

# 动态IPsec配置示例在静态寻址的ASA和一个动态地寻址的IOS路由器之间的有NAT的

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[背景信息](#)

[Configure](#)

[Network Diagram](#)

[配置](#)

[清除安全关联 \(SA\)](#)

[Verify](#)

[ASA安全工具-请显示命令](#)

[远程IOS路由器-请显示命令](#)

[Troubleshoot](#)

[ASA -调试输出](#)

[远程IOS路由器-调试输出](#)

[Related Information](#)

## Introduction

本文为如何给enable (event)可适应的安全工具(ASA)为了接受从IOS路由器的动态IPSec连接提供一配置示例。

## Prerequisites

### Requirements

在您尝试此配置前，请保证ASA和路由器有设立的IPSec隧道互联网连通性。

本文档假定您已在公共接口和专用接口上分配了 IP 地址，并且能够对远程 VPN 设备的 IP 地址执行 ping 操作。

### Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco 2900 Router和Cisco IOS Software Release 15.2(4)M3
- Cisco可适应的安全工具软件版本9.4(1)

The information in this document was created from the devices in a specific lab environment.All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 背景信息

如果专用网络 10.1.1.x 接入 Internet，则远程路由器将执行网络地址转换 (NAT)。从 10.1.1.x 的数据流到在 ASA 后的专用网络 10.2.2.x 从 NAT 进程被排除。IPSec 隧道设立，只有当数据流 (10.1.1.x) 首次从有一个远程网络的路由器的连接与 ASA (10.2.2.x)。路由器可以首次与 ASA 的连接，但是 ASA 不可以首次与路由器的连接。

此配置 enable (event) 创建一条动态 IPsec LAN 对 LAN (L2L) 隧道的 ASA 用一台远程 VPN 路由器。此路由器动态地从其 Internet 服务提供商接受外部公共 IP 地址。动态主机配置协议 (DHCP) 可提供此机制，以便动态地分配提供商提供的 IP 地址。这样，当主机不再需要这些 IP 地址时，就可以重用它们。

在 ASA 您能配置手工的 NAT 保证通过隧道不被转换的数据流。在本例中，如果是在 10.2.2.0 网络并且去 10.1.1.0 网络，过去常常的手工的 NAT 是允许 10.1.1.0 网络流量被加密，不用被转换到外部接口 IP 地址。在路由器上，**路由映射**和**访问列表命令**用于允许 10.1.1.0 网络流量被加密，不用 NAT。然而，当您去别处 (类似互联网) 时，您被转换为外部接口 IP 地址通过端口地址转换 (PAT)。

**Note:** 参考 [适用 NAT](#) 关于 NAT 的更多信息

这些是在 ASA 的配置 required 命令为了数据流不运行通过在隧道的 PAT 和数据流到运行的互联网通过 PAT

```
object network LOCAL
  subnet 10.2.2.0 255.255.255.0
object network REMOTE
  subnet 10.1.1.0 255.255.255.0
```

```
nat (inside,outside) source static LOCAL LOCAL destination static REMOTE REMOTE
```

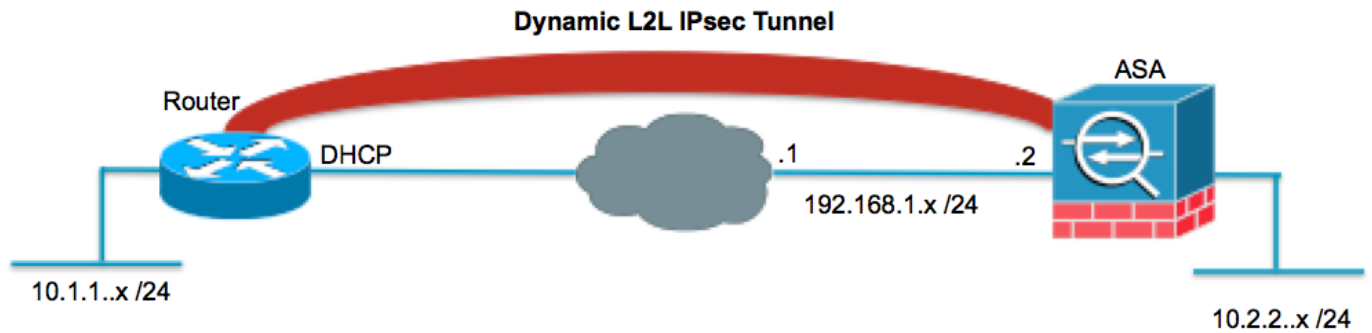
```
object network LOCAL
  nat (inside,outside) dynamic interface
```

## Configure

本部分提供有关如何配置本文档所述功能的信息。

## Network Diagram

本文档使用以下网络设置：



## 配置

本文档使用以下配置：

### 路由器

```

Router#show running-config
Current configuration : 1354 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef

!--- Configuration for IKE policies.
!--- Enables the IKE policy configuration (config-isakmp)
!--- command mode, where you can specify the parameters that
!--- are used during an IKE negotiation.

crypto isakmp policy 1
 encryption aes 256
 hash sha
 authentication pre-share
 group 2

!--- Specifies the preshared key "cisco123" which should
!--- be identical at both peers. This is a global
!--- configuration mode command.

crypto isakmp key cisco123 address 192.168.1.2

