远程访问 IPsec VPN

远程访问 IPsec VPN 概述

远程访问 VPN 使用户可以通过安全的 TCP/IP 网络连接与中心站点相连接。互联网安全关联和密钥管理协议（又称为 IKE）是一种协商协议，让远程 PC 上的 IPsec 客户端和 ASA 可以协商如何构建 IPSec 安全关联。每个 ISAKMP 协商分为两个部分，分别称为阶段 1 和阶段 2。

阶段 1 创建第一条隧道，用于保护随后的 ISAKMP 协商消息。阶段 2 创建的隧道用于保护通过安全连接传输的数据。

如要设置 ISAKMP 协商条款，可以创建 ISAKMP 策略。ISAKMP 策略包括以下部分：

- 身份验证方法，用于确保对等体的身份。
- 加密方法，用于保护数据并确保隐私。
- 散列消息身份验证代码 (HMAC) 方法，用于确保发送方的身份，以及确保消息在传输过程中未发生修改。
- Diffie-Hellman 群，用于设置加密密钥的大小。
- ASA 在更换加密密钥前可使用该加密密钥的时长限制。

转换集由加密方法和身份验证方法组成。在与 ISAKMP 进行 IPsec 安全关联协商期间，对等体同意使用特定转换集来保护特定数据流。转换集对于两个对等体必须相同。

转换集保护关联的加密映射条目中指定的 ACL 的数据流。您可以在 ASA 配置中创建转换集，然后在加密映射条目或动态加密映射条目中指定最多 11 个转换集。有关更多概述信息（包括有效的加密方法和身份验证方法的列表），请参阅本指南创建 IKEv1 转换集或 IKEv2 提议，第 6 页。

通过在 ASA 上创建内部地址池，或者通过向 ASA 上的本地用户分配专用地址，您可以将 ASA 配置为向 Secure Client分配 IPv4 地址和/或 IPv6 地址。

终端必须已在其操作系统中实现双栈协议，才有资格分配得到这两种地址。在上述两种场景中，如果没有 IPv6 地址池但有 IPv4 地址可用，或者没有 IPv4 地址池但有 IPv6 地址可用，仍会进行连接。但是，不会通知客户端；因此，管理员必须查看 ASA 日志才能了解详细信息。

SSL 协议支持向客户端分配 IPv6 地址。

关于 Mobike 和远程访问 VPN

移动 IKEv2 (mobike) 将扩展 ASA RA VPN 以支持移动设备漫游。此支持意味着移动设备 IKE/IPSEC 安全关联 (SA) 的终端 IP 地址在该设备从其当前连接点移至其他连接点时可以更新而不是直接删除。

默认情况下，Mobike 可在 ASA 版本 9.8(1) 以及更高版本中使用，这意味着 Mobike“始终可用”。只有当客户端提议且 ASA 接受 Mobike 时，才可针对每个 SA 启用 Mobike。此协商作为 IKE_AUTH 交换的一部分予以执行。

在系统启用 mobike 支持的情况下建立 SA 后，客户端可以随时更改其地址，并使用 INFORMATIONAL 交换通知 ASA， 以 UPDATE_SA_ADDRESS 负载指示新地址。ASA 将处理此消息，然后使用新的客户端 IP 地址更新 SA。

注释 您可以使用 `show crypto ikev2 sa detail` 命令确定是否针对当前所有 SA 启用了 mobike。

当前 Mobike 实施在以下方面提供支持：

- 仅限 IPv4 地址
- NAT 映射更改
- 路径连接和故障检测，通过可选的返回路由能力检查来执行
- 主用/备用故障转移
- VPN 负载均衡

如果返回路由能力检查 (RRC) 功能已启用，则系统会在更新 SA 之前，向移动客户端发送 RRC 消息确认新的 IP 地址。

Cisco Secure 客户端的 AnyConnect VPN 模块的许可要求

注释 此功能不适用于无负载加密型号。

如果要从 Cisco Secure Firewall ASA 前端部署 Cisco Secure 客户端（包括 AnyConnect）并使用 VPN 和 Cisco Secure Firewall Posture 或 HostScan 模块，则需要 Advantage 或 Premier 许可证。提供试用许可证。请参阅《Cisco Secure 客户端订购指南》。有关每个型号的最大值，请参阅思科 ASA 系列功能许可证。

