ZBFW configureren met behulp van FQDN ACL-patroonmatching in C8300 Series

Inhoud

Inleiding

In dit document wordt de procedure beschreven om ZBFW te configureren met FQDN ACL-patronen die in autonome modus op het C8300-platform worden aangepast.

Voorwaarden

Vereisten

Cisco raadt u aan bekend te zijn met dit onderwerp:

- Zone-Based Policy Firewall (ZBFW)
- Virtual Routing and Forwarding (VRF)
- Netwerkadresomzetting (NAT)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C830-2N2S-6T 17.12.02

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Zone-Based Policy Firewall (ZBFW) is een geavanceerde methode voor het configureren van firewalls op Cisco IOS® en Cisco IOS XE-apparaten waarmee beveiligingszones binnen het netwerk kunnen worden gemaakt.

Met ZBFW kunnen beheerders interfaces in zones groeperen en firewallbeleid toepassen op verkeer dat zich tussen deze zones verplaatst.

FQDN ACL's (Fully Qualified Domain Name Access Control Lists), gebruikt met een ZBFW in Cisco-routers, stellen beheerders in staat firewallregels te maken die verkeer aanpassen op basis van domeinnamen in plaats van alleen IP-adressen.

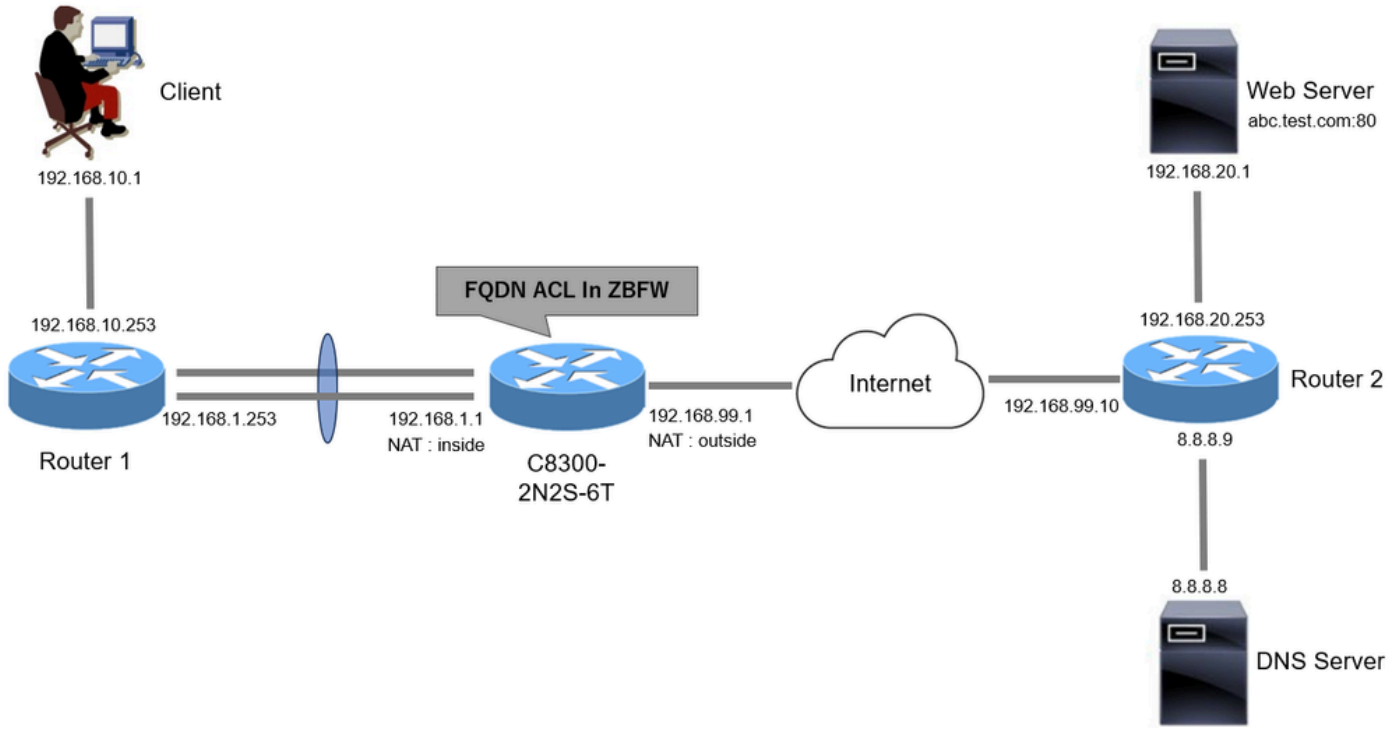
Deze functie is met name nuttig bij het omgaan met diensten die worden gehost op platforms zoals AWS of Azure, waar het IP-adres dat aan een service is gekoppeld vaak kan veranderen.

