PIX/ASA: Führen Sie DNS Doctoring mit dem statischen Befehl und dem Konfigurationsbeispiel für zwei NAT-Schnittstellen durch.

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die DNS-Dokumentation (Domain Name System) auf der Adaptive Security Appliance der Serie ASA 5500 oder der Security Appliance der Serie PIX 500 unter Verwendung statischer NAT-Anweisungen (Network Address Translation). DNS Doctoring ermöglicht der Sicherheitsanwendung das Umschreiben von DNS A-Datensätzen.

DNS Rewrite führt zwei Funktionen aus:

- Übersetzt eine öffentliche Adresse (die routbare oder zugeordnete Adresse) in einer DNS-Antwort in eine private Adresse (die tatsächliche Adresse), wenn sich der DNS-Client auf

einer privaten Schnittstelle befindet.
- Übersetzt eine private Adresse in eine öffentliche Adresse, wenn sich der DNS-Client auf der öffentlichen Schnittstelle befindet.

Hinweis: Die Konfiguration in diesem Dokument enthält zwei NAT-Schnittstellen. innen und außen. Ein Beispiel für die DNS-Dokumentation mit Statistiken und drei NAT-Schnittstellen (innen, außen und dmz) finden Sie unter PIX/ASA: Führen Sie DNS Doctoring mit dem statischen Befehl und dem Konfigurationsbeispiel für drei NAT-Schnittstellen durch.

Unter PIX/ASA 7.x NAT- und PAT-Anweisungen und Verwenden von nat, global, statisch, für Kanäle und Zugriffslisten verwendeten Befehlen und Port Redirection (Weiterleitung) auf PIX finden Sie weitere Informationen zur Verwendung von NAT auf einer Security Appliance.

Voraussetzungen

Anforderungen

DNS Inspection muss aktiviert sein, um DNS-Doctoring auf der Sicherheits-Appliance durchzuführen. Die DNS-Überprüfung ist standardmäßig aktiviert. Wenn die Funktion deaktiviert wurde, lesen Sie den Abschnitt DNS-Prüfung konfigurieren weiter unten in diesem Dokument, um sie erneut zu aktivieren. Wenn die DNS-Überprüfung aktiviert ist, führt die Sicherheits-Appliance die folgenden Aufgaben aus:

- Übersetzt den DNS-Datensatz basierend auf der Konfiguration, die mithilfe der **statischen** und **nat**-Befehle (DNS-Umschreibung) abgeschlossen wurde. Die Übersetzung gilt nur für den A-Datensatz in der DNS-Antwort. Daher sind Reverse Lookups, die den PTR-Datensatz anfordern, von der DNS-Umschreibung nicht betroffen.**Hinweis:** DNS-Umschreibungen sind nicht mit der statischen Port Address Translation (PAT) kompatibel, da für jeden A-Datensatz mehrere PAT-Regeln gelten und die zu verwendende PAT-Regel mehrdeutig ist.
- Erzwingt die maximale Länge von DNS-Nachrichten (der Standardwert ist 512 Byte und die maximale Länge ist 65.535 Byte). Die Reassemblierung wird bei Bedarf durchgeführt, um sicherzustellen, dass die Paketlänge kleiner als die konfigurierte maximale Länge ist. Das Paket wird verworfen, wenn es die maximale Länge überschreitet.**Hinweis:** Wenn Sie den Befehl **inspect dns** ohne die Option maximum length ausgeben, wird die DNS-Paketgröße nicht überprüft.
- Erzwingt eine Domänennamenlänge von 255 Byte und eine Label-Länge von 63 Byte.
- Überprüft die Integrität des vom Zeiger angegebenen Domänennamens, wenn in der DNS-Nachricht Komprimierungspunkte auftreten.
- Überprüft, ob eine Komprimierungszeigerschleife vorhanden ist.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Security Appliance der Serie ASA 5500, Version 7.2(1).

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 Security Appliances der Serie PIX 500, Version 6.2 oder höher, verwendet werden.

Hinweis: Die ASDM-Konfiguration (Cisco Adaptive Security Device Manager) ist nur für Version 7.x verfügbar.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

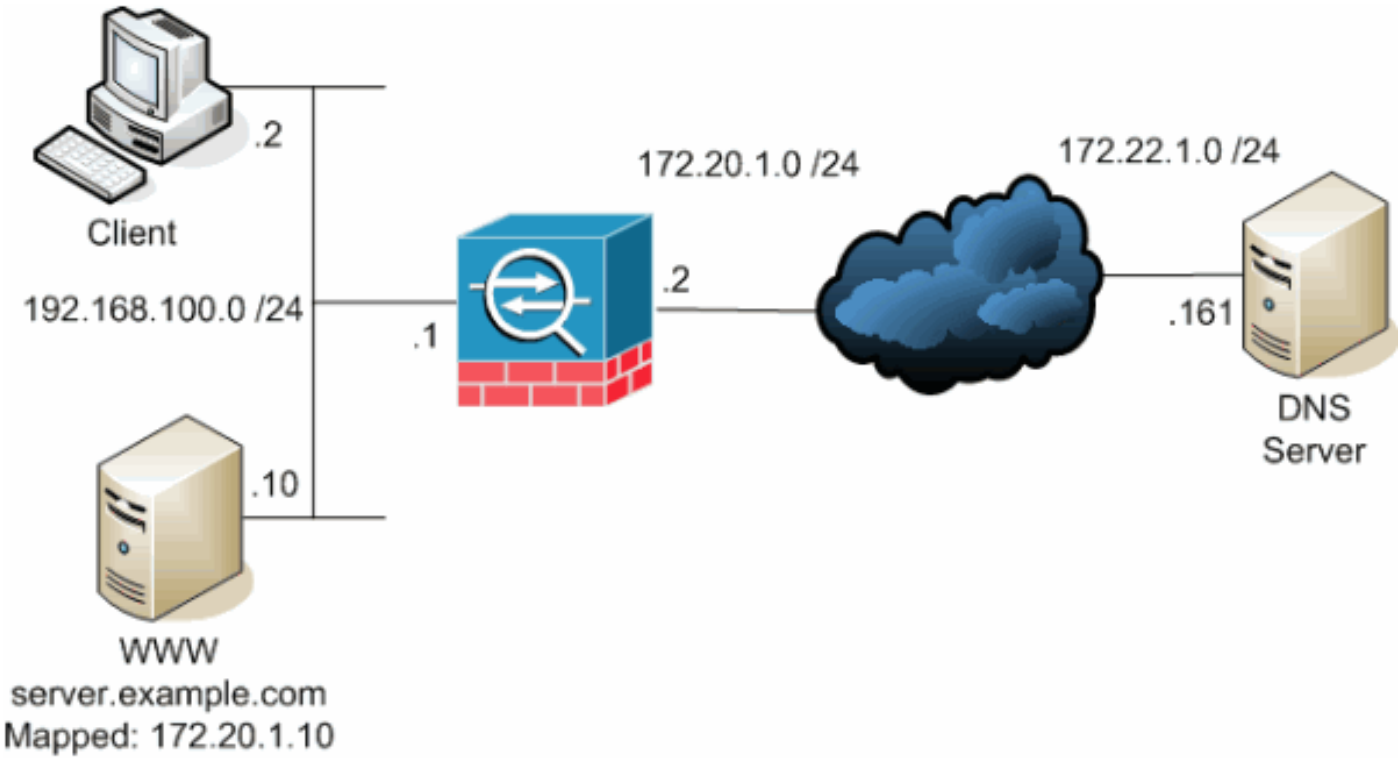
Hintergrundinformationen

Bei einem typischen DNS-Austausch sendet ein Client eine URL oder einen Hostnamen an einen DNS-Server, um die IP-Adresse dieses Hosts zu ermitteln. Der DNS-Server empfängt die Anforderung, sucht nach der Name-zu-IP-Adressenzuordnung für diesen Host und stellt dem Client dann den A-Datensatz mit der IP-Adresse zur Verfügung. Während dieses Verfahren in vielen Situationen gut funktioniert, können Probleme auftreten. Diese Probleme können auftreten, wenn der Client und der Host, auf den der Client zugreifen möchte, sich beide im gleichen privaten Netzwerk hinter NAT befinden, der vom Client verwendete DNS-Server sich jedoch in einem anderen öffentlichen Netzwerk befindet.

Szenario: Zwei NAT-Schnittstellen (innen, außen)

Topologie

In diesem Szenario befinden sich der Client und der WWW-Server, auf den der Client zugreifen möchte, beide auf der internen Schnittstelle der ASA. Dynamische PAT wird konfiguriert, um dem Client den Zugriff auf das Internet zu ermöglichen. Die statische NAT mit einer Zugriffsliste wird so konfiguriert, dass der Serverzugriff auf das Internet sowie der Zugriff von Internet-Hosts auf den WWW-Server ermöglicht wird.



