Fehlerbehebung bei Verbindungen über PIX und ASA

Inhalt

Einführung

Dieses Dokument enthält Vorschläge und Vorschläge zur Fehlerbehebung bei der Verwendung der Cisco Adaptive Security Appliance (ASA) der Serie ASA 5500 und der Cisco Security Appliance der Serie PIX 500. In der Regel sind Firewalls (PIX oder ASA) ein Hauptziel und werden als Ursache für Ausfälle bezeichnet, wenn Anwendungen oder Netzwerkquellen ausfallen oder

nicht verfügbar sind. Bei einigen Tests auf ASA oder PIX kann ein Administrator feststellen, ob ASA/PIX das Problem verursacht.

Weitere Informationen finden Sie unter PIX/ASA: Einrichtung und Fehlerbehebung für Verbindungen über die Cisco Security Appliance, um mehr über die schnittstellenbezogene Fehlerbehebung auf den Cisco Security Appliances zu erfahren.

Hinweis: Im Mittelpunkt dieses Dokuments stehen ASA und PIX. Sobald die Fehlerbehebung für ASA oder PIX abgeschlossen ist, ist es wahrscheinlich, dass weitere Fehlerbehebungen bei anderen Geräten (Routern, Switches, Servern usw.) erforderlich sein werden.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ASA 5510 mit OS 7.2.1 und 8.3.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Dieses Dokument kann auch mit den folgenden Hardware- und Softwareversionen verwendet werden:

- ASA und PIX OS 7.0, 7.1, 8.3 und höher
- Firewall Services Module (FWSM) 2.2, 2.3 und 3.1

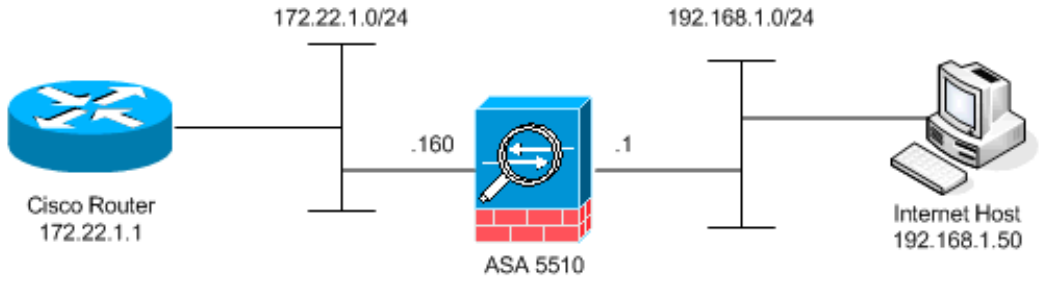
Hinweis: Bestimmte Befehle und Syntax können je nach Softwareversion variieren.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Im Beispiel wird davon ausgegangen, dass ASA oder PIX in Produktion sind. Die ASA/PIX-Konfiguration kann relativ einfach (nur 50 Konfigurationslinien) oder komplex (Hunderte bis Tausende von Konfigurationslinien) sein. Benutzer (Clients) oder Server können sich entweder in einem sicheren Netzwerk (innerhalb) oder in einem unsicheren Netzwerk (DMZ oder außerhalb) befinden.



Die ASA beginnt mit dieser Konfiguration. Die Konfiguration soll dem Labor einen Referenzpunkt geben.

ASA Erstkonfiguration

```
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
```

Problem

Ein Benutzer kontaktiert die IT-Abteilung und berichtet, dass die Anwendung X nicht mehr funktioniert. Der Vorfall wird an den ASA/PIX-Administrator eskaliert. Der Administrator hat wenig Kenntnisse über diese Anwendung. Bei Verwendung von ASA/PIX erkennt der Administrator, welche Ports und Protokolle von Anwendung X verwendet werden und was die Ursache des Problems sein kann.

