DNS Doctoring de la configuración para tres interfaces NAT en la versión 9.x ASA

Contenido

Introducción

Este documento proporciona una configuración de muestra para realizar el Domain Name System (DNS) que cuida en el dispositivo de seguridad adaptante de las 5500-X Series ASA (ASA) ese objeto de las aplicaciones/declaraciones autos del Network Address Translation (NAT). El cuidarse DNS permite que el dispositivo de seguridad reescriba los Uno-expedientes DNS.

La reescritura DNS realiza dos funciones:

- Traduce a una dirección pública (el routable o el direccionamiento asociado) en una contestación DNS a una dirección privada (la dirección real) cuando el cliente DNS está en

una interfaz privada.
- Traduce a una dirección privada a una dirección pública cuando el cliente DNS está en la interfaz pública.

Prerrequisitos

Requisitos

Estados de Cisco que el examen DNS se debe habilitar para realizar el DNS que se cuida en el dispositivo de seguridad. El examen DNS está prendido por abandono.

Cuando se habilita el examen DNS, el dispositivo de seguridad realiza estas tareas:

- Traduce el expediente DNS basado en la configuración completada con el uso del objeto/de los comandos nat autos (reescritura DNS). La traducción se aplica solamente al Uno-expediente en la contestación DNS. Por lo tanto las búsquedas inversas, que piden el expediente del puntero (PTR), no son afectadas por la reescritura DNS. En la versión ASA 9.0(1) y posterior, la traducción del expediente PTR DNS para las búsquedas de DNS reversibles al usar el IPv4 NAT, el IPv6 NAT, y NAT64 con el examen DNS habilitado para la regla NAT.Nota: La reescritura DNS no es compatible con la traducción de la dirección de puerto estática (PALMADITA) porque las reglas múltiples de la PALMADITA son aplicables para cada Uno-expediente, y la regla de la PALMADITA a utilizar es ambigua.
- Aplica la longitud del mensaje del máximo DNS (el valor por defecto es 512 bytes y el Largo máximo es 65535 bytes). El nuevo ensamble se realiza cuanto sea necesario para verificar que la Longitud del paquete es menos que el Largo máximo configurado. Se cae el paquete si excede el Largo máximo.Nota: Si usted ingresa el comando **dns de la inspección** sin la opción del Largo máximo, el tamaño de paquete DNS no se marca.
- Aplica una longitud del Domain Name de 255 bytes y una longitud de la escritura de la etiqueta de 63 bytes.
- Verifica la integridad del Domain Name referido por el puntero si los punteros de la compresión se encuentran en el mensaje DNS.
- Marca para ver si existe un loop del puntero de la compresión.

Componentes Utilizados

La información en este documento se basa en las 5500-X Series dispositivo de seguridad ASA, versión 9.x.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con las 5500 Series dispositivo de seguridad de

Cisco ASA, versión 8.4 o posterior.

Nota: La Configuración de ASDM es aplicable a la versión 7.x solamente.

Antecedentes

En un intercambio típico DNS, un cliente envía un URL o un nombre de host a un servidor DNS para determinar el IP Address de ese host. El servidor DNS recibe la petición, mira para arriba la asignación del nombre-a-IP-direccionamiento para ese host, y después proporciona el Uno-expediente con la dirección IP al cliente. Mientras que este procedimiento trabaja bien en muchas situaciones, los problemas pueden ocurrir. Estos problemas pueden ocurrir cuando cliente y el host que el cliente intenta alcanzar son ambos en la misma red privada detrás del NAT, pero el servidor DNS usado por el cliente está en otra red pública.

Escenario: Tres interfaces NAT - Dentro de, exterior, DMZ

Topología

Este diagrama es un ejemplo de esta situación. En este caso, el cliente en 192.168.100.2 quiere utilizar **server.example.com** URL para acceder al servidor WWW en 10.10.10.10. El servidor DNS externo en 172.22.1.161 proporcionan los servicios DNS para el cliente. Porque el servidor DNS está situado en otra red pública, no conoce el IP Address privado del servidor WWW. En lugar, conoce el direccionamiento asociado servidor WWW de 172.20.1.10. Así, el servidor DNS contiene la asignación del IP-direccionamiento-a-nombre de **server.example.com a 172.20.1.10**.

