ASA/PIX 7.x及更高版本：LAN到LAN和EasyVPN IPsec隧道在同一介面上終止的配置示例

目錄

簡介

本文檔提供了如何啟用HUB ASA以接受同一介面上的站點到站點隧道和Easy VPN IPsec連線的示例配置。Cisco ASA 5520和Cisco Adaptive Security Appliance(ASA)5505之間的IPsec使用帶網路擴展模式(NEM)的Easy VPN。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行7.x及更高版本（集線器）的ASA 5500系列**注意**：HUB ASA配置還可以與運行7.x及更高版本的PIX安全裝置515、515E、525和535一起使用
- 運行7.x及更高版本的Easy VPN ASA 5505
- 運行7.x及更高版本的PIX安全裝置515、515E、525和535

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

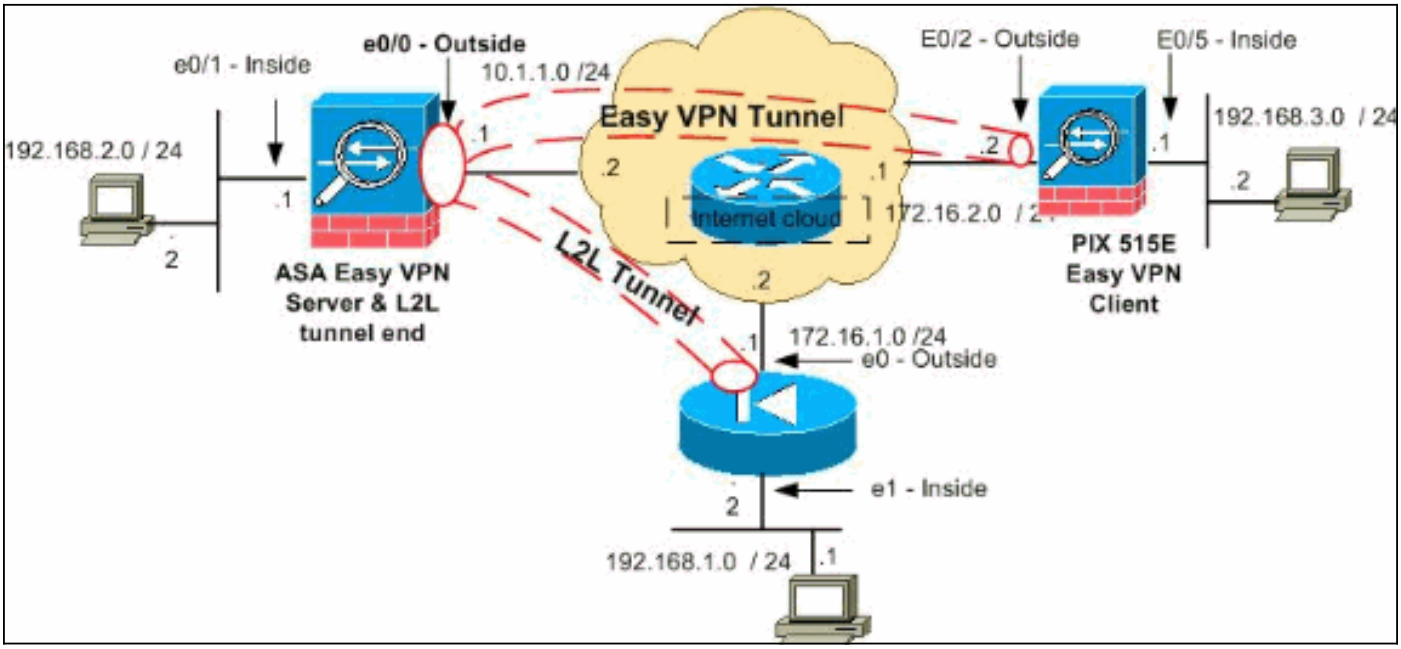
設定

本節提供可用於設定本檔案中所述功能的資訊。

註：使用 Command Lookup Tool(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是RFC 1918 ，在實驗室環境中使用。

