

ASA VPN配置示例与重叠方案的

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[背景信息](#)

[在两个VPN终端的转换](#)

[ASA1](#)

[创建子网的必要的对象在使用中](#)

[配置NAT语句](#)

[用被转换的子网配置加密ACL](#)

[相关加密配置](#)

[ASA2](#)

[创建子网的必要的对象在使用中](#)

[配置NAT语句](#)

[用被转换的子网配置加密ACL](#)

[相关加密配置](#)

[Verify](#)

[ASA1](#)

[ASA2](#)

[有重叠Spoke的星型网拓扑](#)

[ASA1](#)

[创建子网的必要的对象在使用中](#)

[创建手工的语句转换：](#)

[用被转换的子网配置加密ACL](#)

[相关加密配置](#)

[ASA2 \(分支1\)](#)

[配置去被转换的子网\(10.20.20.0 /24\)的加密ACL](#)

[相关加密配置](#)

[R1 \(分支2\)](#)

[配置去被转换的子网\(10.30.30.0 /24\)的加密ACL](#)

[相关加密配置](#)

[Verify](#)

[ASA1](#)

[ASA2 \(分支1\)](#)

[R1 \(分支2\)](#)

[Troubleshoot](#)

[清除安全关联](#)

[查看NAT配置](#)

[故障排除命令](#)

[Related Information](#)

Introduction

在LAN对LAN的本文描述用于的步骤转换VPN流量(L2L) IPsec隧道移动在两可适应的安全工具(ASA)之间在重叠方案并且端口地址转换(PAT)互联网数据流。

Prerequisites

Requirements

在您继续进行此配置示例前，请保证您用在接口的IP地址配置Cisco可适应的安全工具，并且有基本连通性。

Components Used

本文的信息根据此软件版本：

- Cisco可适应的安全工具软件版本8.3和以上。

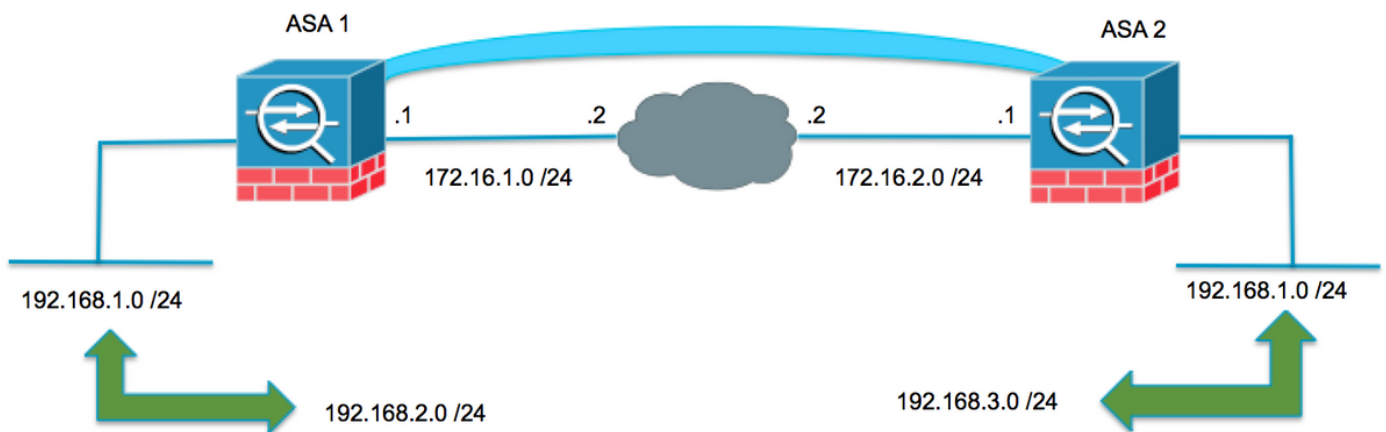
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

背景信息

每个设备有在它后的一个专用，受保护的子网。在重叠方案中，在VPN间的通信从未发生，因为信息包从未离开本地子网，因为数据流被发送到相同子网的IP地址。这可以用网络地址转换(NAT)完成按照以下部分说明。

在两个VPN终端的转换

当VPN受保护的子网交迭，并且时配置在两个终端可以被修改；当去遥控转换了子网时，NAT可以用于转换本地网络为一个不同的子网。



ASA1

创建子网的必要的对象在使用中

```
object network LOCAL
 subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
 subnet 192.168.2.0 255.255.255.0
object network XLATED-REMOTE
 subnet 192.168.3.0 255.255.255.0
```

