Índice

Introdução

Este documento descreve como configurar o Dynamic Multipoint VPN (DMVPN) e o Easy VPN com Xauth no mesmo roteador. Esta instalação compreende os spokes DMVPN com endereços atribuídos dinamicamente. Os perfis do Internet Security Association and Key Management Protocol (ISAKMP) permitem separar os métodos de autenticação dos spokes DMVPN com endereços atribuídos dinamicamente ou dos Easy VPN Clients.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 2691 e 3725 Router que executam Software Release 12.3(3) e 12.3(3)a de Cisco IOS®

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

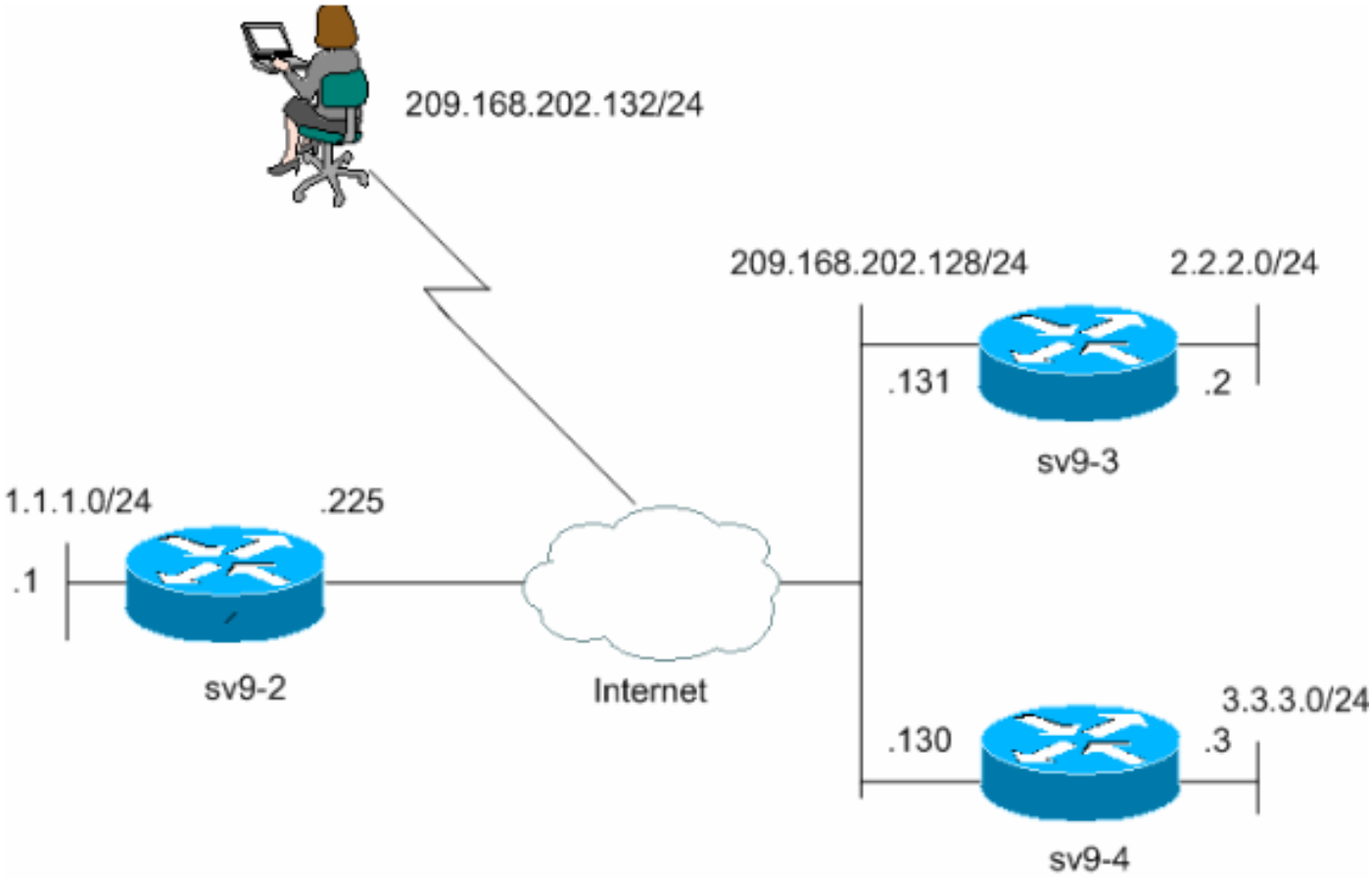
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a ferramenta Command Lookup Tool (apenas para clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.



