PIX/ASA als voorbeeld van een DHCP-server en clientconfiguratie

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten Conventies Configureren DHCP-serverconfiguratie met ASDM DHCP-clientconfiguratie met ASDM **DHCP-serverconfiguratie DHCP-clientconfiguratie** Verifiëren Problemen oplossen Opdrachten voor probleemoplossing Foutberichten FAQ: Toewijzing van adres Gerelateerde informatie

Inleiding

De PIX 500 Series security applicatie en Cisco adaptieve security applicatie (ASA) ondersteunen die werken als Dynamic Host Configuration Protocol (DHCP)-servers en DHCP-clients. DHCP is een protocol dat automatische configuratieparameters zoals een IP-adres met een subnetmasker, standaardgateway, DNS-server en WINS server IP-adres aan hosts levert.

De security applicatie kan fungeren als een DHCP-server of een DHCP-client. Wanneer het als een server werkt, verstrekt de Security applicatie netwerkconfiguratieparameters direct aan DHCP-clients. Wanneer het als een DHCP-client werkt, vraagt de Security applicatie dergelijke configuratieparameters vanaf een DHCP-server.

Dit document concentreert zich op de manier waarop u de DHCP-server en DHCP-client kunt configureren met behulp van Cisco Adaptieve Security Devices Manager (ASDM) op de Security applicatie.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de PIX security applicatie of ASA volledig gebruiksklaar is en geconfigureerd om Cisco ASDM in staat te stellen om configuratiewijzigingen door te voeren.

Opmerking: Raadpleeg <u>HTTPS Access voor ASDM</u> om het apparaat door ASDM te laten configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- PIX 500 Series security applicatie 7.x**Opmerking:** De PIX CLI-configuratie gebruikt in versie 7.x is ook van toepassing op PIX 6.x. Het enige verschil is dat in versies eerder dan PIX 6.3 de DHCP-server alleen op de interne interface ingeschakeld kan worden. In PIX 6.3 en later kan de DHCP-server worden ingeschakeld op een van de beschikbare interfaces. In deze configuratie wordt de externe interface gebruikt voor de DHCP-serverfunctie.
- ASDM 5.xOpmerking: ASDM ondersteunt PIX 7.0 en hoger. PIX Apparaat Manager (PDM) is beschikbaar om PIX versie 6.x te configureren. Raadpleeg <u>Cisco ASA 5500 Series en PIX</u> <u>500 Series security applicatie, hardware en software-compatibiliteit</u> voor meer informatie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco ASA 7.x.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

In deze configuratie zijn er twee PIX security applicaties die versie 7.x uitvoeren. Een functioneert als een DHCP-server die configuratieparameters biedt voor een andere PIX security applicatie 7.x die werkt als een DHCP-client. Wanneer het als een DHCP-server functioneert, kent PIX dynamisch IP-adressen toe aan DHCP-clients vanuit een pool van aangewezen IP-adressen.

U kunt een DHCP-server configureren op elke interface van de security applicatie. Elke interface kan een eigen pool van adressen hebben om uit te tekenen. Maar de andere DHCP-instellingen, zoals DNS-servers, domeinnaam, opties, ping-out en WINS-servers worden mondiaal geconfigureerd en op alle interfaces gebruikt door de DHCP-server.

U kunt geen DHCP-client of DHCP-relais instellen op een interface waarop de server is ingeschakeld. Daarnaast moeten DHCP-clients rechtstreeks worden aangesloten op de interface waarop de server is ingeschakeld.

Tenslotte, terwijl de DHCP-server op een interface is ingeschakeld, kunt u het IP-adres van die interface niet wijzigen.

Opmerking: Er is eigenlijk geen configuratieoptie om het standaardgateway-adres in het DHCPantwoord in te stellen dat vanuit de DHCP-server (PIX/ASA) wordt verzonden. De DHCP-server stuurt altijd zijn eigen adres als gateway voor de DHCP-client. Echter, het bepalen van een standaardroute die aan de router van Internet wijst staat de gebruiker toe om het internet te bereiken.

Opmerking: Het aantal DHCP-pooladressen dat kan worden toegewezen, is afhankelijk van de licentie die wordt gebruikt in de Security Appliance (PIX/ASA). Als u de Base/Security Plus-licentie gebruikt, gelden deze limieten voor de DHCP-pool. Als de Host Limiet 10 hosts is, beperkt u de DHCP-pool tot 32 adressen. Als de Host Limiet 50 hosts is, beperkt u de DHCP-pool tot 128 adressen. Als de Host Limiet onbeperkt is, beperkt u de DHCP-pool tot 256 adressen. De adrespool is dus beperkt op basis van het aantal hosts.