```

```
!  
!  
!--- Configuration for IPsec policies.  
!--- Enables the crypto transform configuration mode,  
!--- where you can specify the transform sets that are used  
!--- during an IPsec negotiation.  
  
crypto ipsec transform-set myset esp-aes 256 esp-sha-hmac  
  
!--- Indicates that IKE is used to establish  
!--- the IPsec Security Association for protecting the  
!--- traffic specified by this crypto map entry.  
  
crypto map mymap 10 ipsec-isakmp  
  
!--- Sets the IP address of the remote end.  
  
set peer 192.168.1.2  
  
!--- Configures IPsec to use the transform-set  
!--- "myset" defined earlier in this configuration.  
  
set transform-set myset  
  
!--- Specifies the interesting traffic to be encrypted.  
  
match address 101  
!  
!  
!  
!  
interface FastEthernet0/0  
  
!--- The interface dynamically learns its IP address  
!--- from the service provider.  
  
ip address DHCP  
  
ip virtual-reassembly  
half-duplex  
  
!--- Configures the interface to use the  
!--- crypto map "mymap" for IPsec.  
  
crypto map mymap  
!  
interface FastEthernet1/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface Serial2/0
```

```

ip address 10.1.1.2 255.255.255.0
ip nat inside
ip virtual-reassembly
no fair-queue
!
interface Serial2/1
no ip address
shutdown
!
interface Serial2/2
no ip address
shutdown
!
interface Serial2/3
no ip address
shutdown
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ip nat inside source route-map nonat interface FastEthernet0/0 overload
!

!--- This crypto ACL 101 -permit identifies the
!--- matching traffic flows to be protected via encryption.

access-list 101 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255

!--- This ACL 110 identifies the traffic flows using route map and
!--- are PATed via outside interface (Ethernet0/0).

access-list 110 deny ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 110 permit ip 10.1.1.0 0.0.0.255 any

!
route-map nonat permit 10
match ip address 110
!
!
control-plane
!

!
line con 0
line aux 0
line vty 0 4
!
!
end

```

## ASA

```

ASA#show running-config
ASA Version 9.4(1)
!
hostname ASA

```

```
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!

!--- Configure the outside and inside interfaces.

interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
!
!

!--- Output is suppressed.

!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

!--- Manual NAT prevents NAT for networks specified in the statement - nonat.
!--- The Object NAT 1 command specifies PAT using
!--- the outside interface for all other traffic.

object network LOCAL
 subnet 10.2.2.0 255.255.255.0
object network REMOTE
 subnet 10.1.1.0 255.255.255.0

pager lines 24
mtu outside 1500
mtu inside 1500
no failover
no asdm history enable
arp timeout 14400

!--- Manual NAT prevents NAT for networks specified in the statement - nonat.
!--- The Object NAT 1 command specifies PAT using
!--- the outside interface for all other traffic.

nat (inside,outside) source static LOCAL LOCAL destination static REMOTE REMOTE
!
object network LOCAL
 nat (inside,outside) dynamic interface

route outside 0.0.0.0 0.0.0.0 192.168.1.1 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
```

```
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 ikev1 transform-set myset esp-aes-256 esp-sha-hmac
```

```
!--- Defines a dynamic crypto map with
!--- the specified encryption settings.
```

```
crypto dynamic-map cisco 1 set ikev1 transform-set myset
```

```
!--- Binds the dynamic map to the IPsec/ISAKMP process.
```

```
crypto map dyn-map 10 ipsec-isakmp dynamic cisco
```

```
!--- Specifies the interface to be used with
!--- the settings defined in this configuration.
```

```
crypto map dyn-map interface outside
```

```
!--- PHASE 1 CONFIGURATION ---!
```

```
!--- This configuration uses isakmp policy 10.
!--- The configuration commands here define the Phase
!--- 1 policy parameters that are used.
```

```
crypto ikev1 enable outside
crypto isakmp policy 10
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
```

```
!--- The security appliance provides the default tunnel groups
!--- for Lan to Lan access (DefaultL2LGroup) and configure the preshared key
!--- (cisco123) to authenticate the remote router.
```

```
tunnel-group DefaultL2LGroup ipsec-attributes
  pre-shared-key cisco123
```

```
telnet timeout 5
ssh timeout 5
console timeout 0
```

```
!
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
prompt hostname context
Cryptochecksum:6ed4a7bce392a439d0a16e86743e2663
: end

```

## 清除安全关联 (SA)

在ASA的特权模式，请使用这些命令：

- **clear crypto ipsec sa** — 删除活动 IPsec SA。crypto的关键字是可选的。
- **clear crypto isakmp sa** — 删除活动 IKE SA。crypto的关键字是可选的。

## Verify

Use this section to confirm that your configuration works properly.