Lösung

Der ASA/PIX-Administrator muss so viele Informationen wie möglich vom Benutzer erfassen. Nützliche Informationen:

- Quell-IP-Adresse - Dies ist in der Regel die Arbeitsstation oder der Computer des Benutzers.
- Ziel-IP-Adresse - Die Server-IP-Adresse, mit der der Benutzer oder die Anwendung eine Verbindung herstellen möchte.
- Ports und Protokolle, die von der Anwendung verwendet werden

Häufig hat der Administrator das Glück, eine dieser Fragen beantworten zu können. In diesem Beispiel kann der Administrator keine Informationen sammeln. Eine Überprüfung der ASA/PIX-Syslog-Meldungen ist ideal, es ist jedoch schwierig, das Problem zu lokalisieren, wenn der Administrator nicht weiß, wonach er suchen soll.

Schritt 1 - Ermitteln der IP-Adresse des Benutzers

Es gibt viele Möglichkeiten, die IP-Adresse des Benutzers zu ermitteln. In diesem Dokument geht es um ASA und PIX. In diesem Beispiel werden ASA und PIX zum Ermitteln der IP-Adresse verwendet.

Der Benutzer versucht, mit der ASA/PIX zu kommunizieren. Diese Kommunikation kann ICMP, Telnet, SSH oder HTTP sein. Das gewählte Protokoll sollte auf ASA/PIX nur über eine begrenzte Aktivität verfügen. In diesem speziellen Beispiel pingt der Benutzer die interne Schnittstelle der ASA an.

Der Administrator muss eine oder mehrere dieser Optionen einrichten und den Benutzer dann dazu veranlassen, einen Ping an die interne Schnittstelle der ASA zu senden.

- **Syslog**Stellen Sie sicher, dass die Protokollierung aktiviert ist. Die Protokollierungsebene muss auf **debug** festgelegt werden. Die Protokollierung kann an verschiedene Standorte gesendet werden. In diesem Beispiel wird der ASA-Protokollpuffer verwendet. Möglicherweise benötigen Sie einen externen Protokollierungsserver in Produktionsumgebungen.

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

  Der Benutzer pingt die interne Schnittstelle der ASA an (ping 192.168.1.1). Diese Ausgabe wird angezeigt.

  ```
  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.
  ```

- **ASA Capture-Funktion**Der Administrator muss eine Zugriffsliste erstellen, die definiert, welchen Datenverkehr die ASA erfassen muss. Nachdem die Zugriffsliste definiert wurde, enthält der Befehl **capture** die Zugriffsliste und wendet sie auf eine Schnittstelle an.

  ```
  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
  ```

  Der Benutzer pingt die interne Schnittstelle der ASA an (ping 192.168.1.1). Diese Ausgabe wird angezeigt.

  ```
  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.
  ```

  Hinweis: Um die Capture-Datei auf ein System wie ätherisch herunterzuladen, können Sie sie wie in dieser Ausgabe dargestellt herunterladen.

  ```
  !--- Open an Internet Explorer and browse with this https link format: https://[
  ```

  Weitere Informationen finden Sie unter ASA/PIX: Paketerfassung mithilfe des CLI- und ASDM-Konfigurationsbeispiels, um mehr über die Paketerfassung in ASA zu erfahren.

- **Debuggen**Der Befehl **debug icmp trace** wird verwendet, um den ICMP-Datenverkehr des Benutzers zu erfassen.

```
ciscoasa#debug icmp trace
```

Der Benutzer pingt die interne Schnittstelle der ASA an (ping 192.168.1.1). Diese Ausgabe wird auf der Konsole angezeigt.

```
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.
```

Um **debug icmp trace** zu deaktivieren, verwenden Sie einen der folgenden Befehle:**Kein debuggen icmp traceundebug icmp traceAlle debug**, **Alle dedebug** oder **alle aus**

Jede dieser drei Optionen hilft dem Administrator, die Quell-IP-Adresse zu bestimmen. In diesem Beispiel ist die Quell-IP-Adresse des Benutzers 192.168.1.50. Der Administrator ist bereit, mehr über Anwendung X zu erfahren und die Ursache des Problems zu bestimmen.

