PIX/ASA como ejemplo del servidor DHCP y de la configuración del cliente

Contenido

Introducción prerrequisitos Requisitos Componentes Utilizados **Productos Relacionados Convenciones** Configurar Configuración del Servidor DHCP con el ASDM Configuración del Cliente DHCP con ASDM Configuración del Servidor DHCP Configuración del cliente DHCP Verificación Troubleshooting Comandos para resolución de problemas Mensajes de error FAQ: Asignación de Dirección Información Relacionada

Introducción

Soporte PIX 500 Series Security Appliance y Cisco Adaptive Security Appliance (ASA) que opera como servidores de Dynamic Host Configuration Protocol (DHCP) y clientes DHCP. El DHCP es un protocolo que suministra los parámetros de la configuración automática tales como una dirección IP una máscara de subred, un gateway predeterminado, servidor DNS, y dirección IP del servidor a los hosts.

El Dispositivo de Seguridad puede actuar como un servidor DHCP o DHCP cliente. Cuando actúa como servidor, el Dispositivo de Seguridad proporciona los parámetros de la configuración de red directamente a clientes DHCP. Cuando actúa como cliente DHCP, el Dispositivo de Seguridad solicita los parámetros de la configuración de un servidor DHCP.

Este documento se centra en cómo configurar el servidor DHCP y el cliente DHCP cliente con el Cisco Adaptive Security Device Manager (ASDM) en el Dispositivo de Seguridad.

prerrequisitos

Requisitos

Este documento asume que el Dispositivo de Seguridad PIX o ASA funciona correctamente y está bien configurado para permitir que el ASDM de Cisco haga los cambios en las configuraciones.

Nota: Consulte <u>Cómo Permitir el Acceso HTTPS para que el ASDM</u> le permite al dispositivo ser configurado por ASDM.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- PIX 500 Series Security Appliance 7.xNota: La configuración CLI PIX utilizada en la versión 7.x es también aplicable a PIX 6.x. La única diferencia es que en las versiones anteriores a PIX 6.3, el servidor DHCP se puede habilitar solamente en la interfaz interior. En PIX 6.3 y posterior el servidor DHCP se puede habilitar en cualquiera de las interfaces disponibles. En esta configuración la interfaz exterior se utiliza para la función del servidor DHCP.
- ASDM 5.xNota: ASDM sólo soporta PIX 7.0 y posterior. El PIX Device Manager (PDM) está disponible configurar la versión de PIX 6.x. Consulte Compatibilidad de Hardware y Software <u>Cisco ASA 5500 Series y PIX 500 Series Security Appliance</u> para más información.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración también se puede utilizar con Cisco ASA 7.x.

Convenciones

Consulte <u>Convenciones de Consejos Técnicos de Cisco</u> para obtener más información sobre las convenciones sobre documentos.

Configurar

En esta configuración, hay dos Dispositivos de Seguridad PIX que funcionan con la versión 7.x. Uno funciona como un servidor DHCP que proporciona los parámetros de la configuración a otro Dispositivo de Seguridad 7.x PIX que funciona como un cliente DHCP. Cuando funciona como un servidor DHCP, el PIX asigna dinámicamente las direcciones IP a los clientes DHCP de un conjunto de direcciones IP señalados.

Puede configurar un servidor DHCP en cada interfaz del Dispositivo de Seguridad. Cada interfaz puede tener su propia agrupación de direcciones para extraer. Sin embargo, las otras configuraciones del DHCP, tales como servidores DNS, nombre de dominio, opciones, tiempo de espera del ping, y servidores WINS se configuran de forma global y son utilizadas por el servidor DHCP en todas las interfaces.

No puede configurar los servicios de un cliente DHCP o relé DHCP en una interfaz en la cual se habilita el servidor. Además, los clientes DHCP se deben conectar directamente con la interfaz en

la cual se habilita el servidor.

Finalmente, mientras que el servidor DHCP se habilita en una interfaz, no puede cambiar la dirección IP de esa interfaz.

Nota: Básicamente, no hay opción de configuración para establecer una dirección de gateway predeterminado en la respuesta DHCP enviada desde el servidor DHCP (PIX/ASA). El servidor DHCP envía siempre su propia dirección como el gateway para el cliente DHCP. Sin embargo, la definición de una ruta predeterminada que señale al router de Internet permite que el usuario acceda a Internet.

Nota: El número de direcciones del conjunto DHCP que puedan ser asignadas depende de la licencia utilizada en el Dispositivo de Seguridad (PIX/ASA). Si utiliza la licencia Base/Security Plus, los límites se aplican al conjunto DHCP. Si el límite del Host es 10 hosts, limita al conjunto DHCP a 32 direcciones. Si el límite del Host es 50 hosts, limita el conjunto DHCP a 128 direcciones. Si el límite del Host es ilimitado, limita el conjunto DHCP a 256 direcciones. Así la agrupación de direcciones se limita en función del número de hosts.

Nota: Utilice la herramienta <u>Command Lookup Tool</u> (<u>clientes registrados solamente</u>) para obtener más información sobre los comandos utilizados en esta sección.

En este documento, se utilizan estas configuraciones:

- <u>Configuración del Servidor DHCP con el ASDM</u>
- <u>Configuración del Cliente DHCP con ASDM</u>
- <u>Configuración del Servidor DHCP</u>
- <u>Configuración del cliente DHCP</u>

Configuración del Servidor DHCP con el ASDM

Siga estos pasos para configurar el Dispositivo de Seguridad PIX o ASA como servidor DHCP con ASDM.

 Elija Configuration > Properties > DHCP Services > DHCP Server de la ventana Home. Seleccione una interfaz y haga clic en Edit para habilitar el servidor DHCP y para crear a conjunto de direcciones DHCP.El conjunto de direcciones debe estar en la misma subred que la interfaz del Dispositivo de Seguridad. En este ejemplo, el servidor DHCP se configura en la interfaz exterior del Dispositivo de Seguridad PIX.

Cisco ASDM 5	.1 for PIX - 10.0.0.1	e Heln						
Home	Configuration Mantoring	Back For	ward Search	Q Refresh	Save	? Help	CI	ISCO SYSTEMS
Interfaces Security Policy NAT WPN Routing Global Objects Properties	Configuration - Properties - D Configuration - Properties - D Configuration - Properties - D Configuration - Configuration Configuration - Configuratio	HCP Services	DHCP Server	Add on interface: auses the Di- e values in th	ress Pool outside HCP server to e fields below Primary V Secondar	Edit Ping Timeo Lease Leng V sautomatically config v takes precedence MINS Server:	ut: 50 tth: 3800 ure DNS, WIN over the Advan	ms secs 6 and

 Verifique Enable servidor DHCP en la interfaz exterior para escuchar las solicitudes de los clientes DHCP. Proporcione el conjunto de direcciones que se ejecutará al cliente DHCP y haga clic la OK para volver a la ventana principal.

Interface: outside			
Enable DHCP serve	r		
DHCP Address Pool:	192.168.1.5	to 192.168.1.7	

3. Verifique **Enable auto-configuration on the interface** para que el servidor DHCP configure automáticamente el DNS, WINS y el Nombre de dominio predeterminado para el cliente DHCP. Haga clic en **Apply** para poner la configuración actual del Dispositivo de Seguridad.

Configuración del Cliente DHCP con ASDM

Siga estos pasos para configurar el Dispositivo de Seguridad PIX como Cliente DHCP cliente con ASDM.

 Elija Configuration > Interfaces y haga clic en Edit para habilitar la interfaz Ethernet0 y obtener los parámetros de configuración como la dirección IP con una máscara de subred, gateway predeterminado, servidor DNS y dirección IP de servidor WINS desde el servidor DHCP.

