



Настройка протокола IPsec между маршрутизаторами (с предварительными общими ключами) для туннеля GRE с использованием межсетевого экрана IOS и NAT

Содержание

Введение

Предварительные условия

Требования

Используемые компоненты

Условные обозначения

Базовые сведения

Настройка

Схема сети

Конфигурации

Проверка

Устранение неполадок

Команды устранения неполадок

Дополнительные сведения

Введение

В этом документе приводится базовая конфигурация межсетевого экрана Cisco IOS® с использованием NAT (преобразование сетевых адресов). Эта конфигурация позволяет инициировать трафик из сетей 10.1.1.x и 172.16.1.x в Интернет и на пути использовать NAT. К IP-туннелю и трафику IPX (Межсетевой пакетный обмен) между двумя частными сетями добавляется туннель GRE (Протокол туннелирования сетевых пакетов). Когда на исходящий интерфейс маршрутизатора поступает пакет и отправляется по туннелю, пакет сначала инкапсулируется при помощи протокола GRE и затем шифруется по протоколу IPsec. Другими словами, любой трафик, который может быть передан по туннелю GRE, также шифруется протоколом IPsec.

Дополнительные сведения о настройке туннеля GRE поверх IPsec с использованием протокола OSPF (Open Shortest Path First, протокол предпочтения кратчайшего пути) см. в документе Настройка туннеля GRE по протоколу IPsec с использованием протокола OSPF.

Дополнительные сведения о настройке сети из трех маршрутизаторов с топологией звезды с помощью протокола IPsec см. в документе Настройка с помощью протокола IPsec звездообразной сети "маршрутизатор-маршрутизатор" с соединением между оконечными устройствами.

Предварительные условия

Требования

В данном документе не выдвигаются никаких особых требований.

Используемые компоненты

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

- ПО Cisco IOS версий 12.2(21a) и 12.3(5a);

- Cisco 3725 и 3640.

Данные для этого документа были получены с помощью указанных устройств в специально созданных лабораторных условиях. Все устройства, используемые в этом документе, запускались с чистой (заданной по умолчанию) конфигурацией. Если сеть находится в коммерческой эксплуатации, при использовании каждой команды следует адекватно оценивать ее потенциальное воздействие.

Условные обозначения

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

Базовые сведения

В данном разделе приводятся указания по осуществлению необходимых настроек.

- Для проверки возможности подключения к Интернету, введите в действие на обоих маршрутизаторах протокол NAT.
- Добавьте к конфигурации протокол GRE и протестируйте ее. Трафик, не подвергнутый шифрованию, необходимо передавать между частными сетями.
- Добавьте в конфигурацию протокол IPsec и протестируйте ее. Трафик между частными сетями должен быть зашифрован.
- Добавьте к внешним интерфейсам, в список контроля исходящего трафика и в список доступа для входящего трафика межсетевой экран Cisco IOS, а затем выполните тестирование этих настроек.
- Если используется версия Cisco IOS ранее 12.1.4, необходимо разрешить IP-трафик между 172.16.1.x и - 10.0.0.0 в списке доступа 103. Дополнительные сведения см. в разделах по ошибкам Cisco: ID CSCdu58486 (только для зарегистрированных пользователей) и ID CSCdm01118 (только для зарегистрированных пользователей).

Настройка

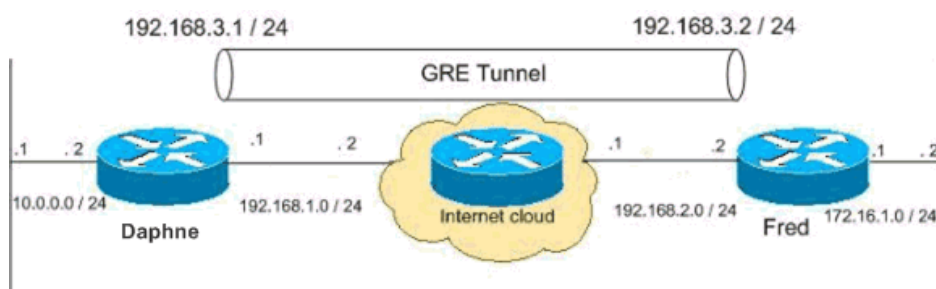
В этом разделе приводится информация по настройке функций, описанных в данном документе.

Примечание. Для поиска дополнительной информации о командах в данном документе используйте Средство поиска команд (только для зарегистрированных клиентов).

