Configuración de ZBFW mediante coincidencia de patrón de ACL de FQDN en la serie C8300

Contenido

Introducción

Este documento describe el procedimiento para configurar ZBFW con coincidencia de patrón de ACL FQDN en modo autónomo en la plataforma C8300.

Prerequisites

Requirements

Cisco le recomienda que tenga conocimiento acerca de este tema:

- Firewall de políticas basadas en zonas (ZBFW)
- Routing y reenvío virtuales (VRF)
- traducción de Dirección de Red (NAT)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- C8300-2N2S-6T 17.12.02

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El firewall de políticas basadas en zonas (ZBFW) es un método avanzado de configuración del firewall en los dispositivos Cisco IOS® y Cisco IOS XE que permite crear zonas de seguridad dentro de la red.

ZBFW permite a los administradores agrupar interfaces en zonas y aplicar políticas de firewall al tráfico que se mueve entre estas zonas.

Las ACL de FQDN (listas de control de acceso de nombres de dominio completamente calificadas), utilizadas con un ZBFW en los routers de Cisco, permiten a los administradores crear reglas de firewall que coincidan con el tráfico basándose en nombres de dominio en lugar de sólo direcciones IP.

Esta característica es especialmente útil cuando se trata de servicios alojados en plataformas como AWS o Azure, donde la dirección IP asociada a un servicio puede cambiar con frecuencia.

Simplifica la gestión de las políticas de control de acceso y mejora la flexibilidad de las configuraciones de seguridad dentro de la red.

Configurar

Diagrama de la red

Este documento presenta la configuración y verificación de ZBFW basándose en este diagrama. Se trata de un entorno simulado que utiliza BlackJumboDog como servidor DNS.

