Konfigurieren von DNS Doctoring für drei NAT-Schnittstellen auf ASA Version 9.x

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration, um DNS (Domain Name System)-Dokumente für die Adaptive Security Appliance (ASA) der Serie ASA 5500-X auszuführen, die NAT-Anweisungen (Object/Auto Network Address Translation) verwendet. 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.

Voraussetzungen

Anforderungen

Cisco gibt an, dass DNS Inspection aktiviert sein muss, um DNS-Doctoring auf der Security Appliance durchzuführen. Die DNS-Überprüfung ist standardmäßig aktiviert.

Wenn die DNS-Überprüfung aktiviert ist, führt die Sicherheits-Appliance die folgenden Aufgaben aus:

- Übersetzt den DNS-Datensatz basierend auf der Konfiguration, die mit der Verwendung von Objekt-/Auto NAT-Befehlen (DNS Rewrite) abgeschlossen wurde. Die Übersetzung gilt nur für den A-Datensatz in der DNS-Antwort. Reverse Lookups, die den Zeiger-Datensatz (PTR) anfordern, sind daher von der DNS-Umschreibung nicht betroffen. In Version ASA 9.0(1) und höher wird die Übersetzung des DNS-PTR-Datensatzes für umgekehrte DNS-Abfragen bei Verwendung von IPv4 NAT, IPv6 NAT und NAT64 bei aktivierter DNS-Prüfung für die NAT-Regel vorgenommen.**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 zu überprüfen, ob 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 eingeben, 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-X, Version 9.x.

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 der Cisco Security Appliance der Serie ASA 5500, Version 8.4 oder höher, verwendet werden.

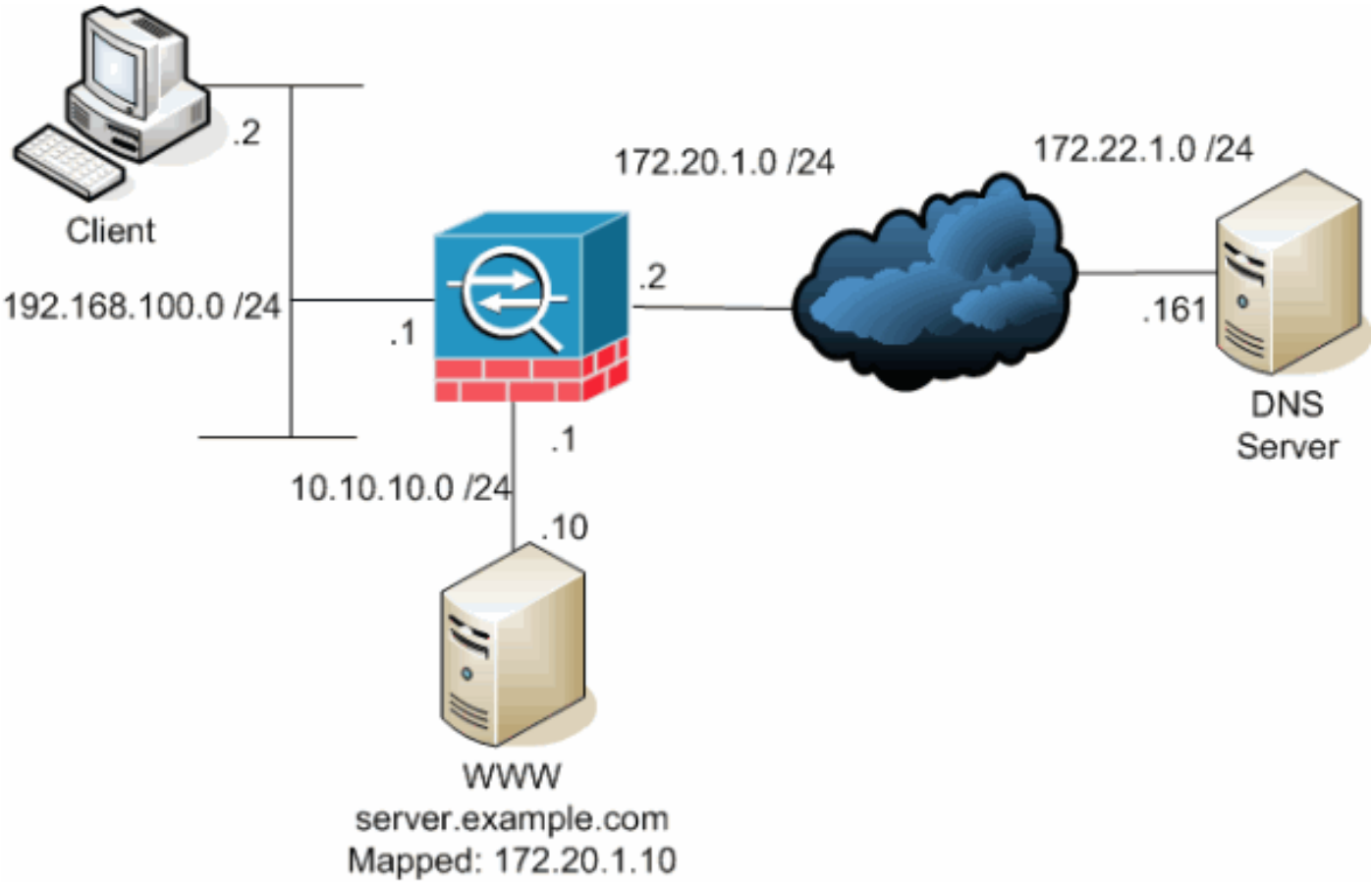
Hinweis: Die ASDM-Konfiguration gilt nur für Version 7.x.