Примечание. Схемы IP-адресации, приведенные в этой конфигурации, нельзя использовать для маршрутизации в Интернете. Это адреса RFC 1918, которые использовались в лабораторной среде.

Схема сети

В этом документе используются следующие параметры сети.



Конфигурации

В данном документе используются следующие конфигурации:

- конфигурация Daphne;
- конфигурация Fred.

Конфигурация Daphne

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname daphne
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$r2sh$XKZR118vcId1lZGzhhz5C/
!
no aaa new-model
ip subnet-zero
!
!
!--- Конфигурация межсетевого экрана Cisco IOS и то, что необходимо проверить.
!--- Подаваемый исходящий трафик на внешнем интерфейсе.

ip inspect name myfw tcp
ip inspect name myfw udp
ip inspect name myfw ftp
ip inspect name myfw realaudio
ip inspect name myfw smtp
ip inspect name myfw streamworks
ip inspect name myfw vdolive
ip inspect name myfw tftp
ip inspect name myfw rcmd
ip inspect name myfw http
ip telnet source-interface FastEthernet0/0
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
!--- Конфигурация протокола IPsec.

!
crypto isakmp policy 10
authentication pre-share

crypto isakmp key ciscokey address 192.168.2.2
!
!
crypto ipsec transform-set to_fred esp-des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp

set peer 192.168.2.2
set transform-set to_fred
match address 101
!
!
!
!
!
!--- Одна сторона туннеля GRE.

!
interface Tunnel0

ip address 192.168.3.1 255.255.255.0
!--- Туннель необходимо связать с физическим интерфейсом.

tunnel source FastEthernet0/1
```

```
tunnel destination 192.168.2.2

!--- Внутренняя сеть.

interface FastEthernet0/0

ip address 10.0.0.2 255.255.255.0
ip nat inside
speed 100
full-duplex
!
!--- Внешний интерфейс и одна сторона туннеля GRE.

interface FastEthernet0/1

ip address 192.168.1.1 255.255.255.0
ip access-group 103 in
ip nat outside
ip inspect myfw out
speed 100
full-duplex
  crypto map myvpn
!
!--- Необходимо определить пул NAT.

ip nat pool ourpool 192.168.1.10 192.168.1.20 netmask 255.255.255.0
ip nat inside source route-map nonat pool ourpool overload
ip classless

ip route 0.0.0.0 0.0.0.0 192.168.1.2

!--- Необходимо принудительно направить трафик частной сети в туннель.

-
ip route 172.16.1.0 255.255.255.0 192.168.3.2
ip http server
no ip http secure-server
!
!

!--- Весь трафик, который поступает в туннель GRE, шифруется протоколом IPsec.
!--- Другие операторы ACE не требуются.

access-list 101 permit gre host 192.168.1.1 host 192.168.2.2
!--- Список доступа в целях безопасности. Разрешение
!--- трафика по протоколам IPsec и GRE между частными сетями.

access-list 103 permit gre host 192.168.2.2 host 192.168.1.1
access-list 103 permit esp host 192.168.2.2 host 192.168.1.1
access-list 103 permit udp host 192.168.2.2 eq isakmp host 192.168.1.1
access-list 103 deny ip any any log

!--- См. раздел Базовые сведения, если для списка доступа 103 используется
!--- версия Cisco IOS ранее 12.1.4.

access-list 175 deny ip 10.0.0.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 175 permit ip 10.0.0.0 0.0.0.255 any

!--- Для адресации в протоколе NAT используется список доступа в маршрутной карте.

