中的資訊是根據以下軟體版本：

- 執行Cisco IOS® 版本17.3.8a的Cisco C8000v(VXE)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

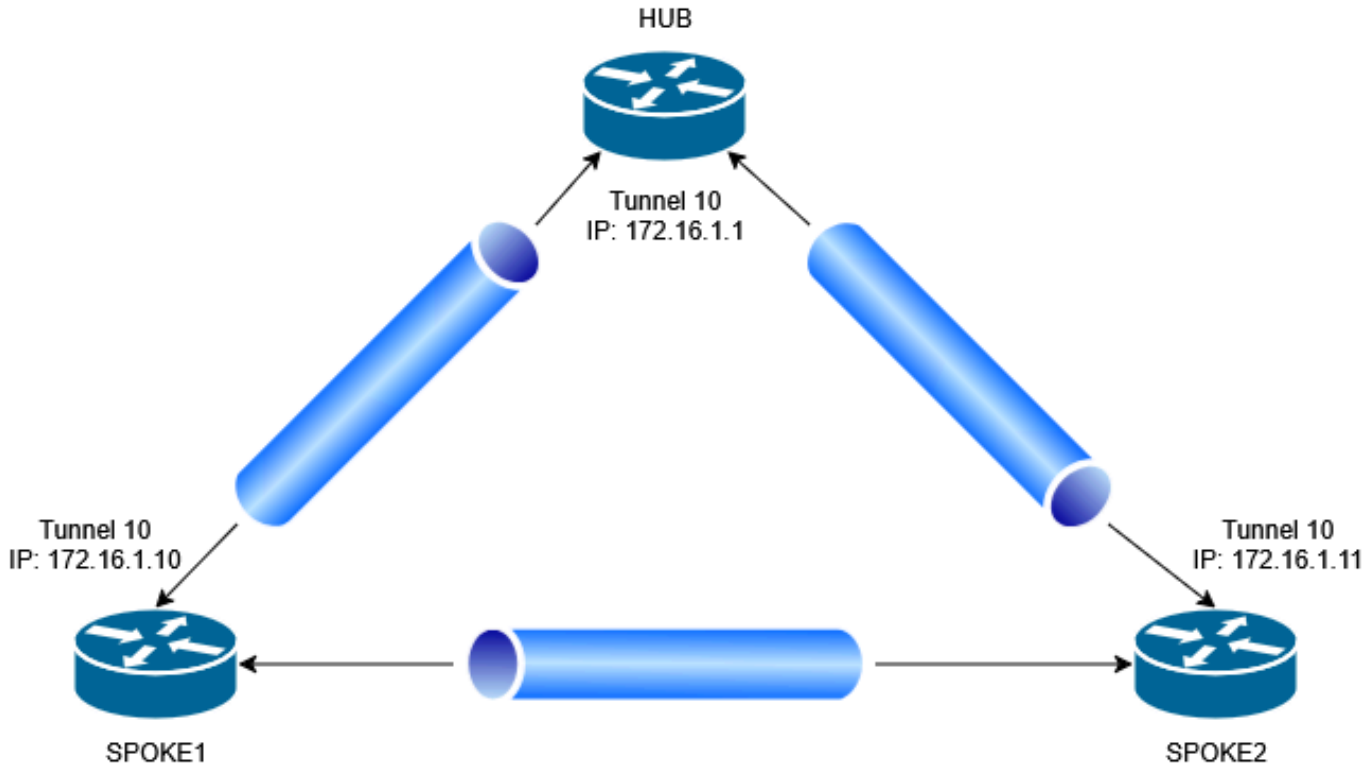
背景資訊

動態多點VPN(DMVPN)第3階段引入了直接輻條到輻條連線，使VPN網路能夠通過繞過集線器而為大多數流量路徑更高效地運行。此設計將延遲降至最低並最佳化了資源利用率。通過使用下一跳解析協定(NHRP)，分支可以動態地識別彼此並建立直接隧道，從而支援大型和複雜的網路拓撲。
Internet金鑰交換版本2(IKEv2)提供了在此環境中建立安全隧道的底層機制。與早期的協定相比，IKEv2提供了高級安全措施、更快的金鑰更新過程，並增強了移動性和多連線的支援。它與DMVPN第3階段的整合可確保安全有效地處理隧道設定和金鑰管理。
為了進一步加強網路安全，IKEv2支援數位證書身份驗證。此方法使裝置能夠使用證書驗證彼此之間的身份，從而簡化管理並降低與共用機密相關的風險。基於證書的信任在擴展部署中特別有益，因為在這種部署中，管理單個金鑰會非常困難。
總而言之，DMVPN第3階段、IKEv2和證書身份驗證可提供強大的VPN框架。此解決方案通過確保靈活的連線、強大的資料保護和簡化的操作，滿足了現代企業的需求。

設定

本節提供使用基於證書的身份驗證配置DMVPN第3階段和IKEv2的分步說明。完成以下步驟，在中心路由器和分支路由器之間啟用安全且可擴展的VPN連線。

網路圖表



組態

準備證書基礎架構

確保所有裝置（集線器和輻條）都安裝了必要的數位證書。這些證書必須由受信任的CA頒發，並在每台裝置上正確註冊，以便啟用安全的IKEv2證書身份驗證。
要在集中星型路由器上註冊證書，請完成以下步驟：