Problema: El cliente no puede acceder al servidor WWW

Sin cuidarse DNS u otra solución habilitada en esta situación, si el cliente envía un pedido DNS la dirección IP de **server.example.com**, no puede acceder al servidor WWW. Esto es porque el cliente recibe un Uno-expediente que contenga a la dirección pública asociada de 172.20.1.10 para el servidor WWW. Cuando el cliente intenta acceder esta dirección IP, el dispositivo de seguridad cae los paquetes porque no permite la redirección de paquete en la misma interfaz. Aquí es lo que parece la porción NAT de la configuración cuando el cuidarse DNS no se habilita:

```
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.
```

Esto es lo que parece la configuración en el ASDM cuando el cuidarse DNS no se habilita:

Aquí está una captura de paquetes de los eventos cuando el cuidarse DNS no se habilita:

1. El cliente envía la interrogación DNS.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. La PALMADITA es realizada en la interrogación DNS por el ASA y se remite la interrogación. Observe que la dirección de origen del paquete ha cambiado a la interfaz exterior del ASA.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. El servidor DNS contesta con el direccionamiento asociado del servidor WWW.

```
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. El ASA deshace la traducción de la dirección destino de la respuesta de DNS y adelante del paquete al cliente. Observe que sin cuidarse DNS habilitado, el **addr** en la respuesta sigue siendo el direccionamiento asociado del servidor WWW.

```
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. En este momento el cliente intenta acceder al servidor WWW en 172.20.1.10. El ASA crea a Entrada de conexión para esta comunicación. Sin embargo, porque no permite que el tráfico fluya desde adentro al exterior al DMZ, los tiempos de conexión hacia fuera. Los registros ASA muestran esto:`%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`**

Solución: palabra clave “dns”

DNS Doctoring con la palabra clave “dns”

El DNS que se cuida con la palabra clave **dns** da a dispositivo de seguridad la capacidad de interceptar y reescribir el contenido del servidor DNS contesta al cliente. Cuando está configurado correctamente, el dispositivo de seguridad puede alterar el Uno-expediente para permitir al cliente en tal escenario como se debate en el “problema: El cliente no puede acceder sección al servidor WWW” para conectar. En esta situación con cuidarse DNS habilitado, el dispositivo de seguridad reescribe el Uno-expediente para dirigir al cliente a 10.10.10.10 en vez de 172.20.1.10. Se habilita el cuidarse DNS cuando usted agrega la palabra clave **dns a una** declaración NAT estática (versión 8.2 y anterior) o al objeto/a la sentencia NAT auto (versión 8.3 y posterior).

Versión 8.2 y anterior

Ésta es la configuración final del ASA para realizar el DNS que se cuida con la palabra clave **dns** y tres interfaces NAT para las versiones 8.2 y anterior.

```
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
```

Versión 8.3 y posterior

```
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.
```

Configuración de ASDM

Complete estos pasos para configurar el DNS que se cuida en el ASDM:

1. Elija la **configuración > las reglas NAT** y elija el objeto/la regla auto que se modificarán. Haga clic en **Editar**.
2. Tecleo **avanzado…**
3. Marque las **contestaciones del traducir DNS para la** casilla de verificación de la **regla**.
4. Haga Click en OK para dejar la ventana de las opciones NAT.
5. Haga Click en OK para dejar el Editar Objeto/la ventana auto de la regla NAT.
6. El tecleo **se aplica** para enviar su configuración al dispositivo de seguridad.

Verificación

Aquí está una captura de paquetes de los eventos cuando se habilita el cuidarse DNS:

1. El cliente envía la interrogación DNS.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. La PALMADITA es realizada en la interrogación DNS por el ASA y se remite la interrogación. Observe que la dirección de origen del paquete ha cambiado a la interfaz exterior del ASA.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. El servidor DNS contesta con el direccionamiento asociado del servidor WWW.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. El ASA deshace la traducción de la dirección destino de la respuesta de DNS y adelante del paquete al cliente. Observe que con cuidarse DNS habilitado, el **addr** en la respuesta está reescrito para ser la dirección real del servidor WWW.

```
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. En este momento, el cliente intenta acceder al servidor WWW en 10.10.10.10. La conexión tiene éxito.

Configuración final con la palabra clave “dns”

Ésta es la configuración final del ASA para realizar el DNS que se cuida con la palabra clave **dns**

y tres interfaces NAT.