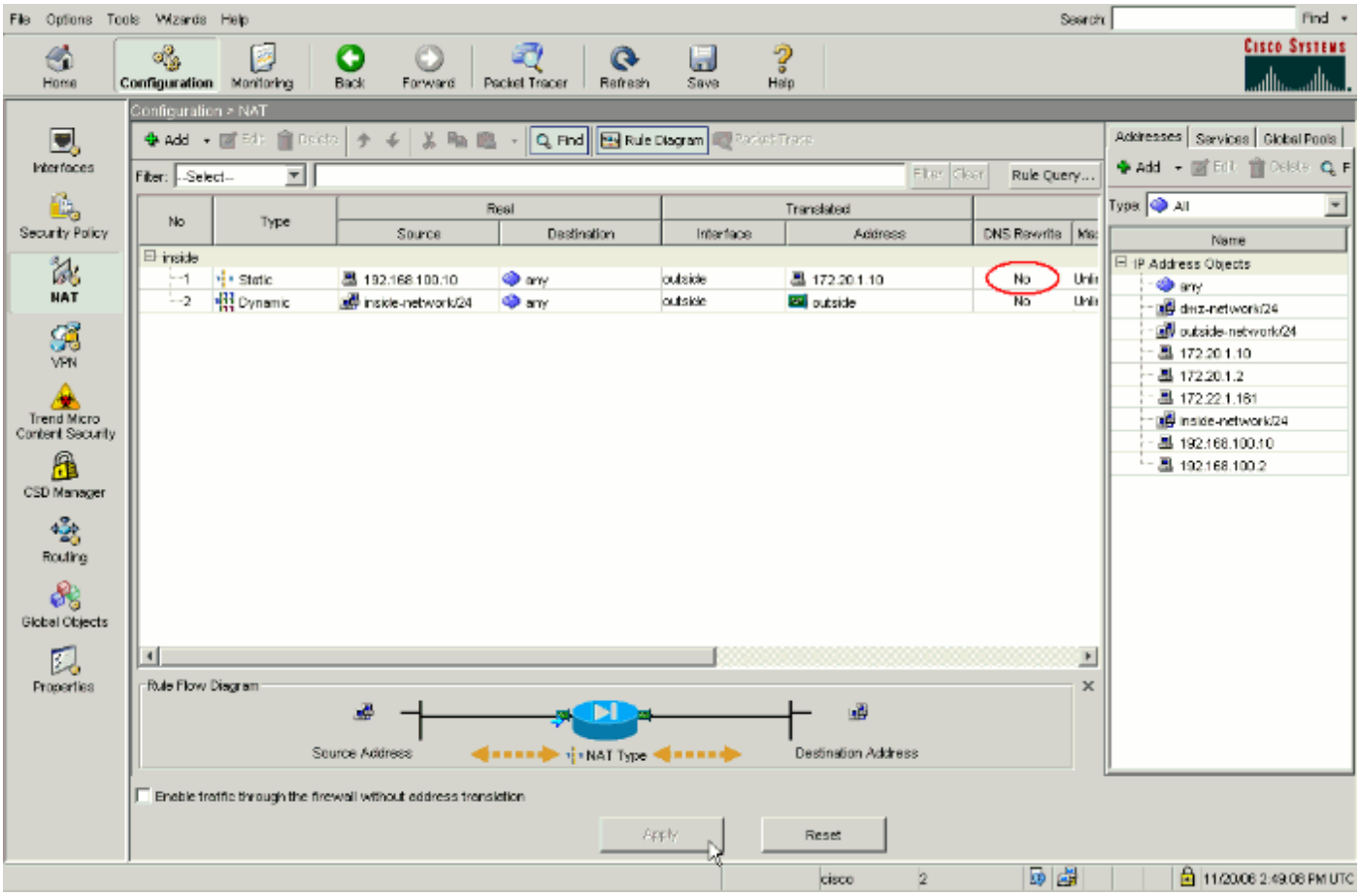
Dieses Diagramm ist ein Beispiel für diese Situation. In diesem Fall möchte der Client unter 192.168.100.2 die URL **server.example.com** für den Zugriff auf den WWW-Server unter 192.168.100.10 verwenden. DNS-Dienste für den Client werden vom externen DNS-Server unter 172.22.1.161 bereitgestellt. Da sich der DNS-Server in einem anderen öffentlichen Netzwerk befindet, kennt er die private IP-Adresse des WWW-Servers nicht. Stattdessen kennt sie die WWW-Server-zugeordnete Adresse 172.20.1.10. Somit enthält der DNS-Server die IP-Adresse-zu-Name-Zuordnung von **server.example.com** zu **172.20.1.10**.

Problem: Client kann nicht auf WWW-Server zugreifen

Wenn in dieser Situation DNS-Doctoring oder eine andere Lösung aktiviert ist und der Client eine DNS-Anforderung für die IP-Adresse von server.example.com sendet, kann er nicht auf den WWW-Server zugreifen. Der Client erhält einen A-Datensatz, der die zugeordnete öffentliche Adresse enthält: 172.20.1.10 des WWW-Servers. Wenn der Client versucht, auf diese IP-Adresse zuzugreifen, verwirft die Sicherheits-Appliance die Pakete, da sie keine Paketumleitung auf derselben Schnittstelle zulässt. Der NAT-Teil der Konfiguration sieht folgendermaßen aus, wenn die DNS-Dokumentation nicht aktiviert ist:

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa

!--- Output suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !---
Output suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 access-group OUTSIDE
in interface outside !--- Output suppressed.
```

So sieht die Konfiguration im ASDM aus, wenn die DNS-Dokumentation nicht aktiviert ist:



Es folgt eine Paketerfassung der Ereignisse, wenn die DNS-Dokumentation nicht aktiviert ist:

1. Der Client sendet die DNS-Abfrage.

```
No.     Time       Source           Destination       Protocol Info
1       0.000000   192.168.100.2    172.22.1.161      DNS      Standard query
                                                              A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
(00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 50879 (50879), Dst Port: domain (53)
Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x0004
    Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
```

2. PAT wird auf der DNS-Abfrage von der ASA ausgeführt, und die Abfrage wird weitergeleitet. Beachten Sie, dass die Quelladresse des Pakets auf die externe Schnittstelle der ASA geändert wurde.

```
No.     Time       Source           Destination       Protocol Info
1       0.000000   172.20.1.2       172.22.1.161      DNS      Standard query
```

```
                                                    A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22
(00:30:94:01:f1:22)
Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 1044 (1044), Dst Port: domain (53)
Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x0004
    Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
```

3. Der DNS-Server antwortet mit der zugeordneten Adresse des WWW-Servers.

```
No.     Time      Source          Destination       Protocol Info
2       0.005005  172.22.1.161    172.20.1.2        DNS      Standard query response
                                                             A 172.20.1.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e
(00:0a:b8:9c:c6:1e)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2
(172.20.1.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 1044 (1044)
Domain Name System (response)
    [Request In: 1]
    [Time: 0.005005000 seconds]
    Transaction ID: 0x0004
    Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
    Answers
        server.example.com: type A, class IN, addr 172.20.1.10
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 1 hour
            Data length: 4
            Addr: 172.20.1.10
```

4. Die ASA löscht die Übersetzung der Zieladresse der DNS-Antwort und leitet das Paket an den Client weiter. Beachten Sie, dass die Addr in der Antwort ohne DNS-Doctoring immer noch die zugeordnete Adresse des WWW-Servers ist.

```
No.     Time      Source          Destination         Protocol Info
2       0.005264  172.22.1.161    192.168.100.2       DNS      Standard query response
                                                              A 172.20.1.10
```

```
Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
(00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
(192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 50879 (50879)
Domain Name System (response)
    [Request In: 1]
    [Time: 0.005264000 seconds]
    Transaction ID: 0x0004
    Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
    Answers
        server.example.com: type A, class IN, addr 172.20.1.10
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 1 hour
            Data length: 4
            Addr: 172.20.1.10
```

5. An diesem Punkt versucht der Client, unter 172.20.1.10 auf den WWW-Server zuzugreifen. Die ASA erstellt für diese Kommunikation einen Verbindungseintrag. Da der Datenverkehr jedoch nicht von innen nach außen fließt, wird die Verbindung mit einem Timeout unterbrochen. Die ASA-Protokolle zeigen Folgendes:

```
%ASA-6-302013: Built outbound TCP connection 54175 for
outside:172.20.1.10/80 (172.20.1.10/80) to inside:192.168.100.2/11001
(172.20.1.2/1024)

%ASA-6-302014: Teardown TCP connection 54175 for outside:172.20.1.10/80 to
inside:192.168.100.2/11001 duration 0:00:30 bytes 0 SYN Timeout
```

Lösung: "dns"-Schlüsselwort

DNS Doctoring mit dem Schlüsselwort "dns"

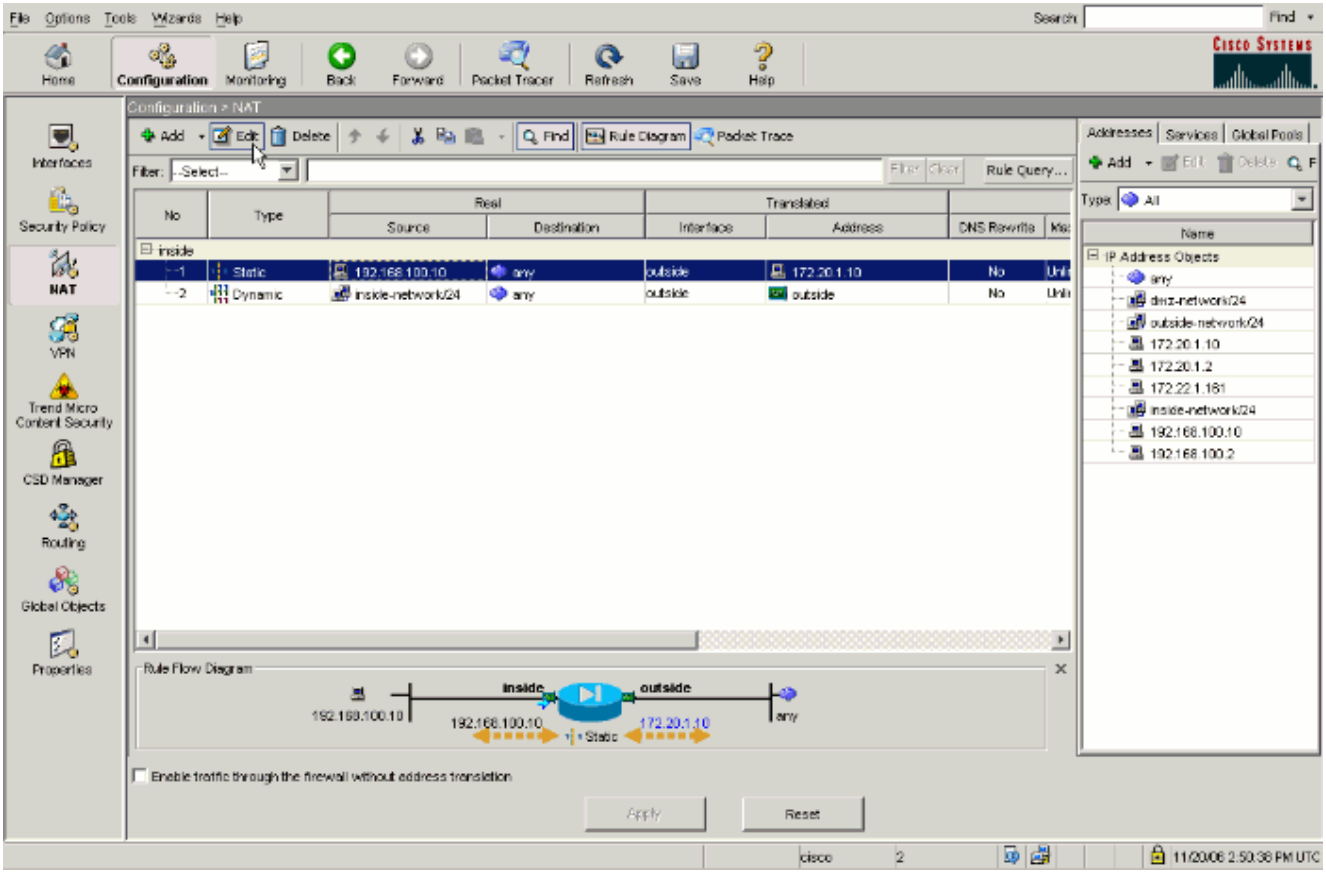
DNS-Doctoring mit dem **dns**-Schlüsselwort gibt der Sicherheitsappliance die Möglichkeit, den Inhalt der DNS-Serverantworten an den Client abzufangen und umzuleiten. Bei ordnungsgemäßer Konfiguration kann die Sicherheits-Appliance den A-Datensatz ändern, um den Client in einem im Problem beschriebenen Szenario zuzulassen: Der Client kann nicht auf den WWW-Server- Abschnitt zugreifen, um eine Verbindung herzustellen. In diesem Fall schreibt die Sicherheits-Appliance bei aktivierter DNS-Dokumentation den A-Datensatz um, um den Client auf **192.168.100.10** zu leiten, anstatt auf **172.20.1.10**. DNS-Doctoring ist aktiviert, wenn Sie das **dns**-Schlüsselwort zu einer statischen NAT-Anweisung hinzufügen. Der NAT-Teil der Konfiguration sieht folgendermaßen aus, wenn die DNS-Dokumentation aktiviert ist:

```
ciscoasa(config)#show run
```

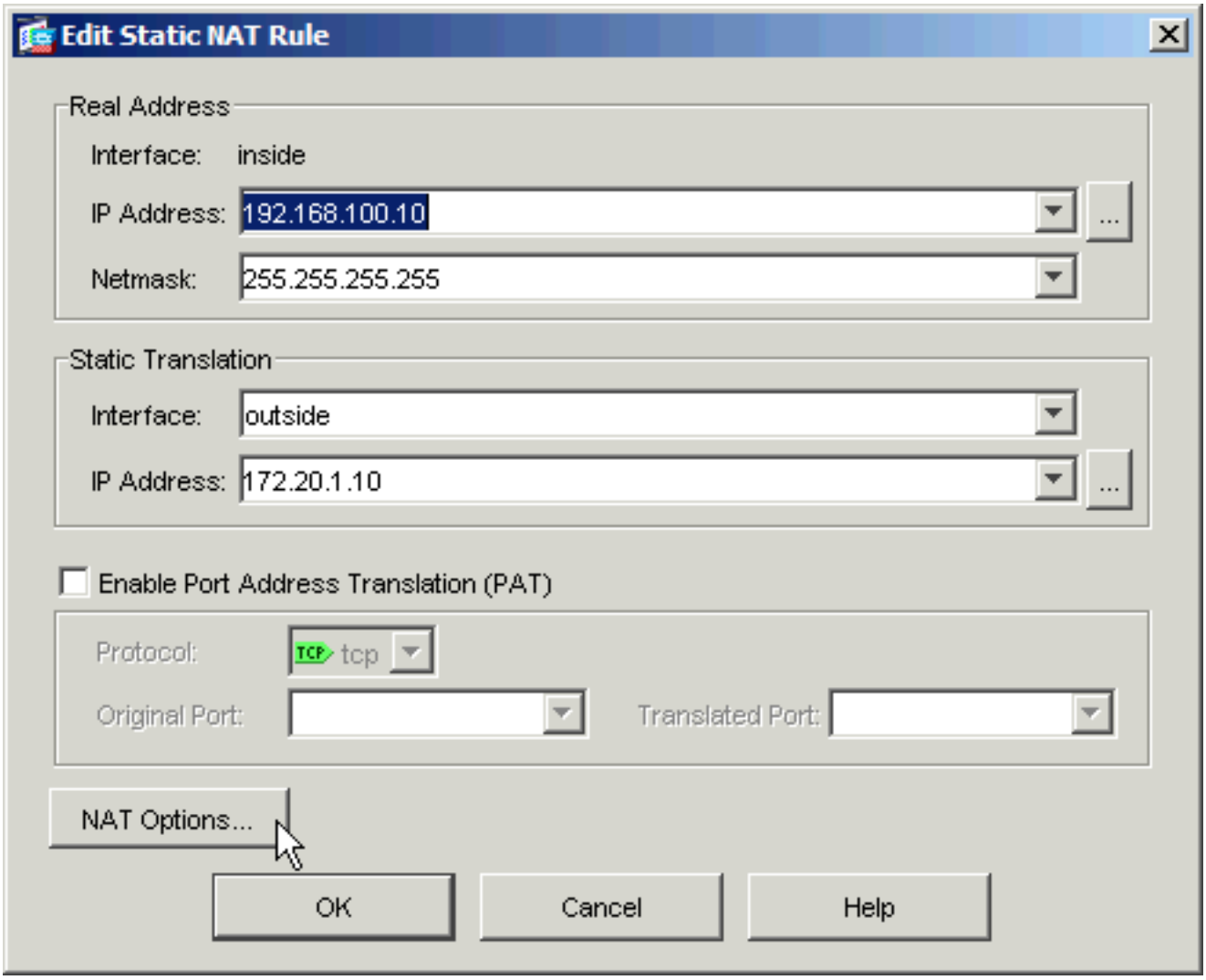
```
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa

!--- Output suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !---
Output suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 dns
!--- The "dns" keyword is added to instruct the security appliance to modify !--- DNS records
related to this entry. access-group OUTSIDE in interface outside !--- Output suppressed.
```

Gehen Sie wie folgt vor, um die DNS-Dokumentation im ASDM zu konfigurieren:

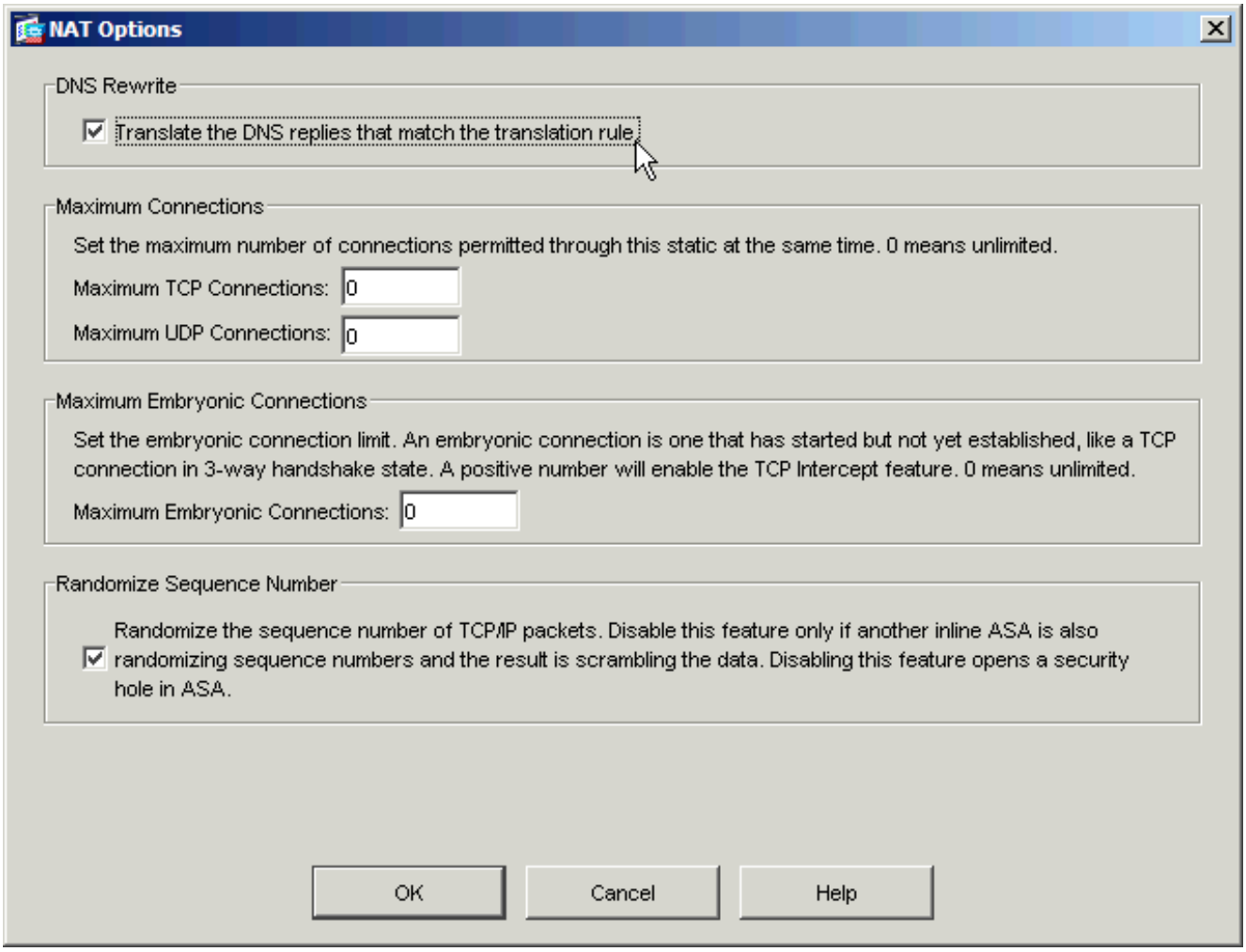
1. Navigieren Sie zu **Configuration > NAT**, und wählen Sie die zu ändernde statische NAT-Regel aus. Klicken Sie auf **Bearbeiten**.



2. Klicken Sie auf **NAT-Optionen...**.



3. Aktivieren Sie das Kontrollkästchen **DNS-Antworten übersetzen, die mit dem** Kontrollkästchen **Übersetzungsregel übereinstimmen**.



4. Klicken Sie auf **OK**, um das Fenster NAT-Optionen zu verlassen. Klicken Sie auf **OK**, um das Fenster "Edit Static NAT Rule" (Statische NAT-Regel bearbeiten) zu verlassen. Klicken Sie auf **Apply**, um Ihre Konfiguration an die Sicherheits-Appliance zu senden.

Im Folgenden finden Sie eine Paketerfassung der Ereignisse, wenn DNS-Doctoring aktiviert ist:

1. Der Client sendet die DNS-Abfrage.