Opmerking: Gebruik het <u>Opname Gereedschap</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Dit document gebruikt deze configuraties:

- DHCP-serverconfiguratie met ASDM
- <u>DHCP-clientconfiguratie met ASDM</u>
- <u>DHCP-serverconfiguratie</u>
- <u>DHCP-clientconfiguratie</u>

DHCP-serverconfiguratie met ASDM

Voltooi deze stappen om de PIX security applicatie of ASA te configureren als een DHCP-server met ASDM.

 Kies Configuration > Properties > DHCP-services > DHCP-server vanuit het Home venster. Selecteer een interface en klik op Bewerken om de DHCP-server in te schakelen en om een DHCP-adrespool te maken.Het adrestoewijzing moet op hetzelfde net zijn als de interface voor security applicatie. In dit voorbeeld wordt de DHCP-server ingesteld op de externe interface van de PIX security applicatie.

Elico ASDM	5.1 for PIX - 10.0.0.1 Such Options Table Mizards	Heln					1202	<u>_ 0 ×</u>
Home	Configuration Montoring	Back For	ward Search	Q Retresh	Save	? Ныр	CI	SCO SYSTEMS
Interfaces Interfaces Security Policy NAT VPN Southing Global Objects Properties	Configuration + Properties + D Configuration + Properties + D Configuration + Properties + D Configuration + Second Configuration + Second Config	HCP Services	DHCP Server	Adds on interface: auses the DF e values in th	ess Pool outside ICP server to e fields below Primary W Secondar	Edit Ping Timeor Lease Leng automatically config takes precedence of NNS Server: VMINS Server: VMINS Server:	ut: 50 th: 3800 ure DNS, WINt over the Advant	ms secs 3 and

 Controleer DHCP-server op de buiteninterface inschakelen om naar de verzoeken van de DHCP-clients te luisteren. Geef het pool van adressen op die aan de DHCP-client moeten worden verstrekt en klik op OK om naar het hoofdvenster terug te keren.

Edit DHCP Server			2
Interface: outside			
Enable DHCP serve	r		
DHCP Address Pool:	192.168.1.5	to 192.168.1.7	
ОК	Cancel	Help	

 Controleer de automatische configuratie van de interface in staat om de DHCP-server ertoe te brengen automatisch de DNS, WINS en de standaard Domain Name te configureren voor de DHCP-client. Klik op Toepassen om de actieve configuratie van het apparaat bij te werken.

Cisco ASDM 5.	l for PTX - 10.0.0.1		
File Rules Be	arch Options Tools Wizard	ts Help	
Home C	onfiguration Montering	O Q Q Q 37	Cisco Systems
Fome C	Configuration > Properties > 0 Configuration > Properties > 0 Configuration > Properties > 0 Configuration > Properties > 0 Configuration > Configuration Configuration > Configuration Configuration Configuration > Configuration Configuration Configuration > Configuration Configuration Configuration > Configuration Configuration Configuration > Configuration Configuration Configuration > Configuration Configuration Configuration > Configuration Configuration > Configuration > Configuration Configuration > Configuration > Configu	DHCP Services > DHCP Server PHCP Services > DHCP Enabled Address Pool Interface DHCP Server Interface DHCP Server Interface DHCP Enabled Address Pool Edit Inside No Outside Yes 192.160.1.5 - 192.160.1.7 Ping Timeout: 50 Lease Length: 3600 Other DHCP Options Image: Configuration on interface; Outside Yes Enabling auto-configuration causes the DHCP server to automatically configure DNS, V The default domain name. The values in the fields below takes precedence over the autoconfigured values. DNS Server 1: 192.168.0.1 DNS Server 2: Secondary WINS Server: Domain Name: Addition Apply Reset	ms secs VIIVS and

DHCP-clientconfiguratie met ASDM

Voltooi deze stappen om de PIX security applicatie als een DHCP-client te configureren met ASDM.

 Kies Configuratie > Interfaces en klik op Bewerken om de Ethernet0 interface in staat te stellen om de configuratieparameters zoals een IP-adres te verkrijgen met een subnetmasker, standaardgateway, DNS-server en IP-adres van WINS-server van de DHCPserver.

