【MVS】Cisco IPsec VPN 的预共享密钥crypto keyring 与 cryto isakmp key 两种配置方法的区别?

VPN技术 胡伟 2024-08-05 发表

问题描述

【MVS】Cisco IPsec VPN 的预共享密钥crypto keyring 与 cryto isakmp key两种配置方法的区别?

解决方法

在 Cisco IOS 设备上，crypto keyring 和 crypto isakmp key 都是用于配置 IPsec VPN 的预共享密钥（Pre-Shared Key, PSK），但它们有不同的使用场景和细节。下面让我们详细比较这两个配置命令，以帮助你理解何时使用它们。

crypto isakmp key

crypto isakmp key 命令是用于配置IPsec VPN的简单预共享密钥。这种方法较为简单，适用于不需要复杂配置的简单VPN环境。每个预共享密钥与一个特定的对等体关联。

示例配置

```
router(config)# crypto isakmp key MYSECRETKEY address 192.0.2.1
```

在这个例子中，MYSECRETKEY 是预共享密钥，而 192.0.2.1 是对等体的IP地址。

要点

- **简单直接**：适合于简单的VPN设置或只有少量对等体的VPN配置。
- **默认全局使用**：预共享密钥在全局范围内可用，不适用于VRF。

crypto keyring

crypto keyring 命令提供了一个更加灵活和组织良好的方式来管理预共享密钥。它允许你创建一个密钥环（keyring），其中包含一个或多个预共享密钥条目。同时，可以将密钥环关联到特定的虚拟路由转发（VRF）实例，以便更好地支持多租户环境或复杂网络结构。

示例配置

```
router(config)# crypto keyring MY_KEYRING vrf WAN
router(config-keyring)# pre-shared-key address 192.0.2.1 key MYSECRETKEY
router(config-keyring)# exit
```

在这个例子中，我们创建了一个名为 MY_KEYRING 的密钥环，并将其关联到一个名为 WAN 的 VRF。然后，我们为特定的对等体 192.0.2.1 配置了预共享密钥 MYSECRETKEY。

要点

- **灵活性**：支持多对等体和Pre-Shared Key管理，更适合于复杂的VPN环境。
- **支持VRF**：密钥环可以与特定的VRF关联，适用于多租户环境。
- **组织良好**：通过密钥环，可以更直观地管理和查看多个预共享密钥。

选择使用哪种方法

选择使用哪种方法主要取决于你的具体需求和网络环境的复杂性：

- 如果你的VPN配置较为简单，网络设备间的连接较少，并且不需要VRF支持，那么使用 crypto isakmp key 可能更为直接和简单。
- 如果你需要管理多个对等体的连接，或者你使用的是带有VRF的复杂网络环境，那么 crypto keyring 将提供更多的灵活性和更好的组织能力。

使用方案示例

简单VPN环境使用 crypto isakmp key

适用于小型或简单的VPN配置，比如一个企业内部的站点到站点VPN连接。

```
router(config)# crypto isakmp policy 10
router(config-isakmp)# encryption aes
router(config-isakmp)# hash sha
router(config-isakmp)# group 2
router(config-isakmp)# exit
```

```
router(config)# crypto isakmp key MYSECRETKEY address 192.0.2.1

router(config)# crypto ipsec transform-set TSET esp-aes 256 esp-sha-hmac
router(config)# crypto map MYMAP 10 ipsec-isakmp
router(config-crypto-map)# set peer 192.0.2.1
router(config-crypto-map)# set transform-set TSET
router(config-crypto-map)# match address 101
router(config-crypto-map)# exit

router(config)# interface GigabitEthernet0/0
router(config-if)# crypto map MYMAP
```

复杂VPN环境使用 crypto keyring

适用于复杂的企业网络、服务提供商网络或多租户环境。

```
router(config)# vrf definition WAN
router(config-vrf)# rd 1:1
router(config-vrf)# exit

router(config)# crypto keyring MY_KEYRING vrf WAN
router(config-keyring)# pre-shared-key address 192.0.2.1 key MYSECRETKEY
router(config-keyring)# exit

router(config)# crypto isakmp policy 10
router(config-isakmp)# encryption aes
router(config-isakmp)# hash sha
router(config-isakmp)# group 2
router(config-isakmp)# exit

router(config)# crypto isakmp profile MY_PROFILE
router(config-isakmp-profile)# keyring MY_KEYRING
router(config-isakmp-profile)# match identity address 192.0.2.1 255.255.255.255
router(config-isakmp-profile)# exit

router(config)# crypto ipsec transform-set TSET esp-aes 256 esp-sha-hmac
router(config)# crypto ipsec profile MY_IPSEC_PROFILE
router(config-ipsec-profile)# set transform-set TSET
router(config-ipsec-profile)# set isakmp-profile MY_PROFILE
router(config-ipsec-profile)# exit

router(config)# interface GigabitEthernet0/0
router(config-if)# tunnel protection ipsec profile MY_IPSEC_PROFILE
```

总结

crypto isakmp key 和 crypto keyring 都用于配置预共享密钥，但它们的适用场景有所不同。crypto isakmp key 适合于简单的VPN环境，而 crypto keyring 则提供了更多的灵活性和组织能力，更适用于复杂的、多对等体的VPN配置，特别是在需要VRF支持的情况下。通过理解和选择适合的方法，你可以更有效地配置和管理IPsec VPN。