ASA 8.3 y posterior: Problemas de rendimiento del monitor y del Troubleshooting

Contenido

Introducción

Este documento proporciona la información sobre el ASA ordena que usted puede utilizar para monitorear y para resolver problemas el funcionamiento de un dispositivo de seguridad adaptante de Cisco (ASA).

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en un dispositivo de seguridad adaptante de Cisco (ASA) esa versión 8.3 y posterior de los funcionamientos.

La información que se presenta en este documento se originó a partir de dispositivos dentro de 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 un comando antes de ejecutarlo.

Convenciones

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

Troubleshooting

Para resolver problemas de funcionamiento, verifique las áreas básicas descritas en esta sección.

Nota: Si usted tiene la salida del **comando show de** su dispositivo de Cisco, usted puede utilizar el analizador del CLI de Cisco (clientes registrados solamente) para visualizar los problemas potenciales y los arreglos. Los ciertos comandos show de los soportes de analizador del CLI de Cisco. Si usted utiliza el analizador del CLI de Cisco, usted debe ser un cliente registrado, usted debe ser abierto una sesión a su cuenta de Cisco, y usted debe tener Javascript habilitado dentro de su navegador.

Configuración de velocidad y dúplex

El dispositivo de seguridad se configura previamente para detectar automáticamente las configuraciones de velocidad y dúplex en una interfaz. Sin embargo, hay varias situaciones que pueden hacer que el proceso de negociación automática falle, lo que provoca discordancias dúplex (y problemas de funcionamiento). Para la infraestructura de red de misión crítica, Cisco codifica manualmente la velocidad y el dúplex en cada interfaz para que no haya posibilidad de error. Estos dispositivos por lo general no se mueven, de manera que si los configura correctamente, no es necesario cambiarlos.

En cualquier dispositivo de red, la velocidad del link puede ser detectada, pero el dúplex debe ser negociado. Si dos dispositivos de red se configuran para autonegociar la velocidad y el dúplex, intercambian las tramas (llamadas Pulsos de Links Rápidos, o FLP) que anuncian sus capacidades de velocidad y dúplex. Para un link partner que no está al tanto (de la autonegociación), estos pulsos son similares a tramas regulares de 10 Mbps. Para un link partner que puede decodificar los pulsos, los FLPs contienen todas las configuraciones de velocidad y dúplex que el link partner puede proporcionar. La estación que recibe los FLPs reconoce las tramas, y los dispositivos acuerdan mutuamente las configuraciones más altas de velocidad y dúplex que cada uno puede alcanzar. Si un dispositivo no soporta la autonegociación, el otro dispositivo recibe los FLPs y las transiciones al modo de detección paralela. Para detectar la velocidad del socio, el dispositivo escucha la longitud de los pulsos, y luego configura la velocidad en consecuencia. El problema surge con la configuración dúplex. Porque el duplex debe ser negociado, el dispositivo que se fija para autonegociar no puede determinar las configuraciones en el otro dispositivo, así que lo omite semidúplex, como se afirma en el estándar de IEEE 802.3u.

Por ejemplo, si usted configura la interfaz ASA para el autonegotiation y la conecta con un Switch que esté puesto en hard-code para el 100 Mbps y el FULL-duplex, el ASA envía los FLP. Sin embargo, el switch no responde porque es codificado para la velocidad y el dúplex y no participa en la autonegociación. Porque no recibe ninguna respuesta del Switch, las transiciones ASA en el modo de detección paralela y detectan la longitud de los pulsos en las tramas que el Switch envía. Es decir, el ASA detecta que el Switch está fijado al 100 Mbps, así que fija la velocidad de la interfaz por consiguiente. Sin embargo, porque el Switch no intercambia los FLP, el ASA no puede detectar si el Switch puede funcionar con el FULL-duplex, así que el ASA fija el duplex de

la interfaz a semidúplex, como se afirma en el estándar de IEEE 803.2u. Porque el Switch está puesto en hard-code al 100 Mbps y al FULL-duplex, y el ASA acaba de autonegociar al 100 Mbps y semidúplex (como debe), el resultado es una discordancia dúplex que puede causar los problemas graves de rendimiento.

