Configurer ZBFW en utilisant la correspondance de modèles ACL FQDN dans la gamme C8300

Table des matières

Introduction

Ce document décrit la procédure pour configurer ZBFW avec la correspondance de modèle ACL FQDN en mode autonome sur la plate-forme C8300.

Conditions préalables

Exigences

Cisco recommande que vous ayez une connaissance de ce sujet :

- ZBFW (Zone-Based Policy Firewall)
- Routage et transfert virtuels (VRF)
- Traduction d'adresses réseau (NAT)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- C8300-2N2S-6T 17.12.02

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

ZBFW (Zone-Based Policy Firewall) est une méthode avancée de configuration de pare-feu sur les périphériques Cisco IOS® et Cisco IOS XE qui permet de créer des zones de sécurité sur le réseau.

ZBFW permet aux administrateurs de regrouper les interfaces en zones et d'appliquer des politiques de pare-feu au trafic circulant entre ces zones.

Les listes de contrôle d’accès FQDN (Fully Qualified Domain Name Access Control Lists), utilisées avec un ZBFW dans les routeurs Cisco, permettent aux administrateurs de créer des règles de pare-feu qui correspondent au trafic en fonction des noms de domaine plutôt que des seules adresses IP.

Cette fonctionnalité est particulièrement utile lorsque vous traitez des services hébergés sur des plates-formes telles qu'AWS ou Azure, où l'adresse IP associée à un service peut changer fréquemment.

Il simplifie la gestion des politiques de contrôle d'accès et améliore la flexibilité des configurations de sécurité au sein du réseau.

Configurer

Diagramme du réseau

Ce document présente la configuration et la vérification de ZBFW sur la base de ce schéma. Il s'agit d'un environnement simulé utilisant BlackJumboDog comme serveur DNS.