```
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
```

Solución alternativa: NAT de destino

El NAT de destino puede proporcionar una alternativa a cuidarse DNS. El uso del NAT de destino en esta situación requiere que un objeto estático/una traducción de NAT auto esté creado entre la dirección pública del servidor WWW en el interior y la dirección real en el DMZ. El NAT de destino no cambia el contenido del Uno-expediente DNS que se vuelve del servidor DNS al cliente. En lugar, cuando usted utiliza el NAT de destino en un escenario tal como discutido en este documento, el cliente puede utilizar al IP Address público **172.20.1.10** que es vuelto por el servidor DNS para conectar con el servidor WWW. El objeto estático/la traducción auto permite que el dispositivo de seguridad traduzca a la dirección destino de **172.20.1.10 a 10.10.10.10**. Aquí está la porción pertinente de la configuración cuando se utiliza el NAT de destino:

```
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
```

NAT de destino alcanzado con el manual/dos veces la sentencia 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

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.
```

Complete estos pasos para configurar el NAT de destino en el ASDM:

1. Elija la **configuración > las reglas NAT** y elija **agregan > Add la regla NAT del "objeto de red"….**
2. Complete la configuración para la nueva traducción estática. En el campo de nombre, ingrese **obj-10.10.10.10**.En el campo del IP Address, ingrese el direccionamiento del IP Address del servidor WWW.De la lista desplegable del tipo, elija los **parásitos atmosféricos**.En el campo traducido del addr, ingrese el direccionamiento e interconecte que usted quiere asociar al servidor WWW a.Haga clic en **Advanced**.En la lista desplegable de la interfaz de origen, elija el **dmz**.En la lista desplegable de la interfaz de destino, elija **dentro**.En este caso, la interfaz interior se elige para permitir que los host en la interfaz interior accedan al servidor WWW vía el direccionamiento asociado 172.20.1.10.Haga Click en OK para dejar el objeto del agregar/la ventana auto de la regla NAT.El tecleo **se aplica** para enviar la configuración al dispositivo de seguridad.

Método alternativo con el manual/dos veces el NAT y el ASDM

1. Elija la **configuración > las reglas NAT** y elija **agregan > Add la regla nacional antes de la regla NAT del "objeto de red"….**
2. Complete la configuración para la traducción manual/dos veces nacional. En la lista desplegable de la interfaz de origen, elija **dentro**.En la lista desplegable de la interfaz de destino, elija el **dmz**.En el campo de dirección de origen, ingrese el objeto de red interna (obj-192.168.100.0).En el campo dirección de destino, ingrese el objeto traducido IP del servidor DMZ (172.20.1.10).En la lista desplegable del tipo de la fuente NAT, elija la **PALMADITA dinámica (piel)**.En la dirección de origen [acción: El campo traducido de la sección del paquete], ingresa el **dmz**.En la dirección destino [acción: El campo traducido de la sección del paquete], ingresa el objeto real IP del servidor DMZ (obj-10.10.10.10).
3. Haga Click en OK para dejar el agregar ventana a manual/dos veces NAT de la regla.
4. El tecleo **se aplica** para enviar la configuración al dispositivo de seguridad.

Aquí está la Secuencia de eventos que ocurre cuando se configura el NAT de destino. Asuma que el cliente ha preguntado al servidor DNS y ha recibido ya una contestación de **172.20.1.10** para el direccionamiento del servidor WWW:

1. El cliente intenta entrar en contacto al servidor WWW en 172.20.1.10.`%ASA-7-609001: Built local-host inside:192.168.100.2`
2. El dispositivo de seguridad ve la petición y reconoce que el servidor WWW es 10.10.10.10.`%ASA-7-609001: Built local-host dmz:10.10.10.10`
3. El dispositivo de seguridad crea una conexión TCP entre el cliente y el servidor WWW. Observe los direccionamientos asociados de cada host entre paréntesis.`%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. El comando show xlate en el dispositivo de seguridad verifica que el tráfico del cliente traduzca a través del dispositivo de seguridad. En este caso, la primera traducción estática es funcionando.
```
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. El comando show conn en el dispositivo de seguridad verifica que la conexión haya tenido éxito entre el cliente y el servidor WWW a través del dispositivo de seguridad. Observe a la dirección real del servidor WWW entre paréntesis.
```
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
```

Configuración final con el NAT de destino

Ésta es la configuración final del ASA para realizar el DNS que se cuida con el NAT de destino y tres interfaces NAT.

