

通过 NAT 与 Cisco VPN 客户端配置 PIX 之间的动态到静态 IPsec

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[“正常”的调试输出示例](#)

[中央 PIX 调试](#)

[远程 PIX 调试](#)

[客户端调试](#)

[相关信息](#)

[简介](#)

在此示例配置中，远程 PIX 通过动态主机配置协议 (DHCP) 接收 IP 地址并连接到中央 PIX。此配置使中央 PIX 可以接受动态 IPsec 连接。远程 PIX 使用网络地址转换 (NAT) 将它后面以特有方式编址的设备“加入”到中央 PIX 后面以特有方式编址的网络。远程 PIX 可以启动与中央 PIX 的连接（它知道端点），但是中央 PIX 不能启动与远程 PIX 的连接（它不知道端点）。

在此示例配置中，Tiger 是远程 PIX，Lion 是中央 PIX。由于 Tiger 的 IP 地址未知，因此必须将 Lion 配置为动态地接受从知道通配符预共享密钥的任意位置启动的连接。Tiger 知道什么数据流将被加密（因为这由访问列表指定），并知道 Lion 端点所在的位置。Tiger 必须启动连接。两端都执行 NAT 和 nat 0 以绕过对 IPsec 数据流执行 NAT。

此外，此配置中的远程用户使用 Cisco VPN 客户端 3.x 连接到中央 PIX (Lion)。远程用户无法连接到远程 PIX (Tiger)，因为两端都将已动态地分配 IP 地址，因此将不知道向何处发送请求。

要了解有关 PIX/ASA 7.x 中使用 Cisco VPN 客户端 4.x 的相同方案的详细信息，请参阅[配置使用 NAT 和 VPN 客户端的 PIX/ASA 7.x PIX 到 PIX 动态到静态 IPsec 配置示例](#)。

[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：

- Cisco PIX 防火墙软件版本 6.0(1) (或适用于 Cisco VPN 客户端 3.x 的更高版本)
- Cisco PIX 防火墙软件版本 5.3.1 (远程 PIX)
- Cisco VPN 客户端 3.x 版

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。

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

Lion 配置

```
Building configuration...
: Saved
:
PIX Version 6.0(1)
nameif gb-ethernet0 spare1 security10
nameif gb-ethernet1 spare2 security15
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname lion
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
```

```

!
!--- ACL to avoid Network Address Translation (NAT) on
the IPsec packets. access-list 100 permit ip 10.2.2.0
255.255.255.0 10.1.1.0 255.255.255.0 access-list 100
permit ip 10.2.2.0 255.255.255.0 10.3.3.0 255.255.255.0
! pager lines 24 logging buffered debugging interface
gb-ethernet0 1000auto shutdown interface gb-ethernet1
1000auto shutdown interface ethernet0 10baset interface
ethernet1 10baset mtu spare1 1500 mtu spare2 1500 mtu
outside 1500 mtu inside 1500 ip address spare1 127.0.0.1
255.255.255.255 ip address spare2 127.0.0.1
255.255.255.255 ! !--- IP addresses on the interfaces ip
address outside 203.1.1.1 255.255.255.0 ip address
inside 10.2.2.1 255.255.255.0 ! ip audit info action
alarm ip audit attack action alarm ip local pool
clientpool 10.3.3.1-10.3.3.10 no failover failover
timeout 0:00:00 failover poll 15 failover ip address
spare1 0.0.0.0 failover ip address spare2 0.0.0.0
failover ip address outside 0.0.0.0 failover ip address
inside 0.0.0.0 pdm history enable arp timeout 14400 !---
global (outside) 1 203.1.1.10-203.1.1.15 !--- Change
from NAT to PAT on the DHCP interface. global (outside)
1 interface ! !--- Binding ACL 100 to the NAT statement
to avoid NAT on the IPsec packets. nat (inside) 0
access-list 100 ! nat (inside) 1 0.0.0.0 0.0.0.0 0 0
conduit permit icmp any any ! !--- Default route to the
Internet route outside 0.0.0.0 0.0.0.0 203.1.1.2 1 !
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 rpc 0:10:00 h323 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 no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable ! !--- The sysopt command
avoids conduit on the IPsec encrypted traffic. sysopt
connection permit-ipsec ! no sysopt route dnat ! !---
Phase 2 encryption type crypto ipsec transform-set myset
esp-des esp-md5-hmac crypto dynamic-map cisco 1 set
transform-set myset crypto map dyn-map 20 ipsec-isakmp
dynamic cisco ! !--- Binds the IPsec engine on the
outside interface. crypto map dyn-map interface outside
! !--- Enables ISAKMP key-exchange. isakmp enable
outside ! !--- ISAKMP policy for accepting dynamic
connections from the remote PIX. isakmp key *****
address 0.0.0.0 netmask 0.0.0.0 !--- ISAKMP policy for
Cisco VPN Client 2.x isakmp policy 10 authentication
pre-share isakmp policy 10 encryption des isakmp policy
10 hash md5 isakmp policy 10 group 1 isakmp policy 10
lifetime 1000 ! !--- ISAKMP policy for Cisco VPN Client
3.x isakmp policy 20 authentication pre-share isakmp
policy 20 encryption des isakmp policy 20 hash sha
isakmp policy 20 group 2 isakmp policy 20 lifetime 86400
! !--- IPsec group configuration for either client
vpngroup unityclient address-pool clientpool vpngroup
unityclient dns-server 10.1.1.3 vpngroup unityclient
wins-server 10.1.1.3 vpngroup unityclient default-domain
cisco.com vpngroup unityclient idle-time 1800 vpngroup
unityclient password ***** ! telnet timeout 5 ssh
timeout 5 terminal width 80
Cryptochecksum:d6fe92db883a052c5765be21a74e7c8d : end
[OK]