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: Drei NAT-Schnittstellen - innen, außen, DMZ

Topologie



Dieses Diagramm ist ein Beispiel für diese Situation. In diesem Fall möchte der Client unter 192.168.100.2 die URL **server.example.com** verwenden, um unter 10.10.10.10 auf den WWW-Server zuzugreifen. DNS-Dienste für den Client werden vom externen DNS-Server unter

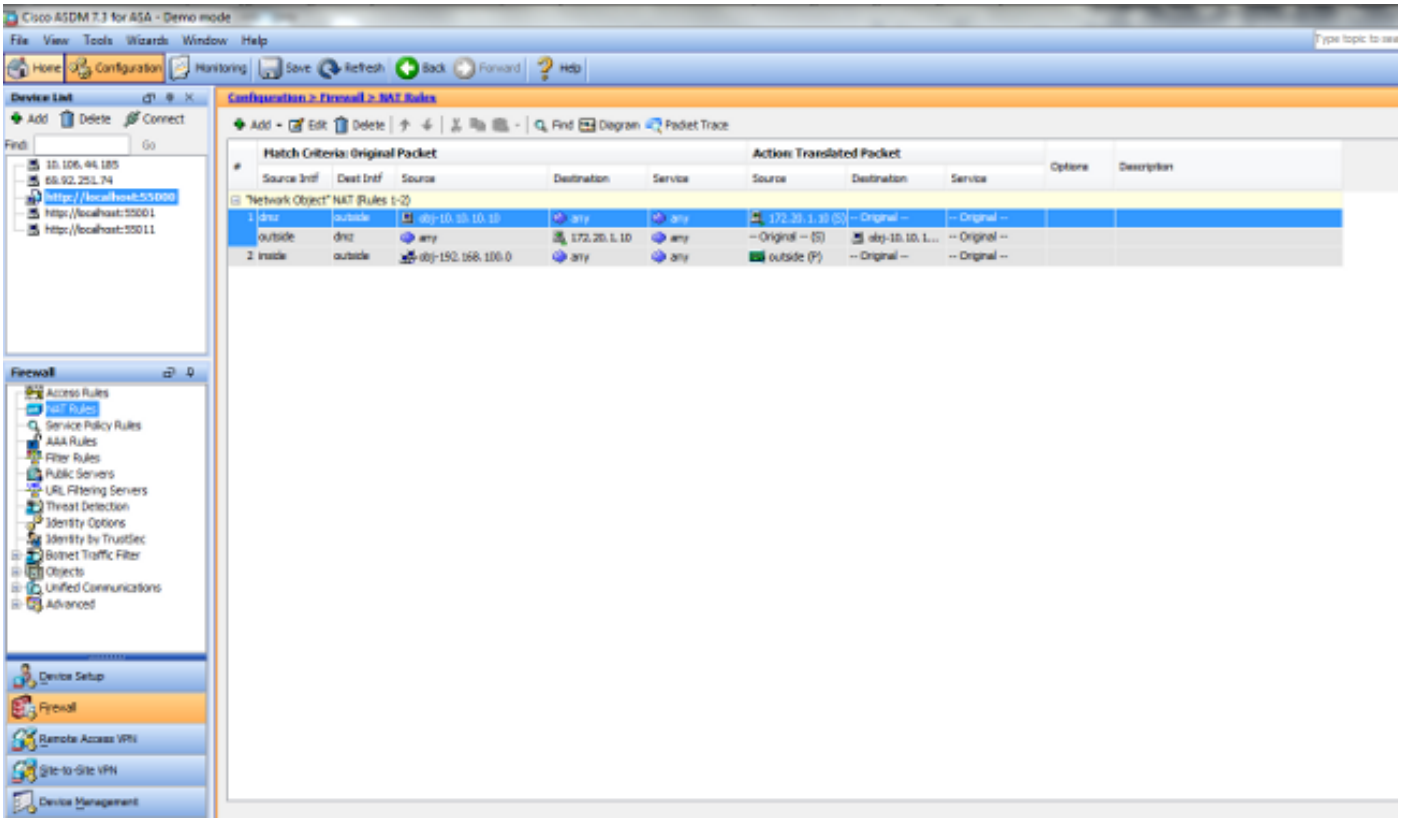
172.22.1.161 bereitgestellt. Da sich der DNS-Server in einem anderen öffentlichen Netzwerk befindet, kennt er die private IP-Adresse des WWW-Servers nicht. Stattdessen kennt sie die WWW-Server-zugeordnete Adresse 172.20.1.10. Somit enthält der DNS-Server die IP-Adresse-zu-Name-Zuordnung von **server.example.com** 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 an die IP-Adresse von **server.example.com** sendet, kann er nicht auf den WWW-Server zugreifen. Dies liegt daran, dass der Client einen A-Record erhält, der die zugeordnete öffentliche Adresse 172.20.1.10 für den WWW-Server enthält. 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:

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.
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 jedoch der Datenverkehr nicht von innen nach außen in die DMZ fließt, wird die Verbindung zeitweise 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 Szenario zu ermöglichen, das unter " Problem: Der Client kann nicht auf den WWW-Server zugreifen", um eine Verbindung herzustellen. In dieser Situation, in der DNS-Doctoring aktiviert ist, schreibt die Sicherheits-Appliance den A-Datensatz um, um den Client auf 10.10.10.10 anstelle von 172.20.1.10 zu leiten. DNS-Doctoring ist aktiviert, wenn Sie das **dns**-Schlüsselwort einer statischen NAT-Anweisung (Version 8.2 und früher) oder einer Objekt-/Auto NAT-Anweisung (Version 8.3 und höher) hinzufügen.

Version 8.2 und früher

Dies ist die endgültige Konfiguration der ASA für die DNS-Dokumentation mit dem **dns**-Schlüsselwort und drei NAT-Schnittstellen für Version 8.2 und frühere Versionen.

```
ciscoasa#show running-config
```

```
: Saved
:
ASA Version 8.2.x
!
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
nameif dmz
security-level 50
ip address 10.10.10.1 255.255.255.0
!
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

pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 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,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0
static (dmz,outside) 172.20.1.10 10.10.10.10 netmask 255.255.255.255 dns

access-group OUTSIDE in interface outside

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:d6637819c6ea981daf20d8c7aa8ca256
: end
```