Configurações

Este documento utiliza estas configurações.

- Configuração do hub sv9-2
- Configuração de raio sv9-3
- Configuração do raio sv9-4

Configuração do hub sv9-2

```
sv9-2#show runBuilding configuration...Current configuration
: 2876 bytes!version 12.3service timestamps debug datetime
msecservice timestamps log datetime msecno service password-
encryption!hostname sv9-2!boot-start-markerboot-end-
marker!enable password cisco!username cisco password 0
ciscoaaa new-model!!!--- Xauth is configured for local
authentication.aaa authentication login userauthen localaaa
authorization network hw-client-groupname local aaa session-
id commonip subnet-zero! !no ip domain lookup!ip audit notify
logip audit po max-events 100ip 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 10hash md5authentication
pre-share!!--- Create an ISAKMP policy for Phase 1
negotiations. !--- This policy is for Easy VPN Clients.crypto
isakmp policy 20hash md5authentication pre-sharegroup 2!!---
VPN Client configuration for group "hw-client-groupname" !---
(this name is configured in the VPN Client).crypto isakmp
client configuration group hw-client-groupnamekey hw-client-
passworddns 1.1.11.10 1.1.11.11wins 1.1.11.12 1.1.11.13domain
cisco.compool dynpool !--- Profile for VPN Client
connections, matches the !--- "hw-client-group" group and
defines the XAuth properties. crypto isakmp profile
VPNclientmatch identity group hw-client-groupnameclient
authentication list userauthenisakmp authorization list hw-
client-groupnameclient 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 DMVPNkeyring dmvpnspokesmatch
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
ciscoset security-association lifetime seconds 120set
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 10set isakmp-profile
VPNclientreverse-routeset transform-set strong!!!--- Crypto
map only references the dynamic crypto map above. crypto map
dynmap 1 ipsec-isakmp dynamic dynmap !!!!!!!!!!no voice hpi
capture bufferno voice hpi capture destination !!!! !!!---
Create a GRE tunnel template which is applied to !--- all the
dynamically created GRE tunnels.interface Tunnel0ip address
192.168.1.1 255.255.255.0no ip redirectsip mtu 1440ip nhrp
authentication cisco123ip nhrp map multicast dynamicip nhrp
network-id 1ip nhrp holdtime 300no ip split-horizon eigrp
90tunnel source FastEthernet0/0tunnel mode gre
multipointtunnel key 0tunnel protection ipsec profile
cisco!interface FastEthernet0/0ip address 209.168.202.225
255.255.255.0duplex autospeed autocrypto map dynmap!interface
FastEthernet0/1ip address 1.1.1.1 255.255.255.0duplex
autospeed auto!interface BRI1/0no ip
addressshutdown!interface BRI1/1no ip
addressshutdown!interface BRI1/2no ip
addressshutdown!interface BRI1/3no ip addressshutdown!!---
Enable a routing protocol to send and receive !--- dynamic
updates about the private networks.router eigrp
90redistribute staticnetwork 1.1.1.0 0.0.0.255network
192.168.1.0no auto-summary!ip local pool dynpool 1.1.11.60
1.1.11.80ip http serverno ip http secure-serverip
classless!!!!!!!!!!!line con 0exec-timeout 0 0transport
preferred alltransport output allescape-character 27line aux
0transport preferred alltransport output allline vty 0
4password ciscotransport preferred alltransport input
alltransport output all!!end
```