Se revela una velocidad o una discordancia dúplex con mayor frecuencia cuando los contadores de errores en las interfaces en cuestión aumentan. La mayoría de los errores comunes son trama, verificaciones por redundancia cíclica (CRC), y runts. Si estos valores se incrementan en su interfaz, se produce una discrepancia de dúplex/velocidad o un problema de cableado. Debe resolver este problema antes de continuar.

Ejemplo:

```
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
 Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
       Input flow control is unsupported, output flow control is unsupported
       MAC address 0013.c480.b2b8, MTU 1500
       IP address 192.168.17.4, subnet mask 255.255.255.0
       311981 packets input, 20497296 bytes, 0 no buffer
       Received 311981 broadcasts, 157 runts, 0 giants
       379 input errors, 107 CRC, 273 frame, 0 overrun, 0 ignored, 0 abort
       0 pause input, 0 resume input
       0 L2 decode drops
       121 packets output, 7744 bytes, 0 underruns
       0 pause output, 0 resume output
       0 output errors, 0 collisions, 1 interface resets
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops, 0 tx hangs
       input queue (blocks free curr/low): hardware (255/249)
       output queue (blocks free curr/low): hardware (255/254)
```

Uso de CPU

Si usted notó la utilización de la CPU es alta, completa estos pasos para resolver problemas:

1. Verifique que el recuento de conexiones en el conteo **show xlate** sea bajo.
2. Verifique que el bloque de memoria sea normal.
3. Verifique que el número de ACL sea más alto.
4. Publique el comando del **Detalle de la memoria de la demostración**, y verifiquelo que la

memoria usada por el ASA es uso normal.

5. Verifique que los conteos en **show processes cpu-hog** y **show processes memory** sean normales.

6. Ningún host presente dentro o fuera del dispositivo de seguridad puede generar el tráfico malintencionado o total que puede ser un tráfico multicast/broadcast y provocar el uso elevado de la CPU. Para resolver este problema, configure una lista de acceso para negar el tráfico entre los hosts (de principio a fin) y verifique el uso.

7. Marque el duplex y las configuraciones de la velocidad en las interfaces ASA. La configuración de discordancia con las interfaces remotas puede aumentar el uso de CPU.

   Este ejemplo muestra el número más elevado en el *error de entrada* y se *satura* debido a la discordancia de velocidad. Utilice el **comando show interface** para verificar los errores:

```
Ciscoasa#sh int GigabitEthernet0/1
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
 Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
       Input flow control is unsupported, output flow control is unsupported
       MAC address 0013.c480.b2b8, MTU 1500
       IP address 192.168.17.4, subnet mask 255.255.255.0
       311981 packets input, 20497296 bytes, 0 no buffer
       Received 311981 broadcasts, 157 runts, 0 giants
       7186 input errors, 0 CRC, 0 frame, 7186 overrun, 0 ignored, 0 abort
       0 pause input, 0 resume input
       0 L2 decode drops
       121 packets output, 7744 bytes, 0 underruns
       0 pause output, 0 resume output
       0 output errors, 0 collisions, 1 interface resets
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops, 0 tx hangs
       input queue (blocks free curr/low): hardware (255/249)
       output queue (blocks free curr/low): hardware (255/254)
```

   Para resolver este problema, configure la velocidad como *automática a la* interfaz correspondiente.

   Nota: Cisco recomienda que habilite el comando **ip verify reverse-path interface** en todas las interfaces ya que descartará paquetes que no tienen una dirección de origen válida y, por lo tanto, reduce el uso de la CPU. Esto se aplica al FWSM que hace frente CPU elevada a los problemas.

8. Otro motivo del uso de CPU elevado puede ser la existencia de demasiadas rutas multicast. Publique el comando de la **ruta multicast de la demostración** para marcar si el ASA recibe demasiadas rutas de Multicast.

9. Utilice el **comando show local-host** para ver si la red experimenta un ataque de negación de servicio, que puede indicar un ataque de virus en la red.

