

# PIX/ASA 7.x и более поздние: IPSec VPN LAN-LAN с примером конфигурации наложений сети

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Родственные продукты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Проверка](#)

[команды показа от ASA 1](#)

[команды показа от ASA 2](#)

[Устранение неполадок](#)

[Очистка ассоциаций безопасности](#)

[Команды для устранения неполадок](#)

[Дополнительные сведения](#)

## **[Введение](#)**

Этот документ описывает порядок действий для преобразования (NAT) трафика VPN, проходящего через туннель IPSec LAN-LAN (L2L) между двумя устройствами защиты, а также применения преобразования PAT к интернет-трафику. Каждое устройство защиты обслуживает частную защищенную сеть. В данном примере два устройства адаптивной защиты Cisco (ASA) с идентичными и перекрывающимися внутренними сетями связаны по VPN-туннелю. В обычном сценарии никогда не происходит связь через VPN, потому что ping - пакеты никогда не оставляют локальную подсеть, так как пользователь пропинговывает IP-адрес той же подсети. Для этих двух частных внутренних сетей для передачи друг с другом Политика NAT используется на обоих ASA для трансляции локальной подсети так, чтобы связь произошла как ожидалось.

## **[Предварительные условия](#)**

### **[Требования](#)**

Удостоверьтесь, что вы настроили устройство адаптивной защиты Cisco с IP-адресами на

интерфейсах и имеет основное подключение перед переходом этот пример конфигурации.

## Используемые компоненты

Сведения в этом документе основываются на этой версии программного обеспечения:

- ПО устройств адаптивной защиты Cisco версии 7.x и более поздних версий.

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.

## Родственные продукты

Эти настройки также могут быть использованы в устройствах защиты Cisco PIX, начиная с версий 7.x.

## Условные обозначения

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

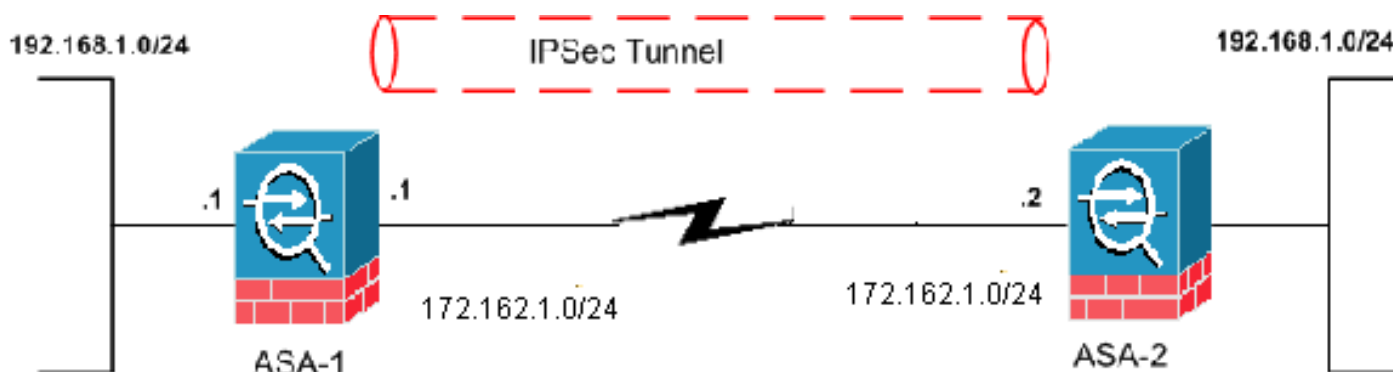
## Настройка

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:



## Конфигурации

Эти конфигурации используются в данном документе:

- [Конфигурация ASA 1](#)

- [Конфигурация ASA 2](#)

