Konfigurieren der ZBFW mithilfe der FQDN-ACL-Musterzuordnung in der C8300-Serie

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Konfiguration von ZBFW mit FQDN-ACL-Mustervergleich im autonomen Modus auf der C8300-Plattform beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in diesem Thema verfügen:

- ZBFW (Zone-Based Policy Firewall)
- Virtual Routing and Forwarding (VRF)
- Network Address Translation (NAT)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C830-2N2S-6T 17.12.02

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die zonenbasierte Richtlinien-Firewall (ZBFW) ist eine erweiterte Methode zur Firewall-Konfiguration auf Cisco IOS®- und Cisco IOS XE-Geräten, mit der Sicherheitszonen innerhalb des Netzwerks erstellt werden können.

ZBFW ermöglicht Administratoren, Schnittstellen in Zonen zu gruppieren und Firewall-Richtlinien auf den Datenverkehr zwischen diesen Zonen anzuwenden.

Mit FQDN-ACLs (Fully Qualified Domain Name Access Control Lists, vollständig qualifizierte Domänenamen-Zugriffskontrolllisten), die mit einer ZBFW in Cisco Routern verwendet werden, können Administratoren Firewall-Regeln erstellen, die den Datenverkehr anhand von Domänennamen statt nur anhand von IP-Adressen zuordnen.

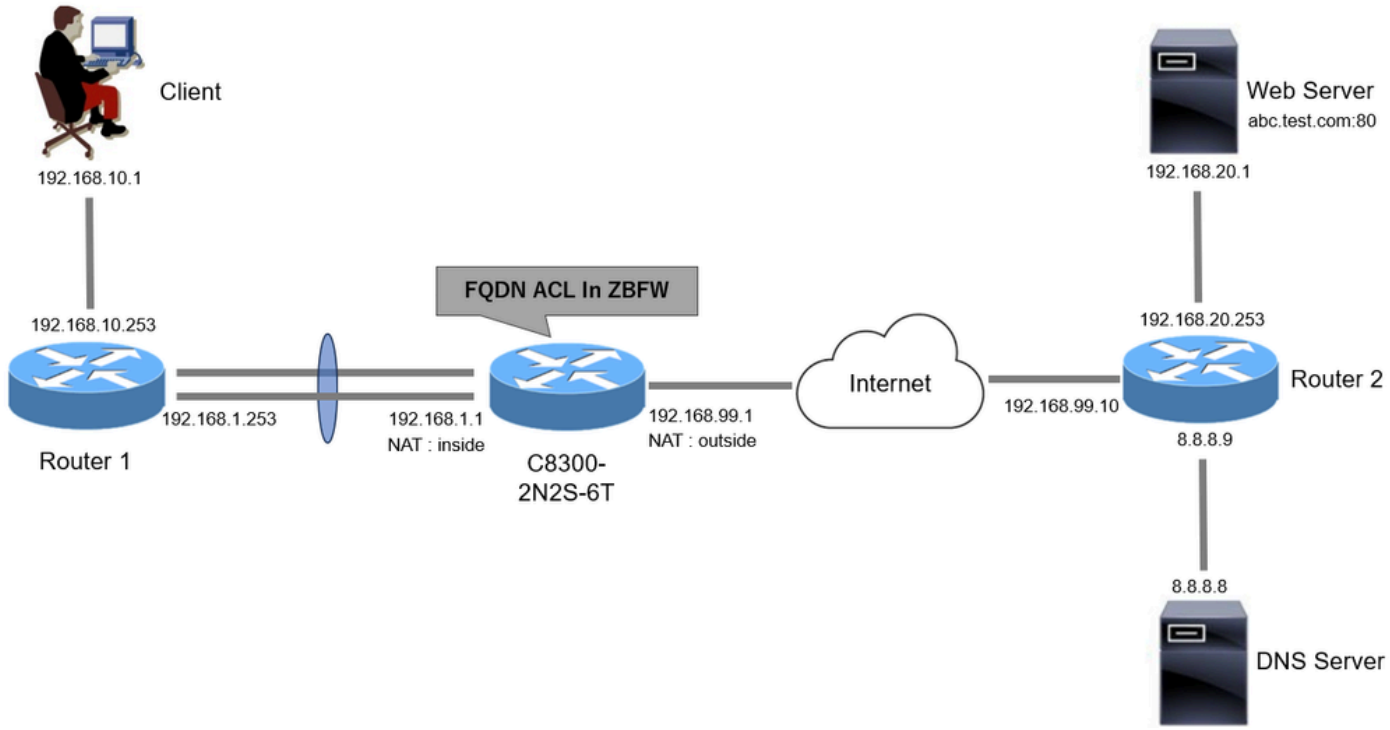
Diese Funktion ist besonders nützlich, wenn Dienste auf Plattformen wie AWS oder Azure gehostet werden, bei denen sich die einem Dienst zugeordnete IP-Adresse häufig ändern kann.