組態

本檔案會使用以下設定：

- HUB ASA
- Easy VPN客戶端ASA 5505
- PIX

HUB ASA

```
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
```

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.2.1 255.255.255.0
!
!--- Output Suppressed. !--- Access-list for interesting
traffic (Site to Site) to be !--- encrypted between hub
ASA and spoke (PIX) networks. access-list
outside_cryptomap_20 extended permit ip 192.168.2.0
255.255.255.0 192.168.1.0 255.255.255.0 !--- Access-list
for interesting traffic to be !--- encrypted between hub
ASA and spoke easy vpn client ASA networks. access-list
ezvpn1 extended permit ip 192.168.2.0 255.255.255.0
192.168.3.0 255.255.255.0 !--- Access-list for traffic
to bypass the network address !--- translation (NAT)
process. access-list nonat extended permit ip
192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list nonat extended permit ip 192.168.2.0
255.255.255.0 192.168.3.0 255.255.255.0 !--- Output
Suppressed. !--- 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. nat-control global (outside) 1
interface nat (inside) 0 access-list nonat nat (inside)
1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 10.1.1.2
1 !--- Output Suppressed. !--- Configuration of IPsec
Phase 2 crypto ipsec transform-set myset esp-3des esp-
sha-hmac !--- IPsec configuration for the dynamic LAN-
to-LAN tunnel crypto dynamic-map ezvpn 30 set transform-
set myset !--- IPsec configuration for the static LAN-
to-LAN tunnel crypto map outside_map 20 match address
outside_cryptomap_20 crypto map outside_map 20 set peer
172.16.1.1 crypto map outside_map 20 set transform-set
myset !--- IPsec configuration that binds dynamic map to
crypto map crypto map outside_map 65535 ipsec-isakmp
dynamic ezvpn !--- Crypto map applied to the outside
interface of the ASA crypto map outside_map interface
outside isakmp enable outside !--- PHASE 1 CONFIGURATION
---! !--- This configuration uses isakmp policy 1. !---
These configuration commands !--- define the Phase 1
policies that are used. crypto isakmp policy 10
authentication pre-share encryption 3des hash sha group
2 lifetime 86400 !--- Output Suppressed. !--- This
defines the group policy you use with Easy VPN. !---
Specify the networks that can pass through !--- the
tunnel and that you want to !--- use network extension
mode. group-policy tunnel internal group-policy tunnel
attributes nem enable !--- The username and password
associated with !--- this VPN connection are defined
here. You !--- can also use AAA for this function.
username cisco password ffIRPGpDSOJh9YLq encrypted
tunnel-group 172.16.1.1 type ipsec-l2l tunnel-group
172.16.1.1 ipsec-attributes pre-shared-key * !--- The
tunnel-group commands bind the configurations !---
defined in this configuration to the tunnel that is !---
used for Easy VPN. This tunnel name is the one !---
specified on the remote side. tunnel-group mytunnel type
remote-access tunnel-group mytunnel general-attributes
default-group-policy tunnel !--- Defines the pre-shared
```

```
key used for !--- IKE authentication for the dynamic
tunnel. tunnel-group mytunnel ipsec-attributes pre-
shared-key * prompt hostname context
Cryptochecksum:e148bf43d04906f5db41fc6f90c52d34 : end
```

Easy VPN客戶端 — ASA 5505

```
ASA Version 7.2(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Vlan1
 nameif outside
 security-level 0
 ip address 172.16.2.2 255.255.255.0
!
interface Vlan2
 nameif inside
 security-level 100
 ip address 192.168.3.1 255.255.255.0
!
interface Ethernet0/0
!
interface Ethernet0/1
 shutdown
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
 switchport access vlan 2