10. CPU elevada pudo ocurrir debido al Id. de bug Cisco CSCsq48636. Refiera al Id. de bug Cisco CSCsq48636 (clientes registrados solamente) para más información.

Nota: Si la solución proporcionó arriba no resuelve el problema, actualiza la plataforma ASA según los requisitos. Refiera a la hoja de datos del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 para más información sobre las capacidades y las capacidades adaptantes de la plataforma del dispositivo de seguridad. Entre en contacto TAC (clientes registrados solamente) para más información.

Uso de Memoria Intensivo

Las siguientes son algunas posibles causas y resoluciones para el uso de memoria intensivo:

- **Registro de evento:** El registro de evento puede consumir una gran cantidad de memoria. Para resolver este problema, instale y registre todos los eventos a un servidor externo, tal como un servidor syslog.
- **Pérdida de Memoria:** Un problema conocido en el software del dispositivo de seguridad puede resultar en un consumo alto de memoria. Para resolver este problema, actualice el software del dispositivo de seguridad.
- **Debugging Habilitado:** El debugging puede consumir una gran cantidad de memoria. Para resolver este problema, inhabilite el debugging con el comando undebug all.
- **Puertos de Bloqueo:** Los puertos de bloqueo en la interfaz externa de un dispositivo de seguridad hacen que el dispositivo de seguridad consuma gran cantidad de memoria para bloquear los paquetes a través de los puertos especificados. Para resolver este problema, bloquee el tráfico defectuoso en el extremo de ISP.
- **Amenaza-detección:** La característica de la detección de la amenaza consiste en diversos niveles de estadísticas que recolectan diversas amenazas, y escanean la detección de amenazas, que determina cuando un host realiza un escaneo. **Apague** esta característica para consumir menos memoria.

PortFast, Canalización y Trunking

De forma predeterminada, muchos switches, tales como los switches Cisco que ejecutan el sistema operativo Catalyst (OS), están diseñados para ser dispositivos listos para el uso. Como tal, muchos de los parámetros del puerto predeterminado no son deseables cuando un ASA está conectado en el Switch. Por ejemplo, en un switch que ejecuta Catalyst OS, la canalización predeterminada se configura en al Automática, y PortFast se inhabilita. Si usted conecta un ASA con un Switch que funcione con el Catalyst OS, inhabilite la canalización, inhabilite el enlace, y habilite PortFast.

La canalización, también conocida como Fast EtherChannel o EtherChannel de Giga, se utiliza para vincular dos o más puertos físicos en un grupo lógico con el fin de aumentar el rendimiento de procesamiento general a través del link. Cuando un puerto se configura para la canalización automática, envía las tramas del Port Aggregation Protocol (PAgP) mientras que el link se vuelve activo para determinar si es parte de un canal. Estas tramas pueden causar problemas si el otro dispositivo intenta autonegociar la velocidad y dúplex del link. Si la canalización en el puerto se configura en Automática, también provoca una demora adicional de cerca de 3 segundos antes de que el puerto comience a reenviar tráfico después de que el link se active.

> Nota: En los Catalyst XL Series Switches, la canalización no se configura en Automática de forma predeterminada. Por este motivo, usted debe inhabilitar la canalización en cualquier puerto del switch que conecte con un ASA.

El trunking, también conocido por los protocolos de trunking comunes Inter-Switch Link (ISL) o Dot1q, combina varias LANs virtuales (VLANs) en un puerto único (o link). La conexión troncal se usa normalmente entre dos switches cuando ambos tienen más de una VLAN definida. Cuando un puerto se configura para el trunking automático, envía las tramas del Dynamic Trunking Protocol (DTP) mientras que el link sube para determinar si el puerto con el que se conecta desea conectarse mediante trunking. Estas tramas DTP pueden provocar problemas con la negociación automática del link. Si el trunking se configura en Automático en un puerto del switch, agrega una demora adicional de cerca de 15 segundos antes de que el puerto comience a reenviar tráfico después de que el link se active.

