

"Настройка подключения маршрутизатор-маршрутизатор IPSec, предварительных ключей, перегрузки NAT между сетью общего доступа и частной сетью"

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Проверка](#)

[Образец команды show output](#)

[Устранение неполадок](#)

[Команды для устранения неполадок](#)

[Дополнительные сведения](#)

[Введение](#)

Этот пример конфигурации иллюстрирует шифрование трафика между частной сетью (10.103.1.x) и внешней сетью (98.98.98.x) с использованием IPSec. Сеть 98.98.98.x определяет сеть 10.103.1.x по частным адресам. Сеть 10.103.1.x определяет сеть 98.98.98.x по открытым адресам.

[Предварительные условия](#)

[Требования](#)

Данный документ требует базовых знаний протокола IPSec. [Дополнительные сведения о протоколе IPSec можно найти в документе Обзор протокола шифрования для защиты IP-пакетов \(IPSec\).](#)

[Используемые компоненты](#)

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

- Выпуск ПО Cisco IOS® 12.3(5)
- Маршрутизаторы Cisco 3640

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.](#)

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: [Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" \(Поиск команд\) \(только для зарегистрированных клиентов\).](#)

Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме.

Конфигурации

Эти конфигурации используются в данном документе:

- [3640-2b – «открытый» маршрутизатор](#)
- [3640-6a – «частный» маршрутизатор](#)

3640-2b – «открытый» маршрутизатор

```
rp-3640-2b#show running config Building configuration...
Current configuration: ! version 12.3 service timestamps
debug uptime service timestamps log uptime no service
password-encryption ! hostname rp-3640-2b ! ip subnet-
zero ! ! !--- Defines the Internet Key Exchange (IKE)
policies. crypto isakmp policy 1 !--- Defines an IKE
policy. Use the crypto isakmp policy !--- command in
global configuration mode. IKE policies !--- define a
set of parameters !--- that are used during the IKE
phase I negotiation. hash md5 authentication pre-share
!--- Specifies preshared keys as the authentication
method. crypto isakmp key cisco123 address 95.95.95.2 !-
-- Configures a preshared authentication key, used in !-
-- global configuration mode. ! crypto ipsec transform-
set rtpset esp-des esp-md5-hmac !--- Defines a
transform-set. This is an acceptable !--- combination of
security protocols and algorithms, !--- which has to be
matched on the peer router. ! crypto map rtp 1 ipsec-
isakmp !--- Indicates that IKE is used to !--- establish
the IPSec security associations (SAs) that protect !---
the traffic specified by this crypto map entry. set peer
```

```

95.95.95.2 !--- Sets the IP address of the remote end.
set transform-set rtpset !--- Configures IPSec to use
the transform-set !--- "rtpset" defined earlier. match
address 115 !--- This is used to assign an extended
access list to a !--- crypto map entry which is used by
IPSec !--- to determine which traffic should be
protected !--- by crypto and which traffic does not !---
need crypto protection. ! interface Ethernet0/0 ip
address 98.98.98.1 255.255.255.0 no ip directed-
broadcast ! interface Ethernet0/1 ip address 99.99.99.2
255.255.255.0 no ip directed-broadcast no ip route-cache
!--- Enable process switching for !--- IPSec to encrypt
outgoing packets. !--- This command disables fast
switching. no ip mroute-cache crypto map rtp !---
Configures the interface to use !--- the crypto map
"rtp" for IPSec. ! . . !--- Output suppressed. . . ip
classless ip route 0.0.0.0 0.0.0.0 99.99.99.1 !---
Default route to the next hop address. no ip http server
! access-list 115 permit ip 98.98.98.0 0.0.0.255
10.103.1.0 0.0.0.255 !--- This access-list option causes
all IP traffic !--- that matches the specified
conditions to be !--- protected by IPSec using the
policy described by !--- the corresponding crypto map
command statements. access-list 115 deny ip 98.98.98.0
0.0.0.255 any ! line con 0 transport input none line aux
0 line vty 0 4 login ! end

```

3640-6a – «частный» маршрутизатор

```

rp-3640-6a#show running config Building configuration...
Current configuration: ! version 12.3 service timestamps
debug uptime service timestamps log uptime no service
password-encryption ! hostname rp-3640-6a ! ! ip subnet-
zero !--- Defines the IKE policies. ! crypto isakmp
policy 1 !--- Defines an IKE policy. !--- Use the crypto
isakmp policy !--- command in global configuration mode.
IKE policies !--- define a set of parameters !--- that
are used during the IKE phase I negotiation. hash md5
authentication pre-share !--- Specifies preshared keys
as the authentication method. crypto isakmp key cisco123
address 99.99.99.2 !--- Configures a preshared
authentication key, !--- used in global configuration
mode. ! crypto ipsec transform-set rtpset esp-des esp-
md5-hmac !--- Defines a transform-set. This is an !---
acceptable combination of security protocols and
algorithms, !--- which has to be matched on the peer
router. crypto map rtp 1 ipsec-isakmp !--- Indicates
that IKE is used to establish !--- the IPSec SAs that
protect the traffic !--- specified by this crypto map
entry. set peer 99.99.99.2 !--- Sets the IP address of
the remote end. set transform-set rtpset !--- Configures
IPSec to use the transform-set !--- "rtpset" defined
earlier. match address 115 !--- Used to assign an
extended access list to a !--- crypto map entry which is
used by IPSec !--- to determine which traffic should be
protected !--- by crypto and which traffic does not !---
need crypto protection. . . !--- Output suppressed. . .
! interface Ethernet3/0 ip address 95.95.95.2
255.255.255.0 no ip directed-broadcast ip nat outside !-
- Indicates that the interface is !--- connected to the
outside network. no ip route-cache !--- Enable process
switching for !--- IPSec to encrypt outgoing packets. !-
- This command disables fast switching. no ip mroute-
cache crypto map rtp !--- Configures the interface to
use the !--- crypto map "rtp" for IPSec. ! interface

