



# Настройка GRE-туннеля по протоколу IPSec при помощи OSPF

---

## Содержание

### Общие сведения

#### Предварительные условия

Требования

Используемые компоненты

Условные обозначения

#### Настройка

Схема сети

Конфигурации

#### Проверка

#### Устранение неполадок

Команды диагностики

#### Дополнительные сведения

---

## Введение

Обычные настройки IP Security (IPSec) запрещают передачу по протоколам маршрутизации, таким как усовершенствованный внутренний протокол маршрутизации шлюзов (EIGRP) и протокол первоочередного предпочтения кратчайшего пути (OSPF), а также трафик не по протоколу IP, а, например, по IPX или AppleTalk. Этот документ иллюстрирует процесс организации передачи данных между разными сетями, использующими протокол маршрутизации и передающими данные не по протоколу IP с IPSec. В данном примере используется общая инкапсуляция маршрутов (GRE) для реализации маршрутизации между различными сетями.

Для получения информации о конфигурации сети со звездообразной топологией и протоколом IPSec для трех маршрутизаторов см. документ "Настройка звездообразной сети между маршрутизаторами с протоколом IPSec и связью между конечными точками".

Для получения информации о настройке базовой конфигурации Cisco IOS® для GRE-туннеля с преобразованием сетевых адресов (NAT) см. документ "Настройка протокола IPSec между маршрутизаторами (с предварительно распределяемыми ключами) в GRE-туннеле с брандмауэром IOS и NAT".

Для получения информации о настройке VPN/IPsec с протоколом OSPF с помощью программного обеспечения Cisco PIX Security Appliance версии 7.x или Cisco Adaptive Security Appliance (ASA) см. документ "Настройка PIX/ASA 7.x VPN/IPsec с примером конфигурации OSPF".

## Предварительные условия

### Требования

Прежде чем использовать эту конфигурацию, убедитесь, что выполняются следующие требования:

- Перед применением криптокарт убедитесь в работоспособности туннеля.
- Для получения информации о возможных проблемах с модулем MTU см. документ "Настройка IP MTU, TCP MSS и PMTUD в операционных системах Windows и Sun".

### Используемые компоненты

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

- Cisco 3600 с запускаемым программным обеспечением Cisco IOS, издание 12.4(8)
- Cisco 2600 с запускаемым программным обеспечением Cisco IOS, издание 12.4(8)
- Программное обеспечение PIX Firewall, издание 6.3(5)
- Программное обеспечение PIX Firewall, издание 6.3(5)

Указанные в данном документе сведения по устройствам были получены в конкретной лабораторной среде. При написании данного документа использовались только устройства с чистой (стандартной) конфигурацией. В производственной сети необходимо изучить потенциальное воздействие всех команд.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. в документе "Условные обозначения технических терминов Cisco".

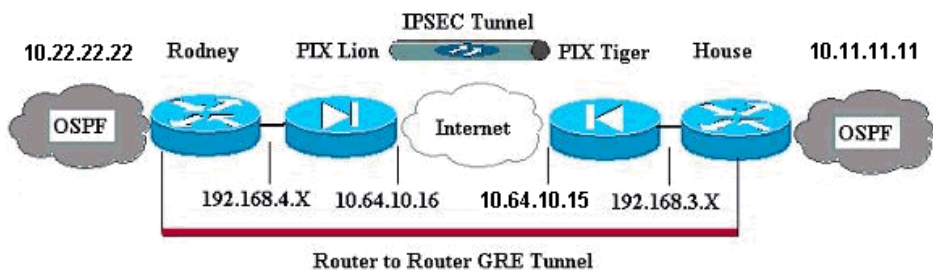
Настройка

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

**Примечание:** для поиска дополнительной информации о командах, упоминаемых в данном документе, используйте средство Command Lookup Tool (только для зарегистрированных пользователей).

Схема сети

В данном документе используется следующая настройка сети:



**Примечание:** схемы IP-адресации, которые использованы в данной конфигурации, запрещено распространять в Интернете. Это адреса RFC 1918 , которые использовались в лабораторной среде.

