

使用 ISAKMP 配置文件的 DMVPN 和 Easy VPN 服务器配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文描述如何在同一路由器上用 Xauth 配置 Dynamic Multipoint VPN (DMVPN) 和 Easy VPN。此设置适合要动态寻址的 DMVPN 分支。互联网安全协会和密钥管理协议 (ISAKMP) 配置文件能够分离动态寻址 DMVPN spoke 或 Easy VPN 客户端的认证方法。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行 Cisco IOS® 软件版本 12.3(3) 和 12.3(3)a 的 Cisco 2691 和 3725 路由器

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

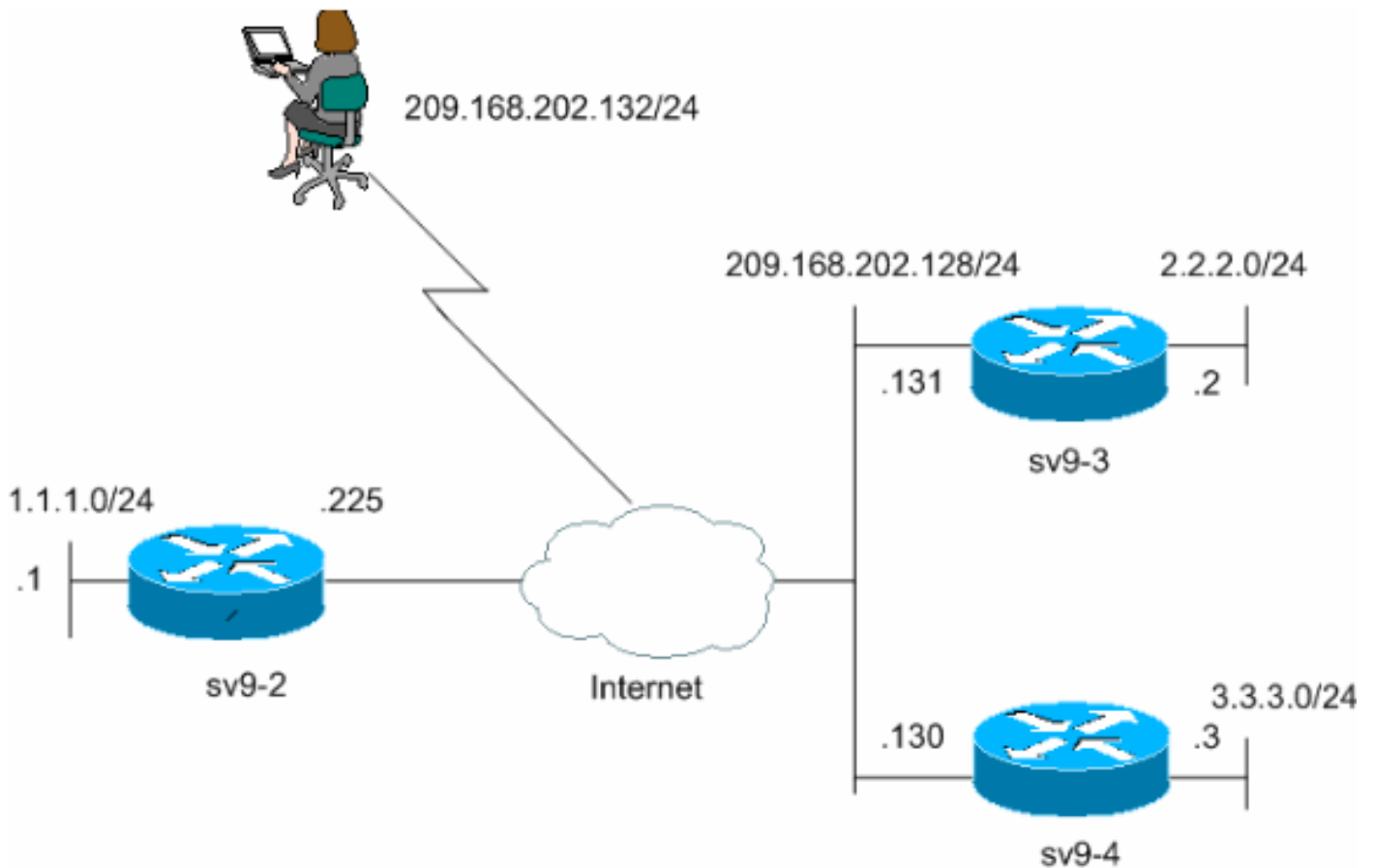
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 有关本文档所用命令的详细信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