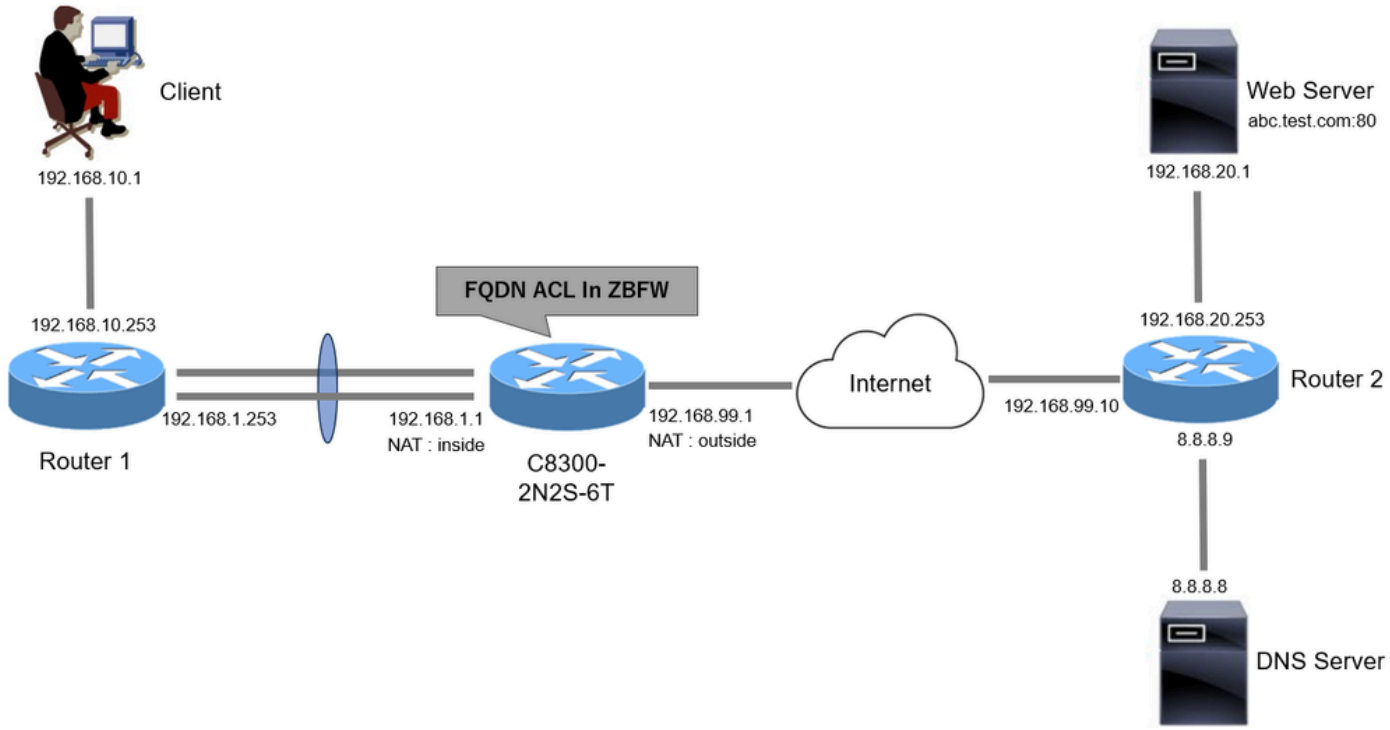


Diagrama de la red

Configuraciones

Esta es la configuración para permitir la comunicación del cliente al servidor web.

Paso 1. (Opcional) Configuración de VRF

La función VRF (Virtual Routing and Forwarding, Enrutamiento y reenvío virtuales) permite crear y administrar varias tablas de enrutamiento independientes en un único router. En este ejemplo, creamos un VRF llamado WebVRF y realizamos el ruteo para las comunicaciones relacionadas.

```
vrf definition WebVRF
rd 65010:10
!
address-family ipv4
route-target export 65010:10
route-target import 65010:10
exit-address-family
!
address-family ipv6
route-target export 65010:10
route-target import 65010:10
exit-address-family

ip route vrf WebVRF 8.8.8.8 255.255.255.255 GigabitEthernet0/0/3 192.168.99.10
ip route vrf WebVRF 192.168.10.0 255.255.255.0 Port-channel1.2001 192.168.1.253
ip route vrf WebVRF 192.168.20.0 255.255.255.0 GigabitEthernet0/0/3 192.168.99.10
```

Paso 2. Configurar interfaz

Configure información básica como miembro de zona, VRF, NAT y direcciones IP para las interfaces interna y externa.

```
interface GigabitEthernet0/0/1
no ip address
negotiation auto
lacp rate fast
channel-group 1 mode active

interface GigabitEthernet0/0/2
no ip address
negotiation auto
lacp rate fast
channel-group 1 mode active

interface Port-channel1
no ip address
no negotiation auto

interface Port-channel1.2001
encapsulation dot1Q 2001
vrf forwarding WebVRF
ip address 192.168.1.1 255.255.255.0
ip broadcast-address 192.168.1.255
no ip redirects
no ip proxy-arp
ip nat inside
zone-member security zone_client

interface GigabitEthernet0/0/3
vrf forwarding WebVRF
ip address 192.168.99.1 255.255.255.0
ip nat outside
zone-member security zone_internet
speed 1000
no negotiation auto
```

Paso 3. (Opcional) Configuración de NAT

Configure NAT para las interfaces internas y externas. En este ejemplo, la dirección IP de origen del cliente (192.168.10.1) se traduce a 192.168.99.100.

```
ip access-list standard nat_source
10 permit 192.168.10.0 0.0.0.255

ip nat pool natpool 192.168.99.100 192.168.99.100 prefix-length 24
ip nat inside source list nat_source pool natpool vrf WebVRF overload
```