Конфигурации

В данном документе используются следующие конфигурации:

- PIX Lion
- PIX Tiger
- Router Rodney
- Router House

## PIX Lion

```
PIX версии 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
```

### hostname Lion

```
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
```

*!--- Определяет целевой трафик, защищенный туннелем IPSec.*

```
access-list 101 permit gre 192.168.4.0 255.255.255.0 192.168.3.0 255.255.255.0
```

*!--- NAT не используется для передачи данных к другому брандмауэру PIX Firewall.*

```
access-list nonat permit gre 192.168.4.0 255.255.255.0 192.168.3.0 255.255.255.0
```

```
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
```

```
ip address outside 10.64.10.16 255.255.255.224
```

```
ip address inside 192.168.4.1 255.255.255.0
```

*!--- Выходные данные подавлены.*

```
global (outside) 1 interface
```

*!--- Не используйте NAT для передачи данных.*

```
nat (inside) 0 access-list nonat
```

```
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

```
route outside 0.0.0.0 0.0.0.0 10.64.10.1 1
```

```
timeout xlate 3:00:00
```

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 s0
```

```
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
```

```
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
```

```
timeout uauth 0:05:00 absolute
```

```
aaa-server TACACS+ protocol tacacs+
```

```
aaa-server TACACS+ max-failed-attempts 3
```

```
aaa-server TACACS+ deadtime 10
```

```
aaa-server RADIUS protocol radius
```

```
aaa-server RADIUS max-failed-attempts 3
```

```
aaa-server RADIUS deadtime 10
```

```
aaa-server LOCAL protocol local
```

```
no snmp-server location
```

```
no snmp-server contact
```

```
snmp-server community public
```

```
no snmp-server enable traps
```

```
floodguard enable
```

*!--- Доверяйте трафику IPSec и избегайте прохождения*

*!--- списков управления доступом (ACL)/NAT.*

```
sysopt connection permit-ipsec
```

```
!--- Конфигурация IPSec.
```

```
crypto ipsec transform-set pixset esp-des esp-md5-hmac
crypto map pixmap 20 ipsec-isakmp
crypto map pixmap 20 match address 101
crypto map pixmap 20 set peer 10.64.10.15
crypto map pixmap 20 set transform-set pixset
crypto map pixmap interface outside
isakmp enable outside
```

```
!--- Параметры IKE.
```

```
isakmp key ***** address 10.64.10.15 netmask 255.255.255.255
isakmp identity address
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 1
isakmp policy 20 lifetime 3600
telnet timeout 5
ssh 64.104.205.124 255.255.255.255 outside
ssh timeout 5
terminal width 80
Cryptochecksum:d39b3d449563c7cd434b43f82f0f0a21
: end
```

## PIX Tiger

```
PIX версии 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Tiger
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list 101 permit gre 192.168.3.0 255.255.255.0 192.168.4.0 255.255.255.0

access-list nonat permit gre 192.168.3.0 255.255.255.0 192.168.4.0 255.255.255.0
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 10.64.10.15 255.255.255.224
ip address inside 192.168.3.1 255.255.255.0
```

```
!--- Выходные данные подавлены.
```

```
global (outside) 1 interface
```

```
!--- Не используйте NAT для передачи данных.
```

```
nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 10.64.10.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 s0
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec

!--- Параметры IPSec.

crypto ipsec transform-set pixset esp-des esp-md5-hmac
crypto map pixmap 20 ipsec-isakmp
crypto map pixmap 20 match address 101
crypto map pixmap 20 set peer 10.64.10.16
crypto map pixmap 20 set transform-set pixset
crypto map pixmap interface outside

!--- Параметры IKE.

isakmp enable outside
isakmp key ***** address 10.64.10.16 netmask 255.255.255.255
isakmp identity address
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 1
isakmp policy 20 lifetime 3600
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:a0a7ac847b05d9d080d1c442ef053a0b
: end
```

## Router Rodney

```
версии 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rodney
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!
!
interface Loopback1
ip address 10.22.22.22 255.255.255.0
!
interface Tunnel0
ip address 10.1.1.2 255.255.255.0

!--- Начальная точка туннеля.

tunnel source Ethernet0/1

!--- Конечная точка туннеля.

tunnel destination 192.168.3.2
!
interface Ethernet0/0
```

```
no ip address
!
interface Serial0/0
no ip address
shutdown
!
interface Ethernet0/1
ip address 192.168.4.2 255.255.255.0
!
interface Serial0/1
no ip address
shutdown
!
router ospf 22
log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0
network 10.22.22.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.4.1

!--- Трафик 10.10.10.0, проходящий через
!--- GRE-туннель.

ip route 10.10.10.0 255.255.255.0 Tunnel0
no ip http server
!
line con 0
line aux 0
line vty 0 4
login
!
end!
End
```