!--- Output Suppressed. ! route outside 0.0.0.0 0.0.0.0
172.16.2.1 1 !--- Output Suppressed. !--- Easy VPN
Client Configuration ---! !--- Specify the IP address of
the VPN server. vpnclient server 10.1.1.1 !--- This
example uses network extension mode. vpnclient mode
network-extension-mode !--- Specify the group name and
the pre-shared key. vpnclient vpngroup mytunnel password
******** !--- Specify the authentication username and
password. vpnclient username cisco password ******** !--
- In order to enable the device as hardware vpnclient,
use this command. vpnclient enable ! !--- Output
Suppressed.
Cryptochecksum:0458ce7a08e6b7f9417b17bc254eb4e2 : end
```

PIX

```
PIX Version 8.0(2)
!
hostname pixfirewall
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
```

```
interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.1.2 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
!--- This access list (inside_nat0_outbound) is used
with the nat zero command. !--- This prevents traffic
which matches the access list from undergoing !---
network address translation (NAT). access-list
inside_nat0_outbound extended permit ip 192.168.1.0
255.255.255.0 192.168.2.0 255.255.255.0 !--- The traffic
specified by this ACL is !--- traffic that is to be
encrypted and !--- sent across the VPN tunnel. This ACL
is intentionally !--- the same as
(inside_nat0_outbound). !--- Two separate access lists
must always be used in this configuration. access-list
outside_cryptomap_20 extended permit ip 192.168.1.0
255.255.255.0 192.168.2.0 255.255.255.0 !--- NAT 0
prevents NAT for networks specified in the ACL
inside_nat0_outbound. nat (inside) 0 access-list
inside_nat0_outbound !--- Output Suppressed. route
outside 0.0.0.0 0.0.0.0 172.16.1.2 1 !--- Output
Suppressed. !--- PHASE 2 CONFIGURATION ---! !--- The
encryption types for Phase 2 are defined here. !---
Define the transform set for Phase 2. crypto ipsec
transform-set myset esp-3des esp-sha-hmac !--- Define
which traffic can be sent to the IPsec peer. crypto map
outside_map 20 match address outside_cryptomap_20 !---
Sets the IPsec peer. crypto map outside_map 20 set peer
10.1.1.1 !--- Sets the IPsec transform set "myset" !---
to be used with the crypto map entry "outside_map".
crypto map outside_map 20 set transform-set myset !---
Specifies the interface to be used with !--- the
settings defined in this configuration. crypto map
outside_map interface outside !--- PHASE 1 CONFIGURATION
---! !--- This configuration uses isakmp policy 10. !---
Policy 65535 is included in the config by default. !---
The configuration commands here define the Phase !--- 1
policy parameters that are used. crypto isakmp enable
outside crypto isakmp policy 10 authentication pre-share
encryption 3des hash sha group 2 lifetime 86400 crypto
isakmp policy 65535 authentication pre-share encryption
3des hash sha group 2 lifetime 86400 !--- Output
Suppressed. !--- In order to create and manage the
database of connection-specific records !--- for ipsec-
l2l-IPsec (LAN-to-LAN) tunnels, use the tunnel-group !--
- command in global configuration mode. !--- For L2L
connections the name of the tunnel group MUST be the IP
!--- address of the IPsec peer. tunnel-group 10.1.1.1
type ipsec-l2l !--- Enter the pre-shared-key in order to
configure the authentication method. tunnel-group
10.1.1.1 ipsec-attributes pre-shared-key * prompt
hostname context
Cryptochecksum:4a2c70f2102113315de795f13f25c2aa : end
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- **show crypto isakmp sa** — 顯示對等體上的所有當前IKE安全關聯(SA)。
- **show crypto ipsec sa** — 顯示所有當前SA。