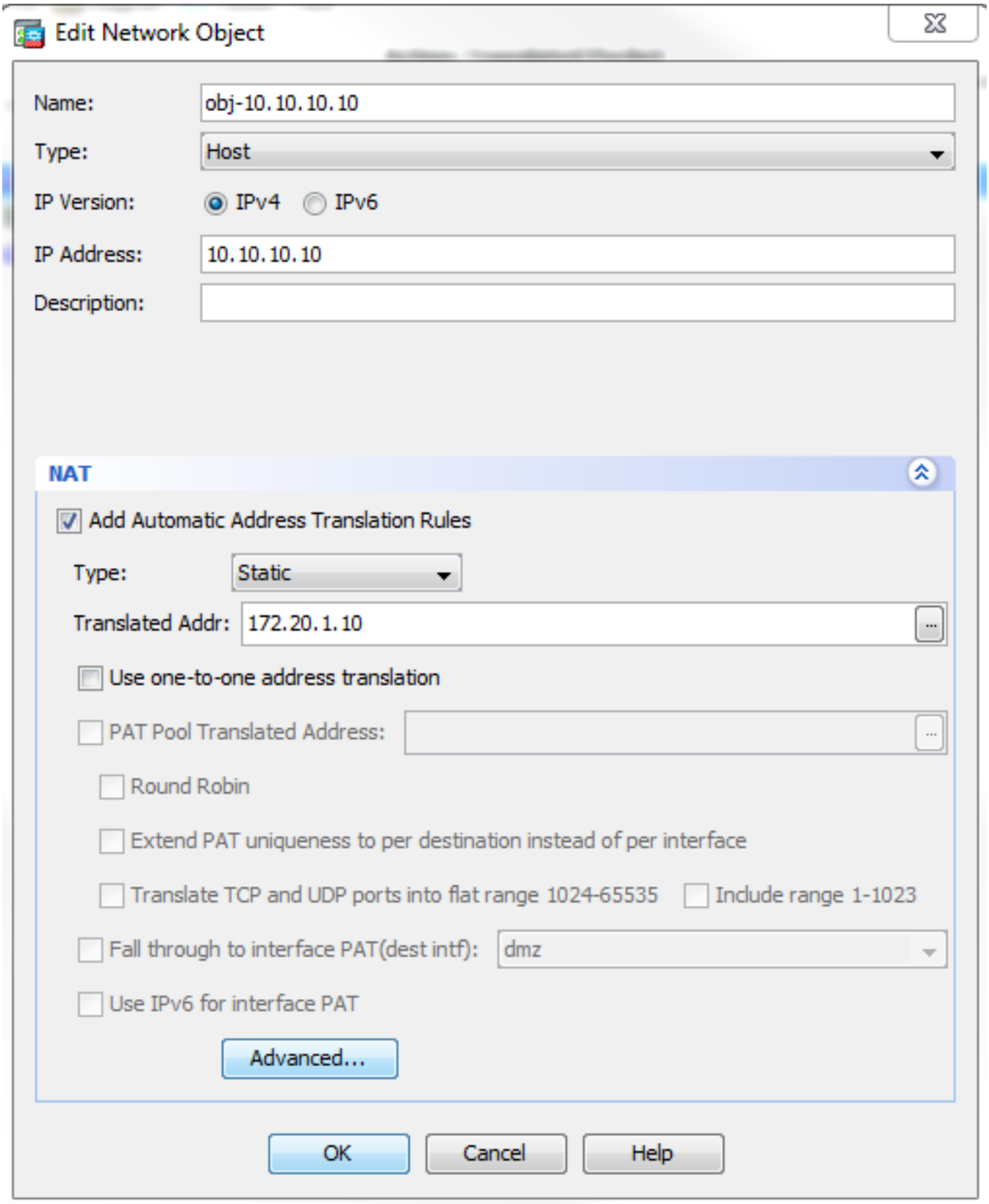
Version 8.3 und höher

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10 dns

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.

access-group OUTSIDE in interface outside

!--- Output suppressed.
```

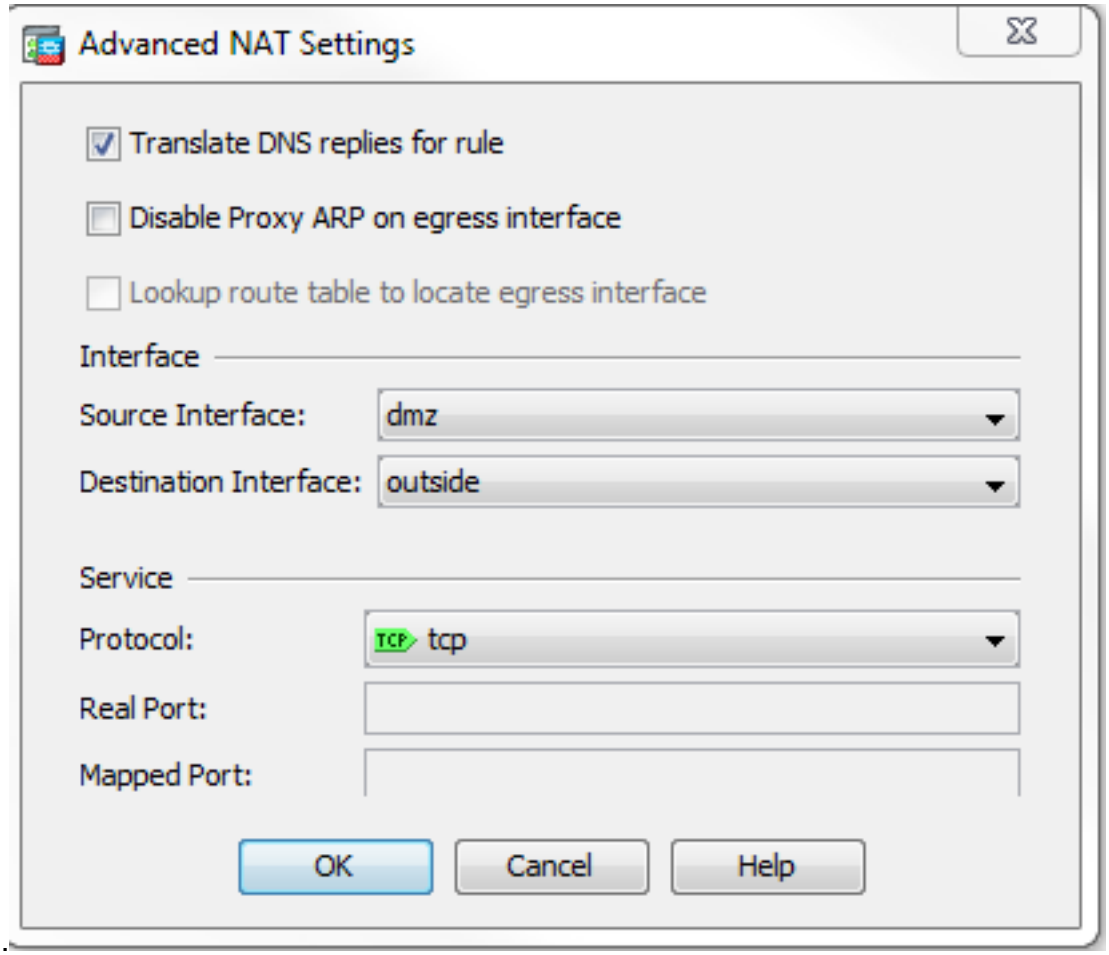
ASDM-Konfiguration

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

1. Wählen Sie **Konfiguration > NAT Rules** und wählen Sie die Objekt-/Auto-Regel aus, die geändert werden soll. Klicken Sie auf **Bearbeiten**.
2. Klicken Sie auf **Erweitert...**



3. Aktivieren Sie das Kontrollkästchen **DNS-Antworten für Regel**



übersetzen.

4. Klicken Sie auf **OK**, um das Fenster NAT-Optionen zu verlassen.
5. Klicken Sie auf **OK**, um das Fenster Objekt bearbeiten/Automatische NAT-Regel zu verlassen.
6. Klicken Sie auf **Apply**, um Ihre Konfiguration an die Sicherheits-Appliance zu senden.

Überprüfen

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
6 2.507191 172.22.1.161   192.168.100.2   DNS Standard query response
A 10.10.10.10

Frame 6 (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: 50752 (50752)
Domain Name System (response)
[Request In: 5]
[Time: 0.002182000 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 10.10.10.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 10.10.10.10
```