远程访问 IPsec VPN 的限制

- 防火墙模式准则 - 仅在路由防火墙模式中受支持。不支持透明模式。
- 故障转移准则 - 仅在主用/备用故障转移配置中复制 IPsec VPN 会话。不支持主用/主用故障转移配置。
- 在 HA 同步期间，配置更改会被阻止。如果用户在此期间尝试登录，防火墙中的 DACL 规则安装可能会失败。完成 HA 同步后，用户即可成功登录。
- 如果第三方客户端发送空用户代理，ASA 不接受远程访问 VPN 会话。
- 对解析到多个频繁变化的 IP 地址的域使用完全限定域名 (FQDN) 访问控制列表 (ACL)，会影响远程访问 VPN 环境中 DHCP 地址的解析。如果配置了外部 DHCP 服务器并启用了网络地址转换 (NAT) 事务提交，则可能会出现此问题。
- 使用高级终端评估进行终端安全评估可能会生成 SSL 连接系统日志消息，并且 不会与 VPN 登录或注销事件相关联。
- 由于 ASA 不会终止任何 EAP 方法，因此无法进行本地身份验证。

  ASA 仅支持 EAP 作为传递，并要求对 VPN 客户端进行证书身份验证以进行客户端的 EAP 身份验证。将 EAP 配置为远程身份验证方法时，请确保为 VPN 客户端配置证书身份验证。即使同时配置了 EAP、PSK 或证书等多个远程身份验证方法，也会显示错误。

配置远程访问 IPsec VPN

本章介绍如何配置远程访问 VPN。

配置接口

一个ASA至少有两个接口，在本指南中分别将它们称为外部接口和内部接口。通常，外部接口连接到公共互联网，内部接口连接到专用网络且不接受公共访问。

首先，请在ASA上配置并启用两个接口。然后，为接口分配名称、IP地址和子网掩码。或者，在安全设备上配置接口的安全级别、速度和双工操作。

过程

步骤 1 从全局配置模式进入接口配置模式：

interface {*interface*}

示例：

```
hostname(config)# interface ethernet0
hostname(config-if)#
```

步骤 2 设置接口的 IP 地址和子网掩码：

ip address *ip_address* [*mask*] [*standby ip_address*]

示例：

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
```

步骤 3 为接口指定名称（最多包含 48 个字符）。设置此名称后，不能对其进行更改。

nameif *name*

示例：

```
hostname(config-if)# nameif outside
hostname(config-if)#
```

步骤 4 启用接口。默认情况下，接口处于禁用状态。

示例：

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

在外部接口上配置 ISAKMP 策略和启用 ISAKMP

过程

步骤 1 指定要在 IKEv1 协商过程中使用的身份验证方法和一组参数。

Priority 唯一标识互联网密钥交换 (IKE) 策略并向该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。

在后续步骤中，我们将优先级设置为 1。

步骤 2 指定要在 IKE 策略中使用的加密方法：

crypto ikev1 policy *priority* **encryption** {**aes-192** | **aes-256** | | }

示例：

步骤 3 为 IKE 策略指定散列算法（又称为 HMAC 变体）：

crypto ikev1 policy *priority* **hash** { | **sha**}

示例：

```
hostname(config)# crypto ikev1 policy 1 hash sha
hostname(config)#
```

步骤 4 为 IKE 策略指定 Diffie-Hellman 群 - 支持 IPsec 客户端与 ASA 建立共享密钥的加密协议：

crypto ikev1 policy *priority* **group** {**14** | | | **19** | **20** | 21}

示例：

```
hostname(config)#crypto ikev1 policy 1 group 14
hostname(config)#
```

步骤 5 指定加密密钥生命周期 - 每个安全关联在到期之前应存在的时长，以秒为单位：

crypto ikev1 policy *priority* **lifetime** {*seconds*}

有限生命周期为 120 到 2147483647 秒。要设置无限生命周期，请使用 0 秒。

示例：

```
hostname(config)# crypto ikev1 policy 1 lifetime 43200
hostname(config)#
```

步骤 6 在名为 outside 的接口上启用 ISAKMP：

crypto ikev1 enable *interface-name*

示例：

