作為DHCP伺服器和客戶端的PIX/ASA配置示例

目錄

簡介 必要條件 需求 採用元件 相關產品 慣例 設定 使用ASDM配置DHCP伺服器 使用ASDM配置DHCP客戶端 DHCP伺服器組態 DHCP使用者端組態 驗證 疑難排解 疑難排解指令 錯誤消息 <u>常見問題:</u>地址分配 相關資訊

<u>簡介</u>

PIX 500系列安全裝置和思科自適應安全裝置(ASA)支援作為動態主機配置協定(DHCP)伺服器和 DHCP客戶端運行。DHCP是一種協定,可為主機提供自動配置引數,如帶有子網掩碼的IP地址、 預設網關、DNS伺服器和WINS伺服器IP地址。

安全裝置可以充當DHCP伺服器或DHCP客戶端。當作為伺服器運行時,安全裝置將直接向DHCP客 戶端提供網路配置引數。當它作為DHCP客戶端運行時,安全裝置從DHCP伺服器請求此類配置引 數。

本文檔重點介紹如何使用安全裝置上的思科自適應安全裝置管理器(ASDM)配置DHCP伺服器和 DHCP客戶端。

<u>必要條件</u>

<u>需求</u>

本文檔假定PIX安全裝置或ASA完全正常運行並且配置為允許Cisco ASDM更改配置。

註:請參閱<u>允許ASDM進行HTTPS訪</u>問,以允許ASDM配置裝置。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

• PIX 500系列安全裝置7.x**註:**7.x版中使用的PIX CLI配置也適用於PIX 6.x。唯一的區別是,在 低於PIX 6.3的版本中,只能在內部介面上啟用DHCP伺服器。在PIX 6.3及更高版本中,可以在 任何可用介面上啟用DHCP伺服器。在此配置中,外部介面用於DHCP伺服器功能。

ASDM 5.x注意:ASDM僅支援PIX 7.0及更高版本。PIX裝置管理器(PDM)可用於配置PIX版本
 6.x。有關詳細資訊,請參閱Cisco ASA 5500系列和PIX 500系列安全裝置硬體和軟體相容性。
 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。

相關產品

此配置也可與Cisco ASA 7.x一起使用。

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。

<u>設定</u>

在此配置中,有兩個運行7.x版的PIX安全裝置。其中一個充當一個DHCP伺服器,為另一個充當 DHCP客戶端的PIX安全裝置7.x提供配置引數。當它充當DHCP伺服器時,PIX從指定IP地址池中動 態地將IP地址分配給DHCP客戶端。

您可以在安全裝置的每個介面上配置DHCP伺服器。每個介面可以有自己的地址池可供使用。但是 ,其他DHCP設定(如DNS伺服器、域名、選項、ping超時和WINS伺服器)是全域性配置的,由 DHCP伺服器在所有介面上使用。

不能在啟用伺服器的介面上配置DHCP客戶端或DHCP中繼服務。此外,DHCP客戶端必須直接連線 到啟用伺服器的介面。

最後,當介面上啟用DHCP伺服器時,您無法更改該介面的IP地址。

注意:基本上,沒有配置選項來設定從DHCP伺服器(PIX/ASA)傳送的DHCP應答中的預設網關地址 。 DHCP伺服器始終將自己的地址作為DHCP客戶端的網關傳送。但是,定義指向Internet路由器的 預設路由使使用者可以訪問Internet。

注意:可分配的DHCP池地址數量取決於安全裝置(PIX/ASA)中使用的許可證。 如果您使用 Base/Security Plus許可證,則這些限制適用於DHCP池。如果主機限製為10台主機,則將DHCP地 址池限製為32個地址。如果主機限製為50台主機,則將DHCP地址池限製為128個地址。如果主機 限製為無限制,則將DHCP地址池限製為256個地址。因此,地址池根據主機數量受到限制。

註:使用<u>Command Lookup Tool</u>(僅<u>供</u>已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