[思科 CLI 分析器 \(仅适用于注册客户\)](#) 支持某些 **show** 命令。要查看对 show 命令输出的分析，请使用思科 CLI 分析器。

## ASA安全工具-请显示命令

- **show crypto isakmp sa** - 显示对等体上的所有当前 IKE SA。

```

ASA#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: 172.16.1.3
  Type    : L2L           Role    : responder
  Rekey   : no          State   : MM_ACTIVE

```

- **show crypto ipsec sa** — 显示对等体上的所有当前 IPsec SA。

```

ASA#show crypto ipsec sa
interface: outside
Crypto map tag: cisco, seq num: 1, local addr: 192.168.1.2

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: 172.16.1.3

```



```
#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.: 192.168.1.2, remote crypto endpt.: 172.16.1.3
```

```
path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 28C8C1BD
```

```
inbound esp sas:
```

```
spi: 0x33785672 (863524466)
transform: esp-3des esp-md5-hmac
in use settings = {L2L, Tunnel, }
slot: 0, conn_id: 6, crypto-map: cisco
sa timing: remaining key lifetime (kB/sec): (4274999/3564)
IV size: 8 bytes
replay detection support: Y
```

```
outbound esp sas:
```

```
spi: 0x28C8C1BD (684245437)
transform: esp-3des esp-md5-hmac
in use settings = {L2L, Tunnel, }
slot: 0, conn_id: 6, crypto-map: cisco
sa timing: remaining key lifetime (kB/sec): (4274999/3562)
IV size: 8 bytes
replay detection support: Y
```

## 远程IOS路由器-请显示命令

- **show crypto isakmp sa** - 显示对等体上的所有当前 IKE SA。

```
Router#show crypto isakmp sa
```

dst	src	state	conn-id	slot	status
192.168.1.2	172.16.1.3	QM_IDLE	1	0	ACTIVE

- **show crypto ipsec sa** — 显示对等体上的所有当前 IPsec SA。

```
Router#show crypto ipsec sa
```

```
interface: Ethernet0/0
```

```
Crypto map tag: pix, local addr 172.16.1.3
```

```
protected vrf: (none)
```

```
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 192.168.1.2 port 500
```

```
PERMIT, flags={origin_is_acl,}
```

```
#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 compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 62, #recv errors 0
```

```
local crypto endpt.: 172.16.1.3, remote crypto endpt.: 192.168.1.2
```

```
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
```

```
current outbound spi: 0x33785672(863524466)
```

```
inbound esp sas:
```

```
spi: 0x28C8C1BD(684245437)
```

```
transform: esp-3des esp-md5-hmac ,
```

```

in use settings ={Tunnel, }
conn id: 2002, flow_id: SW:2, crypto map: pix
sa timing: remaining key lifetime (k/sec): (4431817/3288)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x33785672(863524466)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: SW:1, crypto map: pix
sa timing: remaining key lifetime (k/sec): (4431817/3286)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

## Troubleshoot

本部分提供的信息可用于对配置进行故障排除。

[思科 CLI 分析器 \( 仅适用于注册客户 \)](#) 支持某些 **show** 命令。要查看对 show 命令输出的分析，请使用思科 CLI 分析器。

**Note:**使用 **debug** 命令之前，请参阅[有关 debug 命令的重要信息](#)和 [IP 安全故障排除 - 了解和 使用 debug 命令](#)。

- [可适应的安全工具-调试输出](#) **debug crypto ipsec 7** - 显示第 2 阶段的 IPsec 协商。 **debug crypto isakmp 7** - 显示第 1 阶段的 ISAKMP 协商。
- [远程 IOS 路由器 - debug 输出](#) **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。

## ASA -调试输出