网络图

本文档使用此网络设置。



配置

本文档使用以下配置。

- [sv9-2 中心配置](#)
- [sv9-3 分支配置](#)
- [sv9-4 分支配置](#)

sv9-2 中心配置

```
sv9-2#show run
Building configuration...

Current configuration : 2876 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname sv9-2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
username cisco password 0 cisco
aaa new-model
!
!
!--- Xauth is configured for local authentication. aaa
authentication login userauthen local
aaa authorization network hw-client-groupname local
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!--- Keyring that defines the wildcard pre-shared key.
crypto keyring dmvpnspokes
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!

!--- Create an ISAKMP policy for Phase 1 negotiations.
!--- This policy is for DMVPN spokes. crypto isakmp
policy 10
hash md5
authentication pre-share
!

!--- Create an ISAKMP policy for Phase 1 negotiations.
!--- This policy is for Easy VPN Clients. crypto isakmp
policy 20
hash md5
authentication pre-share
group 2
!

!--- VPN Client configuration for group "hw-client-
groupname" !--- (this name is configured in the VPN
Client). crypto isakmp client configuration group hw-
client-groupname
key hw-client-password
dns 1.1.11.10 1.1.11.11
wins 1.1.11.12 1.1.11.13
domain cisco.com
pool dynpool

!--- Profile for VPN Client connections, matches the !--
```

```
- "hw-client-group" group and defines the XAuth
properties. crypto isakmp profile VPNclient
match identity group hw-client-groupname
client authentication list userauthen
isakmp authorization list hw-client-groupname
client configuration address respond

!--- Profile for LAN-to-LAN connection, references !---
the wildcard pre-shared key and a wildcard !--- identity
(this is what is broken in !--- Cisco bug ID CSCea77140)
!--- and no XAuth. crypto isakmp profile DMVPN
keyring dmvpnsokes
match identity address 0.0.0.0
!
!

!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set strong esp-3des
esp-md5-hmac
mode transport
!

!--- Create an IPsec profile to be applied dynamically
to the !--- generic routing encapsulation (GRE) over
IPsec tunnels. crypto ipsec profile cisco
set security-association lifetime seconds 120
set transform-set strong
set isakmp-profile DMVPN
!
!

!--- This dynamic crypto map references the ISAKMP !---
Profile VPN Client above. !--- Reverse route injection
is used to provide the !--- DMVPN networks access to any
Easy VPN Client networks. crypto dynamic-map dynmap 10
set isakmp-profile VPNclient
reverse-route
set transform-set strong
!
!

!--- Crypto map only references the dynamic crypto map
above. crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!
!
!
!
!
!
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!
!
!

!--- Create a GRE tunnel template which is applied to !-
```

```
-- all the dynamically created GRE tunnels. interface
Tunnel0
ip address 192.168.1.1 255.255.255.0
no ip redirects
ip mtu 1440
ip nhrp authentication cisco123
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp holdtime 300
no ip split-horizon eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
!
interface FastEthernet0/0
ip address 209.168.202.225 255.255.255.0
duplex auto
speed auto
crypto map dynmap
!
interface FastEthernet0/1
ip address 1.1.1.1 255.255.255.0
duplex auto
speed auto
!
interface BRI1/0
no ip address
shutdown
!
interface BRI1/1
no ip address
shutdown
!
interface BRI1/2
no ip address
shutdown
!
interface BRI1/3
no ip address
shutdown
!
!--- Enable a routing protocol to send and receive !---
dynamic updates about the private networks. router eigrp
90
redistribute static
network 1.1.1.0 0.0.0.255
network 192.168.1.0
no auto-summary
!
ip local pool dynpool 1.1.11.60 1.1.11.80
ip http server
no ip http secure-server
ip classless
!
!
!
!
!
!
!
!
```

```
!  
!  
line con 0  
exec-timeout 0 0  
transport preferred all  
transport output all  
escape-character 27  
line aux 0  
transport preferred all  
transport output all  
line vty 0 4  
password cisco  
transport preferred all  
transport input all  
transport output all  
!  
!  
end
```

