使用IKEv2多密钥交换在两台ASA之间配置站点到站点IKEv2隧道

目录

- 先决条件
  - 要求
  - 使用的组件
  - 限制
  - 许可
- 背景信息
  - 需要额外的密钥交换
- 配置
  - 网络图
  - ASA 配置
    - 配置ASA接口
    - 使用多密钥交换配置IKEv2策略并在外部接口上启用IKEv2
    - 配置隧道组
    - 配置相关流量和加密ACL
    - 配置身份NAT（可选）
    - 配置IKEv2 IPSec提议
    - 配置加密映射并将其绑定到接口
  - 本地ASA最终配置
  - 远程ASA最终配置
- 验证
- 故障排除

简介

本文档介绍如何使用IKEv2多密钥交换在两个思科ASA之间配置站点到站点IKEv2 VPN连接。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科自适应安全设备(ASA)

- 一般IKEv2概念

使用的组件

本文档中的信息基于运行9.20.1的Cisco ASA。

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。

限制

IKEv2多密钥交换具有以下限制：

- 仅ASA CLI支持
- 在多情景和HA设备上受支持
- 集群设备不支持

许可

许可要求与ASA上的站点到站点VPN的许可要求相同。

背景信息

需要额外的密钥交换

大量子计算机的出现给安全系统带来了巨大的风险，尤其是那些使用公钥密码系统的系统。量子计算机可以轻易地破坏那些被认为对常规计算机来说非常困难的密码方法。因此，需要切换到新的量子抗性方法，也称为后量子密码术(PQC)算法。目的是通过使用多个密钥交换来增强IPsec通信的安全性。这涉及将传统密钥交换和后量子密钥交换相结合。此方法可确保产生的交换至少与传统密钥交换一样强大，从而增加一层安全性。

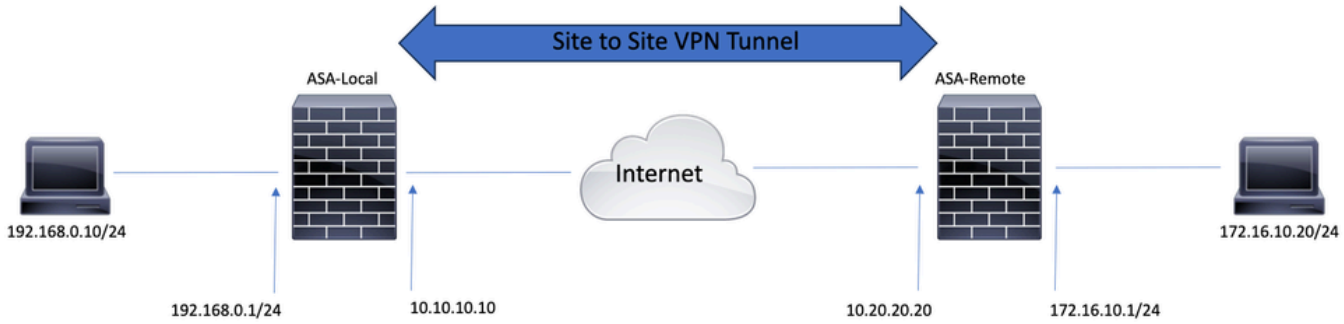
计划通过添加对多个密钥交换的支持来改进IKEv2。这些额外的密钥交换可以处理免受量子威胁的算法。为了交换有关这些附加密钥的信息，引入了一种称为中间交换的新消息类型。这些密钥交换使用常规IKEv2方法通过SA负载进行协商。

配置

本节介绍ASA配置。

网络图

本文档中的信息使用以下网络设置：



ASA 配置

配置ASA接口

如果未配置ASA接口，请确保至少配置IP地址、接口名称和安全级别：

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
```

注意：确保与内部和外部网络都有连接，尤其是与用于建立站点到站点VPN隧道的远程对等体都有连接。您可以使用ping检验基本连通性。

使用多密钥交换配置IKEv2策略并在外部接口上启用IKEv2

要为这些连接配置IKEv2策略，请输入以下命令：

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

crypto ikev2 policy 可使用命令在配置其他密钥交换转换additional-key-exchange中。总共可以配置七种额外的exchange转换。在本例中，配置了另外两个交换转换（使用DH组21和31）。

