Dépannage des connexions via PIX et ASA

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Produits connexes
Conventions
Informations générales
Problème
Solution
Étape 1 - Découvrir l'adresse IP de l'utilisateur
Étape 2 - Localiser la cause du problème
Étape 3 - Vérifier et surveiller le trafic d'une application
Opérations suivantes
Problème : **Message d'erreur Terminating TCP-Proxy connection**
Solution
Problème : "%ASA-6-110003 : Le routage n'a pas localisé le prochain-saut pour le protocole message d'erreur de src d'interface »
Solution
Problème : Connexion bloquée par ASA avec le « %ASA-5-305013 : Les règles NAT asymétriques se sont assorties pour message d'erreur en avant et de flux inverses le »
Solution
Problème : Recevez l'erreur - %ASA-5-321001 : La limite de « conns » de ressource de 10000 a atteint pour le système
Solution
Problème : Recevez l'erreur %PIX-1-106021 : Refusez le contrôle de chemin inverse TCP/UDP du src_addr au dest_addr sur l'int_name d'interface
Solution
Problème : Interruption de la connexion Internet due à la détection de menace
Solution
Informations connexes

Introduction

Ce document fournit des idées et des suggestions de dépannage pour quand vous utilisez le dispositif de sécurité adaptatif dédié (ASA) de la gamme Cisco ASA 5500 et le dispositif de sécurité de la gamme Cisco PIX 500. Le plus souvent, quand des applications ou sources réseau sont endommagées ou ne sont pas disponibles, les pare-feu (PIX ou ASA) ont tendance à être une cible primaire et à être accusés d'être la cause des pannes. Avec certains tests sur ASA ou PIX, un administrateur peut déterminer si ASA/PIX pose le problème.

Reportez-vous à la section PIX/ASA : Établir et dépanner la connectivité via le dispositif de sécurité Cisco afin d'en savoir plus sur le dépannage lié à l'interface sur les dispositifs de sécurité Cisco.

Remarque: Ce document se concentre sur ASA et PIX. Une fois que le dépannage est terminé sur ASA ou PIX, il est probable qu'un dépannage supplémentaire sera nécessaire avec d'autres périphériques (routeurs, commutateurs, serveurs, etc.).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur le Cisco ASA 5510 avec du SYSTÈME D'EXPLOITATION 7.2.1 et 8.3.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- SYSTÈME D'EXPLOITATION ASA et PIX 7.0, 7.1, 8.3, et plus tard
- Module de services pare-feu (FWSM) 2.2, 2.3 et 3.1

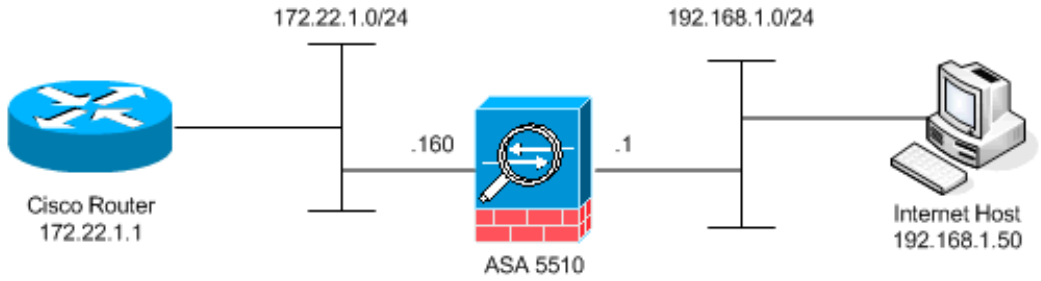
Remarque: Des commandes spécifiques et la syntaxe peuvent varier entre les versions de logiciel.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

L'exemple suppose qu'ASA ou PIX est en production. La configuration ASA/PIX peut être relativement simple (seulement 50 lignes de configuration) ou complexe (des centaines à des milliers de lignes de configuration). Les utilisateurs (clients) ou les serveurs peuvent être sur un réseau sécurisé (interne) ou sur un réseau non sécurisé (DMZ ou externe).



ASA démarre avec cette configuration. La configuration est destinée à donner au laboratoire un point de référence.