Paso 4. Configurar ACL de FQDN

Configure la ACL de FQDN para que coincida con el tráfico de destino. En este ejemplo, utilice el carácter comodín '*' en la coincidencia de patrones del grupo de objetos FQDN para que coincida con el FQDN de destino.

```
object-group network src_net
192.168.10.0 255.255.255.0

object-group fqdn dst_test_fqdn
pattern .*\.test\.com

object-group network dst_dns
host 8.8.8.8

ip access-list extended Client-WebServer
1 permit ip object-group src_net object-group dst_dns
5 permit ip object-group src_net fqdn-group dst_test_fqdn
```

Paso 5. Configuración de ZBFW

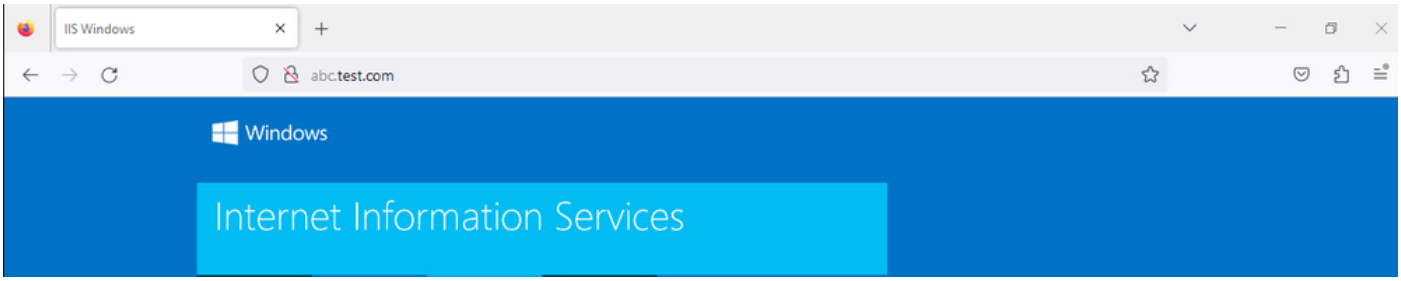
Configuración de zona, mapa de clase y mapa de política para ZBFW. En este ejemplo, mediante el uso del mapa de parámetros, los registros se generan cuando ZBFW permite el tráfico.

```
zone security zone_client
zone security zone_internet

parameter-map type inspect inspect_log
audit-trail on

class-map type inspect match-any Client-WebServer-Class
match access-group name Client-WebServer

policy-map type inspect Client-WebServer-Policy
class type inspect Client-WebServer-Class
inspect inspect_log
class class-default
drop log

zone-pair security Client-WebServer-Pair source zone_client destination zone_internet
service-policy type inspect Client-WebServer-Policy
```

Verificación

Paso 1. Iniciar conexión HTTP desde el cliente

Verifique que la comunicación HTTP desde el cliente al servidor WEB sea exitosa.



Conexión HTTP

Paso 2. Confirmar caché IP

Ejecute show platform hardware qfp active feature dns-snoop-agent datapath ip-cache all el comando para confirmar que la memoria caché IP para el FQDN de destino se genera en C8300-2N2S-6T.

<#root>

02A7382#

show platform hardware qfp active feature dns-snoop-agent datapath ip-cache all

```
IP Address Client(s) Expire RegexId Dirty VRF ID Match
-----------------------------------------------------------------------------------------------------------
192.168.20.1 0x1 117 0xdbccd400 0x00 0x0 .*\.test\.com
```

Paso 3. Confirmar registro de ZBFW

Confirme que la dirección IP (192.168.20.1) coincide con el FQDN (.*\.test\.com) y compruebe que ZBFW permite la comunicación HTTP en el paso 1.