```
No.     Time       Source           Destination        Protocol Info
1       0.000000   192.168.100.2    172.22.1.161       DNS      Standard query
                                                       A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
(00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 52985 (52985), Dst Port: domain (53)
Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x000c
    Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
```

2. PAT wird auf der DNS-Abfrage von der ASA ausgeführt, und die Abfrage wird weitergeleitet. Beachten Sie, dass die Quelladresse des Pakets auf die externe Schnittstelle der ASA geändert wurde.

```
No.     Time      Source           Destination         Protocol Info
1       0.000000  172.20.1.2       172.22.1.161        DNS      Standard query
                                                               A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22
(00:30:94:01:f1:22)
Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 1035 (1035), Dst Port: domain (53)
Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x000c
    Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
```

3. Der DNS-Server antwortet mit der zugeordneten Adresse des WWW-Servers.

```
No.     Time      Source           Destination       Protocol Info
2       0.000992  172.22.1.161     172.20.1.2        DNS      Standard query response
                                                               A 172.20.1.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e
(00:0a:b8:9c:c6:1e)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2
(172.20.1.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 1035 (1035)
Domain Name System (response)
    [Request In: 1]
    [Time: 0.000992000 seconds]
    Transaction ID: 0x000c
    Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
    Answers
        server.example.com: type A, class IN, addr 172.20.1.10
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 1 hour
            Data length: 4
            Addr: 172.20.1.10
```

4. Die ASA löscht die Übersetzung der Zieladresse der DNS-Antwort und leitet das Paket an

den Client weiter. Beachten Sie, dass bei aktivierter DNS-Dokumentation die **Addr** in der Antwort als reale Adresse des WWW-Servers umgeschrieben wird.

```
No.     Time      Source          Destination        Protocol Info
2       0.001251  172.22.1.161    192.168.100.2      DNS      Standard query response
                                                              A 192.168.100.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
(00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
(192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 52985 (52985)
Domain Name System (response)
    [Request In: 1]
    [Time: 0.001251000 seconds]
    Transaction ID: 0x000c
    Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
    Answers
        server.example.com: type A, class IN, addr 192.168.100.10
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 1 hour
            Data length: 4
            Addr: 192.168.100.10
!--- 172.20.1.10 has been rewritten to be 192.168.100.10.
```

5. An diesem Punkt versucht der Client, unter 192.168.100.10 auf den WWW-Server zuzugreifen. Die Verbindung ist erfolgreich. Auf der ASA wird kein Datenverkehr erfasst, da sich der Client und der Server im gleichen Subnetz befinden.

Endgültige Konfiguration mit dem "dns"-Schlüsselwort

Dies ist die endgültige Konfiguration der ASA für die DNS-Dokumentation mit dem **dns-**Schlüsselwort und zwei NAT-Schnittstellen.

Endgültige ASA 7.2(1)-Konfiguration

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
```

```
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

access-list OUTSIDE extended permit tcp any host
172.20.1.10 eq www
!--- Simple access-list that permits HTTP access to the
mapped !--- address of the WWW server. pager lines 24
logging enable logging buffered debugging mtu outside
1500 mtu inside 1500 asdm image disk0:/asdm512-k8.bin no
asdm history enable arp timeout 14400 global (outside) 1
interface
nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10
netmask 255.255.255.255 dns
!--- PAT and static NAT configuration. The DNS keyword
instructs !--- the security appliance to rewrite DNS
records related to this entry. access-group OUTSIDE in
interface outside
!--- The Access Control List (ACL) that permits HTTP
access !--- to the WWW server is applied to the outside
interface. route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
username cisco password ffIRPGpDSOJh9YLq encrypted http
server enable 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 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns MY_DNS_INSPECT_MAP
 parameters
  message-length maximum 512
!--- DNS inspection map. policy-map global_policy class
inspection_default inspect ftp inspect h323 h225 inspect
h323 ras inspect rsh inspect rtsp inspect esmtp inspect
sqlnet inspect skinny inspect sunrpc inspect xdmcp
inspect sip inspect netbios inspect tftp inspect dns
MY_DNS_INSPECT_MAP
!--- DNS inspection is enabled using the configured map.
inspect icmp policy-map type inspect dns
migrated_dns_map_1 parameters message-length maximum 512
```

```
! service-policy global_policy global prompt hostname
context Cryptochecksum:a4a38088109887c3ceb481efab3dcf32
: end
```

Alternative Lösung: Hairpinning

Hairpinning mit statischer NAT

Vorsicht: Hairpinning mit statischer NAT beinhaltet das Senden des gesamten Datenverkehrs zwischen dem Client und dem WWW-Server über die Sicherheits-Appliance. Bevor Sie diese Lösung implementieren, sollten Sie die erwartete Datenverkehrsmenge und die Funktionen Ihrer Sicherheitslösung sorgfältig berücksichtigen.

Hairpinning ist der Prozess, bei dem Datenverkehr über dieselbe Schnittstelle zurückgesendet wird, über die er angekommen ist. Diese Funktion wurde in Version 7.0 der Security Appliance-Software eingeführt. Bei Versionen vor 7.2(1) muss mindestens ein Arm des hairpinned Datenverkehrs (ein- oder ausgehend) verschlüsselt werden. Ab Version 7.2(1) und höher gilt diese Anforderung nicht mehr. Wenn Sie 7.2(1) verwenden, können sowohl der ein- als auch der ausgehende Datenverkehr unverschlüsselt sein.

Hairpinning kann in Verbindung mit einer statischen NAT-Anweisung verwendet werden, um dieselbe Wirkung wie die DNS-Doktoring zu erzielen. Diese Methode ändert nicht den Inhalt des DNS A-Datensatzes, der vom DNS-Server an den Client zurückgegeben wird. Stattdessen kann der Client bei der Verwendung von Hairpinning (wie im in diesem Dokument beschriebenen Szenario) die Adresse **172.20.1.10** verwenden, die vom DNS-Server zurückgegeben wird, um eine Verbindung herzustellen.

Der relevante Teil der Konfiguration sieht folgendermaßen aus, wenn Sie Hairpinning und statische NAT verwenden, um einen DNS-Doctoring-Effekt zu erzielen. Die fett formatierten Befehle werden am Ende dieser Ausgabe genauer erläutert:

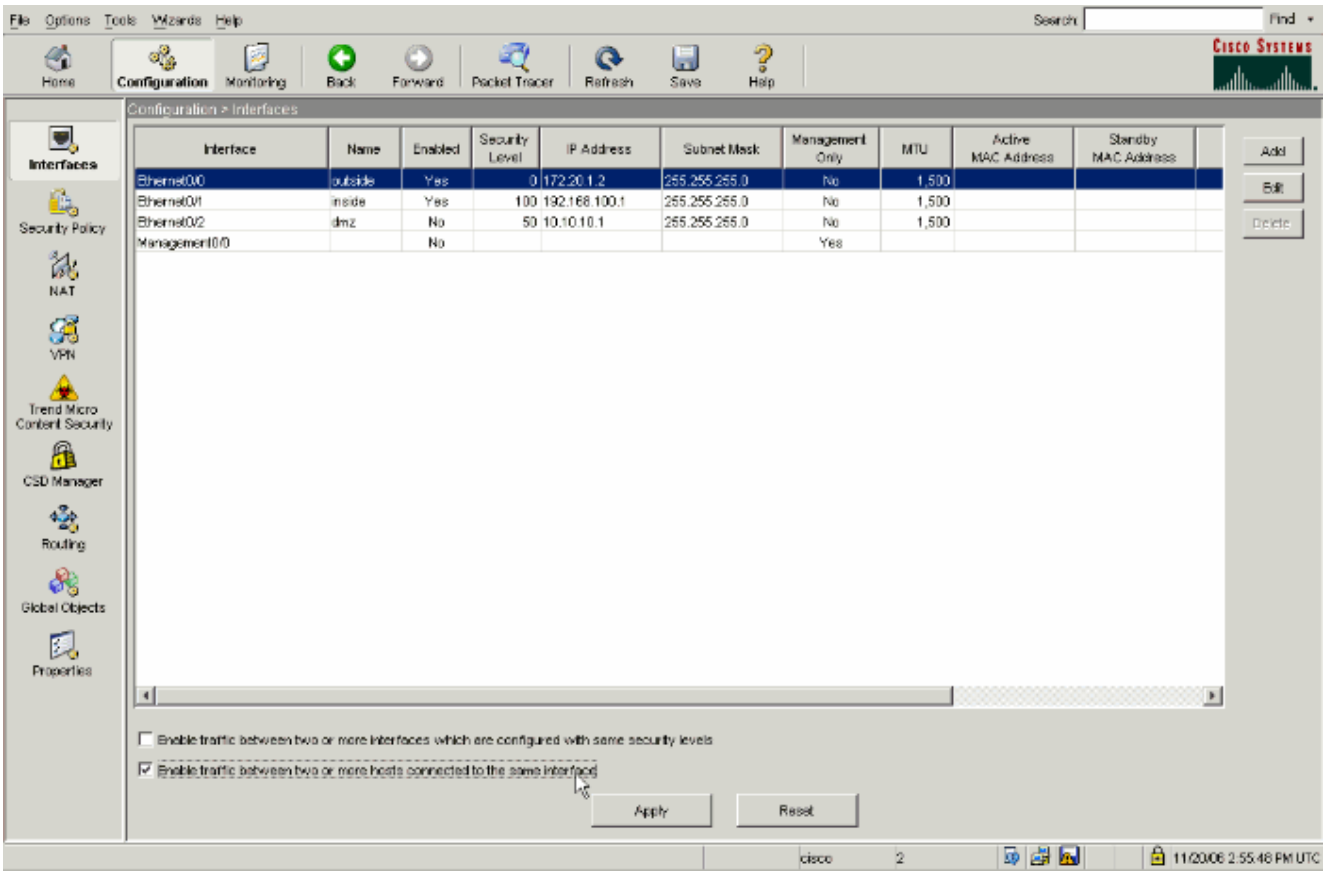
```
ciscoasa(config)#show run
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
!--- Output suppressed. same-security-traffic permit intra-interface
!--- Enable hairpinning. global (outside) 1 interface !--- Global statement for client access to
the Internet. global (inside) 1 interface
!--- Global statment for hairpinned client access through !--- the security appliance. nat
(inside) 1 192.168.100.0 255.255.255.0 !--- The NAT statement defines which traffic should be
natted. !--- The whole inside subnet in this case. static (inside,outside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT statement mapping the WWW server's real
address to a !--- public address on the outside interface. static (inside,inside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255
!--- Static NAT statment mapping requests for the public IP address of !--- the WWW server that
appear on the inside interface to the WWW server's !--- real address of 192.168.100.10.
```

- **same Sicherheit - Datenverkehr**: Mit diesem Befehl kann Datenverkehr derselben Sicherheitsstufe über die Sicherheits-Appliance geleitet werden. Die Schlüsselwörter für **Intra-Interface** erlauben es diesem gleichen Sicherheitsdatenverkehr, dieselbe Schnittstelle einzugeben und zu verlassen, sodass Hairpinning aktiviert ist.**Hinweis:** Weitere Informationen zu Hairpinning und dem Befehl für **gleichen Sicherheitsdatenverkehr** finden Sie unter Datenverkehr.