Sie vereinfacht die Verwaltung von Zugriffskontrollrichtlinien und verbessert die Flexibilität von Sicherheitskonfigurationen im Netzwerk.

Konfigurieren

Netzwerkdiagramm

In diesem Dokument wird die Konfiguration und Verifizierung für ZBFW anhand dieses Diagramms vorgestellt. Dies ist eine simulierte Umgebung, die BlackJumboDog als DNS-Server verwendet.



Netzwerkdiagramm

Konfigurationen

Dies ist die Konfiguration, die die Kommunikation vom Client zum Webserver zulässt.

Schritt 1: (Optional) Konfigurieren von VRF

Mit der VRF-Funktion (Virtual Routing and Forwarding) können Sie mehrere unabhängige Routing-Tabellen innerhalb eines Routers erstellen und verwalten. In diesem Beispiel erstellen wir eine VRF mit der Bezeichnung "WebVRF" und führen Routing für die zugehörige Kommunikation durch.

```
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
```

Schritt 2: Konfigurieren der Schnittstelle

Konfigurieren Sie grundlegende Informationen wie Zonenmember, VRF, NAT und IP-Adressen für die internen und externen Schnittstellen.

```
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
```

Schritt 3: (Optional) Konfigurieren von NAT

Konfigurieren Sie NAT für interne und externe Schnittstellen. In diesem Beispiel wird die IP-Quelladresse des Clients (192.168.10.1) in 192.168.99.100 umgewandelt.

```
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
```

Schritt 4: Konfigurieren der FQDN-ACL

Konfigurieren Sie die FQDN-ACL so, dass sie dem Zieldatenverkehr entspricht. Verwenden Sie in diesem Beispiel den Platzhalter '*' in der Musterübereinstimmung der FQDN-Objektgruppe, um mit dem Ziel-FQDN übereinzustimmen.

```
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
```

Schritt 5: Konfigurieren von ZBFW

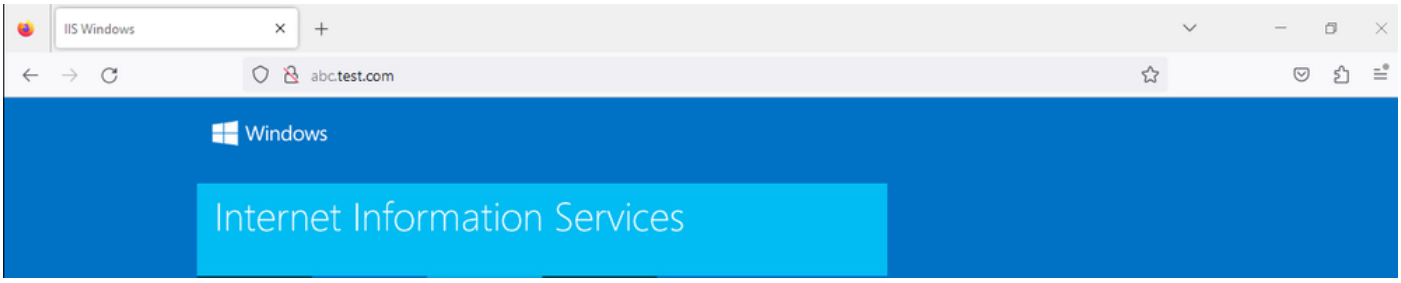
Konfigurieren von Zone, Klassenzuordnung und Richtlinienzuweisung für ZBFW In diesem Beispiel werden mithilfe der Parameterzuordnung Protokolle generiert, wenn der Datenverkehr von der ZBFW zugelassen wird.

```
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
```

Überprüfung

Schritt 1: HTTP-Verbindung vom Client initiieren

Überprüfen Sie, ob die HTTP-Kommunikation vom Client zum WEB-Server erfolgreich ist.



