Conexiones del Troubleshooting con el PIX y el ASA

Contenido

Introducción

Este documento proporciona ideas y sugerencias de Troubleshooting para cuando utilice Cisco ASA 5500 Series Adaptive Security Appliance (ASA) y Cisco PIX 500 Series Security Appliance. A menudo, cuando las aplicaciones o los orígenes de red se rompen o no están disponibles, los Firewall (PIX o ASA) tienden a ser un objetivo principal y culpado como la causa de las caídas del

sistema. Con alguna prueba en el ASA o el PIX, un administrador puede determinar independientemente de si ASA/PIX causa el problema.

Consulte PIX/ASA: Establezca y resuelva problemas la Conectividad a través del dispositivo del Cisco Security para aprender más sobre el troubleshooting relacionado interfaz en los dispositivos de seguridad de Cisco.

Nota: Este documento se centra en el ASA y el PIX. Una vez que el resolver problemas es completo en el ASA o el PIX, es probable que el Troubleshooting adicional pueda ser necesario con los otros dispositivos (Routers, Switches, los servidores, y así sucesivamente).

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en Cisco ASA 5510 con OS 7.2.1 y 8.3.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Este documento se puede también utilizar con estas versiones de software y hardware:

- ASA y PIX OS 7.0, 7.1, 8.3, y posterior
- Módulo de servicios del Firewall (FWSM) 2.2, 2.3, y 3.1

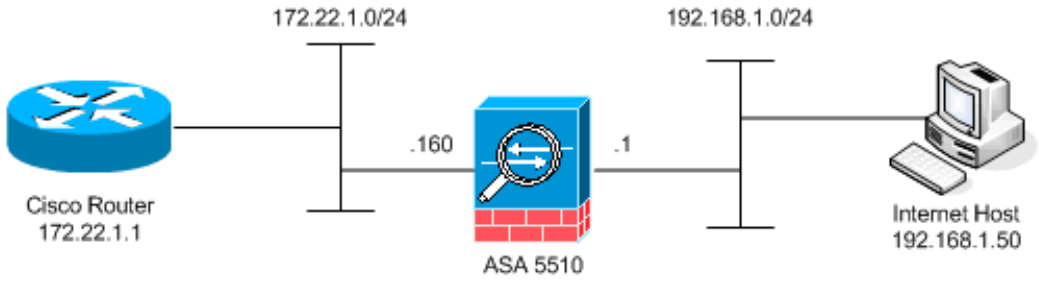
Nota: Los comandos y el sintaxis específicos pueden variar entre las versiones de software.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

El ejemplo asume que el ASA o el PIX está en la producción. ASA/PIX la configuración puede ser relativamente simple (solamente 50 líneas de configuración) o el complejo (centenares a los millares de líneas de configuración). Los usuarios (clientes) o los servidores pueden estar en una red segura (dentro) o una red unsecure (DMZ o exterior).



El comienzo ASA con esta configuración. La configuración se piensa para dar al laboratorio al punto de referencia.