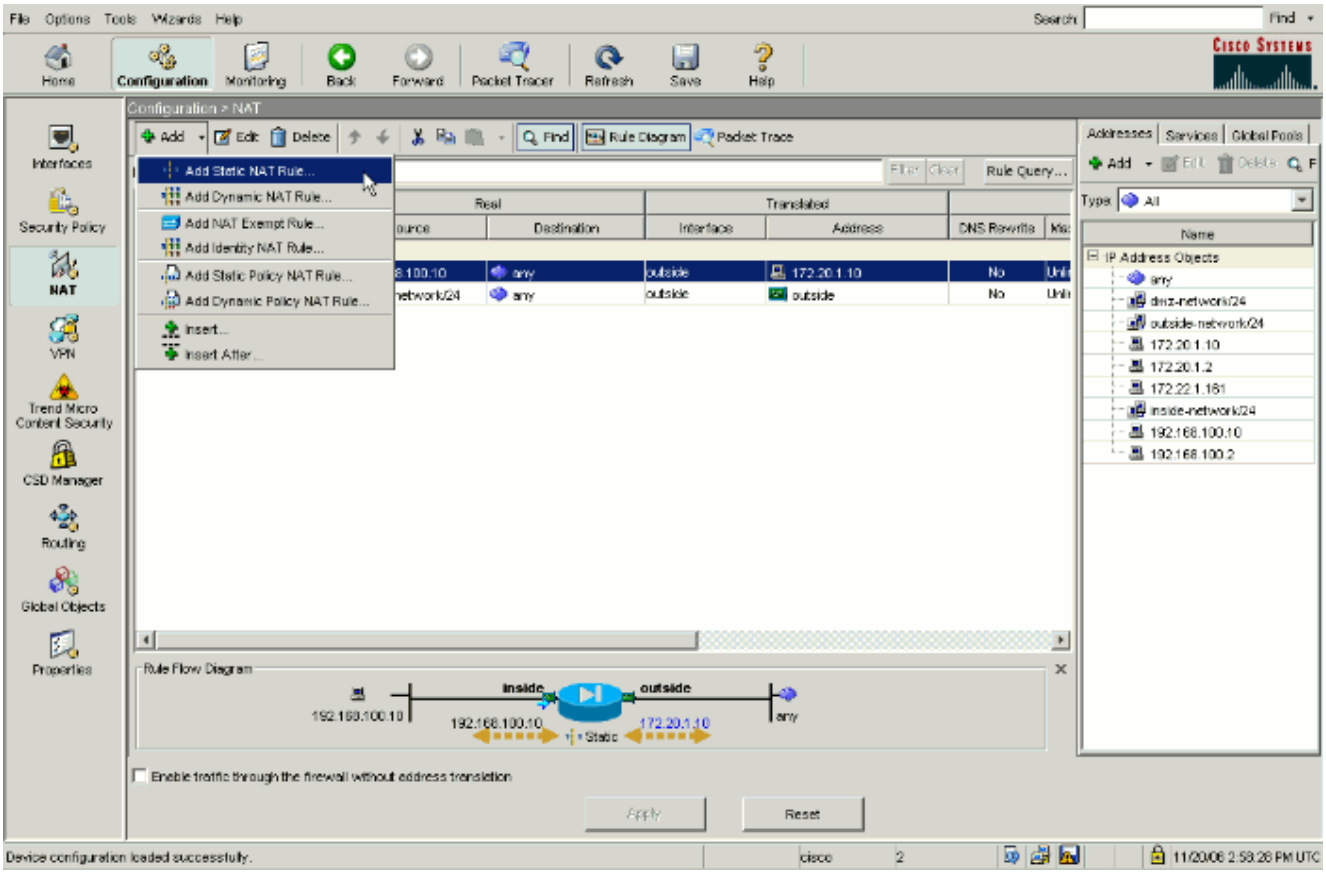
- **globale (interne) 1-Schnittstelle** - Der gesamte Datenverkehr, der die Sicherheits-Appliance passiert, muss NAT unterzogen werden. Bei diesem Befehl wird die interne Schnittstellenadresse der Sicherheits-Appliance verwendet, um Datenverkehr, der in die interne Schnittstelle eingeht, so zu aktivieren, dass er PAT durchlaufen kann, wenn er über die interne Schnittstelle abgesichert ist.
- **static (inside,inside) 172.20.1.10 192.168.100.10 netmask 255.255.255.25** - Dieser statische NAT-Eintrag erstellt eine zweite Zuordnung für die öffentliche IP-Adresse des WWW-Servers. Im Gegensatz zum ersten statischen NAT-Eintrag wird die Adresse 172.20.1.10 diesmal jedoch der internen Schnittstelle der Sicherheits-Appliance zugeordnet. Dadurch kann die Sicherheits-Appliance auf Anfragen reagieren, die sie für diese Adresse auf der internen Schnittstelle sieht. Anschließend werden diese Anfragen selbst an die tatsächliche Adresse des WWW-Servers umgeleitet.

Gehen Sie wie folgt vor, um Hairpinning mit statischer NAT im ASDM zu konfigurieren:

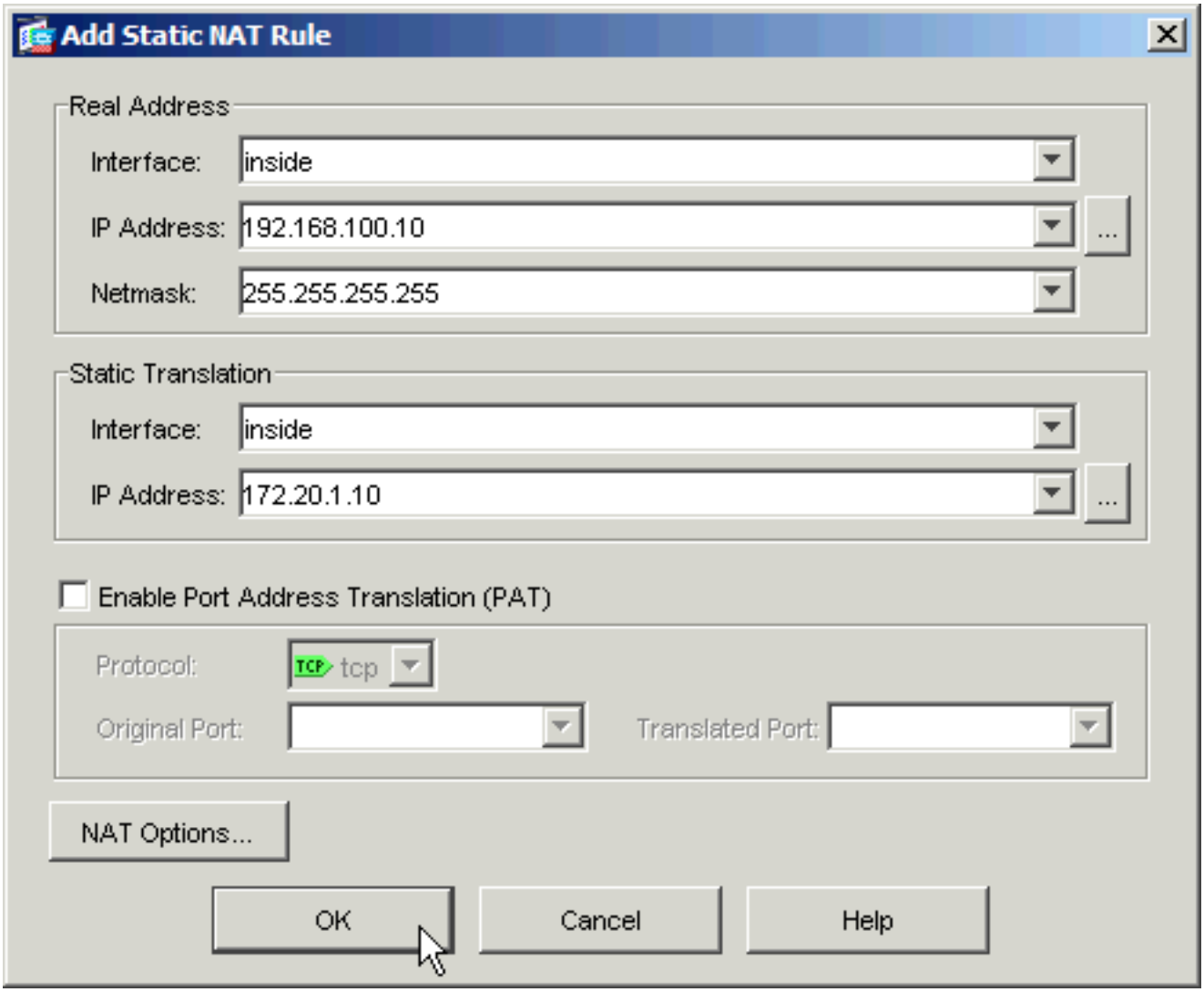
1. Navigieren Sie zu **Konfiguration > Schnittstellen**.
2. Aktivieren Sie unten im Fenster das Kontrollkästchen **Datenverkehr zwischen zwei oder mehr Hosts aktivieren, die mit derselben Schnittstelle verbunden sind**.