配置NAT语句

创建手工的语句转换本地网络为不同的子网，只有当去远程子网时(也被转换)

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

用被转换的子网配置加密ACL

```
access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE Rel
```

相关加密配置

```
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
 ikev1 pre-shared-key secure_PSK
```

ASA2

创建子网的必要的对象在使用中

```
object network LOCAL
 subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
 subnet 192.168.3.0 255.255.255.0
object network XLATED-REMOTE
 subnet 192.168.2.0 255.255.255.0
```

配置NAT语句

创建手工的语句转换本地网络为不同的子网，只有当去远程子网时(也被转换)

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

用被转换的子网配置加密ACL

```
access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE Rel
```

相关加密配置

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
```

```
crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside
```

```
tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

Verify

Use this section to confirm that your configuration works properly.

ASA1

```
ASA1(config)# sh cry isa sa
```

```
IKEv1 SAs:
```

```
  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: 172.16.2.1
   Type    : L2L           Role    : initiator
   Rekey   : no           State   : MM_ACTIVE
```

```
There are no IKEv2 SAs
```

```
ASA1(config)# show crypto ipsec sa
interface: outside
```

```
  Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1

  access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 192.168.3.0
255.255.255.0
  local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer: 172.16.2.1
```

```
#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: F90C149A
current inbound spi : 6CE656C7
```

inbound esp sas:

```
spi: 0x6CE656C7 (1827034823)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 16384, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/28768)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000003FF
```

outbound esp sas:

```
spi: 0xF90C149A (4178318490)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 16384, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/28768)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

ASA2

```
ASA2(config)# show crypto isa sa
```

IKEv1 SAs:

```
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
```

There are no IKEv2 SAs

```
ASA2(config)# show crypto ipsec sa
```

interface: outside

```
Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1
```

```
access-list VPN-TRAFFIC extended permit ip 192.168.3.0 255.255.255.0 192.168.2.0
```

255.255.255.0

```
local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer: 172.16.1.1
```

```
#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 6CE656C7
current inbound spi : F90C149A
```

inbound esp sas:

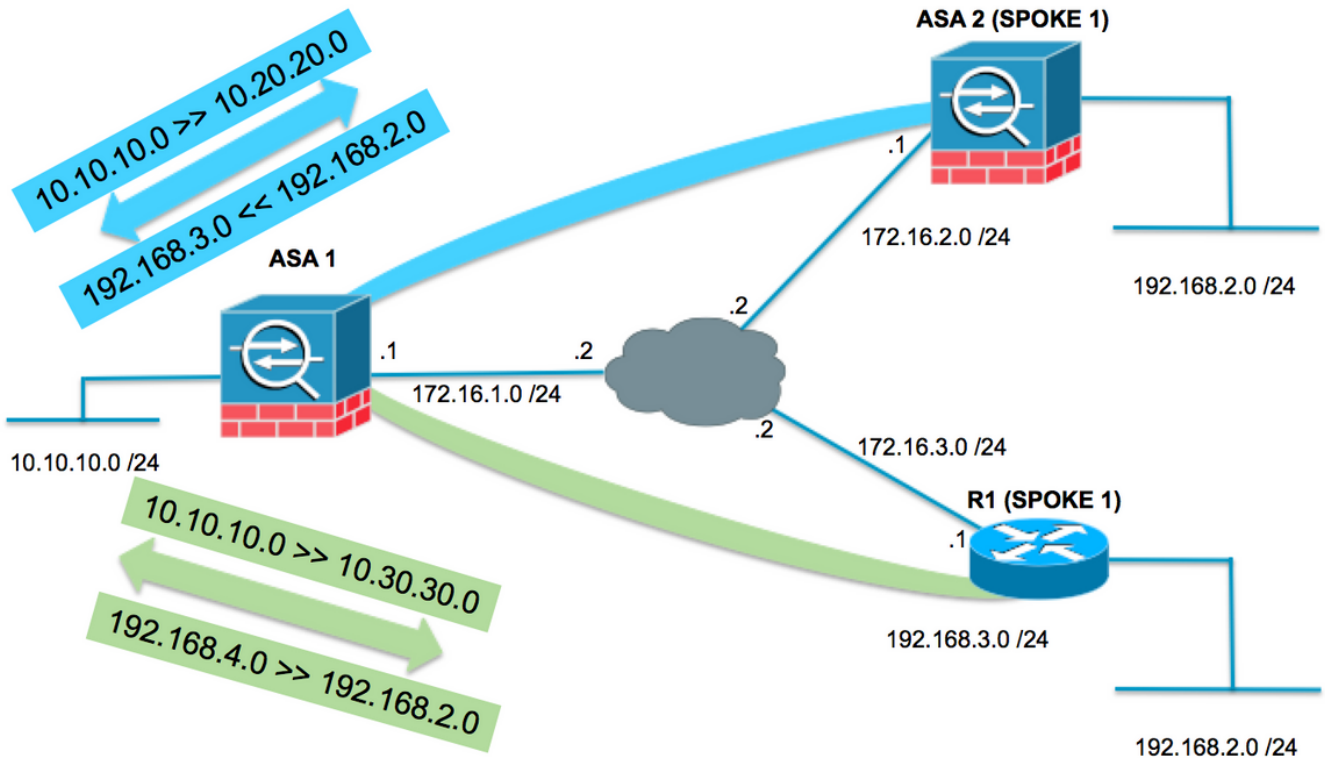
```
spi: 0xF90C149A (4178318490)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28684)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000003FF
```

outbound esp sas:

```
spi: 0x6CE656C7 (1827034823)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28683)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

有重叠Spoke的星型网拓扑

在following的拓扑里，两个spoke有需要在往集线器的IPSec隧道保护的相同子网。要实现在spoke的管理NAT配置到解决方法重叠问题在仅集线器被执行。



ASA1

创建子网的必要的对象在使用中

```
object network LOCAL
  subnet 10.10.10.0 255.255.255.0
object network SPOKES-NETWORK
  subnet 192.168.2.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE1
  subnet 10.20.20.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE2
  subnet 10.30.30.0 255.255.255.0
object network REMOTE-XLATE-SPOKE1
  subnet 192.168.3.0 255.255.255.0
object network REMOTE-XLATE-SPOKE2
  subnet 192.168.4.0 255.255.255.0
```

创建手工的语句转换：

- 本地网络对10.20.20.0 /24的10.10.10.0 /24，当去分支1时(192.168.2.0 /24)。
- 分支1网络对192.168.3.0 /24的192.168.2.0 /24，当来到10.20.20.0 /24时。
- 本地网络对10.30.30.0 /24的10.10.10.0 /24，当去SPOKE3时(192.168.2.0 /24)。
- 分支2网络对192.168.4.0 /24的192.168.2.0 /24，当来到10.30.30.0 /24时。

```
nat (inside,outside) source static LOCAL LOCAL-XLATE-SPOKE1 destination static REMOTE-XLATE-SPOKE1 SPOKES-NETWORK
nat (inside,outside) source static LOCAL LOCAL-XLATE-SPOKE2 destination static REMOTE-XLATE-SPOKE2 SPOKES-NETWORK
```

用被转换的子网配置加密ACL

```
access-list VPN-to-SPOKE1 extended permit ip object LOCAL-XLATE-SPOKE1 object SPOKES-NETWORKS
access-list VPN-to-SPOKE2 extended permit ip object LOCAL-XLATE-SPOKE2 object SPOKES-NETWORKS
```

相关加密配置

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
```

```
crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-to-SPOKE1
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP 20 match address VPN-to-SPOKE2
crypto map MYMAP 20 set peer 172.16.3.1
crypto map MYMAP 20 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside
```

```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
tunnel-group 172.16.3.1 type ipsec-l2l
tunnel-group 172.16.3.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

ASA2 (分支1)

配置去被转换的子网(10.20.20.0 /24)的加密ACL

```
access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0 255.255.255.0
```

相关加密配置

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
```

```
crypto ipsec ikev1 transform-set esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside
```

```
tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

R1 (分支2)

配置去被转换的子网(10.30.30.0 /24)的加密ACL

```
ip access-list extended VPN-TRAFFIC
permit ip 192.168.2.0 0.0.0.255 10.30.30.0 0.0.0.255
```