*Mar 7 11:08:23.018: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:003 TS:00000551336606461468 %FW-6-SESS_AUDIT_TRAIL_START

*Mar 7 11:08:24.566: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:002 TS:00000551338150591101 %FW-6-SESS_AUDIT_TRAIL: (target:

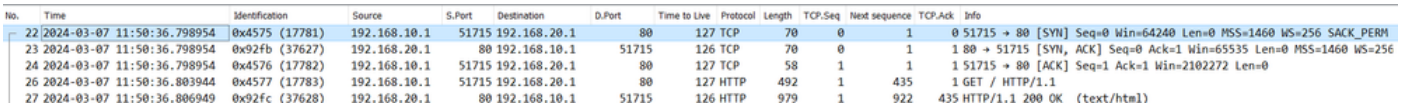
Paso 4. Confirmar captura de paquetes

Confirme que la resolución DNS del FQDN de destino y la conexión HTTP entre el cliente y el servidor WEB se han realizado correctamente.

Captura de paquetes en el interior:

No.	Time	Identification	Source	S.Port	Destination	D.Port	Time to Live	Protocol	Length	TCP.Seq	Next sequence	TCP.Ack	Info
15	2024-03-07 11:50:36.775945	0x0511 (1297)	192.168.10.1	64078	8.8.8.8	53	127	DNS	76				Standard query 0xa505 A abc.test.com
18	2024-03-07 11:50:36.782949	0xe036 (57398)	8.8.8.8	53	192.168.10.1	64078	126	DNS	92				Standard query response 0xa505 A abc.test.com A 192.168.20.1

Paquetes DNS dentro



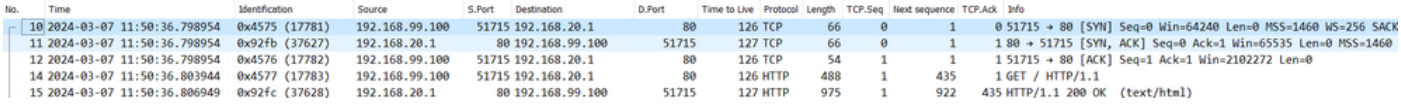
No.	Time	Identification	Source	S.Port	Destination	D.Port	Time to Live	Protocol	Length	TCP.Seq	Next sequence	TCP.Ack	Info
22	2024-03-07 11:50:36.798954	0x4575 (17781)	192.168.10.1	51715	192.168.20.1	80	127	TCP	70	0	1	0	51715 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
23	2024-03-07 11:50:36.798954	0x92fb (37627)	192.168.20.1	80	192.168.10.1	51715	126	TCP	70	0	1	1	80 → 51715 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256
24	2024-03-07 11:50:36.798954	0x4576 (17782)	192.168.10.1	51715	192.168.20.1	80	127	TCP	58	1	1	1	51715 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
26	2024-03-07 11:50:36.803944	0x4577 (17783)	192.168.10.1	51715	192.168.20.1	80	127	HTTP	492	1	435	1	GET / HTTP/1.1
27	2024-03-07 11:50:36.806949	0x92fc (37628)	192.168.20.1	80	192.168.10.1	51715	126	HTTP	979	1	922	435	HTTP/1.1 200 OK (text/html)

Paquetes HTTP en el interior

Captura de paquetes en Onside (192.168.10.1 es NAT a 192.168.19.100) :

No.	Time	Identification	Source	S.Port	Destination	D.Port	Time to Live	Protocol	Length	TCP.Seq	Next sequence	TCP.Ack	Info
3	2024-03-07 11:50:36.775945	0x0511 (1297)	192.168.99.100	64078	8.8.8.8	53	126	DNS	72				Standard query 0xa505 A abc.test.com
6	2024-03-07 11:50:36.782949	0xe036 (57398)	8.8.8.8	53	192.168.99.100	64078	127	DNS	88				Standard query response 0xa505 A abc.test.com A 192.168.20.1