HTTP-Verbindung

Schritt 2: IP-Cache bestätigen

Führen Sie einen Befehl ausshow platform hardware qfp active feature dns-snoop-agent datapath ip-cache all, um zu bestätigen, dass der IP-Cache für den Ziel-FQDN in C8300-2N2S-6T generiert wird.

<#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
```

Schritt 3: ZBFW-Protokoll bestätigen

Bestätigen Sie, dass die IP-Adresse (192.168.20.1) mit dem FQDN (.*\.test\.com) übereinstimmt, und stellen Sie sicher, dass die HTTP-Kommunikation in Schritt 1 von der ZBFW zugelassen wird.

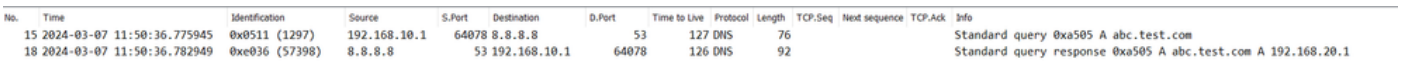
*Mar 7 11:08:23.018: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:003 TS:00000551336606461468 %FW-6-SESS_AUDIT_TRAIL_START

*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:

Schritt 4: Paketerfassung bestätigen

Bestätigen Sie, dass die DNS-Auflösung für den Ziel-FQDN und die HTTP-Verbindung zwischen dem Client und dem WEB-Server erfolgreich sind.

Paketerfassung im Inneren:



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-Pakete intern

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-Pakete intern

Paketerfassung in Onside (192.168.10.1 ist NAT bis 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-Pakete extern

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-Pakete extern

Fehlerbehebung

Bei der Behebung von Kommunikationsproblemen im Zusammenhang mit ZBFW mithilfe des FQDN-ACL-Pattern-Matching können Sie die Protokolle während des Problems erfassen und dem Cisco TAC zur Verfügung stellen. Beachten Sie, dass die Protokolle zur Fehlerbehebung von der Art des Problems abhängen.

Beispiel für zu sammelnde Protokolle:

!!!! 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

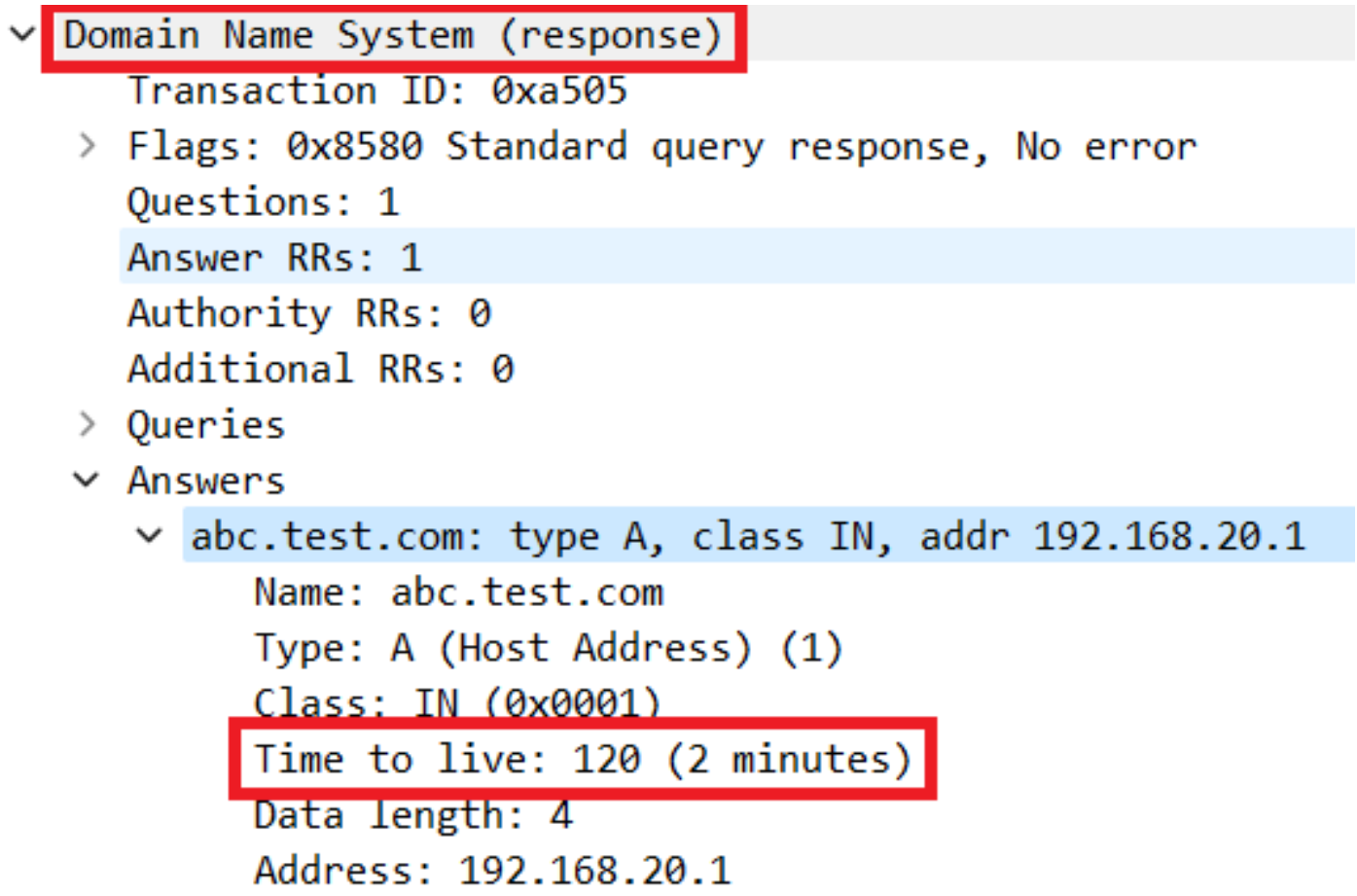
```
monitor capture CAPOUT buffer size 32
monitor capture CAPOUT start

