Konfigurationsbeispiel für einen DHCP-Server und einen Client mit PIX/ASA

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Konventionen Konfigurieren DHCP-Serverkonfiguration mit ASDM **DHCP-Client-Konfiguration mit ASDM DHCP-Serverkonfiguration DHCP-Client-Konfiguration** Überprüfen Fehlerbehebung Befehle zur Fehlerbehebung Fehlermeldungen Häufig gestellte Fragen: Adressenzuweisung Zugehörige Informationen

Einführung

Die Sicherheitslösung der Serie PIX 500 und die Cisco Adaptive Security Appliance (ASA) unterstützen sowohl als DHCP-Server (Dynamic Host Configuration Protocol) als auch als DHCP-Clients. DHCP ist ein Protokoll, das automatisch Konfigurationsparameter wie eine IP-Adresse mit einer Subnetzmaske, einem Standard-Gateway, einem DNS-Server und einer IP-Adresse des WINS-Servers für Hosts bereitstellt.

Die Sicherheits-Appliance kann als DHCP-Server oder DHCP-Client fungieren. Wenn die Sicherheits-Appliance als Server fungiert, stellt sie Netzwerkkonfigurationsparameter direkt für DHCP-Clients bereit. Wenn die Sicherheits-Appliance als DHCP-Client betrieben wird, werden diese Konfigurationsparameter von einem DHCP-Server angefordert.

In diesem Dokument wird erläutert, wie der DHCP-Server und der DHCP-Client mithilfe des Cisco Adaptive Security Device Manager (ASDM) auf der Security Appliance konfiguriert werden.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die PIX Security Appliance oder ASA voll betriebsbereit und konfiguriert ist, damit der Cisco ASDM Konfigurationsänderungen vornehmen kann.

Hinweis: Unter <u>Zulassen von HTTPS-Zugriff für ASDM</u> wird die Konfiguration des Geräts durch den ASDM beschrieben.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Security Appliance der Serie PIX 500 7.xHinweis: Die in Version 7.x verwendete PIX-CLI-Konfiguration gilt auch für PIX 6.x. Der einzige Unterschied besteht darin, dass der DHCP-Server in Versionen vor PIX 6.3 nur auf der internen Schnittstelle aktiviert werden kann. In PIX 6.3 und höher kann der DHCP-Server auf allen verfügbaren Schnittstellen aktiviert werden. In dieser Konfiguration wird die externe Schnittstelle für die DHCP-Serverfunktion verwendet.
- ASDM 5.xHinweis: ASDM unterstützt nur PIX 7.0 und höher. Der PIX Device Manager (PDM) ist für die Konfiguration der PIX-Version 6.x verfügbar. Weitere Informationen zur Hardwareund Softwarekompatibilität von Sicherheitsgeräten der Serien Cisco ASA 5500 und PIX 500 finden Sie.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit Cisco ASA 7.x verwendet werden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In dieser Konfiguration gibt es zwei PIX Security Appliances, die Version 7.x ausführen. Ein Server fungiert als DHCP-Server, der Konfigurationsparameter für eine andere PIX Security Appliance 7.x bereitstellt, die als DHCP-Client fungiert. Wenn es als DHCP-Server fungiert, weist das PIX DHCP-Clients aus einem Pool von zugewiesenen IP-Adressen dynamisch IP-Adressen zu.

Sie können auf jeder Schnittstelle der Sicherheits-Appliance einen DHCP-Server konfigurieren. Jede Schnittstelle kann über einen eigenen Adresspool verfügen, aus dem Sie schöpfen können. Die anderen DHCP-Einstellungen wie DNS-Server, Domänenname, Optionen, Ping-Timeout und WINS-Server werden jedoch global konfiguriert und vom DHCP-Server auf allen Schnittstellen verwendet.

