

在ASA 5505和ASA/PIX之间的LAN-to-LAN隧道配置示例

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](#)

[故障排除](#)

[相关信息](#)

简介

本文档提供了 Cisco 安全设备 (ASA/PIX) 与自适应安全设备 (ASA) 5505 之间的 LAN 到 LAN (站点到站点) IPSec 隧道的示例配置。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 7.x 及更高版本的 Cisco 5500 系列 ASA
- 运行软件版本 7.x 及更高版本的 Cisco 5505 ASA

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

此配置也可用于以下硬件和软件版本：

- 运行软件版本 7.x 及更高版本的 Cisco 500 系列 PIX 安全设备
- 运行软件版本 7.x 及更高版本的 Cisco 5505 ASA

规则

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

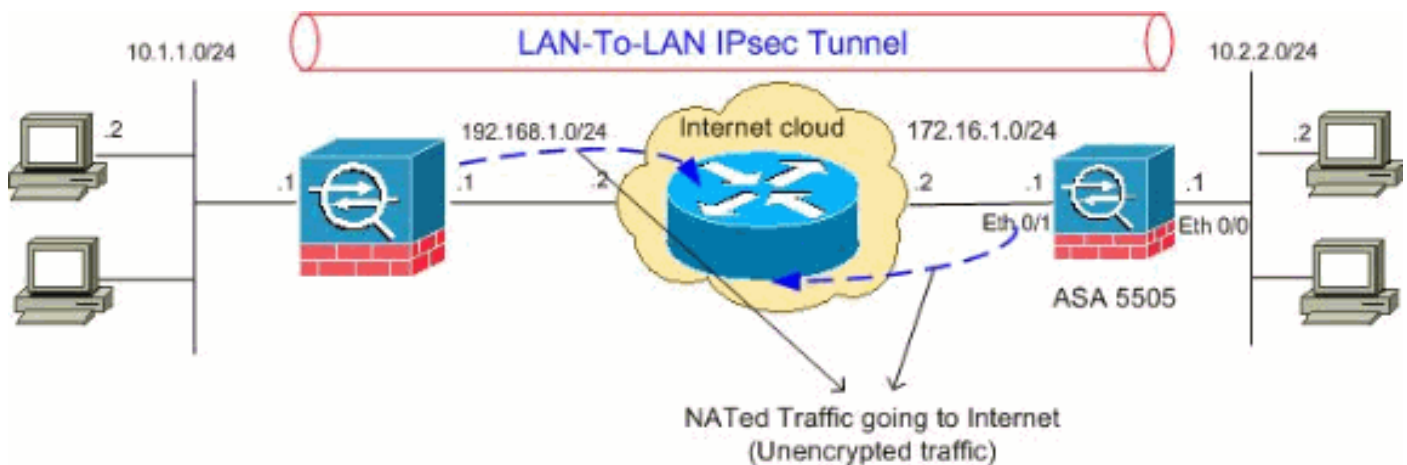
配置

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](#)([仅限注册客户](#))可获取有关本节中使用的命令的详细信息。

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：

- [Cisco 5505 ASA 配置](#)
- [Cisco 5510 ASA 配置](#)

Cisco 5505 ASA 配置

```
ASA5505#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ASA5505
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Vlan1
 no nameif
 no security-level
 no ip address
```

```

!
interface Vlan2
  nameif outside
  security-level 0
  ip address 172.16.1.1 255.255.255.0
!
interface Vlan3
  nameif inside
  security-level 100
  ip address 10.2.2.1 255.255.255.0
!
interface Ethernet0/0
  switchport access vlan 3
!
interface Ethernet0/1
  switchport access vlan 2
!
interface Ethernet0/2
  shutdown
!
interface Ethernet0/3
  shutdown
!
interface Ethernet0/4
  shutdown
!
interface Ethernet0/5
  shutdown
!
interface Ethernet0/6
  shutdown
!
interface Ethernet0/7
  shutdown
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
access-list 100 extended permit ip 10.2.2.0
255.255.255.0 10.1.1.0 255.255.255.0

!--- Access-list for interesting traffic (Site to Site)
to be !--- encrypted between ASA 5505 and ASA/PIX
networks. access-list nonat extended permit ip 10.2.2.0
255.255.255.0 10.1.1.0 255.255.255.0

!--- Access-list for traffic to bypass the network
address !--- translation (NAT) process. pager lines 24
mtu inside 1500 mtu outside 1500 no failover icmp
unreachable rate-limit 1 burst-size 1 asdm image
disk0:/asdm-602.bin no asdm history enable arp timeout
14400 nat-control global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0

!--- 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.

route outside 10.1.1.0 255.255.255.0 172.16.1.2 1
route outside 192.168.1.0 255.255.255.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00