Configuración inicial 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
```

Problema

Un usuario entra en contacto el departamento TIC y señala que la aplicación X trabaja no más. El incidente se extiende ASA/PIX al administrador. El administrador tiene poco conocimiento de esta aplicación determinada. Con el uso del ASA/PIX, el administrador descubre qué aplicaciones de la aplicación X de los puertos y protocolos así como qué pudo ser la causa del problema.

Solución

ASA/PIX el administrador necesita recopilar tanta información del usuario como sea posible. La información útil incluye:

- Dirección IP de origen — Éste es típicamente la estación de trabajo o el ordenador del usuario.
- IP Address de destino — El dirección IP del servidor que el usuario o la aplicación intenta conectar.
- Puertos y protocolos las aplicaciones de la aplicación

El administrador es a menudo afortunado si es capaz de conseguir una respuesta a una de estas preguntas. Por este ejemplo, el administrador no puede recopilar ninguna información. Un estudio ASA/PIX de los mensajes de Syslog es ideal pero es difícil localizar el problema si el administrador no conoce qué buscar.

Paso 1 - Descubra la dirección IP del usuario

Hay muchas maneras de descubrir la dirección IP del usuario. Este documento está sobre el ASA y el PIX, así que este ejemplo utiliza el ASA y el PIX para descubrir la dirección IP.

El usuario intenta comunicar al ASA/PIX. Esta comunicación puede ser ICMP, Telnet, SSH, o HTTP. El protocolo elegido debe haber limitado la actividad en ASA/PIX. En este ejemplo específico, el usuario hace ping la interfaz interior del ASA.

El administrador necesita configurar uno o más de estas opciones y después tener el usuario hacer ping la interfaz interior del ASA.

- SyslogAseegurese el registro se habilita. El nivel de registro necesita ser fijado **para hacer el debug de**. El registro se puede enviar a las diversas ubicaciones. Este ejemplo utiliza el búfer del registro ASA. Usted puede ser que necesite a un servidor de registro externo en los entornos de producción.`ciscoasa(config)#`**`logging enable`** `ciscoasa(config)#`**`logging buffered debugging`** El usuario hace ping la interfaz interior del ASA (ping 192.168.1.1). Se visualiza esta salida.`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.`*
- **Característica de la captura ASA**El administrador necesita crear una lista de acceso que defina qué tráfico necesita el ASA capturar. Después de que se defina la lista de acceso, el **comando capture** incorpora la lista de acceso y la aplica a una interfaz.`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`** El usuario hace ping la interfaz interior del ASA (ping 192.168.1.1). Se visualiza esta salida.`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.`* **Nota:** Para descargar el capturar archivo a un sistema tal como etéreo, usted puede hacerlo mientras que esta salida muestra.
`!--- Open an Internet Explorer and browse with this https link format:`
`https://[<pix_ip>/<asa_ip>]/capture/<capture name>/pcap` Refiérase ASA/PIX: Paquete que captura usando el CLI y el ejemplo de la Configuración de ASDM para saber más sobre el paquete que captura en el ASA.

- DepurarUtilizan al **comando debug icmp trace** de capturar el tráfico ICMP del usuario.`ciscoasa#`**`debug icmp trace`** El usuario hace ping la interfaz interior del ASA (ping 192.168.1.1). Esta salida se visualiza en la consola.`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.`* Para inhabilitar la **traza ICMP del debug**, utilice uno de estos comandos:**ninguna traza ICMP del debugtraza ICMP del undebugundebug todo**, **Undebug todo**, o la **O.N.U toda**

Cada uno de estas tres opciones ayuda al administrador a determinar la dirección IP de origen. En este ejemplo, la dirección IP de origen del usuario es 192.168.1.50. El administrador está listo para aprender más sobre la aplicación X y para determinar la causa del problema.

Paso 2 - Localice la causa del problema

Referente a la información enumerada en la sección del paso 1 de este documento, el administrador ahora conoce la fuente de una sesión de la aplicación X. El administrador está listo para aprender más sobre la aplicación X y para comenzar a localizar donde los problemas pudieron estar.

ASA/PIX el administrador necesita preparar el ASA por lo menos uno de estas sugerencias mencionadas. Una vez que el administrador está listo, el usuario inicia la aplicación X y limita el resto de la actividad puesto que la actividad adicional del usuario pudo causar la confusión o engañar ASA/PIX al administrador.

- **Mensajes de Syslog del monitor.**Busque para la dirección IP de origen del usuario que usted localizó en el paso 1. El usuario inicia la aplicación X. El administrador ASA publica el **comando show logging** y ve la salida.`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)` Los registros revelan que el IP Address de destino es 172.22.1.1, el protocolo son TCP, el puerto destino es HTTP/80, y que el tráfico está enviado a la interfaz exterior.
- **Modifique los filtros de la captura.**El comando **más inside_test de la lista de acceso** fue utilizado y se utiliza previamente aquí.`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.`* El usuario inicia la aplicación X.