Sie können einen DHCP-Client oder DHCP-Relay-Dienste nicht auf einer Schnittstelle

konfigurieren, auf der der Server aktiviert ist. Zusätzlich müssen DHCP-Clients direkt mit der Schnittstelle verbunden werden, auf der der Server aktiviert ist.

Während der DHCP-Server auf einer Schnittstelle aktiviert ist, können Sie die IP-Adresse dieser Schnittstelle nicht ändern.

Hinweis: Grundsätzlich gibt es keine Konfigurationsoption, um die Standard-Gateway-Adresse in der DHCP-Antwort festzulegen, die vom DHCP-Server (PIX/ASA) gesendet wird. Der DHCP-Server sendet immer seine eigene Adresse als Gateway für den DHCP-Client. Durch die Definition einer Standardroute, die auf den Internet-Router verweist, kann der Benutzer jedoch auf das Internet zugreifen.

Hinweis: Die Anzahl der DHCP-Pool-Adressen, die zugewiesen werden können, hängt von der in der Security Appliance (PIX/ASA) verwendeten Lizenz ab. Wenn Sie die Base/Security Plus-Lizenz verwenden, gelten diese Beschränkungen für den DHCP-Pool. Wenn der Host-Grenzwert 10 Hosts beträgt, beschränken Sie den DHCP-Pool auf 32 Adressen. Wenn der Host-Grenzwert 50 Hosts beträgt, beschränken Sie den DHCP-Pool auf 128 Adressen. Wenn das Hostlimit unbegrenzt ist, beschränken Sie den DHCP-Pool auf 256 Adressen. Daher ist der Adresspool abhängig von der Anzahl der Hosts begrenzt.

Hinweis: Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

In diesem Dokument werden folgende Konfigurationen verwendet:

- DHCP-Serverkonfiguration mit ASDM
- DHCP-Client-Konfiguration mit ASDM
- DHCP-Serverkonfiguration
- DHCP-Client-Konfiguration

DHCP-Serverkonfiguration mit ASDM

Führen Sie diese Schritte aus, um die PIX Security Appliance oder ASA als DHCP-Server mithilfe von ASDM zu konfigurieren.

 Wählen Sie im Hauptfenster Konfiguration > Eigenschaften > DHCP-Dienste > DHCP-Server aus. Wählen Sie eine Schnittstelle aus, und klicken Sie auf Bearbeiten, um den DHCP-Server zu aktivieren und einen DHCP-Adresspool zu erstellen.Der Adresspool muss sich im gleichen Subnetz wie die Security Appliance-Schnittstelle befinden. In diesem Beispiel wird der DHCP-Server auf der externen Schnittstelle der PIX Security Appliance konfiguriert.

| Home Configuration Monitoring | O O Q O Refresh Save Help | CISCO SYSTEM |
|---|---|---|
| Image: Security Policy Image: Security Poli | HCP Services > DHCP Server Interface DHCP Enabled Address Pool Interface No Ping Tin Lease L Other DHCP Options Image: Second and the second | reout: 50 mis ength: 3600 secs nfigure DNS, WINS and ce over the Advanced |

 Aktivieren Sie DHCP-Server auf der externen Schnittstelle aktivieren, um die Anfragen der DHCP-Clients zu überwachen. Geben Sie den Adresspool an, der dem DHCP-Client zugewiesen werden soll, und klicken Sie auf OK, um zum Hauptfenster zurückzukehren.

| Edit DHCP Server | | | > |
|---------------------|-------------|----------------|---|
| Interface: outside | | | |
| Finable DHCP server | | | |
| DHCP Address Pool: | 192.168.1.5 | to 192.168.1.7 | |
| | | | |
| OK | Cancel | Help | E |

3. Aktivieren Sie **die Option Autokonfiguration auf der Schnittstelle aktivieren**, damit der DHCP-Server den DNS, WINS und den Standard-Domänennamen für den DHCP-Client automatisch konfiguriert. Klicken Sie auf **Apply**, um die aktuelle Konfiguration der Sicherheits-Appliance zu aktualisieren.