```

```

icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:0
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart

!--- PHASE 2 CONFIGURATION !--- The encryption types for
Phase 2 are defined here. crypto ipsec transform-set
myset esp-3des esp-sha-hmac

!--- Define the transform set for Phase 2. crypto map
outside_map 20 match address 100

!--- Define which traffic can be sent to the IPsec peer.
crypto map outside_map 20 set peer 192.168.1.1

!--- Sets the IPsec peer. crypto map outside_map 20 set
transform-set myset

!--- Sets the IPsec transform set "myset" !--- to be
used with the crypto map entry "outside_map" crypto map
outside_map interface outside

!--- Crypto map applied to the outside interface of the
ASA crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

!--- PHASE 1 CONFIGURATION ---! !--- This configuration
uses isakmp policy 10. !--- These configuration commands
!--- define the Phase 1 policies that are used. telnet
timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global tunnel-group 192.168.1.1
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.

tunnel-group 192.168.1.1 ipsec-attributes

```

pre-shared-key *

!--- Enter the pre-shared-key in order to configure the authentication method. prompt hostname context
Cryptochecksum:68eba159fd8e4c893f24185ffb40bb6f : end
ASA5505#

Cisco 5510 ASA 配置

```
ASA5510#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
  nameif inside
  security-level 100
  ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
  nameif outside
  security-level 0
  ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/2
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Ethernet0/3
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  shutdown
  no nameif
  no security-level
  no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list 100 extended permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0

!--- Access-list for interesting traffic (Site to Site)
to be !--- encrypted between ASA 5505 and ASA/PIX
networks. access-list nonat extended permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0

!--- Access-list for traffic to bypass the network
address !--- translation (NAT) process. pager lines 24
mtu inside 1500 mtu outside 1500 no failover icmp
unreachable rate-limit 1 burst-size 1 asdm image
disk0:/asdm-522.bin no asdm history enable arp timeout
14400 nat-control global (outside) 1 interface
nat (inside) 0 access-list nonat
```

```

nat (inside) 1 0.0.0.0 0.0.0.0

!--- 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.

route outside 10.2.2.0 255.255.255.0 192.168.1.2 1
route outside 172.16.1.0 255.255.255.0 192.168.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart

!--- PHASE 2 CONFIGURATION !--- The encryption types for Phase 2 are defined here. crypto ipsec transform-set myset esp-3des esp-sha-hmac

!--- Define the transform set for Phase 2. crypto map outside_map 20 match address 100

!--- Define which traffic can be sent to the IPsec peer. crypto map outside_map 20 set peer 172.16.1.1

!--- Sets the IPsec peer. crypto map outside_map 20 set transform-set myset

!--- Sets the IPsec transform set "myset" !--- to be used with the crypto map entry "outside_map" crypto map outside_map interface outside

!--- Crypto map applied to the outside interface of the ASA crypto isakmp enable outside
crypto isakmp policy 10
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400

!--- PHASE 1 CONFIGURATION ---! !--- This configuration uses isakmp policy 10. !--- These configuration commands !--- define the Phase 1 policies that are used. crypto isakmp policy 65535 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-

```

```

policy global_policy global tunnel-group 172.16.1.1 type ipsec-121

!--- In order to create and manage the database of connection-specific records !--- for ipsec-121-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 172.16.1.1 ipsec-attributes
  pre-shared-key *
!--- Enter the pre-shared-key in order to configure the authentication method. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ASA5510#

```

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 可查看对 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** — 显示所有当前 IPsec SA。

本部分显示用于以下配置的示例验证配置：

- [Cisco 5505 ASA](#)
- [Cisco 5510 ASA](#)

Cisco 5505 ASA 配置

```

ASA5505#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: 192.168.1.1
   Type    : L2L                Role    : initiator
   Rekey   : no                State   : MM_ACTIVE

ASA5505#show crypto ipsec sa
interface: outside
Crypto map tag: outside_map, seq num: 20, local
addr: 172.16.1.1

access-list 100 permit ip 10.2.2.0 255.255.255.0
10.1.1.0 255.255.255.0
local ident (addr/mask/prot/port):
(10.2.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
current_peer: 192.168.1.1

```

```

#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.: 172.16.1.1, remote crypto
endpt.: 192.168.1.1

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: A0411DE6

inbound esp sas:
spi: 0x8312C39C (2199045020)
transform: esp-3des esp-sha-hmac none
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 8192, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec):
(3824999/27807)
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0xA0411DE6 (2688622054)
transform: esp-3des esp-sha-hmac none
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 8192, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec):
(3824999/27807)
IV size: 8 bytes
replay detection support: Y