El administrador ASA después publica el comando del **inside_interface de la captura de la demostración** y ve la salida.`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>` El tráfico capturado proporciona al administrador con varios pedazos de información valiosa:Dirección destino — 172.22.1.1Número del puerto — 80/httpProtocolo — TCP (note el “S” o el indicador del syn)Además, el administrador también sabe que el tráfico de datos para la aplicación X llega el ASA.Si la salida había sido esta salida de comando del **inside_interface de la captura de la demostración**, después el tráfico de aplicación o nunca alcanzó el ASA o el filtro de la captura no fue fijado para capturar el tráfico:`ciscoasa#`**`show capture inside_interface`** `0 packet captured 0 packet shown` En este caso, el administrador debe considerar investigar el equipo del usuario y cualquier router u otros dispositivos de red en la trayectoria entre el ordenador del usuario y el ASA.**Nota:** Cuando el tráfico llega una interfaz, el **comando capture** registra los datos antes de que cualquier política de seguridad ASA analice el tráfico. Por ejemplo, una lista de acceso niega todo el tráfico entrante en una interfaz. **El comando capture** todavía registra el tráfico. La política de seguridad ASA entonces analiza el tráfico.
- DepurarEl administrador no es familiar con la aplicación X y por lo tanto no conoce a cuáles de los servicios del debug a habilitar para la investigación de la aplicación X. El debug no pudo ser la mejor opción del troubleshooting en este momento.

Con la información recopilada en el paso 2, el administrador ASA gana varios bits de la información valiosa. El administrador sabe que el tráfico llega la interfaz interior del ASA, de la dirección IP de origen, del IP Address de destino y de las aplicaciones de la aplicación de servicios X (TCP/80). De los Syslog, el administrador también sabe que la comunicación fue permitida inicialmente.

Paso 3 - Confirme y monitoree el tráfico de aplicación

El administrador ASA quiere confirmar que el tráfico de la aplicación X ha salido del ASA así como monitorear cualquier tráfico de retorno del servidor X de la aplicación.

- **Mensajes de Syslog del monitor.**Filtre los mensajes de Syslog para la dirección IP de origen (192.168.1.50) o el IP Address de destino (172.22.1.1). De la línea de comando, los mensajes de Syslog de filtración parecen el **registro de la demostración | incluya 192.168.1.50** o **muestre el registro | incluya 172.22.1.1**. En este ejemplo, utilizan al **comando show logging** sin los filtros. La salida se suprime para hacer la lectura fácil.`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` El mensaje de Syslog indica la conexión cerrada porque del tiempo de espera SYN. Esto dice a administrador que no se recibió ningunas respuestas del servidor X de la aplicación por el ASA. Las razones de la terminación del mensaje de Syslog pueden variar.El tiempo de espera SYN consigue registrado debido a una finalización de la conexión forzada después de 30 segundos que

ocurra después de la realización de la entrada en contacto de tres vías. Este problema ocurre generalmente si el servidor no puede responder a un pedido de conexión, y, en la mayoría de los casos, no se relaciona con la configuración en el PIX/ASA.Para resolver este problema, refiera a esta lista de verificación:Aseegurese el comando static se ingresa correctamente y eso que no solapa con otros comandos static, por ejemplo,`static (inside,outside) x.x.x.x y.y.y.y netmask 255.255.255.255`

El NAT estático en ASA 8.3 y posterior se puede configurar como se muestra aquí:`object network obj-y.y.y.y`
` host y.y.y.y`
` nat (inside,outside) static x.x.x.x`Aseegurese que una lista de acceso existe para permitir el acceso al IP Address global del exterior y que esté limitada a la interfaz:

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

Para una conexión satisfactoria con el servidor, el default gateway en el servidor debe señalar hacia la interfaz DMZ del PIX/ASA.Refiera a los mensajes del sistema ASA para más información sobre los mensajes de Syslog.

- **Cree un nuevo filtro de la captura.**Del tráfico y de mensajes de Syslog capturados anteriores, el administrador sabe que la aplicación X debe dejar el ASA a través de la interfaz exterior.`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`** El usuario necesita iniciar una nueva sesión con la aplicación X. Después de que el usuario haya iniciado una sesión de la nueva aplicación X, el administrador ASA necesita publicar el comando del **outside_interface de la captura de la demostración** en el 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` El tráfico de las demostraciones de la captura que sale de la interfaz exterior pero no muestra ningún tráfico de la contestación del servidor de 172.22.1.1. Esta captura muestra los datos mientras que sale del ASA.
- **Utilice la opción del paquete-trazalíneas.**De las secciones anteriores, el administrador ASA ha aprendido bastante información para utilizar la opción del paquete-**trazalíneas** en el ASA.**Nota:** El ASA soporta el comando del paquete-**trazalíneas** que comienza en la versión 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 salida más importante del comando del paquete-**trazalíneas** es la línea más reciente, que es `acción: permita`.

Las tres opciones en el paso 3 por cada uno muestran a administrador que el ASA no es responsable de los problemas de la aplicación X. El tráfico de la aplicación X sale del ASA y el ASA no recibe una contestación del servidor X de la aplicación.

¿Cuál es siguiente?

Hay muchos componentes que permiten que la aplicación X trabaje correctamente para los usuarios. Los componentes incluyen el equipo del usuario, el cliente de la aplicación X, la encaminamiento, las políticas de acceso, y el servidor X de la aplicación. En el ejemplo anterior, probamos que el ASA recibe y adelante el tráfico de la aplicación X. El servidor y los administradores de la aplicación X deben conseguir implicados ahora. Los administradores deben verificar que los servicios de aplicación se estén ejecutando, revisan ningunos abren una sesión el servidor, y lo verifican que el tráfico del usuario es recibido por el servidor y la aplicación X.

Problema: Terminar el mensaje de error de conexión del TCP-proxy

Recibe este mensaje de error:

```
%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
```

Solución

Explicación: Este presentaciones del mensaje cuando el límite de memoria intermedia de reensamblado se excede durante ensamblar los segmentos TCP.

- *source_address/source_port* - La dirección IP de origen y el puerto de origen del paquete que inicia la conexión.
- *dest_address/dest_port* - El IP Address de destino y el puerto destino del paquete que inicia la conexión.
- *interface_inside* - El nombre de la interfaz en la cual el paquete que inició la conexión llega.
- *interface_outside* - El nombre de la interfaz en la cual el paquete que inició la conexión sale.
- *límite* - El límite configurado de la conexión embrionaria para la clase de tráfico.

La resolución para este problema es inhabilitar el examen RTSP en el dispositivo de seguridad como se muestra.

```
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
```

Refiera al Id. de bug Cisco CSCsl15229 (clientes registrados solamente) para más detalles.

Problema: "%ASA-6-110003: El rutear no podido para localizar el Next-Hop para el protocolo mensaje de error de la interfaz del src"

El ASA cae el tráfico con el `error:%ASA-6-110003: El rutear no podido para localizar el Next-Hop para el protocolo del src interconecta: puerto del src IP/src a la interfaz dest:` mensaje de `error de puerto dest IP/dest.`

Solución

Este error ocurre cuando los intentos ASA para encontrar el salto siguiente en una tabla de ruteo de la interfaz. Típicamente, se recibe este mensaje cuando el ASA tiene una traducción (xlate) construida a una interfaz y a una ruta que señala una diversa interfaz. Comprobación para un misconfiguration en las sentencias NAT. La resolución del misconfiguration puede resolver el error.

Problema: Conexión bloqueada por el ASA con el "%ASA-5-305013: Reglas asimétricas NAT correspondidas con para mensaje de error delantero y de los flujos inversos el"

La conexión es bloqueada por el ASA, y se recibe este mensaje de error:

```
%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.
```

Solución

Cuando se realiza el NAT, el ASA también intenta invertir el paquete y marca si éste golpea cualquier traducción. Si no golpea ningunos o una diversa traducción de NAT, después hay una discordancía. Usted ve lo más comúnmente posible este mensaje de error cuando hay diversas reglas NAT configuradas para saliente y el tráfico entrante con la misma fuente y destino. Marque la sentencia NAT para el tráfico en cuestión.

Problema: Reciba el error - %ASA-5-321001: Límite del "conns" del recurso de 10000 alcanzados para el sistema

Solución

Este error significa que las conexiones para un servidor situado a través de un ASA han alcanzado su límite máximo. Ésta podía ser una indicación de un ataque DOS a un servidor en su red. Utilice el MPF en el ASA y reduzca el límite de las conexiones embrionarias. También, habilite la detección muerta de la conexión (DCD). Refiera a estos fragmentos de la configuración:

```
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
```

Problema: Reciba el error %PIX-1-106021: Niegue el control del trayecto inverso TCP/UDP del src_addr al dest_addr en el int_name de la interfaz

Solución

Se recibe este mensaje del registro cuando se habilita el control del trayecto inverso. Publique este comando para resolver el problema y inhabilitar el control del trayecto inverso:

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

Problema: Interrupción de la conectividad a Internet debido a la detección de la amenaza

Este mensaje de error se recibe en el ASA:

```
%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
```

Solución

Este mensaje es generado por la detección de la amenaza debido a la configuración predeterminada cuando se detecta una conducta de tráfico anómala. El mensaje se centra en Miralix Licen 3000 que sea un puerto TCP/UDP. Localice el dispositivo que está utilizando el puerto 3000. Compruebe las estadísticas gráficas del ASDM para la detección de la amenaza y verifique los ataques superiores para ver si muestra el puerto 3000 y la dirección IP de origen. Si es un dispositivo legítimo, usted puede incrementar la tarifa básica de la detección de la amenaza en el ASA para resolver este mensaje de error.

Información Relacionada

- Referencia de comandos de Cisco ASA
- Referencia de comandos del Cisco PIX

- Mensajes de error y de sistema de Cisco ASA
- Mensajes de error y de sistema del Cisco PIX
- Soporte del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Soporte del Cisco PIX 500 Series Security Appliances
- Soporte Técnico y Documentación - Cisco Systems