在ASA上将基于策略的加密隧道迁移至基于路由的加密隧道

目录

简介

本文档介绍如何在ASA上将基于策略的隧道迁移至基于路由的隧道。

先决条件

要求

思科建议您了解以下主题：

- 基本了解IKEv2-IPSec VPN概念。
- 了解ASA上的IPSec VPN及其配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ASA：ASA代码版本9.8(1)或更高版本。

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。

配置

迁移步骤：

1. 删除现有的基于策略的VPN配置
2. 配置IPSec配置文件
3. 配置虚拟隧道接口(VTI)
4. 配置静态路由或动态路由协议

配置

现有基于策略的隧道：

1. 接口配置：

绑定加密映射的出口接口。

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.10.10.10 255.255.255.0
```

2. IKEv2策略：

它定义了IPsec协商过程第1阶段的参数。

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

3. 隧道组：

它定义VPN连接的参数。隧道组对于配置站点到站点VPN至关重要，因为它们包含有关对等体、身份验证方法和各种连接参数的信息。

```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

4. 加密ACL：

它定义了必须通过隧道加密和发送的流量。

```
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0

access-list asa-vpn extended permit ip object-group local-network object-group remote-network
```

5. 加密IPSec提议：

它定义了IPsec方案，该方案指定了IPsec协商第2阶段的加密和完整性算法。

```
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
```

6. 加密映射配置：

它定义了IPsec VPN连接的策略，包括要加密的流量、对等体以及之前配置的ipsec提议。它还绑定到处理VPN流量的接口。

```
crypto map outside_map 10 match address asa-vpn
crypto map outside_map 10 set peer 10.20.20.20
crypto map outside_map 10 set ikev2 ipsec-proposal IKEV2_TSET

crypto map outside_map interface outside
```

将基于策略的隧道迁移至基于路由的隧道：

1. 删除现有的基于策略的VPN配置：
   首先，删除现有的基于策略的VPN配置。其中包括该对等体的加密映射条目、ACL和任何相关设置。

```
no crypto map outside_map 10 match address asa-vpn
no crypto map outside_map 10 set peer 10.20.20.20
no crypto map outside_map 10 set ikev2 ipsec-proposal IKEV2_TSET
```

2. 配置IPSec配置文件：
   使用现有IKEv2 ipsec-proposal或transform-set定义IPsec配置文件。

```
crypto ipsec profile PROPOSAL_IKEV2_TSET
 set ikev2 ipsec-proposal IKEV2_TSET
```

3. 配置虚拟隧道接口(VTI)：
   创建虚拟隧道接口(VTI)并将IPsec配置文件应用到该接口。

```
interface Tunnel1
 nameif VPN-BRANCH
 ip address 10.1.1.2 255.255.255.252
 tunnel source interface outside
 tunnel destination 10.20.20.20
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile PROPOSAL_IKEV2_TSET
```

4. 配置静态路由或动态路由协议：
   添加静态路由或配置动态路由协议以通过隧道接口路由流量。在此场景中，我们使用静态路由。

   静态路由：

```
route VPN-BRANCH 172.16.10.0 255.255.255.0 10.1.1.10
```

验证

在使用思科ASA上的虚拟隧道接口(VTI)从基于策略的VPN迁移到基于路由的VPN后，验证隧道是否已启用并正常运行至关重要。以下是几个步骤和命令，您可以使用这些步骤和命令来验证状态并进行故障排除（如有必要）。

1. 检验隧道接口
检查隧道接口的状态以确保其处于启用状态。

<#root>

```
ciscoasa# show interface Tunnel1


Interface Tunnel1 "VPN-BRANCH", is up, line protocol is up


Hardware is Virtual Tunnel Interface
Description: IPsec VPN Tunnel to Remote Site
Internet address is

10.1.1.2/24


MTU 1500 bytes, BW 10000 Kbit/sec, DLY 500000 usec
65535 packets input, 4553623 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
65535 packets output, 4553623 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops

Tunnel source 10.10.10.10, destination 10.20.20.20


Tunnel protocol/transport IPSEC/IP
Tunnel protection

IPsec profile PROPOSAL_IKEV2_TSET
```

此命令提供有关隧道接口的详细信息，包括其运行状态、IP地址和隧道源/目标。请查找以下指示符：

· 接口状态为up。
· 线路协议状态为up。

2. 检验IPsec安全关联(SA)

检查IPsec SA的状态，确保已成功协商隧道。

```
<#root>

ciscoasa# show crypto ipsec sa

interface: Tunnel1
Crypto map tag: Tunnel1-head-0, seq num: 1, local addr:

10.10.10.10


local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer:

10.20.20.20
```

#pkts encaps: 1000, #pkts encrypt: 1000, #pkts digest: 1000

#pkts decaps: 1000, #pkts decrypt: 1000, #pkts verify: 1000

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 1000, #pkts compr. failed: 0, #pkts decompress failed: 0

local crypto endpt.:

10.10.10.10

/500, remote crypto endpt.:

10.20.20.20

/500
path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: 0xC0A80101(3232235777)
current inbound spi : 0xC0A80102(3232235778)

inbound esp sas:

spi: 0xC0A80102(3232235778)

transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: CSR:1, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (kB/sec): (4608000/3540)
IV size: 16 bytes
replay detection support: Y

Status: ACTIVE

outbound esp sas:

spi: 0xC0A80101(3232235777)

transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={Tunnel, }
slot: 0, conn id: 2002, flow_id: CSR:2, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (kB/sec): (4608000/3540)
IV size: 16 bytes
replay detection support: Y

Status: ACTIVE

此命令显示IPsec SA的状态，包括封装的数据包和解封数据包的计数器。请确保：
· 隧道有活动SA。
· 封装和解封计数器增加，表示流量。

有关更多详细信息，您可以使用：

<#root>

```
ciscoasa# show crypto ikev2 sa

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE

, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
3363898555

10.10.10.10/500 10.20.20.20/500 READY INITIATOR

Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/259 sec
```

此命令显示IKEv2 SA的状态，处于READY状态。

3. 检验路由
检查路由表以确保路由通过隧道接口正确指向。

<#root>

```
ciscoasa# show route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF Intra, IA - OSPF Inter, E1 - OSPF External Type 1
E2 - OSPF External Type 2, N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
i - IS-IS, su - IS-IS summary null, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

S 0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside

C 10.1.1.0 255.255.255.0 is directly connected, Tunnel1

S 172.16.10.0 255.255.255.0 [1/0] via 10.1.1.10, Tunnel1
```

查找通过隧道接口路由的路由。

故障排除

本部分提供的信息可用于对配置进行故障排除。

1. 验证ASA的基于路由的隧道配置。

2. 要排除IKEv2隧道故障，可以使用以下调试：

```
debug crypto condition peer <peer IP address>
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
```

3. 要排除ASA上的流量问题，请捕获数据包并检查配置。

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）。