```

ASA#debug crypto isakmp 7
Jan 01 21:42:13 [IKEv1]: IP = 172.16.1.3, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 144
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, processing SA payload
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, Oakley proposal is acceptable
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, processing VID payload
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, processing VID payload
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, Received NAT-Traversal ver 03 VID
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, processing VID payload
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, Received NAT-Traversal ver 02 VID
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, processing IKE SA payload
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 3

```

Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, constructing ISAKMP SA payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, constructing Fragmentation VID +  
extended capabilities payload  
Jan 01 21:42:13 [IKEv1]: IP = 172.16.1.3, IKE\_DECODE SENDING Message (msgid=0) w  
ith payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 108  
Jan 01 21:42:13 [IKEv1]: IP = 172.16.1.3, IKE\_DECODE RECEIVED Message (msgid=0)  
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 256  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, processing ke payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, processing ISA\_KE payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, processing nonce payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, processing VID payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, Received Cisco Unity client VID  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, processing VID payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, Received DPD VID  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, processing VID payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, Processing IOS/PIX Vendor ID pay  
load (version: 1.0.0, capabilities: 0000077f)  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, processing VID payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, Received xauth V6 VID  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, constructing ke payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, constructing nonce payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, constructing Cisco Unity VID payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, constructing xauth V6 VID payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, Send IOS VID  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, Constructing ASA spoofing IOS Ve  
ndor ID payload (version: 1.0.0, capabilities: 20000001)  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, constructing VID payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, Send Altiga/Cisco  
VPN3000/CiscoASA GW VID  
Jan 01 21:42:13 [IKEv1]: IP = 172.16.1.3, Connection landed on tunnel\_group  
DefaultL2LGroup  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3, Generat  
ing keys for Responder...  
Jan 01 21:42:13 [IKEv1]: IP = 172.16.1.3, IKE\_DECODE SENDING Message (msgid=0) w  
ith payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 256  
Jan 01 21:42:13 [IKEv1]: IP = 172.16.1.3, IKE\_DECODE RECEIVED Message (msgid=0)  
with payloads : HDR + ID (5) + HASH (8) + NOTIFY (11) + NONE (0) total length : 88  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
processing ID payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
processing hash payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
Computing hash for ISAKMP  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
processing notify payload  
Jan 01 21:42:13 [IKEv1]: IP = 172.16.1.3, Connection landed on tunnel\_group  
DefaultL2LGroup  
Jan 01 21:42:13 [IKEv1]: Group = DefaultL2LGroup, IP = 172.16.1.3, Freeing  
previously allocated memory for authorization-dn-attributes  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
constructing ID payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
constructing hash payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
Computing hash for ISAKMP  
Jan 01 21:42:13 [IKEv1 DEBUG]: IP = 172.16.1.3, Constructing IOS keep alive  
payload: proposal=32767/32767 sec.  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
constructing dpd vid payload  
Jan 01 21:42:13 [IKEv1]: IP = 172.16.1.3, IKE\_DECODE SENDING Message (msgid=0)  
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +  
NONE (0) total length : 92

Jan 01 21:42:13 [IKEv1]: Group = DefaultL2LGroup, IP = 172.16.1.3, **PHASE 1 COMPLETED**  
Jan 01 21:42:13 [IKEv1]: IP = 172.16.1.3, Keep-alive type for this connection: DPD  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3, Starting  
P1 rekey timer: 82080 seconds.  
Jan 01 21:42:13 [IKEv1]: IP = 172.16.1.3, IKE\_DECODE RECEIVED Message (msgid=4bc  
07a70) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +  
NONE (0) total length : 164  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
processing hash payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
processing SA payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
processing nonce payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
processing ID payload  
Jan 01 21:42:13 [IKEv1]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
Received remote IP Proxy Subnet data in ID Payload:  
Address 10.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
processing ID payload  
Jan 01 21:42:13 [IKEv1]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
Received local IP Proxy Subnet data in ID Payload:  
Address 10.2.2.0, Mask 255.255.255.0, Protocol 0, Port 0  
Jan 01 21:42:13 [IKEv1]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
QM IsRekeyedold sa not found by addr  
Jan 01 21:42:13 [IKEv1]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
IKE Remote Peer configured for crypto map: cisco  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
processing IPsec SA payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3, IPsec S  
A Proposal # 1, Transform # 1 acceptable Matches global IPsec SA entry # 1  
Jan 01 21:42:13 [IKEv1]: Group = DefaultL2LGroup, IP = 172.16.1.3, IKE:  
requesting SPI!  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
IKE got SPI from key engine: SPI = 0xc3fe4fb0  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
oakleyconstructing quick mode  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
constructing blank hash payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
constructing IPsec SA payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
constructing IPsec nonce payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
constructing proxy ID  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
Transmitting Proxy Id:  
    **Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0**  
    **Local subnet: 10.2.2.0 mask 255.255.255.0 Protocol 0 Port 0**  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
constructing qm hash payload  
Jan 01 21:42:13 [IKEv1]: IP = 172.16.1.3, IKE\_DECODE SENDING Message (msgid=4bc0  
7a70) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + N  
ONE (0) total length : 164  
Jan 01 21:42:13 [IKEv1]: IP = 172.16.1.3, IKE\_DECODE RECEIVED Message (msgid=4bc  
07a70) with payloads : HDR + HASH (8) + NONE (0) total length : 48  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
processing hash payload  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
loading all IPSEC SAs  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
Generating Quick Mode Key!  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
Generating Quick Mode Key!

Jan 01 21:42:13 [IKEv1]: Group = DefaultL2LGroup, IP = 172.16.1.3, Security nego-  
tiation complete for LAN-to-LAN Group (DefaultL2LGroup) Responder,  
Inbound SPI= 0xc3fe4fb0, Outbound SPI = 0x9acle72c  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
IKE got a KEY\_ADD msg for SA: SPI = 0x9acle72c  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
Pitcher: received KEY\_UPDATE, spi 0xc3fe4fb0  
Jan 01 21:42:13 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.16.1.3,  
Starting P2 rekey timer: 3420 seconds.  
Jan 01 21:42:13 [IKEv1]: Group = DefaultL2LGroup, IP = 172.16.1.3, **PHASE 2 COMPL-  
ETED** (msgid=4bc07a70)

pixfirewall#**debug crypto ipsec 7**

pixfirewall# IPSEC: New embryonic SA created @ 0x028B6EE0,

SCB: 0x028B6E50,  
Direction: inbound  
SPI : 0x97550AC8  
Session ID: 0x00000009  
VPIF num : 0x00000001  
Tunnel type: l2l  
Protocol : esp  
Lifetime : 240 seconds

IPSEC: New embryonic SA created @ 0x028B75E8,

SCB: 0x028B7528,  
Direction: outbound  
SPI : 0xB857E226  
Session ID: 0x00000009  
VPIF num : 0x00000001  
Tunnel type: l2l  
Protocol : esp  
Lifetime : 240 seconds

IPSEC: Completed host OBSA update, SPI 0xB857E226

IPSEC: Creating outbound VPN context, SPI 0xB857E226

Flags: 0x00000005  
SA : 0x028B75E8  
SPI : 0xB857E226  
MTU : 1500 bytes  
VCID : 0x00000000  
Peer : 0x00000000  
SCB : 0x028B7528  
Channel: 0x01693F28

IPSEC: Completed outbound VPN context, SPI 0xB857E226

VPN handle: 0x0002524C

IPSEC: New outbound encrypt rule, SPI 0xB857E226

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 0xB857E226

Rule ID: 0x028A9988

IPSEC: New outbound permit rule, SPI 0xB857E226

