

Пример конфигурации "ASA/PIX 7.x и более поздние версии: LAN-to-LAN и EasyVPN IPsec Tunnels Terminate on Same Interface "

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Проверка](#)

[Устранение неполадок](#)

[Команды для устранения неполадок](#)

[Дополнительные сведения](#)

Введение

Этот документ содержит пример конфигурации, разрешающей концентратору ASA принимать туннель, соединяющий сети двух объектов, и соединения Easy VPN IPsec на одном и том же интерфейсе. Для соединения IPsec между Cisco ASA 5520 и устройством адаптивной защиты Cisco ASA 5505 используется Easy VPN с режимом расширения сети (NEM).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Серия 5500 ASA, которая выполняет версию 7.x и позже (Концентратор)**Примечание:** Конфигурация ASA КОНЦЕНТРАТОРА может также использоваться с Устройством безопасности PIX 515, 515E, 525, и 535, который

выполняет версию 7.x и позже

- Легкий VPN ASA 5505, который выполняет версию 7.x и позже
- Устройство безопасности PIX 515, 515E, 525, и 535, который выполняет версию 7.x и позже

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

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

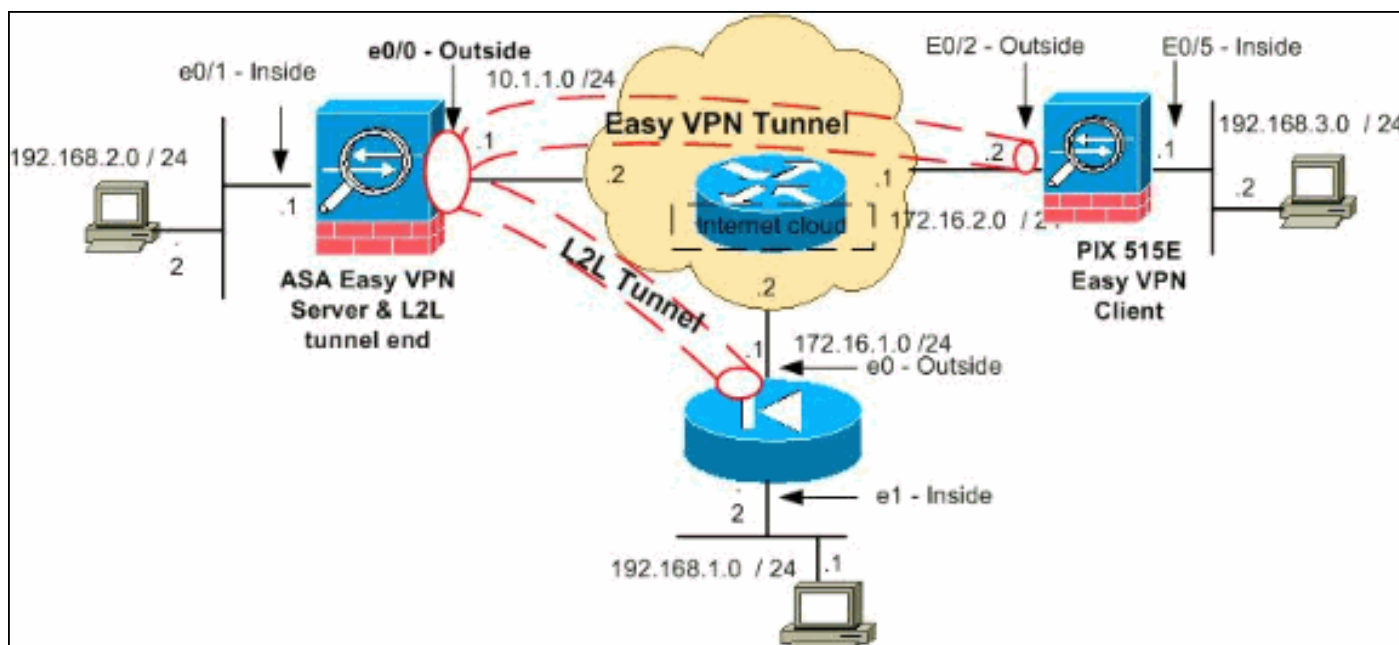
Настройка

В данном разделе приводятся 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:



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. [Это адреса RFC 1918, которые используются в лабораторной среде.](#)

Конфигурации

Эти конфигурации используются в данном документе:

- [ASA КОНЦЕНТРАТОРА](#)
- [Клиент Easy VPN ASA 5505](#)
- [PIX](#)