!! (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
```

Häufig gestellte Fragen

F: Wie wird der Timeout-Wert des IP-Caches auf dem Router bestimmt?

A: Der Timeoutwert des IP-Cache wird durch den TTL-Wert (Time-To-Live) des vom DNS-Server zurückgegebenen DNS-Pakets bestimmt. In

diesem Beispiel sind es 120 Sekunden. Wenn die Zeitüberschreitung im IP-Cache auftritt, wird dieser automatisch vom Router entfernt. Dies sind die Details der Paketerfassung.



Paketdetails der DNS-Auflösung

F: Ist es akzeptabel, wenn der DNS-Server den CNAME-Eintrag anstelle des A-Eintrags zurückgibt?

A: Ja, das ist kein Problem. Die DNS-Auflösung und die HTTP-Kommunikation erfolgen ohne Probleme, wenn der CNAME-Eintrag vom DNS-Server zurückgegeben wird. Dies sind die Details der Paketerfassung.

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-Pakete intern

```
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
```

Paketdetails der DNS-Auflösung

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-Pakete intern

F: Welcher Befehl überträgt die auf einem C8300-Router gesammelten Paketerfassungen an einen FTP-Server?

A: Verwenden Sie monitor capture <capture name> export bootflash:<capture name>.pcap und copy bootflash:<capture name>.pcap ftp://<user>:<password>@<FTP IP Address> Befehle, um Paketerfassungen an einen FTP-Server zu übertragen. Dies ist ein Beispiel für die Übertragung von CAPIN auf einen FTP-Server.

<#root>

monitor capture CAPIN export bootflash:CAPIN.pcap

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

Referenz

Verständnis des Firewall-Designs mit zonenbasierten Richtlinien

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.