```

```

Ethernet3/2 ip address 10.103.1.75 255.255.255.0 no ip
directed-broadcast ip nat inside !--- Indicates that the
interface is connected to !--- the inside network (the
network subject to NAT translation). ! ip nat pool FE30
95.95.95.10 95.95.95.10 netmask 255.255.255.0 !--- Used
to define a pool of IP addresses for !--- NAT. Use the
ip nat pool command in !--- global configuration mode.
ip nat inside source route-map nonat pool FE30 overload
!--- Used to enable NAT of !--- the inside source
address. Use the ip nat inside source !--- command in
global configuration mode. !--- The 'overload' option
enables the router to use one global !--- address for
many local addresses. ip classless ip route 0.0.0.0
0.0.0.0 95.95.95.1 !--- Default route to the next hop
address. no ip http server ! access-list 110 deny ip
10.103.1.0 0.0.0.255 98.98.98.0 0.0.0.255 access-list
110 permit ip 10.103.1.0 0.0.0.255 any !--- Addresses
that match this ACL are NATed while !--- they access the
Internet. They are not NATed !--- if they access the
98.98.98.0 network. access-list 115 permit ip 10.103.1.0
0.0.0.255 98.98.98.0 0.0.0.255 !--- This access-list
option causes all IP traffic that !--- matches the
specified conditions to be !--- protected by IPSec using
the policy described !--- by the corresponding crypto
map command statements. access-list 115 deny ip
10.103.1.0 0.0.0.255 any route-map nonat permit 10 match
ip address 110 ! ! line con 0 line vty 0 4 ! end

```

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

Для проверки этой конфигурации воспользуйтесь расширенной командой ping с интерфейса Ethernet на частном маршрутизаторе 10.103.1.75, адресованной интерфейсу Ethernet на открытом маршрутизаторе 98.98.98.1

- [команда ping](#) — [Используется для диагностики подключения основной сети.](#) rp-3640-6a#ping Protocol [ip]: Target IP address: 98.98.98.1 Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y Source address or interface: 10.103.1.75 Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 98.98.98.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
- [show crypto ipsec sa](#) — [показывает настройки, используемые текущими ассоциациями безопасности IPSec.](#)
- [show crypto isakmp sa](#) — [отображает все текущие ассоциации безопасности \(SA\) IKE узла.](#)
- [show crypto engine](#) — [показывает сводку по конфигурации криптоядер.](#) Команду show crypto engine следует выполнять в привилегированном режиме EXEC.

Образец команды show output

Ниже показаны выходные данные при выполнении команды `show crypto ipsec sa` на маршрутизаторе-концентраторе.

```
rp-3640-6a#show crypto ipsec sa interface: Ethernet0/0 Crypto map tag: rtp, local addr.
95.95.95.2 protected vrf: local ident (addr/mask/prot/port): (10.103.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (98.98.98.0/255.255.255.0/0/0) current_peer: 99.99.99.2:500
PERMIT, flags={origin_is_acl,} #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5 #pkts decaps:
14, #pkts decrypt: 14, #pkts verify 14 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0 local crypto endpt.: 95.95.95.2, remote crypto endpt.: 99.99.99.2
path mtu 1500, media mtu 1500 current outbound spi: 75B6D4D7 inbound esp sas: spi:
0x71E709E8(1910966760) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2000, flow_id: 1, crypto map: rtp sa timing: remaining key lifetime (k/sec):
(4576308/3300) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas:
outbound esp sas: spi: 0x75B6D4D7(1974916311) transform: esp-des esp-md5-hmac , in use settings
={Tunnel, } slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp sa timing: remaining key
lifetime (k/sec): (4576310/3300) IV size: 8 bytes replay detection support: Y outbound ah sas:
outbound pcp sas:
```

Эта команда отображает ассоциации безопасности IPSec, установленные между одноранговыми сторонами. Между узлами 95.95.95.2 и 99.99.99.2 создается зашифрованный туннель, обеспечивающий передачу трафика между сетями 98.98.98.0 и 10.103.1.0. Можно видеть, что входящий и исходящий потоки формируют две ассоциации безопасности (SA) протокола инкапсулирующей защиты содержимого (ESP). Ассоциации безопасности заголовка аутентификации (AH) не используются, поскольку таких заголовков нет.

[Устранение неполадок](#)

В этом разделе описывается процесс устранения неполадок конфигурации.

[Команды для устранения неполадок](#)

Некоторые команды `show` поддерживаются Средством интерпретации выходных данных (только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды `show`.

Примечание: Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

- `debug crypto ipsec sa`– служит для просмотра данных о согласовании IPSec на 2-м этапе.
- `debug crypto isakmp sa`– служит для просмотра данных о согласовании ISAKMP на 1-м этапе.
- `debug crypto engine`– служит для просмотра шифруемых сеансов.

[Дополнительные сведения](#)

- [Преобразование сетевых адресов: порядок работы](#)
- [Устранение проблем IPSec — общие сведения и использование команд debug](#)
- [Страница поддержки IPSec](#)
- [Страница поддержки NAT](#)
- [Техническая поддержка - Cisco Systems](#)