Cisco ASDM	.1 for PIX - 10.0.0.14		-				
File Rules S	earch Options Tools Wizards	Help					
dia norma di constante di const	Configuration Mentioring	Back Forv	ward Sear	ch Refresh	Save Help		Cisco Systems
	Configuration > Interfaces						
Interfaces	* £ ¥ 🖬 📋 X 4		9				
Security Policy	Interface	Name E	nabled Secu	IP Address	Subnet Mask	Management M	TU Add
24	Ethemel0		No	0		No	Edit
NAT	Ethemet1	Inside	Yes	10010.0.0.14	255.0.0.0	No 150	0 Delete
2	Ethemet2		No			No	
VPN	Ethernet3		No			No	-
*28	Ethernet4		No			No	-
Routing	Ethemet5		No			No	-
8			1				-
Global Objects							
20							
Properties							
							_
					_		•
	Enable traffic between tw	o or more interf	faces which a	e configured with s	ame security levels		
			Aop	R	eset		

 Verifique Enable Interface e ingrese el Nombre de la Interfaz y el Nivel de Seguridad para la interfaz. Elija Obtain address via DHCP para la dirección IP y Obtain default route using DHCP para el gateway predeterminado y luego haga clic en OK para ir a la ventana Principal.

lardware Port:	Ethernet0	Configure Hardware Properties
Enable Interface	Dedicate this interface to	o management only
nterface Name:	outside	
ecurity Level:	0	
IP Address		
C Use Static IP 🤇	Obtain Address via DHC	P
The interface au	tomatically gets its IP address	using DHCP.
I Obtain defau	It route using DHCP	Renew DHCP Lease
ITU:	It route using DHCP	Renew DHCP Lease
ITU: Pescription:	It route using DHCP	Renew DHCP Lease

3. Haga clic en **Apply** para ver la dirección IP obtenida para la Interfaz Ethernet0 desde el servidor DHCP.

Cisco ASDM 5 File Rules Be	.1 for PIX - 10.0.0.14 earch: Options Tools V	Vizards Help	1						
Home	Configuration Monitoring	g Back	Forv) werd :	Q Q Search Ratresh	🗐 ? Save Help			Cisco Systems
Interfaces	Configuration > Interface	5 B 🕰	6 E	9	_		_		_
Security Policy	Interface	Name E	nabled	Security Level	IP Address	Subnet Mask	Management Only	MTI	Add
24	Ethernet0	outside	Yes	đ	192.168.1.5 (DHCP)	255.255.255.0 (DHCP)	No	1500	Edit
NAT	Ethemeti	inside	Yes	100	10.0.0.14	255.0.0.0	No	1500	Delete
93	Ethemet5		No				No		
VPN	Ethemet3		No				No		
120	Ethemet2		No				No		
Routing	Ethemet4		No				No		
Global Okjects	■ Enable traffic betv	veen two or ma	ore inter	faces whi	ch are configured with Apply	same security levels Reset		×	

Configuración del Servidor DHCP

Esta configuración es creada por el ASDM:

Servidor DHCP 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 1 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
!
!--- Output is suppressed. service-policy global_policy
global Cryptochecksum:7a8cd028ee1c56083b64237c832fb5ab :
end
```

Configuración del cliente DHCP

Esta configuración es creada por el ASDM:

DHCP Client

```
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
sip_media 0:02:00 timeout uauth 0:05:00 absolute http
server enable http 10.0.0.0 255.0.0.0 inside ! Output
<i>is suppressed.</i> ! service-policy global_policy global
Cryptochecksum:86dd1153e8f14214524359a5148a4989 : end

Verificación

Siga estos pasos para verificar las estadísticas del DHCP y la información obligatoria del servidor DHCP y el DHCP cliente con ASDM.

 Elija Monitoring > Interfaces > DHCP > DHCP Statistics del servidor DHCP para verificar las estadísticas DHCP, como DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, y DHCPACK.Ingrese el comando show dhcpd statistics del CLI para ver las estadísticas DHCP.

Cisco ASDM 5	.1 for PIX - 10.0.0.1 earch: Options Tools Wizards	Help	<u>a 🖆 e</u>	_O×
Home	Centiguration Monitoring	Back Forward Search Retresh	Save Help	Cisco Systems
Interfaces	Monitoring > Interfaces > DHCP		e type. Count 5 4 0 1 8 0 5 12 0 Total Messages Se Value 0 1 1 1 1 0 Refresh	Direction Received Received Received Received Received Received Sent Sent Sent Sent Sent
Data Refreshed	Successfully.	<admin></admin>	NA (15) 🛛 🔗 🕼	ast Updated: 6/5/06 3:17:17 PM

 Elija Monitoring > Interfaces > DHCP > DHCP Client Lease Information del cliente DHCP para ver información sobre la conexión del DHCP.Ingrese el comando show dhcpd binding para ver información de conexión del DHCP desde el CLI.

Cisco ASDM 5	.1 for PIX - 10.0.0.14		-				<u> </u>
File Rules B	earch Options Tools Wizard	is Help					and the second sec
Icme	Configuration Monitoring	Back	Forward Search	Refresh	Seve Help		Cisco Systems
Interfaces	Manitoring > Interfaces > DHO ARP Table DHCP DHCP Server Table DHCP Statistics Dynamic ACLs Dynamic ACLs minterface Graphs inside outside	P ► DHCP C	Client Lease Information Select a DHCP All Temp IP addr: Temp sub nat DHCP Lease s state: Lease: Renewal: Rebind: Temp default-g Next imer fires Retry count: Client-ID: Proxy: Hostname;	on Interface: ou tribute mask: erver: ateway addr: after:	tside - 192.168.1.5 V 192.168.1.5 255.255.255.0 192.168.1.1 Bound 3600 seconds 1800 seconds 192.168.1.1 1486 seconds 0 cisco-0015.fa56 FALSE pixfirewall	alue .f046-outside-pixf	
Data Refreshed	Successfully	-		<admin></admin>	NA (15)	Last Updated: 6/5/	06 3:01:19 PM
Data rtenesneu	adecessiony.			Starting the start of the start		- 00s	a rater teo Altro Of C

 Elija Monitoring > Logging > Real-time Log Viewer para seleccionar el Nivel de Registro y el buffer limit para ver los mensajes Log en Tiempo Real.



4. Vea los eventos en tiempo real del registro del cliente DHCP. La dirección IP se asigna a la interfaz exterior del cliente

DHCP	
D1101 .	

🗟 Real-ti	ime Log Viewer 🛛 🛶	
00 Pau	se 🔄 🔜 Save 🖙 Cle	ar 🔄 Color Bettings 🐚 Create Ruis 📓 Strow Rule Find:
Filter By	-Show All-	All Filt
Severity	Time	Message ID: Description
<u>4</u> 6	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 (10.0.0.2/1
<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)
<u>¢</u> 6	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 FI
<u>4</u> 6	Jan 01 1993 00:42:32	725007: SSL session with client inside:10.0.0.2/1524 terminated.
<u>i</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</u> 6	Jan 01 1993 00:42:32	725002: Device completed SSL handshake with client inside:10.0.0.2/1524
6 6	Jan 01 1993 00:42:32	725003: SSL client inside:10.0.0.2/1524 request to resume previous session.
<u>i</u> 6	Jan 01 1993 00:42:32	725001: Starting SSL handshake with client inside:10.0.0.2/1524 for TLSv1 session.
<u>i</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 Ifc:10.0.0.14/443 (10.0.0.14/443)
6	Jan 01 1993 00:42:32	302014: Teardown TCP connection 88 for inside:10.0.0.24 523 to NP Identity Ifc:10.0.0.14/443 duration 0:00:08 bytes 1695 TCP FI
1.6	Jan 01 1993 00:42:32	725007: SSL session with client inside:10.0.0.2/1523 terminated.
à. 5	Jan 01 1993 00:42:32	111008: User 'enable_15' executed the 'lp address dhop setroute' command.
i 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 (10.0.0.2/1
£ 6	Jan 01 1993 00:42:25	609002: Teardown local-host NP Identity ffc:255.255.255.255 duration 0:02:03
£ 6	Jan 01 1993 00:42:25	609002: Teardown local-host outside:10.0.0.2 duration 0:02:03
£ 6	Jan 01 1993 00:42:25	302016: Teardnum UDP connection 79 for outside 10.0.0 2/68 to NP Identity In: 255:255:255:255:255:257 duration 0:02:03 bytes 248
6	Jan 01 1993 00:42:24	604101: DHCP client interface outside: Allocated ip = 192.168.1.5, mask = 255.255.255.255.0, gw = 192.168.1.1
6 6	Jan 01 1993 00:42:24	6644.02 DHCP client interface outside: address released
8.5	Jan 01 1993 00:42:24	111008: User 'enable_15' executed the interace Einemer or command.
£ 5	Jan 01 1993 00:42:24	111007: Begin configuration: 10.0.0.2 reading from http [POST]
6 6	Jan 01 1993 00 42:24	605005: Login permitted from 10.0.0.2/1523 to inside:10.0.0.14/https for user "enable_15"
6	Jan 01 1993 00:42:24	725002: Device completed SSL handshake with client inside 10.0.0.2/1523
6 6	Jan 01 1993 00:42:24	725001: Starting SSL handshake with client inside:10.0.0.2/1523 for TLSv1 session.
6	Jan 01 1993 00:42:24	302013: Built inbound TCP connection 88 for inside:10.0.0.2/1523 (10.0.0.2/1523) to NP Identity Ifc:10.0.0.14/443 (10.0.0.14/443)
6	Jan 01 1993 00:42:22	302015: Built outbound UDP connection 87 for outside:192.122.173.131/53 (192.122.173.131/53) to inside:10.0.0.2/1522 (10.0.0.
·		
	Emergencies	🗿 Alerts 🔞 Critical 🤨 Errors 🏦 Warnings 🗼 Notifications 🧎 informational 💿 Debugging

Troubleshooting

Comandos para resolución de problemas

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

- debug dhcpd event: muestra información del evento asociada al servidor DHCP.
- debug dhcpd packet: muestra información del paquete asociada al servidor DHCP.

Mensajes de error

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

Explicación: Los tamaños del conjunto de direcciones se limitan a 256 direcciones por conjunto en el dispositivo de seguridad. Esto no se puede cambiar y es una limitación del software. El total sólo puede llegar a 256. Si el rango del conjunto de direcciones es superior a 253 direcciones (por ejemplo 254, 255, 256), la máscara de red de la interfaz del dispositivo de seguridad no puede ser una dirección de clase C (por ejemplo, 255.255.255.0). Necesita ser algo más grande, por ejemplo, 255.255.254.0.

Consulte <u>Guía de Configuración de la Línea de Comando de Cisco Security</u> Appliance para obtener la información sobre cómo implementar la función del servidor DHCP en el dispositivo de seguridad.

FAQ: Asignación de Dirección

Pregunta - ¿Es posible asignar una dirección IP estática/permanente al equipo que utiliza el ASA como el servidor DHCP?

Respuesta - No es posible si se usa el PIX/ASA.

Pregunta - ¿Es posible unir direcciones DHCP a direcciones MAC específicas en el ASA?

Respuesta - No, no es posible.

Información Relacionada

- Páginas de Soporte de PIX Security Appliance
- Referencias de Comandos de Cisco Secure PIX Firewall
- Soporte Técnico y Documentación Cisco Systems