

PIX/ASA: Realice el DNS Doctoring con el comando static y el ejemplo de configuración de dos interfaces NAT

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[Antecedentes](#)

[Escenario: Dos interfaces NAT \(dentro, afuera\)](#)

[Topología](#)

[Problema: El cliente no puede acceder al servidor WWW](#)

[Solución: palabra clave "dns"](#)

[Solución alternativa: Hairpinning](#)

[Examen de la configuración DNS](#)

[Configuración del DNS dividido](#)

[Verificación](#)

[Capture el tráfico DNS](#)

[Troubleshooting](#)

[La reescritura DNS no se realiza](#)

[Creación de la traducción fallada](#)

[Contestación del descenso UDP DNS](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una configuración de muestra para realizar el Domain Name System (DNS) que se cuida en el dispositivo de seguridad adaptante de las 5500 Series ASA o el dispositivo de seguridad de la serie PIX 500 usando las declaraciones de la traducción de dirección de red estática (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.

Nota: La configuración en este documento contiene dos interfaces NAT; dentro y afuera. Por un ejemplo del DNS que se cuida con el statics y tres interfaces NAT (dentro, exterior y dmz), refiera al [PIX/ASA: Realice el DNS Doctoring con el comando static y el ejemplo de configuración de tres interfaces NAT](#).

Refiera al [PIX/ASA 7.x NAT y las declaraciones](#) y el [usar nacionales, globales, estáticos, conducto, y los comandos access-list y redirección de puerto de la PALMADITA \(expedición\) en el PIX](#) para más información sobre cómo utilizar el NAT en un dispositivo de seguridad.

[prerrequisitos](#)

[Requisitos](#)

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. Si se ha apagado, vea la sección del [examen de la configuración DNS](#) más adelante en este documento para volverlo a permitir.

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

- Traduce el expediente DNS basado en la configuración completada usando los **parásitos atmosféricos** y los **comandos nat** (reescritura DNS). La traducción se aplica solamente al Uno-expediente en la contestación DNS. Por lo tanto, búsquedas inversas, que piden el expediente PTR, no son afectados por la reescritura DNS. **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 publica 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 Series dispositivo de seguridad ASA, versión 7.2(1).

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 el dispositivo de seguridad de la serie del Cisco PIX 500, versión 6.2 o posterior.

Nota: La configuración del Cisco Adaptive Security Device Manager (ASDM) es aplicable a la versión 7.x solamente.

[Convenciones](#)

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

[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: Dos interfaces NAT \(dentro, afuera\)](#)

[Topología](#)

En este escenario, cliente y el servidor WWW que el cliente intenta alcanzar son ambos situados en la interfaz interior del ASA. La PALMADITA dinámica se configura para permitir el acceso al cliente a Internet. El NAT estático con una lista de acceso se configura para permitir el acceso al servidor a Internet, así como permite que los host de Internet accedan al servidor WWW.

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 192.168.100.10. 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: 172.20.1.10 del 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:

```
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.
```

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 a dentro, 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 la sección del servidor WWW](#) para conectar. En esta situación, con cuidarse DNS habilitado, el dispositivo de seguridad reescribe el Uno-expediente para dirigir al cliente a **192.168.100.10**, en vez de **172.20.1.10**. Se habilita el cuidarse DNS cuando usted agrega la palabra clave **dns** a una declaración NAT estática. Aquí es lo que parece la porción NAT de la configuración cuando se habilita el cuidarse DNS:

```
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.
```

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

1. Navegue a la **configuración > al NAT** y elija la regla NAT estática que se modificará. Haga clic en **Editar**.
2. **Opciones NAT del teclado....**
3. Marca el **traducir DNS contesta que hace juego** la casilla de verificación de la **regla de traducción**.
4. Haga Click en OK para dejar la ventana de las opciones NAT. Haga Click en OK para dejar al editar la ventana NAT estática de la regla. El teclado **se aplica** para enviar su configuración al dispositivo de seguridad.

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
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. En este momento, el cliente intenta acceder al servidor WWW en 192.168.100.10. La conexión tiene éxito. No se captura ningún tráfico en el ASA porque el cliente y servidor está en la misma subred.