本節顯示以下各項的驗證配置示例：

- HUB ASA
- Easy VPN客戶端ASA 5505
- PIX

HUB ASA

```
ciscoasa #show crypto isakmp sa

   Active SA: 2
    Rekey SA: 0 (A tunnel will report 1 Active and 1
Rekey SA during rekey)
Total IKE SA: 2
!--- Dynamic LAN-to-LAN tunnel establishment 1 IKE Peer:
172.16.2.2 Type : user Role : responder Rekey : no State
: AM_ACTIVE !--- Static LAN-to-LAN tunnel establishment
2 IKE Peer: 172.16.1.1 Type : L2L Role : initiator Rekey
: no State : MM_ACTIVE ciscoasa #show crypto ipsec sa
ciscoasa(config)#sh crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 20, local
addr: 10.1.1.1


      access-list outside_cryptomap_20 permit ip
192.168.2.0 255.255.255.0
 192.168.1.0 255.255.255.0
      local ident (addr/mask/prot/port):
(192.168.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
      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.: 10.1.1.1, remote crypto
endpt.: 172.16.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: E4312E13

    inbound esp sas:
      spi: 0x9ABAC3DD (2595931101)
         transform: esp-3des esp-sha-hmac none
         in use settings ={L2L, Tunnel, }
```

```
         slot: 0, conn_id: 741376, crypto-map:
outside_map
         sa timing: remaining key lifetime (kB/sec):
(4274999/28783)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xE4312E13 (3828428307)
         transform: esp-3des esp-sha-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 741376, crypto-map:
outside_map
         sa timing: remaining key lifetime (kB/sec):
(4274999/28783)
         IV size: 8 bytes
         replay detection support: Y

   Crypto map tag: ezvpn, seq num: 30, local addr:
10.1.1.1

     local ident (addr/mask/prot/port):
(10.1.1.1/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port):
(172.16.2.2/255.255.255.255/0/0)
      current_peer: 172.16.2.2, username: cisco
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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.: 10.1.1.1, remote crypto
endpt.: 172.16.2.2

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 2647B59C

    inbound esp sas:
      spi: 0x21685AF8 (560487160)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 737280, crypto-map: ezvpn
         sa timing: remaining key lifetime (sec): 28146
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x2647B59C (642233756)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 737280, crypto-map: ezvpn
         sa timing: remaining key lifetime (sec): 28146
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: ezvpn, seq num: 30, local addr:
10.1.1.1
```

```
      local ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
      current_peer: 172.16.2.2, username: cisco
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
      #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 5, #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.: 10.1.1.1, remote crypto
endpt.: 172.16.2.2

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 07997B21

    inbound esp sas:
      spi: 0xB5B6013D (3048603965)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 737280, crypto-map: ezvpn
         sa timing: remaining key lifetime (sec): 28145
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x07997B21 (127499041)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 737280, crypto-map: ezvpn
         sa timing: remaining key lifetime (sec): 28145
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: ezvpn, seq num: 30, local addr:
10.1.1.1

      local ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port):
(172.16.2.2/255.255.255.255/0/0)
      current_peer: 172.16.2.2, username: cisco
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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.: 10.1.1.1, remote crypto
endpt.: 172.16.2.2
```

```
      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 0F0B1A75

    inbound esp sas:
      spi: 0x68B0EA75 (1756424821)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 737280, crypto-map: ezvpn
         sa timing: remaining key lifetime (sec): 28143
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x0F0B1A75 (252385909)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 737280, crypto-map: ezvpn
         sa timing: remaining key lifetime (sec): 28143
         IV size: 8 bytes
         replay detection support: Y
```