5. An diesem Punkt versucht der Client, unter 10.10.10.10 auf den WWW-Server zuzugreifen. Die Verbindung ist erfolgreich.

Endgültige Konfiguration mit dem "dns"-Schlüsselwort

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

```
ciscoasa# sh running-config
: Saved
:
: Serial Number: JMX1425L48B
: Hardware:   ASA5510, 1024 MB RAM, CPU Pentium 4 Celeron 1600 MHz
:
ASA Version 9.1(5)4
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard
!
interface Ethernet0/0
 shutdown
 nameif outside
```

```
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object network obj-192.168.100.0
 subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
 host 10.10.10.10
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
 nat (inside,outside) dynamic interface
object network obj-10.10.10.10
 nat (dmz,outside) static 172.20.1.10 dns
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
```

```
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
 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 ip-options
 inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
 message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
 parameters
 message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:3a8e3009aa3db1d6dba143abf25ee408
: end
```

Alternative Lösung: Ziel-NAT

Ziel-NAT kann eine Alternative zur DNS-Dokumentation darstellen. Die Verwendung von Ziel-NAT in dieser Situation erfordert, dass zwischen der öffentlichen Adresse des WWW-Servers auf der Innenseite und der realen Adresse auf der DMZ eine statische Objekt-/automatische NAT-Übersetzung erstellt wird. Ziel-NAT ändert nicht den Inhalt des DNS-A-Datensatzes, der vom DNS-Server an den Client zurückgegeben wird. Stattdessen kann der Client bei Verwendung der

Ziel-NAT in einem Szenario, wie in diesem Dokument beschrieben, die öffentliche IP-Adresse 172.20.1.10 verwenden, die vom DNS-Server zurückgegeben wird, um eine Verbindung zum WWW-Server herzustellen. Mithilfe der statischen Objekt-/Auto-Übersetzung kann die Sicherheits-Appliance die Zieladresse von 172.20.1.10 auf 10.10.10.10 übersetzen. Dies ist der relevante Teil der Konfiguration bei Verwendung der Ziel-NAT:

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

!--- The nat and global commands allow
!--- clients access to the Internet.

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.

object network obj-10.10.10.10-1
host 10.10.10.10
nat (dmz,inside) static 172.20.1.10
```

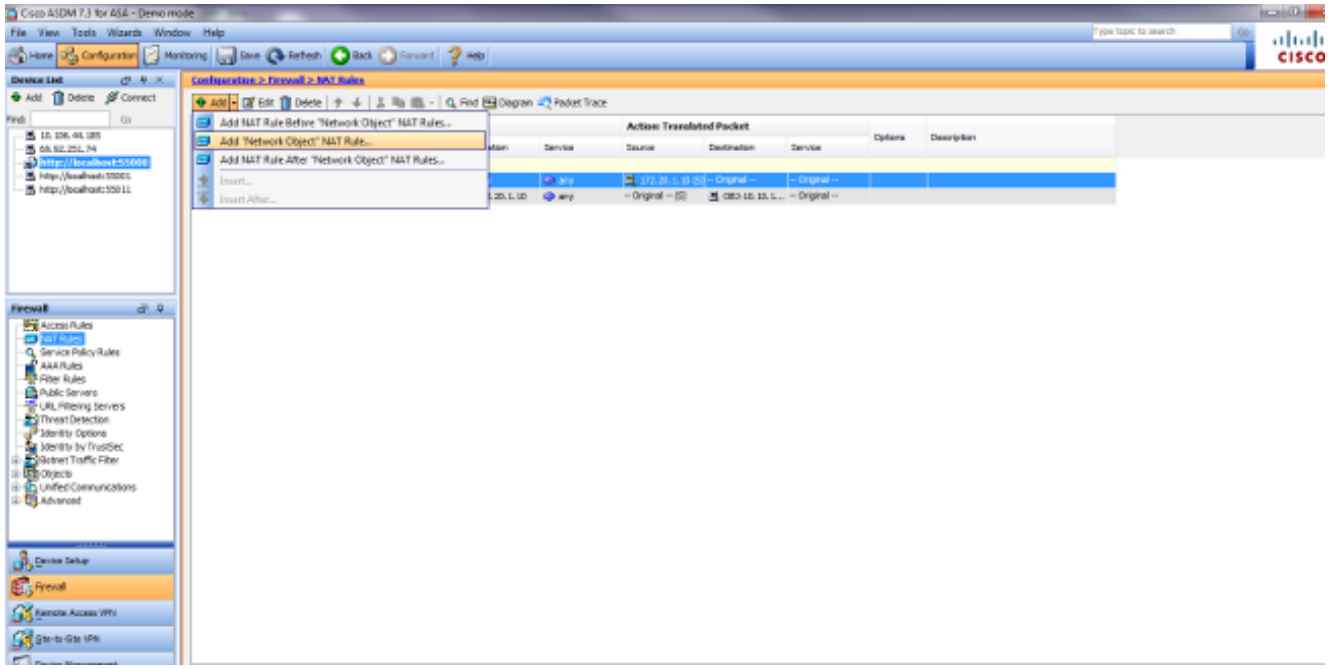
Ziel-NAT erreicht mit manueller/doppelter NAT-Anweisung

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10

object network obj-172.20.1.10
host 172.20.1.10

nat (inside,dmz) source dynamic obj-192.168.100.0 interface
destination static obj-172.20.1.10 obj-10.10.10.10

!--- Static translation to allow hosts on the inside access
!--- to the WWW server via its outside address.
```