本檔案會使用以下設定:

- 使用ASDM配置DHCP伺服器
- 使用ASDM配置DHCP客戶端

- DHCP伺服器組態
- DHCP使用者端組態

使用ASDM配置DHCP伺服器

完成以下步驟,使用ASDM將PIX安全裝置或ASA配置為DHCP伺服器。

1. 從主視窗中選擇Configuration > Properties > DHCP Services > DHCP Server。選擇一個介面 ,然後按一下Edit以啟用DHCP伺服器並建立DHCP地址池。地址池必須與安全裝置介面位於



2. 選中**Enable DHCP server** on the outside interface以偵聽DHCP客戶端的請求。提供要傳送到 DHCP客戶端的地址池,然後按一下**OK**以返回主視窗。

	~			
 Ellable DHCF Selve 				
DHCP Address Pool:	192.168.1.5	to 192.	168.1.7	

3. 選中Enable auto-configuration on the interface,以使DHCP伺服器自動配置DHCP客戶端的 DNS、WINS和預設域名。按一下Apply以更新安全裝置的運行配置。

Cisco ASDM 5.	l for PIX - 10.0.0.1	And and a second second			
File Rules Be	arch Options Tools Wizard	s Help			
S	s []	00	Q @	3	CISCO SYSTEMS
Home (C	onnguration wontering	Back Forward	Search Kerresh	Save Help	Retillinentilline
Interfaces Security Policy NAT VPN CVPN CVPN Colored Global Cojects Properties	Configuration > Properties > D	HCP Services > DHCP DHCP Server Interface DHCI Inside outside Other DHCP Opti I♥ Enable auto-co Enabling auto-cor the default domain autoconfigured va DNS Server 1 DNS Server 2 Domain Name:	P Enabled Add No Yes 192.166.1.5 ons infiguration on interface) infiguration causes the Di in name. The values in th tues. 192.168.0.1 Apply	ress Pool - 192.158.1.7 Outside HCP server to automate fields below takes Primary WINS So Secondary WINS Rese	Edit Ping Timeout 50 ms Lease Length: 3600 secs atically configure DNS, WINS and precedence over the erver: 172.0.0.1 Server: Advanced

使用ASDM配置DHCP客戶端

完成以下步驟,使用ASDM將PIX安全裝置配置為DHCP客戶端。

1. 選擇**Configuration > Interfaces**,然後按一下**Edit**以啟用Ethernet0介面從DHCP伺服器獲取配 置引數,例如帶有子網掩碼的IP地址、預設網關、DNS伺服器和WINS伺服器IP地址。

Cisco ASDM	5.1 for PIX - 10.0.0.14								
File Rules S	earch Options Tools Wizards	s Help							
Home	Configuration Mentioning	O Back Fr	orward	Q Search	Refresh	Save Help			Cisco Systems
	Configuration > Interfaces								
Interfaces	● <u>●</u> ∓ ■ ① X 4	e (6. <u>6.</u> 6	5191						
Security Policy	Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU	Add
24	Ethernet0		No	0			No		Edit
NAT	Ethemet1	inside	Yes	-100	10.0.0.14	255.0.0.0	No	1500	Delete
23	Ethemet2		No				No		
VPN	Ethernet3		No				No	_	
*28	Ethernet4		No				No	_	
Routing	Ethemet5		No				No	_	
8									
Global Objects									
Properties									
Properties									
								_	
						_		,	
	Enable traffic between tw	o or mare int	erfaces w	hich are c	onfigured with s	ame security levels			
			_	Apply	R	eset			

2. 選中Enable Interface並輸入介面的介面名稱和安全級別。對於IP地址,選擇Obtain address via DHCP,對於預設網關,選擇Obtain default route using DHCP,然後按一下OK以轉至主 視窗。