```
hostname(config)# crypto ikev1 enable outside
hostname(config)#
```

步骤 7 保存对配置的更改：

write memory

配置地址池

ASA 需要有用于向用户分配 IP 地址的方法。本节以地址池为例。

过程

使用一系列 IP 地址创建地址池，ASA 会从该地址池向客户端分配地址。

ip local pool *poolname first-address—last-address* [**mask** *mask*]

地址掩码是可选的。但是，如果将 IP 地址分配给属于非标准网络的 VPN 客户端，则必须提供掩码值；如果使用默认掩码，数据路由可能会出错。这种情况的一个典型例子是本地 IP 地址池包含 10.10.10.0/255.255.255.0 地址，因为默认情况下这是 A 类网络。当 VPN 客户端需要通过不同接口访问 10 网络中的不同子网时，可能会导致路由问题。

示例：

```
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)#
```

添加用户

过程

为用户创建用户、密码和权限级别：

username *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*]

示例：

```
Hostname(config)# username testuser password 12345678
```

创建 IKEv1 转换集或 IKEv2 提议

本节介绍如何配置转换集(IKEv1) 或提议 (IKEv2)（由加密方法和身份验证方法组成）。

以下步骤显示如何创建 IKEv1 和 IKEv2 提议。

过程

步骤 1 配置 IKEv1 转换集，用于指定为确保数据完整性而要使用的 IPsec IKEv1 加密和散列算法。

crypto ipsec ikev1 transform-set *transform-set-name encryption-method* [*authentication*]

对 encryption 使用以下其中一个值：

- esp-aes 使用带 128 位密钥的 AES。
- esp-aes-192 使用带 192 位密钥的 AES。
- esp-aes-256 使用带 256 位密钥的 AES。
- esp-null 不使用加密。

对 authentication 使用以下其中一个值：

- esp-md5-hmac 使用 MD5/HMAC-128 作为散列算法。
- esp-sha-hmac 使用 SHA/HMAC-160 作为散列算法。
- esp-none 不使用 HMAC 身份验证。

示例：

要使用 AES 配置 IKEv1 转换集：

```
hostname(config)# crypto ipsec transform set FirstSet esp-aes esp-sha-hmac
```

步骤 2 配置 IKEv2 提议集，用于指定要使用的 IPsec IKEv2 协议、加密和完整性算法。

esp 指定封装安全负载 (ESP) IPsec 协议（目前唯一支持的 IPsec 协议）。

crypto ipsec ikev2 ipsec-proposal *proposal_name*

protocol {**esp**} {**encryption** { | | **aes** | **aes-192** | **aes-256** | } | **integrity** { | **sha-1**}

对 encryption 使用以下其中一个值：

- aes - 对 ESP 结合使用 AES（默认）和 128 位密钥加密。
- aes-192 - 对 ESP 结合使用 AES 和 192 位密钥加密。
- aes-256 - 对 ESP 结合使用 AES 和 256 位密钥加密。

对 integrity 使用以下其中一个值：

- sha-1 （默认）为 ESP 完整性保护指定美国联邦信息处理标准 (FIPS) 中定义的安全散列算法 (SHA) SHA-1。

如要配置 IKEv2 提议，请使用以下命令：

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure_proposal

hostname(config-ipsec-proposal)# protocol esp encryption aes intergrity sha-1
```

定义隧道组

隧道组是一组隧道连接策略。您可以配置隧道组来标识AAA服务器，指定连接参数，以及定义默认组策略。ASA 会在内部存储隧道组。

ASA 系统中有两个默认隧道组：DefaultRAGroup 和 DefaultL2Lgroup，前者是默认的远程访问隧道组，后者是默认的LAN间隧道组。可以更改这些组，但不能将其删除。如果在隧道协商过程中没有标识特定隧道组，ASA 将会使用这两个隧道组来配置远程访问隧道组和 LAN 间隧道组的默认隧道参数。

过程

步骤 1 创建 IPsec 远程访问隧道组（又称为连接配置文件）：

tunnel-group *name* **type** *type*

示例：

```
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)#
```

步骤 2 进入隧道组常规属性模式（在该模式下可输入身份验证方法）：

tunnel-group *name* **general-attributes**

示例：

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#
```

步骤 3 指定要用于隧道组的地址池：

address-pool [*(interface name)*] *address_pool1* [*...address_pool6*]

示例：

```
hostname(config-general)# address-pool testpool
```

步骤 4 进入隧道组 IPsec 属性模式（在该模式下可输入用于 IKEv1 连接的 IPsec 特定属性）：

tunnel-group *name* **ipsec-attributes**

示例：