Cisco ASDM	5.1 for PIX - 10.0.0.14							
File Rules S	earch Options Tools Wizards	s Help						
Home	Configuration Monitoring	Back Forwa	rd Search	Refresh	Save Help			Cisco Systems
	Configuration = Interfaces							
Interfaces	● 主 筆 ■ ① ※ 8		9					
Security Policy	Interface	Name Ena	abled Security Level	IP Address	Subnet Mask	Management Only	MTU	Add
24	Ethernet0		No C	i i	Ĩ.	No		Edit
NAT	Ethemet1	inside Y	'es 100	010.0.0.14	255.0.0.0	No 1	500	Delete
23	Ethemet2	1	No			No		
VPN	Ethemet3	1	No	1		No		
*28	Ethernet4	1	No			No	_	
Routing	Ethernet5	1	No			No		
8			1				_	
Global Objects								
5								
Properties								
	1						Þ	
	Enable traffic between M	ro or more interfac	ces which are c	onfigured with sa	ame security levels			
			Aaply	Re	eset			
			Aoply	R	eset			

2. Controleer Interface inschakelen en voer het niveau Interface Name en Security in voor de interface. Kies Adres via DHCP voor het IP-adres en verkrijg de standaardroute met DHCP voor de standaardgateway en klik vervolgens op OK om naar het hoofdvenster te gaan.

lardware Port:	Ethernet0	Configure Hardware Propertie
Enable Interface	Dedicate this interface	to management only
nterface Name:	outside	
ecurity Level:	0	
IP Address	· · · · · · · · · · · · · · · · · · ·	
C Use Static IP 🤇	Obtain Address via DH0	2P
		and the second
The interface au	itomatically gets its IP address	s using DHCP.
The interface au	Itomatically gets its IP address	s using DHCP. Renew DHCP Lease
The interface au	Itomatically gets its IP address	s using DHCP. Renew DHCP Lease
The interface au	Itomatically gets its IP address	s using DHCP. Renew DHCP Lease
The interface au	Itomatically gets its IP address It route using DHCP 1500	s using DHCP. Renew DHCP Lease
The interface au Obtain defau ITU: Description:	Itomatically gets its IP address It route using DHCP	s using DHCP. Renew DHCP Lease

3. Klik op **Toepassen** om het IP-adres voor de Ethernet0-interface te bekijken op de DHCPserver.

ome Con	figuration Montoring onfiguration > Interface	Bac S	k For	ward	Search Refresh	Save Help	_	_	itlltion
erfaces	* £ ¥ 🖬 🗊	8 B C	66	9					
Lanty Policy	Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTI	Add
23.0	Ethernet0	outside	Yes	đ	192.168.1.5 (DHCP)	255.255.255.0 (DHCP	No	1500	Edit
NAT	Ethemet1	inside	Yes	100	10.0.0.14	255.0.0.0	No.	1500	Delete
9	Ethernet5		No				No		
VPN	Ethernet3		No				No		
- <u>*</u>	Ethemet2		No				No		
touting	Ethemet4		No				No	_	
al Objects	4							Þ	

DHCP-serverconfiguratie

Deze configuratie wordt gemaakt door de ASDM:

DHCP-server
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
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
!
<i>! Output is suppressed.</i> 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
```

DHCP-clientconfiguratie

Deze configuratie wordt gemaakt door de 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

Verifiëren

Voltooi deze stappen om de DHCP-statistieken en de bindende informatie van de DHCP-server en DHCP-client te controleren met behulp van ASDM.

 Kies Controle > Interfaces > DHCP > Statistieken van DHCP van de server van DHCP om de statistieken van DHCP te verifiëren, zoals DHCPCPDISCOVER, DHCPREQUEST, DHCPOFFER, en DHCPACK.Voer de opdracht Statistieken van de show dhcpd in van de CLI om de DHCP-statistieken te



 Kies Monitoring > Interfaces > DHCP > DHCP-clientleaseinformatie van de DHCP-client om de DHCP-bindende informatie te bekijken.Voer de opdracht dhcpd-binding in om de DHCPbindingsinformatie uit de CLI te bekijken.

File Referes Desch Desch <t< th=""></t<>
Image: Configuration Image: Configuration <th< th=""></th<>
Monitoring > Interfaces > DHCP > DHCP Client Lease Information Image: Select a DHCP Client Lease Information Image: Select a DHCP Statistics Image: Select a DHCP Statistics Image: Select a DHCP Interface:
Temp default-gateway addr: 192.168.1.1 Next timer fires after: 1486 seconds Retry count: 0 Client-ID: cisco-0015.fa56.f046-outside-pixf Proxy: FALSE Hostname: pixfirewall Refresh
Data Refreshed Successfully. Admin> NA (15)

3. Kies **Monitoring > Vastlegging > Realtime logvenster** om het Logging Level en de bufferlimiet te selecteren voor het weergeven van de realtime logberichten.

盾 Cisco ASDM	5.1 for PIX - 10.0.0.14					_ D ×
File Rules B	Bearch Options Tools V	Vizards Help				
G Home	Centiguration Monitorin	ng Back f	orward Search	Refresh Save		Cisco Systems
Interfaces VPN	Menitoring > Logging > T ■ Real-time Log Vie ■ Log Buffer	Resi-time Log View Internet in the second se	er Log Viewer Click the View button bel Select the desired loggin Logging Level: Buffer Limit	ow to start displayin ig level to see mess Debugging 1000 View	ng syslog mess sages at that se	ages in real time. verity or higher.

4. Bekijk de real-time loggebeurtenissen van de DHCP-client. Het IP-adres wordt toegewezen voor de externe interface van de DHCP-

C	IDI	nt
		π.

🙍 Real-t	ime Log Yiewer	
00 Pau	se 🔄 🔜 Save 🖙 Cle	ar 📓 Color Bettings 🔹 Create Rule 📓 Show Rule Find: 🔍 🔍 🕅 Help
Filter By	-Show All-	ille final
Severity	Time	Message ID: Description
<u>a</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>é</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)
6 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>6</u> 6	Jan 01 1993 00:42:32	725007: SSL session with client inside:10.0.0.2/1524 terminated.
<u>k</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"
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 (fc: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 If: 10.0.0.14/443 duration 0:00:08 bytes 1695 TCP FI
<u>1</u> 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 1p address dhop setroute' command.
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: Tearding UDP connection 79 for outside: 10.0.0.2/68 to NP Identity IIC.255.255.255/97 duration 0:02:03 bytes 248
6	Jan 01 1993 00:42:24	1604101: DHCP client interface outside: Allocated ip = 192.168.1.5, mask = 255.255.255.0, gw = 192.168.1.1
6 6	Jan 01 1993 00:42:24	664102 DHCP client interface outside: address released
8.5	Jan 01 1993 00:42:24	111008: User 'enable_15' executed the intenace Einemer of command.
5	Jan 01 1993 00:42:24	111007: Begin configuration: 10.0.0.2 reading from http [POST]
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	Jan 01 1993 00:42:24	725001: Starting SSL handshake with client inside:10.0.0.2/1523 for TLSv1 session.
6 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

Problemen oplossen

Opdrachten voor probleemoplossing

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg <u>Belangrijke informatie over debug Commands</u> voordat u **debug**opdrachten gebruikt.

- debug dhcpd gebeurtenis-displays die wordt gekoppeld aan de DHCP-server.
- debug HD-pakket—Hier wordt pakketinformatie weergegeven die met de DHCP-server is gekoppeld.

Foutberichten

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

Uitleg: De omvang van de adrespool is beperkt tot 256 adressen per pool op het beveiligingsapparaat. Dit kan niet worden gewijzigd en is een softwarebeperking. Het totaal kan slechts 256 zijn. Als het bereik van de adrespool groter is dan 253 adressen (bijvoorbeeld 254, 255, 256), kan het netmasker van de interface van het veiligheidsapparaat geen Klasse C adres zijn (bijvoorbeeld 255.255.255.0). Het moet iets groters zijn, bijvoorbeeld 255.255.254.0.

Raadpleeg de <u>Cisco Security Opdracht Line Configuration</u> voor <u>Cisco-applicatie</u> voor informatie over het implementeren van de DHCP-serverfunctie in het beveiligingsapparaat.

FAQ: Toewijzing van adres

Vraag-Is het mogelijk om een statisch/permanent IP adres aan de computer toe te wijzen die ASA als DHCP-server gebruikt?

Antwoord: Het is niet mogelijk om PIX/ASA te gebruiken.

Vraag-Is het mogelijk om DHCP-adressen aan specifieke MAC-adressen op ASA te verbinden?

Antwoord: Nee, het is niet mogelijk.

Gerelateerde informatie

- Ondersteuning van PIX-security applicatie
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Technische ondersteuning en documentatie Cisco Systems