使用具有证书身份验证的IKEv2配置DMVPN第3阶段

目录

简介

本文档介绍如何使用IKEv2配置动态多点VPN(DMVPN)第3阶段证书身份验证的信息。

先决条件

要求

思科建议了解以下主题：

- DMVPN基础知识。
- EIGRP 的基础知识.
- 公钥基础设施(PKI)基础知识。

使用的组件

本文档中的信息基于以下软件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

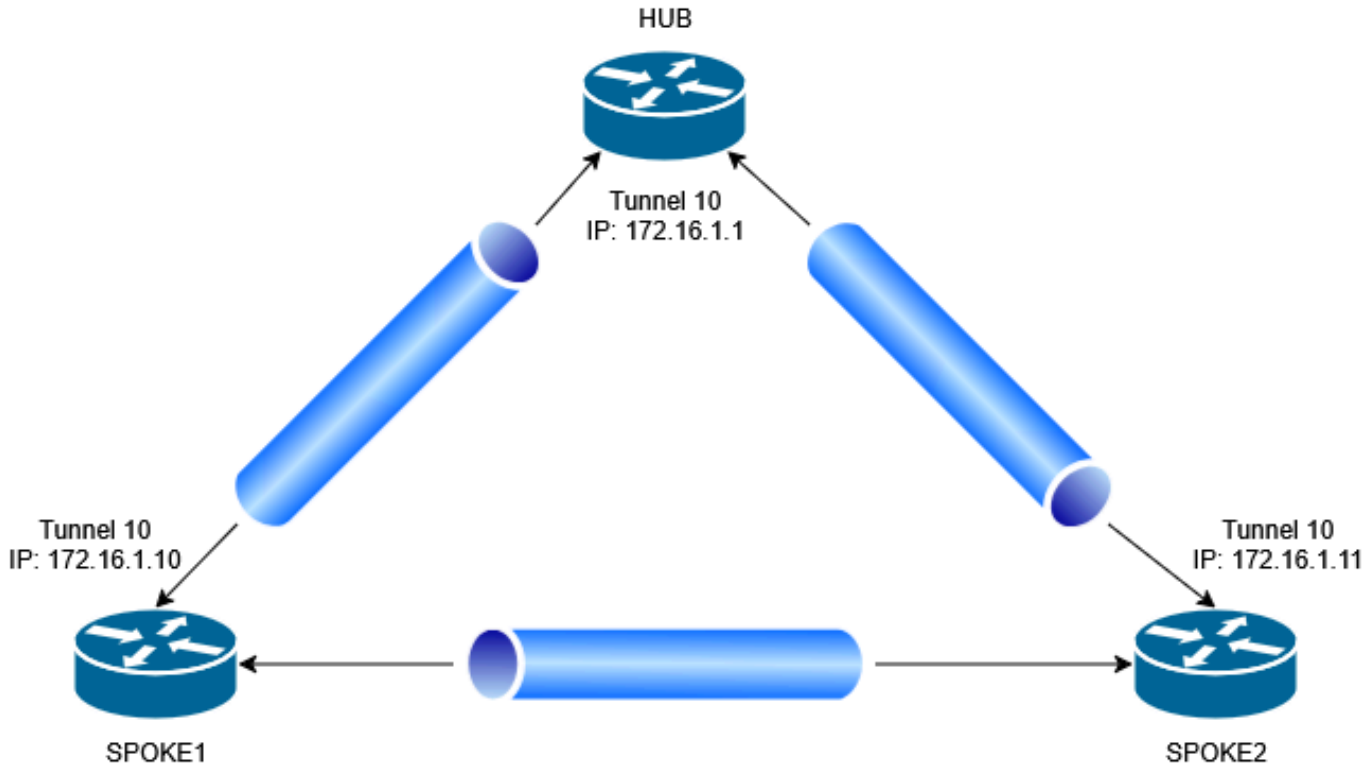
背景信息

动态多点VPN(DMVPN)第3阶段引入了直接分支到分支连接，使VPN网络能够通过绕过集线器来绕过大多数流量路径而更高效地运行。此设计可最大限度地减少延迟并优化资源利用率。通过使用下一跳解析协议(NHRP)，分支可以动态识别彼此并创建直接隧道，从而支持大型复杂网络拓扑。
Internet密钥交换版本2(IKEv2)提供在此环境中建立安全隧道的底层机制。与早期的协议相比，IKEv2提供高级安全措施、更快的密钥更新过程，并增强了对移动性和多个连接的支持。它与DMVPN第3阶段的集成可确保安全有效地处理隧道设置和密钥管理。
为了进一步加强网络安全，IKEv2支持数字证书身份验证。此方法使设备能够使用证书验证彼此之间的身份，从而简化管理并降低与共享密钥相关的风险。基于证书的信任在扩展部署中特别有用，因为在这种部署中，管理单个密钥非常困难。
总之，DMVPN第3阶段、IKEv2和证书身份验证可提供强大的VPN框架。此解决方案通过确保灵活的连接、强大的数据保护和简化的操作，满足了现代企业的需求。

配置

本节提供使用基于证书的身份验证配置DMVPN第3阶段与IKEv2的逐步说明。完成以下步骤，在集中星型路由器之间启用安全且可扩展的VPN连接。

网络图



配置

准备证书基础设施

确保所有设备（集线器和辐条）都安装了必要的数字证书。这些证书必须由受信任CA颁发，并在每台设备上正确注册，才能启用安全的IKEv2证书身份验证。
要在集中星型路由器上注册证书，请完成以下步骤：

1.使用命令crypto pki trustpoint <Trustpoint Name>配置包含所需信息的信任点。

<#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>命令对信任点进行身份验证。

<#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：在发出命令crypto pki authenticate后，您必须粘贴来自证书颁发机构(CA)的证书，该证书用于签署设备证书。在中心和分支路由器上继续证书注册之前，此步骤对于在设备和CA之间建立信任至关重要。

3.使用命令crypto pki enroll <Trustpoint Name>生成私钥和证书签名请求(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]:
```

注意：此过程中使用的私钥是路由器生成的默认私钥。但是，如果需要，也支持使用自定义私钥。

4.生成CSR后，将其发送到要签名的证书颁发机构(CA)。

5.证书签名后，使用命令crypto pki import <Trustpoint Name> certificate导入与创建的信任点关联的签名证书。