```
Src addr: 192.168.1.2
Src mask: 255.255.255.255
Dst addr: 172.16.1.3
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: 0xB857E226
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xB857E226
  Rule ID: 0x028B5D90
IPSEC: Completed host IBSA update, SPI 0x97550AC8
IPSEC: Creating inbound VPN context, SPI 0x97550AC8
  Flags: 0x00000006
  SA   : 0x028B6EE0
  SPI  : 0x97550AC8
  MTU  : 0 bytes
  VCID : 0x00000000
  Peer : 0x0002524C
  SCB  : 0x028B6E50
  Channel: 0x01693F28
IPSEC: Completed inbound VPN context, SPI 0x97550AC8
  VPN handle: 0x0002B344
IPSEC: Updating outbound VPN context 0x0002524C, SPI 0xB857E226
  Flags: 0x00000005
  SA   : 0x028B75E8
  SPI  : 0xB857E226
  MTU  : 1500 bytes
  VCID : 0x00000000
  Peer : 0x0002B344
  SCB  : 0x028B7528
  Channel: 0x01693F28
IPSEC: Completed outbound VPN context, SPI 0xB857E226
  VPN handle: 0x0002524C
IPSEC: Completed outbound inner rule, SPI 0xB857E226
  Rule ID: 0x028A9988
IPSEC: Completed outbound outer SPD rule, SPI 0xB857E226
  Rule ID: 0x028B5D90
IPSEC: New inbound tunnel flow rule, SPI 0x97550AC8
  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 0x97550AC8
  Rule ID: 0x027FF7F8
```

```

IPSEC: New inbound decrypt rule, SPI 0x97550AC8
  Src addr: 172.16.1.3
  Src mask: 255.255.255.255
  Dst addr: 192.168.1.2
  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: 0x97550AC8
  Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x97550AC8
  Rule ID: 0x028BB318
IPSEC: New inbound permit rule, SPI 0x97550AC8
  Src addr: 172.16.1.3
  Src mask: 255.255.255.255
  Dst addr: 192.168.1.2
  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: 0x97550AC8
  Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x97550AC8
  Rule ID: 0x028A7460

```

## 远程IOS路由器-调试输出