Configuração de raio sv9-3

```
sv9-3#show runBuilding configuration...Current configuration
: 2052 bytes!version 12.3service timestamps debug datetime
msecservice timestamps log datetime msecno service password-
```

```
encryption!hostname sv9-3!boot-start-markerboot system
flash:c3725-ik9o3s-mz.123-3.binboot-end-marker!!no aaa new-
modelip subnet-zero!!no ip domain lookup!ip audit notify
logip audit po max-events 100ip ssh break-string no ftp-
server write-enable!! !!--- Create an ISAKMP policy for Phase
1 negotiations.crypto isakmp policy 10hash md5authentication
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 ciscoset security-association lifetime seconds
120set transform-set strong !!no voice hpi capture bufferno
voice hpi capture destination !!!--- Create a GRE tunnel
template which is applied to !--- all the dynamically created
GRE tunnels.interface Tunnel0ip address 192.168.1.3
255.255.255.0no ip redirectsip mtu 1440ip nhrp authentication
cisco123ip nhrp map multicast dynamicip nhrp map 192.168.1.1
209.168.202.225ip nhrp map multicast 209.168.202.225ip nhrp
network-id 1ip nhrp holdtime 300ip nhrp nhs 192.168.1.1no ip
split-horizon eigrp 90tunnel source FastEthernet0/0tunnel
mode gre multipointtunnel key 0tunnel protection ipsec
profile cisco!interface FastEthernet0/0ip address
209.168.202.130 255.255.255.0duplex autospeed auto!interface
FastEthernet0/1ip address 3.3.3.3 255.255.255.0duplex
autospeed auto!interface BRI1/0no ip
addressshutdown!interface BRI1/1no ip addressshutdown
!interface BRI1/2no ip addressshutdown!interface BRI1/3no ip
addressshutdown!!--- Enable a routing protocol to send and
receive !--- dynamic updates about the private
networks.router eigrp 90network 3.3.3.0 0.0.0.255network
192.168.1.0no auto-summary!ip http serverno ip http secure-
serverip classlessip route 0.0.0.0 0.0.0.0 209.168.202.225ip
route 2.2.2.0 255.255.255.0 Tunnel0!!line con 0exec-timeout 0
0transport preferred alltransport output allescape-character
27line aux 0transport preferred alltransport output allline
vty 0 4logintransport preferred alltransport input
alltransport output all!!end
```

Configuração do raio sv9-4

```
sv9-4#show runBuilding configuration...Current configuration
: 1992 bytes!version 12.3service timestamps debug datetime
msecservice timestamps log datetime msecno service password-
encryption!hostname sv9-4!boot-start-markerboot system
flash:c2691-jk9o3s-mz.123-3a.binboot-end-marker!enable
password cisco!no aaa new-modelip subnet-zero!!no ip domain
lookup!ip audit notify logip audit po max-events 100ip ssh
break-string no ftp-server write-enable!! !!--- Create an
ISAKMP policy for Phase 1 negotiations.crypto isakmp policy
10hash md5authentication 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 ciscoset security-association lifetime seconds
120set transform-set strong !!no voice hpi capture bufferno
voice hpi capture destination !!!--- Create a GRE tunnel
template which is applied to !--- all the dynamically created
GRE tunnels.interface Tunnel0ip address 192.168.1.2
255.255.255.0no ip redirectsip mtu 1440ip nhrp authentication
cisco123ip nhrp map multicast dynamicip nhrp map 192.168.1.1
```

```
209.168.202.225ip nhrp map multicast 209.168.202.225ip nhrp
network-id 1ip nhrp holdtime 300ip nhrp nhs 192.168.1.1no ip
split-horizon eigrp 90tunnel source FastEthernet0/0tunnel
mode gre multipointtunnel key 0tunnel protection ipsec
profile ciscointerface FastEthernet0/0ip address
209.168.202.131 255.255.255.0duplex autospeed auto!interface
FastEthernet0/1ip address 2.2.2.2 255.255.255.0duplex
autospeed auto!!--- Enable a routing protocol to send and
receive !--- dynamic updates about the private
networks.router eigrp 90network 2.2.2.0 0.0.0.255network
192.168.1.0no auto-summary!ip http serverno ip http secure-
serverip classlessip route 0.0.0.0 0.0.0.0
209.168.202.225!!dial-peer cor custom!!line con 0exec-timeout
0 0transport output lat pad v120 lapb-ta mop telnet rlogin
udptn sshescape-character 27line aux 0transport output lat
pad v120 lapb-ta mop telnet rlogin udptn sshline vty 0
4logintransport input lat pad v120 lapb-ta mop telnet rlogin
udptn sshtransport output lat pad v120 lapb-ta mop telnet
rlogin udptn ssh!!end
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

Os comandos Debug que são executado no roteador de hub confirmam que os parâmetros corretos estão combinados para o spoke e as conexões de cliente de VPN. Execute estes **comandos debug**.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **isakmp do debug crypto**? Indica mensagens sobre eventos IKE.
- **IPsec do debug crypto**? Indica a informação sobre eventos de IPSec.

