SDM：ASA/PIX和IOS路由器之間的站點間IPsec VPN配置示例

目錄

簡介

本文檔提供了Cisco安全裝置(ASA/PIX)和Cisco IOS路由器之間的LAN到LAN（站點到站點）IPsec隧道的示例配置。靜態路由用於簡單操作。

要瞭解有關PIX/ASA安全裝置運行軟體版本7.x的相同方案的詳細資訊，請參閱PIX/ASA 7.x安全裝置到IOS路由器LAN到LAN IPsec隧道配置示例。

必要條件

需求

嘗試此組態設定之前，請確保您符合以下需求：

- 開始此配置之前，必須建立端到端IP連線。
- 必須針對資料加密標準(DES)加密（最低加密等級）啟用安全裝置授權。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 8.x及更高版本的思科自適應安全裝置(ASA)
- ASDM 6.x版及更高版本
- 採用Cisco IOS®軟體版本12.3的Cisco 1812路由器
- Cisco安全裝置管理員(SDM)版本2.5

注意：要使ASDM可配置ASA，請參閱允許ASDM進行HTTPS訪問。

注意：請參閱使用SDM執行基本路由器配置，以便使用SDM配置路由器。

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。

註：有關在路由器上使用Cisco Configuration Professional的類似配置，請參閱Configuration Professional：ASA/PIX和IOS路由器之間的站點到站點IPsec VPN配置示例。

相關產品

此配置還可用於運行版本7.x及更高版本的Cisco PIX 500系列安全裝置。

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。

組態

網路圖表

本文檔使用下圖所示的網路設定。

注意：此配置中使用的IP編址方案在Internet上無法合法路由。這些地址是在實驗室環境中使用的RFC 1918 地址。

- VPN隧道ASDM配置
- 路由器SDM配置
- ASA CLI配置
- 路由器CLI配置

VPN隧道ASDM配置

完成以下步驟以建立VPN隧道：

1. 打開瀏覽器並輸入https://<為訪問ASDM而配置的ASA介面的IP地址>，以訪問ASA上的ASDM。

   請務必授權瀏覽器提供的與SSL憑證真實性相關的任何警告。預設使用者名稱和密碼均為空。

   ASA顯示此窗口以允許下載ASDM應用程式。此範例會將應用程式載入本機電腦，而且不會在Java Applet中執行。

2. 按一下Download ASDM Launcher and Start ASDM以下載ASDM應用程式的安裝程式。

3. 下載ASDM Launcher後，請完成提示指導的步驟，以安裝軟體並運行Cisco ASDM Launcher。

4. 輸入使用http -命令配置的介面的IP地址，以及使用者名稱和口令（如果已指定）。

   此示例使用cisco123作為使用者名稱並使用cisco123作為口令。

5. 在ASDM應用程式連線到ASA之後，運行IPsec VPN Wizard。

6. 選擇Site-to-Site IPsec VPN隧道型別，然後按一下Next（如圖所示）。

7. 指定遠端對等體的外部IP地址。輸入要使用的驗證資訊，在本範例中為預先共用金鑰。本示例中使用的預共用金鑰是cisco123。如果您配置L2L VPN，預設情況下Tunnel Group Name將是外部IP地址。按「Next」（下一步）。

8. 指定要用於IKE（也稱為階段1）的屬性。ASA和IOS路由器上的這些屬性必須相同。按「Next」（下一步）。

9. 指定要用於IPsec（也稱為階段2）的屬性。這些屬性在ASA和IOS路由器上都必須匹配。按「Next」（下一步）。

10. 指定應允許其流量透過VPN隧道的主機。在此步驟中，必須提供VPN隧道的本地和遠端網路。按一下Local Networks旁邊的按鈕（如圖所示），從下拉選單中選擇本地網路地址。

11. 選擇Local Network地址，然後按一下OK（如圖所示）。

12. 按一下Remote Networks旁邊的按鈕（如此處所示），從下拉選單中選擇遠端網路地址。

13. 選擇Remote Network地址，然後按一下OK（如下所示）。

    注意：如果清單中沒有「遠端網路」，則必須透過按一下增加將該網路增加到清單中。

14. 選中Exempt ASA side host/network from address translation覈取方塊，以防止隧道資料流進行網路地址轉換。然後按一下Next。

15. VPN嚮導定義的屬性顯示在此摘要中。仔細檢查配置，如果您確保設定正確，請按一下Finish。

路由器SDM配置

要在Cisco IOS路由器上配置站點到站點VPN隧道，請完成以下步驟：

1. 打開瀏覽器並輸入https://<為訪問SDM而配置的路由器介面的IP地址>，以訪問路由器上的SDM。

   請務必授權瀏覽器提供的與SSL憑證真實性相關的任何警告。預設使用者名稱和密碼均為空。

   路由器將顯示此窗口，允許下載SDM應用程式。此範例會將應用程式載入本機電腦，而且不會在Java Applet中執行。

2. SDM下載現在開始。下載SDM啟動程式後，請完成提示中指示的步驟，以安裝軟體並運行Cisco SDM啟動程式。

3. 輸入使用者名稱和口令（如果已指定），然後按一下確定。

   此示例使用cisco123作為使用者名稱並使用cisco123作為口令。

4. 選擇Configuration -> VPN -> Site-to-Site VPN，然後在SDM首頁上按一下Create a Site-to-Site VPN旁邊的單選按鈕。然後，按一下Launch The selected Task（如圖所示）：