Hardware Port:	Ethernet0	Configure Hardware Properties
Enable Interface	Dedicate this interface to	management only
nterface Name:	outside	
Security Level:	0	
IP Address		
C Use Static IP	Obtain Address via DHCP	\bigcirc
The interface au	tomatically gets its IP address u It route using DHCP	Ising DHCP.
MTU:	1500	
MTU: Description:		

3. 按一下Apply檢視從DHCP伺服器為Ethernet0介面獲取的IP地址。

lisco ASDM 5.1 fe Rules Beard	ar PIX - 10.0.0.14 fr: Options Taals W	Azərds He	lp.							
ne Con	Nonitoring	Bac	For	o ward	Q Q Search Refresh	Carre Save	? Help			Cisco Syste
nfaces	onfiguration > Interface * 🚊 🐨 😰 🗊 1	3 B 6	5 E	9	_	_		_		_
Nolicy	Interface	Name	Enabled	Security Level	IP Address	Suhnet	Mask	Management Only	МTI	Add
	Ethemet0	outside	Yes	0	192.168.1.5 (DHCP)	265.265.265	0 (DHCP)	No	1500	Edit
	Ethemet1	inside	Yes	100	10.0.0.14	255.0.0.0		No.	1500	Delete
	Ethemet5		No		-			No		
	Ethemet3		No					No	_	
	Ethemet2		No					No	_	
	Ethernet4		No					No	_	
ts										
	Enable traffic betw	een two or n	nore inter	faces whi	ch are configured with	same securit	y levels		•	
					Apply	Reset				

DHCP伺服器組態

此配置由ASDM建立:

DHCP伺服器
pixfirewall# show running-config
PIX Version 7.1(1)
1
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 10.0.0.1 255.0.0.0

!--- Output is suppressed. logging enable logging asdm informational mtu inside 1500 mtu outside 1500 no failover asdm image flash:/asdm-511.bin http server enable http 10.0.0.0 255.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart telnet

```
timeout 5 ssh timeout 5 console timeout 0 !--- Specifies
a DHCP address pool and the interface for the client to
connect. dhcpd address 192.168.1.5-192.168.1.7 outside
!--- Specifies the IP address(es) of the DNS and WINS
server !--- that the client uses. dhcpd dns 192.168.0.1
dhcpd wins 172.0.0.1
!--- Specifies the lease length to be granted to the
client. !--- This lease equals the amount of time (in
seconds) the client !--- can use its allocated IP
address before the lease expires. !--- Enter a value
between 0 to 1,048,575. The default value is 3600
seconds. dhcpd lease 3600
dhcpd ping_timeout 50
dhcpd auto_config outside
!--- Enables the DHCP daemon within the Security
Appliance to listen for !--- DHCP client requests on the
enabled interface. dhcpd enable outside
dhcprelay timeout 60
1
!--- Output is suppressed. service-policy global_policy
global Cryptochecksum:7a8cd028ee1c56083b64237c832fb5ab :
end
```

DHCP使用者端組態

此配置由ASDM建立:

DHCP使用者端

```
pixfirewall#show running-config
PIX Version 7.1(1)
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
nameif outside
security-level 0
!--- Configures the Security Appliance interface as a
DHCP client. !--- The setroute keyword causes the
Security Appliance to set the default !--- route using
the default gateway the DHCP server returns.
ip address dhcp setroute
1
interface Ethernet1
nameif inside
security-level 100
ip address 10.0.0.14 255.0.0.0
!--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive dns server-group DefaultDNS
domain-name default.domain.invalid pager lines 24
```

logging enable logging console debugging logging asdm
informational mtu outside 1500 mtu inside 1500 no
failover asdm image flash:/asdm-511.bin no asdm history
enable arp timeout 14400 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
<pre>sip_media 0:02:00 timeout uauth 0:05:00 absolute http</pre>
server enable http 10.0.0.0 255.0.0.0 inside ! Output
is suppressed. ! service-policy global_policy global
Cryptochecksum:86dd1153e8f14214524359a5148a4989 : end