```

Router#debug crypto isakmp
*Dec 31 01:18:51.830: ISAKMP: received ke message (1/1)
*Dec 31 01:18:51.830: ISAKMP:(0:0:N/A:0): SA request profile is (NULL)
*Dec 31 01:18:51.830: ISAKMP: Created a peer struct for 192.168.1.2, peer port 500
*Dec 31 01:18:51.830: ISAKMP: New peer created peer = 0x64DC2CB4 peer_handle = 0
x80000022
*Dec 31 01:18:51.834: ISAKMP: Locking peer struct 0x64DC2CB4, IKE refcount 1 for
  isakmp_initiator
*Dec 31 01:18:51.834: ISAKMP: local port 500, remote port 500
*Dec 31 01:18:51.834: ISAKMP: set new node 0 to QM_IDLE
*Dec 31 01:18:51.834: insert sa successfully sa = 640D2660
*Dec 31 01:18:51.834: ISAKMP:(0:0:N/A:0):Can not start Aggressive mode,
trying Main mode.
*Dec 31 01:18:51.834: ISAKMP:(0:0:N/A:0):found peer pre-shared key
matching 192.168.1.2
*Dec 31 01:18:51.838: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-07 ID
*Dec 31 01:18:51.838: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-03 ID
*Dec 31 01:18:51.838: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-02 ID
*Dec 31 01:18:51.838: ISAKMP:(0:0:N/A:0):Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_MM
*Dec 31 01:18:51.838: ISAKMP:(0:0:N/A:0):Old State = IKE_READY New State = IKE_I_MM1
*Dec 31 01:18:51.838: ISAKMP:(0:0:N/A:0): beginning Main Mode exchange

```

\*Dec 31 01:18:51.842: ISAKMP:(0:0:N/A:0): sending packet to 192.168.1.2 my\_port 500 peer\_port 500 (I) MM\_NO\_STATE  
\*Dec 31 01:18:51.846: ISAKMP (0:0): received packet from 192.168.1.2 dport 500 sport 500 Global (I) MM\_NO\_STATE  
\*Dec 31 01:18:51.850: ISAKMP:(0:0:N/A:0):Input = IKE\_MESG\_FROM\_PEER, IKE\_MM\_EXCH  
\*Dec 31 01:18:51.850: ISAKMP:(0:0:N/A:0):Old State = IKE\_I\_MM1 New State = IKE\_I\_MM2  
  
\*Dec 31 01:18:51.850: ISAKMP:(0:0:N/A:0): processing SA payload. message ID = 0  
\*Dec 31 01:18:51.850: ISAKMP:(0:0:N/A:0): processing vendor id payload  
\*Dec 31 01:18:51.850: ISAKMP:(0:0:N/A:0): vendor ID seems Unity/DPD but major 194 mismatch  
\*Dec 31 01:18:51.850: ISAKMP:(0:0:N/A:0):**found peer pre-shared key matching 192.168.1.2**  
\*Dec 31 01:18:51.854: ISAKMP:(0:0:N/A:0): local preshared key found  
\*Dec 31 01:18:51.854: ISAKMP : Scanning profiles for xauth ...  
\*Dec 31 01:18:51.854: ISAKMP:(0:0:N/A:0):Checking ISAKMP transform 1 against priority 1 policy  
\*Dec 31 01:18:51.854: ISAKMP: encryption 3DES-CBC  
\*Dec 31 01:18:51.854: ISAKMP: hash MD5  
\*Dec 31 01:18:51.854: ISAKMP: default group 2  
\*Dec 31 01:18:51.854: ISAKMP: auth pre-share  
\*Dec 31 01:18:51.854: ISAKMP: life type in seconds  
\*Dec 31 01:18:51.854: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80  
\*Dec 31 01:18:51.858: ISAKMP:(0:0:N/A:0):atts are acceptable. Next payload is 0  
\*Dec 31 01:18:51.998: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Dec 31 01:18:51.998: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD but major 194 mismatch  
\*Dec 31 01:18:51.998: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL, IKE\_PROCESS\_MAIN\_MODE  
\*Dec 31 01:18:51.998: ISAKMP:(0:1:SW:1):Old State = IKE\_I\_MM2 New State = IKE\_I\_MM2  
\*Dec 31 01:18:52.002: ISAKMP:(0:1:SW:1): sending packet to 192.168.1.2 my\_port 500 peer\_port 500 (I) MM\_SA\_SETUP  
\*Dec 31 01:18:52.006: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL, **IKE\_PROCESS\_COMPLETE**  
\*Dec 31 01:18:52.006: ISAKMP:(0:1:SW:1):Old State = IKE\_I\_MM2 New State = IKE\_I\_MM3  
\*Dec 31 01:18:52.066: ISAKMP (0:134217729): received packet from 192.168.1.2 dport 500 sport 500 Global (I) MM\_SA\_SETUP  
\*Dec 31 01:18:52.066: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_FROM\_PEER, IKE\_MM\_EXCH  
\*Dec 31 01:18:52.066: ISAKMP:(0:1:SW:1):Old State = IKE\_I\_MM3 New State = IKE\_I\_MM4  
\*Dec 31 01:18:52.070: ISAKMP:(0:1:SW:1): processing KE payload. message ID = 0  
\*Dec 31 01:18:52.246: ISAKMP:(0:1:SW:1): processing NONCE payload. message ID =0  
\*Dec 31 01:18:52.246: ISAKMP:(0:1:SW:1):found peer pre-shared key matching 192.168.1.2  
\*Dec 31 01:18:52.250: ISAKMP:(0:1:SW:1):SKEYID state generated  
\*Dec 31 01:18:52.250: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Dec 31 01:18:52.250: ISAKMP:(0:1:SW:1): vendor ID is Unity  
\*Dec 31 01:18:52.250: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Dec 31 01:18:52.250: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD but major 227 mismatch  
\*Dec 31 01:18:52.250: ISAKMP:(0:1:SW:1): vendor ID is XAUTH  
\*Dec 31 01:18:52.250: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Dec 31 01:18:52.254: ISAKMP:(0:1:SW:1): speaking to another IOS box!  
\*Dec 31 01:18:52.254: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Dec 31 01:18:52.254: ISAKMP:(0:1:SW:1):vendor ID seems Unity/DPD but hash mismatch  
\*Dec 31 01:18:52.254: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL, IKE\_PROCESS\_MAIN\_MODE  
\*Dec 31 01:18:52.254: ISAKMP:(0:1:SW:1):Old State = IKE\_I\_MM4 New State = IKE\_I\_MM4  
\*Dec 31 01:18:52.262: ISAKMP:(0:1:SW:1):Send initial contact  
\*Dec 31 01:18:52.262: ISAKMP:(0:1:SW:1):**SA is doing pre-shared key authentication using id type ID\_IPV4\_ADDR**  
\*Dec 31 01:18:52.266: ISAKMP (0:134217729): ID payload  
    next-payload : 8  
    type : 1  
    address : 172.16.1.3  
    protocol : 17