## ASA 1

```
ASA-1#show running-config : Saved : ASA Version 8.0(3) !
hostname ciscoasa enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0 nameif outside
security-level 0 ip address 172.162.1.1 255.255.255.0 !-
-- Configure the outside interface. ! interface
Ethernet1 nameif inside security-level 100 ip address
192.168.1.1 255.255.255.0 !--- Configure the inside
interface. passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive access-list new extended permit ip 192.168.2.0
255.255.255.0 192.168.3.0 255.255.255.0 !--- This access
list (new) is used with the crypto map (outside_map) !-
- in order to determine which traffic should be
encrypted !--- and sent across the tunnel. access-list
policy-nat extended permit ip 192.168.1.0 255.255.255.0
192.168.3.0 255.255.255.0 !--- The policy-nat ACL is
used with the static !--- command in order to match the
VPN traffic for translation. pager lines 24 mtu outside
1500 mtu inside 1500 no failover asdm image flash:/asdm-
615.bin no asdm history enable arp timeout 14400 static
(inside,outside) 192.168.2.0 access-list policy-nat !---
It is a Policy NAT statement. !--- The static command
with the access list (policy-nat), !--- which matches
the VPN traffic and translates the source (192.168.1.0)
to !--- 192.168.2.0 for outbound VPN traffic. global
(outside) 1 interface nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- The previous statements PAT the Internet traffic !-
- except for the VPN traffic that uses the IP address
172.17.1.1. route outside 0.0.0.0 0.0.0.0 172.162.1.2 1
!--- Output is suppressed. !--- PHASE 2 CONFIGURATION --
-! !--- The encryption types for Phase 2 are defined
here. crypto ipsec transform-set CISCO esp-des esp-md5-
hmac !--- Define the transform set for Phase 2. crypto
map outside_map 20 match address new !--- Define which
traffic should be sent to the IPsec peer with the !---
access list (new). crypto map outside_map 20 set peer
172.162.1.2 !--- Sets the IPsec peer (remote end point)
crypto map outside_map 20 set transform-set CISCO !---
Sets the IPsec transform set "CISCO" !--- to be used
with the crypto map entry "outside_map" crypto map
outside_map interface outside !--- Specifies the
interface to be used with !--- the settings defined in
this configuration !--- PHASE 1 CONFIGURATION ---! !---
This configuration uses isakmp policy 65535. !--- Policy
65535 is included in the configuration by default. !---
These configuration commands define the !--- Phase 1
policy parameters that are used. crypto isakmp identity
address crypto isakmp enable outside crypto isakmp
policy 65535 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 tunnel-group 172.162.1.2
type ipsec-l2l !--- 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 (remote peer end).
tunnel-group 172.162.1.2 ipsec-attributes pre-shared-key
* !--- Enter the pre-shared key in order to configure
the authentication method. telnet timeout 5 ssh timeout
5 console timeout 0 ! class-map inspection_default match
```

```
default-inspection-traffic !! policy-map global_policy
class inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtplib inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
Cryptochecksum:33e1e37cd1280d908210dac0cc26e706 : end
```

## ASA 2

```
ASA-2#show running-config : Saved : ASA Version 8.0(3) !
hostname ASA-2 enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0 nameif outside
security-level 0 ip address 172.162.1.2 255.255.255.0 !
interface Ethernet1 nameif inside security-level 100 ip
address 192.168.1.1 255.255.255.0 ! !--- Output is
suppressed. access-list new extended permit ip
192.168.3.0 255.255.255.0 192.168.2.0 255.255.255.0 !---
This access list (new) is used with the crypto map
(outside_map) !--- in order to determine which traffic
needs to be encrypted !--- and sent across the tunnel.
access-list policy-nat extended permit ip 192.168.1.0
255.255.255.0 192.168.2.0 255.255.255.0 !--- The policy-
nat ACL is used with the static !--- command in order to
match the VPN traffic for translation. pager lines 24
mtu outside 1500 mtu inside 1500 no failover asdm image
flash:/asdm-615.bin no asdm history enable arp timeout
14400 static (inside,outside) 192.168.3.0 access-list
policy-nat !--- This is a Policy NAT statement. !--- The
static command with the access list (policy-nat), !---
which matches the VPN traffic and translates the source
(192.168.1.0) to !--- 192.168.3.0 for outbound VPN
traffic. global (outside) 1 interface nat (inside) 1
0.0.0.0 0.0.0.0 0 0 !--- The previous statements PAT the
Internet traffic !--- except the VPN traffic that uses
the outside interface IP address. route outside 0.0.0.0
0.0.0.0 172.162.1.2 1 !--- PHASE 2 CONFIGURATION ---! !-
-- The encryption types for Phase 2 are defined here.
crypto ipsec transform-set CISCO esp-des esp-md5-hmac !-
-- Define the transform set for Phase 2. crypto map
outside_map 20 match address new !--- Define which
traffic needs to be sent to the IPsec peer. crypto map
outside_map 20 set peer 172.162.1.1 !--- Sets the IPsec
peer. crypto map outside_map 20 set transform-set CISCO
!--- Sets the IPsec transform set "CISCO" !--- to be
used with the crypto map entry "outside_map". crypto map
outside_map interface outside !--- Specifies the
interface to be used with !--- the settings defined in
this configuration. !--- PHASE 1 CONFIGURATION ---! !---
This configuration uses isakmp policy 65535 !--- which
is included in the configuration by default. !--- The
configuration commands here define the !--- Phase 1
policy parameters that are used. crypto isakmp identity
address crypto isakmp enable outside crypto isakmp
policy 65535 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 !--- Output is
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
172.162.1.1 type ipsec-l2l tunnel-group 172.162.1.1
ipsec-attributes pre-shared-key * !--- Enter the pre-
shared key in order to configure the authentication
```

```
method. prompt hostname context
Cryptochecksum:6b505b4a05c1aee96a71e67c23e71865 : end
```

## Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

[Средство Output Interpreter \(OIT\) \(только для зарегистрированных клиентов\) поддерживает определенные команды show.](#) Используйте OIT для просмотра анализа выходных данных команды show:

- **show crypto isakmp sa** — Показывает все текущие ассоциации безопасности (SA) протокола IKE для узла.
- **show crypto ipsec sa**—отображает параметры, используемые текущими SA.