PortFast, también conocido como Fast Start, es una opción que informa al switch que un dispositivo de la Capa 3 está conectado fuera de un puerto del switch. El puerto no espera los 30 segundos predeterminados (15 segundos para escuchar y 15 segundos para aprender); en cambio, esta acción hace que el switch coloque al puerto en el estado de reenvío inmediatamente después que el link se inicie. Es importante comprender que cuando habilita PortFast, el spanning tree no se inhabilita. El Spanning tree todavía está activo en ese puerto. Cuando habilita PortFast, se informa al switch solamente que no hay otro switch o hub (dispositivo de capa 2 solamente) conectado en el otro extremo del link. El switch elimina la demora normal de 30 segundos mientras intenta determinar si surge un loop de Capa 2 al activarse ese puerto. Una vez activado el link, todavía participa en el spanning tree. El puerto envía las unidades de datos de paquetes de bridge (BPDU), y el switch todavía escucha las BPDUs en ese puerto. Por estas razones, se recomienda que usted habilita PortFast en cualquier puerto del switch que conecte con un ASA.

> Nota: Catalyst OS releases 5.4 y posterior incluyen el comando **set port host <mod>/<port>** que le permite utilizar un solo comando para inhabilitar la canalización, inhabilitar trunking, y habilitar PortFast.

traducción de Dirección de Red (NAT)

A cada NAT o sesión de Sobrecarga NAT (PAT) se le asigna una ranura de traducción conocida como *xlate*. Estas xlates pueden persistir incluso después de realizar cambios a las reglas de NAT que las afectan. Esto puede llevar a un agotamiento de las ranuras de traducción o a una conducta inesperada, o a ambas por el tráfico que experimenta la traducción. Esta sección explica cómo ver y borrar las xlates en el dispositivo de seguridad.

> Precaución: Una interrupción momentánea del flujo de todo el tráfico a través del dispositivo puede ocurrir cuando usted los xlates global claros en el dispositivo de seguridad.

Muestree la configuración ASA para la PALMADITA que utiliza la dirección IP de la interfaz exterior:

```
Ciscoasa#sh int GigabitEthernet0/1
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
 Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
       Input flow control is unsupported, output flow control is unsupported
       MAC address 0013.c480.b2b8, MTU 1500
       IP address 192.168.17.4, subnet mask 255.255.255.0
       311981 packets input, 20497296 bytes, 0 no buffer
       Received 311981 broadcasts, 157 runts, 0 giants
       7186 input errors, 0 CRC, 0 frame, 7186 overrun, 0 ignored, 0 abort
       0 pause input, 0 resume input
       0 L2 decode drops
       121 packets output, 7744 bytes, 0 underruns
       0 pause output, 0 resume output
       0 output errors, 0 collisions, 1 interface resets
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops, 0 tx hangs
       input queue (blocks free curr/low): hardware (255/249)
       output queue (blocks free curr/low): hardware (255/254)
```

El tráfico que fluye a través del dispositivo de seguridad por lo general se somete a NAT. Para ver las traducciones que funcionan en el dispositivo de seguridad, ejecute el **comando show xlate**:

```
Ciscoasa#show xlate

5 in use, 5 most used

Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice

NAT from any:192.168.1.10 to any:172.16.1.1/24
```

```
    flags s idle 277:05:26 timeout 0:00:00
```

Las ranuras de traducción pueden persistir después de que se realicen los cambios clave. Para borrar las ranuras de la traducción actual en el dispositivo de seguridad, ejecute el **comando clear xlate**:

```
Ciscoasa#clear xlate
```

```
Ciscoasa#show xlate
0 in use, 1 most used
```

El comando clear xlate borra toda la traducción dinámica actual de la tabla xlate. Para borrar una traducción determinada de IP, puede utilizar el **comando clear xlate** con la palabra clave **global [ip address]**.