```

Tiger 配置

Building configuration...

```

: Saved
:
PIX Version 5.3(1)
nameif gb-ethernet0 spare1 security10
nameif gb-ethernet1 spare2 security15
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname tiger
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!
!--- ACL to avoid NAT on the IPsec packets access-list
101 permit ip 10.1.1.0 255.255.255.0 10.2.2.0
255.255.255.0 ! pager lines 24 logging on no logging
timestamp no logging standby no logging console no
logging monitor logging buffered debugging no logging
trap no logging history logging facility 20 logging
queue 512 interface gb-ethernet0 1000auto shutdown
interface gb-ethernet1 1000auto shutdown interface
ethernet0 10baset interface ethernet1 10baset mtu spare1
1500 mtu spare2 1500 mtu outside 1500 mtu inside 1500 ip
address spare1 127.0.0.1 255.255.255.255 ip address
spare2 127.0.0.1 255.255.255.255 ! ip address outside
dhcp ip address inside 10.1.1.1 255.255.255.0 ! ip audit
info action alarm ip audit attack action alarm no
failover failover timeout 0:00:00 failover poll 15
failover ip address spare1 0.0.0.0 failover ip address
spare2 0.0.0.0 failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0 arp timeout 14400
global (outside) 1 204.1.1.10-204.1.1.15 ! !--- Binds
ACL 101 to the NAT statement to avoid NAT on the IPsec
packets. nat (inside) 0 access-list 101 ! nat (inside) 1
0.0.0.0 0.0.0.0 0 0 conduit permit icmp any any route
outside 0.0.0.0 0.0.0.0 204.1.1.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h323 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 no snmp-server location no snmp-server contact
snmp-server community public no snmp-server enable traps
floodguard enable ! !--- The sysopt command avoids
conduit on the IPsec encrypted traffic. sysopt
connection permit-ipsec ! no sysopt route dnats ! !---
Phase 2 encryption type crypto ipsec transform-set myset
esp-des esp-md5-hmac crypto map newmap 10 ipsec-isakmp
crypto map newmap 10 match address 101 crypto map newmap
10 set peer 203.1.1.1 crypto map newmap 10 set
transform-set myset ! !--- Binds the IPsec engine on the
outside interface. crypto map newmap interface outside !
!--- Enables ISAKMP key-exchange isakmp enable outside !
!--- ISAKMP policy for connecting to the central PIX.
isakmp key ***** address 203.1.1.1 netmask
255.255.255.255 isakmp identity hostname isakmp policy
10 authentication pre-share isakmp policy 10 encryption
des isakmp policy 10 hash md5 isakmp policy 10 group 1
isakmp policy 10 lifetime 1000 ! telnet timeout 5 ssh

```

```
timeout 5 terminal width 80
Cryptochecksum:6743b7bf9476590ecd1a1a8c6d75245b : end
[OK]
```