sv9-3 分支配置

```
sv9-3#show run  
Building configuration...  
  
Current configuration : 2052 bytes  
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname sv9-3  
!  
boot-start-marker  
boot system flash:c3725-ik9o3s-mz.123-3.bin  
boot-end-marker  
!  
!  
no aaa new-model  
ip subnet-zero  
!  
!  
no ip domain lookup  
!  
ip audit notify log  
ip audit po max-events 100  
ip ssh break-string  
no ftp-server write-enable  
!  
!  
!  
!--- Create an ISAKMP policy for Phase 1 negotiations.  
crypto isakmp policy 10  
hash md5  
authentication pre-share  
!--- Add dynamic pre-shared keys for all remote VPN  
routers. crypto isakmp key cisco123 address 0.0.0.0  
0.0.0.0  
!  
!  
!--- Create the Phase 2 policy for actual data  
encryption. crypto ipsec transform-set strong esp-3des  
esp-md5-hmac
```

```
mode transport
!
!--- Create an IPsec profile to be applied dynamically
to the !--- GRE over IPsec tunnels. crypto ipsec profile
cisco
set security-association lifetime seconds 120
set transform-set strong
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!--- Create a GRE tunnel template which is applied to !-
-- all the dynamically created GRE tunnels. interface
Tunnel0
ip address 192.168.1.3 255.255.255.0
no ip redirects
ip mtu 1440
ip nhrp authentication cisco123
ip nhrp map multicast dynamic
ip nhrp map 192.168.1.1 209.168.202.225
ip nhrp map multicast 209.168.202.225
ip nhrp network-id 1
ip nhrp holdtime 300
ip nhrp nhs 192.168.1.1
no ip split-horizon eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
!
interface FastEthernet0/0
ip address 209.168.202.130 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 3.3.3.3 255.255.255.0
duplex auto
speed auto
!
interface BRI1/0
no ip address
shutdown
!
interface BRI1/1
no ip address
shutdown
!
interface BRI1/2
no ip address
shutdown
!
interface BRI1/3
no ip address
shutdown
!
!--- Enable a routing protocol to send and receive !---
dynamic updates about the private networks. router eigrp
90
network 3.3.3.0 0.0.0.255
network 192.168.1.0
no auto-summary
```

```
!  
ip http server  
no ip http secure-server  
ip classless  
ip route 0.0.0.0 0.0.0.0 209.168.202.225  
ip route 2.2.2.0 255.255.255.0 Tunnel0  
!  
!  
line con 0  
exec-timeout 0 0  
transport preferred all  
transport output all  
escape-character 27  
line aux 0  
transport preferred all  
transport output all  
line vty 0 4  
login  
transport preferred all  
transport input all  
transport output all  
!  
!  
end
```

sv9-4 分支配置

```
sv9-4#show run  
Building configuration...  
  
Current configuration : 1992 bytes  
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname sv9-4  
!  
boot-start-marker  
boot system flash:c2691-jk9o3s-mz.123-3a.bin  
boot-end-marker  
!  
enable password cisco  
!  
no aaa new-model  
ip subnet-zero  
!  
!  
no ip domain lookup  
!  
ip audit notify log  
ip audit po max-events 100  
ip ssh break-string  
no ftp-server write-enable  
!  
!  
!  
!--- Create an ISAKMP policy for Phase 1 negotiations.  
crypto isakmp policy 10  
hash md5  
authentication pre-share  
!--- Add dynamic pre-shared keys for all remote VPN
```



```
routers. crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0
!
!
!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set strong esp-3des
esp-md5-hmac
mode transport
!
!--- Create an IPsec profile apply dynamically to the !-
-- GRE over IPsec tunnels. crypto ipsec profile cisco
set security-association lifetime seconds 120
set transform-set strong
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!--- Create a GRE tunnel template which is applied to !-
-- all the dynamically created GRE tunnels. interface
Tunnel0
ip address 192.168.1.2 255.255.255.0
no ip redirects
ip mtu 1440
ip nhrp authentication cisco123
ip nhrp map multicast dynamic
ip nhrp map 192.168.1.1 209.168.202.225
ip nhrp map multicast 209.168.202.225
ip nhrp network-id 1
ip nhrp holdtime 300
ip nhrp nhs 192.168.1.1
no ip split-horizon eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
!
interface FastEthernet0/0
ip address 209.168.202.131 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 2.2.2.2 255.255.255.0
duplex auto
speed auto
!
!--- Enable a routing protocol to send and receive !---
dynamic updates about the private networks. router eigrp
90
network 2.2.2.0 0.0.0.255
network 192.168.1.0
no auto-summary
!
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 209.168.202.225
!
!
dial-peer cor custom
!
!
```

```
line con 0
exec-timeout 0 0
transport output lat pad v120 lapb-ta mop telnet rlogin
udptn ssh
escape-character 27
line aux 0
transport output lat pad v120 lapb-ta mop telnet rlogin
udptn ssh
line vty 0 4
login
transport input lat pad v120 lapb-ta mop telnet rlogin
udptn ssh
transport output lat pad v120 lapb-ta mop telnet rlogin
udptn ssh
!
!
end
```