```
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-tunnel-ipsec)#
```

步骤 5 （可选） 配置预共享密钥（仅适用于 IKEv1）。该密钥可以是包含 1 到 128 个字符的字母数字字符串。

用于自适应安全设备和客户端的密钥必须相同。如果具有不同预共享密钥大小的思科VPN客户端尝试连接，该客户端将会记录错误消息，表明其无法对对等体进行身份验证。

ikev1 pre-shared-key *key*

示例：

```
hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx
```

创建动态加密映射

动态加密映射定义的策略模板并未配置所有参数。这样，ASA 就可以接受来自 IP 地址未知的对等体（例如远程访问客户端）的连接。

动态加密映射条目标识用于连接的转换集。您还可以启用反向路由，让 ASA 可以获悉所连接客户端的路由信息，并通过 RIP 或 OSPF 通告这些信息。

过程

步骤 1 创建动态加密映射并为其指定 IKEv1 转换集或 IKEv2 提议：

- 对于 IKEv1，请使用以下命令：

  crypto dynamic-map *dynamic-map-name seq-num* **set ikev1 transform-set** *transform-set-name*

- 对于 IKEv2，请使用以下命令：

  crypto dynamic-map *dynamic-map-name seq-num* **set ikev2 ipsec-proposal** *proposal-name*

示例：

```
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet
hostname(config)#

hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal secure_proposal
hostname(config)#
```

步骤 2 （可选）根据此加密映射条目为任何连接启用反向路由注入：

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse-route**

示例：

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse route
hostname(config)#
```

创建加密映射条目以使用动态加密映射

创建加密映射条目，确保 ASA 能够使用动态加密映射来设置 IPsec 安全关联的参数。

在以下命令示例中，加密映射的名称是 mymap，序号是 1，动态加密映射的名称是 dyn1（是在创建动态加密映射主体中创建的）。

过程

步骤 1 创建使用动态加密映射的加密映射条目：

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

示例：

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
```

步骤 2 将加密映射应用于外部接口：

crypto map *map-name* **interface** *interface-name*

示例：