Configuration initiale d'ASA

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 10.1.1.1 255.255.255.0
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list outside_acl extended permit tcp any host
172.22.1.254 eq www
access-list inside_acl extended permit icmp 192.168.1.0
255.255.255.0 any
access-list inside_acl extended permit tcp 192.168.1.0
255.255.255.0 any eq www
access-list inside_acl extended permit tcp 192.168.1.0
255.255.255.0 any eq telnet
pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no asdm history enable
arp timeout 14400
```

```
global (outside) 1 172.22.1.253
nat (inside) 1 192.168.1.0 255.255.255.0


!--- The above NAT statements are replaced by the
following statements !--- for ASA 8.3 and later. object
network obj-192.168.1.0 subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic 172.22.1.253 static
(inside,outside) 192.168.1.100 172.22.1.254 netmask
255.255.255.255 !--- The above Static NAT statement is
replaced by the following statements !--- for ASA 8.3
and later. object network obj-172.22.1.254 host
172.22.1.254 nat (inside,outside) static 192.168.1.100
access-group outside_acl in interface outside access-
group inside_acl in interface inside 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 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
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

Problème

Un utilisateur contacte le service informatique et signale que l'application X ne fonctionne plus. L'incident est remonté à l'administrateur ASA/PIX. L'administrateur a peu de connaissances de cette application particulière. À l'aide d'ASA/de PIX, l'administrateur découvre quels ports et protocoles l'application X utilise, ainsi que ce qui pourrait être la cause du problème.

Solution

L'administrateur ASA/PIX doit recueillir autant d'informations que possible de l'utilisateur. Les informations utiles sont :

- Adresse IP source — C'est typiquement la station de travail ou l'ordinateur de l'utilisateur.
- Adresse IP de destination — L'adresse IP du serveur que l'utilisateur ou l'application essaye de connecter.
- Les ports et protocoles que l'application utilise.

Souvent, l'administrateur est chanceux s'il est capable d'obtenir une réponse à l'une de ces questions. Pour cet exemple, l'administrateur ne peut recueillir aucune information. Un examen des messages syslog ASA/PIX est idéal, mais il est difficile de localiser le problème si l'administrateur ne sait pas quoi rechercher.

Étape 1 - Découvrir l'adresse IP de l'utilisateur

Il y a beaucoup de façons de découvrir l'adresse IP de l'utilisateur. Ce document est relatif à ASA et à PIX. Cet exemple utilise donc ASA et PIX pour découvrir l'adresse IP.

L'utilisateur tente de communiquer avec ASA/PIX. Cette communication peut être ICMP, Telnet, SSH ou HTTP. Le protocole choisi devrait avoir limité l'activité sur ASA/PIX. Dans cet exemple spécifique, l'utilisateur effectue un ping sur l'interface interne d'ASA.

L'administrateur a besoin de configurer une ou plusieurs des options suivantes, puis que l'utilisateur effectue un ping sur l'interface interne d'ASA.

- **Syslog**Assurez-vous que la journalisation est activée. Le niveau de journalisation doit être défini sur **debug**. La journalisation peut être envoyée à différents emplacements. Cet exemple utilise la mémoire tampon du journal ASA. Vous pouvez avoir besoin d'un serveur de journalisation externe dans les environnements de production.

  ```
  ciscoasa(config)#logging enable
  ciscoasa(config)#logging buffered debugging
  ```

  L'utilisateur effectue un ping sur l'interface interne d'ASA (ping 192.168.1.1). La sortie suivante s'affiche.

  ```
  ciscoasa#show logging
  !--- Output is suppressed. %ASA-6-302020: Built ICMP connection for faddr 192.168.1.50/512
  gaddr 192.168.1.1/0 laddr 192.168.1.1/0
  %ASA-6-302021: Teardown ICMP connection for faddr 192.168.1.50/512
  gaddr 192.168.1.1/0 laddr 192.168.1.1/0
  !--- The user IP address is 192.168.1.50.
  ```

- **Fonctionnalité Capture d'ASA**L'administrateur a besoin de créer une liste d'accès qui définit quel trafic ASA doit capturer. Une fois la liste d'accès créée, la commande **capture** incorpore la liste d'accès et l'applique à l'interface.

  ```
  ciscoasa(config)#access-list inside_test permit icmp any host 192.168.1.1
  ciscoasa(config)#capture inside_interface access-list inside_test interface inside
  ```

  L'utilisateur effectue un ping sur l'interface interne d'ASA (ping 192.168.1.1). La sortie suivante s'affiche.

  ```
  ciscoasa#show capture inside_interface
     1: 13:04:06.284897 192.168.1.50 > 192.168.1.1: icmp: echo request
   !--- The user IP address is 192.168.1.50.
  ```

  Remarque: Afin de télécharger le fichier de capture sur le système comme éthéré, vous pouvez le faire comme le montre la sortie suivante.

  ```
  !--- Open an Internet Explorer and browse with this https link format:
  https://[<pix_ip>/<asa_ip>]/capture/<capture name>/pcap
  ```

  Reportez-vous à la section ASA/PIX : Exemple de configuration pour la capture de paquets à l'aide de CLI et ASDM afin d'en savoir plus sur la capture de paquets dans ASA.