<#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格式粘贴CA签名的证书。

加密IKEv2和IPSec配置

Crypto IKEv2和IPSec的配置在分支和集线器上可以相同。这是因为，提议和使用的密码等元素必须始终在所有设备上匹配，以确保可以成功建立隧道。这种一致性可确保DMVPN第3阶段环境中的互操作性和安全通信。

1.配置IKEv2提议。

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

2.配置IKEv2配置文件。

<#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

注意：此处定义了PKI证书身份验证和用于身份验证的信任点。

3.配置IPSec配置文件和转换集。

```
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
```

隧道配置

本节介绍集线器和辐射点的隧道配置，特别关注DMVPN设置的第3阶段。

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
```

验证

要确认DMVPN第3阶段网络是否正常运行，请使用以下命令：

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

使用show dmvpn interface <Tunnel Name>命令，您可以看到集线器和辐射点之间的活动会话。从Spoke1的角度来看，输出可以反映这些已建立的连接。

<#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命令显示在分支和集线器之间形成的IKEv2隧道，确认第1阶段协商成功。

<#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，您可以验证在分支和中心之间建立的IPSec隧道，从而确保DMVPN网络内的安全数据传输。

```
<#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:
```

故障排除

要进行故障排除，可以使用以下命令：

- debug dmvpn condition peer [nbma/tunnelIP](debug dmvpn condition peer [nbma/tunnelIP])，为来自对等体的NBMA或隧道IP地址特定的DMVPN会话启用条件调试，帮助隔离与该对等体相关的问题。
- debug dmvpn all，启用DMVPN所有方面的全面调试，包括NHRP、加密IKE、IPsec、隧道保护和加密套接字。建议将此命令与条件过滤器结合使用，以避免过多调试信息覆盖路由器。
- show dmvpn，显示当前DMVPN状态，包括隧道接口、NHRP映射和对等体信息。
- show crypto ikev2 sa，显示IKEv2安全关联的状态，对于验证第1阶段VPN协商很有用。
- show crypto ipsec sa，显示IPsec安全关联，显示第2阶段隧道状态和流量统计信息。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。