Пример конфигурации DMVPN и сервера Easy VPN с профилями ISAKMP

Содержание

Введение

В данном документе описываются способы настройки Dynamic Multipoint VPN (DMVPN) и Easy VPN с Xauth на одном и том же маршрутизаторе. Данная настройка обеспечивает динамическую адресацию оконечных устройств DMVPN. Профили протокола Internet Security Association and Key Management Protocol (ISAKMP) предоставляют возможность разделять способы аутентификации динамически адресуемых оконечных устройств DMVPN или клиентов Easy VPN.

Предварительные условия

Требования

Для данного документа нет особых требований.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного и аппаратного обеспечения:

- Маршрутизаторы Cisco 2691 и 3725, поддерживающие версии ПО Cisco IOS® 12.3(3) и 12.3(3)a

Данные для документа были получены в специально созданных лабораторных условиях. Все устройства, используемые в этом документе, были запущены с чистой (заданной по умолчанию) конфигурацией. Если ваша сеть работает в реальных условиях, убедитесь, что вы понимаете потенциальное воздействие каждой команды.

Условные обозначения

Более подробные сведения о применяемых в документе обозначениях см. в документе Условные обозначения, используемые в технической документации Cisco.

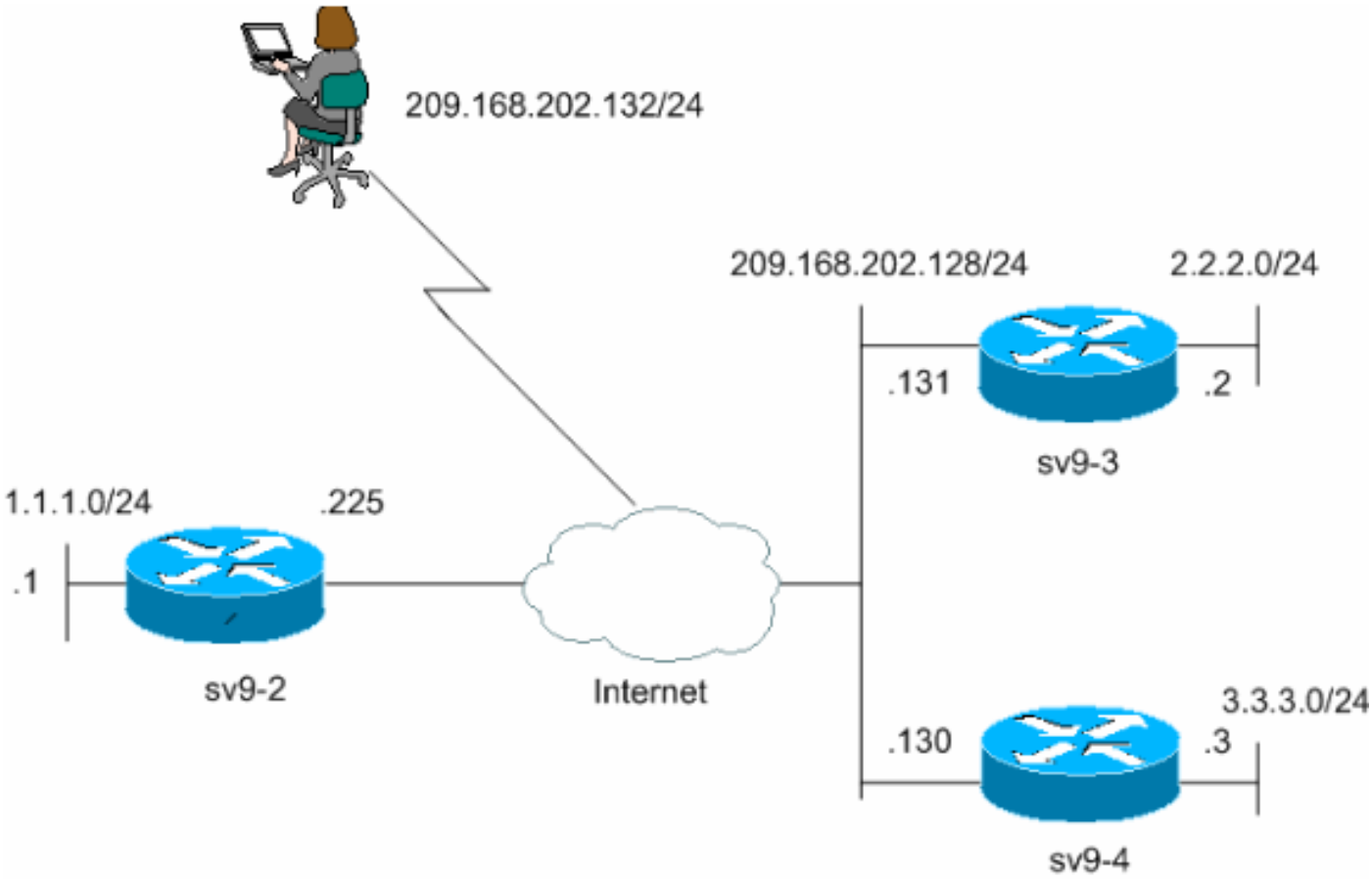
Настройка

В этом разделе приводится информация по настройке функций, описанных в данном документе.