- **Debug**La commande **debug icmp trace** est utilisée pour capturer le trafic ICMP de l'utilisateur.

  ```
  ciscoasa#debug icmp trace
  ```

  L'utilisateur effectue un ping sur l'interface interne d'ASA (ping 192.168.1.1). Cette sortie est affichée sur la console.

  ```
  ciscoasa#
  !--- Output is suppressed. ICMP echo request from 192.168.1.50 to 192.168.1.1 ID=512
  ```

```
seq=5120 len=32
ICMP echo reply from 192.168.1.1 to 192.168.1.50 ID=512 seq=5120 len=32
!--- The user IP address is 192.168.1.50.
```

Afin de désactiver **debug icmp trace**, utilisez l'une des commandes suivantes :**no debug icmp traceundebug icmp traceundebug all**, **Undebug all** ou **un all**

Chacune de ces trois options aide l'administrateur à déterminer l'adresse IP source. En cet exemple, l'adresse IP source de l'utilisateur est 192.168.1.50. L'administrateur est prêt à en apprendre plus sur l'application X et à déterminer la cause du problème.

Étape 2 - Localiser la cause du problème

Concernant les informations mentionnées dans la section Étape 1 de ce document, l'administrateur connaît maintenant la source d'une session de l'application x. L'administrateur est prêt à en apprendre plus sur l'application X et à commencer à localiser le problème.

L'administrateur ASA/PIX doit préparer ASA pour au moins l'une des suggestions énumérées. Une fois que l'administrateur est prêt, l'utilisateur lance l'application X et limite toute autre activité car une activité utilisateur supplémentaire pourrait entraîner la confusion ou tromper l'administrateur ASA/PIX.

- **Surveiller les messages syslog.**Recherchez l'adresse IP source de l'utilisateur que vous avez localisée à l'étape 1. L'utilisateur lance l'application X. L'administrateur ASA émet la commande **show logging** et affiche la sortie.

```
ciscoasa#show logging
!--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-6-
305011: Built dynamic TCP translation from inside:192.168.1.50/1107 to
outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP connection 90 for
outside:172.22.1.1/80
(172.22.1.1/80) to inside:192.168.1.50/1107 (172.22.1.254/1025)
```

  Les journaux indiquent que l'adresse IP de destination est 172.22.1.1, que le protocole est TCP, que le port de destination est HTTP/80 et que le trafic est envoyé à l'interface externe.
- **Modifier les filtres de capture.**La commande **access-list inside_test** a été utilisée précédemment et est utilisée ici.

```
ciscoasa(config)#access-list inside_test permit ip host 192.168.1.50 any
!--- This ACL line captures all traffic from 192.168.1.50 !--- that goes to or through the
ASA. ciscoasa(config)#access-list inside_test permit ip any host 192.168.1.50 any
!--- This ACL line captures all traffic that leaves !--- the ASA and goes to 192.168.1.50.
ciscoasa(config)#no access-list inside_test permit icmp any host 192.168.1.1
ciscoasa(config)#clear capture inside_interface
!--- Clears the previously logged data. !--- The no capture inside_interface removes/deletes
the capture.
```

  L'utilisateur lance l'application X. L'administrateur ASA émet alors la commande **show capture inside_interface** et affiche la sortie.

```
ciscoasa(config)#show capture inside_interface
1: 15:59:42.749152 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
2: 15:59:45.659145 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
3: 15:59:51.668742 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
```

  Le trafic capturé fournit à l'administrateur plusieurs informations précieuses :Adresse de destination — 172.22.1.1Numéro de port — 80/httpProtocol tcp (notez le « S » ou l'indicateur de syn)En outre, l'administrateur sait également que le trafic de données pour l'application X

arrive à ASA.Si la sortie avait été la sortie de commande **show capture inside_interface** suivante, le trafic de l'application n'a jamais atteint ASA ou le filtre de capture n'était pas défini pour capturer le trafic :

```
ciscoasa#show capture inside_interface
0 packet captured
0 packet shown
```