```
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
```

Configurar

Complete estos pasos para habilitar el examen DNS (si se ha inhabilitado previamente). En este ejemplo, el examen DNS se agrega a la directiva global predeterminada del examen, que es aplicada global por un **comando service-policy** como si el ASA comenzó con una configuración predeterminada.

1. Cree una correspondencia de políticas del examen para el DNS.`ciscoasa(config)#`**`policy-map type inspect dns MY_DNS_INSPECT_MAP`**
2. Del modo de la configuración de correspondencia de políticas, ingrese el modo de la Configuración de parámetros para especificar los parámetros para el motor del examen.`ciscoasa(config-pmap)#`**`parameters`**
3. En el modo de la Configuración de parámetros del directiva-mapa, especifique la longitud del mensaje máxima para que los mensajes DNS sean 512.`ciscoasa(config-pmap-p)#`**`message-length maximum 512`**
4. Salga fuera del modo de la Configuración de parámetros del directiva-mapa y del modo de la configuración de correspondencia de políticas.`ciscoasa(config-pmap-p)#`**`exit`**
   `ciscoasa(config-pmap)#`**`exit`**

5. Confirme que el directiva-mapa del examen fue creado según lo deseado.
```
ciscoasa(config)#show run policy-map type inspect dns
!
policy-map type inspect dns MY_DNS_INSPECT_MAP
parameters
message-length maximum 512
!
```
6. Ingrese el modo de la configuración de correspondencia de políticas para el **global_policy**.
```
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#
```
7. En el modo de la configuración de correspondencia de políticas, especifique la correspondencia predeterminada de la clase de la capa 3/4, **inspection_default**.
```
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#
```
8. En el modo de configuración de clase del directiva-mapa, utilice la correspondencia de políticas del examen creada en los pasos 1-3 para especificar que el DNS debe ser examinado.
```
ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP
```
9. Salga fuera del modo de configuración de clase del directiva-mapa y del modo de la configuración de correspondencia de políticas.
```
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```
10. Verifique que el directiva-mapa del **global_policy** esté configurado según lo deseado.
```
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. Verifique que el global_policy sea aplicado global por una servicio-directiva.
```
ciscoasa(config)#show run service-policy
service-policy global_policy global
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos

comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Capture el tráfico DNS

Un método a verificar que los expedientes de las reescrituras DNS del dispositivo de seguridad sean correctamente capturar los paquetes en la pregunta, como se debate en el ejemplo anterior. Complete estos pasos para capturar el tráfico en el ASA:

1. Cree una lista de acceso para cada caso de la captura que usted quiere crear. El ACL debe especificar el tráfico que usted quiere capturar. En este ejemplo, se han creado dos ACL. El ACL para el tráfico en la interfaz exterior:`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.
   ```

   El ACL para el tráfico en la interfaz interior:`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. Cree los casos de la captura:`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. Vea las capturas.Aquí es lo que parecen las capturas del ejemplo después de que se haya pasado un cierto tráfico DNS:`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. (Opcional) copie las capturas a un servidor TFTP en el formato PCAP para el análisis en otra aplicación.Las aplicaciones que pueden analizar el formato PCAP pueden mostrar los detalles adicionales tales como el nombre y la dirección IP en los expedientes DNS A.`ciscoasa#`**`copy /pcap capture:DNSINSIDE tftp`**

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

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

La reescritura DNS no se realiza

Aseegurese que usted tiene examen DNS configurado en el dispositivo de seguridad.

Creación de la traducción fallada

Si una conexión no se puede crear entre el cliente y el servidor WWW, puede ser que sea debido a un misconfiguration NAT. Marque los registros del dispositivo de seguridad para los mensajes que indican que un protocolo no pudo crear una traducción a través del dispositivo de seguridad. Si aparecen tales mensajes, verifique que el NAT se haya configurado para el tráfico deseado y que no hay direccionamientos incorrectos.

```
%ASA-3-305006: portmap translation creation failed for tcp src
inside:192.168.100.2/11000 dst inside:192.168.100.10/80
```

Borre las entradas del xlate, y entonces quite y reaplique las sentencias NAT para resolver este error.

Información Relacionada

- Guía de configuración de Cisco ASA 5500-x
- Referencias de comandos de las 5500-x Series de Cisco ASA
- Field Notice de seguridad del producto
- Request For Comments (RFC)
- Soporte Técnico y Documentación - Cisco Systems