Het vereenvoudigt het beheer van het toegangscontrolebeleid en verbetert de flexibiliteit van de beveiligingsconfiguraties binnen het netwerk.

Configureren

Netwerkdiagram

Dit document introduceert de configuratie en verificatie voor ZBFW op basis van dit diagram. Dit is een gesimuleerde omgeving met BlackJumboDog als DNS-server.



Netwerkdiagram

Configuraties

Dit is de configuratie om communicatie van de client naar de webserver toe te laten.

Stap 1. (optioneel) VRF configureren

Met de functie VRF (Virtual Routing and Forwarding) kunt u meerdere onafhankelijke routingtabellen binnen één router maken en beheren. In dit voorbeeld maken we een VRF genaamd WebVRF en voeren we routing uit voor gerelateerde communicatie.

```
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
```

Stap 2. Interface configureren

Configureer basisinformatie zoals zone-lid, VRF-, NAT- en IP-adressen voor de interfaces binnen en buiten.

```
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
```

Stap 3. (optioneel) Configureer NAT

Configureer NAT voor interfaces binnen en buiten. In dit voorbeeld wordt het IP-bronadres van de client (192.168.10.1) vertaald naar 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
```

Stap 4. FQDN-ACL configureren

Configureer FQDN ACL om het doelverkeer aan te passen. In dit voorbeeld, gebruik de vervanging '*' in de patroonaanpassing van de FQDN-objectgroep om de bestemming FQDN aan te passen.

```
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
```

Stap 5. ZBFW configureren

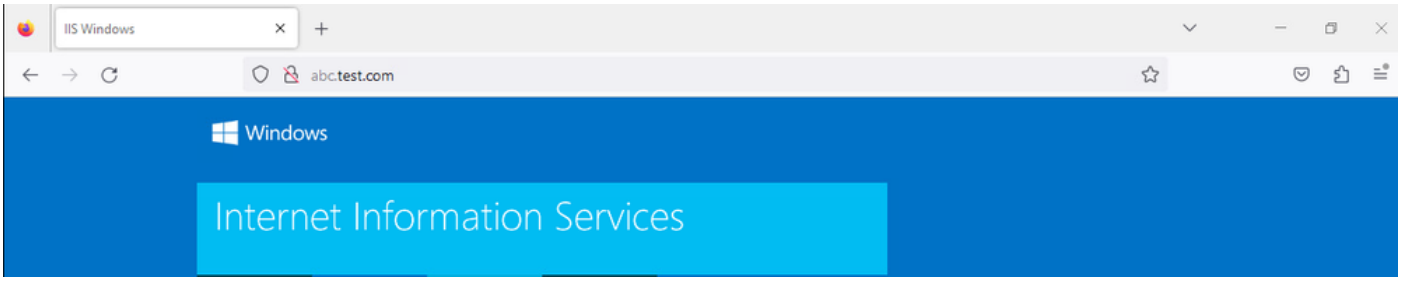
Zone, class-map en policy-map configureren voor ZBFW. In dit voorbeeld worden logbestanden met behulp van parameter-map gegenereerd wanneer het verkeer is toegestaan door ZBFW.

```
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
```

Verifiëren

Stap 1. HTTP-verbinding vanaf client starten

Controleer of HTTP-communicatie van de client naar de WEBserver succesvol is.



HTTP-verbinding

Stap 2. IP-cachegeheugen bevestigen

Voer show platform hardware qfp active feature dns-snoop-agent datapath ip-cache all de opdracht uit om te bevestigen dat het IP-cache voor het doel-FQDN in C8300-2N2S-6T is gegenereerd.

<#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
```

Stap 3. ZBFW-log bevestigen

Bevestig dat het IP-adres (192.168.20.1) overeenkomt met de FQDN (.*\.test\.com) en controleer of de HTTP-communicatie in stap 1 is toegestaan door ZBFW.