```
hostname(config)# crypto map mymap interface outside
```

步骤 3 保存对配置的更改：

write memory

在多情景模式下配置 IPSec IKEv2 远程访问 VPN

有关远程访问 IPsec VPN 配置的详细信息，请参阅以下各节：

- 配置接口，第 3 页
- 配置地址池，第 5 页
- 添加用户，第 6 页
- 创建 IKEv1 转换集或 IKEv2 提议，第 6 页
- 定义隧道组，第 7 页
- 创建动态加密映射，第 9 页
- 创建加密映射条目以使用动态加密映射，第 9 页

使用后量子预共享密钥进行 VPN 身份验证

您可以使用新密钥（后量子预共享密钥(PPK)）和预共享密钥(PSK)配置IKEv2，以确保安全客户端和ASA之间的IPsec通信免受量子计算机攻击。您必须在客户端和ASA上配置匹配的PPK和PSK，以实现安全的IPsec连接。安全客户端和ASA使用PPK和PSK获取网络流量的加密和解密密钥。

PPK以二进制格式加密生成。对于ASA和安全客户端配置，必须将二进制PPK转换为256位64个字符的十六进制字符串。

使用后量子预共享密钥进行 VPN 身份验证的前提条件

- 许可证：ASA 必须拥有强加密许可证。
- 支持的版本

- ASA 9.18.1 及更高版本。
- 安全客户端 5.1.8 及更高版本。

- 在 ASA 上配置远程访问 IPsec/IKEv2 VPN 连接的所有其他参数，如地址池、IKEv2 提议和加密映射。
- 生成二进制 PPK。
- 将二进制 PPK 转换为 256 位 64 个字符的十六进制字符串。
- 在客户端计算机的 Windows 凭证管理器 (WCM) 中为安全客户端配置 PPK 和两个 PSK。请参阅在 Windows 凭证管理器上配置后量子预共享密钥和预共享密钥，第 12 页。
- 在安全客户端的 VPN 配置文件中配置 PPK 属性。请参阅使用后量子预共享密钥属性为安全客户端配置 VPN 配置文件，第 13 页。
- 确保 ASA 和安全客户端上的 PPK 和 PPK ID 值相同。

在 VPN 身份验证中使用后量子预共享密钥的准则和限制

准则

- 管理员必须确保 PPK 和 PSK 的生成、质量以及向每个客户端设备的分发。

限制

- 仅支持带有 PSK 和 PPK 的 IKEv2。
- 安全客户端仅支持 Windows。
- 客户端只能在 WCM 中为一个 ASA 存储凭证。

使用后量子预共享密钥进行 VPN 验证的工作流程

表 *1:* 使用后量子预共享密钥进行 *VPN* 验证的工作流程

步骤	操作	更多信息
1	生成二进制 PPK 并将其转换为 256 位 64 个字符的十六进制字符串。	-
2	在 Windows 凭证管理器 (WCM) 中配置 PPK 和 PSK。	在 Windows 凭证管理器上配置后量子预共享密钥和预共享密钥，第 12 页

步骤	操作	更多信息
3	使用 PPK 参数配置安全客户端 VPN 配置文件。	使用后量子预共享密钥属性为安全客户端配置 VPN 配置文件，第 13 页
4	配置 ASA 隧道组。	使用后量子预共享密钥在 ASA 上配置 VPN 身份验证，第 13 页
5	用户登录安全客户端以连接 ASA。	-
6	安全客户端使用 VPN 配置文件中的 PPK_ID 从 WCM 获取 PPK 和两个 PSK。	-
7	安全客户端使用 ASA 隧道组参数验证 WCM 中的 PPK 和 PSK 参数。	-
8	如果安全客户端和 ASA 的 PPK 和 PSK 匹配，则安全客户端会与 ASA 建立 VPN 连接。 如果 PPK 和 PSK 不匹配，则与 ASA 的 VPN 连接会失败。	-

在 Windows 凭证管理器上配置后量子预共享密钥和预共享密钥

您必须为 PPK、本地 PSK 和远程 PSK 配置单独的凭证条目。

开始之前

确保您查看 使用后量子预共享密钥进行 VPN 身份验证的前提条件，第 10 页 和 在 VPN 身份验证中使用后量子预共享密钥的准则和限制，第 11 页。

过程

步骤 1 在 Windows 客户端设备中，依次选择**控制面板 (Control Panel)** > **用户账户 (User Accounts)** > **凭证管理器 (Credential Manager)**。

步骤 2 点击 **Windows 凭证 (Windows Credentials)** 选项卡。

步骤 3 点击**添加通用凭证 (Add a Generic Credential)**。

步骤 4 在 **Internet 或网络地址 (Internet or network address)** 字段中，指定以下值之一：

- 对于 PPK，请将值指定为 **AC/PPK/**<HostAddress：后量子预共享密钥。它在 WCM 中存储为 64 个十六进制字符，客户端将其转换为二进制，然后在 IKEv2 的加密和解密密钥派生中包含该密钥。
- 对于本地 PSK，请将值指定为 **AC/PSK_Local/<HostAddress以表示**客户端的 PSK 配置。

- 对于远程 PSK，请将值指定为 **AC/PSK_Remote/<HostAddress**，以表示 ASA 的 PSK 配置。

步骤 5 在**用户名 (User name)** 字段中，请将值指定为**不适用**，因为安全客户端不使用该值。

步骤 6 在**密码 (Password)** 字段中，指定以下值之一：

- 对于 PPK，请指定 256 位 64 个字符的十六进制字符串。
- 对于本地和远程 PSK，请指定一个字符串来指定隧道组别名。

步骤 7 点击**确定 (OK)**。

安全客户端使用 VPN 配置文件中的 PPK_ID 从 WCM 获取 PPK 和两个 PSK。安全客户端使用上述 PPK 和 PSK 值，将 PPK 转换为二进制，将 PPK 和 PSK 值与 ASA 配置相匹配，并执行 VPN 身份验证。建立 VPN 连接不需要其他输入，因为这三个密钥就是身份验证凭证。

使用后量子预共享密钥属性为安全客户端配置 VPN 配置文件

VPN 配置文件中的 **HostEntry** 参数具有以下新字段，用于配置安全客户端的 PPK 参数：

- **IKEIdentity** - 指定用于标识对等体 ASA 的字符串。此字符串必须与 ASA 中的隧道组名称匹配。
- **PPK_ID** - 指定用于标识 PPK 的唯一字符串。该值必须与 ASA 中的 PPK ID 一致。
- **PPK_mandatory** - 如果 PPK 对于 VPN 连接为强制，则将值指定为 true。如果不配置该值，则 PPK 配置将是可选的。

示例

以下给出了 VPN 配置文件中的 HostEntry 的示例：