完成以下步驟,使用ASDM驗證DHCP統計資訊以及來自DHCP伺服器和DHCP客戶端的繫結資訊。

 從DHCP伺服器選擇Monitoring > Interfaces > DHCP > DHCP Statistics以驗證DHCP統計資訊 ,例如DHCPDISCOVER、DHCPREQUEST、DHCPOFFER和DHCPACK。從CLI輸入show dhcpd statistics命令以檢視DHCP統計資訊。

2. 從DHCP客戶端選擇Monitoring > Interfaces > DHCP > DHCP Client Lease Information以檢視 DHCP繫結資訊。輸入show dhcpd binding命令以從CLI檢視DHCP繫結資訊。



 3. 選擇Monitoring > Logging > Real-time Log Viewer以選擇Logging Level和緩衝區限制以檢視 即時日誌消息。

Gisco ASDM 5	5.1 for PIX - 10.0.0.14	de Hale				_ 🗆 ×
Home	Centiguration Monitoring	Back Forward	Q Search R	C	? Help	Cisco Systems
Interfaces VPN A Routing Properties Logging	Monitoring > Logging > Real- Real-time Log Viewer Log Buffer	time Log Viewer Real-time Log View Click the Select th	ver View button belov e desired logging Logging Levei: Buffer Limit	v to start displaying level to see messa Debugging 1000 View) syslog message ages at that seven	is in real time. ity or higher.