| Cisco ASDM 5 | 1 for PIX - 10.0.0.1 | | _ 0 × |
|---|--------------------------------|--|---------------|
| File Rules' 80 | arch Options Tools Wizard | s Help | |
| Sin Home | Configuration Montering | O O Q O Q Back Forward Search Refresh Save Help | Cisco Systems |
| Interfaces Security Policy NAT Security Policy NAT Security Policy NAT Security Realing Global Objects Properties | Configuration > Properties > D | HCP Services - DHCP Server Interface DHCP Enabled Address Pool Edit Inside No Edit Edit Inside No Edit Edit Inside No Edit Edit Outside Yes 192.160.1.5 - 192.160.1.7 Ping Timeout 50 Lease Length: 360 Enables auto-configuration on interface; Outside Image: Configuration causes the DHCP server to automatically configure DNS the default domain name. The values in the fields below takes precedence over the autoconfigured values. DNS Server 1 192.158.0.1 Primary WINS Server: 172.0.0.1 DNS Server 2: Secondary WINS Server: 7 Domain Name: 7 | MINS and |

DHCP-Client-Konfiguration mit ASDM

Führen Sie diese Schritte aus, um die PIX Security Appliance als DHCP-Client mithilfe von ASDM zu konfigurieren.

 Wählen Sie Configuration > Interfaces (Konfiguration > Schnittstellen) aus, und klicken Sie auf Edit, um die Ethernet0-Schnittstelle so zu aktivieren, dass sie die Konfigurationsparameter wie eine IP-Adresse mit Subnetzmaske, Standard-Gateway, DNS-Server- und WINS-Server-IP-Adresse vom DHCP-Server abruft.

| Cisco ASDM | 5.1 for PIX - 10.0.0.14 | | | | | | | • | |
|-----------------|-----------------------------|----------------|-----------|-------------------|------------------|------------------------|--------------------|------|---------------|
| File Rules S | earch Options Tools Wizards | Help | | | | | | | |
| Home | Configuration Mentioning | O Beck Fr | orward | Q Search | Refresh | Save Help | | | Cisco Systews |
| - | Configuration > Interfaces | | | | | | | | |
| Interfaces | ● 主 筆 ■ ① ※ 9 | 8 (B) (B) (B) | 5191 | | | | | | |
| Security Policy | Interface | Name | Enabled | Security Level | IP Address | Subnet Mask | Management Only | MTU | Add |
| 24 | Ethernet0 | | No | 0 | | T. | No | | Edit |
| NAT | Ethemet1 | inside | Yes | 100 | 10.0.0.14 | 255.0.0.0 | Ng | 1500 | Delete |
| | Ethemet2 | | No | | | | No | | |
| VPN | Ethernet3 | | No | | | | No | | |
| *** | Ethemet4 | | No | | | | No | | |
| Routing | Ethemet5 | | No | | | | No | | |
| 8 | | | | | | | | | |
| Global Objects | | | | | | | | | |
| 5 | | | | | | | | | |
| Properties | | | | | | | | | |
| | | | | | | | | | |
| | 1 | | | | | | | F | |
| | Enable institution by | o or provi int | offeries | hielo one er | antinumed with m | area e a curito levale | | | |
| | 1 Enable Dame Detween th | | Bilares M | Inch are ci | unngureu war sa | arrie security levels | | | |
| | | | | Apply | R | eset | | | |
| | | | - | | | | | | |

 Aktivieren Sie Enable Interface (Schnittstelle aktivieren), und geben Sie den Schnittstellennamen und die Sicherheitsstufe für die Schnittstelle ein. Wählen Sie Adresse über DHCP für die IP-Adresse beziehen und Standardroute über DHCP für das Standard-Gateway beziehen und klicken Sie dann auf OK, um zum Hauptfenster zu gelangen.