```
<HostEntry>
<HostName> ASAv_PPK</HostName>
<HostAddress>192.168.1.2</HostAddress>
<UserGroup>IPSec_Profile</UserGroup>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true</StandardAuthenticationOnly>
 <IKEIdentity>secure_client_PPK</IKEIdentity>
 <PPK_ID>PPKID_test</PPK_ID>
</PrimaryProtocol>
</HostEntry>
```

使用后量子预共享密钥在 ASA 上配置 VPN 身份验证

ASA 中的隧道组用于标识 VPN 连接的组策略。您可以配置隧道组策略，使用 PPK 和 PSK 启用 VPN 身份验证。

开始之前

确保您查看 使用后量子预共享密钥进行 VPN 身份验证的前提条件，第 10 页 和 在 VPN 身份验证中使用后量子预共享密钥的准则和限制，第 11 页。

过程

步骤 1 配置隧道组的 IPsec 属性。

tunnel-group *name* **ipsec-attributes**

示例：

```
hostname(config)# tunnel-group secure_client_PPK ipsec-attributes
hostname(config-tunnel-ipsec)#
```

步骤 2 配置客户端的 PSK。

ikev2 remote-authentication pre-shared-key *key*

示例：

```
hostname(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key *****
```

步骤 3 配置 ASA 的 PSK。

ikev2 local-authentication pre-shared-key *key*

示例：

```
hostname(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key *****
```

步骤 4 配置客户端的 PPK。

ikev2 remote-authentication post-quantum-key *key* **identifier** *id* mandatory

- key：指定 PPK 密钥。
- ID：指定用于标识 PPK 的唯一字符串。此值必须与安全客户端的 VPN 配置文件中的 PPK ID 匹配。
- mandatory：指定 PPK 对于 VPN 连接是否为强制。如果未指定为强制，则 PPK 配置为可选。

示例：

```
hostname(config-tunnel-ipsec)#ikev2 remote-authentication post-quantum-key  *****
 identifier PPKID_test mandatory
```

以下示例显示了 ASA 使用 PPK 和 PSK 进行隧道组配置的片段：

示例

```
tunnel-group secure_client_PPK ipsec-attributes
       ikev2 remote-authentication pre-shared-key *****
       ikev2 local-authentication pre-shared-key *****
       ikev2 remote-authentication post-quantum-key ***** identity PPKID_test mandatory
```

请注意以下提示：

- 隧道组名称必须与 VPN 配置文件的 IKEIdentity 字符串匹配。
- 隧道组配置中的 PPK ID 必须与 VPN 配置文件的 PPK_ID 相匹配。

其他参考资料

- RFC 8784
- Cisco Secure 客户端（包括 AnyConnect）管理员指南，5 版

配置门户访问规则

您可以配置全局无客户端 SSL VPN 访问策略，根据 HTTP 标头中的数据允许或拒绝无客户端 SSL VPN 会话。ASA 在验证端点之前会评估该访问策略。如果 ASA 根据访问策略拒绝无客户端 SSL VPN 会话，它会立即向端点返回错误代码。

开始之前

登录 ASA 并进入全局配置模式。

过程

步骤 1 使用以下命令进入无客户端 SSL VPN 配置模式：

webvpn

步骤 2 根据 HTTP 报头代码或 HTTP 报头中的字符串，使用以下命令允许或拒绝无客户端 SSL VPN 会话：

portal-access-rule *priority* {**permit** | **deny** [**code** *code*]} {**any** | **user-agent match** *string*}

表 *2: portal-access-rule* 命令关键字和变量

参数	说明
priority	指定规则的优先级。
permit	根据此设置允许无客户端 SSL VPN 连接。
deny	根据此设置拒绝无客户端 SSL VPN 连接。
code *code*	指定 HTTP 消息代码。范围从 200 到 599。
user-agent match *string*	指定一个字符串，用于识别请求用户代理的应用程序、操作系统、供应商和版本。

- 要指定字符串，请使用通配符(*)开始和结束字符串。如果不使用通配符，规则可能不匹配任何字符串或者匹配的字符串数量远远低于预期。例如，*Thunderbird*。
- 要指定带空格的字符串，请在字符串的开头和结尾使用通配符(*)，然后在开头和结尾加上引号(“ ”)。在第二个示例中，`my agent` 是字符串。

示例：

```
hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*
hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match “*my agent*”
```

远程访问 IPsec VPN 配置示例

以下示例显示如何配置远程访问 IPsec/IKEv1 VPN：