验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

[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。

注意： 必须在配置模式下执行 **clear** 命令。

- **clear crypto ipsec sa** - 在尝试协商 VPN 隧道失败后重置 IPsec 关联。
- **clear crypto isakmp sa** - 在尝试协商 VPN 隧道失败后重置 Internet 安全连接和密钥管理协议 (ISAKMP) 安全关联。
- **show crypto engine ipsec** - 显示加密的会话。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

[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。

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** - 用于查看客户端是否协商 VPN 连接的 IPsec 部分。
- **debug crypto isakmp connection** - 用于查看对等体是否协商 VPN 的 ISAKMP 部分。

“正常”的调试输出示例

- [中央 PIX 调试](#)
- [远程 PIX 调试](#)
- [客户端调试](#)

中央 PIX 调试

```
crypto_isakmp_process_block: src 204.1.1.1, dest 203.1.1.1
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
```

```
ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
```

```
ISAKMP:      life duration (basic) of 1000
ISAKMP (0):  atts are acceptable. Next payload is 0
ISAKMP (0):  SA is doing pre-shared key authentication using id type ID_FQDN
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 204.1.1.1, dest 203.1.1.1
OAK_MM exchange
ISAKMP (0):  processing KE payload. message ID = 0

ISAKMP (0):  processing NONCE payload. message ID = 0

ISAKMP (0):  processing vendor id payload

ISAKMP (0):  processing vendor id payload

ISAKMP (0):  processing vendor id payload

ISAKMP (0):  speaking to another IOS box!

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 204.1.1.1, dest 203.1.1.1
OAK_MM exchange
ISAKMP (0):  processing ID payload. message ID = 0
ISAKMP (0):  processing HASH payload. message ID = 0
ISAKMP (0):  SA has been authenticated

ISAKMP (0):  ID payload
      next-payload : 8
      type          : 2
      protocol      : 17
      port          : 500
      length        : 10
ISAKMP (0):  Total payload length: 14
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 204.1.1.1, dest 203.1.1.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0):  processing SA payload. message ID = 1223411072

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:  attributes in transform:
ISAKMP:  encaps is 1
ISAKMP:  SA life type in seconds
ISAKMP:  SA life duration (basic) of 28800
ISAKMP:  SA life type in kilobytes
ISAKMP:  SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:  authenticator is HMAC-MD5
ISAKMP (0):  atts are acceptable.IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 203.1.1.1, src= 204.1.1.1,
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0):  processing NONCE payload. message ID = 1223411072

ISAKMP (0):  processing ID payload. message ID = 1223411072
ISAKMP (0):  ID_IPV4_ADDR_SUBNET src 10.2.2.0/255.255.255.0 prot 0 port 0
ISAKMP (0):  processing ID payload. message ID = 1223411072
ISAKMP (0):  ID_IPV4_ADDR_SUBNET dst 10.1.1.0/255.255.255.0 prot 0 port
0IPSEC(key_engine): got a queue event...
```

IPSEC(spi_response): getting spi 0xd0e27cb6(3504503990) for SA from 204.1.1.1 to 203.1.1.1 for prot 3

return status is IKMP_NO_ERROR

crypto_isakmp_process_block: src 204.1.1.1, dest 203.1.1.1

OAK_QM exchange

oakley_process_quick_mode:

OAK_QM_AUTH_AWAIT

ISAKMP (0): Creating IPsec SAs

inbound SA from 204.1.1.1 to 203.1.1.1 proxy 10.2.2.0 to 10.1.1.0)

has spi 3504503990 and conn_id 4 and flags 4

lifetime of 28800 seconds

lifetime of 4608000 kilobytes

outbound SA from 203.1.1.1 to 204.1.1.1(proxy 10.1.1.0 to 10.2.2.0)

has spi 2729504033 and conn_id 3 and flags 4

lifetime of 28800 seconds

lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...