Schritt 2 - Bestimmen der Ursache des Problems

Mit Bezug auf die Informationen, die im Abschnitt Schritt 1 dieses Dokuments aufgeführt sind, kennt der Administrator jetzt die Quelle einer Anwendung X. Der Administrator ist bereit, mehr über Anwendung X zu erfahren und zu beginnen, herauszufinden, wo die Probleme sein könnten.

Der ASA/PIX-Administrator muss die ASA für mindestens einen der aufgeführten Vorschläge vorbereiten. Sobald der Administrator bereit ist, initiiert der Benutzer die Anwendung X und beschränkt alle anderen Aktivitäten, da zusätzliche Benutzeraktivitäten zu Verwirrung führen oder den ASA/PIX-Administrator irreführen können.

- **Syslog-Meldungen überwachen.**Suchen Sie in Schritt 1 nach der Quell-IP-Adresse des Benutzers, den Sie gefunden haben. Der Benutzer initiiert die Anwendung X. Der ASA-Administrator gibt den Befehl **show logging aus** und zeigt die Ausgabe an.

  ```
  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)
  ```

  Die Protokolle zeigen an, dass die Ziel-IP-Adresse 172.22.1.1, das Protokoll TCP, der Zielport HTTP/80 ist und dass der Datenverkehr an die externe Schnittstelle gesendet wird.
- **Ändern Sie die Erfassungsfilter.**Der Befehl **access-list inside_test** wurde bereits verwendet und wird hier verwendet.

  ```
  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.
  ```

  Der Benutzer initiiert die Anwendung X. Der ASA-Administrator gibt dann den Befehl **show capture inside_interface aus** und zeigt die Ausgabe an.

  ```
  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>
```

Der erfasste Datenverkehr bietet dem Administrator mehrere wertvolle Informationen:Zieladresse - 172.22.1.1Portnummer: 80/httpProtokoll - TCP (beachten Sie die "S"- oder Syn-Markierung)Darüber hinaus weiß der Administrator auch, dass der Datenverkehr für Anwendung X bei der ASA eingeht.Wenn die Ausgabe diese Ausgabe des Befehls **show capture inside_interface** war, erreichte der Anwendungsdatenverkehr entweder nie die ASA oder der Erfassungsfilter war nicht so eingestellt, dass der Datenverkehr erfasst wurde:

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

In diesem Fall sollte der Administrator erwägen, den Computer des Benutzers und alle Router oder anderen Netzwerkgeräte im Pfad zwischen dem Benutzercomputer und der ASA zu untersuchen.**Hinweis:** Wenn der Datenverkehr an einer Schnittstelle eingeht, werden die Daten vom **Erfassungs-**Befehl aufgezeichnet, bevor ASA-Sicherheitsrichtlinien den Datenverkehr analysieren. Beispielsweise verweigert eine Zugriffsliste den gesamten eingehenden Datenverkehr an einer Schnittstelle. Der Befehl **zur Erfassung** zeichnet den Datenverkehr noch auf. Die ASA-Sicherheitsrichtlinie analysiert anschließend den Datenverkehr.

- **Debuggen**Der Administrator ist nicht mit Anwendung X vertraut und weiß daher nicht, welche der Debugdienste für die Untersuchung von Anwendung X aktiviert werden sollen. Möglicherweise ist Debug zu diesem Zeitpunkt nicht die beste Fehlerbehebungsoption.

Mit den Informationen, die in Schritt 2 gesammelt wurden, erhält der ASA-Administrator einige wertvolle Informationen. Der Administrator weiß, dass der Datenverkehr über die interne Schnittstelle der ASA, die Quell-IP-Adresse, die Ziel-IP-Adresse und die Service-Anwendung X (TCP/80) eingeht. In den Syslogs weiß der Administrator auch, dass die Kommunikation ursprünglich erlaubt war.