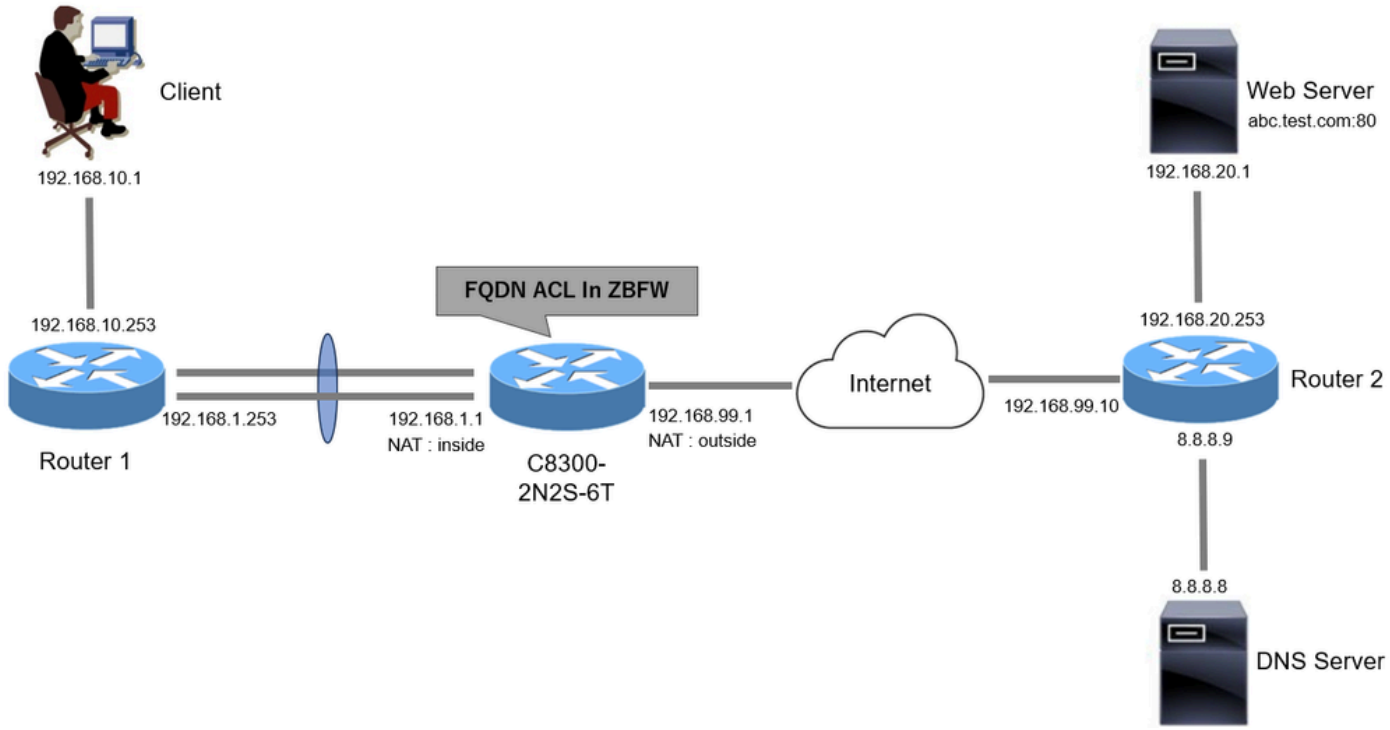


Diagramme du réseau

Configurations

Il s'agit de la configuration permettant la communication du client au serveur Web.

Étape 1. (Facultatif) Configuration du VRF

La fonctionnalité VRF (Virtual Routing and Forwarding) vous permet de créer et de gérer plusieurs tables de routage indépendantes au sein d'un seul routeur. Dans cet exemple, nous créons un VRF appelé WebVRF et effectuons le routage pour les communications associées.

```
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
```

Étape 2. Configurer l’interface

Configurez les informations de base telles que les adresses de membre de zone, VRF, NAT et IP pour les interfaces interne et externe.

```
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
```

Étape 3 : configuration de la fonction NAT (facultatif)

Configurez NAT pour les interfaces internes et externes. Dans cet exemple, l'adresse IP source du client (192.168.10.1) est traduite en 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
```

Étape 4. Configurer la liste ACL FQDN

Configurez la liste de contrôle d'accès FQDN pour correspondre au trafic cible. Dans cet exemple, utilisez le caractère générique « * » dans la correspondance de modèle du groupe d'objets FQDN pour correspondre au nom de domaine complet de destination.

```
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
```

Étape 5. Configurer ZBFW

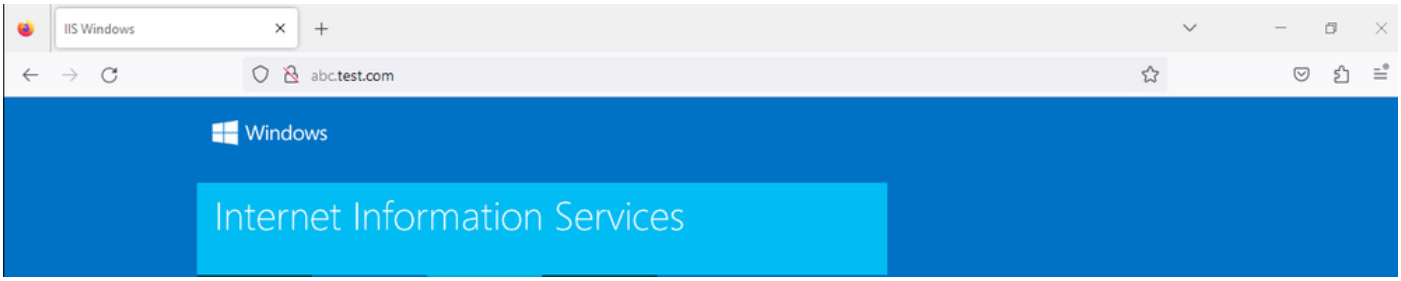
Configurez zone, class-map, policy-map pour ZBFW. Dans cet exemple, à l'aide de parameter-map, des journaux sont générés lorsque le trafic est autorisé par ZBFW.