```
sv9-4#show runBuilding configuration...Current configuration : 1992 bytes!version 12.3service timestamps
debug datetime msecservice timestamps log datetime msecno service password-encryption!hostname sv9-
4!boot-start-markerboot system flash:c2691-jk9o3s-mz.123-3a.binboot-end-marker!enable password cisco!no
aaa new-modelip subnet-zero!!no ip domain lookup!ip audit notify logip audit po max-events 100ip ssh
break-string no ftp-server write-enable!! !!--- Create an ISAKMP policy for Phase 1 negotiations.crypto
isakmp policy 10hash md5authentication 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 ciscoset
security-association lifetime seconds 120set transform-set strong !!no voice hpi capture bufferno voice
hpi capture destination !!!--- Create a GRE tunnel template which is applied to !--- all the dynamically
created GRE tunnels.interface Tunnel0ip address 192.168.1.2 255.255.255.0no ip redirectsip mtu 1440ip
nhrp authentication cisco123ip nhrp map multicast dynamicip nhrp map 192.168.1.1 209.168.202.225ip nhrp
map multicast 209.168.202.225ip nhrp network-id 1ip nhrp holdtime 300ip nhrp nhs 192.168.1.1no ip split-
horizon eigrp 90tunnel source FastEthernet0/0tunnel mode gre multipointtunnel key 0tunnel protection
ipsec profile ciscointerface FastEthernet0/0ip address 209.168.202.131 255.255.255.0duplex autospeed
auto!interface FastEthernet0/1ip address 2.2.2.2 255.255.255.0duplex autospeed auto!!--- Enable a routing
protocol to send and receive !--- dynamic updates about the private networks.router eigrp 90network
2.2.2.0 0.0.0.255network 192.168.1.0no auto-summary!ip http serverno ip http secure-serverip classlessip
route 0.0.0.0 0.0.0.0 209.168.202.225!!dial-peer cor custom!!line con 0exec-timeout 0 0transport output
```

```
lat pad v120 lapb-ta mop telnet rlogin udptn sshescape-character 27line aux 0transport output lat pad
v120 lapb-ta mop telnet rlogin udptn sshline vty 0 4logintransport input lat pad v120 lapb-ta mop telnet
rlogin udptn sshtransport output lat pad v120 lapb-ta mop telnet rlogin udptn ssh!!end
```

Troubleshooting

Consulte IP Security Troubleshooting - Understanding and Using debug Commands para obter informações adicionais sobre a resolução de problemas.

Informações Relacionadas

- DMVPN e vista geral do Cisco IOS Software
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems