Esempio di configurazione di PIX/ASA come server DHCP e client

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Prodotti correlati Convenzioni Configurazione Configurazione del server DHCP con ASDM Configurazione del client DHCP con ASDM Configurazione server DHCP Configurazione client DHCP Verifica Risoluzione dei problemi Comandi per la risoluzione dei problemi Messaggi di errore Domande frequenti: Assegnazione indirizzo Informazioni correlate

Introduzione

I modelli PIX serie 500 Security Appliance e Cisco Adaptive Security Appliance (ASA) supportano il funzionamento sia come server DHCP (Dynamic Host Configuration Protocol) sia come client DHCP. DHCP è un protocollo che fornisce agli host parametri di configurazione automatica, ad esempio un indirizzo IP con subnet mask, gateway predefinito, server DNS e indirizzo IP del server WINS.

Appliance di sicurezza può funzionare come server DHCP o client DHCP. Quando funziona come server, Security Appliance fornisce i parametri di configurazione della rete direttamente ai client DHCP. Quando funziona come client DHCP, Appliance di sicurezza richiede tali parametri di configurazione a un server DHCP.

Nel documento viene spiegato come configurare il server DHCP e il client DHCP usando Cisco Adaptive Security Device Manager (ASDM) sull'appliance di sicurezza.

Prerequisiti

Requisiti

In questo documento si presume che l'appliance di sicurezza PIX o l'ASA sia completamente operativa e configurata per consentire a Cisco ASDM di apportare modifiche alla configurazione.

Nota: per consentire al dispositivo di essere configurato da ASDM, consultare il documento sull'<u>autorizzazione</u> dell'<u>accesso HTTPS per ASDM</u>.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- PIX serie 500 Security Appliance 7.x**Nota:** la configurazione PIX CLI utilizzata nella versione 7.x è applicabile anche a PIX 6.x. L'unica differenza è che nelle versioni precedenti a PIX 6.3, il server DHCP può essere abilitato solo sull'interfaccia interna. In PIX 6.3 e versioni successive, il server DHCP può essere abilitato su qualsiasi interfaccia disponibile. In questa configurazione, viene usata l'interfaccia esterna per la funzionalità del server DHCP.
- ASDM 5.xNota: ASDM supporta solo PIX 7.0 e versioni successive. PIX Device Manager (PDM) è disponibile per la configurazione della versione 6.x di PIX. Per ulteriori informazioni, fare riferimento alla <u>compatibilità hardware e software delle appliance di sicurezza Cisco ASA</u> <u>serie 5500 e PIX serie 500</u>.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco ASA 7.x.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Configurazione

In questa configurazione sono presenti due appliance di sicurezza PIX con versione 7.x. Una funziona come server DHCP che fornisce i parametri di configurazione a un altro PIX Security Appliance 7.x che funziona come client DHCP. Quando funziona come server DHCP, il PIX assegna dinamicamente indirizzi IP ai client DHCP da un pool di indirizzi IP designati.

Èpossibile configurare un server DHCP su ciascuna interfaccia dell'appliance di sicurezza. Ogni interfaccia può disporre di un proprio pool di indirizzi da cui estrarre. Tuttavia, le altre impostazioni DHCP, ad esempio i server DNS, il nome di dominio, le opzioni, il timeout del ping e i server WINS, sono configurate globalmente e utilizzate dal server DHCP su tutte le interfacce.

Non è possibile configurare un client DHCP o i servizi di inoltro DHCP su un'interfaccia su cui è abilitato il server. Inoltre, i client DHCP devono essere connessi direttamente all'interfaccia su cui è abilitato il server.

Infine, quando il server DHCP è abilitato su un'interfaccia, non è possibile modificare l'indirizzo IP di tale interfaccia.

Nota: fondamentalmente, non è disponibile un'opzione di configurazione per impostare l'indirizzo del gateway predefinito nella risposta DHCP inviata dal server DHCP (PIX/ASA). Il server DHCP invia sempre il proprio indirizzo come gateway per il client DHCP. Tuttavia, la definizione di un percorso predefinito che punti al router Internet consente all'utente di raggiungere Internet.

Nota: il numero di indirizzi del pool DHCP che possono essere assegnati dipende dalla licenza utilizzata nell'appliance di sicurezza (PIX/ASA). Se si usa la licenza Base/Security Plus, questi limiti sono validi per il pool DHCP. Se il limite per gli host è 10, il pool DHCP può essere limitato a 32 indirizzi. Se il limite per gli host è 50, il pool DHCP può essere limitato a 128 indirizzi. Se il limite dell'host è illimitato, il pool DHCP può essere limitato a 256 indirizzi. Pertanto, il pool di indirizzi è limitato in base al numero di host.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> ricerca dei comandi (solo utenti registrati).

Nel documento vengono usate queste configurazioni:

- <u>Configurazione del server DHCP con ASDM</u>
- <u>Configurazione del client DHCP con ASDM</u>
- <u>Configurazione server DHCP</u>
- <u>Configurazione client DHCP</u>

Configurazione del server DHCP con ASDM

Completare la procedura descritta di seguito per configurare l'appliance di sicurezza PIX o l'ASA come server DHCP con ASDM.

 Scegliere Configurazione > Proprietà > Servizi DHCP > Server DHCP dalla finestra Home. Selezionare un'interfaccia e fare clic su Modifica per abilitare il server DHCP e creare un pool di indirizzi DHCP.II pool di indirizzi deve trovarsi nella stessa subnet dell'interfaccia di Security Appliance. Nell'esempio, il server DHCP è configurato sull'interfaccia esterna di PIX Security

Appliance.

File Roles (5.1 for PIX - 10.0.0.1 Tearch Oplions Tools Wizards	s Help					<u></u>	
Si Home	Configuration Montoring	O (Back For	wvard Search	Q Refresh	Save	? Ныр	(CISCO SYSTEMS
interfaces Security Policy NAT VPN Routing Global Objects Properties	Configuration > Properties > D Configuration > D Configuration > D Configuration > Properties > D Configuration > D Configur	HCP Services DHCP Serve Interface Inside Outside Other DH Enable Enabling the defaul autoconfig DNS Serv DNS Serv Domain N	DHCP Server Server DHCP Enabled No No No CP Options auto-configuration auto-configuration t domain name. Th pured values. er 1: Fer 2: Iame:	Add on interface: auses the Di e values in th	ress Paol outside HCP server 1 e fields belo Primary Seconda	Edit Ping Tim Lease L Ving Server: any WINS Server: any WINS Server:	neout: 50 ength: 3600 nfigure DNS, With ce over the Advar	ms secs J6 and

2. Selezionare **Abilita server DHCP** sull'interfaccia esterna per l'ascolto delle richieste dei client DHCP. Specificare il pool di indirizzi da inviare al client DHCP e fare clic su **OK** per tornare alla finestra principale

Edit DHCP Server			
Interface: outside			
Enable DHCP serve	r		
DHCP Address Pool:	192.168.1.5	to 192.168.1.7	
OK	Cancel	Help	

3. Selezionare Abilita configurazione automatica sull'interfaccia per fare in modo che il server DHCP configuri automaticamente il DNS, il WINS e il nome di dominio predefinito per il client DHCP. Fare clic su Applica per aggiornare la configurazione in esecuzione dell'appliance di sicurezza.

Cisco ASDM 5.	1 for PIX - 10.0.0.1		_ [] ×
File Rules Be	arch Options Tools Wizard	s Help	
Si Home	Configuration Monitoring	O O Q O O Back Forward Search Refresh Save Help	CISCO STATENS
Home Home Interfaces Security Policy NAT VPN VPN Sicken Objects Properties	Configuration Monitoring Configuration Properties Configuration Properties Configuration Properties Configuration Properties Configuration Properties Configuration Configuration Configuration AAA Setup Configuration AAA Setup Configuration AAA Setup Configuration AAA Setup Configuration Device Access Device Access Device Access PhiCP Server Device Access Philosopy Provide Access Philosopy Philosopy Philosopy Philosopy Philosopy Philosopy Philosopy Philosopy Philos	Back Forward Search Refresh Save Help HCP Services > DHCP Server Interface DHCP Server Interface DHCP Enabled Address Pool Edit Inside No Edit Inside Yes Other DHCP Options Fing Timeout 50 Lease Length: 3800 Other DHCP Options Image: Server to automatically configure DNS, We the default domain name. The values in the fields below takes precedence over the autoconfiguration causes the DHCP server to automatically configure DNS, We the default domain name. The values in the fields below takes precedence over the autoconfigure values. DNS Server 1: 192.158.0.1 Primary WINS Server: 172.0.1 DNS Server 2: Secondary WINS Server: 172.0.1	ms secs
	· MTCP Options 행Timeouts - 뀀URL Filtering	Adv Apply Reset	anced

Configurazione del client DHCP con ASDM

Completare la procedura seguente per configurare PIX Security Appliance come client DHCP utilizzando ASDM.

 Scegliere Configurazione > Interfacce e fare clic su Modifica per abilitare l'interfaccia Ethernet0 e ottenere dal server DHCP i parametri di configurazione, ad esempio un indirizzo IP con subnet mask, gateway predefinito, server DNS e indirizzo IP del server WINS.

Cisco ASDM	5.1 for PIX - 10.0.0.14							n <u>1</u> .1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	
File Rules S	learch Options Tools Wizard	s Help							
Home -	Configuration Mentering	O Back F	orward	Q Search	Refresh	Save Help			Cisco Systews
	Configuration > Interfaces								
Interfaces	●主筆 11 (自) ※	10.0	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
<u> 3</u>	Ethemet2		No				No		
VPN	Ethernet3		Nó				No		
****	Ethernet4		No				No		
Routing	Ethernet5		No				No		
8									
Global Objects									
3									
Properties									
								•	
	Enable traffic between h	wo or more in	lerfaces w	hich are ci	onfigured with sa	ame security levels			
				Aapiy	R	eset			
			1						

 Selezionare Abilita interfaccia e immettere il nome e il livello di sicurezza dell'interfaccia. Selezionare Obtain address via DHCP (Ottieni indirizzo via DHCP) per l'indirizzo IP e Obtain default route using DHCP (Ottieni percorso predefinito tramite DHCP per il gateway predefinito), quindi fare clic su OK per andare alla finestra principale.

Edit Interface		
Hardware Port:	EthernetO	Configure Hardware Properties.
Enable Interface	Dedicate this interface to	o management only
Interface Name:	outside	
Security Level:	0	
IP Address		
C Use Static IP	Obtain Address via DHC	P
The interface au	itomatically gets its IP address Ilt route using DHCP	using DHCP. Renew DHCP Lease
MTU:	1500	
Description:		
	OK Cancel	Help

3. Fare clic su **Apply** (Applica) per visualizzare l'indirizzo IP ottenuto per l'interfaccia Ethernet0 dal server DHCP.

Cisco ASDM 5.1 fo le Rules Beard	r PIX - 10.0.0.14 1: Options Taals Vi	Azards He	lp						
Gine Cont	Nguration Monitoring	Bac	k Forv) werd	Q Q Search Ratresh	🗐 🢡 Save Help			Cisco System
Interfaces	onfiguration > Interface ▶ 🟦 🐨 💕 📋 🗍	: X B R	6 E	9	_	_	_		_
Ess Security Policy	Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management	MT	Add
24	Ethernet0	outside	Yes	0	192.168.1.5 (DHCP)	255.255.255.0 (DHCF	2 No	1500	Edit
NAT	Ethernet1	inside	Yes	100	10.0.0.14	255.0.0.0	No	1500	Delete
9	Ethernet5		No				No		
VPN	Ethemet3		No				No		
420	Ethemet2		No				No		
Routing	Ethemet4		No				No		
Global Okjects	Enable traffic betw	een two or r	nore inter	faces whi	ch are configured with Apply	same security levels Reset		×	

Configurazione server DHCP

Questa configurazione viene creata da ASDM:



```
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
```

Configurazione client DHCP

Questa configurazione viene creata da ASDM:

```
Client DHCP
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

Verifica

Completare la procedura seguente per verificare le statistiche DHCP e le informazioni di binding dal server DHCP e dal client DHCP tramite ASDM.

 Scegliere Monitoraggio > Interfacce > DHCP > Statistiche DHCP dal server DHCP per verificare le statistiche DHCP, ad esempio DHCPDISCOVER, DHCPREQUEST, DHCPOFFER e DHCPACK.Immettere il comando show dhcpd statistics dalla CLI per visualizzare le statistiche



 Scegliere Monitoraggio > Interfacce > DHCP > Informazioni sul lease del client DHCP dal client DHCP per visualizzare le informazioni sul binding DHCP.Immettere il comando show dhcpd binding per visualizzare le informazioni sul binding DHCP dalla CLI.

🖆 Cisco ASDM 5.1 for PIX - 10.0.0.14		-		<u> </u>
File Rules Bearch Options Tools V	Wizards Help			
Home Configuration Monitoria	ng Back Forward See	rch Retresh Si	ave Heb	CISCO SYSTEMS
Monitoring > Interfaces + ARP Table ARP Table ARP Table ARP Table ARP Table ARP Table ARP Table ARP Table ARP Table DHCP Server ARP Table DHCP Server ARD DHCP Statist Dynamic ACLs Dynamic ACLs ARD DHCP Statist ARD DHCP Statist A	DHCP > DHCP Client Lease Infom DHCP Client Lease Infom DHCP Client Lease Infom DHCP Client Lease Infom Select a DI Temp IP a Temp State: Lease: Renewal: Rebind: Temp defa Next timer Rebind: Rebind: Next timer Rebind: Next timer Next timer Rebind: Next timer Next timer Next ti	rmation hation HCP Interface: Outsid Attribute ddr: o net mask: ase server: ault-gateway addr: fires after: nt: x:	Se - 192.168.1.5 Value 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.f046-outside-; FALSE pixfirewall	bkf
Data Refreshed Successfully.	<u>)</u>	<admin> NA</admin>	Last Updated	: 6/5/06 3:01:19 PM

3. Scegliere **Monitoraggio > Log > Visualizzatore log in tempo reale** per selezionare il livello di log e il limite del buffer per visualizzare i messaggi di log in tempo reale.

盾 Cisco ASDM	5.1 for PIX - 18.0.0.14					_ D ×
File Rules I	Bearch Options Tools Wizar	ds Help				
G Home	Contiguration Monitoring	O Beck	Forward Search I	Refresh Save	? Help	Cisco Systems
Interfaces VPN 4 Routing Properties Logging	Monitoring > Logging > Reak ■ Reaktime Log Viewer ■ Log Buffer	tme Log View	ver Log Viewer Click the View button belo Select the desired loggin Logging Level: Buffer Limit	w to start displayin g level to see mess Debugging 1000 View	ig syslog mess sages at that se	ages in real time. venty or higher.

4. Visualizzare gli eventi del registro in tempo reale dal client DHCP. L'indirizzo IP viene allocato per l'interfaccia esterna del client

Filter B	/ -Show All-				Ster Filt			
Beverity	Time					Message ID: Descrip	tion	
6	Jan 01 1993 00:42	44	302015: Built outbound	UDP connection 92	2 for outside:192.	122.173.44/53 (192.1)	22.173.44/53) to inside 1	0.0.0.2/1525 (10.0.0.
6	Jan 01 1993 00:42:	39 :	302015: Built outbound	UDP connection 91	1 for outside:192.	122.173.131/53 (192.1	122.173.131/53) to inside	e:10.0.0 2/1525 (10.0
6	Jan 01 1993 00:42:	32	302014: Teardown TCP	connection 90 for i	inside:10.0.0.2/15	24 to NP Identity Ifc:10	0.0.0.14/443 duration 0:0	0:00 bytes 1377 TCP
6 6	Jan 01 1993 00:42:	32	725007: SBL session w	ith client inside:10.	.0.0.2/1524 termin	nated.		
6	Jan 01 1993 00:42:	32	605005: Login permittee	d from 10.0.0.2/152	4 to inside:10.0.0	0.14/https for user "ena	ble_15"	
6 6	Jan 01 1993 00:42:	32	725002: Device complete	ted SSL handshak	e with client insid	e:10.0.0.2/1524		
6 6	Jan 01 1993 00:42:	32	725003: SSL client insid	le:10.0.0.2/1524 re	quest to resume	previous session.		
6	Jan 01 1993 00:42:	32	725001: Starting SSL ha	andshake with clier	nt inside:10.0.0.2/	1524 for TLSv1 session	on.	
6	Jan 01 1993 00:42:	32	302013: Built inbound T	CP connection 901	for inside:10.0.0.2	2/1524 (10.0.0.2/1524)	to NP Identity Ifc:10.0.0.1	4/443 (10.0.0.14/44
6	Jan 01 1993 00:42:	32	302014: Teardown TCP	connection 88 for	inside:10.0.0.2/15	23 to NP Identity Ifc:10	0.0.0.14/443 duration 0:0	0:08 bytes 1696 TCP
6	Jan 01 1993 00:42:	32	725007: SSL session w	ith client inside:10.	.0.0.2/1 523 termin	nated.		
5	Jan 01 1993 00:42:	32	111008: User 'enable_1	5' executed the 1p	address dhop set	troute" command.		
5	Jan 01 1993 00:42:	27	302015: Built outbound	UDP connection B	9 for outside:192.	122.173.44/53 (192.1)	22.173.44/53) to inside:1	0.0.0.2/1522 (10.0.0.
6	Jan 01 1993 00:42:	25	609002: Teardown local	I-host NP Identity If	0:255.255.255.25	5 duration 0:02:03		
6	Jan 01 1993 00:42:	25	609002: Teardown local	-hast outside:10.0	.0.2 duration 0:02	:03		
6	Jan 01 1993 00:42:	25	302016: Teardown UDP	sonnection 79 for	ouiside.10.0.0.20	Se to NP Identity lic.25	5.205.265.255/87 duratio	in 0:02:03 bytes 248
6	Jan 01 1993 00:42:	2	604101: DHCP client int	terface outside: Allo	ocated ip = 192.10	89.1.5, mask= 255.25	5.255.0, gw = 192.189.1.	1
6	Jan 01 1993 00:42:	24	664102 DHCP client int	lerface outside: ad	dress released			
5	Jan 01 1993 00:42	24	111008: User 'enable_1	5' executed the Int	enace Einemer u	commane.		
5	Jan 01 1993 00:42:	24	111007: Begin configura	ation: 10.0.0.2 read	ing from http (PO:	6T]		
6	Jan 01 1993 00:42:	24	605005: Login permittee	d from 10.0.0.2/152	:3 to inside:10.0.0	0.14/https for user "ena	ible_15"	
6	Jan 01 1993 00:42:	24	725002: Device complete	ted SSL handshak	e with client insid	e:10.0.0.2/1523		
6	Jan 01 1993 00:42:	24	725001: Starting SSL ha	andshake with clier	nt inside:10.0.0.2/	1523 for TL8v1 session	on.	
6	Jan 01 1993 00:42:	24	302013: Built inbound T	CP connection 881	for inside:10.0.0.2	2/1523 (10.0.0.2/1523)	to NP Identity Ifc:10.0.0.1	14/443 (10.0.0.14/44
6	Jan 01 1993 00:42:	22	302015: Built outbound	UDP connection 87	7 for outside:192.	122.173.131/53 (192.1	(22.173.131/53) to inside	s:10.0.0.2/1522 (10.0

Risoluzione dei problemi

Comandi per la risoluzione dei problemi

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

- debug dhcpd event: visualizza le informazioni sull'evento associate al server DHCP.
- debug dhcpd packet: visualizza le informazioni sul pacchetto associate al server DHCP.

Messaggi di errore