```
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
```

Vérifier

Étape 1. Établir une connexion HTTP à partir du client

Vérifiez que la communication HTTP entre le client et le serveur WEB a réussi.



Connexion HTTP

Étape 2. Confirmer le cache IP

Exécutez show platform hardware qfp active feature dns-snoop-agent datapath ip-cache all la commande pour confirmer que le cache IP du nom de domaine complet cible est généré dans 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
```

Étape 3. Confirmer le journal ZBFW

Vérifiez que l'adresse IP (192.168.20.1) correspond au nom de domaine complet (.*\.test\.com) et que la communication HTTP de l'étape 1 est autorisée par 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:

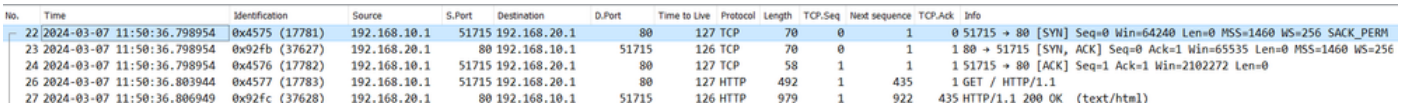
Étape 4. Confirmer la capture de paquets

Vérifiez que la résolution DNS pour le nom de domaine complet cible et la connexion HTTP entre le client et le serveur Web ont réussi.

Capture de paquets à l'intérieur :

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

Paquets DNS internes



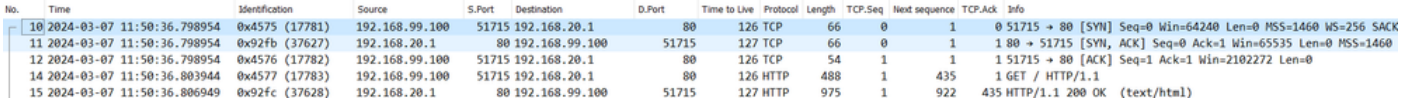
No.	Time	Identification	Source	S.Port	Destination	D.Port	Time to Live	Protocol	Length	TCP.Seq	Next sequence	TCP.Ack	Info
22	2024-03-07 11:50:36.798954	0x4575 (17781)	192.168.10.1	51715	192.168.20.1	80	127	TCP	70	0	1	0	51715 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
23	2024-03-07 11:50:36.798954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

Paquets HTTP internes

Capture de paquets en interne (192.168.10.1 correspond à la NAT vers 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

Paquets DNS externes



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)

Paquets HTTP dans l'extérieur

Dépannage

Pour le dépannage des problèmes de communication liés à ZBFW à l'aide de la correspondance des modèles de liste de contrôle d'accès FQDN, vous pouvez collecter les journaux pendant le problème et les fournir au TAC Cisco. Notez que les journaux de dépannage dépendent de la nature du problème.

Exemple de journaux à collecter :