ASA КОНЦЕНТРАТОРА

```

ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.2.1 255.255.255.0
!
!--- Output Suppressed. !--- Access-list for interesting
traffic (Site to Site) to be !--- encrypted between hub
ASA and spoke (PIX) networks. access-list
outside_cryptomap_20 extended permit ip 192.168.2.0
255.255.255.0 192.168.1.0 255.255.255.0 !--- Access-list
for interesting traffic to be !--- encrypted between hub
ASA and spoke easy vpn client ASA networks. access-list
ezvpn1 extended permit ip 192.168.2.0 255.255.255.0
192.168.3.0 255.255.255.0 !--- Access-list for traffic
to bypass the network address !--- translation (NAT)
process. access-list nonat extended permit ip
192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list nonat extended permit ip 192.168.2.0
255.255.255.0 192.168.3.0 255.255.255.0 !--- Output
Suppressed. !--- Specify the NAT configuration. !--- NAT
0 prevents NAT for the ACL defined in this
configuration. !--- The nat 1 command specifies NAT for
all other traffic. nat-control global (outside) 1
interface nat (inside) 0 access-list nonat nat (inside)
1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 10.1.1.2
1 !--- Output Suppressed. !--- Configuration of IPsec
Phase 2 crypto ipsec transform-set myset esp-3des esp-
sha-hmac !--- IPsec configuration for the dynamic LAN-
to-LAN tunnel crypto dynamic-map ezvpn 30 set transform-
set myset !--- IPsec configuration for the static LAN-
to-LAN tunnel crypto map outside_map 20 match address
outside_cryptomap_20 crypto map outside_map 20 set peer
172.16.1.1 crypto map outside_map 20 set transform-set
myset !--- IPsec configuration that binds dynamic map to
crypto map crypto map outside_map 65535 ipsec-isakmp
dynamic ezvpn !--- Crypto map applied to the outside
interface of the ASA crypto map outside_map interface
outside isakmp enable outside !--- PHASE 1 CONFIGURATION
---! !--- This configuration uses isakmp policy 1. !---
These configuration commands !--- define the Phase 1
policies that are used. crypto isakmp policy 10
authentication pre-share encryption 3des hash sha group
2 lifetime 86400 !--- Output Suppressed. !--- This
defines the group policy you use with Easy VPN. !---
Specify the networks that can pass through !--- the
tunnel and that you want to !--- use network extension

```

```

mode. group-policy tunnel internal group-policy tunnel
attributes nem enable !--- The username and password
associated with !--- this VPN connection are defined
here. You !--- can also use AAA for this function.
username cisco password ffIRPGpDSOJh9YLq encrypted
tunnel-group 172.16.1.1 type ipsec-l2l tunnel-group
172.16.1.1 ipsec-attributes pre-shared-key * !--- The
tunnel-group commands bind the configurations !---
defined in this configuration to the tunnel that is !---
used for Easy VPN. This tunnel name is the one !---
specified on the remote side. tunnel-group mytunnel type
remote-access tunnel-group mytunnel general-attributes
default-group-policy tunnel !--- Defines the pre-shared
key used for !--- IKE authentication for the dynamic
tunnel. tunnel-group mytunnel ipsec-attributes pre-
shared-key * prompt hostname context
Cryptochecksum:e148bf43d04906f5db41fc6f90c52d34 : end

```

Клиент Easy VPN - ASA 5505

```

ASA Version 7.2(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Vlan1
 nameif outside
 security-level 0
 ip address 172.16.2.2 255.255.255.0
!
interface Vlan2
 nameif inside
 security-level 100
 ip address 192.168.3.1 255.255.255.0
!
interface Ethernet0/0
!
interface Ethernet0/1
 shutdown
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
 switchport access vlan 2

!--- Output Suppressed. ! route outside 0.0.0.0 0.0.0.0
172.16.2.1 1 !--- Output Suppressed. !--- Easy VPN
Client Configuration ---! !--- Specify the IP address of
the VPN server. vpnclient server 10.1.1.1 !--- This
example uses network extension mode. vpnclient mode
network-extension-mode !--- Specify the group name and
the pre-shared key. vpnclient vpngroup mytunnel password
***** !--- Specify the authentication username and
password. vpnclient username cisco password ***** !--
- In order to enable the device as hardware vpnclient,
use this command. vpnclient enable ! !--- Output
Suppressed.
Cryptochecksum:0458ce7a08e6b7f9417b17bc254eb4e2 : end