```

Cisco 5510 ASA 配置

```
ASA5510#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: 172.16.1.1
Type      : L2L           Role       : responder
Rekey     : no           State      : MM_ACTIVE

```

```
ASA5510#show crypto ipsec sa
```

```

interface: outside
Crypto map tag: outside_map, seq num: 20, local
addr: 192.168.1.1

access-list 100 permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
local ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(10.2.2.0/255.255.255.0/0/0)
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.: 192.168.1.1, remote crypto
endpt.: 172.16.1.1

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 8312C39C

inbound esp sas:
spi: 0xA0411DE6 (2688622054)
transform: esp-3des esp-sha-hmac none
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 8192, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec):
(4274999/27844)
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x8312C39C (2199045020)
transform: esp-3des esp-sha-hmac none
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 8192, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec):
(4274999/27844)
IV size: 8 bytes
replay detection support: Y

```

故障排除

本部分提供的信息可用于对配置进行故障排除。

使用以下命令可以：

- **clear crypto isakmp sa** — 清除第 1 阶段 SA。注意：clear crypto isakmp sa 命令是侵入式的，它将清除所有活动 VPN 隧道。从 PIX/ASA 软件的 8.0(3) 版本开始，可以使用 **clear crypto isakmp sa <peer ip address>** 命令清除单个 IKE SA。[在软件版本 8.0\(3\) 之前，可以使用 vpn-sessiondb logoff tunnel-group <tunnel-group-name> 命令清除单个隧道的 IKE 和 IPsec SA。](#)

```
ASA5505#vpn-sessiondb logoff tunnel-group 192.168.1.1
```

```
Do you want to logoff the VPN session(s)? [confirm] Y
```

```
INFO: Number of sessions from TunnelGroup "192.168.1.1" logged off : 1
```

```
ASA5505# Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, P
itcher: received key delete msg, spi 0xaa157573
```

```
Jan 19 13:58:43 [IKEv1]: Group = 192.168.1.1, IP = 192.168.1.1, Connection termi
nated for peer 192.168.1.1. Reason: Administrator Reset Remote Proxy 10.1.1.0,
Local Proxy 10.2.2.0
```

```
Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, IKE SA MM:
116f1ccf rcv'd Terminate: state MM_ACTIVE flags 0x0021c042, refcnt 1, tuncnt 1
```

```
Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, sending de
lete/delete with reason message
```

```
Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructi
```

```

ng blank hash payload
Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructi
ng IPsec delete payload
Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructi
ng qm hash payload
Jan 19 13:58:43 [IKEv1]: IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=c17
46fb4) with payloads : HDR + HASH (8) + DELETE (12) + NONE (0) total length : 68
Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, Active uni
t receives a delete event for remote peer 192.168.1.1.

Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, IKE Deleti
ng SA: Remote Proxy 10.1.1.0, Local Proxy 10.2.2.0
Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, IKE SA MM:
116f1ccf terminating: flags 0x0121c002, refcnt 0, tuncnt 0
Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, sending de
lete/delete with reason message
Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructi
ng blank hash payload
Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructi
ng IKE delete payload
Jan 19 13:58:43 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructi
ng qm hash payload
Jan 19 13:58:43 [IKEv1]: IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=a7e
78fac) with payloads : HDR + HASH (8) + DELETE (12) + NONE (0) total length : 80
Jan 19 13:58:43 [IKEv1 DEBUG]: Pitcher: received key delete msg, spi 0xaa157573
Jan 19 13:58:43 [IKEv1 DEBUG]: Pitcher: received key delete msg, spi 0x746fe476
Jan 19 13:58:43 [IKEv1]: IP = 192.168.1.1, Received encrypted packet with no mat
ching SA, dropping

```

- **clear crypto ipsec sa peer <peer IP address>** — 清除所需的第 2 阶段 SA。

```

ASA5505(config)#clear ipsec sa peer 192.168.1.1
ASA5505(config)# IPSEC: Deleted inbound decrypt rule, SPI 0x8030618F
    Rule ID: 0xD4E56A18
IPSEC: Deleted inbound permit rule, SPI 0x8030618F
    Rule ID: 0xD4DF4110
IPSEC: Deleted inbound tunnel flow rule, SPI 0x8030618F
    Rule ID: 0xD4DAE1F0
IPSEC: Deleted inbound VPN context, SPI 0x8030618F
    VPN handle: 0x00058FBC
IPSEC: Deleted outbound encrypt rule, SPI 0x0D6CDEEB
    Rule ID: 0xD4DA4348
IPSEC: Deleted outbound permit rule, SPI 0x0D6CDEEB
    Rule ID: 0xD4DAE7A8
IPSEC: Deleted outbound VPN context, SPI 0x0D6CDEEB
    VPN handle: 0x0005633C