5. 選擇Step by step wizard繼續進行配置：

6. 在下一個窗口中，在各自空間中提供VPN連線資訊。從下拉選單中選擇VPN隧道的介面。此處選擇FastEthernet0。在Peer Identity部分中，選擇Peer with static IP address並提供遠端對等體IP地址。然後，在Authentication部分提供預共用金鑰(在本示例中為cisco123)，如下所示。然後按一下Next。

7. 按一下Add增加指定加密演算法、驗證演算法和金鑰交換方法的IKE建議。

8. 提供加密演算法、驗證演算法和金鑰交換方法（如圖所示），然後按一下確定。加密演算法、驗證演算法和金鑰交換方法值應與ASA中提供的資料匹配。

9. 按一下Next（如圖所示）。

10. 應在此新窗口中提供轉換集詳細資訊。「轉換集」指定用於保護VPN隧道中的資料的加密和身份驗證演算法。然後，按一下Add提供這些詳細資訊。透過按一下Add並提供詳細資訊，您可以根據需要增加任何數量的轉換集。

11. 提供轉換集詳細資訊(加密和身份驗證演算法)，然後按一下OK（如圖所示）。

12. 從下拉選單中選擇要使用的所需轉換集（如下所示）。

13. 按「Next」（下一步）。

14. 在以下窗口中提供有關要保護的資料流（透過VPN隧道）的詳細資訊。提供要保護的資料流的源網路和目標網路，以便保護指定的源網路和目標網路之間的資料流。在本例中，源網路是10.20.10.0，目標網路是10.10.10.0。然後按一下Next。

15. 此窗口顯示完成的站點到站點VPN配置的摘要。如果您要測試VPN連線性，請選中Test VPN Connectivity after configuring 覈取方塊。此時，該框已選中，因為需要檢查連線。然後按一下Finish。

16. 按一下Start（如圖所示）以檢查VPN連線性。

17. 下一個窗口中提供了VPN連線性測試的結果。您可以在此處看到隧道處於啟用還是停用停用狀態。在此示例配置中，隧道處於啟用狀態，顯示為綠色。

    這樣就完成了Cisco IOS路由器上的配置。

ASA CLI配置

```
<#root>

ASA#

show run

: Saved
ASA Version 8.0(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!

!--- Configure the outside interface. !

interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0

!--- Configure the inside interface. !

interface Ethernet0/2
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0



 !-- Output suppressed !

passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid

access-list 100 extended permit ip any any

access-list inside_nat0_outbound extended permit ip 10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0


 !--- 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 tra
(outside_1_cryptomap)
. !--- Two separate access lists should always be used in this configuration.

access-list outside_1_cryptomap extended permit ip 10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0

!--- This access list
(outside_cryptomap)
 is used !--- with the crypto map
outside_map
 !--- to determine which traffic should be encrypted and sent !--- across the tunnel. !--- This ACL is
(inside_nat0_outbound)
. !--- Two separate access lists should always be used in this configuration.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image disk0:/asdm-613.bin
asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 10.10.10.0 255.255.255.0


nat (inside) 0 access-list inside_nat0_outbound

!--- NAT 0 prevents NAT for networks specified in !--- the ACL
inside_nat0_outbound
.


access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1


timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 dmz
no snmp-server location
no snmp-server contact


!--- PHASE 2 CONFIGURATION ---! !--- The encryption types for Phase 2 are defined here.
```

```
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac

!--- Define the transform set for Phase 2.


crypto map outside_map 1 match address outside_1_cryptomap

!--- Define which traffic should be sent to the IPsec peer.


crypto map outside_map 1 set peer 172.17.1.1

!--- Sets the IPsec peer


crypto map outside_map 1 set transform-set ESP-DES-SHA

!--- Sets the IPsec transform set "ESP-AES-256-SHA" !--- to be used with the crypto map entry "outside_

crypto map outside_map interface outside

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

!--- PHASE 1 CONFIGURATION ---! !--- This configuration uses isakmp policy 10. !--- The configuration

crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash sha
 group 1
 lifetime 86400

telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!


tunnel-group 172.17.1.1 type ipsec-l2l

!--- In order to create and manage the database of connection-specific !--- records for ipsec-l2l-IPsec

tunnel-group
```

```
 in global configuration mode. !--- For L2L connections the name of the tunnel group
MUST
 be the IP !--- address of the IPsec peer.



tunnel-group 172.17.1.1 ipsec-attributes


pre-shared-key *


!--- Enter the pre-shared-key in order to configure the !--- authentication method.


telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!


 !-- Output suppressed!

username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d
: end
```

