

Пример конфигурации туннеля между локальными сетями (LAN-to-LAN) IPsec между Catalyst 6500 с сервисным модулем VPN и брандмауэром PIX

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Общие сведения](#)

[Настройка](#)

[Схема сети](#)

[Настройка для IPsec с использованием порта доступа или группового порта 2-го уровня](#)

[Конфигурация для IPsec с использованием маршрутизируемого порта](#)

[Проверка](#)

[Устранение неполадок](#)

[Команды устранения неполадок](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает, как создать IPSec-туннель между локальными сетями между коммутатором Cisco Catalyst серии 6500 с сервисным модулем IPSEC VPN (W) и Межсетевым экраном Cisco PIX.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Релиз 12.2 Программного обеспечения Cisco IOS (14) SY2 для Supervisor Engine

Коммутатора Catalyst серии 6000, с сервисным модулем IPSEC VPN

- Версия 6.3 (3) программного обеспечения Cisco PIX Firewall

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 см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

Общие сведения

Сервисный модуль VPN Catalyst 6500 имеет два порта Gigabit Ethernet (GE) без видимых снаружи разъемов. Эти порты предусматривают обращение только для целей настройки. Порт 1 всегда является внутренним. Этот порт обслуживает весь обмен трафиком с внутренней сетью. Второй порт (порт 2) обслуживает весь обмен трафиком с глобальной сетью WAN или внешними сетями. Эти два порта всегда настраиваются в режиме группообразования 802.1Q. Сервисный модуль сети VPN обрабатывает пакетный трафик по методике перехвата.

Пакеты обрабатываются парой сетей VLAN: внутренней сетью 3-го уровня и внешней сетью 2-го уровня. Для маршрутизации пакетов из внутренней сети во внешнюю применяется метод, именуемый «кодируемой логикой распознавания адресов» (EARL) и действующий для внутренней сети VLAN. После шифрования пакетов сервисный модуль сети VPN использует соответствующую внешнюю сеть VLAN. В процессе расшифровки пакеты, поступающие с внешней стороны во внутреннюю, передаются сервисному модулю сети VPN по мостовому соединению с использованием внешней сети VLAN. После того как сервисный модуль VPN расшифрует пакет и назначит сеть VLAN на соответствующую внутреннюю сеть VLAN, EARL выполняет маршрутизацию пакета на подходящий порт сети LAN. Уровень 3 в VLAN и Уровне 2 вне VLAN объединен с командой **crypto connect vlan**. В коммутаторах серии Catalyst 6500 имеются три типа портов:

- **Маршрутизируемые порты** — По умолчанию, все Порты Ethernet являются маршрутизируемыми портами в Cisco IOS. С этими портами связана скрытая сеть VLAN.
- **Порты доступа.** С этими портами связана внешняя сеть VLAN или сеть VLAN протокола группообразования (VTP). С конкретной сетью VLAN можно связать сразу несколько портов.
- **Групповые порты.** Эти порты служат для транспортировки большого числа внешних сетей VLAN или VTP VLAN, в которых все пакеты инкапсулируются с заголовком 802.1Q.

Настройка

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

Примечание: [Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд \(только для зарегистрированных клиентов\).](#)

Схема сети

В настоящем документе используется следующая схема сети:

Настройка для IPsec с использованием порта доступа или группового порта 2-го уровня

Чтобы настроить IPsec с использованием порта доступа или группового порта 2-го уровня для внешнего физического интерфейса, выполните следующие шаги.

1. Добавьте внутренние сети VLAN на внутренний порт сервисного модуля VPN. Предположим, что сервисный модуль VPN занимает слот 4. В качестве внутренней сети VLAN используется сеть 100, а в качестве внешней — 209. Настройте порты GE сервисного модуля сети VPN следующим образом:

```
interface GigabitEthernet4/1
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable
```

```
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
```

2. VLAN 100 (-interface Vlan 209,).

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224
```

```
interface Vlan209
no ip address
crypto connect vlan 100
```

3. Настройте внешний физический порт как доступ или магистральный порт (в этом случае, FastEthernet 2/48, как показано здесь).