## Router House

```
версии 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
!
ip subnet-zero
no ip domain-lookup
!
!
interface Loopback1
ip address 10.11.11.11 255.255.255.0
!
interface Tunnel0
ip address 10.1.1.1 255.255.255.0

!--- Начальная точка туннеля.

tunnel source FastEthernet0/1

!--- Конечная точка туннеля.

tunnel destination 192.168.4.2
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.3.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
```

```
speed auto
!
router ospf 11
log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0
network 10.11.11.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.3.1

!--- Трафик 10.20.20.0, проходящий через
!--- GRE-туннель.

ip route 10.20.20.0 255.255.255.0 Tunnel0
ip http server
!
line con 0
line aux 0
line vty 0 4
```

## Проверка

Для этой конфигурации отсутствует процедура проверки.

## Устранение неполадок

В данном разделе описывается процесс устранения неполадок конфигурации.

Дополнительные сведения об устранении неполадок в PIX и туннелях IPSec см. в документе "Устранение неполадок PIX при передаче трафика по установленному туннелю IPSec".

### Команды диагностики

Средство Output Interpreter Tool (только для зарегистрированных пользователей) (OIT) поддерживает некоторые команды **show**. Используйте OIT для просмотра аналитики выходных данных команды **show**.

**Примечание:** ознакомьтесь с документом "Важные сведения о командах отладки", прежде чем применять команды **debug**.

### Безошибочная отладка PIX IPSec

- show crypto isakmp sa** — отображает сопоставление безопасности (SA) протокола ISAKMP, построенную между двумя одноранговыми узлами.

```
Lion#show crypto isakmp sa
Total : 1
Embryonic : 0
dst src state pending created
10.64.10.15 10.64.10.16 QM_IDLE 0 1

Tiger#show crypto isakmp sa
Total SAs : 1
Embryonic : 0
dst src state pending created
10.64.10.15 10.64.10.16 QM_IDLE 0 1
```

- show crypto engine connection active** — отображает все встроенные сопоставления безопасности второго этапа и объем отправленного трафика.

```
Lion#show crypto engine connection active
```

```
Crypto Engine Connection Map:
```

```
size = 8, free = 6, used = 2, active = 2
```

```
Tiger#show crypto engine connection active
```

```
Crypto Engine Connection Map:
```

```
size = 8, free = 6, used = 2, active = 2
```