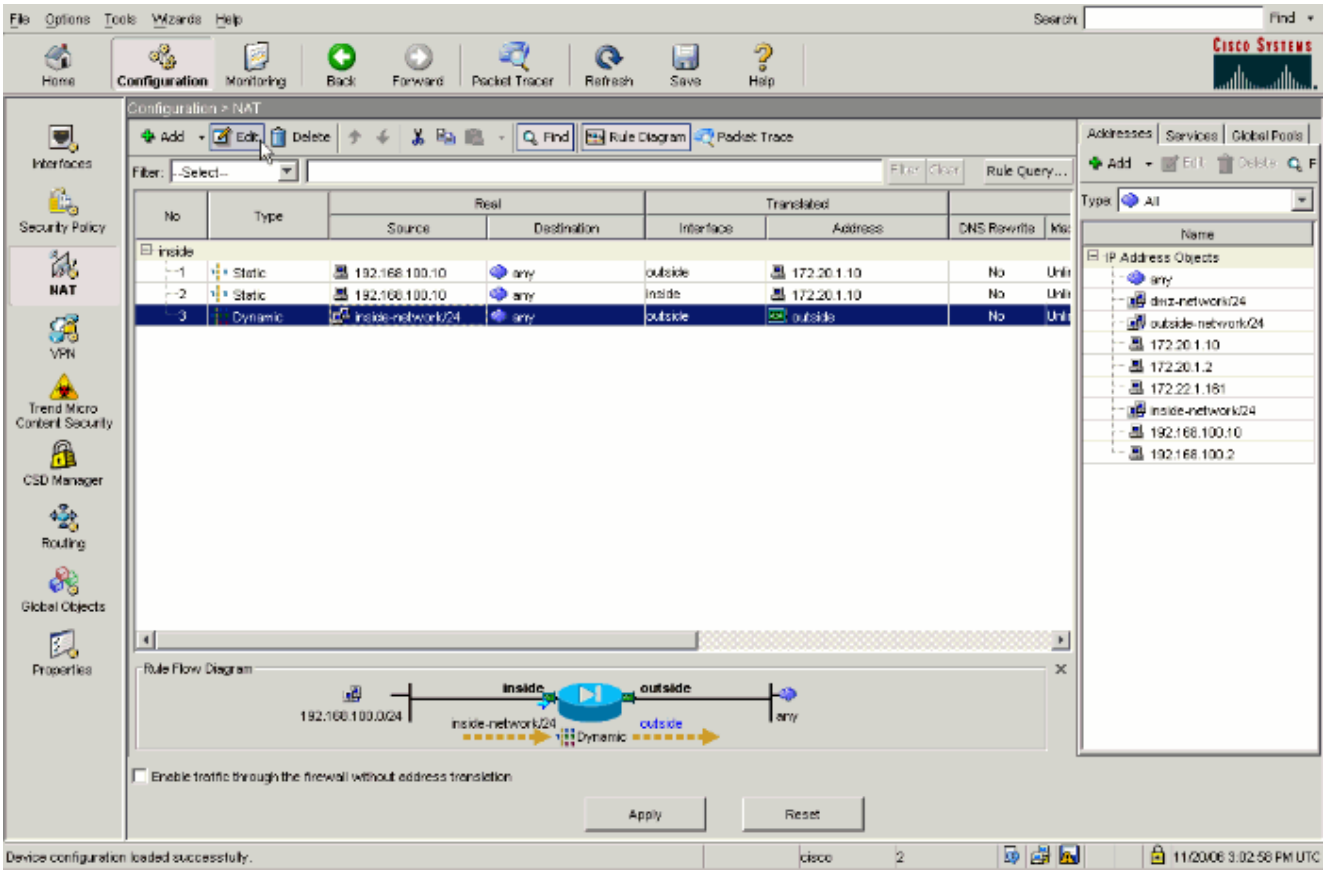
3. Klicken Sie auf **Übernehmen**.
4. Navigieren Sie zu **Konfiguration > NAT**, und wählen Sie **Hinzufügen > Statische NAT-Regel hinzufügen aus...**



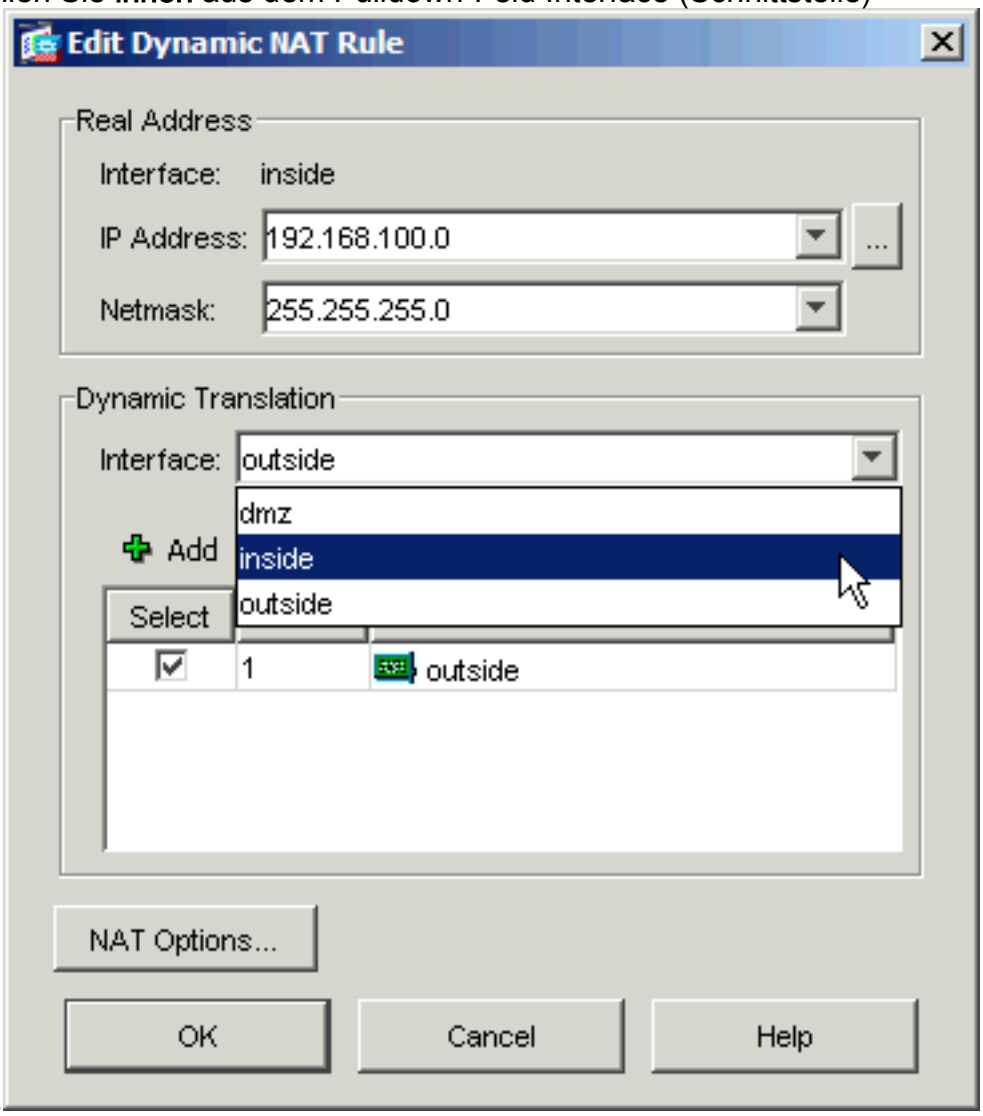
5. Füllen Sie die Konfiguration für die neue statische Übersetzung aus.Füllen Sie den Bereich **Real Address** mit den WWW-Serverinformationen aus.Füllen Sie den Bereich **Statische Übersetzung** mit der Adresse und Schnittstelle aus, der Sie den WWW-Server zuordnen möchten.In diesem Fall wird die interne Schnittstelle so gewählt, dass Hosts auf der internen Schnittstelle über die zugeordnete Adresse 172.20.1.10 auf den WWW-Server zugreifen können.



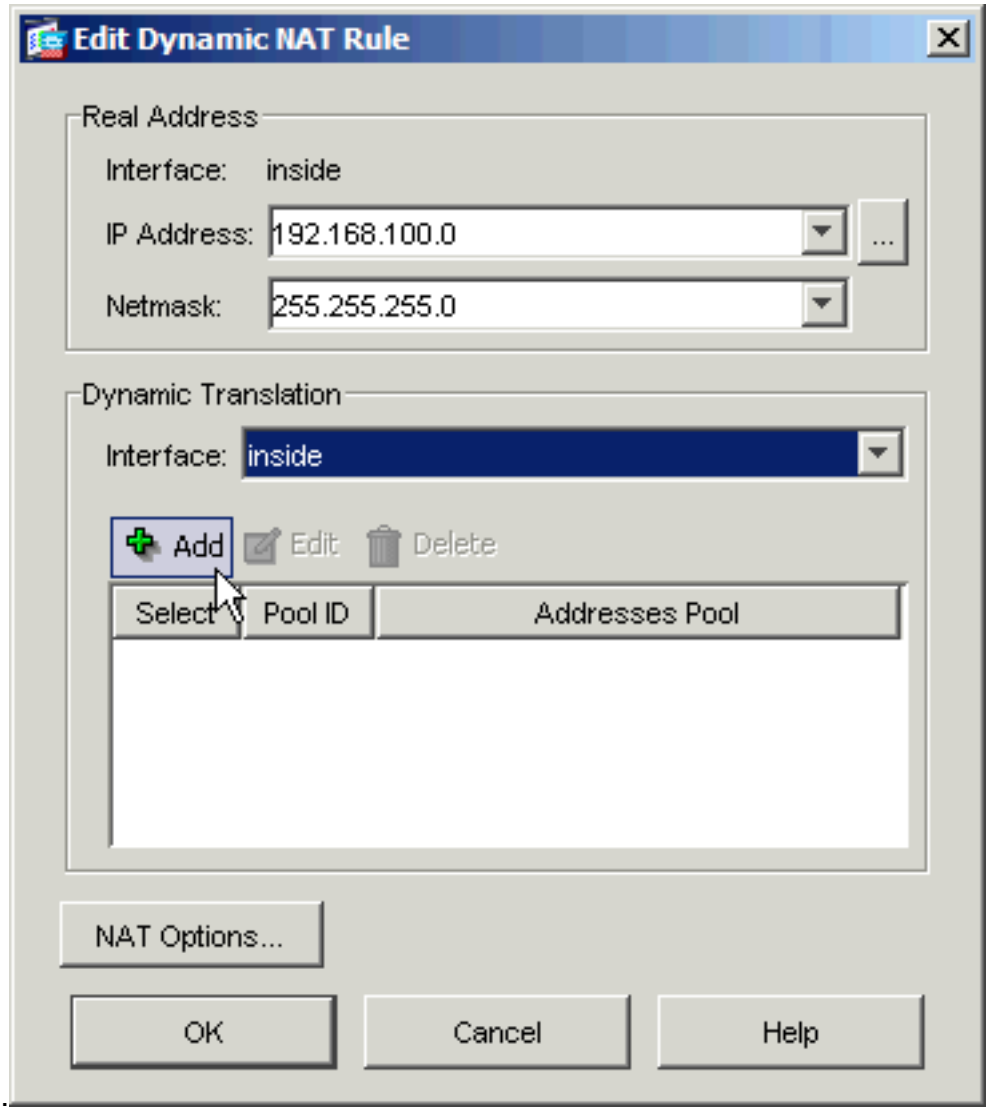
6. Klicken Sie auf **OK**, um das Fenster Statische NAT-Regel hinzufügen zu verlassen.
7. Wählen Sie die vorhandene dynamische PAT-Übersetzung aus, und klicken Sie auf **Bearbeiten**.