```

PIX

```
PIX Version 8.0(2)
```

```
!  
hostname pixfirewall  
enable password 8Ry2YjIyt7RRXU24 encrypted  
names  
!  
interface Ethernet0  
  nameif outside  
  security-level 0  
  ip address 172.16.1.1 255.255.255.0  
!  
interface Ethernet1  
  nameif inside  
  security-level 100  
  ip address 192.168.1.2 255.255.255.0  
!  
passwd 2KFQnbNIdI.2KYOU encrypted  
ftp mode passive  
!--- 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). access-list  
inside_nat0_outbound extended permit ip 192.168.1.0  
255.255.255.0 192.168.2.0 255.255.255.0 !--- 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  
(inside_nat0_outbound). !--- Two separate access lists  
must always be used in this configuration. access-list  
outside_cryptomap_20 extended permit ip 192.168.1.0  
255.255.255.0 192.168.2.0 255.255.255.0 !--- NAT 0  
prevents NAT for networks specified in the ACL  
inside_nat0_outbound. nat (inside) 0 access-list  
inside_nat0_outbound !--- Output Suppressed. route  
outside 0.0.0.0 0.0.0.0 172.16.1.2 1 !--- Output  
Suppressed. !--- PHASE 2 CONFIGURATION ---! !--- The  
encryption types for Phase 2 are defined here. !---  
Define the transform set for Phase 2. crypto ipsec  
transform-set myset esp-3des esp-sha-hmac !--- Define  
which traffic can be sent to the IPsec peer. crypto map  
outside_map 20 match address outside_cryptomap_20 !---  
Sets the IPsec peer. crypto map outside_map 20 set peer  
10.1.1.1 !--- Sets the IPsec transform set "myset" !---  
to be used with the crypto map entry "outside_map".  
crypto map outside_map 20 set transform-set myset !---  
Specifies the interface to be used with !--- the  
settings defined in this configuration. crypto map  
outside_map interface outside !--- PHASE 1 CONFIGURATION  
---! !--- This configuration uses isakmp policy 10. !---  
Policy 65535 is included in the config by default. !---  
The configuration commands here define the Phase !--- 1  
policy parameters that are used. crypto isakmp enable  
outside crypto isakmp policy 10 authentication pre-share  
encryption 3des hash sha group 2 lifetime 86400 crypto  
isakmp policy 65535 authentication pre-share encryption  
3des hash sha group 2 lifetime 86400 !--- Output  
Suppressed. !--- In order to create and manage the  
database of connection-specific records !--- for ipsec-  
l2l-IPsec (LAN-to-LAN) tunnels, use the tunnel-group !--  
- command in global configuration mode. !--- For L2L  
connections the name of the tunnel group MUST be the IP  
!--- address of the IPsec peer. tunnel-group 10.1.1.1  
type ipsec-l2l !--- Enter the pre-shared-key in order to  
configure the authentication method. tunnel-group  
10.1.1.1 ipsec-attributes pre-shared-key * prompt
```

```
hostname context
Cryptochecksum:4a2c70f2102113315de795f13f25c2aa : end
```

Проверка

В данном разделе содержатся сведения для проверки правильности конфигурации.

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

- **show crypto isakmp sa** – отображает все текущие сопоставления безопасности IKE (SA) на одноранговом узле.
- **show crypto ipsec sa** – отображает все текущие SA.

В данном разделе показан пример конфигурации проверки для:

- [ASA КОНЦЕНТРАТОРА](#)
- [Клиент Easy VPN ASA 5505](#)
- [PIX](#)