Schritt 3: Überprüfen und Überwachen des Anwendungsdatenverkehrs

Der ASA-Administrator möchte bestätigen, dass der Anwendungs-X-Datenverkehr die ASA verlassen hat, und den Rückverkehr vom Anwendungs-X-Server überwachen.

- **Syslog-Meldungen überwachen.**Syslog-Meldungen für die Quell-IP-Adresse (192.168.1.50) oder die Ziel-IP-Adresse (172.22.1.1) filtern. Über die Befehlszeile sehen die Filterfunktionen von Syslog-Meldungen wie **die Protokollierung** aus. **| einschließlich 192.168.1.50** oder **Show Logging | einschließlich 172.22.1.1**. In diesem Beispiel wird der Befehl **show logging** ohne Filter verwendet. Die Ausgabe wird unterdrückt, um das Lesen zu vereinfachen.

```
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
```

Die Syslog-Meldung weist darauf hin, dass die Verbindung aufgrund des SYN-Timeouts

geschlossen wurde. Dies weist den Administrator darauf hin, dass von der ASA keine Serverantworten von Anwendung X empfangen wurden. Die Gründe für die Terminierung von Syslog-Nachrichten können variieren.Das SYN-Timeout wird protokolliert, weil eine erzwungene Verbindungsabbruch nach 30 Sekunden erfolgt, die nach der Drei-Wege-Handshake-Beendigung auftritt. Dieses Problem tritt in der Regel dann auf, wenn der Server nicht auf eine Verbindungsanforderung reagiert und in den meisten Fällen nicht mit der Konfiguration auf PIX/ASA zusammenhängt.Um dieses Problem zu beheben, lesen Sie die folgende Checkliste:Stellen Sie sicher, dass der statische Befehl korrekt eingegeben wird und sich nicht mit anderen statischen Befehlen überschneidet, z. B.

```
static (inside,outside) x.x.x.x  y.y.y.y netmask 255.255.255.255
```

Die statische NAT in ASA 8.3 und höher kann wie hier gezeigt konfiguriert werden:

```
object network obj-y.y.y.y
 host y.y.y.y
 nat (inside,outside) static x.x.x.x
```

Stellen Sie sicher, dass eine Zugriffsliste vorhanden ist, um den Zugriff von außen auf die globale IP-Adresse zuzulassen und dass sie an die Schnittstelle gebunden ist:

```
access-list OUTSIDE_IN extended permit tcp any host x.x.x.x eq www
access-group OUTSIDE_IN in interface outside
```

Für eine erfolgreiche Verbindung mit dem Server muss das Standard-Gateway auf die DMZ-Schnittstelle von PIX/ASA zeigen.Weitere Informationen zu den Syslog-Meldungen finden Sie unter ASA-Systemmeldungen.

- **Erstellen Sie einen neuen Erfassungsfilter.**Aus früheren erfassten Datenverkehr- und Syslog-Meldungen weiß der Administrator, dass die Anwendung X die ASA über die externe Schnittstelle verlassen sollte.

```
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
```

Der Benutzer muss eine neue Sitzung mit Anwendung X starten. Nachdem der Benutzer eine neue Sitzung mit Anwendung X initiiert hat, muss der ASA-Administrator den Befehl **show capture outside_interface** auf der ASA ausgeben.

```
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
```

Die Erfassung zeigt den Datenverkehr, der von der externen Schnittstelle ausgeht, aber keinen Antwortverkehr vom Server 172.22.1.1 an. Diese Erfassung zeigt die Daten, während diese die ASA verlassen.