!!!! 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

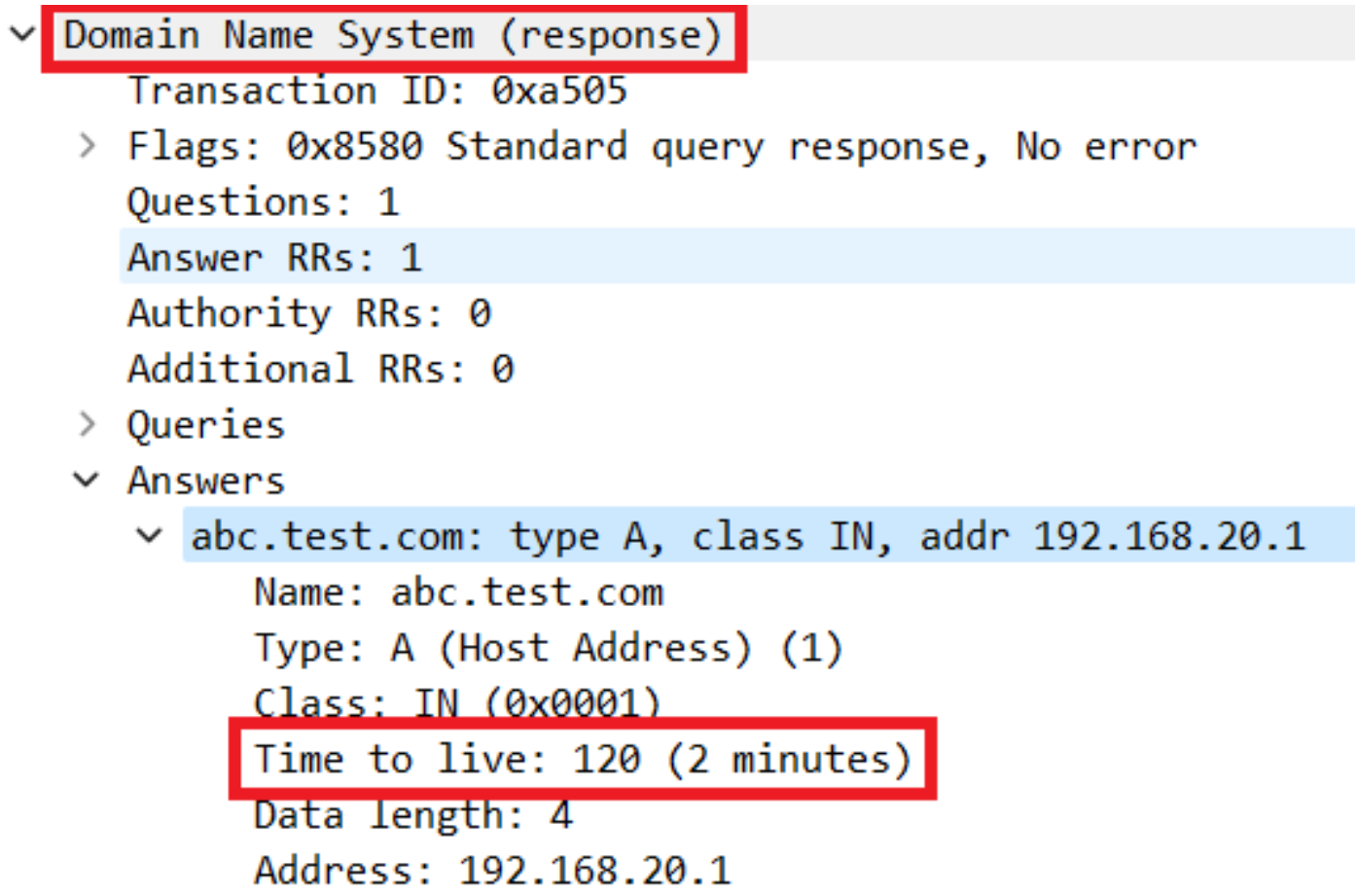
!! Run the show commands
show platform hardware qfp active feature firewall drop all
show policy-map type inspect zone-pair Client-WebServer-Pair sessions
show platform packet-trace statistics
show platform packet-trace summary
show logging process cpp_cp internal start last boot
show platform hardware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

Forum aux questions

Q : Comment la valeur de délai d'attente du cache IP est-elle déterminée sur le routeur ?

R : La valeur de délai d'attente du cache IP est déterminée par la valeur TTL (Time-To-Live) du paquet DNS renvoyé par le serveur DNS. Dans cet exemple, il est de 120 secondes. Lorsque le cache IP expire, il est automatiquement supprimé du routeur. Il s’agit du détail de la capture de paquets.



Détail des paquets de la résolution DNS

Q : Est-il acceptable lorsque le serveur DNS renvoie un enregistrement CNAME plutôt qu'un enregistrement A ?

R : Oui, ce n'est pas un problème. La résolution DNS et la communication HTTP se poursuivent sans problème lorsque l'enregistrement CNAME est renvoyé par le serveur DNS. Il s’agit du détail de la capture de paquets.

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.

Paquets DNS internes

```
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
```

Détail des paquets de la résolution 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)

Paquets HTTP internes

Q : Quelle est la commande permettant de transférer les captures de paquets collectées sur un routeur C8300 vers un serveur FTP ?

R : Utilisez lesmonitor capture <capture name> export bootflash:<capture name>.pcap copy bootflash:<capture name>.pcap ftp://<user>:<password>@<FTP IP Address> commandes et pour transférer des captures de paquets vers un serveur FTP. Il s'agit d'un exemple de transfert de CAPIN vers un serveur FTP.

<#root>

monitor capture CAPIN export bootflash:CAPIN.pcap

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

Référence

Comprendre la conception du pare-feu à politique basée sur les zones

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.