route-map nonat permit 10
match ip address 175
!
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password ww
login
!
!
end
```

Конфигурация Fred

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname fred
!
enable secret 5 $1$AtxD$MycLGaJvF/tAIFXkikCes1
!
ip subnet-zero
!
!
ip telnet source-interface FastEthernet0/0
!
ip inspect name myfw tcp
ip inspect name myfw udp
ip inspect name myfw ftp
ip inspect name myfw realaudio
ip inspect name myfw smtp
ip inspect name myfw streamworks
ip inspect name myfw vdolive
ip inspect name myfw tftp
ip inspect name myfw rcmd
ip inspect name myfw http
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 10
authentication pre-share
-
crypto isakmp key ciscokey address 192.168.1.1
!
!
crypto ipsec transform-set to_daphne esp-des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp

set peer 192.168.1.1
set transform-set to_daphne
match address 101
!
call rsvp-sync
!
!
!
!
!
!
!
!
interface Tunnel0
-
ip address 192.168.3.2 255.255.255.0
tunnel source FastEthernet0/1
-
tunnel destination 192.168.1.1
!
interface FastEthernet0/0
ip address 172.16.1.1 255.255.255.0
ip nat inside
speed 100
full-duplex
!
interface Serial0/0
no ip address
clockrate 2000000
!
interface FastEthernet0/1

ip address 192.168.2.2 255.255.255.0
ip access-group 103 in
ip nat outside
ip inspect myfw out
speed 100
full-duplex
crypto map myvpn
!
```

```

!--- Выходные данные обрезаны.

!

ip nat pool ourpool 192.168.2.10 192.168.2.20 netmask 255.255.255.0
ip nat inside source route-map nonat pool ourpool overload
ip classless

ip route 0.0.0.0 0.0.0.0 192.168.2.1
ip route 10.0.0.0 255.255.255.0 192.168.3.1
ip http server
!

access-list 101 permit gre host 192.168.2.2 host 192.168.1.1
access-list 103 permit gre host 192.168.1.1 host 192.168.2.2
access-list 103 permit udp host 192.168.1.1 eq isakmp host 192.168.2.2
access-list 103 permit esp host 192.168.1.1 host 192.168.2.2
access-list 175 deny ip 172.16.1.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 175 permit ip 172.16.1.0 0.0.0.255 any

route-map nonat permit 10
match ip address 175
!
!
!
dial-peer cor custom
!
!
!
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password ww
login
!
end

```

Проверка

В этом разделе приведена информация о способах проверки настроенной конфигурации.

Интерпретатор выходных данных (только для зарегистрированных пользователей) (OIT) поддерживает некоторые команды **show**. Используйте этот интерпретатор для анализа выходных данных команды **show**.

Для проверки конфигурации VPN, попробуйте отправить с хоста в сети 172.16.1.x запрос "ICMP-эхо" на хост в удаленной подсети – 10.0.0.x. Этот трафик должен проходить через туннель GRE и подвергнут шифрованию.

Для проверки работоспособности туннеля IPsec, используйте команду **show crypto ipsec sa**. Сначала убедитесь, что номера SPI (service provider interface, интерфейс поставщика услуг) отличны от 0. Также должны увеличиться значения счетчиков `pkts encrypt` и `pkts decrypt`.

- **show crypto ipsec sa** – проверяет состояние готовности туннеля IPsec.
- **show access-lists 103** – проверяет правильность работы конфигурации межсетевого экрана Cisco IOS.
- **show ip nat translations** – проверяет правильность работы NAT.

```

fred#show crypto ipsec sa

interface: FastEthernet0/1

Crypto map tag: myvpn, local addr. 192.168.2.2

local ident (addr/mask/prot/port): (192.168.2.2/255.255.255.255/47/0)

```

```

remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)
current_peer: 192.168.1.1
  PERMIT, flags={transport_parent,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

-
local crypto endpt.: 192.168.2.2, remote crypto endpt.: 192.168.1.1
path mtu 1500, media mtu 1500
current outbound spi: 0

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

-
local ident (addr/mask/prot/port): (192.168.2.2/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
current_peer: 192.168.1.1
  PERMIT, flags={origin_is_acl,parent_is_transport,}
#pkts encaps: 42, #pkts encrypt: 42, #pkts digest 42
#pkts decaps: 39, #pkts decrypt: 39, #pkts verify 39
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 2, #recv errors 0

local crypto endpt.: 192.168.2.2, remote crypto endpt.: 192.168.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3C371F6D

inbound esp sas:
  spi: 0xF06835A9(4033361321)
  transform: esp-des esp-md5-hmac ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 940, flow_id: 1, crypto map: myvpn
  sa timing: remaining key lifetime (k/sec): (4607998/2559)
  IV size: 8 bytes
  replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x3C371F6D(1010245485)
  transform: esp-des esp-md5-hmac ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 941, flow_id: 2, crypto map: myvpn
  sa timing: remaining key lifetime (k/sec): (4607998/2559)
  IV size: 8 bytes
  replay detection support: Y

outbound ah sas:

outbound pcp sas:

```

Для того чтобы убедиться в правильности работы конфигурации межсетевого экрана Cisco IOS, сначала дайте эту команду.

```
fred#show access-lists 103
```

```

Extended IP access list 103
 permit gre host 192.168.1.1 host 192.168.2.2 (4 matches)
 permit udp host 192.168.1.1 eq isakmp host 192.168.2.2 (4 matches)
 permit esp host 192.168.1.1 host 192.168.2.2 (4 matches)