- **Verwenden Sie die Option Packet-Tracer.**Aus den vorherigen Abschnitten hat der ASA-Administrator genügend Informationen gesammelt, um die **Packet-Tracer-**Option in der ASA zu verwenden.**Hinweis:** Die ASA unterstützt den Befehl **Packet-Tracer** ab 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
```

Die wichtigste Ausgabe des Befehls **Packet-Tracer** ist die letzte Zeile, nämlich `Action: erlauben`.

Die drei Optionen in Schritt 3 zeigen dem Administrator, dass die ASA nicht für die X-Probleme der Anwendung verantwortlich ist. Der Datenverkehr mit der Anwendung X verlässt die ASA, und die ASA erhält keine Antwort vom Server mit der Anwendung X.

Nächste Schritte

Es gibt viele Komponenten, mit denen die Anwendung X für Benutzer korrekt funktioniert. Zu den Komponenten gehören der Computer des Benutzers, der Client der Anwendung X, Routing, Zugriffsrichtlinien und der Server der Anwendung X. Im vorherigen Beispiel haben wir bewiesen, dass die ASA den Anwendungs-X-Datenverkehr empfängt und weiterleitet. Der Server- und der Anwendungs-X-Administrator sollten sich nun einmischen. Administratoren sollten überprüfen, ob die Anwendungsdienste ausgeführt werden, alle Protokolle auf dem Server überprüfen und sicherstellen, dass der Datenverkehr des Benutzers vom Server und von der Anwendung X empfangen wird.

Problem: Beenden der TCP-Proxy-Verbindungsfehlermeldung

Sie erhalten diese Fehlermeldung:

```
%PIX|ASA-5-507001: Terminating TCP-Proxy connection from
interface_inside:source_address/source_port to interface_outside:dest_address/dest_port -
reassembly limit of limit bytes exceeded
```

Lösung

Erläuterung: Diese Meldung wird angezeigt, wenn der Grenzwert für den Reassemblierungspuffer beim Zusammenfügen von TCP-Segmenten überschritten wird.

- *source_address/source_port* - Die Quell-IP-Adresse und der Quell-Port des Pakets, das die Verbindung initiiert.
- *dest_address/dest_port* - Die Ziel-IP-Adresse und der Ziel-Port des Pakets, das die Verbindung initiiert.
- *interface_inside* - Der Name der Schnittstelle, auf der das Paket, das die Verbindung initiiert hat, eingeht.
- *interface_outside* - Der Name der Schnittstelle, auf der das Paket, das die Verbindung initiiert hat, beendet.
- *limit* - Die konfigurierte embryonale Verbindungsgrenze für die Datenverkehrsklasse.

Die Lösung für dieses Problem ist, die RTSP-Prüfung in der Security Appliance wie gezeigt zu deaktivieren.

```
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
```

Weitere Informationen finden Sie unter Cisco Bug ID CSCsl15229 (nur registrierte Kunden).

Problem: "%ASA-6-110003: Routing konnte nächsten Hop für Protokoll von der src-Schnittstelle nicht gefunden werden" Fehlermeldung

ASA verwirft Datenverkehr mit dem `Fehler:%ASA-6-110003: Beim Routing konnte der nächste Hop für das Protokoll von src interface:src IP/src port to dest interface:dest IP/dest port` Fehlermeldung `nicht gefunden werden`.

Lösung

Dieser Fehler tritt auf, wenn die ASA versucht, den nächsten Hop in einer Schnittstellenrouting-Tabelle zu finden. In der Regel wird diese Nachricht empfangen, wenn die ASA über eine auf eine Schnittstelle erstellte Übersetzung (Xlate) und eine Route verfügt, die auf eine andere Schnittstelle hinweist. Überprüfen Sie die NAT-Anweisungen auf eine Fehlkonfiguration. Die Behebung der Fehlkonfiguration kann den Fehler beheben.

Problem: Durch ASA blockierte Verbindung mit dem " %ASA-5-

305013: Asymmetrische NAT-Regeln für Vor- und Rücklauf zugeordnet" Fehlermeldung

Die Verbindung wird von ASA blockiert, und diese Fehlermeldung wird empfangen:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward
 and reverse flows; Connection protocol src
 interface_name:source_address/source_port dest
 interface_name:dest_address/dest_port denied due to NAT reverse path
 failure.
```

