

PIX/ASA 7.x 及更高版本：与重叠网络配置示例的 LAN 对 LAN IPsec VPN

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[相关产品](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[显示从 ASA-1 发出的命令](#)

[显示从 ASA-2 发出的命令](#)

[故障排除](#)

[清除安全关联](#)

[故障排除命令](#)

[相关信息](#)

[简介](#)

本文档介绍了对通过两个安全设备间的 LAN 到 LAN (L2L) IPsec 隧道进行传输的 VPN 数据流进行转换 (NAT) 的步骤以及对 Internet 数据流进行 PAT 的步骤。每个安全设备身后都有一个受保护的专用网络。在本示例中，具有相同和重叠的内部网络的两台 Cisco 自适应安全设备 (ASA) 通过 VPN 隧道连接。通常情况下，不会出现通过 VPN 进行通信的情况，因为用户对同一子网的 IP 地址进行 ping 操作导致 ping 数据包从不会离开本地子网。为使这两个专用内部网络能够互相通信，在两台 ASA 上使用了策略 NAT 以转换本地子网，以便按预期进行通信。

[先决条件](#)

[要求](#)

在继续本配置示例之前，请确保您已在接口上对 Cisco 自适应安全设备进行了 IP 地址配置并具备基本的连接。

[使用的组件](#)

本文档中的信息基于以下软件版本：

- Cisco 自适应安全设备软件版本 7.x 及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也可用于 Cisco PIX 安全设备版本 7.x 及更高版本。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

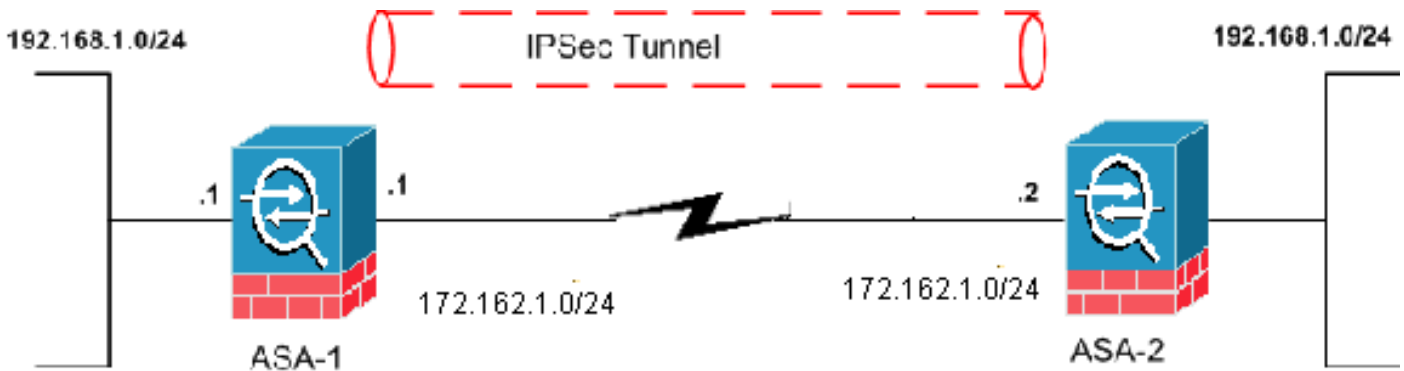
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用 [命令查找工具](#)（[仅限注册用户](#)）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- [ASA-1 配置](#)
- [ASA-2 配置](#)

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

```

验证

使用本部分可确认配置能否正常运行。

[命令输出解释程序 \(仅限注册用户 \)](#) (OIT) 支持某些 **show** 命令。使用 OIT 查看对 **show** 命令输出的分析：

- **show crypto isakmp sa** - 显示对等体上的所有当前 IKE 安全关联 (SA)。

- **show crypto ipsec sa** - 显示当前 SA 使用的设置。

显示从 ASA-1 发出的命令

```
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
```

显示从 ASA-2 发出的命令

```
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
```

故障排除

清除安全关联

排除故障时，请务必在进行更改后清除现有的 SA。在 PIX 的特权模式下，使用以下命令：

- **clear crypto ipsec sa** - 删除活动的 IPsec SA。
- **clear crypto isakmp sa** - 删除活动的 IKE SA。

[故障排除命令](#)

[命令输出解释程序工具](#) ([仅限注册用户](#)) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto isakmp** - 显示第 1 阶段的 ISAKMP 协商。

[相关信息](#)

- [最常用的 L2L 和远程访问 IPsec VPN 故障排除解决方案](#)
- [PIX 7.0 和使用 nat、global、static、conduit 和 access-list 命令进行自适应安全设备端口重定向 \(转发\)](#)
- [PIX/ASA 7.x和FWSM : NAT和PAT语句](#)
- [Cisco ASA 5500 系列安全设备](#)
- [Cisco PIX 500 系列安全设备](#)
- [IPsec 协商/IKE 协议](#)
- [技术支持和文档 - Cisco Systems](#)