```
port          : 500
length        : 12
*Dec 31 01:18:52.266: ISAKMP:(0:1:SW:1):Total payload length: 12
*Dec 31 01:18:52.266: ISAKMP:(0:1:SW:1): sending packet to 192.168.1.2 my_port 5
00 peer_port 500 (I) MM_KEY_EXCH
*Dec 31 01:18:52.270: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Dec 31 01:18:52.270: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM4 New State = IKE_I_MM5
*Dec 31 01:18:52.342: ISAKMP (0:134217729): received packet from 192.168.1.2 dpo
rt 500 sport 500 Global (I) MM_KEY_EXCH
*Dec 31 01:18:52.342: ISAKMP:(0:1:SW:1): processing ID payload. message ID = 0
*Dec 31 01:18:52.342: ISAKMP (0:134217729): ID payload
next-payload : 8
type          : 1
address       : 192.168.1.2
protocol      : 17
port         : 500
length       : 12
*Dec 31 01:18:52.342: ISAKMP:(0:1:SW:1):: peer matches *none* of the profiles
*Dec 31 01:18:52.346: ISAKMP:(0:1:SW:1): processing HASH payload. message ID = 0
*Dec 31 01:18:52.346: ISAKMP:received payload type 17
*Dec 31 01:18:52.346: ISAKMP:(0:1:SW:1): processing vendor id payload
*Dec 31 01:18:52.346: ISAKMP:(0:1:SW:1): vendor ID is DPD
*Dec 31 01:18:52.346: ISAKMP:(0:1:SW:1):SA authentication status: authenticated
*Dec 31 01:18:52.346: ISAKMP:(0:1:SW:1):SA has been authenticated with 192.168.1.2
*Dec 31 01:18:52.346: ISAKMP: Trying to insert a peer 172.16.1.3/192.168.1.2/500
/, and inserted successfully 64DC2CB4.
*Dec 31 01:18:52.346: ISAKMP:(0:1:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Dec 31 01:18:52.350: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM5 New State =
IKE_I_MM6
*Dec 31 01:18:52.350: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Dec 31 01:18:52.350: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM6 New State = IKE_I_MM6
*Dec 31 01:18:52.354: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Dec 31 01:18:52.354: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM6 New State =
IKE_P1_COMPLETE
*Dec 31 01:18:52.358: ISAKMP:(0:1:SW:1):beginning Quick Mode exchange, M-ID
of 1270905456
*Dec 31 01:18:52.362: ISAKMP:(0:1:SW:1): sending packet to 192.168.1.2 my_port 5
00 peer_port 500 (I) QM_IDLE
*Dec 31 01:18:52.362: ISAKMP:(0:1:SW:1):Node 1270905456, Input =
IKE_MESG_INTERNAL, IKE_INIT_QM
*Dec 31 01:18:52.362: ISAKMP:(0:1:SW:1):Old State = IKE_QM_READY
New State = IKE_QM_I_QM1
*Dec 31 01:18:52.362: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
*Dec 31 01:18:52.366: ISAKMP:(0:1:SW:1):Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE

*Dec 31 01:18:52.374: ISAKMP (0:134217729): received packet from 192.168.1.2 dpo
rt 500 sport 500 Global (I) QM_IDLE
*Dec 31 01:18:52.378: ISAKMP:(0:1:SW:1): processing HASH payload.
message ID = 1270905456
*Dec 31 01:18:52.378: ISAKMP:(0:1:SW:1): processing SA payload.
message ID = 1270905456
*Dec 31 01:18:52.378: ISAKMP:(0:1:SW:1):Checking IPsec proposal 1
*Dec 31 01:18:52.378: ISAKMP: transform 1, ESP_3DES
*Dec 31 01:18:52.378: ISAKMP: attributes in transform:
*Dec 31 01:18:52.378: ISAKMP: SA life type in seconds
*Dec 31 01:18:52.378: ISAKMP: SA life duration (basic) of 3600
*Dec 31 01:18:52.378: ISAKMP: SA life type in kilobytes
*Dec 31 01:18:52.378: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Dec 31 01:18:52.378: ISAKMP: encaps is 1 (Tunnel)
*Dec 31 01:18:52.382: ISAKMP: authenticator is HMAC-MD5
```

\*Dec 31 01:18:52.382: ISAKMP:(0:1:SW:1):atts are acceptable.  
\*Dec 31 01:18:52.382: ISAKMP:(0:1:SW:1): processing NONCE payload.  
message ID =1270905456  
\*Dec 31 01:18:52.382: ISAKMP:(0:1:SW:1): processing ID payload.  
message ID = 1270905456  
\*Dec 31 01:18:52.382: ISAKMP:(0:1:SW:1): processing ID payload.  
message ID = 1270905456  
\*Dec 31 01:18:52.386: ISAKMP: Locking peer struct 0x64DC2CB4,  
IPSEC refcount 1 for for stuff\_ke  
\*Dec 31 01:18:52.390: ISAKMP:(0:1:SW:1): Creating IPsec SAs  
\*Dec 31 01:18:52.390: inbound SA from 192.168.1.2 to 172.16.1.3 (f/i) 0  
/ 0  
(proxy 10.2.2.0 to 10.1.1.0)  
\*Dec 31 01:18:52.390: has spi 0x9AC1E72C and conn\_id 0 and flags 2  
\*Dec 31 01:18:52.390: lifetime of 3600 seconds  
\*Dec 31 01:18:52.390: lifetime of 4608000 kilobytes  
\*Dec 31 01:18:52.390: has client flags 0x0  
\*Dec 31 01:18:52.390: outbound SA from 172.16.1.3 to 192.168.1.2 (f/i) 0  
/0  
(proxy 10.1.1.0 to 10.2.2.0)  
\*Dec 31 01:18:52.394: has spi -1006743632 and conn\_id 0 and flags A  
\*Dec 31 01:18:52.394: lifetime of 3600 seconds  
\*Dec 31 01:18:52.394: lifetime of 4608000 kilobytes  
\*Dec 31 01:18:52.394: has client flags 0x0  
\*Dec 31 01:18:52.394: ISAKMP:(0:1:SW:1): sending packet to 192.168.1.2 my\_port 5  
00 peer\_port 500 (I) QM\_IDLE  
\*Dec 31 01:18:52.398: ISAKMP:(0:1:SW:1):deleting node 1270905456 error  
FALSE reason "No Error"  
\*Dec 31 01:18:52.398: ISAKMP:(0:1:SW:1):Node 1270905456, Input =  
IKE\_MSG\_FROM\_PEER, IKE\_QM\_EXCH  
\*Dec 31 01:18:52.398: ISAKMP:(0:1:SW:1):Old State = IKE\_QM\_I\_QM1  
New State = IKE\_QM\_PHASE2\_COMPLETE  
\*Dec 31 01:18:52.402: ISAKMP: Locking peer struct 0x64DC2CB4, IPSEC  
refcount 2 for from create\_transforms  
\*Dec 31 01:18:52.402: ISAKMP: Unlocking IPSEC struct 0x64DC2CB4 from  
create\_transforms, count 1  
\*Dec 31 01:19:06.130: ISAKMP (0:134217729): received packet from 192.168.1.2 dpo  
rt 500 sport 500 Global (I) QM\_IDLE  
\*Dec 31 01:19:06.130: ISAKMP: set new node 372376968 to QM\_IDLE  
\*Dec 31 01:19:06.130: ISAKMP:(0:1:SW:1): processing HASH payload.  
message ID = 372376968  
\*Dec 31 01:19:06.134: ISAKMP:(0:1:SW:1): processing NOTIFY DPD/R\_U\_THERE protocol 1  
spi 0, message ID = 372376968, sa = 640D2660  
\*Dec 31 01:19:06.134: ISAKMP:(0:1:SW:1):deleting node 372376968 error  
FALSE reason "Informational (in) state 1"  
\*Dec 31 01:19:06.134: ISAKMP:(0:1:SW:1):Input = IKE\_MSG\_FROM\_PEER,  
IKE\_INFO\_NOTIFY  
\*Dec 31 01:19:06.134: ISAKMP:(0:1:SW:1):Old State = IKE\_P1\_COMPLETE  
New State = IKE\_P1\_COMPLETE  
  
\*Dec 31 01:19:06.134: ISAKMP:(0:1:SW:1):DPD/R\_U\_THERE received from  
peer 192.168.1.2, sequence 0x7E805468  
\*Dec 31 01:19:06.138: ISAKMP: set new node 2096423279 to QM\_IDLE  
\*Dec 31 01:19:06.138: ISAKMP:(0:1:SW:1):Sending NOTIFY DPD/R\_U\_THERE\_ACK protocol 1  
spi 1689358936, message ID = 2096423279  
\*Dec 31 01:19:06.138: ISAKMP:(0:1:SW:1): seq. no 0x7E805468  
\*Dec 31 01:19:06.138: ISAKMP:(0:1:SW:1): sending packet to 192.168.1.2 my\_port 5  
00 peer\_port 500 (I) QM\_IDLE  
\*Dec 31 01:19:06.142: ISAKMP:(0:1:SW:1):purging node 2096423279  
\*Dec 31 01:19:06.142: ISAKMP:(0:1:SW:1):Input = IKE\_MSG\_FROM\_PEER,  
**IKE\_MSG\_KEEP\_ALIVE**  
\*Dec 31 01:19:06.142: ISAKMP:(0:1:SW:1):Old State = IKE\_P1\_COMPLETE  
New State = IKE\_P1\_COMPLETE

Router#**debug crypto ipsec**