Paquetes DNS en el exterior



No.	Time	Identification	Source	S.Port	Destination	D.Port	Time to Live	Protocol	Length	TCP.Seq	Next sequence	TCP.Ack	Info
10	2024-03-07 11:50:36.798954	0x4575 (17781)	192.168.99.100	51715	192.168.20.1	80	126	TCP	66	0	1	0	51715 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
11	2024-03-07 11:50:36.798954	0x92fb (37627)	192.168.20.1	80	192.168.99.100	51715	127	TCP	66	0	1	1	80 → 51715 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
12	2024-03-07 11:50:36.798954	0x4576 (17782)	192.168.99.100	51715	192.168.20.1	80	126	TCP	54	1	1	1	51715 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
14	2024-03-07 11:50:36.803944	0x4577 (17783)	192.168.99.100	51715	192.168.20.1	80	126	HTTP	488	1	435	1	GET / HTTP/1.1
15	2024-03-07 11:50:36.806949	0x92fc (37628)	192.168.20.1	80	192.168.99.100	51715	127	HTTP	975	1	922	435	HTTP/1.1 200 OK (text/html)

Paquetes HTTP en el exterior

Troubleshoot

Para solucionar problemas de comunicación relacionados con ZBFW mediante la coincidencia de patrones de ACL de FQDN, puede recopilar los registros durante el problema y proporcionárselos al TAC de Cisco. Tenga en cuenta que los registros para la resolución de problemas dependen de la naturaleza del problema.

Ejemplo de registros que se deben recopilar:

!!!! before reproduction
!! Confirm the IP cache
show platform hardware qfp active feature dns-snoop-agent datapath ip-cache all

!! Enable packet-trace
debug platform packet-trace packet 8192 fia-trace
debug platform packet-trace copy packet both
debug platform condition ipv4 access-list Client-WebServer both
debug platform condition feature fw dataplane submode all level verbose

!! Enable debug-level system logs and ZBFW debug logs
debug platform packet-trace drop
debug acl cca event
debug acl cca error
debug ip domain detail
!! Start to debug
debug platform condition start

!! Enable packet capture on the target interface (both sides) and start the capture
monitor capture CAPIN interface Port-channel1.2001 both
monitor capture CAPIN match ipv4 any any
monitor capture CAPIN buffer size 32
monitor capture CAPIN start