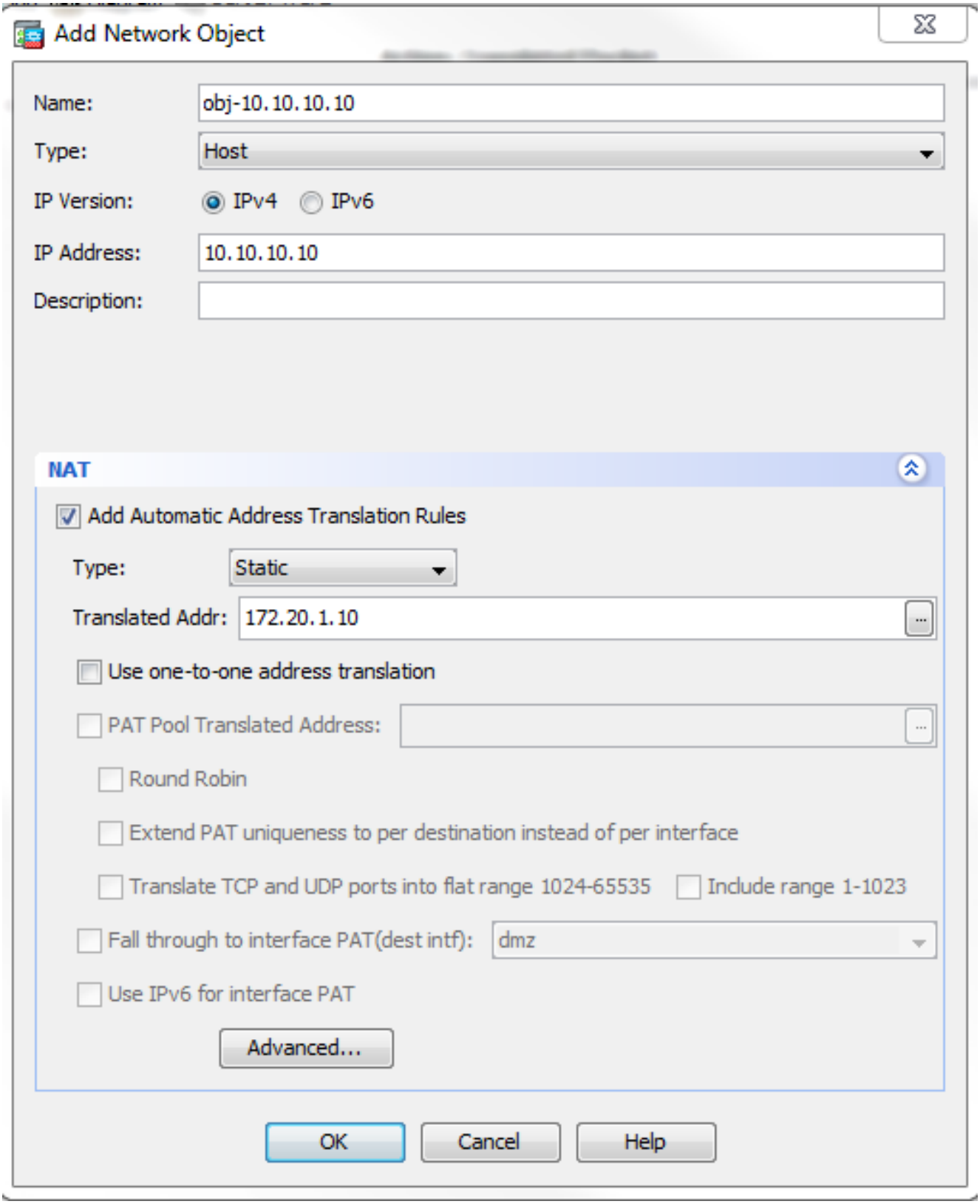
```
access-group OUTSIDE in interface outside

!--- Output suppressed.
```

Gehen Sie wie folgt vor, um die Ziel-NAT im ASDM zu konfigurieren:

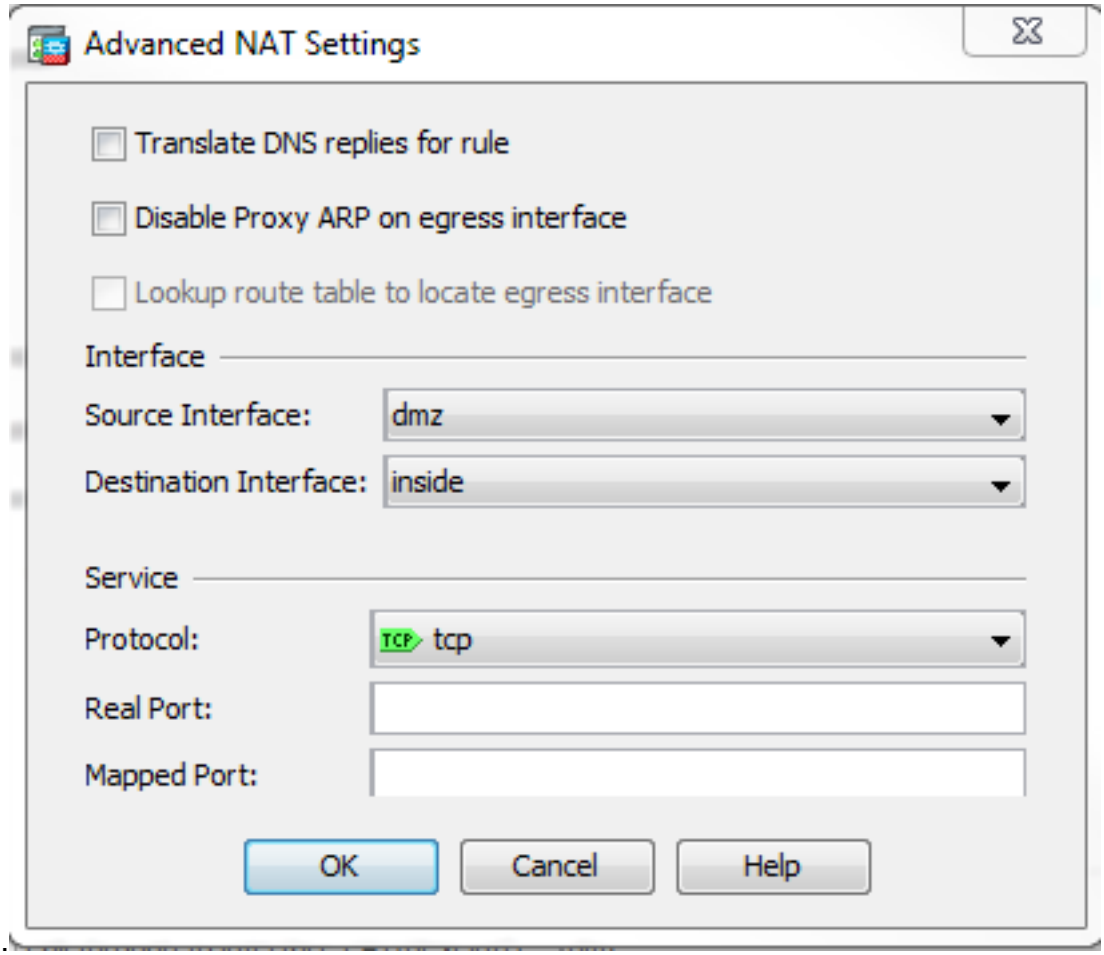
1. Wählen Sie **Configuration > NAT Rules** und wählen Sie **Add > Add "Network Object" NAT Rule (Hinzufügen > "Network Object"-NAT-Regel hinzufügen) aus.**.



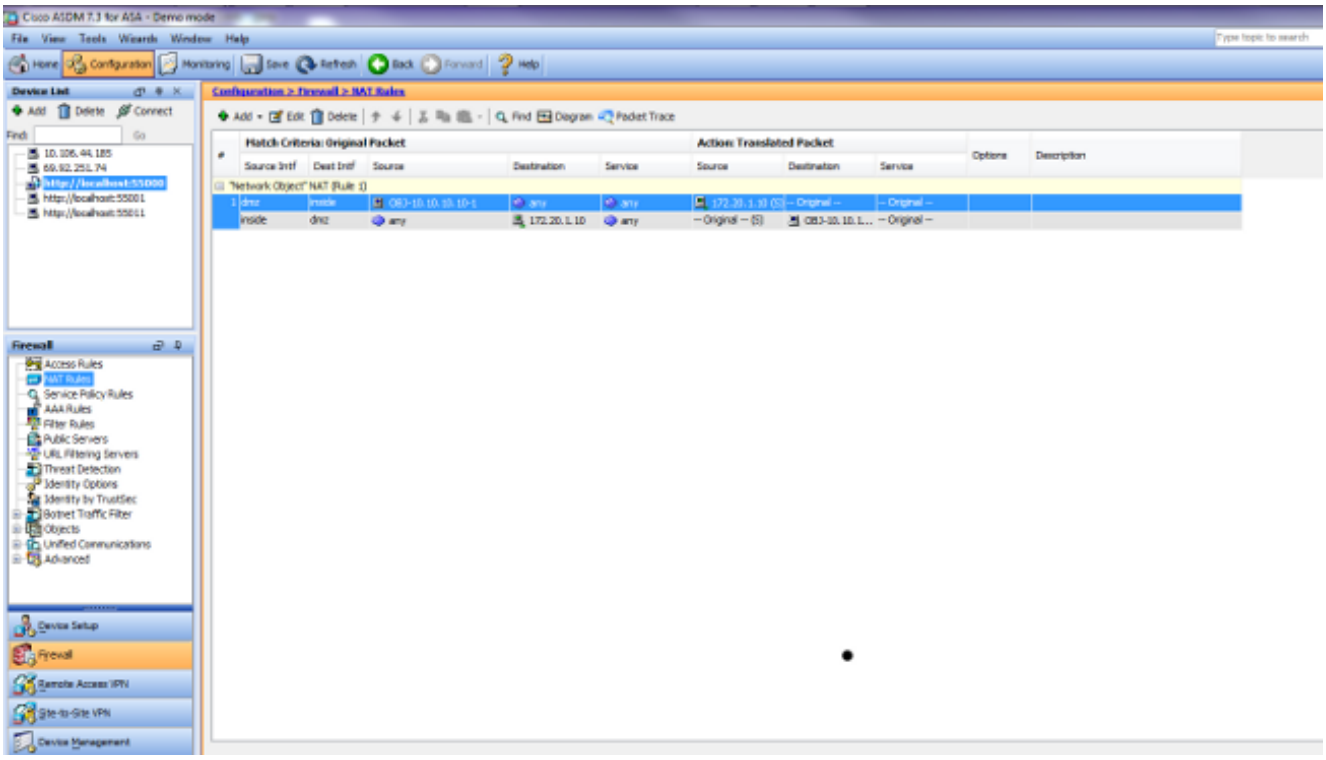
2. Füllen Sie die Konfiguration für die neue statische Übersetzung aus. Geben Sie im Feld Name den Text **obj-10.10.10.10 ein**.Geben Sie im Feld IP Address (IP-Adresse) die Adresse der IP-Adresse des WWW-Servers ein.Wählen Sie in der Dropdown-Liste Type (Typ) die Option **Statisch**.Geben Sie im Feld Translated Addr (Übersetzte Adresse) die Adresse und Schnittstelle ein, der Sie den WWW-Server zuordnen möchten.Klicken Sie auf **Erweitert**.