```
*Dec 31 01:29:05.402: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 172.16.1.3, remote= 192.168.1.2,
  local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0xB857E226(3092767270), conn_id= 0, keysize= 0, flags= 0x400A
*Dec 31 01:29:05.774: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 172.16.1.3, remote= 192.168.1.2,
  local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel),
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Dec 31 01:29:05.778: Crypto mapdb : proxy_match
  src addr      : 10.1.1.0
  dst addr      : 10.2.2.0
  protocol      : 0
  src port      : 0
  dst port      : 0
*Dec 31 01:29:05.782: IPSEC(key_engine): got a queue event with 2 kei messages
*Dec 31 01:29:05.782: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 172.16.1.3, remote= 192.168.1.2,
  local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0xB857E226(3092767270), conn_id= 0, keysize= 0, flags= 0x2
*Dec 31 01:29:05.786: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 172.16.1.3, remote= 192.168.1.2,
  local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0x97550AC8(2538932936), conn_id= 0, keysize= 0, flags= 0xA
*Dec 31 01:29:05.786: Crypto mapdb : proxy_match
  src addr      : 10.1.1.0
  dst addr      : 10.2.2.0
  protocol      : 0
  src port      : 0
  dst port      : 0
*Dec 31 01:29:05.786: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with
the same proxies and 192.168.1.2
*Dec 31 01:29:05.786: IPsec: Flow_switching Allocated flow for sibling 80000006
*Dec 31 01:29:05.786: IPSEC(policy_db_add_ident): src 10.1.1.0, dest 10.2.2.0, d
est_port 0
*Dec 31 01:29:05.790: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.1.3, sa_proto= 50,
  sa_spi= 0xB857E226(3092767270),
  sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
*Dec 31 01:29:05.790: IPSEC(create_sa): sa created,
  (sa) sa_dest= 192.168.1.2, sa_proto= 50,
  sa_spi= 0x97550AC8(2538932936),
  sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
```

## Related Information

- [Cisco ASA 5500-X系列下一代防火墙](#)
- [Cisco ASA命令参考](#)
- [IPsec 协商/IKE 协议支持页](#)
- [请求注解 \(RFC\)](#)
- [Technical Support & Documentation - Cisco Systems](#)