### команды показа от ASA 1

```
ASA-1#show 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: 172.162.1.2 Type : L2L Role : initiator Rekey : no
State : MM_ACTIVE ASA-1#show crypto ipsec sa interface: outside Crypto map tag: outside_map, seq
num: 20, local addr: 172.162.1.1 access-list new permit ip 192.168.2.0 255.255.255.0 192.168.3.0
255.255.2 5.0 local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0) current_peer: 172.162.1.2 #pkts encaps:
9, #pkts encrypt: 9, #pkts digest: 9 #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9 #pkts
compressed: 0, #pkts decompressed: 0 #pkts not compressed: 9, #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.: 172.162.1.1, remote crypto endpt.: 172.162.1.2 path mtu 1500, ipsec overhead 58,
media mtu 1500 current outbound spi: 0BA6CD7E inbound esp sas: spi: 0xFB4BD01A (4216049690)
transform: esp-des esp-md5-hmac none in use settings ={L2L, Tunnel, } slot: 0, conn_id: 8192,
crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (3824999/27738) IV size: 8
bytes replay detection support: Y outbound esp sas: spi: 0x0BA6CD7E (195480958) transform: esp-
des esp-md5-hmac none in use settings ={L2L, Tunnel, } slot: 0, conn_id: 8192, crypto-map:
outside_map sa timing: remaining key lifetime (kB/sec): (3824999/27738) IV size: 8 bytes replay
detection support: Y ASA-1#show nat NAT policies on Interface inside: match ip inside 192.168.1.0
255.255.255.0 outside 192.168.3.0 255.255.255.0 static translation to 192.168.2.0 translate_hits
= 12, untranslate_hits = 5 match ip inside any outside any dynamic translation to pool 1
(172.162.1.1 [Interface PAT]) translate_hits = 0, untranslate_hits = 0 match ip inside any
inside any dynamic translation to pool 1 (No matching global) translate_hits = 0,
untranslate_hits = 0 match ip inside any dmz any dynamic translation to pool 1 (No matching
global) translate_hits = 0, untranslate_hits = 0 ASA-1#show xlate 1 in use, 1 most used Global
192.168.2.0 Local 192.168.1.0
```

### команды показа от ASA 2

```
ASA-2#show crypto ipsec sa interface: outside Crypto map tag: outside_map, seq num: 20, local
addr: 172.162.1.2 access-list new permit ip 192.168.3.0 255.255.255.0 192.168.2.0 255.255.25 5.0
local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0) current_peer: 172.162.1.1 #pkts encaps:
9, #pkts encrypt: 9, #pkts digest: 9 #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9 #pkts
compressed: 0, #pkts decompressed: 0 #pkts not compressed: 9, #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.: 172.162.1.2, remote crypto endpt.: 172.162.1.1 path mtu 1500, ipsec overhead 58,
media mtu 1500 current outbound spi: FB4BD01A inbound esp sas: spi: 0x0BA6CD7E (195480958)
transform: esp-des esp-md5-hmac none in use settings ={L2L, Tunnel, } slot: 0, conn_id: 8192,
```

```
crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4274999/26902) IV size: 8
bytes replay detection support: Y outbound esp sas: spi: 0xFB4BD01A (4216049690) transform: esp-
des esp-md5-hmac none in use settings ={L2L, Tunnel, } slot: 0, conn_id: 8192, crypto-map:
outside_map sa timing: remaining key lifetime (kB/sec): (4274999/26902) IV size: 8 bytes replay
detection support: Y ASA-2#show 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: 172.162.1.1 Type : L2L Role :
responder Rekey : no State : MM_ACTIVE
```

## Устранение неполадок

### Очистка ассоциаций безопасности

Когда вы устраняете неполадки, убедитесь очистить существующие SA после внесения изменения. В привилегированном режиме PIX используйте следующие команды:

- `clear [crypto] ipsec sa`— удаляет все активные ассоциации безопасности IPsec.
- `clear crypto isakmp sa`— удаляет активные ассоциации безопасности IKE.

### Команды для устранения неполадок

[Средство интерпретации выходных данных \(только зарегистрированные клиенты\)](#) поддерживает некоторые команды `show`. Используйте OIT для просмотра анализа выходных данных команды `show`.

**Примечание:** [Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки"](#).

- `debug crypto ipsec` – отображает согласования IPsec на Этапе 2.
- `debug crypto isakmp` – отображает согласования ISAKMP на 1-м этапе.

## Дополнительные сведения

- [Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN на базе протокола IPsec](#)
- [PIX 7.0 и перенаправление \(пересылка\) портов адаптированного устройства безопасности с помощью команд nat, global, static, conduit и access-list](#)
- [PIX/ASA 7.x и FWSM: NAT и инструкции PAT](#)
- [Устройства обеспечения безопасности Cisco ASA серии 5500](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [Согласование IPsec/Протоколы IKE](#)
- [Cisco Systems – техническая поддержка и документация](#)