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 dos interfaces NAT.

Configuración final ASA 7.2(1)

```
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
```

Solución alternativa: Hairpinning

Hairpinning con el NAT estático

Precaución: El hairpinning con el NAT estático implica el enviar de todo el tráfico entre el cliente y el servidor WWW a través del dispositivo de seguridad. Considere cuidadosamente la cantidad de tráfico prevista y las capacidades de su dispositivo de seguridad antes de que usted implemente esta solución.

El hairpinning es el proceso por el cual se retira el tráfico es enviado la misma interfaz en la cual llegó. Esta característica fue introducida en la versión de software 7.0 del dispositivo de seguridad. Para las versiones anterior de 7.2(1), se requiere que por lo menos un brazo del tráfico hairpinned (entrante o saliente) esté cifrado. A partir de la 7.2(1) y posterior, este requisito es no más en el lugar. El tráfico entrante y el tráfico saliente pudieron ser unencrypted cuando usted el uso 7.2(1).

El hairpinning, conjuntamente con una declaración NAT estática, se puede utilizar para alcanzar el mismo efecto que cuidarse DNS. Este método no cambia el contenido del Uno-expediente DNS que se vuelve del servidor DNS al cliente. En lugar, cuando el hairpinning se utiliza, por ejemplo en el escenario discutido en este documento, el cliente puede utilizar el direccionamiento de **172.20.1.10** que es vuelto por el servidor DNS para conectar.

Aquí es lo que parece la porción pertinente de la configuración cuando usted utiliza el hairpinning y el NAT estático para alcanzar un efecto que se cuida DNS. Los comandos en intrépido se explican minuciosamente en el extremo de esta salida:

```
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 statement 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.
```

- **tráfico de seguridad igual** — Este comando permite al tráfico del mismo nivel de seguridad para transitar el dispositivo de seguridad. Las palabras claves de la **intra-interfaz del permiso** admiten que el tráfico de seguridad igual para ingresar y para dejar lo mismo interconecta, así el hairpinning se habilita. **Nota:** Refiera al [tráfico de seguridad igual](#) para más información sobre el hairpinning y el **comando same-security-traffic**.
- **(dentro) 1 interfaz global** — Todo el tráfico que cruza el dispositivo de seguridad debe experimentar el NAT. Este comando utiliza el direccionamiento de la interfaz interior del dispositivo de seguridad para habilitar el tráfico que ingresa la interfaz interior para experimentar la PALMADITA mientras que hairpinned se retira la interfaz interior.
- **(dentro, dentro) netmask estático 255.255.255.255 de 172.20.1.10 192.168.100.10** — esta entrada NAT estática crea una segunda asignación para el IP Address público del servidor WWW. Sin embargo, a diferencia de la primera entrada NAT estática, este vez el direccionamiento 172.20.1.10 se asocia a la interfaz interior del dispositivo de seguridad. Esto permite que el dispositivo de seguridad responda a las peticiones que ve para este direccionamiento en la interfaz interior. Entonces, reorienta esas peticiones a la dirección real del servidor WWW consigo mismo.

Complete estos pasos para configurar el hairpinning con el NAT estático en el ASDM:

1. Navegue al **Configuration (Configuración) > Interfaces (Interfaces)**.
2. En la parte inferior de la ventana, marque el **tráfico del permiso entre dos o más host conectados con el mismo** cuadro de comprobaciones de interfaz.
3. Haga clic en Apply (Aplicar).
4. Navegue a la **configuración > al NAT** y elija **agregar > Add la regla NAT estática....**
5. Completan la configuración para la nueva traducción estática. Pueble el área de la **dirección real** con la información del servidor WWW. Pueble el área de la **traducción estática** con el direccionamiento e interconecte que usted quiere asociar al servidor WWW a. 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.
6. Haga Click en OK para dejar al agregar la ventana NAT estática de la regla.
7. Elija la traducción dinámica existente de la PALMADITA y el tecleo **edita**.
8. Elija **dentro del** cuadro de la desconexión de la interfaz.
9. Haga clic en Add (Agregar).
10. Elija el **Port Address Translation (PAT)** marcado botón de radio **usando la dirección IP de la interfaz**. Haga clic en Add (Agregar).
11. Haga Click en OK para dejar la ventana de la agrupación global de direcciones del agregar. Haga Click en OK para dejar al editar la ventana dinámica de la regla NAT. El tecleo **se aplica** para enviar su configuración al dispositivo de seguridad.