Easy VPN客戶端ASA 5505

```
ciscoasa(config)# sh 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: 10.1.1.1
    Type    : user            Role    : initiator
    Rekey   : no              State   : AM_ACTIVE



ciscoasa(config)# sh crypto ipsec sa
interface: outside
    Crypto map tag: _vpnc_cm, seq num: 10, local addr:
172.16.2.2

      access-list _vpnc_acl permit ip host 172.16.2.2
host 10.1.1.1
      local ident (addr/mask/prot/port):
(172.16.2.2/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port):
(10.1.1.1/255.255.255.255/0/0)
      current_peer: 10.1.1.1, username: 10.1.1.1
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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.: 172.16.2.2, remote crypto
endpt.: 10.1.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 21685AF8

    inbound esp sas:
      spi: 0x2647B59C (642233756)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 178, crypto-map: _vpnc_cm
         sa timing: remaining key lifetime (sec): 28298
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x21685AF8 (560487160)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 178, crypto-map: _vpnc_cm
         sa timing: remaining key lifetime (sec): 28298
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: _vpnc_cm, seq num: 10, local addr:
172.16.2.2

      access-list _vpnc_acl permit ip host 172.16.2.2
any
      local ident (addr/mask/prot/port):
(172.16.2.2/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/0/0)
      current_peer: 10.1.1.1, username: 10.1.1.1
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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.: 172.16.2.2, remote crypto
endpt.: 10.1.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 68B0EA75

    inbound esp sas:
      spi: 0x0F0B1A75 (252385909)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 178, crypto-map: _vpnc_cm
         sa timing: remaining key lifetime (sec): 28298
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x68B0EA75 (1756424821)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
```

```
        slot: 0, conn_id: 178, crypto-map: _vpnc_cm
        sa timing: remaining key lifetime (sec): 28298
        IV size: 8 bytes
        replay detection support: Y

    Crypto map tag: _vpnc_cm, seq num: 10, local addr:
172.16.2.2

      access-list _vpnc_acl permit ip 192.168.3.0
255.255.255.0 any
      local ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/0/0)
      current_peer: 10.1.1.1, username: 10.1.1.1
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
      #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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.: 172.16.2.2, remote crypto
endpt.: 10.1.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: B5B6013D

    inbound esp sas:
      spi: 0x07997B21 (127499041)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 178, crypto-map: _vpnc_cm
         sa timing: remaining key lifetime (sec): 28294
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xB5B6013D (3048603965)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 178, crypto-map: _vpnc_cm
         sa timing: remaining key lifetime (sec): 28294
         IV size: 8 bytes
         replay detection support: Y
```

PIX

```
pixfirewall(config)# sh 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: 10.1.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
```

```
pixfirewall(config)# sh crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 20, local
addr: 172.16.1.1

     access-list outside_cryptomap_20 permit ip
192.168.1.0 255.255.255.0
    192.168.2.0 255.255.255.0
      local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port):
(192.168.2.0/255.255.255.0/0/0)
      current_peer: 10.1.1.1

      #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: 0, #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.: 10.1.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 9ABAC3DD

    inbound esp sas:
      spi: 0xE4312E13 (3828428307)
         transform: esp-3des esp-sha-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 12288, crypto-map:
outside_map
         sa timing: remaining key lifetime (kB/sec):
(3824999/28628)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x9ABAC3DD (2595931101)
         transform: esp-3des esp-sha-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 12288, crypto-map:
outside_map
         sa timing: remaining key lifetime (kB/sec):
(3824999/28628)
         IV size: 8 bytes
         replay detection support: Y
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

註：發出debug指令之前，請先參閱有關Debug指令的**重要**資訊。

在配置模式下發出PIX命令：

- **clear crypto isakmp sa** — 清除第1階段SA
- **clear crypto ipsec sa** — 清除第2階段SA

VPN隧道的**debug**命令：

- **debug crypto isakmp sa** — 調試ISAKMP SA協商
- **debug crypto ipsec sa** — 調試IPSec SA協商

相關資訊

- **Cisco PIX 500系列安全裝置 — 簡介**
- **最常見的L2L和遠端訪問IPSec VPN故障排除解決方案**
- **Cisco ASA 5500系列調適型安全裝置 — 產品支援**
- **IPSec 協商/IKE 通訊協定**
- **技術支援與文件 - Cisco Systems**