Aquí está una configuración de la muestra ASA para el NAT:

```
Ciscoasa#show xlate
0 in use, 1 most used
```

Observe el resultado **show xlate** para la traducción para la dirección 10.2.2.2 interna a la dirección externa global 10.10.10.10:

```
Ciscoasa#show xlate
2 in use, 2 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T -
twice
TCP PAT from inside:10.2.2.2/1429 to any:10.10.10.10/64768 flags ri
idle 62:33:57 timeout 0:00:30
TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri
idle 62:33:57 timeout 0:00:30
```

Borre la traducción para la dirección IP global de 10.10.10.10:

```
Ciscoasa# clear xlate global 10.10.10.10
```

En este ejemplo, desaparece la traducción para la dirección 10.2.2.2 interna a la dirección externa global 10.10.10.10:

```
Ciscoasa#show xlate
1 in use, 2 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T -
twice
TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri
idle 62:33:57 timeout 0:00:30
```

Registros del sistema

Los Syslog permiten que usted resuelva problemas los problemas en el ASA. Cisco ofrece a un servidor de Syslog libre para el Windows NT llamado el servidor de Syslog del Firewall ASA (PFSS). Puede descargar el PFSS de la página Descargas de Software (sólo clientes registrados).

Otros vendedores, tales como Kiwis Enterprises , ofrecen los servidores de syslog para las diversas plataformas de Windows, como Windows 2000 y Windows XP. La mayoría de los equipos UNIX y Linux tienen servidores syslog instalados de forma predeterminada.

Cuando usted configura al servidor de Syslog, configure el ASA para enviarle los registros.

Por ejemplo:

```
logging on
logging host <ip_address_of_syslog_server> logging trap debugging
```

> Nota: Este ejemplo configura el ASA para enviar el debugging (nivel 7) y más registros críticos del sistema al servidor de Syslog. Porque estos registros ASA son los más prolijos, utilícelos solamente cuando usted resuelve problemas un problema. Para obtener un funcionamiento normal, configure el nivel de registro a Advertencia (nivel 4) o Error (nivel 3).

Si tiene un problema con el funcionamiento lento, abra el syslog en un archivo de texto y busque la dirección IP de origen asociada al problema de funcionamiento. (Si utiliza UNIX, puede buscar cadenas (grep) con el syslog para la dirección IP de origen). Marque para saber si hay mensajes que indiquen al servidor externo intentado para acceder al IP Address interno en el puerto TCP 113 (para el protocolo de identificación, o la identificación), pero el ASA negó el paquete. El mensaje debe ser similar a este ejemplo:

```
logging on
logging host <ip_address_of_syslog_server> logging trap debugging
```

Si usted recibe este mensaje, publique el comando service resetinbound al ASA. El ASA no cae silenciosamente los paquetes; en lugar, este comando hace el ASA reajustar inmediatamente cualquier conexión hacia adentro que sea negada por la política de seguridad. El servidor no espera el paquete del Identificador para interrumpir su conexión TCP; en su lugar, recibe inmediatamente un paquete de restablecimiento.

SNMP

Monitorear el funcionamiento de Cisco ASA usando el SNMP es el método recomendado para los despliegues en empresas. Cisco ASA apoya el Monitoreo de red con las versiones de SNMP 1, 2c y 3.

Usted puede configurar el dispositivo de seguridad para enviar los desvíos a un Network Management Server (NMS), o usted puede utilizar el NMS para hojear el MIB en el dispositivo de seguridad. El MIB es una colección de definiciones, y el dispositivo de seguridad mantiene una base de datos de los valores para cada definición. Para más información sobre esto, refiera a configurar el SNMP en Cisco ASA.

Todo el MIB soportado para Cisco ASA se puede encontrar en la lista de soporte MIB ASA. De esta lista, este MIB es útil para la supervisión de rendimiento:

- CISCO-FIREWALL-MIB ---- Contiene los objetos útiles para la Conmutación por falla
- CISCO-PROCESS-MIB ---- Contiene los objetos útiles para la utilización de la CPU
- CISCO-MEMORY-POOL-MIB ---- Contiene los objetos útiles para los objetos de la memoria.