ASA КОНЦЕНТРАТОРА

```
ciscoasa #show crypto isakmp sa Active SA: 2 Rekey SA: 0
(A tunnel will report 1 Active and 1 Rekey SA during
rekey) Total IKE SA: 2 !--- Dynamic LAN-to-LAN tunnel
establishment 1 IKE Peer: 172.16.2.2 Type : user Role :
responder Rekey : no State : AM_ACTIVE !--- Static LAN-
to-LAN tunnel establishment 2 IKE Peer: 172.16.1.1 Type
: L2L Role : initiator Rekey : no State : MM_ACTIVE
ciscoasa #show crypto ipsec sa ciscoasa(config)#sh
crypto ipsec sa interface: outside Crypto map tag:
outside_map, seq num: 20, local addr: 10.1.1.1 access-
list outside_cryptomap_20 permit ip 192.168.2.0
255.255.255.0 192.168.1.0 255.255.255.0 local ident
(addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0) current_peer: 172.16.1.1
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4 #pkts
decaps: 4, #pkts decrypt: 4, #pkts verify: 4 #pkts
compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 4, #pkts comp failed: 0, #pkts decomp
failed: 0 #pre-frag successes: 0, #pre-frag failures: 0,
#fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0,
#decapsulated frgs needing reassembly: 0 #send errors:
0, #recv errors: 0 local crypto endpt.: 10.1.1.1, remote
crypto endpt.: 172.16.1.1 path mtu 1500, ipsec overhead
58, media mtu 1500 current outbound spi: E4312E13
inbound esp sas: spi: 0x9ABAC3DD (2595931101) transform:
esp-3des esp-sha-hmac none in use settings ={L2L,
Tunnel, } slot: 0, conn_id: 741376, crypto-map:
outside_map sa timing: remaining key lifetime (kB/sec):
(4274999/28783) IV size: 8 bytes replay detection
support: Y outbound esp sas: spi: 0xE4312E13
(3828428307) transform: esp-3des esp-sha-hmac none in
use settings ={L2L, Tunnel, } slot: 0, conn_id: 741376,
crypto-map: outside_map sa timing: remaining key
lifetime (kB/sec): (4274999/28783) IV size: 8 bytes
replay detection support: Y Crypto map tag: ezvpn, seq
```

```
num: 30, local addr: 10.1.1.1 local ident
(addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port):
(172.16.2.2/255.255.255.255/0/0) current_peer:
172.16.2.2, username: cisco dynamic allocated peer ip:
0.0.0.0 #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 comp failed: 0, #pkts decomp
failed: 0 #pre-frag successes: 0, #pre-frag failures: 0,
#fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0,
#decapsulated frgs needing reassembly: 0 #send errors:
0, #recv errors: 0 local crypto endpt.: 10.1.1.1, remote
crypto endpt.: 172.16.2.2 path mtu 1500, ipsec overhead
58, media mtu 1500 current outbound spi: 2647B59C
inbound esp sas: spi: 0x21685AF8 (560487160) transform:
esp-3des esp-sha-hmac none in use settings ={RA, Tunnel,
} slot: 0, conn_id: 737280, crypto-map: ezvpn sa timing:
remaining key lifetime (sec): 28146 IV size: 8 bytes
replay detection support: Y outbound esp sas: spi:
0x2647B59C (642233756) transform: esp-3des esp-sha-hmac
none in use settings ={RA, Tunnel, } slot: 0, conn_id:
737280, crypto-map: ezvpn sa timing: remaining key
lifetime (sec): 28146 IV size: 8 bytes replay detection
support: Y Crypto map tag: ezvpn, seq num: 30, local
addr: 10.1.1.1 local ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/0/0) remote ident
(addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer: 172.16.2.2, username: cisco dynamic
allocated peer ip: 0.0.0.0 #pkts encaps: 5, #pkts
encrypt: 5, #pkts digest: 5 #pkts decaps: 5, #pkts
decrypt: 5, #pkts verify: 5 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 5, #pkts comp
failed: 0, #pkts decomp failed: 0 #pre-frag successes:
0, #pre-frag failures: 0, #fragments created: 0 #PMTUs
sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0 #send errors: 0, #recv errors: 0 local
crypto endpt.: 10.1.1.1, remote crypto endpt.:
172.16.2.2 path mtu 1500, ipsec overhead 58, media mtu
1500 current outbound spi: 07997B21 inbound esp sas:
spi: 0xB5B6013D (3048603965) transform: esp-3des esp-
sha-hmac none in use settings ={RA, Tunnel, } slot: 0,
conn_id: 737280, crypto-map: ezvpn sa timing: remaining
key lifetime (sec): 28145 IV size: 8 bytes replay
detection support: Y outbound esp sas: spi: 0x07997B21
(127499041) transform: esp-3des esp-sha-hmac none in use
settings ={RA, Tunnel, } slot: 0, conn_id: 737280,
crypto-map: ezvpn sa timing: remaining key lifetime
(sec): 28145 IV size: 8 bytes replay detection support:
Y Crypto map tag: ezvpn, seq num: 30, local addr:
10.1.1.1 local ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/0/0) remote ident
(addr/mask/prot/port): (172.16.2.2/255.255.255.255/0/0)
current_peer: 172.16.2.2, username: cisco dynamic
allocated peer ip: 0.0.0.0 #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 comp
failed: 0, #pkts decomp failed: 0 #pre-frag successes:
0, #pre-frag failures: 0, #fragments created: 0 #PMTUs
sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0 #send errors: 0, #recv errors: 0 local
crypto endpt.: 10.1.1.1, remote crypto endpt.:
172.16.2.2 path mtu 1500, ipsec overhead 58, media mtu
```

```
1500 current outbound spi: 0F0B1A75 inbound esp sas:  
spi: 0x68B0EA75 (1756424821) transform: esp-3des esp-  
sha-hmac none in use settings ={RA, Tunnel, } slot: 0,  
conn_id: 737280, crypto-map: ezvpn sa timing: remaining  
key lifetime (sec): 28143 IV size: 8 bytes replay  
detection support: Y outbound esp sas: spi: 0x0F0B1A75  
(252385909) transform: esp-3des esp-sha-hmac none in use  
settings ={RA, Tunnel, } slot: 0, conn_id: 737280,  
crypto-map: ezvpn sa timing: remaining key lifetime  
(sec): 28143 IV size: 8 bytes replay detection support:  
Y
```