8. Wählen Sie **innen** aus dem Pulldown-Feld Interface (Schnittstelle) aus.

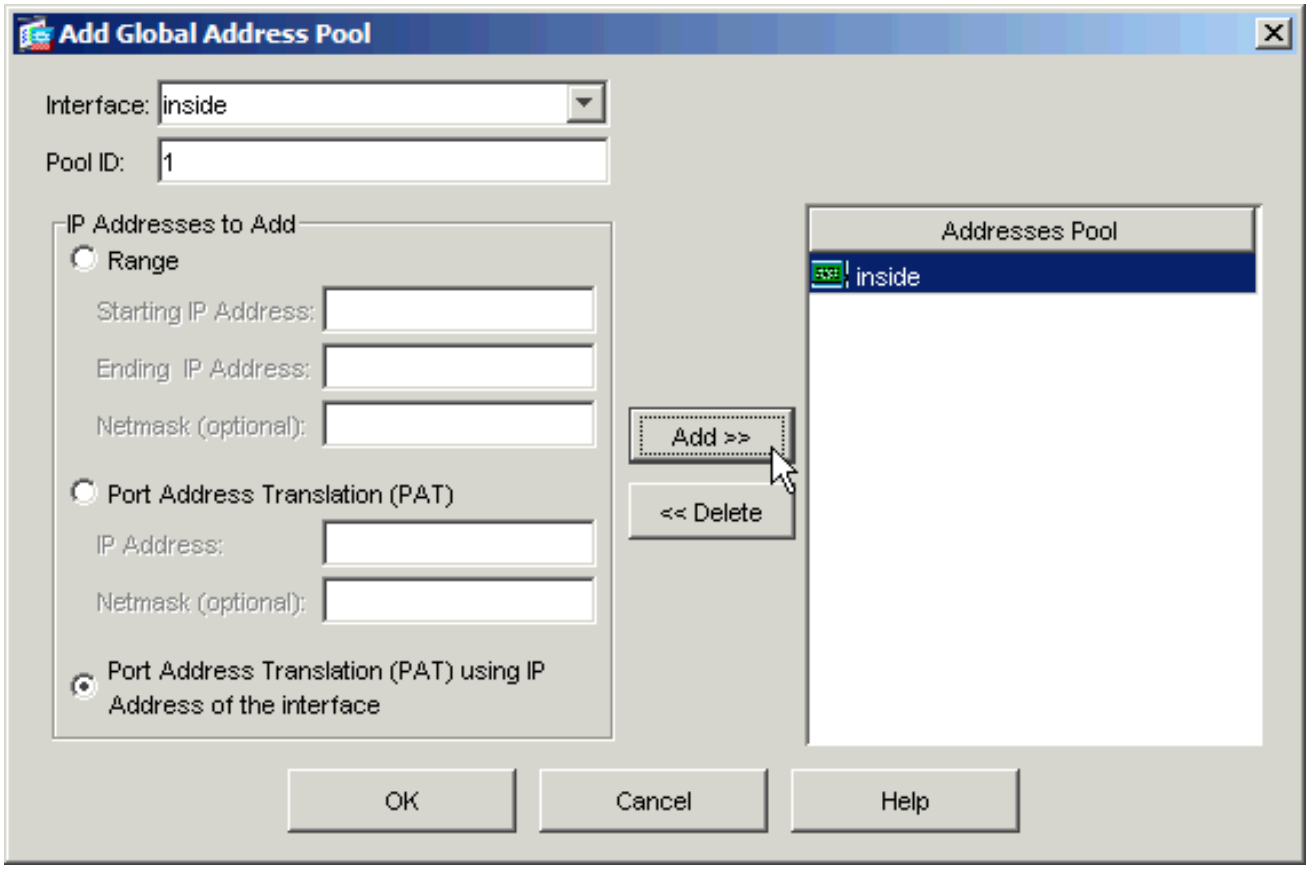


9. Klicken Sie auf



Hinzufügen.

10. Wählen Sie das Optionsfeld **Port Address Translation (PAT) mit der IP-Adresse der Schnittstelle aus**. Klicken Sie auf **Hinzufügen**.



11. Klicken Sie auf **OK**, um das Fenster Globalen Adresspool hinzufügen zu verlassen. Klicken Sie auf **OK**, um das Fenster Edit Dynamic NAT Rule (Dynamische NAT-Regel bearbeiten) zu verlassen. Klicken Sie auf **Apply**, um Ihre Konfiguration an die Sicherheits-Appliance zu senden.

Hier sehen Sie die Reihenfolge der Ereignisse, die bei der Konfiguration von Hairpinning auftreten. Angenommen, der Client hat den DNS-Server bereits abgefragt und eine Antwort von **172.20.1.10** auf die WWW-Serveradresse erhalten:

1. Der Client versucht, unter 172.20.1.10 mit dem WWW-Server Kontakt aufzunehmen.
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.2
   ```
2. Die Sicherheits-Appliance erkennt die Anforderung und erkennt, dass der WWW-Server die Adresse 192.168.100.10 hat.
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.10
   ```
3. Die Sicherheits-Appliance erstellt eine dynamische PAT-Übersetzung für den Client. Die Quelle für den Client-Datenverkehr ist jetzt die interne Schnittstelle der Sicherheits-Appliance: 192.168.100.1
   ```
   %ASA-6-305011: Built dynamic TCP translation from inside:192.168.100.2/11012 to
   inside:192.168.100.1/1026
   ```

4. Die Sicherheits-Appliance erstellt über sich eine TCP-Verbindung zwischen dem Client und dem WWW-Server. Beachten Sie die zugeordneten Adressen der einzelnen Hosts in Klammern.
   ```
   %ASA-6-302013: Built inbound TCP connection 67399 for inside:192.168.100.2/11012
   (192.168.100.1/1026) to inside:192.168.100.10/80 (172.20.1.10/80)
   ```

5. Der Befehl **show xlate** auf der Sicherheits-Appliance überprüft, ob der Client-Datenverkehr über die Sicherheits-Appliance übertragen wird.
   ```
   ciscoasa(config)#show xlate
   3 in use, 9 most used
   Global 172.20.1.10 Local 192.168.100.10
   ```

```
Global 172.20.1.10 Local 192.168.100.10
PAT Global 192.168.100.1(1027) Local 192.168.100.2(11013)
```

6. Der Befehl **show conn** auf der Sicherheits-Appliance überprüft, ob die Verbindung zwischen der Sicherheits-Appliance und dem WWW-Server für den Client erfolgreich hergestellt wurde. Beachten Sie die tatsächliche Adresse des Clients in Klammern.

```
ciscoasa#show conn
TCP out 192.168.100.1(192.168.100.2):11019 in 192.168.100.10:80
idle 0:00:03 bytes 1120 flags UIOB
```

Endgültige Konfiguration mit Hairpinning und statischer NAT

Dies ist die endgültige Konfiguration der ASA, die Hairpinning und statische NAT verwendet, um bei zwei NAT-Schnittstellen einen DNS-Doctoring-Effekt zu erzielen.

Endgültige ASA 7.2(1)-Konfiguration

```
ciscoasa(config-if)#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
same-security-traffic permit intra-interface
access-list OUTSIDE extended permit tcp any host
172.20.1.10 eq www
!--- Simple access-list that permits HTTP access to the
mapped !--- address of the WWW server. pager lines 24
logging enable logging buffered debugging mtu outside
1500 mtu inside 1500 asdm image disk0:/asdm512-k8.bin no
asdm history enable arp timeout 14400 global (outside) 1
```

```
interface !--- Global statement for client access to the
Internet. global (inside) 1 interface !--- Global
statment for hairpinned client access through !--- the
security appliance. nat (inside) 1 192.168.100.0
255.255.255.0 !--- The NAT statement defines which
traffic should be natted. !--- The whole inside subnet
in this case. static (inside,outside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT
statement mapping the WWW server's real address to a
public !--- address on the outside interface. static
(inside,inside) 172.20.1.10 192.168.100.10 netmask
255.255.255.255 !--- Static NAT statement mapping
requests for the public IP address of the !--- WWW
server that appear on the inside interface to the WWW
server's real address !--- of 192.168.100.10. access-
group OUTSIDE in interface outside !--- The ACL that
permits HTTP access to the WWW server is applied !--- to
the outside interface. route outside 0.0.0.0 0.0.0.0
172.20.1.1 1 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
mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00
sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth
0:05:00 absolute username cisco password
ffIRPGpDSOJh9YLq encrypted http server enable 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 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
MY_DNS_INSPECT_MAP parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect ftp inspect h323 h225 inspect h323 ras inspect
rsh inspect rtsp inspect esmtp inspect sqlnet inspect
skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp inspect dns MY_DNS_INSPECT_MAP
inspect icmp policy-map type inspect dns
migrated_dns_map_1 parameters message-length maximum 512
! service-policy global_policy global prompt hostname
context Cryptochecksum:7c9b4e3aff085ba90ee194e079111e1d
: end
```

Hinweis: In diesem Video, Hair-Pinning auf der Cisco ASA (nur registrierte Kunden), finden Sie weitere Informationen zu verschiedenen Szenarien, in denen Hairpinning verwendet werden könnte.