| lardware Port: | Ethernet0 | Configure Hardware Propertie |
|----------------------|---------------------------------|------------------------------|
| Z Enable Interface | Dedicate this interface to | o management only |
| iterface 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. |
| 🗹 Obtain defau | Ilt route using DHCP | Renew DHCP Lease |
| ITU: | Ilt route using DHCP | Renew DHCP Lease |
| ITU: rescription: | Ilt route using DHCP | Renew DHCP Lease |

3. Klicken Sie auf **Apply**, um die IP-Adresse anzuzeigen, die vom DHCP-Server für die Ethernet0-Schnittstelle abgerufen wurde.

| 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 | | × | |

DHCP-Serverkonfiguration

Diese Konfiguration wird vom ASDM erstellt:

DHCP-Server 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
```

DHCP-Client-Konfiguration

Diese Konfiguration wird vom ASDM erstellt:

```
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
is suppressed. ! service-policy global_policy global
Cryptochecksum:86dd1153e8f14214524359a5148a4989 : end
```

<u>Überprüfen</u>

Führen Sie diese Schritte aus, um die DHCP-Statistiken und die Bindungsinformationen vom DHCP-Server und DHCP-Client mithilfe von ASDM zu überprüfen.

 Wählen Sie Monitoring > Interfaces > DHCP > DHCP Statistics vom DHCP-Server aus, um die DHCP-Statistiken wie DHCPDISCOVER, DHCPREQUEST, DHCPOFFER und DHCPACK zu überprüfen.Geben Sie den Befehl show dhcpd statistics aus der CLI ein, um die DHCP-Statistiken



2. Wählen Sie Monitoring > Interfaces > DHCP > DHCP Client Lease Information (Überwachung > Schnittstellen > DHCP > DHCP Client Lease Information) vom DHCP-Client aus, um die DHCP-Bindungsinformationen anzuzeigen.Geben Sie den Befehl show dhcpd binding ein, um die DHCP-Bindungsinformationen aus der CLI

| Rules Be | Contiguration Tools Wizards | Help Back Forward Score | ch Refresh Se | an 🤗 | Cisco System |
|-----------|---|---|---|--|--------------|
| Iterfaces | Monitoring > Interfaces > DHCF ARP Table DHCP Server Table DHCP Server Table DHCP Client Leas Dynamic ACLs Dynamic ACLs Similaritace Graphs Similaritace Graphs Similaritace outside | DHCP Client Lease Inform DHCP Client Lease Inform Select a DH Temp IP ad Temp sub DHCP Least state: Lease: Renewal: Rebind: Temp defait Next timer ff Retry count Client-ID: Proxy: Hostname: | mation ation ICP Interface: OutSide Attribute Idr: net mask: se server: ult-gateway addr: fires after: : | e - 192.168.1.5 ▼ Value 192.168.1.5 255.255.255.0 192.168.1.1 Bound 3600 seconds 1800 seconds 1800 seconds 192.168.1.1 1486 seconds 0 cisco-0015.fa56.f046-outside-pit FALSE pixfirewall | м |
| | | | R | efresh | |

3. Wählen Sie **Monitoring > Logging > Real-time Log Viewer** aus, um die Protokollierungsebene und die Puffergrenze für die Anzeige der Real-Time Log-Meldungen auszuwählen.



4. Zeigen Sie die Echtzeit-Protokollereignisse vom DHCP-Client aus an. Die IP-Adresse ist der externen Schnittstelle des DHCP-Clients

zugewiesen.

| 💼 Real-t | ime Log Viewer 🚽 🛶 | |
|------------|----------------------|---|
| 00 Pau | ise 🛛 🔜 Save 😭 Cle | ar 📓 Color Bettings 🕼 Create Ruis 📓 Strow Rule Find: |
| Filter By | -Show All- | High Fill |
| Severity | Time | Message ID: Description |