Примечание. Чтобы найти дополнительные сведения о применяемых в данном документе командах, используйте Средство поиска команд (только для зарегистрированных пользователей).

Схема сети

В этом документе использованы параметры данной сети.



Конфигурации

В данном документе используются следующие конфигурации.

- Конфигурация концентратора sv9-2
- Конфигурация оконечного устройства sv9-3
- Конфигурация оконечного устройства sv9-4

Конфигурация концентратора sv9-2
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    . 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
!
!

!---  ,     . crypto keyring dmvpnspokes
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!



!---   ISAKMP    . !---       DMVPN. crypto isakmp
policy 10
hash md5
authentication pre-share
!

!---   ISAKMP    . !---      Easy VPN. crypto isakmp
policy 20
hash md5
authentication pre-share
group 2

!

!---   VPN   "hw-client-groupname" !--- (     VPN).
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
```

```
!---     VPN,    !---  "hw-client-group"    XAuth. crypto
isakmp profile VPNclient
match identity group hw-client-groupname
client authentication list userauthen
isakmp authorization list hw-client-groupname
client configuration address respond


!---    LAN-LAN,    !---      !---  (     !---   Cisco
ID CSCea77140), !--- XAuth . crypto isakmp profile DMVPN
keyring dmvpnspokes
match identity address 0.0.0.0
!
!

!---        . crypto ipsec transform-set strong esp-3des
esp-md5-hmac
mode transport
!

!---   IPSec,      !---    (GRE)   IPsec. crypto ipsec
profile cisco
set security-association lifetime seconds 120
set transform-set strong
set isakmp-profile DMVPN
!
!

!---      !---    VPN ISAKMP. !---     ,    !---   DMVPN
 Easy VPN. crypto dynamic-map dynmap 10
set isakmp-profile VPNclient
reverse-route
set transform-set strong
!
!

!---      . crypto map dynmap 1 ipsec-isakmp dynamic
dynmap
!
!
!
!
!
!
!
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!
!
!
!

!---   GRE,    !---     GRE. 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
!

!---        !---      . 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
```

Конфигурация оконечного устройства sv9-3

```
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
!
!
!
!---   ISAKMP    . crypto isakmp policy 10
hash md5
authentication pre-share
!---         VPN. crypto isakmp key cisco123 address
0.0.0.0 0.0.0.0
!
!
!---        . crypto ipsec transform-set strong esp-3des
esp-md5-hmac
mode transport
!
!---   IPSec,      !---  GRE   IPSec. crypto ipsec
profile cisco
set security-association lifetime seconds 120
set transform-set strong
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!---   GRE,    !---     GRE. 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
!
!---        !---      . 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
```

Конфигурация оконечного устройства sv9-4

```
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
!
!
!
!---   ISAKMP    . crypto isakmp policy 10
hash md5
authentication pre-share
!---         VPN. crypto isakmp key cisco123 address
0.0.0.0 0.0.0.0
!
!
!---        . crypto ipsec transform-set strong esp-3des
esp-md5-hmac
mode transport
!
!---   IPSec,      !---  GRE   IPSec. crypto ipsec
profile cisco
set security-association lifetime seconds 120
set transform-set strong
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!---   GRE,    !---     GRE. 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
!
!---        !---      . 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
```

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Команды отладки, которые выполняются на маршрутизаторе концентратора, могут подтвердить, что корректные параметры согласованы для подключений оконечного

устройства и клиента VPN. Выполните данные команды **debug**.

Средство Интерпретатор выходных данных (только для зарегистрированных клиентов) (OIT) поддерживает некоторые команды **show**. Используйте OIT для просмотра аналитики выходных данных команды **show**.

Примечание. Перед использованием **команд отладки** обратитесь к документу Важные сведения о командах отладки.

- **debug crypto isakmp** – отображает сообщения о событиях IKE.
- **debug crypto ipsec** – отображает информацию о событиях IPsec.

```
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
!
!
!
!---   ISAKMP    . crypto isakmp policy 10
hash md5
authentication pre-share
!---         VPN. crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
!
!---        . crypto ipsec transform-set strong esp-3des esp-md5-hmac
mode transport
!
!---   IPSec,      !---  GRE   IPSec. crypto ipsec profile cisco
set security-association lifetime seconds 120
set transform-set strong
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!---   GRE,    !---     GRE. 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
!
!---        !---      . 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
```

Устранение неполадок

Дополнительные сведения об устранении неполадок см. в разделе Устранение неполадок IP-безопасности – общие сведения и использование команд **debug**.

Дополнительные сведения

- Обзор DMVPN и ПО Cisco IOS
- Развертывание виртуальных частных сетей IPsec
- Протоколы согласования IPsec/IKE
- Cisco Systems – техническая поддержка и документация