```
hostname(config)# crypto ikev1 policy 10
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption aes-256
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config)# crypto ikev1 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev1 transform set AES256-SHA
esp-aes-256 esp-sha-hmac
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-ipsec)# ikev1 pre-shared-key ravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev1
transform-set AES256-SHA
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

以下示例显示如何配置远程访问 IPsec/IKEv2 VPN：

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha512
hostname(config-ikev2-policy)# prf sha512
hostname(config)# crypto ikev2 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev2 ipsec-proposal  AES256-SHA512
hostname(config-ipsec-proposal)# protocol esp encryption  aes-256
hostname(config-ipsec-proposal)# protocol esp integrity sha-512
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
```

```
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-tunnel-ipsec)# ikev2 local-authentication
pre-shared-key localravpnkey
hostname(config-tunnel-ipsec)# ikev2 remote-authentication
pre-shared-key remoteravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev2
ipsec-proposal AES256-SHA512
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

多情景模式下基于标准的 IPSec IKEv2 远程访问 VPN 的配置示例

以下示例显示如何为多情景模式下基于标准的远程访问 IPsec/IKEv2 VPN 配置 ASA。示例分别提供有关系统情景配置和用户情景配置的信息。

对于系统情景配置：

```
class default
  limit-resource All 0
  limit-resource Mac-addresses 65536
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource VPN AnyConnect 4.0%
```

```
hostname(config)#context CTX2
hostname(config-ctx)#member default   ===============> License allotment for contexts using
 class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX2.cfg
```

对于用户情景配置：

```
hostname/CTX2(config)#ip local pool CTX2-pool 1.1.2.1-1.1.2.250 mask 255.255.255.0
hostname/CTX2(config)#aaa-server ISE protocol radius
hostname/CTX2(config)#aaa-server ISE (inside) host 10.10.190.100
hostname/CTX2(config-aaa-server-host)#key *****
hostname/CTX2(config-aaa-server-host)#exit
hostname/CTX2(config)#
```

```
hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 internal
hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 attributes
hostname/CTX2(config-group-policy)#vpn-tunnel-protocol ikev2
hostname/CTX2(config-group-policy)#exit
hostname/CTX2(config)#
```

```
hostname/CTX2(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
```

```
hostname/CTX2(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
hostname/CTX2(config)#crypto map outside_map interface outside
```

默认情况下，从基于标准的客户端的 IPSec/IKEv2 远程访问连接位于隧道组 DefaultRAGroup 中。

```
hostname/CTX2(config)#tunnel-group DefaultRAGroup type remote-access
hostname/CTX2(config)#tunnel-group DefaultRAGroup general-attributes
hostname/CTX2(config-tunnel-general)#default-group-policy GroupPolicy_CTX2-IKEv2
hostname/CTX2(config-tunnel-general)#address-pool CTX2-pool
hostname/CTX2(config-tunnel-general)#authentication-server-group ISE
hostname/CTX2(config-tunnel-general)#exit
hostname/CTX2(config)#
```

```
hostname/CTX2(config)#tunnel-group DefaultRAGroup ipsec-attributes
hostname/CTX2(config-tunnel-ipsec)#ikev2 remote-authentication eap query-identity
hostname/CTX2(config-tunnel-ipsec)#ikev2 local-authentication certificate ASDM_TrustPoint0
hostname/CTX2(config-tunnel-ipsec)#exit
hostname/CTX2(config)#
```

多情景模式下 Secure Client IPSec IKEv2 远程访问 VPN 的配置示例

以下示例显示如何为多情景模式下 Secure Client 远程访问 IPsec/IKEv2 VPN 配置 ASA。示例分别提供有关系统情景配置和用户情景配置的信息。

对于系统情景配置：

```
class default
    limit-resource All 0
    limit-resource Mac-addresses 65536
    limit-resource ASDM 5
    limit-resource SSH 5
    limit-resource Telnet 5
    limit-resource VPN AnyConnect 4.0%
```

```
hostname(config)#context CTX3
hostname(config-ctx)#member default   ===============> License allotment for contexts using
 class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX3.cfg
```

每种情景的虚拟文件系统创建都会包含 Secure Client 文件，例如映像和配置文件。

```
hostname(config-ctx)#storage-url shared disk0:/shared disk0
```