验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

在中心路由器上运行的 Debug 命令会确认分支和 VPN 客户端连接具有匹配的正确参数。运行以下 debug 命令。

[命令输出解释程序 \(仅限注册用户 \)](#) (OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 debug 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- **debug crypto isakmp** — 显示关于 IKE 事件的消息。
- **debug crypto ipsec** - 显示有关 IPsec 事件的信息。

```
sv9-4#show run
Building configuration...

Current configuration : 1992 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sv9-4
!
boot-start-marker
boot system flash:c2691-jk9o3s-mz.123-3a.bin
boot-end-marker
!
enable password cisco
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
```

```
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!  
!--- Create an ISAKMP policy for Phase 1 negotiations. crypto isakmp policy 10
hash md5
authentication pre-share
!--- Add dynamic pre-shared keys for all remote VPN routers. crypto isakmp key cisco123 address
0.0.0.0 0.0.0.0
!
!  
!--- Create the Phase 2 policy for actual data encryption. crypto ipsec transform-set strong
esp-3des esp-md5-hmac
mode transport
!  
!--- Create an IPsec profile apply dynamically to the !--- GRE over IPsec tunnels. crypto ipsec
profile cisco
set security-association lifetime seconds 120
set transform-set strong
!  
!
no voice hpi capture buffer
no voice hpi capture destination
!  
!  
!--- Create a GRE tunnel template which is applied to !--- all the dynamically created GRE
tunnels. interface Tunnel0
interface Tunnel0
ip address 192.168.1.2 255.255.255.0
no ip redirects
ip mtu 1440
ip nhrp authentication cisco123
ip nhrp map multicast dynamic
ip nhrp map 192.168.1.1 209.168.202.225
ip nhrp map multicast 209.168.202.225
ip nhrp network-id 1
ip nhrp holdtime 300
ip nhrp nhs 192.168.1.1
no ip split-horizon eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
!  
interface FastEthernet0/0
ip address 209.168.202.131 255.255.255.0
duplex auto
speed auto
!  
interface FastEthernet0/1
ip address 2.2.2.2 255.255.255.0
duplex auto
speed auto
!  
!--- Enable a routing protocol to send and receive !--- dynamic updates about the private
networks. router eigrp 90
router eigrp 90
network 2.2.2.0 0.0.0.255
network 192.168.1.0
no auto-summary
!  
ip http server
no ip http secure-server
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 209.168.202.225
!
!
dial-peer cor custom
!
!
line con 0
exec-timeout 0 0
transport output lat pad v120 lapb-ta mop telnet rlogin udptn ssh
escape-character 27
line aux 0
transport output lat pad v120 lapb-ta mop telnet rlogin udptn ssh
line vty 0 4
login
transport input lat pad v120 lapb-ta mop telnet rlogin udptn ssh
transport output lat pad v120 lapb-ta mop telnet rlogin udptn ssh
!
!
end
```

[故障排除](#)

有关其他故障排除信息，请参阅 [IP 安全故障排除 - 了解和使用 debug 命令](#)。

[相关信息](#)

- [DMVPN 和 Cisco IOS 软件概述](#)
- [IPsec 协商/IKE 协议](#)
- [技术支持和文档 - Cisco Systems](#)