- **show debug** — отображает выходные данные команды "debug".

```
Lion#show debug
```

```
debug crypto ipsec
```

```
debug crypto isakmp
```

```
debug crypto engine
```

```
crypto_isakmp_process_block: src 10.64.10.15, dest 10.64.10.16
```

```
OAK_MM exchange
```

```
ISAKMP (0): processing SA payload. message ID = 0
```

```
ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy
```

```
ISAKMP: encryption DES-CBC
```

```
ISAKMP: hash MD5
```

```
ISAKMP: default group 1
```

```
ISAKMP: auth pre-share
```

```
ISAKMP: life type in seconds
```

```
ISAKMP: life duration (basic) of 3600
```

```
ISAKMP (0): atts are acceptable. Next payload is 0
```

```
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
```

```
return status is IKMP_NO_ERROR#
```

```
crypto_isakmp_process_block: src 10.64.10.15, dest 10.64.10.16
```

```
OAK_MM exchange
```

```
ISAKMP (0): processing KE payload. message ID = 0
```

```
ISAKMP (0): processing NONCE payload. message ID = 0
```

```
ISAKMP (0): processing vendor id payload
```

```
ISAKMP (0): speaking to another IOS box!
```

```
ISAKMP (0): ID payload
```

```
next-payload : 8
```

```
type : 1
```

```
protocol : 17
```

```
port : 500
```

```
length : 8
```

```
ISAKMP (0): Total payload length: 12
```

```
return status is IKMP_NO_ERROR
```

```
crypto_isakmp_process_block: src 10.64.10.15, dest 10.64.10.16
```

```
OAK_MM exchange
```

```
ISAKMP (0): processing ID payload. message ID = 0
```

```
ISAKMP (0): processing HASH payload. message ID = 0
```

```
ISAKMP (0): SA has been authenticated
```

```
ISAKMP (0): beginning Quick Mode exchange, M-ID of 1220019031:48b80357IPSEC(key.
```

```
IPSEC(spi_response): getting spi 0xa67177c5(2792454085) for SA
```

```
from 10.64.10.15 to 10.64.10.16 for prot 3
```

```
return status is IKMP_NO_ERROR
```

```
crypto_isakmp_process_block: src 10.64.10.15, dest 10.64.10.16
```

```
OAK_QM exchange
```

```
oakley_process_quick_mode:
```

```
OAK_QM_IDLE
```

```
ISAKMP (0): processing SA payload. message ID = 1220019031
```

```
ISAKMP : Checking IPSec proposal 1
```

```
ISAKMP: transform 1, ESP_DES
```

```
ISAKMP: attributes in transform:
```

```
ISAKMP: encaps is 1
```

```
ISAKMP: SA life type in seconds
```

```
ISAKMP: SA life duration (basic) of 28800
```

```
ISAKMP: SA life type in kilobytes
```

```
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
```

```
ISAKMP: authenticator is HMAC-MD5
```

```
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part,
```

```
(key eng. msg.) dest= 10.64.10.15, src= 10.64.10.16,
```

```
dest_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4),
```

```
src_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
```

```
protocol= ESP, transform= esp-des esp-md5-hmac ,
```

```
lifedur= 0s and 0kb,
```

```
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
```



```

ISAKMP (0): processing NONCE payload. message ID = 1220019031

ISAKMP (0): processing ID payload. message ID = 1220019031
ISAKMP (0): processing ID payload. message ID = 1220019031map_alloc_entry: allo2
map_alloc_entry: allocating entry 1

ISAKMP (0): Creating IPSec SAs
inbound SA from 10.64.10.15 to 10.64.10.16 (proxy 192.168.3)
has spi 2792454085 and conn_id 2 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 10.64.10.16 to 10.64.10.15 (proxy 192.168.)
has spi 285493108 and conn_id 1 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 10.64.10.16, src= 10.64.10.15,
dest_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0xa67177c5(2792454085), conn_id= 2, keysizes= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 10.64.10.16, dest= 10.64.10.15,
src_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
dest_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0x11044774(285493108), conn_id= 1, keysizes= 0, flags= 0x4

return status is IKMP_NO_ERROR

```

## Прохождение маршрутизации и запросов "ping" в GRE-туннеле для маршрутизатора

- **show ip route** — отображает элементы таблицы IP-маршрутизации.

```

rodney#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 192.168.4.1 to network 0.0.0.0

10.0.0.0/24 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
C 10.20.20.0 is directly connected, Loopback0
10.0.0.0/24 is subnetted, 1 subnets
C 10.22.22.0 is directly connected, Loopback1
C 192.168.4.0/24 is directly connected, Ethernet0/1
10.0.0.0/24 is subnetted, 1 subnets
S 10.10.10.0 is directly connected, Tunnel0
10.0.0.0/32 is subnetted, 1 subnets
O 10.11.11.11 [110/11112] via 10.1.1.1, 03:34:01, Tunnel0
S* 0.0.0.0/0 [1/0] via 192.168.4.1
rodney#
rodney#ping 10.11.11.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.11.11.11, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```

```

house#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

```

```
Gateway of last resort is 192.168.3.1 to network 0.0.0.0

10.0.0.0/24 is subnetted, 1 subnets
C 1.1.1.0 is directly connected, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
S 10.20.20.0 is directly connected, Tunnel0
10.0.0.0/32 is subnetted, 1 subnets
O 10.22.22.22 [110/11112] via 10.1.1.2, 03:33:39, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
C 10.10.10.0 is directly connected, Loopback0
10.0.0.0/24 is subnetted, 1 subnets
C 10.11.11.0 is directly connected, Loopback1
C 192.168.3.0/24 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 192.168.3.1

house#ping 10.22.22.22

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

## Дополнительные сведения

- **Согласование IPSec/протоколы IKE**
- **Документация по PIX Firewall**
- **Справочник по командам PIX**
- **Поддержка продукта PIX**
- **Техническая поддержка & документация - Cisco Systems**

---

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

---

Дата генерации PDF файла: Jan 05, 2010

---

[http://www.cisco.com/support/RU/customer/content/9/92034/gre\\_ipsec\\_ospf.shtml](http://www.cisco.com/support/RU/customer/content/9/92034/gre_ipsec_ospf.shtml)

---