IPSEC(initialize_sas): ,

(key eng. msg.) dest= 203.1.1.1, src= 204.1.1.1,

dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),

src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),

protocol= ESP, transform= esp-des esp-md5-hmac ,

lifedur= 28800s and 4608000kb,

spi= 0xd0e27cb6(3504503990), conn_id= 4, keysize= 0, flags= 0x4

IPSEC(initialize_sas): ,

(key eng. msg.) src= 203.1.1.1, dest= 204.1.1.1,

src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),

dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),

protocol= ESP, transform= esp-des esp-md5-hmac ,

lifedur= 28800s and 4608000kb,

spi= 0xa2b0ed21(2729504033), conn_id= 3, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR

[远程 PIX 调试](#)

ISAKMP (0): beginning Main Mode exchange

crypto_isakmp_process_block: src 203.1.1.1, dest 204.1.1.1

OAK_MM exchange

ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy

ISAKMP: encryption DES-CBC

ISAKMP: hash MD5

ISAKMP: default group 1

ISAKMP: auth pre-share

ISAKMP: life type in seconds

ISAKMP: life duration (basic) of 1000

ISAKMP (0): atts are acceptable. Next payload is 0

ISAKMP (0): SA is doing pre-shared key authentication using id type ID_FQDN

return status is IKMP_NO_ERROR

crypto_isakmp_process_block: src 203.1.1.1, dest 204.1.1.1

OAK_MM exchange

ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to another IOS box!

ISAKMP (0): ID payload

next-payload : 8

```
type          : 2
protocol      : 17
port         : 500
length       : 18
ISAKMP (0): Total payload length: 22
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 203.1.1.1, dest 204.1.1.1
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated

ISAKMP (0): beginning Quick Mode exchange, M-ID of
1223411072:48ebc580IPSEC(key_engine):got a queue event...
IPSEC(spi_response): getting spi 0xa2b0ed21(2729504033) for SA
from          203.1.1.1 to          204.1.1.1 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 203.1.1.1, dest 204.1.1.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1223411072

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:  attributes in transform:
ISAKMP:  encaps is 1
ISAKMP:  SA life type in seconds
ISAKMP:  SA life duration (basic) of 28800
ISAKMP:  SA life type in kilobytes
ISAKMP:  SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:  authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 203.1.1.1, src= 204.1.1.1,
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 1223411072

ISAKMP (0): processing ID payload. message ID = 1223411072
ISAKMP (0): processing ID payload. message ID = 1223411072
ISAKMP (0): Creating IPsec SAs
inbound SA from 203.1.1.1 to 204.1.1.1 (proxy 10.1.1.0 to 10.2.2.0)
has spi 2729504033 and conn_id 4 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 204.1.1.1 to 203.1.1.1 (proxy 10.2.2.0 to 10.1.1.0)
has spi 3504503990 and conn_id 3 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 204.1.1.1, src= 203.1.1.1,
dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0xa2b0ed21(2729504033), conn_id= 4, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 204.1.1.1, dest= 203.1.1.1,
```



```
src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0xd0e27cb6(3504503990), conn_id= 3, keysize= 0, flags= 0x4
```

return status is IKMP_NO_ERROR

客户端调试

```
19      16:43:20.402 06/28/01 Sev=Info/4      CM/0x63100004
Establish secure connection using Ethernet

20      16:43:20.402 06/28/01 Sev=Info/4      CM/0x63100025
Attempt connection with server "203.1.1.1"

21      16:43:20.402 06/28/01 Sev=Info/6      IKE/0x6300003B
Attempting to establish a connection with 203.1.1.1.

22      16:43:20.442 06/28/01 Sev=Info/4      IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to 203.1.1.1

23      16:43:20.452 06/28/01 Sev=Info/4      IPSEC/0x63700014
Deleted all keys

24      16:43:20.492 06/28/01 Sev=Info/5      IKE/0x6300002F
Received ISAKMP packet: peer = 203.1.1.1

25      16:43:20.492 06/28/01 Sev=Info/4      IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, KE, ID, NON, HASH) from 203.1.1.1

26      16:43:20.492 06/28/01 Sev=Info/5      IKE/0x63000059
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

27      16:43:20.492 06/28/01 Sev=Info/5      IKE/0x63000001
Peer is a Cisco-Unity compliant peer

28      16:43:20.492 06/28/01 Sev=Info/5      IKE/0x63000059
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

29      16:43:20.492 06/28/01 Sev=Info/5      IKE/0x63000001
Peer supports DPD

30      16:43:20.492 06/28/01 Sev=Info/5      IKE/0x63000059
Vendor ID payload = A0EB477E6627B406AA10F958254B3517

31      16:43:20.542 06/28/01 Sev=Info/4      IKE/0x63000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT) to 203.1.1.1

32      16:43:20.542 06/28/01 Sev=Info/4      CM/0x6310000E
Established Phase 1 SA. 1 Phase 1 SA in the system

33      16:43:21.143 06/28/01 Sev=Info/4      IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 203.1.1.1

34      16:43:24.067 06/28/01 Sev=Info/5      IKE/0x6300002F
Received ISAKMP packet: peer = 203.1.1.1

35      16:43:24.067 06/28/01 Sev=Info/4      IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 203.1.1.1
```