```

- **debug crypto isakmp sa <debug level>** — 调试 ISAKMP SA 协商。

```

ASA5505(config)#debug crypto isakmp 7
ASA5505(config)# Jan 19 13:39:49 [IKEv1]: IP = 192.168.1.1, IKE_DECODE RECEIVED
Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VEN
DOR (13) + NONE (0) total length : 188
Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing SA payload
Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Oakley proposal is acceptable
Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing VID payload
Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Received NAT-Traversal ver 02 V
ID
Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing VID payload
Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Received NAT-Traversal ver 03 V
ID
Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing VID payload
Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Received Fragmentation VID
Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, IKE Peer included IKE fragmenta
tion capability flags: Main Mode: True Aggressive Mode: True
Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing IKE SA payload

```

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 2

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, constructing ISAKMP SA payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, constructing NAT-Traversal VID ver 02 payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, constructing Fragmentation VID + extended capabilities payload

Jan 19 13:39:49 [IKEv1]: IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 128

Jan 19 13:39:49 [IKEv1]: IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing ke payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing ISA_KE payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing nonce payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing VID payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Received Cisco Unity client VID

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing VID payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Received xauth V6 VID

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing VID payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Processing VPN3000/ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing VID payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Received Altiga/Cisco VPN3000/Cisco ASA GW VID

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing NAT-Discovery payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, computing NAT Discovery hash

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, processing NAT-Discovery payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, computing NAT Discovery hash

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, constructing ke payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, constructing nonce payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, constructing Cisco Unity VID payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, constructing xauth V6 VID payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Send IOS VID

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, constructing VID payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Send Altiga/Cisco VPN3000/Cisco ASA GW VID

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, constructing NAT-Discovery payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, computing NAT Discovery hash

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, constructing NAT-Discovery payload

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, computing NAT Discovery hash

Jan 19 13:39:49 [IKEv1]: IP = 192.168.1.1, Connection landed on tunnel_group 192.168.1.1

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, Generating keys for Responder...

Jan 19 13:39:49 [IKEv1]: IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304

Jan 19 13:39:49 [IKEv1]: IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, processing hash payload

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, Computing hash for ISAKMP

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Processing IOS keep alive payload: proposal=32767/32767 sec.

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, processing VID payload

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, Received DPD VID

Jan 19 13:39:49 [IKEv1]: Group = 192.168.1.1, IP = 192.168.1.1, Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

Jan 19 13:39:49 [IKEv1]: IP = 192.168.1.1, Connection landed on tunnel_group 192.168.1.1

Jan 19 13:39:49 [IKEv1]: Group = 192.168.1.1, IP = 192.168.1.1, Freeing previously allocated memory for authorization-dn-attributes

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructing ID payload

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructing hash payload

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, Computing hash for ISAKMP

Jan 19 13:39:49 [IKEv1 DEBUG]: IP = 192.168.1.1, Constructing IOS keep alive payload: proposal=32767/32767 sec.

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructing dpd vid payload

Jan 19 13:39:49 [IKEv1]: IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96

Jan 19 13:39:49 [IKEv1]: Group = 192.168.1.1, IP = 192.168.1.1, PHASE 1 COMPLETE

Jan 19 13:39:49 [IKEv1]: IP = 192.168.1.1, Keep-alive type for this connection: DPD

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, Starting P1 rekey timer: 73440 seconds.

Jan 19 13:39:49 [IKEv1]: IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=9421905f) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 196

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, processing hash payload

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, processing SA payload

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, processing nonce payload

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload

Jan 19 13:39:49 [IKEv1]: Group = 192.168.1.1, IP = 192.168.1.1, Received remote IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload

Jan 19 13:39:49 [IKEv1]: Group = 192.168.1.1, IP = 192.168.1.1, Received local IP Proxy Subnet data in ID Payload: Address 10.2.2.0, Mask 255.255.255.0, Protocol 0, Port 0

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, processing notify payload

Jan 19 13:39:49 [IKEv1]: Group = 192.168.1.1, IP = 192.168.1.1, QM IsRekeyed old sa not found by addr

Jan 19 13:39:49 [IKEv1]: Group = 192.168.1.1, IP = 192.168.1.1, Static Crypto Map check, checking map = outside_map, seq = 20...