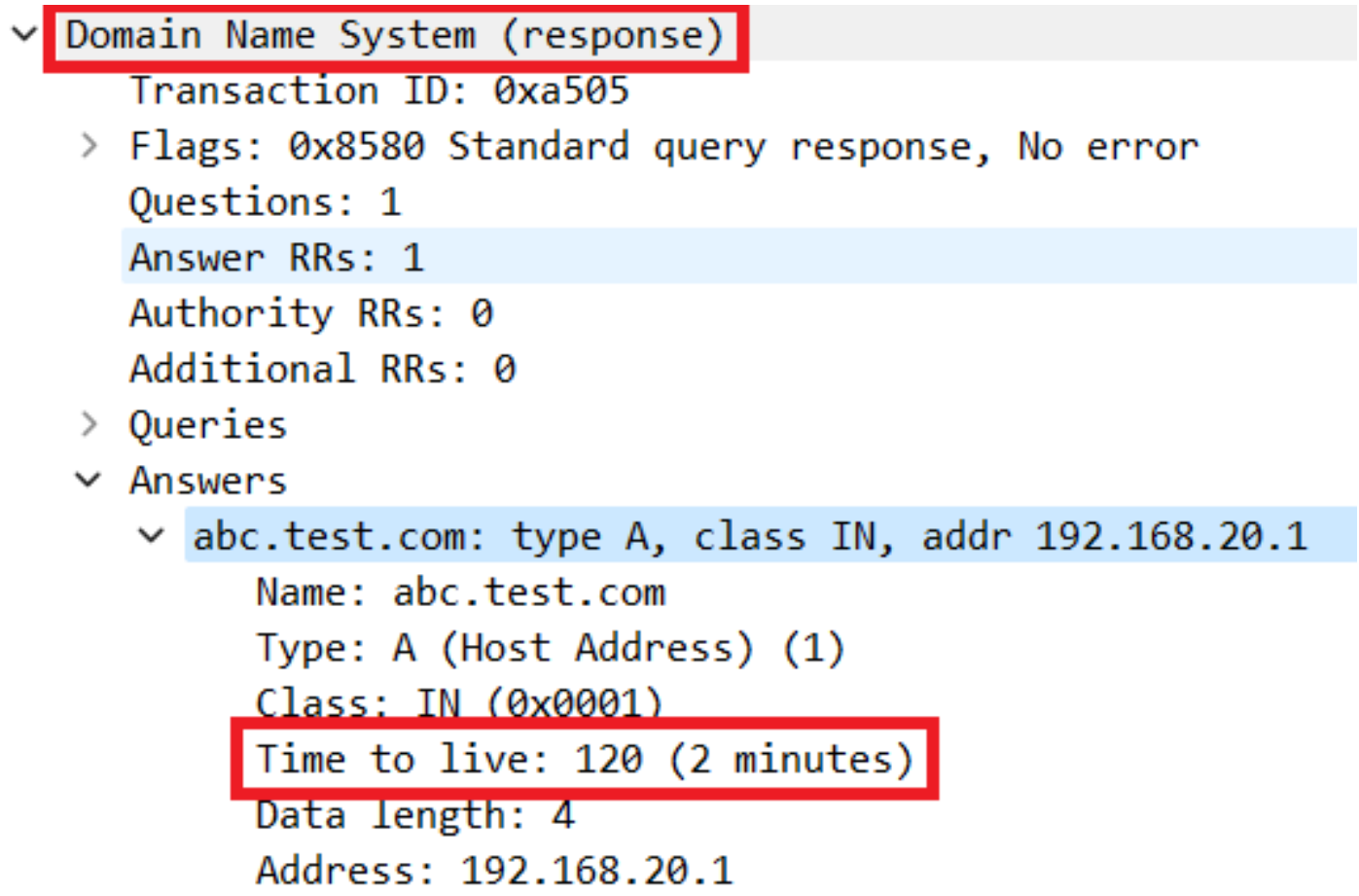
monitor capture CAPOUT interface g0/0/3 both
monitor capture CAPOUT match ipv4 any any
monitor capture CAPOUT buffer size 32
monitor capture CAPOUT start

```
!! (Optional) Clear the DNS cache on the client
ipconfig/flushdns
ipconfig /displaydns

!! Run the show command before reproduction
show platform hardware qfp active feature firewall drop all
show policy-map type inspect zone-pair Client-WebServer-Pair sessions
show platform packet-trace statistics
show platform packet-trace summary
show logging process cpp_cp internal start last boot
show platform hardware qfp active feature dns-snoop-agent client hw-pattern-list
show platform hardware qfp active feature dns-snoop-agent client info
show platform hardware qfp active feature dns-snoop-agent datapath stats
show ip dns-snoop all
show platform hardware qfp active feature dns-snoop-agent datapath ip-cache all
show platform software access-list F0 summary

!!!! Reproduce the issue - start

!! During the reproductionof the issue, run show commands at every 10 seconds
!! Skip show ip dns-snoop all command if it is not supported on the specific router
show ip dns-snoop all
show platform hardware qfp active feature dns-snoop-agent datapath ip-cache all

!!!! After reproduction
!! Stop the debugging logs and packet capture
debug platform condition stop
monitor capture CAPIN stop
monitor capture CAPOUT stop

!! Run the show commands
show platform hardware qfp active feature firewall drop all
show policy-map type inspect zone-pair Client-WebServer-Pair sessions
show platform packet-trace statistics
show platform packet-trace summary
show logging process cpp_cp internal start last boot
show platform hardware qfp active feature dns-snoop-agent client hw-pattern-list
show platform hardware qfp active feature dns-snoop-agent client info
show platform hardware qfp active feature dns-snoop-agent datapath stats
show ip dns-snoop all
show platform hardware qfp active feature dns-snoop-agent datapath ip-cache all
show platform software access-list F0 summary

show platform packet-trace packet all decode
show running-config
```

Preguntas Frecuentes

P: ¿Cómo se determina el valor de tiempo de espera de la memoria caché IP en el router?