DNS-Inspektion konfigurieren

Führen Sie die folgenden Schritte aus, um die DNS-Überprüfung zu aktivieren (falls sie zuvor deaktiviert wurde). In diesem Beispiel wird die DNS-Inspektion der globalen Standardinspektionsrichtlinie hinzugefügt, die von einem **Service-Policy-**Befehl global angewendet wird, als ob die ASA mit einer Standardkonfiguration begann. Weitere Informationen zu Service-Richtlinien und Inspektionen finden Sie unter Using Modular Policy Framework.

1. Erstellen Sie eine Inspection Policy Map für DNS.
   ```
   ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
   ```

2. Geben Sie im Konfigurationsmodus für die Richtlinienzuweisung den

Parameterkonfigurationsmodus ein, um Parameter für die Prüfungs-Engine anzugeben.

```
ciscoasa(config-pmap)#parameters
```

3. Geben Sie im Konfigurationsmodus für Richtlinienzuordnungsparameter die maximale Nachrichtenlänge für DNS-Nachrichten für 512 an.

```
ciscoasa(config-pmap-p)#message-length maximum 512
```

4. Beenden Sie den Konfigurationsmodus für Richtlinienzuordnungsparameter und den Konfigurationsmodus für Richtlinienzuordnung.

```
ciscoasa(config-pmap-p)#exit
ciscoasa(config-pmap)#exit
```

5. Bestätigen Sie, dass die Richtlinienzuordnung für die Inspektion wie gewünscht erstellt wurde.

```
ciscoasa(config)#show run policy-map type inspect dns
!
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
  message-length maximum 512
!
```

6. Wechseln Sie in den Konfigurationsmodus für die Richtlinienzuweisung für **global_policy**.

```
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#
```

7. Geben Sie im Konfigurationsmodus für die Richtlinienzuweisung die standardmäßige Klassenzuordnung für Layer 3/4 an, **Inspection_default**.

```
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#
```

8. Geben Sie im Konfigurationsmodus der Richtlinienzuordnung an, dass DNS mithilfe der in den Schritten 1-3 erstellten Richtlinienzuordnung überprüft werden soll.

```
ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP
```

9. Beenden Sie den Konfigurationsmodus "policy-map class"" und den Konfigurationsmodus "policy-map".

```
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```

10. Überprüfen Sie, ob die Richtlinienzuordnung **global_policy** wie gewünscht konfiguriert ist.

```
ciscoasa(config)#show run policy-map
!
!--- The configured DNS inspection policy map. policy-map type inspect dns
MY_DNS_INSPECT_MAP parameters message-length maximum 512 policy-map global_policy class
inspection_default inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp
inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip
inspect netbios inspect tftp inspect dns MY_DNS_INSPECT_MAP
!--- DNS application inspection enabled. !
```

11. Überprüfen Sie, ob die globale_Richtlinie global von einer Dienstrichtlinie angewendet wird.

```
ciscoasa(config)#show run service-policy
service-policy global_policy global
```

Split-DNS-Konfiguration

Geben Sie den Befehl **split-dns** im Konfigurationsmodus für Gruppenrichtlinien aus, um eine Liste der Domänen einzugeben, die durch den Split Tunnel gelöst werden sollen. Verwenden Sie das Formular no (*Kein*), um eine Liste zu löschen.

Wenn keine Split-Tunneling-Domänenlisten vorhanden sind, erben die Benutzer alle Domänen, die in der Standardgruppenrichtlinie vorhanden sind. Geben Sie den Befehl **split-dns none** aus, um die Vererbung von Split-Tunneling-Domänenlisten zu verhindern.

Trennen Sie jeden Eintrag in der Domänenliste durch einen einzigen Leerzeichen. Die Anzahl der Einträge ist nicht begrenzt, aber die gesamte Zeichenfolge darf maximal 255 Zeichen lang sein. Sie können nur alphanumerische Zeichen, Bindestriche (-) und Punkte (.) verwenden. Der Befehl **no split-dns** löscht bei Verwendung ohne Argumente alle aktuellen Werte, einschließlich eines NULL-Werts, der bei Ausgabe des Befehls **split-dns none** erstellt wurde.

Dieses Beispiel zeigt, wie die Domänen Domain1, Domain2, Domain3 und Domain4 so konfiguriert werden, dass sie durch Split-Tunneling für die Gruppenrichtlinie mit dem Namen FirstGroup aufgelöst werden:

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)#split-dns value Domain1 Domain2 Domain3 Domain4
```

Überprüfen

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

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

Erfassung von DNS-Datenverkehr

Eine Möglichkeit, zu überprüfen, ob die Sicherheits-Appliance DNS-Datensätze korrekt umschreibt, besteht darin, die betreffenden Pakete zu erfassen, wie im vorherigen Beispiel beschrieben. Gehen Sie wie folgt vor, um den Datenverkehr auf der ASA zu erfassen:

1. Erstellen Sie eine Zugriffsliste für jede Erfassungsinstanz, die Sie erstellen möchten.Die ACL sollte den Datenverkehr angeben, den Sie erfassen möchten. In diesem Beispiel wurden zwei ACLs erstellt.Die ACL für Datenverkehr an der externen Schnittstelle:
   ```
   access-list DNSOUTCAP extended permit ip host 172.22.1.161 host 172.20.1.2
   !--- All traffic between the DNS server and the ASA. access-list DNSOUTCAP extended permit
   ip host 172.20.1.2 host 172.22.1.161 !--- All traffic between the ASA and the DNS server.
   ```
   Die ACL für den Datenverkehr an der internen Schnittstelle:
   ```
   access-list DNSINCAP extended permit ip host 192.168.100.2 host 172.22.1.161
   !--- All traffic between the client and the DNS server. access-list DNSINCAP extended
   permit ip host 172.22.1.161 host 192.168.100.2 !--- All traffic between the DNS server and
   the client.
   ```
2. Erstellen Sie die Erfassungsinstanz(en):
   ```
   ciscoasa#capture DNSOUTSIDE access-list DNSOUTCAP interface outside
   !--- This capture collects traffic on the outside interface that matches !--- the ACL
   DNSOUTCAP. ciscoasa#capture DNSINSIDE access-list DNSINCAP interface inside
   !--- This capture collects traffic on the inside interface that matches !--- the ACL
   DNSINCAP.
   ```
3. Zeigen Sie die Erfassung(en) an.Die Beispielaufnahmen sehen nach dem Bestehen von DNS-Datenverkehr folgendermaßen aus:
   ```
   ciscoasa#show capture DNSOUTSIDE
   2 packets captured
      1: 14:07:21.347195 172.20.1.2.1025 > 172.22.1.161.53:  udp 36
   ```

```
   2: 14:07:21.352093 172.22.1.161.53 > 172.20.1.2.1025:  udp 93
2 packets shown
ciscoasa#show capture DNSINSIDE
2 packets captured
   1: 14:07:21.346951 192.168.100.2.57225 > 172.22.1.161.53:  udp 36
   2: 14:07:21.352124 172.22.1.161.53 > 192.168.100.2.57225:  udp 93
2 packets shown
```

4. (Optional) Kopieren Sie die Erfassung(en) zur Analyse in einer anderen Anwendung auf einen TFTP-Server im pcap-Format.Anwendungen, die das pcap-Format analysieren können, können zusätzliche Details wie den Namen und die IP-Adresse in DNS-A-Datensätzen anzeigen.

```
ciscoasa#copy /pcap capture:DNSINSIDE tftp
...
ciscoasa#copy /pcap capture:DNSOUTSIDE tftp
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

DNS Rewrite wird nicht durchgeführt

Stellen Sie sicher, dass die DNS-Inspektion auf der Sicherheits-Appliance konfiguriert ist. Weitere Informationen finden Sie im Abschnitt DNS-Überprüfung konfigurieren.

Erstellung der Übersetzung fehlgeschlagen

Wenn keine Verbindung zwischen dem Client und dem WWW-Server hergestellt werden kann, kann dies auf eine falsche NAT-Konfiguration zurückzuführen sein. Prüfen Sie die Protokolle der Sicherheits-Appliance auf Meldungen, die darauf hinweisen, dass ein Protokoll keine Übersetzung über die Sicherheits-Appliance erstellt hat. Wenn solche Meldungen angezeigt werden, stellen Sie sicher, dass NAT für den gewünschten Datenverkehr konfiguriert wurde und keine Adressen falsch sind.

```
%ASA-3-305006: portmap translation creation failed for tcp src
inside:192.168.100.2/11000 dst dmz:10.10.10.10/23
```

Löschen Sie die Übersetzungseinträge, entfernen Sie die NAT-Anweisungen, und wenden Sie sie erneut an, um diesen Fehler zu beheben.

UDP-DNS-Antwort löschen

Es ist möglich, dass Sie diese Fehlermeldung aufgrund eines DNS-Paketverfalls erhalten:

```
 %PIX|ASA-4-410001: UDP DNS request from source_interface:source_address/source_port
to dest_interface:dest_address/dest_port; (label length | domain-name length)
52 bytes exceeds remaining packet length of 44 bytes.
```

Um dieses Problem zu beheben, können Sie die Länge des DNS-Pakets zwischen 512 und 65535 erhöhen.

Beispiel:

```
ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
ciscoasa(config-pmap)#parameters
ciscoasa(config-pmap-p)#message-length maximum <512-65535>
```

Zugehörige Informationen

- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten
- Request for Comments (RFCs)
- Hair Pinning auf Cisco ASA
- Cisco Adaptive Security Appliances der Serie ASA 5500