```
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
```

最终的IKEv2策略如下所示：

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
```



注意：当来自两个对等体的两个策略包含相同的身份验证、加密、哈希、Diffie-Hellman参数和其他密钥交换参数值时，存在IKEv2策略匹配。

必须在终止VPN隧道的接口上启用IKEv2。通常，这是外部（或互联网）接口。要启用IKEv2，请在全局配置模式下输入命令crypto ikev2 enable outside。

配置隧道组

对于站点到站点隧道，连接配置文件类型为IPSec-l2l。要配置IKEv2预共享密钥，请输入以下命令：

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

配置相关流量和加密ACL

ASA使用访问控制列表(ACL)来区分必须使用IPSec加密保护的流量和不需要保护的流量。它保护与permit Application Control Engine(ACE)匹配的出站数据包，并确保与permit ACE匹配的入站数据包具有保护。

```
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
```



注意：VPN对等体必须具有镜像格式的同一ACL。

配置身份NAT（可选）

通常，需要身份NAT以防止相关流量到达动态NAT。在这种情况下，配置的身份NAT为：

```
nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup
```

配置IKEv2 IPSec提议

IKEv2 IPSec建议用于定义一组加密和完整性算法以保护数据流量。为了成功构建IPSec SA，此建议必须匹配两个VPN对等体。本例中使用的命令如下：

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

配置加密映射并将其绑定到接口

加密映射组合了所有必需的配置，并且必须包含：

- 匹配必须加密的流量（通常称为加密ACL）的访问列表
- 对等体识别
- 至少一个IKEv2 IPSec提议

此处使用的配置如下：

```
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.20.20.20
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
```

最后一部分是使用命令将此加密映射应用到外部（公共）接口crypto map outside_map interface outside。

本地ASA最终配置

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
!
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
```

```
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
!
crypto ikev2 enable outside
!
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
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
!
nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
!
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.20.20.20
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
!
crypto map outside_map interface outside
```

远程ASA最终配置

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.20.20.20 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 172.16.10.1 255.255.255.0
!
crypto ikev2 policy 10
encryption aes-256
integrity sha256
group 20
prf sha256
lifetime seconds 86400
additional-key-exchange 1
```

```
key-exchange-method 21
additional-key-exchange 2
key-exchange-method 31
!
crypto ikev2 enable outside
!
tunnel-group 10.10.10.10 type ipsec-l2l
tunnel-group 10.10.10.10 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco
ikev2 local-authentication pre-shared-key cisco
!
object-group network local-network
network-object 172.16.10.0 255.255.255.0
!
object-group network remote-network
network-object 192.168.0.0 255.255.255.0
!
access-list asa-vpn extended permit ip object-group local-network object-group remote-network
!
nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
protocol esp encryption aes-256
protocol esp integrity sha-256
!
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.10.10.10
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
!
crypto map outside_map interface outside
```



注意：ACL采用镜像格式，两端预共享密钥相同。

验证

在验证隧道是否启用以及是否正在传递流量之前，必须确保相关流量将发送到ASA。



注意：使用Packet Tracer来模拟流量。可以使用packet-tracer命令完成此操作；packet-tracer input inside icmp 192.168.0.11 8 0 172.16.10.11，详见本地ASA。

要验证其他密钥交换，您可以使用命令show crypto ikev2 sa。如输出所示，您可以检查AKE参数以验证所选交换算法。

<#root>

```
Local-ASA# show crypto ikev2 sa

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf     Status        Role
  246015 10.10.10.10/500        10.20.20.20/500                     READY    INITIATOR
    Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:20, Auth sign: PSK, Auth verify: PSK
    Additional Key Exchange Group:

AKE1: 21 AKE2: 31


      Life/Active Time: 86400/7 sec
Child sa: local selector  192.168.0.0/0 - 192.168.0.255/65535
          remote selector 172.16.10.0/0 - 172.16.10.255/65535
          ESP spi in/out: 0xf41ca3b5/0xda0e693b
```

故障排除

上述调试可用于对IKEv2隧道进行故障排除：

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
```



注意：如果您希望仅排除一个隧道的故障（如果设备处于生产中则必须如此），则必须使用debug crypto condition peer X.X.X.X命令有条件地启用调试。

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）。