```
!--- This is the configuration that uses an access port. interface FastEthernet2/48
no ip address
switchport
switchport access vlan 209
switchport mode access
```

```
!--- This is the configuration that uses a trunk port. interface FastEthernet2/48
no ip address switchport
switchport trunk encapsulation dot1q
switchport mode trunk
```

4. Создайте обходное преобразование NAT. Добавьте следующие записи к оператору `no nat` для исключения преобразования NAT между этими сетями:

```
!--- This is the configuration that uses an access port. interface FastEthernet2/48
no ip address
switchport
```

```
switchport access vlan 209
switchport mode access
```

```
!--- This is the configuration that uses a trunk port. interface FastEthernet2/48
no ip address switchport
switchport trunk encapsulation dot1q
switchport mode trunk
```

5. Создайте собственную конфигурацию шифрования и список контроля доступа (ACL) для определения трафика, подлежащего шифрованию. Создайте Кристо-ACL (в этом случае, ACL 100 - Представляющий интерес трафик), который определяет трафик от внутренней сети 192.168.5.0/24 к удаленной сети 192.168.6.0/24, как это:

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

Определите собственные предложения политик протокола ISAKMP, например:

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

Выполните следующую команду (в данном примере) для использования и задания

предварительно согласованных ключей:

```
crypto isakmp key cisco address 10.66.79.73
```

Определите предложения IPsec, например:

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

Создайте собственный оператор crypto map, например:

```
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.73
set transform-set cisco
match address 100
```

6. Примените оператор crypto map к интерфейсу VLAN 100, например:

```
interface vlan100
crypto map cisco
```

Используются следующие конфигурации:

- [Catalyst 6500](#)
- [Сетевой экран PIX](#)

Catalyst 6500

```
!--- Define the Phase 1 policy. crypto isakmp policy 1
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 10.66.79.73
!
!
!--- Define the encryption policy for this setup. crypto
ipsec transform-set cisco esp-des esp-md5-hmac
!
!--- Define a static crypto map entry for the peer !---
with mode ipsec-isakmp. !--- This indicates that
Internet Key Exchange (IKE) !--- is used to establish
the IPsec !--- security associations (SAs) to protect
the traffic !--- specified by this crypto map entry.
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.73
set transform-set cisco
match address 100
!
!
```

```

no spanning-tree vlan 100
!
!
!
interface FastEthernet2/1
 ip address 192.168.5.1 255.255.255.0
!
!--- This is the outside Layer 2 port that allows !---
VLAN 209 traffic to enter. interface FastEthernet2/48 no
ip address switchport switchport trunk encapsulation
dot1q switchport mode trunk ! interface
GigabitEthernet4/1 no ip address flowcontrol receive on
flowcontrol send off switchport switchport trunk
encapsulation dot1q !--- VLAN 100 is defined as the
Interface VLAN (IVLAN). switchport trunk allowed vlan
1,100,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet4/2
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
!--- The Port VLAN (PVLAN) configuration is handled
transparently by !--- the VPN service module without
user configuration !--- or involvement. It also is not
shown in the configuration. !--- Note: For every IVLAN,
a corresponding PVLAN exists.

switchport trunk allowed vlan 1,209,1002-1005
 switchport mode trunk
 cdp enable
 spanning-tree portfast trunk
!
interface Vlan1
 no ip address
 shutdown
!
!--- This is the IVLAN that is configured to intercept
the traffic !--- destined to the secure port on which
the inside port !--- of the VPN service module is the
only port present. interface Vlan100 ip address
10.66.79.180 255.255.255.224 crypto map cisco
!--- This is the secure port that is a virtual Layer 3
interface. !--- This interface purposely does not have a
Layer 3 IP address !--- configured. This is normal for
the BITW process. !--- The IP address is moved from this
interface to the VLAN 100 to !--- accomplish BITW. This
brings the VPN service module into !--- the packet path.
interface Vlan209 no ip address crypto connect vlan 100
!
ip classless

global (outside) 1 interface
!--- NAT 0 prevents NAT for networks specified in the
ACL inside_nat0_outbound. nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 192.168.5.0
255.255.255.0 !--- Configure the routing so that the
device !--- is directed to reach its destination
network. ip route 0.0.0.0 0.0.0.0 10.66.79.161
!--- This access list (inside_nat0_outbound) is used
with the nat zero command. !--- This prevents traffic

```

```
which matches the access list from undergoing !---
network address translation (NAT). The traffic specified
by this ACL is !--- traffic that is to be encrypted and
!--- sent across the VPN tunnel. This ACL is
intentionally !--- the same as (100). !--- Two separate
access lists should always be used in this
configuration. access-list inside_nat0_outbound permit
ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

```
!--- This is the crypto ACL. access-list 100 permit ip
192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

Сетевой экран PIX