Клиент Easy VPN ASA 5505

```
ciscoasa(config)# sh crypto isakmp sa Active SA: 1 Rekey  
SA: 0 (A tunnel will report 1 Active and 1 Rekey SA  
during rekey) Total IKE SA: 1 1 IKE Peer: 10.1.1.1 Type  
: user Role : initiator Rekey : no State : AM ACTIVE  
ciscoasa(config)# sh crypto ipsec sa interface: outside  
Crypto map tag: _vpnc_cm, seq num: 10, local addr:  
172.16.2.2 access-list _vpnc_acl permit ip host  
172.16.2.2 host 10.1.1.1 local ident  
(addr/mask/prot/port): (172.16.2.2/255.255.255.255/0/0)  
remote ident (addr/mask/prot/port):  
(10.1.1.1/255.255.255.255/0/0) current_peer: 10.1.1.1,  
username: 10.1.1.1 dynamic allocated peer ip: 0.0.0.0  
#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 comp failed: 0, #pkts decomp  
failed: 0 #pre-frag successes: 0, #pre-frag failures: 0,  
#fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0,  
#decapsulated frgs needing reassembly: 0 #send errors:  
0, #recv errors: 0 local crypto endpt.: 172.16.2.2,  
remote crypto endpt.: 10.1.1.1 path mtu 1500, ipsec  
overhead 58, media mtu 1500 current outbound spi:  
21685AF8 inbound esp sas: spi: 0x2647B59C (642233756)  
transform: esp-3des esp-sha-hmac none in use settings  
={RA, Tunnel, } slot: 0, conn_id: 178, crypto-map:  
_vpnc_cm sa timing: remaining key lifetime (sec): 28298  
IV size: 8 bytes replay detection support: Y outbound  
esp sas: spi: 0x21685AF8 (560487160) transform: esp-3des  
esp-sha-hmac none in use settings ={RA, Tunnel, } slot:  
0, conn_id: 178, crypto-map: _vpnc_cm sa timing:  
remaining key lifetime (sec): 28298 IV size: 8 bytes  
replay detection support: Y Crypto map tag: _vpnc_cm,  
seq num: 10, local addr: 172.16.2.2 access-list  
_vpnc_acl permit ip host 172.16.2.2 any local ident  
(addr/mask/prot/port): (172.16.2.2/255.255.255.255/0/0)  
remote ident (addr/mask/prot/port):  
(0.0.0.0/0.0.0.0/0/0) current_peer: 10.1.1.1, username:  
10.1.1.1 dynamic allocated peer ip: 0.0.0.0 #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 comp failed: 0, #pkts decomp  
failed: 0 #pre-frag successes: 0, #pre-frag failures: 0,  
#fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0,  
#decapsulated frgs needing reassembly: 0 #send errors:  
0, #recv errors: 0 local crypto endpt.: 172.16.2.2,  
remote crypto endpt.: 10.1.1.1 path mtu 1500, ipsec  
overhead 58, media mtu 1500 current outbound spi:  
68B0EA75 inbound esp sas: spi: 0x0F0B1A75 (252385909)  
transform: esp-3des esp-sha-hmac none in use settings
```



```
={RA, Tunnel, } slot: 0, conn_id: 178, crypto-map:
_vpnc_cm sa timing: remaining key lifetime (sec): 28298
IV size: 8 bytes replay detection support: Y outbound
esp sas: spi: 0x68B0EA75 (1756424821) transform: esp-
3des esp-sha-hmac none in use settings ={RA, Tunnel, }
slot: 0, conn_id: 178, crypto-map: _vpnc_cm sa timing:
remaining key lifetime (sec): 28298 IV size: 8 bytes
replay detection support: Y Crypto map tag: _vpnc_cm,
seq num: 10, local addr: 172.16.2.2 access-list
_vpnc_acl permit ip 192.168.3.0 255.255.255.0 any local
ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 10.1.1.1, username: 10.1.1.1 dynamic
allocated peer ip: 0.0.0.0 #pkts encaps: 5, #pkts
encrypt: 5, #pkts digest: 5 #pkts decaps: 5, #pkts
decrypt: 5, #pkts verify: 5 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 0, #pkts comp
failed: 0, #pkts decomp failed: 0 #pre-frag successes:
0, #pre-frag failures: 0, #fragments created: 0 #PMTUs
sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0 #send errors: 0, #recv errors: 0 local
crypto endpt.: 172.16.2.2, remote crypto endpt.:
10.1.1.1 path mtu 1500, ipsec overhead 58, media mtu
1500 current outbound spi: B5B6013D inbound esp sas:
spi: 0x07997B21 (127499041) transform: esp-3des esp-sha-
hmac none in use settings ={RA, Tunnel, } slot: 0,
conn_id: 178, crypto-map: _vpnc_cm sa timing: remaining
key lifetime (sec): 28294 IV size: 8 bytes replay
detection support: Y outbound esp sas: spi: 0xB5B6013D
(3048603965) transform: esp-3des esp-sha-hmac none in
use settings ={RA, Tunnel, } slot: 0, conn_id: 178,
crypto-map: _vpnc_cm sa timing: remaining key lifetime
(sec): 28294 IV size: 8 bytes replay detection support:
Y
```