1.使用crypto pki trustpoint <Trustpoint Name>命令使用所需資訊配置信任點。

<#root>

```
Hub(config)#

crypto pki trustpoint myCertificate


Hub(ca-trustpoint)# enrollment terminal
Hub(ca-trustpoint)# ip-address 10.10.1.2
Hub(ca-trustpoint)# subject-name cn=Hub, o=cisco
Hub(ca-trustpoint)# revocation-check none
```

2.使用crypto pki authenticate <Trustpoint Name>命令對信任點進行身份驗證。

<#root>

```
Hub(config)#

crypto pki authenticate myCertificate


Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

注意：發出crypto pki authenticate命令後，必須貼上來自證書頒發機構(CA)的證書，該證書用於對裝置證書進行簽名。在中心和分支路由器上繼續證書註冊之前，此步驟對於在裝置和CA之間建立信任至關重要。

3.使用命令crypto pki enroll <Trustpoint Name>生成私鑰和證書簽名請求(CSR)。

<#root>

```
Hub(config)#

crypto pki enroll myCertificate


% Start certificate enrollment ..

% The subject name in the certificate will include: cn=Hub, o=cisco
% The subject name in the certificate will include: Hub
% Include the router serial number in the subject name? [yes/no]: n
% The IP address in the certificate is 10.10.1.2
```

```
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

MIICsDCCAZgCAQAwSjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAMTA0hVQjEqMBAG
CSqGSIb3DQEJAhYDSFVCMBYGCSqGSIb3DQEJCBMJMTAuMTAuMS4yMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAo/M4O+ivsqJhpF0PRUxdCGSUVgLQUhzQ
cwnuMtSbfdn5fMKIj7wO6Qa7Gvx2rjrdoyxH9JgXjTEMzMv6HP9/EuN2o+qKzR/+
CNzMUDJobb0lBNbeOWKL4IAQjbvNTOyA5iuUzHZCgMrCFG3oU7v+a2tMiSZihvdu
+m2JSDNXn5cXyewQbQsEaELAO0yosi2t6BQyzM3FRU23dCwnFVwY1VAADC7CrNh3
o44SifYW5HtWq1tU1cLTY4sjNf6XJQxjmHPudbUp164RDfUSo37Zjvjt7S8OOoLU
+XUBrE3aRDlwJ+Ug2DO31ZWzfc+rBZ1BsKWlYFBlLk3mL9RA1nf3eQIDAQABoCEw
HwYJKoZIhvcNAQkOMRIwEDAOBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEFBQAD
ggEBAEKUQURWZ+YeCx9T7kuzIaDwJ53vMqq6rITDJcNF9FJ4IgJ7PsxFOcWXm7MM
O3Oi1yq1K/4X7Mb5Iz6CjtdyXVqakgcEPY7W9NoO3Xo8Nxb4pFfe19EO2Xuj8fxm
GTqi7UAw8ZslzJ2jrS7bXasVMb5jjr39cqQkrXfNIAwF1Sw6IA3oKfTelq8/iCJu
TEjFOD8Si2PWziuxJVS4Adjg5GxbJpd/tDKrKUuvqD2z4HD3M4OoGVvoBWQOtjhB
4gx1q2D2O9KOnMCvVZrOfp/PFd6+cYc57E73ZPVSGQpHIiiWCYtuRKdKArN6vRcP
iiugceU2F3Ll4CI7wXMYqCxQOGU=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
```

附註：在此過程中使用的私鑰是路由器生成的預設私鑰。但是，如果需要，也支援使用自定義私鑰。

4.產生CSR後，將其傳送到憑證授權單位(CA)進行簽署。

5.簽名證書後，使用命令crypto pki import <Trustpoint Name> certificate匯入與建立的信任點關聯的簽名證書。

<#root>

```
Hub(config)#
crypto pki import myCertificate certificate


% You must authenticate the Certificate Authority before
you can import the router's certificate.
```

6.以PEM格式貼上CA簽署的憑證。

加密IKEv2和IPSec配置

分支和集線器上的加密IKEv2和IPSec的配置可以相同。這是因為建議方案和使用的密碼等元素必須始終在所有裝置上匹配，以確保可以成功建立隧道。這種一致性可確保DMVPN第3階段環境中的互操作性和安全通訊。

1.配置IKEv2提議。

```
crypto ikev2 proposal ikev2
encryption aes-cbc-256
integrity sha256
group 14
```

2.配置IKEv2配置檔案。

```
<#root>

crypto ikev2 profile ikev2Profile
match identity remote address 0.0.0.0
identity local address 10.10.1.2

authentication remote rsa-sig


authentication local rsa-sig


pki trustpoint

myCertificate
```

附註：此處定義了PKI證書身份驗證和用於身份驗證的信任點。

3.配置IPSec配置檔案和轉換集。

```
crypto ipsec transform-set ipsec esp-aes 256 esp-sha256-hmac
mode tunnel
crypto ipsec profile ipsec
set transform-set ipsec
set ikev2-profile ikev2Profile
```

通道組態

本節介紹集線器和輻條的通道配置，特別關注DMVPN設定的第3階段。

1.中心隧道配置。