Dans ce cas, l'administrateur doit envisager d'examiner l'ordinateur de l'utilisateur ainsi que tout routeur ou autres périphériques réseau sur le chemin entre l'ordinateur de l'utilisateur et ASA.**Remarque:** Quand le trafic arrive à une interface, la commande **capture** enregistre les données avant que des stratégies de sécurité ASA analysent le trafic. Par exemple, une liste d'accès refuse tout le trafic entrant sur une interface. La commande **capture** enregistre néanmoins le trafic. La stratégie de sécurité ASA analyse alors le trafic.

- **Debug**L'administrateur n'est pas familiarisé avec l'application X ; il ne sait donc pas lequel des services de débogage activer pour l'examen de l'application X. Le débogage n'est peut-être pas la meilleure option de dépannage à ce stade.

Avec les informations collectées à l'étape 2, l'administrateur ASA gagne plusieurs bribes d'informations précieuses. L'administrateur sait que le trafic arrive à l'interface interne d'ASA, il connaît l'adresse IP source et l'adresse IP de destination, et il sait quel service l'application X utilise (TCP/80). À partir des messages syslog, l'administrateur sait également que la communication a été initialement permise.

Étape 3 - Vérifier et surveiller le trafic d'une application

L'administrateur ASA veut vérifier que le trafic de l'application X a quitté ASA et également surveiller tout trafic de retour à partir du serveur de l'application X.

- **Surveiller les messages syslog.**Filtrez les messages syslog pour l'adresse IP source (192.168.1.50) ou l'adresse IP de destination (172.22.1.1). À partir de la ligne de commande, le filtrage des messages syslog ressemble à **show logging | include 192.168.1.50** ou **show logging | include 172.22.1.1**. Dans cet exemple, la commande **show logging** est utilisé sans filtres. La sortie est supprimée afin de rendre la lecture facile.

```
ciscoasa#show logging
!--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-7-
609001: Built local-host outside:172.22.1.1 %ASA-6-305011: Built dynamic TCP translation
from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP
connection 90 for outside:172.22.1.1/80 (172.22.1.1/80) to inside:192.168.1.50/1107
(172.22.1.254/1025) %ASA-6-302014: Teardown TCP connection 90 for outside:172.22.1.1/80
to inside:192.168.1.50/1107 duration 0:00:30 bytes 0 SYN Timeout
%ASA-7-609002: Teardown local-host outside:172.22.1.1 duration 0:00:30
%ASA-6-305012: Teardown dynamic TCP translation from inside:192.168.1.50/1107
to outside:172.22.1.254/1025 duration 0:01:00
%ASA-7-609002: Teardown local-host inside:192.168.1.50 duration 0:01:00
```

Le message syslog indique que la connexion est fermée en raison de l'expiration de SYN. Cela indique à l'administrateur qu'aucune réponse du serveur de l'application X n'a été reçue par ASA. Les raisons d'arrêt des messages syslog peuvent varier.L'expiration de SYN est enregistrée dans un journal en raison d'un arrêt de connexion forcé après 30 secondes qui se produit après l'achèvement de la connexion en trois temps. Ce problème se produit habituellement si le serveur ne répond pas à une demande de connexion, et, dans la plupart des cas, n'est pas lié à la configuration sur PIX/ASA.Afin de résoudre ce problème, référez-vous à la liste de contrôle suivante :Assurez-vous que la commande static est entrée correctement et qu'elle ne chevauche pas d'autres commandes static, par exemple,

```
ciscoasa#show logging
```

```
!--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-7-
609001: Built local-host outside:172.22.1.1 %ASA-6-305011: Built dynamic TCP translation
from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP
connection 90 for outside:172.22.1.1/80 (172.22.1.1/80) to inside:192.168.1.50/1107
(172.22.1.254/1025) %ASA-6-302014: Teardown TCP connection 90 for outside:172.22.1.1/80
to inside:192.168.1.50/1107 duration 0:00:30 bytes 0 SYN Timeout
%ASA-7-609002: Teardown local-host outside:172.22.1.1 duration 0:00:30
%ASA-6-305012: Teardown dynamic TCP translation from inside:192.168.1.50/1107
to outside:172.22.1.254/1025 duration 0:01:00
%ASA-7-609002: Teardown local-host inside:192.168.1.50 duration 0:01:00
```