*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:

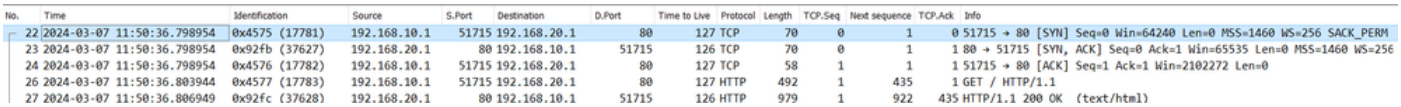
Stap 4. Packet Capture bevestigen

Bevestig dat de DNS-resolutie voor doel-FQDN en de HTTP-verbinding tussen de client en de WEBserver succesvol zijn.

PacketCapture in binnenkant:

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

DNS-pakketten binnen



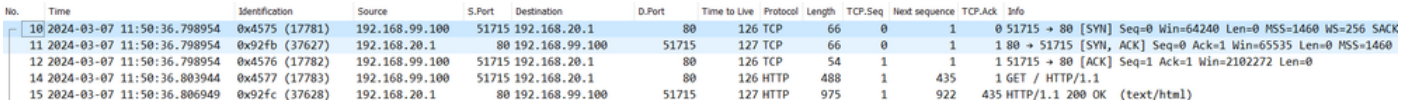
No.	Time	Identification	Source	S.Port	Destination	D.Port	Time to Live	Protocol	Length	TCP.Seq	Next sequence	TCP.Ack	Info
22	2024-03-07 11:50:36.798954	0x4575 (17781)	192.168.10.1	51715	192.168.20.1	80	127	TCP	70	0	1	0	51715 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
23	2024-03-07 11:50:36.798954	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)

HTTP-pakketten binnen

Packet Capture in Onside (192.168.10.1 is NAT naar 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

DNS-pakketten binnen



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)

HTTP-pakketten binnen en buiten

Problemen oplossen

Voor communicatieproblemen met betrekking tot ZBFW met behulp van FQDN ACL-patroonmatching, kunt u de logbestanden tijdens het probleem verzamelen en aan Cisco TAC leveren. Houd er rekening mee dat de logbestanden voor probleemoplossing afhankelijk zijn van de aard van het probleem.

Voorbeeld van te verzamelen stammen:

!!!! 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

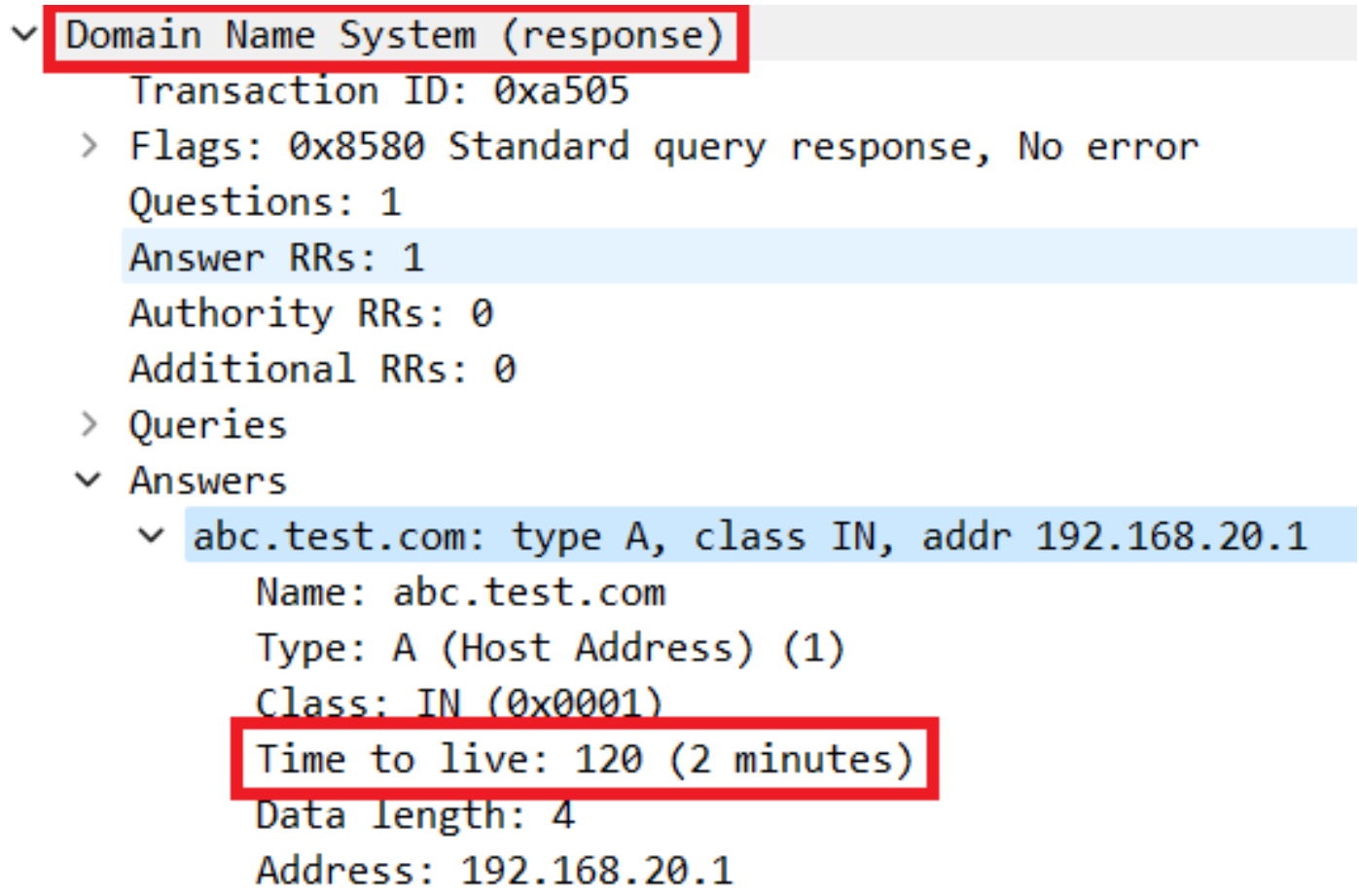
!! Run the show commands
show platform hardware qfp active feature firewall drop all
show policy-map type inspect zone-pair Client-WebServer-Pair sessions
show platform packet-trace statistics
show platform packet-trace summary
show logging process cpp_cp internal start last boot
show platform hardware 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

Veelgestelde vragen

Q: Hoe wordt de onderbrekingswaarde van het IP geheim voorgeheugen bepaald op de router?

A: De tijdelijke waarde van het IP-cache wordt bepaald door de TTL-waarde (Time-To-Live) van het DNS-pakket dat van de DNS-server is geretourneerd. In dit voorbeeld is het 120 seconden. Wanneer het IP-cachegeheugen is uitgevallen, wordt het automatisch van de router verwijderd. Dit is het detail van pakketopname.



Packet Detail van DNS-resolutie

Q: Is het aanvaardbaar wanneer de DNS server CNAME verslag eerder dan A verslag terugkeert?

A: Ja, dat is geen probleem. DNS-resolutie en HTTP-communicatie worden zonder problemen uitgevoerd wanneer CNAME-record door DNS-server wordt teruggestuurd. Dit is het detail van pakketopname.

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.

DNS-pakketten binnen

```
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
```

Packet Detail van DNS-resolutie

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)

HTTP-pakketten binnen

V: Wat is de opdracht om pakketopnamen die op een C8300-router zijn verzameld over te brengen naar een FTP-server?

A: Gebruik monitor capture <capture name> export bootflash:<capture name>.pcap en copy bootflash:<capture name>.pcap ftp://<user>:<password>@<FTP IP Address> commando's om pakketopnamen naar een FTP-server over te brengen. Dit is een voorbeeld om CAPIN over te brengen naar een FTP server.

<#root>

monitor capture CAPIN export bootflash:CAPIN.pcap

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

Referentie

Het Zone-Based Policy Firewall Design begrijpen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.