Lösung

Wenn die NAT durchgeführt wird, versucht ASA auch, das Paket umzukehren, und überprüft, ob es auf eine Übersetzung trifft. Wenn keine oder keine andere NAT-Übersetzung aufgerufen wird, tritt eine Diskrepanz auf. Diese Fehlermeldung wird am häufigsten angezeigt, wenn für ausgehenden und eingehenden Datenverkehr mit derselben Quelle und demselben Ziel unterschiedliche NAT-Regeln konfiguriert sind. Überprüfen Sie die NAT-Anweisung für den betreffenden Datenverkehr.

Problem: Empfangsfehler - %ASA-5-321001: Ressource 'conns'-Grenzwert für das System von 10.000 erreicht

Lösung

Dieser Fehler bedeutet, dass die Verbindungen für einen Server, der sich über eine ASA befindet, ihre maximale Grenze erreicht haben. Dies könnte ein Hinweis auf einen DoS-Angriff auf einen Server in Ihrem Netzwerk sein. Verwenden Sie MPF auf der ASA und reduzieren Sie den Grenzwert für embryonale Verbindungen. Aktivieren Sie außerdem die Option Dead Connection Detection (DCD). Weitere Informationen finden Sie in diesem Konfigurationsausschnitt:

```
class-map limit
 match access-list limit
!
policy-map global_policy
 class limit
  set connection embryonic-conn-max 50
  set connection timeout embryonic 0:00:10 dcd
!
access-list limit line 1 extended permit tcp any host x.x.x.x
```

Problem: Receive-Fehler %PIX-1-106021: Verweigern Sie die Überprüfung des TCP/UDP-Pfads von src_addr auf dest_addr auf der Schnittstelle int_name.

Lösung

Diese Protokollmeldung wird empfangen, wenn die Überprüfung des umgekehrten Pfads aktiviert

ist. Geben Sie diesen Befehl ein, um das Problem zu beheben und die Überprüfung des umgekehrten Pfads zu deaktivieren:

```
no ip verify reverse-path interface
```

Problem: Unterbrechung der Internetverbindung durch Bedrohungserkennung

Diese Fehlermeldung wird auf der ASA angezeigt:

```
%ASA-4-733100: [Miralix Licen 3000] drop rate-1 exceeded. Current burst
rate is 100 per second, max configured rate is 10; Current average rate is 4
per second, max configured rate is 5; Cumulative total count is 2526
```

Lösung

Diese Nachricht wird durch die Erkennung von Bedrohungen generiert, da die Standardkonfiguration verwendet wird, wenn ein ungewöhnliches Datenverkehrsverhalten erkannt wird. Die Nachricht konzentriert sich auf Miralix Licen 3000, einen TCP/UDP-Port. Suchen Sie das Gerät, das Port 3000 verwendet. Prüfen Sie die grafische ASDM-Statistik zur Erkennung von Bedrohungen, und überprüfen Sie die häufigsten Angriffe, um festzustellen, ob Port 3000 und die Quell-IP-Adresse angezeigt werden. Wenn es sich um ein legitimes Gerät handelt, können Sie die grundlegende Bedrohungserkennungsrate auf ASA erhöhen, um diese Fehlermeldung zu beheben.

Zugehörige Informationen

- Cisco ASA-Befehlsreferenz
- Cisco PIX-Befehlsreferenz
- Fehler- und Systemmeldungen der Cisco ASA
- Cisco PIX-Fehler und -Systemmeldungen
- Unterstützung von Cisco Adaptive Security Appliances der Serie ASA 5500
- Unterstützung von Cisco PIX Security Appliances der Serie 500
- Technischer Support und Dokumentation - Cisco Systems