Wählen Sie in der Dropdown-Liste Quellschnittstelle die Option **dmz aus**.Wählen Sie in der Dropdown-Liste Destination Interface (Zielschnittstelle) die Option **inside** aus.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



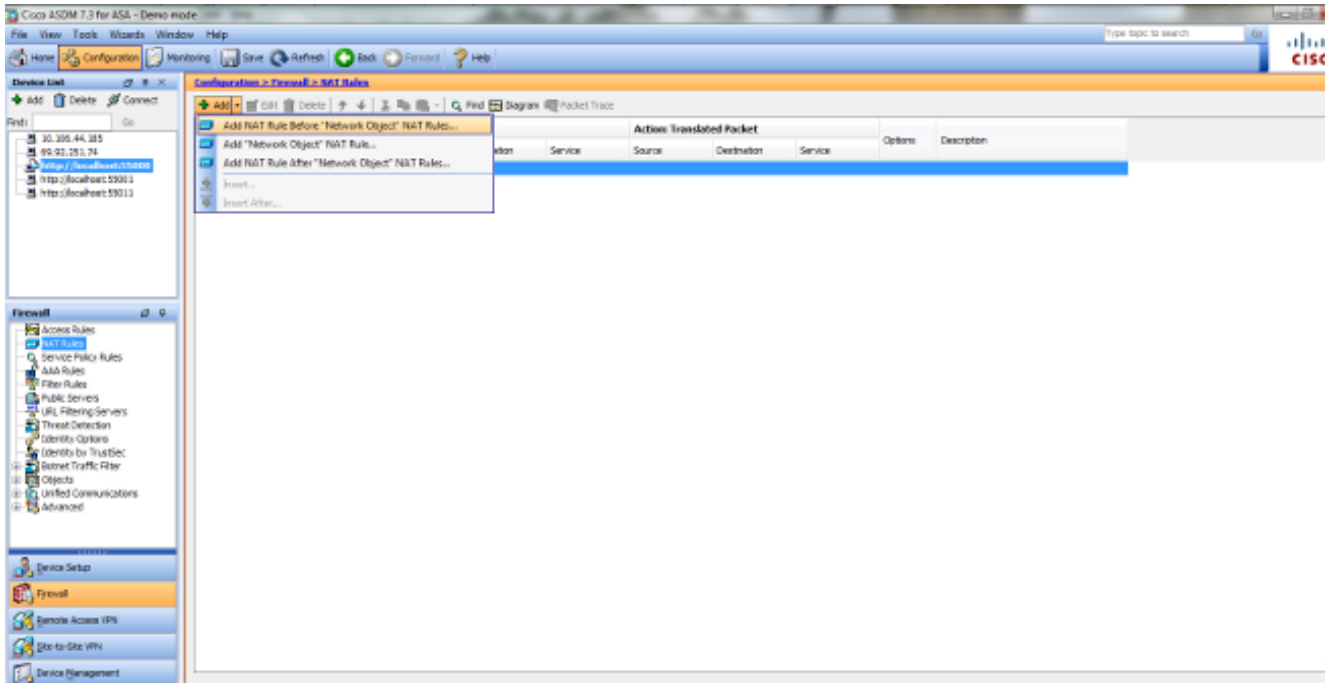
können.



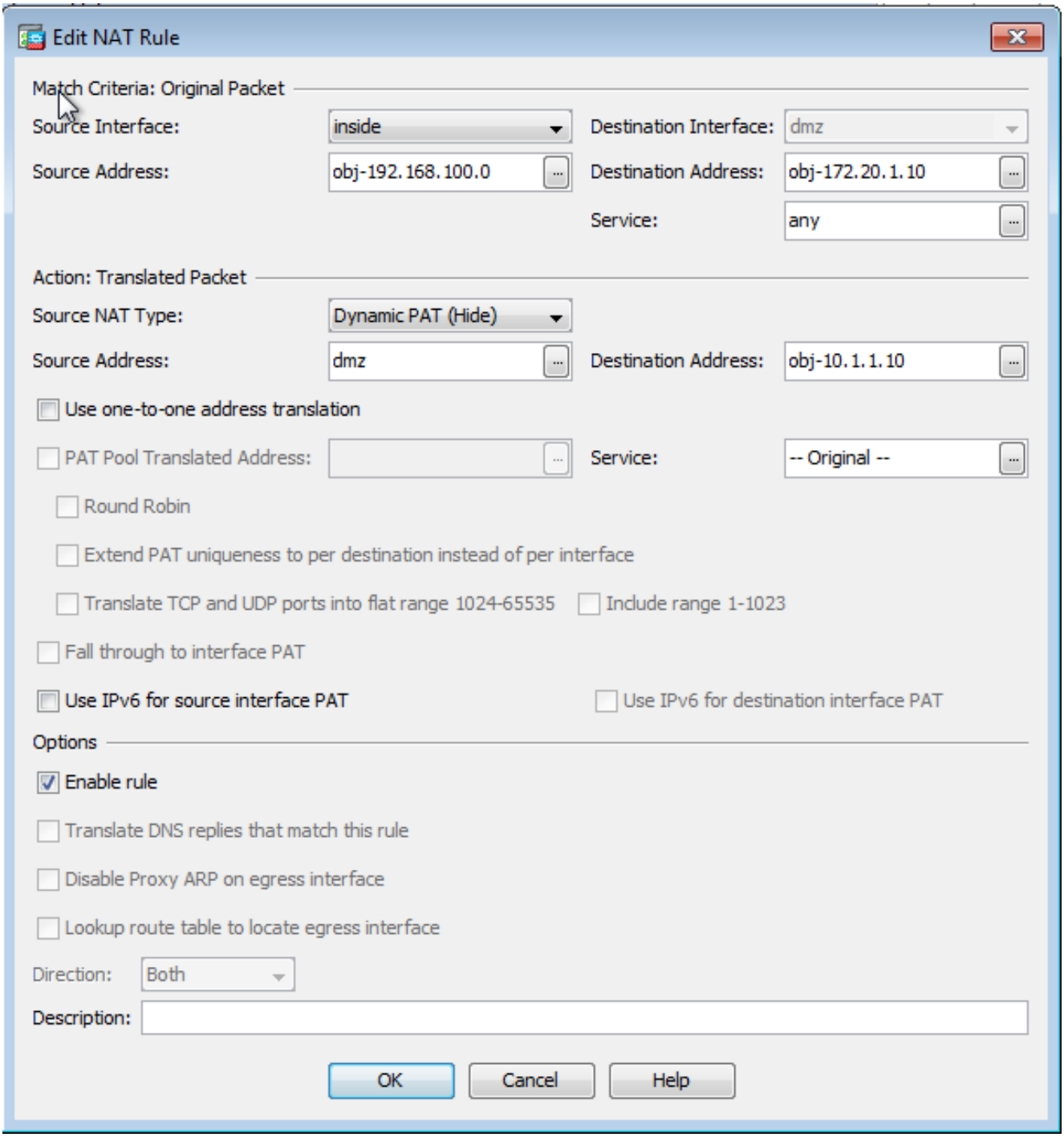
Klicken Sie auf **OK**, um das Fenster Objekt-/automatische NAT-Regel hinzufügen zu verlassen.Klicken Sie auf **Apply**, um die Konfiguration an die Sicherheits-Appliance zu senden.