R: El valor de tiempo de espera de la caché IP viene determinado por el valor TTL (tiempo de vida) del paquete DNS devuelto por el servidor DNS. En este ejemplo, son 120 segundos. Cuando se agota el tiempo de espera de la caché IP, se elimina automáticamente del router. Este es el detalle de la captura de paquetes.



Detalle de paquetes de resolución DNS

P: ¿Es aceptable que el servidor DNS devuelva un registro CNAME en lugar de un registro A?

R: Sí, no es un problema. La resolución DNS y la comunicación HTTP se llevan a cabo sin problemas cuando el servidor DNS devuelve el registro CNAME. Este es el detalle de la captura de paquetes.

No.	Time	Identification	Source	S.Port	Destination	D.Port	Time to Live	Protocol	Length	TCP.Seq	Next sequence	TCP.Ack	Info
350	2024-03-07 12:09:55.625959	0x0bc5 (3013)	192.168.10.1	63777	8.8.8.8	53	127	DNS	76				Standard query 0x6bd8 A abc.test.com
352	2024-03-07 12:09:55.629957	0xe4fe (58622)	8.8.8.8	53	192.168.10.1	63777	126	DNS	114				Standard query response 0x6bd8 A abc.test.com CNAME def.test.

Paquetes DNS dentro

```
Domain Name System (response)
    Transaction ID: 0x6bd8
  > Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v abc.test.com: type CNAME, class IN, cname def.test.com
        Name: abc.test.com
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 120 (2 minutes)
        Data length: 6
        CNAME: def.test.com
    v def.test.com: type A, class IN, addr 192.168.20.1
        Name: def.test.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 120 (2 minutes)
        Data length: 4
        Address: 192.168.20.1
```

Detalle de paquetes de resolución DNS

No.	Time	Identification	Source	S.Port	Destination	D.Port	Time to Live	Protocol	Length	TCP.S	Next :	TCP.A	Info
356	2024-03-07 12:09:55.644955	0x4589 (17801)	192.168.10.1	51801	192.168.20.1	80	127	TCP	70	0	1	0	51801 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2
357	2024-03-07 12:09:55.644955	0x9349 (37705)	192.168.20.1	80	192.168.10.1	51801	126	TCP	70	0	1	1	80 → 51801 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
358	2024-03-07 12:09:55.644955	0x458a (17802)	192.168.10.1	51801	192.168.20.1	80	127	TCP	58	1	1	1	51801 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
359	2024-03-07 12:09:55.645962	0x458b (17803)	192.168.10.1	51801	192.168.20.1	80	127	HTTP	492	1	435	1	GET / HTTP/1.1
362	2024-03-07 12:09:55.646954	0x934a (37706)	192.168.20.1	80	192.168.10.1	51801	126	HTTP	979	1	922	435	HTTP/1.1 200 OK (text/html)

Paquetes HTTP en el interior

P: ¿Cuál es el comando para transferir capturas de paquetes recolectadas en un router C8300 a un servidor FTP?

R: Utilice monitor capture <capture name> export bootflash:<capture name>.pcap y copy bootflash:<capture name>.pcap ftp://<user>:<password>@<FTP IP Address> comandos para transferir capturas de paquetes a un servidor FTP. Este es un ejemplo para transferir CAPIN a un servidor FTP.

<#root>

monitor capture CAPIN export bootflash:CAPIN.pcap

copy bootflash:CAPIN.pcap ftp://<user>:<password>@<FTP IP Address>

Referencia

Comprender el diseño de firewall de políticas basado en zonas

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).