对于用户情景配置：

```
hostname/CTX3(config)#ip local pool ctx3-pool 1.1.3.1-1.1.3.250 mask 255.255.255.0
hostname/CTX3(config)#webvpn
hostname/CTX3(config-webvpn)#enable outside
hostname/CTX3(config-webvpn)# anyconnect image
disk0:/anyconnect-win-4.6.00010-webdeploy-k9.pkg 1
```

```
hostname/CTX3(config-webvpn)#anyconnect profiles IKEv2-ctx1 disk0:/ikev2-ctx1.xml
hostname/CTX3(config-webvpn)#anyconnect enable
hostname/CTX3(config-webvpn)#tunnel-group-list enable


hostname/CTX3(config)#username cisco password *****
hostname/CTX3(config)#ssl trust-point ASDM_TrustPoint0 outside
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 internal
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 attributes


hostname/CTX3(config-group-policy)#vpn-tunnel-protocol ikev2 ssl-client
hostname/CTX3(config-group-policy)#dns-server value 10.3.5.6
hostname/CTX3(config-group-policy)#wins-server none
hostname/CTX3(config-group-policy)#default-domain none
hostname/CTX3(config-group-policy)#webvpn
hostname/CTX3(config-group-webvpn)#anyconnect profiles value IKEv2-ctx1 type user
```

在以下示例中，要启用客户端服务，请使用 **crypto ikev2 enable outside client-services** 命令。

客户端服务服务器提供 HTTPS (SSL) 访问，以允许安全客户端下载程序接收软件升级、配置文件、本地化和自定义文档、CSD、SCEP以及客户端所需的其他文件下载。如果选择此选项，请指定客户端服务端口号。如果不启用客户端服务服务器，用户将无法下载安全客户端可能需要的任何文件。

注释 您可以使用与在同一设备上运行的SSL VPN相同的端口。即使配置了SSL VPN，您也必须选择此选项，以便通过 SSL 为 IPsec-IKEv2 客户端启用文件下载。

```
hostname/CTX3(config)#crypto ikev2 enable outside client-services port 443
hostname/CTX3(config)#crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
hostname/CTX3(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX3(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
hostname/CTX3(config)#crypto map outside_map interface outside


hostname/CTX3(config)#tunnel-group CTX3-IKEv2 type remote-access
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 general-attributes
hostname/CTX3(config-tunnel-general)#default-group-policy GroupPolicy_CTX3-IKEv2
hostname/CTX3(config-tunnel-general)#address-pool ctx3-pool
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 webvpn-attributes
hostname/CTX3(config-tunnel-webvpn)#group-alias CTX3-IKEv2 enable
```

远程访问 VPN 的功能历史记录

功能名称	版本	功能信息
用于 IPsec IKEv1 和 SSL 的远程访问 VPN。	7.0	远程访问 VPN 使用户可以通过安全的 TCP/IP 网络连接（例如互联网）连接到中心站点。

功能名称	版本	功能信息
用于 IPsec IKEv2 的远程访问 VPN。	8.4(1)	添加了对 Secure Client 的 IPsec IKEv2 支持。
远程访问 VPN 的 mobike 自动支持。	9.8(1)	添加了 IPsec IKEv2 RA VPN 的移动 IKE (mobike) 支持。Mobike 始终开启。 添加了 `ikev2 mobike rrc` 命令以在 IKEv2 RA VPN 连接的 mobike 通信期间启用返回路由能力检查。
多情景模式下 IPsec IKEv2 的远程访问 VPN	9.9(2)	支持配置 ASA，以允许 Secure Client 和基于标准的第三方 IPSec IKEv2 VPN 客户端建立远程访问 VPN 会话，连接到以多情景模式运行的 ASA。 添加了 `ikev2 rsa-sig-hash sha1` 命令，以便对身份验证负载进行签名。
使用 SHA-1 散列算法的 RSA，用于对身份验证负载签名	9.12(1)	在使用第三方基于标准的 IPSec IKEv2 VPN 客户端与 ASA 建立远程访问 VPN 会话时，支持使用 SHA-1 散列算法来对身份验证负载进行签名。
弃用 IKE/IPsec 加密和完整性/PRF 密码 对 IKEv1 的 DH 组 14 支持	9.13(1)	以下加密/完整性/PRF 密码已弃用，并将在后续版本 - 9.14(1) 中删除： • 3DES 加密 • DES 加密 • MD5 完整性 添加了对 IKEv1 的 DH 组 14（默认）支持。group 2 和 group 5 命令选项已弃用，并将在后续版本 9.14(1) 中删除。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。