36 16:43:24.067 06/28/01 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.3.3.1

37 16:43:24.067 06/28/01 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 10.1.1.3

38 16:43:24.067 06/28/01 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS) : , value = 10.1.1.3

39 16:43:24.067 06/28/01 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: , value = cisco.com

40 16:43:24.067 06/28/01 Sev=Info/4 CM/0x63100018
Mode Config data received

41 16:43:24.668 06/28/01 Sev=Info/5 IKE/0x63000055
Received a key request from Driver for IP address 203.1.1.1, GW IP = 203.1.1.1

42 16:43:24.668 06/28/01 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 203.1.1.1

43 16:43:24.668 06/28/01 Sev=Info/5 IKE/0x63000055
Received a key request from Driver for IP address 10.10.10.255, GW IP = 203.1.1.1

44 16:43:24.668 06/28/01 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 203.1.1.1

45 16:43:24.668 06/28/01 Sev=Info/4 IPSEC/0x63700014
Deleted all keys

46 16:43:25.619 06/28/01 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 203.1.1.1

47 16:43:25.619 06/28/01 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 203.1.1.1

48 16:43:25.619 06/28/01 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

49 16:43:25.619 06/28/01 Sev=Info/5 IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

50 16:43:25.619 06/28/01 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 203.1.1.1

51 16:43:25.619 06/28/01 Sev=Info/5 IKE/0x63000058
Loading IPsec SA (Message ID = 0x59515364 OUTBOUND SPI = 0xB24CDB55 INBOUND SPI = 0x83AA0042)

52 16:43:25.619 06/28/01 Sev=Info/5 IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0xB24CDB55

53 16:43:25.619 06/28/01 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x83AA0042

54 16:43:25.619 06/28/01 Sev=Info/4 CM/0x63100019
One secure connection established

55 16:43:25.629 06/28/01 Sev=Info/6 DIALER/0x63300003
Connection established.

56 16:43:25.669 06/28/01 Sev=Info/6 DIALER/0x63300008
MAPI32 Information - Outlook not default mail client

57 16:43:25.960 06/28/01 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 203.1.1.1

58 16:43:25.960 06/28/01 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 203.1.1.1

59 16:43:25.960 06/28/01 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

60 16:43:25.960 06/28/01 Sev=Info/5 IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

61 16:43:25.960 06/28/01 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 203.1.1.1

62 16:43:25.960 06/28/01 Sev=Info/5 IKE/0x63000058
Loading IPsec SA (Message ID = 0x23A23005 OUTBOUND SPI = 0xAD0599DB INBOUND SPI = 0x2B74D4A4)

63 16:43:25.960 06/28/01 Sev=Info/5 IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0xAD0599DB

64 16:43:25.960 06/28/01 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x2B74D4A4

65 16:43:25.960 06/28/01 Sev=Info/4 CM/0x63100021
Additional Phase 2 SA established.

66 16:43:25.960 06/28/01 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

67 16:43:25.960 06/28/01 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x55db4cb2 into key list

68 16:43:25.960 06/28/01 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

69 16:43:25.960 06/28/01 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x4200aa83 into key list

70 16:43:25.960 06/28/01 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

71 16:43:25.960 06/28/01 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0xdb9905ad into key list

72 16:43:25.960 06/28/01 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

73 16:43:25.960 06/28/01 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0xa4d4742b into key list

74 16:43:35.173 06/28/01 Sev=Info/6 IKE/0x6300003D
Sending DPD request to 203.1.1.1, seq# = 1856135987

75 16:43:35.173 06/28/01 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST) to 203.1.1.1

76 16:43:35.173 06/28/01 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 203.1.1.1

77 16:43:35.173 06/28/01 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK) from 203.1.1.1

78 16:43:35.173 06/28/01 Sev=Info/5 IKE/0x6300003F
Received DPD ACK from 203.1.1.1, seq# received = 1856135987, seq# expected = 1856135987

[相关信息](#)

- [PIX 支持页](#)
- [PIX 命令参考](#)
- [配置 IPsec 网络安全](#)
- [IP 安全 \(IPsec\) 产品支持页面](#)
- [技术支持和文档 - Cisco Systems](#)