La charge statique NAT dans ASA 8.3 et plus tard peut être configurée comme affiché ici :

```
ciscoasa#show logging
!--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-7-
609001: Built local-host outside:172.22.1.1 %ASA-6-305011: Built dynamic TCP translation
from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP
connection 90 for outside:172.22.1.1/80 (172.22.1.1/80) to inside:192.168.1.50/1107
(172.22.1.254/1025) %ASA-6-302014: Teardown TCP connection 90 for outside:172.22.1.1/80
to inside:192.168.1.50/1107 duration 0:00:30 bytes 0 SYN Timeout
%ASA-7-609002: Teardown local-host outside:172.22.1.1 duration 0:00:30
%ASA-6-305012: Teardown dynamic TCP translation from inside:192.168.1.50/1107
to outside:172.22.1.254/1025 duration 0:01:00
%ASA-7-609002: Teardown local-host inside:192.168.1.50 duration 0:01:00
```

Assurez-vous qu'il existe une liste d'accès afin de permettre l'accès à l'adresse IP globale à partir de l'extérieur et qu'elle est liée à l'interface :

```
ciscoasa#show logging
!--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-7-
609001: Built local-host outside:172.22.1.1 %ASA-6-305011: Built dynamic TCP translation
from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP
connection 90 for outside:172.22.1.1/80 (172.22.1.1/80) to inside:192.168.1.50/1107
(172.22.1.254/1025) %ASA-6-302014: Teardown TCP connection 90 for outside:172.22.1.1/80
to inside:192.168.1.50/1107 duration 0:00:30 bytes 0 SYN Timeout
%ASA-7-609002: Teardown local-host outside:172.22.1.1 duration 0:00:30
%ASA-6-305012: Teardown dynamic TCP translation from inside:192.168.1.50/1107
to outside:172.22.1.254/1025 duration 0:01:00
%ASA-7-609002: Teardown local-host inside:192.168.1.50 duration 0:01:00
```

Pour une connexion réussie avec le serveur, la passerelle par défaut sur le serveur doit pointer vers l'interface DMZ de PIX/ASA.Référez-vous à Messages système ASA pour plus d'informations sur les messages syslog.

- **Créer un nouveau filtre de capture.**Grâce au précédent trafic capturé et aux précédents messages syslog, l'administrateur sait que l'application X devrait quitter ASA via l'interface externe.

```
ciscoasa(config)#access-list outside_test permit tcp any host 172.22.1.1 eq 80
!--- When you leave the source as 'any', it allows !--- the administrator to monitor any
network address translation (NAT). ciscoasa(config)#access-list outside_test permit tcp host
172.22.1.1 eq 80 any
!--- When you reverse the source and destination information, !--- it allows return traffic
to be captured. ciscoasa(config)#capture outside_interface access-list outside_test
interface outside
```

L'utilisateur doit lancer une nouvelle session avec l'application X. Une fois que l'utilisateur a lancé une nouvelle session de l'application X, l'administrateur ASA doit émettre la commande **show capture outside_interface** sur ASA.

```
ciscoasa(config)#show capture outside_interface
3 packets captured
   1: 16:15:34.278870 172.22.1.254.1026 > 172.22.1.1.80:
S 1676965539:1676965539(0) win 65535 <mss 1380,nop,nop,sackOK>
   2: 16:15:44.969630 172.22.1.254.1027 > 172.22.1.1.80:
S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK>
   3: 16:15:47.898619 172.22.1.254.1027 > 172.22.1.1.80:
```

```
S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK>
3 packets shown
```

La capture montre le trafic quittant l'interface externe mais ne montre aucun trafic de réponse en provenance du serveur 172.22.1.1. Cette capture montre les données lorsqu'elles quittent ASA.