Alternative Methode mit manueller/doppelter NAT und ASDM

1. Wählen Sie **Configuration > NAT Rules** und wählen Sie **Add > Add Nat Rule (Hinzufügen > NAT Rule (NAT-Regel hinzufügen) vor "Network Object" (Netzwerkobjekt) NAT Rule (NAT-Regel)...**.



2. Füllen Sie die Konfiguration für die manuelle/doppelte NAT-Übersetzung aus. Wählen Sie in der Dropdownliste Quellschnittstelle **innen** aus.Wählen Sie in der Dropdown-Liste Destination Interface (Zielschnittstelle) die Option **dmz**.Geben Sie im Feld Quelladresse das interne Netzwerkobjekt (obj-192.168.100.0) ein.Geben Sie im Feld Zieladresse den Wert t ein.übersetztes DMZ-Server-IP-Objekt (172.20.1.10).Wählen Sie in der Dropdown-Liste Source NAT Type (Quelle-NAT-Typ) die Option **Dynamic PAT (Hide) aus.**.Geben Sie in der Quelladresse [Aktion: Translated Packet section] ein, geben Sie **dmz ein**.Im Ziel Adresse [Aktion: Abschnitt "Übersetztes Paket"] Feld, geben Sie das reale IP-Objekt des DMZ-Servers ein (obj-
10.10.10.10).



3. Klicken Sie auf **OK**, um das Fenster Manuelle/doppelte NAT-Regel hinzufügen zu verlassen.
4. Klicken Sie auf **Apply**, um die Konfiguration an die Sicherheits-Appliance zu senden.

Im Folgenden sind die Ereignisse aufgeführt, die bei der Konfiguration der Ziel-NAT stattfinden. 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 10.10.10.10 ist.
   ```
   %ASA-7-609001: Built local-host dmz:10.10.10.10
   ```
3. Die Sicherheits-Appliance erstellt eine TCP-Verbindung zwischen dem Client und dem WWW-Server. Beachten Sie die zugeordneten Adressen der einzelnen Hosts in Klammern.
   ```
   %ASA-6-302013: Built outbound TCP connection 67956 for dmz:10.10.10.10/80
   (172.20.1.10/80) to inside:192.168.100.2/11001 (192.168.100.2/11001)
   ```
4. Der Befehl **show xlate** auf der Sicherheits-Appliance überprüft, ob der Client-Datenverkehr

über die Sicherheits-Appliance übertragen wird. In diesem Fall wird die erste statische Übersetzung verwendet.

```
ciscoasa#show xlate
3 in use, 9 most used
Global 192.168.100.0 Local 192.168.100.0
Global 172.20.1.10 Local 10.10.10.10
Global 172.20.1.10 Local 10.10.10.10
```

5. Der Befehl **show conn** auf der Sicherheits-Appliance überprüft, ob die Verbindung zwischen Client und WWW-Server über die Sicherheits-Appliance erfolgreich hergestellt wurde. Beachten Sie die tatsächliche Adresse des WWW-Servers in Klammern.

```
ciscoasa#show conn
TCP out 172.20.1.10(10.10.10.10):80 in 192.168.100.2:11001
idle 0:01:38 bytes 1486 flags UIO
```

Endgültige Konfiguration mit Ziel-NAT

Dies ist die endgültige Konfiguration der ASA für die DNS-Dokumentation mit Ziel-NAT und drei NAT-Schnittstellen.

```
ASA Version 9.x
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard
!
interface Ethernet0/0
 shutdown
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
```

```
object network obj-192.168.100.0
 subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
 host 10.10.10.10
object network obj-10.10.10.10-1
 host 10.10.10.10
object network obj-172.20.1.10
 host 172.20.1.10
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
 nat (inside,outside) dynamic interface
object network obj-10.10.10.10
 nat (dmz,outside) static 172.20.1.10
object network obj-10.10.10.10-1
 nat (dmz,inside) static 172.20.1.10
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
```

```
 message-length maximum client auto
 message-length maximum 512
policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
 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 ip-options
 inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
 message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
 parameters
 message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:2cdcc45bfc13f9e231f3934b558f1fd4
: end
```

Konfigurieren

Führen Sie diese 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.

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. Verwenden Sie im Konfigurationsmodus der Richtlinienzuordnung die in den Schritten 1-3 erstellte Richtlinienzuordnung, um anzugeben, dass DNS 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
```

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.

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 inside:192.168.100.10/80
```

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

Zugehörige Informationen

- Cisco ASA 5500-x - Konfigurationsleitfaden
- Cisco Serie ASA 5500-x - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten
- Request for Comments (RFCs)
- Technischer Support und Dokumentation - Cisco Systems