| <u> </u> | 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>4</u> 6 | 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 SSL 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 SBL 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 1p address dhcp 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 |
| 1 6 | Jan 01 1993 00:42:25 | 609002: Teardown local-host NP Identity Ifc:255.255.255.255 duration 0:02:03 |
| 1 6 | Jan 01 1993 00:42:25 | 609002: Teardown local-host outside:10.0.0.2 duration 0:02:03 |
| <u> 6</u> | Jan 01 1993 00:42:25 | 302016: Tearning UDP serviced on 79 for outside 10.0.0 2/68 to HP identity in 255,255,255,255,256,254 autoin 0.02:03 bytes 246 |
| <u> </u> | Jan 01 1993 00:42:24 | T604101: DHCP client interface outside: Allocated ip = 192.168.1.5, mask = 255.255.0, gw = 192.168.1.1 |
| <u>*</u> 6 | 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 interact Enternet'u command. |
| 8.5 | Jan 01 1993 00:42:24 | 111007: Begin configuration: 10.0.0.2 reading from http [POST] |
| 1.6 | Jan 01 1993 00 42:24 | 605005 Login permitted from 10.0.0.27523 to inside:10.0.14/https for user 'enable_15' |
| 1.6 | Jan 01 1993 00:42:24 | 725002 Device completed SSL handshake with client inside 10.0 0.21523 |
| 1 0 | Jan 01 1993 00:42:24 | (25001) Starting SBL handshake with client inside; 10.00.2/1523 for ILSVI session. |
| 1 0 | Jan 01 1993 00:42:24 | 302013: Built inbound TCP connection 88 for inside:10.002/15/23 (10.00.2/15/23) to NP (centry itc:10.00.14/443 (10.00.14/443) |
| 4 5 | Jan 01 1993 00:42:22 | 302015: Built outbound ODP connection 87 for outside:192.122.173.131/53 (192.122.173.131/53) to inside:10.0.0.2/1522 (10.0.0.2/1 |
| | | |
| H | | |
| | e Emergencies | 🗿 Alerts 🧶 Critical 🤨 Errors 🚖 Warnings 🗼 Notifications 🎄 Informational 📧 Debugging |

Fehlerbehebung

Befehle zur Fehlerbehebung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie <u>vor der</u> Verwendung von **Debug-**Befehlen die <u>Informationen</u> zu <u>Debug-</u><u>Befehlen</u>.

- debug dhcpd event (dhcpd-Ereignis debug): Zeigt Ereignisinformationen an, die dem DHCP-Server zugeordnet sind.
- debug dhcpd packet: Zeigt Paketinformationen an, die dem DHCP-Server zugeordnet sind.

Fehlermeldungen

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

Erläuterung: Die Größe des Adresspools ist auf 256 Adressen pro Pool auf der Sicherheits-Appliance beschränkt. Dies kann nicht geändert werden und ist eine Softwarebeschränkung. Die Gesamtzahl kann nur 256 betragen. Wenn der Adresspoolbereich größer als 253 Adressen ist (z. B. 254, 255, 256), darf die Netzmaske der Security Appliance-Schnittstelle keine Class C-Adresse sein (z. B. 255.255.255.0). Es muss etwas Größeres sein, zum Beispiel 255.255.254.0.

Weitere Informationen zur Implementierung der DHCP-Serverfunktion in die Sicherheits-Appliance finden Sie im <u>Cisco Security Appliance Command Line Configuration Guide</u>.

Häufig gestellte Fragen: Adressenzuweisung

Frage - Ist es möglich, dem Computer, der ASA als DHCP-Server verwendet, eine statische/permanente IP-Adresse zuzuweisen?

Antwort: PIX/ASA ist nicht möglich.

Frage - Ist es möglich, DHCP-Adressen mit bestimmten MAC-Adressen auf ASA zu verknüpfen?

Antwort: Nein, es ist nicht möglich.

Zugehörige Informationen

- <u>Support-Seite für PIX Security Appliance</u>
- <u>Cisco Secure PIX Firewall Befehlsreferenzen</u>
- <u>Technischer Support und Dokumentation Cisco Systems</u>