- **Utiliser l'option de suivi de paquets.**Grâce aux sections précédentes, l'administrateur ASA a appris assez d'informations pour utiliser l'option **packet-tracer** dans ASA.**Remarque:** ASA prend en charge la commande **packet-tracer** à partir de la version 7.2.

```
ciscoasa#packet-tracer input inside tcp 192.168.1.50 1025 172.22.1.1 http
!--- This line indicates a source port of 1025. If the source !--- port is not known, any
number can be used. !--- More common source ports typically range !--- between 1025 and
65535. Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC
Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule
Additional Information: MAC Access list Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW
Config: Additional Information: Found no matching flow, creating a new flow Phase: 4 Type:
ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.22.1.0
255.255.255.0 outside Phase: 5 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-
group inside_acl in interface inside
access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq www
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
  match ip inside 192.168.1.0 255.255.255.0 outside any
    dynamic translation to pool 1 (172.22.1.254)
    translate_hits = 6, untranslate_hits = 0
Additional Information:
Dynamic translate 192.168.1.50/1025 to 172.22.1.254/1028
using netmask 255.255.255.255

Phase: 9
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
  match ip inside 192.168.1.0 255.255.255.0 outside any
    dynamic translation to pool 1 (172.22.1.254)
    translate_hits = 6, untranslate_hits = 0
Additional Information:

Phase: 10
Type: CAPTURE
Subtype:
```

```
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 94, packet dispatched to next module

Phase: 15
Type: ROUTE-LOOKUP
Subtype: output and adjacency
Result: ALLOW
Config:
Additional Information:
found next-hop 172.22.1.1 using egress ifc outside
adjacency Active
next-hop mac address 0030.a377.f854 hits 11
!--- The MAC address is at Layer 2 of the OSI model. !--- This tells the administrator the
next host !--- that should receive the data packet. Result: input-interface: inside input-
status: up input-line-status: up output-interface: outside output-status: up output-line-
status: up Action: allow
```

La sortie la plus importante de la commande **packet-tracer** est la dernière ligne, qui est Action: `laissez`.

Les trois options à l'étape 3 montrent chacune à l'administrateur qu'ASA n'est pas responsable des problèmes de l'application X. Le trafic de l'application X quitte ASA et ASA ne reçoit pas de réponse du serveur de l'application X.

Opérations suivantes

Il y a beaucoup de composants qui permettent à l'application X de fonctionner correctement pour des utilisateurs. Ces composants incluent l'ordinateur de l'utilisateur, le client de l'application X, le routage, les stratégies d'accès et le serveur de l'application X. Dans l'exemple précédent, nous avons montré qu'ASA reçoit et transfert le trafic de l'application X. Les administrateurs du serveur et de l'application X doivent maintenant s'impliquer. Les administrateurs doivent vérifier que les services de l'application s'exécutent, passer en revue tous les journaux sur le serveur et vérifier

que le trafic de l'utilisateur est reçu par le serveur et l'application X.

Problème : Message d'erreur Terminating TCP-Proxy connection

Vous recevez le message d'erreur suivant :

```
ciscoasa#packet-tracer input inside tcp 192.168.1.50 1025 172.22.1.1 http
!--- This line indicates a source port of 1025. If the source !--- port is not known, any number
can be used. !--- More common source ports typically range !--- between 1025 and 65535. Phase: 1
Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 2
Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC
Access list Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information:
Found no matching flow, creating a new flow Phase: 4 Type: ROUTE-LOOKUP Subtype: input Result:
ALLOW Config: Additional Information: in 172.22.1.0 255.255.255.0 outside Phase: 5 Type: ACCESS-
LIST Subtype: log Result: ALLOW Config: access-group inside_acl in interface inside
access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq www
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
  match ip inside 192.168.1.0 255.255.255.0 outside any
    dynamic translation to pool 1 (172.22.1.254)
    translate_hits = 6, untranslate_hits = 0
Additional Information:
Dynamic translate 192.168.1.50/1025 to 172.22.1.254/1028
using netmask 255.255.255.255

Phase: 9
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
  match ip inside 192.168.1.0 255.255.255.0 outside any
    dynamic translation to pool 1 (172.22.1.254)
    translate_hits = 6, untranslate_hits = 0
Additional Information:

Phase: 10
Type: CAPTURE
Subtype:
Result: ALLOW
```

```
Config:
Additional Information:

Phase: 11
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 94, packet dispatched to next module

Phase: 15
Type: ROUTE-LOOKUP
Subtype: output and adjacency
Result: ALLOW
Config:
Additional Information:
found next-hop 172.22.1.1 using egress ifc outside
adjacency Active
next-hop mac address 0030.a377.f854 hits 11
!--- The MAC address is at Layer 2 of the OSI model. !--- This tells the administrator the next
host !--- that should receive the data packet. Result: input-interface: inside input-status: up
input-line-status: up output-interface: outside output-status: up output-line-status: up Action:
allow
```

Solution

Explication : Ce message s'affiche quand la limite de la mémoire tampon de réassemblage est dépassée pendant l'assemblage de segments TCP.