4. 從DHCP客戶端檢視即時日誌事件。IP地址分配給DHCP客戶端的外部介面。

🙍 Real-t	ime Log Viewer 💫 🛶	
00 Pau	ise 🔛 Save 🕞 Cle	ar 🔚 Color Bettings 🕼 Create Rule 📓 Show Rule Find:
Filter By	-Show All-	Star Fill
Severity	Time	Message ID: Description
<u>∔</u> 8	Jan 01 1993 00:42:44	302015: Built outbound UDP connection 92 for outside 192.122.173.44/53 (192.122.173.44/53) to inside 10.0.0.2/1525 (10.0.0.2/152
<u>4</u> 6	Jan 01 1993 00:42:39	302015: Built outbound UDP connection 91 for outside:192.122.173.131/53 (192.122.173.131/53) to inside 10.0.0 2/1525 (10.0.0.2/1
<u> </u>	Jan 01 1993 00:42:32	302014: Teardown TCP connection 90 for inside:10.0.0.2/1524 to NP Identity If: 10.0.0.14/443 duration 0.00.00 bytes 1377 TCP FINe
<u> </u>	Jan 01 1993 00:42:32	725007: SSL session with client inside:10.0.0.2/1524 terminated.
<u>)</u> 6	Jan 01 1993 00:42:32	605005: Login permitted from 10.0.0.2/1524 to inside;10.0.0.14/https for user "enable_15"
<u>i 6</u>	Jan 01 1993 00:42:32	725002: Device completed S8L handshake with client inside:10.0.0.2/1524
<u> </u>	Jan 01 1993 00:42:32	725003: SSL client inside:10.0.0.2/1524 request to resume previous session.
<u>4</u> 6	Jan 01 1993 00:42:32	725001: Starting SSL handshake with client inside:10.0.0.2/1524 for TLSv1 session.
<u>4</u> 6	Jan 01 1993 00:42:32	302013: Built inbound TCP connection 90 for inside:10.0.0.2/1524 (10.0.0.2/1524) to NP Identity (fc:10.0.0.14/443 (10.0.0.14/443)
4.6	Jan 01 1993 00:42:32	302014: Teardown TCP connection 88 for inside:10.0.0.2/1523 to NP Identity If:10.0.0.14/443 duration 0:00:08 bytes 1695 TCP FINs
1 6	Jan 01 1993 00:42:32	725007: SSL session with client inside:10.0.0.2/1523 terminated.
<u>a</u> 5	Jan 01 1993 00:42:32	111008: User 'enable_15' executed the 'lp address dhop setroute' command.
1 6	Jan 01 1993 00:42:27	302015: Built outbound UDP connection 89 for outside:192.122.173.44/53 (192.122.173.44/53) to inside:10.0.0.2/1522 (10.0.0.2/152
<u>4</u> 6	Jan 01 1993 00:42:25	609002: Teardown local-host NP Identity Ifc:255.255.255.255 duration 0:02:03
<u>1</u> 6	Jan 01 1993 00:42:25	609002: Teardown local-host outside:10.0.0.2 duration 0:02:03
<u>4</u> 6	Jan 01 1993 00:42:25	302016: Tearnings UDP semection 79 for outside 10.0.0 268 to HP Identity Inc. 255.255.255.255.256.7 duration 0.02:03 bytes 248
1 6	Jan 01 1993 00:42:2	T604101: DHCP client interface outside: Allocated ip = 192.168.1.5, mask = 255.255.0, gw = 192.168.1.1
<u> </u>	Jan 01 1993 00:42:24	664102 DHCP client interface outside: address released
# 5	Jan 01 1993 00:42:24	111008. User 'enable_15' executed the internace Enternet of command.
* 5	Jan 01 1993 00 42:24	111007: Birgin conliguration; 10.0.02 reading from http://POS1]
1.0	Jan 01 1993 00 42:24	Bulsous: Login permitted from 10.010.27523 to inside 10.00.14mtps for user renable_15"
1.0	Jan 01 1993 00:42:24	725002: Device completed SSL handshake with client instant 0.00 (2015)23
1 D	Jan 01 1993 00:42:24	(22001) Starting SSL nandshake with client inside: 0.00.2/1523 for LEVE Section.
1 0 1 0	Jan 01 1883 00:42:24	302013: Built Indounts TeP connection 85 for inside: 1.00.2/1523 (1.00.0.2/1523) to NP (Gently Inc. 10.0.1 4)443 (10.00.1 4)443)
* •	Jan 01 1883 00:42:22	302013: Buildoutad ODH contraction 87 for outside:132.172.173.13193 (182.122.173.13193) to Inside:10.0.0.21 322 (10.0.0.21
4		
	\varTheta Emergencies	🗿 Alerts 🧶 Crittical 🤨 Errors 🚖 Warnings 🍌 Notifications 🗼 Informational 📧 Debugging



<u>疑難排解指令</u>

使用本節內容,確認您的組態是否正常運作。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>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 。

附註:使用 debug 指令之前,請先參閱<u>有關 Debug 指令的重要資訊</u>。

- debug dhcpd event 顯示與DHCP伺服器關聯的事件資訊。
- debug dhcpd packet 顯示與DHCP伺服器關聯的資料包資訊。

錯誤消息

CiscoASA(config)#dhcpd address 10.1.1.10-10.3.1.150 inside Warning, DHCP pool range is limited to 256 addresses, set address range as: 10.1.1.10-10.3.1.150

說明:在安全裝置上,地址池的大小限製為每池256個地址。不能更改,這是軟體限制。總數只能為 256。如果地址池範圍大於253個地址(例如254、255、256),則安全裝置介面的網路掩碼不能是 C類地址(例如255.255.255.0)。 它必須是更大的值,例如255.255.254.0。

有關如何將DHCP伺服器功能實施到安全裝置的資訊,請參閱<u>思科安全裝置命令列配置指南</u>。

常見問題:地址分配

- 問題 能否為使用ASA作為DHCP伺服器的電腦分配靜態/永久IP地址?
- 答案— 無法使用PIX/ASA。
- 問題 是否有可能將DHCP地址與ASA上的特定MAC地址關聯?
- 答案— 不,不可能。

<u>相關資訊</u>

- PIX安全裝置支援頁
- Cisco Secure PIX防火牆命令參考
- 技術支援與文件 Cisco Systems