```

Затем с хоста в сети 172.16.1.x попытайтесь установить связь через Telnet с удаленным хостом в Интернете. Сначала можно проверить,

правильно ли работает NAT. Локальный адрес 172.16.1.2 был преобразован в 192.168.2.10.

```
fred#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 192.168.2.10:11006 172.16.1.2:11006 192.168.2.1:23    192.168.2.1:23
```

При повторной проверке списка доступа можно увидеть, что в него динамически добавлена строка.

```
fred#show access-lists 103
Extended IP access list 103
  permit tcp host 192.168.2.1 eq telnet host 192.168.2.10 eq 11006 (11 matches)
  permit gre host 192.168.1.1 host 192.168.2.2 (4 matches)
  permit udp host 192.168.1.1 eq isakmp host 192.168.2.2 (4 matches)
  permit esp host 192.168.1.1 host 192.168.2.2 (4 matches)
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды устранения неполадок

Интерпретатор выходных данных (только для зарегистрированных пользователей) (OIT) поддерживает некоторые команды **show**. Используйте этот интерпретатор для анализа выходных данных команды **show**.

Примечание. См. документ Важные сведения о командах Debug перед использованием команд отладки **debug**.

Протокол NAT:

- **debug ip nat access-list number** – отображает информацию об IP-пакетах, преобразованных функцией IP NAT.

IPSec:

- **debug crypto ipsec** – отображает события IPSec.
- **debug crypto isakmp** – выдает сообщения о событиях обмена ключами в Интернете (IKE, Internet Key Exchange).
- **debug crypto engine** – отображает информацию от криптографического модуля.

СВАС (Контроль доступа на основе контекста):

- **debug ip inspect {protocol| detailed}** – отображает сообщения о событиях межсетевого экрана Cisco IOS.

Списки доступа:

- **debug ip packet** (с **no ip route-cache** на интерфейсе) – отображает общую информацию по отладке IP и безопасные транзакции с установленными параметрами безопасности IP (IPSO - IP security option).

daphne#**show version**

Cisco Internetwork Operating System Software
IOS (tm) 3700 Software (C3725-ADVSECURITYK9-M), Version 12.3(5a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 24-Nov-03 20:36 by kellythw
Image text-base: 0x60008AF4, data-base: 0x613C6000

ROM: System Bootstrap, Version 12.2(8r)T2, RELEASE SOFTWARE (fc1)

daphne uptime is 6 days, 19 hours, 39 minutes
System returned to ROM by reload
System image file is "flash:c3725-advsecurityk9-mz.123-5a.bin"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

cisco 3725 (R7000) processor (revision 0.1) with 196608K/65536K bytes of memory.
Processor board ID JHY0727K212
R7000 CPU at 240MHz, Implementation 39, Rev 3.3, 256KB L2 Cache
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
1 Virtual Private Network (VPN) Module(s)
DRAM configuration is 64 bits wide with parity disabled.
55K bytes of non-volatile configuration memory.
125952K bytes of ATA System CompactFlash (Read/Write)

Configuration register is 0x2002

fred#**show version**

Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-JK9O3S-M), Version 12.2(21a), RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 09-Jan-04 16:23 by kellmill
Image text-base: 0x60008930, data-base: 0x615DE000

ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)

fred uptime is 6 days, 19 hours, 36 minutes
System returned to ROM by reload
System image file is "flash:c3640-jk9o3s-mz.122-21a.bin"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

cisco 3640 (R4700) processor (revision 0x00) with 124928K/6144K bytes of memory.
Processor board ID 25120505
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 FastEthernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
4 Serial(sync/async) network interface(s)

1 Virtual Private Network (VPN) Module(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)

Configuration register is 0x2002

Примечание. Если эта конфигурация настраивается по шагам, выбор команды **debug**, которую необходимо использовать, зависит от того этапа, на котором возникает сбой.

Дополнительные сведения

- **Протоколы согласования IPsec / IKE**
- **Cisco Systems – Техническая поддержка и документация**

© 1992-2010 Cisco Systems, Inc. Все права защищены.

Дата генерации PDF файла: Jan 05, 2010

<http://www.cisco.com/support/RU/customer/content/10/107601/quicktip.shtml>