路由器CLI配置

```
<#root>

Building configuration...

Current configuration : 2403 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no logging buffered
```

```
!
username cisco123 privilege 15 password 7 1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!


!--- Configuration for IKE policies. !--- Enables the IKE policy configuration (config-isakmp) !--- co


crypto isakmp policy 2
 authentication pre-share


!--- Specifies the pre-shared key "cisco123" which should !--- be identical at both peers. This is a g

crypto isakmp key cisco123 address 172.16.1.1

!
!

!--- Configuration for IPsec policies. !--- Enables the crypto transform configuration mode, !--- where

crypto ipsec transform-set ASA-IPSEC esp-des esp-sha-hmac


!


!--- !--- Indicates that IKE is used to establish !--- the IPsec Security Association for protecting t

crypto map SDM_CMAP_1 1 ipsec-isakmp


 description Tunnel to172.16.1.1


!--- !--- Sets the IP address of the remote end.


set peer 172.16.1.1


!--- !--- Configures IPsec to use the transform-set !--- "ASA-IPSEC" defined earlier in this configura


set transform-set ASA-IPSEC
```

```
!--- !--- Specifies the interesting traffic to be encrypted.


match address 100

!
!
!

!--- Configures the interface to use the !--- crypto map "SDM_CMAP_1" for IPsec.

interface FastEthernet0
 ip address 172.17.1.1 255.255.255.0
 duplex auto
 speed auto


crypto map SDM_CMAP_1

!
interface FastEthernet1
 ip address 10.20.10.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!
interface Vlan1
 ip address 10.77.241.109 255.255.255.192
!
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
!
!
ip nat inside source route-map nonat interface FastEthernet0 overload
!
ip http server
ip http authentication local
ip http secure-server
!

!--- Configure the access-lists and map them to the Crypto map configured.


access-list 100 remark SDM_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255

!
!
!

!--- This ACL 110 identifies the traffic flows using route map


access-list 110 deny ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
```

```
!
control-plane
!
!
line con 0
 login local
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
!
end
```

驗證

使用本節內容，確認您的組態是否正常運作。

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

- PIX安全裝置- show命令
- 遠端IOS路由器- show命令

ASA/PIX安全裝置- show命令

- show crypto isakmp sa -顯示對等體上的所有當前IKE SA。

```
<#root>

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: 172.17.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

- show crypto ipsec sa -顯示對等體上的所有當前IPsec SA。

```
<#root>

ASA#
```

```
show crypto ipsec sa

             interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1



local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)

      current_peer: 172.17.1.1



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



local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.1.1


      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 434C4A7F

    inbound esp sas:
      spi: 0xB7C1948E (3082917006)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x434C4A7F (1129073279)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
```

遠端IOS路由器- show命令

- show crypto isakmp sa -顯示對等體上的所有當前IKE SA。

```
<#root>

Router#

show crypto isakmp sa
```

```
dst             src             state          conn-id slot status
172.17.1.1      172.16.1.1
```

QM_IDLE

```
              3    0
```

ACTIVE

- show crypto ipsec sa -顯示對等體上的所有當前IPsec SA。

<#root>

```
Router#
```

show crypto ipsec sa

```
        interface: FastEthernet0
    Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1

   protected vrf: (none)
```

local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer 172.16.1.1 port 500

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

#pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
#pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68

```
    #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.: 172.17.1.1, remote crypto endpt.: 172.16.1.1

```
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xB7C1948E(3082917006)

     inbound esp sas:
      spi: 0x434C4A7F(1129073279)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3004)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB7C1948E(3082917006)
```

```
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3002)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
```

- show crypto engine connections active -顯示當前連線及加密和解密資料包的相關資訊（僅限路由器）。

<#root>

```
Router#

show crypto engine connections active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
3	FastEthernet0	172.17.1.1	set	HMAC_SHA+DES_56_CB	0	0
2001	FastEthernet0	172.17.1.1	set	DES+SHA	0	59
2002	FastEthernet0	172.17.1.1	set	DES+SHA	59	0

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

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

注意：使用debug命令之前，請參閱有關debug命令的重要資訊和IP安全故障排除-瞭解和使用debug命令。

- debug crypto ipsec 7 -顯示第2階段的IPsec協商。

  debug crypto isakmp 7 -顯示第1階段的ISAKMP協商。

- debug crypto ipsec -顯示第2階段的IPsec協商。

  debug crypto isakmp -顯示第1階段的ISAKMP協商。

有關站點到站點VPN故障排除的詳細資訊，請參閱最常見的L2L和遠端訪問IPsec VPN故障排除解決方案。

相關資訊

- Cisco PIX防火牆軟體
- 思科調適型資安裝置管理員
- 思科 ASA 5500 系列調整型安全設備
- Configuration Professional：ASA/PIX和IOS路由器之間的站點到站點IPsec VPN配置示例
- Cisco Secure PIX防火牆命令參考
- 思科路由器和安全裝置管理員
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。