Aquí está la Secuencia de eventos que ocurre cuando se configura el hairpinning. 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 está en 192.168.100.10.%ASA-7-609001: Built local-host inside:192.168.100.10
3. El dispositivo de seguridad crea una traducción dinámica de la PALMADITA para el cliente. La fuente del tráfico del cliente ahora es la interfaz interior del dispositivo de seguridad: 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. El dispositivo de seguridad crea una conexión TCP entre el cliente y el servidor WWW consigo mismo. Observe los direccionamientos asociados de cada host entre paréntesis.%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. El comando **show xlate** en el dispositivo de seguridad verifica que el tráfico del cliente traduzca a través del dispositivo de seguridad.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. El comando **show conn** en el dispositivo de seguridad verifica que la conexión haya tenido éxito entre el dispositivo de seguridad y el servidor WWW en nombre del cliente. Observe a la dirección real del cliente entre paréntesis.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

Configuración final con el hairpinning y el NAT estático

Ésta es la configuración final del ASA que utiliza el hairpinning y el NAT estático para alcanzar un efecto que se cuida DNS con dos interfaces NAT.

Configuración final ASA 7.2(1)

```
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 statement 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

```

Nota: Refiera a este vídeo, [Conexión mediante pines en Cisco ASA \(clientes registrados solamente\)](#), para más información sobre diversos escenarios donde la conexión mediante pines podría ser utilizada.

Configure el examen DNS

Para habilitar el examen DNS (si se ha inhabilitado previamente), realice estos pasos. 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. Refiérase [usando el Marco de políticas modular](#) para más información sobre las políticas de servicio y el examen.

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 del maxiumum 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, especifique que el DNS se debe examinar usando la correspondencia de políticas del examen creada en los pasos 1-3.

```
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
```

Configuración del DNS dividido

Publique el **DNS dividido** ordenan en el modo de configuración de la grupo-directiva para ingresar una lista de dominios que se resolverán a través del túnel dividido. No utilice la **ninguna** forma de este comando para borrar una lista.

Cuando no hay listas del dominio del Túnel dividido, los usuarios heredan cualquiera que existe en la directiva del grupo predeterminado. Publique el **comando none del DNS dividido** para prevenir la herencia de las listas del dominio del Túnel dividido.

Utilice un único espacio para separar cada entrada en la lista de dominios. No hay límite en el número de entradas, pero la cadena entera puede estar no más que 255 caracteres. Usted puede utilizar solamente los caracteres alfanuméricos, los guiones (-), y los períodos (.). **El ningún DNS dividido** ordena, cuando está utilizado sin los argumentos, borra todos los valores actuales, que incluye un valor nulo creado cuando usted publica el **comando none del DNS dividido**.

Este ejemplo muestra cómo configurar los dominios Domain1, Domain2, Domain3 y Domain4 para ser resuelto a través del Túnel dividido para la directiva del grupo nombrada FirstGroup:

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

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 del pcap para el análisis en otra aplicación. Las aplicaciones que pueden analizar el formato del pcap pueden mostrar los detalles adicionales tales como el nombre y la dirección IP en los Uno-expedientes DNS.

```
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

Asegúrese que usted tiene examen DNS configurado en el dispositivo de seguridad. Vea la sección del [examen de la configuración DNS](#).

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 misconfiguración 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 dmz:10.10.10.10/23
```

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

error.

[Caiga la contestación UDP DNS](#)

Es posible que usted recibe este mensaje de error debido al descenso del paquete DNS:

```
%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.
```

Aumente la longitud del paquete DNS entre 512-65535 para resolver este problema.

Ejemplo:

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

[Información Relacionada](#)

- [Cisco PIX Firewall Software](#)
- [Referencias de Comandos de Cisco Secure PIX Firewall](#)
- [Field Notice de seguridad del producto](#)
- [Request For Comments \(RFC\)](#)
- [Conexión mediante pines en Cisco ASA](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)