```
interface Tunnel10
ip address 172.16.1.1 255.255.255.0
no ip redirects
no ip split-horizon eigrp 10
ip nhrp authentication cisco123
ip nhrp network-id 10
ip nhrp redirect
tunnel source GigabitEthernet1
```

```
tunnel mode gre multipoint
tunnel protection ipsec profile ipsec
end
```

2. Spoke1隧道配置。

```
interface Tunnel10
ip address 172.16.1.10 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp map 172.16.1.1 10.10.1.2
ip nhrp map multicast 10.10.1.2
ip nhrp network-id 10
ip nhrp nhs 172.16.1.1
tunnel source GigabitEthernet2
tunnel mode gre multipoint
tunnel protection ipsec profile ipsec
end
```

3. Spoke2隧道配置。

```
interface Tunnel10
ip address 172.16.1.11 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp map 172.16.1.1 10.10.1.2
ip nhrp map multicast 10.10.1.2
ip nhrp network-id 10
ip nhrp nhs 172.16.1.1
tunnel source GigabitEthernet3
tunnel mode gre multipoint
tunnel protection ipsec profile ipsec
end
```

驗證

要確認DMVPN第3階段網路是否正常運行，請使用以下命令：

- show dmvpn interface <Tunnel Name>
- show crypto ikev2 sa
- show crypto ipsec sa peer <peer IP>

使用show dmvpn interface <Tunnel Name>指令，您可以看到集線器和輻條之間的作用中作業階段。從Spoke1的角度來看，輸出可以反映這些已建立的連線。

<#root>

SPOKE1#

show dmvpn interface tunnel10

```
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
T1 - Route Installed, T2 - Nexthop-override, B - BGP
C - CTS Capable, I2 - Temporary
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface: Tunnel10, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

# Ent Peer NBMA Addr Peer Tunnel Add
```

State

```
 UpDn Tm Attrb
----- -------------- --------------- ----- -------- -----
   1  10.10.1.2           172.16.1.1
```

UP

```
      1w6d     S
   1  10.10.3.2          172.16.1.11
```

UP

```
  00:00:04     D
```

show crypto ikev2 sa命令顯示在輻條和集線器之間形成的IKEv2隧道，確認第1階段協商成功。

<#root>

SPOKE1#

show crypto ikev2 sa

```
IPv4 Crypto IKEv2 SA

Tunnel-id Local            Remote             fvrf/ivrf
```

Status

```
1       10.10.2.2/500      10.10.3.2/500      none/none
```

READY

```
     Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify:
```

RSA

```
     Life/Active Time: 86400/184 sec

Tunnel-id Local            Remote             fvrf/ivrf
Status

2      10.10.2.2/500       10.10.1.2/500      none/none
READY

     Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify:
RSA

     Life/Active Time: 86400/37495 sec

IPv6 Crypto IKEv2 SA
```

使用show crypto ipsec sa peer <peer IP>命令，您可以驗證在分支和集線器之間建立的IPSec隧道，確保DMVPN網路內的安全資料傳輸。

```
<#root>

SPOKE1#show
crypto ipsec sa peer 10.10.3.2



interface: Tunnel10
Crypto map tag: Tunnel10-head-0, local addr 10.10.2.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.10.2.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.10.3.2/255.255.255.255/47/0)
current_peer 10.10.3.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.10.2.2, remote crypto endpt.: 10.10.3.2
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet2
current outbound spi: 0xF341E02E(4081180718)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8ED55E26(2396347942)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
conn id: 2701, flow_id: CSR:701, sibling_flags FFFFFFFF80000048, crypto map: Tunnel10-head-0
sa timing: remaining key lifetime (k/sec): (4607999/3188)
IV size: 16 bytes
replay detection support: Y
```

```
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xF341E02E(4081180718)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
conn id: 2702, flow_id: CSR:702, sibling_flags FFFFFFFF80000048, crypto map: Tunnel10-head-0
sa timing: remaining key lifetime (k/sec): (4607999/3188)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

疑難排解

要進行故障排除，可以使用以下命令：

- debug dmvpn condition peer [nbma/tunnelIP]，為來自對等體的NBMA或隧道IP地址特定的DMVPN會話啟用條件調試，幫助隔離與該對等體相關的問題。
- debug dmvpn all，啟用DMVPN所有方面的全面調試，包括NHRP、加密IKE、IPsec、隧道保護和加密套接字。建議將此命令與條件過濾器結合使用，以避免過多調試資訊覆蓋路由器。
- show dmvpn，顯示當前DMVPN狀態，包括隧道介面、NHRP對映和對等體資訊。
- show crypto ikev2 sa ，顯示IKEv2安全關聯的狀態，對於驗證第1階段VPN協商很有用。
- show crypto ipsec sa, Displaying IPsec Security Associations， showing Phase 2 tunnel status and traffic statistics。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。