Jan 19 13:39:49 [IKEv1]: Group = 192.168.1.1, IP = 192.168.1.1, Static Crypto Map check, map outside_map, seq = 20 is a successful match

Jan 19 13:39:49 [IKEv1]: Group = 192.168.1.1, IP = 192.168.1.1, IKE Remote Peer configured for crypto map: outside_map

Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, processing

```
IPSec SA payload
Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, IPSec SA P
roposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20
Jan 19 13:39:49 [IKEv1]: Group = 192.168.1.1, IP = 192.168.1.1, IKE: requesting
SPI!
Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, IKE got SP
I from key engine: SPI = 0x826ff027
Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, oakley con
structing quick mode
Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructi
ng blank hash payload
Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructi
ng IPSec SA payload
Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructi
ng IPSec nonce payload
Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, constructi
ng proxy ID
Jan 19 13:39:49 [IKEv1 DEBUG]: Group = 192.168.1.1, IP = 192.168.1.1, Transmitti
```

• **debug crypto ipsec sa <debug level> — 调试 IPsec SA 协商。**

```
ASA5505(config)#debug crypto ipsec 7
ASA5505(config)# IPSEC: New embryonic SA created @ 0xD4E56E18,
  SCB: 0xD4E56CF8,
  Direction: inbound
  SPI      : 0x8030618F
  Session ID: 0x00006000
  VPIF num  : 0x00000001
  Tunnel type: 121
  Protocol  : esp
  Lifetime  : 240 seconds
IPSEC: New embryonic SA created @ 0xD4E57AD8,
  SCB: 0xD4DAE608,
  Direction: outbound
  SPI      : 0x0D6CDEEB
  Session ID: 0x00006000
  VPIF num  : 0x00000001
  Tunnel type: 121
  Protocol  : esp
  Lifetime  : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x0D6CDEEB
IPSEC: Creating outbound VPN context, SPI 0x0D6CDEEB
  Flags: 0x00000005
  SA    : 0xD4E57AD8
  SPI   : 0x0D6CDEEB
  MTU   : 1500 bytes
  VCID  : 0x00000000
  Peer  : 0x00000000
  SCB   : 0x015E69CB
  Channel: 0xD3D60A98
IPSEC: Completed outbound VPN context, SPI 0x0D6CDEEB
  VPN handle: 0x0005633C
IPSEC: New outbound encrypt rule, SPI 0x0D6CDEEB
  Src addr: 10.2.2.0
  Src mask: 255.255.255.0
  Dst addr: 10.1.1.0
  Dst mask: 255.255.255.0
  Src ports
    Upper: 0
    Lower: 0
    Op    : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op    : ignore
```

Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x0D6CDEEB
Rule ID: 0xD4DA4348
IPSEC: New outbound permit rule, SPI 0x0D6CDEEB
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x0D6CDEEB
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x0D6CDEEB
Rule ID: 0xD4DAE7A8
IPSEC: Completed host IBSA update, SPI 0x8030618F
IPSEC: Creating inbound VPN context, SPI 0x8030618F
Flags: 0x00000006
SA : 0xD4E56E18
SPI : 0x8030618F
MTU : 0 bytes
VCID : 0x00000000
Peer : 0x0005633C
SCB : 0x015DD135
Channel: 0xD3D60A98
IPSEC: Completed inbound VPN context, SPI 0x8030618F
VPN handle: 0x00058FBC
IPSEC: Updating outbound VPN context 0x0005633C, SPI 0x0D6CDEEB
Flags: 0x00000005
SA : 0xD4E57AD8
SPI : 0x0D6CDEEB
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00058FBC
SCB : 0x015E69CB
Channel: 0xD3D60A98
IPSEC: Completed outbound VPN context, SPI 0x0D6CDEEB
VPN handle: 0x0005633C
IPSEC: Completed outbound inner rule, SPI 0x0D6CDEEB
Rule ID: 0xD4DA4348
IPSEC: Completed outbound outer SPD rule, SPI 0x0D6CDEEB
Rule ID: 0xD4DAE7A8
IPSEC: New inbound tunnel flow rule, SPI 0x8030618F
Src addr: 10.1.1.0
Src mask: 255.255.255.0
Dst addr: 10.2.2.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0

```
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x8030618F
Rule ID: 0xD4DAE1F0
IPSEC: New inbound decrypt rule, SPI 0x8030618F
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x8030618F
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x8030618F
Rule ID: 0xD4E56A18
IPSEC: New inbound permit rule, SPI 0x8030618F
Src addr: 192.168.1.1
```

[相关信息](#)

- [Cisco ASA 5500 系列自适应安全设备支持页](#)
- [Cisco PIX 500 系列安全设备支持页](#)
- [最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案](#)
- [IPsec 协商/IKE 协议支持页](#)