- *source_address/source_port* - Adresse IP source et port source du paquet lançant la connexion.
- *dest_address/dest_port* - Adresse IP de destination et port de destination du paquet lançant la connexion.
- *interface_inside* - Nom de l'interface sur laquelle le paquet qui a lancé la connexion arrive.
- *interface_outside* - Nom de l'interface sur laquelle le paquet qui a lancé la connexion sort.
- *limit* - Limite de la connexion embryonnaire configurée pour la classe de trafic.

La résolution de ce problème est de désactiver l'inspection RTSP dans le dispositif de sécurité, comme indiqué.

```
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  no inspect rtsp
```

Référez-vous à l'ID de bogue Cisco CSCsl15229 (clients enregistrés seulement) pour plus de détails.

Problème : "%ASA-6-110003 : Le routage n'a pas localisé le prochain-saut pour le protocole message d'erreur de src d'interface »

Le trafic de baisses ASA avec l'`error:%ASA-6-110003 : Le routage n'a pas localisé le prochain-saut pour le protocole de l'interface de src : port du src IP/src à l'interface DEST :` message d'`erreur de port DEST IP/dest`.

Solution

Cette erreur se produit quand les essais ASA pour trouver le prochain saut sur une table de routage d'interface. Typiquement, ce message est reçu quand l'ASA a une traduction (xlate) établie à une interface et à une artère précisant une interface différente. Vérifiez une mauvaise configuration sur les déclarations NAT. La résolution de la mauvaise configuration peut résoudre l'erreur.

Problème : Connexion bloquée par ASA avec le « %ASA-5-305013 : Les règles NAT asymétriques se sont assorties pour message d'erreur en avant et de flux inverses le »

La connexion est bloquée par ASA, et ce message d'erreur est reçu :


```
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  no inspect rtsp
```


Solution

Quand le NAT est exécuté, ASA des essais également pour renverser le paquet et les contrôles si ceci frappe n'importe quelle traduction. S'il n'en frappe pas ou une traduction NAT différente, alors il y a une non-concordance. Vous voyez le plus généralement ce message d'erreur quand il y a

différentes règles NAT configurées pour sortant et le trafic entrant avec la mêmes source et destination. Vérifiez la déclaration NAT pour le trafic intéressé.

Problème : Recevez l'erreur - %ASA-5-321001 : La limite de « conns » de ressource de 10000 a atteint pour le système

Solution

Cette erreur signifie que les connexions pour un serveur situé à travers une ASA ont atteint leur limite maximum. Ceci a pu être une indication d'une attaque DoS à un serveur dans votre réseau. Utilisez MPF sur l'ASA et réduisez la limite embryonnaire de connexions. En outre, activez la détection morte de connexion (DCD). Référez-vous à cet extrait de configuration :

```
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  no inspect rtsp
```

Problème : Recevez l'erreur %PIX-1-106021 : Refusez le contrôle de chemin inverse TCP/UDP du src_addr au dest_addr sur l'int_name d'interface

Solution

Ce message de log est reçu quand le contrôle de chemin inverse est activé. Émettez cette commande afin de résoudre le problème et désactiver le contrôle de chemin inverse :

```
no ip verify reverse-path interface <interface name>
```

Problème : Interruption de la connexion Internet due à la détection de menace

Ce message d'erreur est reçu sur l'ASA :

```
no ip verify reverse-path interface <interface name>
```

Solution

Ce message est généré par la détection de menace due à la configuration par défaut quand un

comportement de trafic anormal est détecté. Le message se concentre sur Miralix Licen 3000 qui est un port TCP/UDP. Localisez le périphérique qui utilise le port 3000. Vérifiez les statistiques graphiques ASDM pour la détection de menace et vérifiez les attaques par le haut pour voir si elle affiche le port 3000 et l'adresse IP source. Si c'est un périphérique légitime, vous pouvez incrémenter le débit de base de détection de menace sur l'ASA afin de résoudre ce message d'erreur.

Informations connexes

- Référence des commandes Cisco ASA
- Référence des commandes Cisco PIX
- Messages d'erreur et messages système Cisco ASA
- Messages d'erreur et messages système Cisco PIX
- Assistance des dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Assistance des dispositifs de sécurité de la gamme Cisco PIX 500
- Support et documentation techniques - Cisco Systems