```
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
```

Spiegazione: La dimensione del pool di indirizzi è limitata a 256 indirizzi per pool sull'appliance di sicurezza. Non è possibile modificare questa impostazione e si tratta di una limitazione del software. Il totale può essere solo 256. Se l'intervallo dell'insieme di indirizzi è maggiore di 253 indirizzi (ad esempio 254, 255, 256), la maschera di rete dell'interfaccia dell'appliance di sicurezza non può essere un indirizzo di classe C (ad esempio 255.255.255.0). Deve essere qualcosa di più grande, ad esempio 255.255.254.0.

Per informazioni su come implementare la funzionalità server DHCP nell'appliance di sicurezza, consultare la <u>guida alla configurazione della riga di comando di Cisco Security Appliance</u>.

Domande frequenti: Assegnazione indirizzo

Domanda: è possibile assegnare un indirizzo IP statico/permanente al computer che usa ASA come server DHCP?

Risposta - Non è possibile utilizzare PIX/ASA.

Domanda: è possibile associare gli indirizzi DHCP a indirizzi MAC specifici sull'appliance ASA?

Risposta-No, non è possibile .

Informazioni correlate

- Pagina di supporto per PIX Security Appliance
- <u>Riferimenti per i comandi di Cisco Secure PIX Firewall</u>
- Documentazione e supporto tecnico Cisco Systems