相关加密配置

```
crypto isakmp policy 1
  encr aes 256
  authentication pre-share
  group 2

crypto isakmp key secure_PSK address 172.16.1.1

crypto ipsec transform-set AES256-SHA esp-aes 256 esp-sha-hmac
mode tunnel

crypto map MYMAP 10 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set AES256-SHA
  match address VPN-TRAFFIC

interface GigabitEthernet0/1
  ip address 172.16.3.1 255.255.255.0
  duplex auto
  speed auto
  media-type rj45
  crypto map MYMAP
```

Verify

ASA1

```
ASA1(config)# show crypto isakmp sa
```

```
IKEv1 SAs:
```

```
Active SA: 2
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2
```

```
1  IKE Peer: 172.16.3.1
   Type      : L2L                Role      : responder
   Rekey     : no                 State     : MM_ACTIVE
2  IKE Peer: 172.16.2.1
   Type      : L2L                Role      : responder
   Rekey     : no                 State     : MM_ACTIVE
```

```
There are no IKEv2 SAs
```

```
ASA1(config)# show crypto ipsec sa
```

```
interface: outside
  Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1

    access-list VPN-to-SPOKE1 extended permit ip 10.20.20.0 255.255.255.0 192.168.2.0
    255.255.255.0
    local ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
```

current_peer: 172.16.2.1

#pkts encaps: 10, #pkts encrypt: 9, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 9, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 79384296
current inbound spi : 2189BF7A

inbound esp sas:

spi: 0x2189BF7A (562675578)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/28618)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000003FF

outbound esp sas:

spi: 0x79384296 (2033730198)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/28618)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

Crypto map tag: MYMAP, seq num: 20, local addr: 172.16.1.1

access-list VPN-to-SPOKE2 extended permit ip 10.30.30.0 255.255.255.0 192.168.2.0
255.255.255.0

local ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer: 172.16.3.1

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#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
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.3.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled

```
current outbound spi: 65FDF4F5
current inbound spi : 05B7155D
```

```
inbound esp sas:
```

```
spi: 0x05B7155D (95884637)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/2883)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F
```

```
outbound esp sas:
```

```
spi: 0x65FDF4F5 (1711142133)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/2883)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

ASA2 (分支1)

```
ASA2(config)# show crypto isakmp sa
```

```
IKEv1 SAs:
```

```
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      : initiator
Rekey     : no           State     : MM_ACTIVE
```

```
There are no IKEv2 SAs
```

```
ASA2(config)# show crypto ipsec sa
```

```
interface: outside
```

```
Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1
```

```
access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0
255.255.255.0
```

```
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
```

```
current_peer: 172.16.1.1
```

```
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
```

```
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
```

```
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

```
#TFC rcvd: 0, #TFC sent: 0
```

```
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```

```
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
```

```
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 2189BF7A
current inbound spi : 79384296
```

inbound esp sas:

```
spi: 0x79384296 (2033730198)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28494)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000003FF
```

outbound esp sas:

```
spi: 0x2189BF7A (562675578)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28494)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

R1 (分支2)

R3lshow crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
172.16.1.1	172.16.3.1	QM_IDLE	1001	ACTIVE

IPv6 Crypto ISAKMP SA

R1#show crypto ipsec sa

interface: GigabitEthernet0/1

Crypto map tag: MYMAP, local addr 172.16.3.1

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)

current_peer 172.16.1.1 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

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

#send errors 0, #recv errors 0

local crypto endpt.: 172.16.3.1, remote crypto endpt.: 172.16.1.1

plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1

current outbound spi: 0x5B7155D(95884637)

PFS (Y/N): N, DH group: none

inbound esp sas:

```
spi: 0x65FDF4F5(1711142133)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
```

```
conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map: MYMAP
sa timing: remaining key lifetime (k/sec): (4188495/2652)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0x5B7155D(95884637)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map: MYMAP
sa timing: remaining key lifetime (k/sec): (4188495/2652)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(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。

清除安全关联

当您排除故障时，请务必清除现有的SAS，在您做一个变动后。在 PIX 的特权模式下，使用以下命令：

- `clear crypto ipsec sa` -删除活动IPSec SAS。
- `clear crypto isakmp sa` -删除活动IKE SAS。

复核NAT配置

- `show nat`详细资料-显示与膨胀的对象/对象组的NAT配置

故障排除命令

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。

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](#)。

- `debug crypto ipsec` -显示第2阶段的IPsec协商。
- `debug crypto isakmp` -显示阶段1的ISAKMP协商。

Related Information

- [NAT配置指南](#)
- [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](#)
- [Technical Support & Documentation - Cisco Systems](#)