PIX

```
pixfirewall(config)#sh crypto isakmp sa Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey
SA during rekey) Total IKE SA: 1 1 IKE Peer: 10.1.1.1
Type : L2L Role : responder Rekey : no State : MM_ACTIVE
pixfirewall(config)# sh crypto ipsec sa interface:
outside Crypto map tag: outside_map, seq num: 20, local
addr: 172.16.1.1 access-list outside_cryptomap_20 permit
ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer: 10.1.1.1 #pkts encaps: 4, #pkts encrypt:
4, #pkts digest: 4 #pkts decaps: 4, #pkts decrypt: 4,
#pkts verify: 4 #pkts compressed: 0, #pkts decompressed:
0 #pkts not compressed: 0, #pkts comp failed: 0, #pkts
decomp failed: 0 #pre-frag successes: 0, #pre-frag
failures: 0, #fragments created: 0 #PMTUs sent: 0,
#PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0 local crypto endpt.:
172.16.1.1, remote crypto endpt.: 10.1.1.1 path mtu
1500, ipsec overhead 58, media mtu 1500 current outbound
spi: 9ABAC3DD inbound esp sas: spi: 0xE4312E13
(3828428307) transform: esp-3des esp-sha-hmac none in
use settings ={L2L, Tunnel, } slot: 0, conn_id: 12288,
crypto-map: outside_map sa timing: remaining key
lifetime (kB/sec): (3824999/28628) IV size: 8 bytes
replay detection support: Y outbound esp sas: spi:
```

```
0x9ABAC3DD (2595931101) transform: esp-3des esp-sha-hmac
none in use settings ={L2L, Tunnel, } slot: 0, conn_id:
12288, crypto-map: outside_map sa timing: remaining key
lifetime (kB/sec): (3824999/28628) IV size: 8 bytes
replay detection support: Y
```

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей 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: [Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.](#)

Выполните команды PIX в режиме конфигурации:

- `clear crypto isakmp sa` — удаляет SA фазы 1
- `clear crypto ipsec sa` – удаляет SA фазы 2

Команды debug для туннелей VPN:

- `debug crypto isakmp sa` – для отладки согласований SA ISAKMP
- `debug crypto ipsec sa` – для отладки согласований SA IPSec

Дополнительные сведения

- [Устройства защиты Cisco PIX серии 500 - введение](#)
- [Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN на базе протокола IPSec](#)
- [Поддержка устройств адаптивной безопасности Cisco ASA серии 5500](#)
- [Согласование IPsec/Протоколы IKE](#)
- [Cisco Systems – техническая поддержка и документация](#)