```
SV2-8(config)# show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
interface ethernet6 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
nameif ethernet6 intf6 security30
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SV2-8
domain-name cisco.com
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 ils 389
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
!--- This is the traffic to the router. access-list 100
permit ip 192.168.6.0 255.255.255.0 192.168.5.0
255.255.255.0
access-list nonat permit ip 192.168.6.0 255.255.255.0
192.168.5.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
ip address outside 10.66.79.73 255.255.255.224
```

```
ip address inside 192.168.6.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
no ip address intf3
no ip address intf4
no ip address intf5
no ip address intf6
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
no failover ip address intf6
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 192.168.6.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 10.66.79.65 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- These are IPsec policies. sysopt connection permit-
ipsec
crypto ipsec transform-set cisco esp-des esp-md5-hmac
crypto map cisco 10 ipsec-isakmp
crypto map cisco 10 match address 100
crypto map cisco 10 set peer 10.66.79.180
crypto map cisco 10 set transform-set cisco
crypto map cisco interface outside
!--- These are IKE policies. isakmp enable outside
isakmp key ***** address 10.66.79.180 netmask
255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:244c86c9beab00bda8f790502ca74db9
: end
```

[Конфигурация для IPsec с использованием маршрутизируемого порта](#)

Чтобы настроить IPsec с использованием маршрутизируемого порта 3-го уровня для внешнего физического интерфейса, выполните следующие шаги.

1. Добавьте внутренние сети VLAN на внутренний порт сервисного модуля VPN. Предположим, что сервисный модуль VPN занимает слот 4. В качестве внутренней сети VLAN используется сеть 100, а в качестве внешней — 209. Настройте порты GE сервисного модуля сети VPN следующим образом:

```
interface GigabitEthernet4/1
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable
```

```
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
```

2. Добавьте интерфейс VLAN 100 и интерфейс, где туннель завершен (который, в этом случае, является FastEthernet2/48, как показано здесь).

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224
```

```
interface FastEthernet2/48
no ip address
crypto connect vlan 100
```

3. Создайте обходное преобразование NAT. Добавьте следующие записи к оператору по nat для исключения преобразования NAT между этими сетями:

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224
```

```
interface FastEthernet2/48
no ip address
crypto connect vlan 100
```

4. Создайте собственную конфигурацию шифрования и ACL для определения трафика, подлежащего шифрованию. Создайте список контроля доступа (в данном случае – ACL 100), который описывал бы трафик из внутренней сети 192.168.5.0/24 в удаленную сеть 192.168.6.0/24, например следующего вида:

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

Определите предложения политик ISAKMP, например:

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

Выполните следующую команду (в данном примере) для использования и задания предварительно согласованных ключей:

```
crypto isakmp key cisco address 10.66.79.73
```

Определите предложения IPsec, например:

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```


Создайте собственный оператор crypto map, например:

```
crypto map cisco 10 ipsec-isakmp
  set peer 10.66.79.73
  set transform-set cisco
  match address 100
```

5. Примените оператор crypto map к интерфейсу VLAN 100, например:

```
interface vlan100
  crypto map cisco
```

Используются следующие конфигурации:

- [Catalyst 6500](#)
- [Сетевой экран PIX](#)

Catalyst 6500

```
!--- Define the Phase 1 policy. crypto isakmp policy 1
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.66.79.73
!
!
!--- Define the encryption policy for this setup. crypto
ipsec transform-set cisco esp-des esp-md5-hmac
!
!--- Define a static crypto map entry for the peer !---
with mode ipsec-isakmp. !--- This indicates that IKE is
used to establish the !--- IPsec SAs to protect the
traffic !--- specified by this crypto map entry. crypto
map cisco 10 ipsec-isakmp
  set peer 10.66.79.73
  set transform-set cisco
  match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet2/1
  ip address 192.168.5.1 255.255.255.0
!
!--- This is the secure port that is configured in
routed port mode. !--- This routed port mode does not
have a Layer 3 IP address !--- configured. This is
normal for the BITW process. !--- The IP address is
moved from this interface to the VLAN 100 to !---
accomplish BITW. This brings the VPN service module into
!--- the packet path. This is the Layer 2 port VLAN on
which the !--- outside port of the VPN service module
also belongs. ! interface FastEthernet2/48 no ip address
crypto connect vlan 100
!
interface GigabitEthernet4/1
  no ip address
  flowcontrol receive on
  flowcontrol send off
  switchport
  switchport trunk encapsulation dot1q
!--- VLAN 100 is defined as the IVLAN.  switchport trunk
allowed vlan 1,100,1002-1005
```

```

switchport mode trunk
cdp enable
!
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
!--- The PVLAN configuration is handled transparently by
the !--- VPN service module without user configuration
!--- or involvement. It also is not shown in the
configuration. !--- Note: For every IVLAN, a
corresponding PVLAN exists.

switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
!
interface Vlan1
no ip address
shutdown
!
!--- This is the IVLAN that is configured to intercept
the traffic !--- destined to the secure port on which
the inside port of the !--- VPN service module is the
only port present. interface Vlan100 ip address
10.66.79.180 255.255.255.224 crypto map cisco
!--- This is the secure port that is a virtual Layer 3
interface. !--- This interface purposely does not have a
Layer 3 IP address !--- configured. This is normal for
the BITW process. !--- The IP address is moved from this
interface to the VLAN 100 to !--- accomplish BITW. This
brings the VPN service module into !--- the packet path.
! ip classless global (outside) 1 interface !--- NAT 0
prevents NAT for networks specified in the ACL
inside_nat0_outbound. nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 192.168.6.0
255.255.255.0 !--- Configure the routing so that the
device !--- is directed to reach its destination
network. ip route 0.0.0.0 0.0.0.0 10.66.79.161
!
!--- This access list (inside_nat0_outbound) is used
with the nat zero command. !--- This prevents traffic
which matches the access list from undergoing !---
network address translation (NAT). The traffic specified
by this ACL is !--- traffic that is to be encrypted and
!--- sent across the VPN tunnel. This ACL is
intentionally !--- the same as (100). !--- Two separate
access lists should always be used in this
configuration.

access-list inside_nat0_outbound permit ip 192.168.5.0
0.0.0.255 192.168.6.0 0.0.0.255

!--- This is the crypto ACL. access-list 100 permit ip
192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

```

Сетевой экран PIX

```

SV2-8(config)# show run
: Saved

```

```
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
interface ethernet6 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
nameif ethernet6 intf6 security30
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SV2-8
domain-name cisco.com
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 ils 389
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
!--- This is the traffic to the router. access-list 100
permit ip 192.168.6.0 255.255.255.0 192.168.5.0
255.255.255.0
access-list nonat permit ip 192.168.6.0 255.255.255.0
192.168.5.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
ip address outside 10.66.79.73 255.255.255.224
ip address inside 192.168.6.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
no ip address intf3
no ip address intf4
no ip address intf5
no ip address intf6
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
```

```

no failover ip address intf4
no failover ip address intf5
no failover ip address intf6
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 192.168.6.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 10.66.79.65 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- These are IPSec policies. sysopt connection permit-
ipsec
crypto ipsec transform-set cisco esp-des esp-md5-hmac
crypto map cisco 10 ipsec-isakmp
crypto map cisco 10 match address 100
crypto map cisco 10 set peer 10.66.79.180
crypto map cisco 10 set transform-set cisco
crypto map cisco interface outside
!--- These are IKE policies. isakmp enable outside
isakmp key ***** address 10.66.79.180 netmask
255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:244c86c9beab00bda8f790502ca74db9
: end

```

Проверка

В этом разделе дается информация для проверки правильности функционирования вашей конфигурации.

[Средство Output Interpreter \(OIT\) \(только для зарегистрированных клиентов\) поддерживает определенные команды show.](#) Посредством OIT можно анализировать выходные данные команд show.

- **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 vlan`— показывает сеть VLAN, связанную с конфигурацией шифрования.
- `show crypto eli` — показывает статистику сервисного модуля сети VPN.

[Дополнительные сведения о проверке и устранении проблем с IPSec см. в документе Устранение проблем, связанных с безопасностью IP. Обзор команд debug и порядок их использования.](#)

Устранение неполадок

В этом разделе содержатся сведения по устранению неполадок конфигурации.

Команды устранения неполадок

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

- команда `debug crypto ipsec` отображает согласование IPSec на втором этапе.
- `debug crypto isakmp` – вывод данных о согласовании ISAKMP в фазе 1.
- "debug crypto engine" - отображается зашифрованный трафик.
- `clear crypto isakmp`— удаляет ассоциации безопасности, связанные с 1-м этапом.
- `clear crypto sa`— удаляет ассоциации безопасности, связанные со 2-м этапом.

[Дополнительные сведения о проверке и устранении проблем с IPSec см. в документе Устранение проблем, связанных с безопасностью IP. Обзор команд debug и порядок их использования.](#)

Дополнительные сведения

- [Страница поддержки IPSec](#)
- [Настройка параметров сетевой безопасности IPSec Network Security](#)
- [Настройка протокола защищенного обмена ключами IKE](#)
- [Техническая поддержка - Cisco Systems](#)