Búsquedas de DNS inverso

Si usted experimenta el rendimiento lento con el ASA, verifique que usted tenga expedientes del puntero del Sistema de nombres de dominio (DNS) (PTR DNS), también conocidos como expedientes de la búsqueda de DNS reversible, en el servidor DNS autoritario para las

direcciones externas que el ASA utiliza. Esto incluye cualquier direccionamiento en su pool de la traducción de dirección de red global (NAT) (o la interfaz exterior ASA si usted sobrecarga en la interfaz), cualquier dirección estática, y dirección interna (si usted no utiliza el NAT con ellos). Algunas aplicaciones, tales como File Transfer Protocol (FTP) y servidores Telnet, pueden utilizar las búsquedas de DNS inversas para determinar de dónde proviene el usuario y si es un host válido. Si la búsqueda de DNS inversa no se resuelve, el funcionamiento se degrada ya que se interrumpe la solicitud.

Para asegurarse de que un registro PTR exista para estos hosts, ejecute el **comando nslookup de** su equipo o máquina UNIX; incluya la dirección IP global que utiliza para conectar con Internet.

Ejemplo:

```
% nslookup 198.133.219.25
25.219.133.198.in-addr.arpa     name = www.cisco.com.
```

Debe recibir una respuesta con el nombre DNS del dispositivo asignado a esa dirección IP. Si no recibe una respuesta, comuníquese con la persona que controla sus DNS para pedir la adición de registros PTR para cada una de sus direcciones IP globales.

Sobrantes en la interfaz

Si usted tiene una ráfaga de tráfico, los paquetes perdidos pueden ocurrir si la explosión excede la capacidad que mitiga de memoria intermedia primero en entrar, primero en salir en el NIC y los buffers del anillo de recepción. Habilitar las tramas de pausa para el control de flujo puede paliar este problema. La pausa (XOFF) y las tramas XON son generadas automáticamente por el NIC basado en hardware en el uso de memoria intermedia primero en entrar, primero en salir. Se envía una trama de pausa cuando el uso de búfer excede la marca de alta. Para habilitar las tramas de la pausa (XOFF) para el control de flujo, utilice este comando:

```
hostname(config)#interface tengigabitethernet 1/0

hostname(config-if)#
flowcontrol send on
```

Refiera a habilitar la interfaz física y a configurar los parámetros de los Ethernetes para más información.

Comandos show

show cpu usage

Utilizan al **comando show cpu usage** de determinar la carga de tráfico puesta en el ASA CPU. Durante tráfico máximo, sobrecargas de red o ataques, puede producirse un pico en el uso de CPU.

El ASA tiene una CPU única para procesar una variedad de tareas; por ejemplo, procesa los paquetes e imprime los mensajes de debug en la consola. Cada proceso tiene su propio propósito, y algunos procesos requieren más tiempo de uso de CPU que otros procesos. El cifrado es probablemente lo más proceso que exige a la CPU posible, así que si su ASA pasa mucho tráfico a través de los túneles encriptados, usted debe considerar un ASA más rápido, un concentrador VPN dedicado, tal como el VPN 3000. El VAC descarga el cifrado y el desciframiento del ASA CPU y lo realiza en hardware en el indicador luminoso LED amarillo de la placa muestra gravedad menor. Esto permite que el ASA cifre y desencripte el 100 Mbps del tráfico con 3DES (cifrado del 168-bit).

Registrarse es otro proceso que puede consumir enormes cantidades de recursos del sistema. Debido a esto, se recomienda que usted inhabilita la consola, el monitor, y el buffer abriendo una sesión el ASA. Puede habilitar estos procesos al resolver un problema, pero debe inhabilitarlos para el funcionamiento diario, especialmente si se queda sin capacidad de CPU. También se sugiere que syslogging o el registro Simple Network Management Protocol (SNMP) (historial de registro) deben configurarse al nivel 5 (Notificación) o inferior. Además, puede inhabilitar las IDs específicas de syslog message con el **comando no logging message <syslog_id>**.

El Cisco Adaptive Security Device Manager (ASDM) también proporciona un gráfico en la lengueta de la supervisión que permite que usted vea el USO de la CPU del ASA en un cierto plazo. Usted puede utilizar este gráfico para determinar la carga en su ASA.

El comando show cpu usage puede utilizarse para mostrar las estadísticas de uso de la CPU.

Ejemplo:

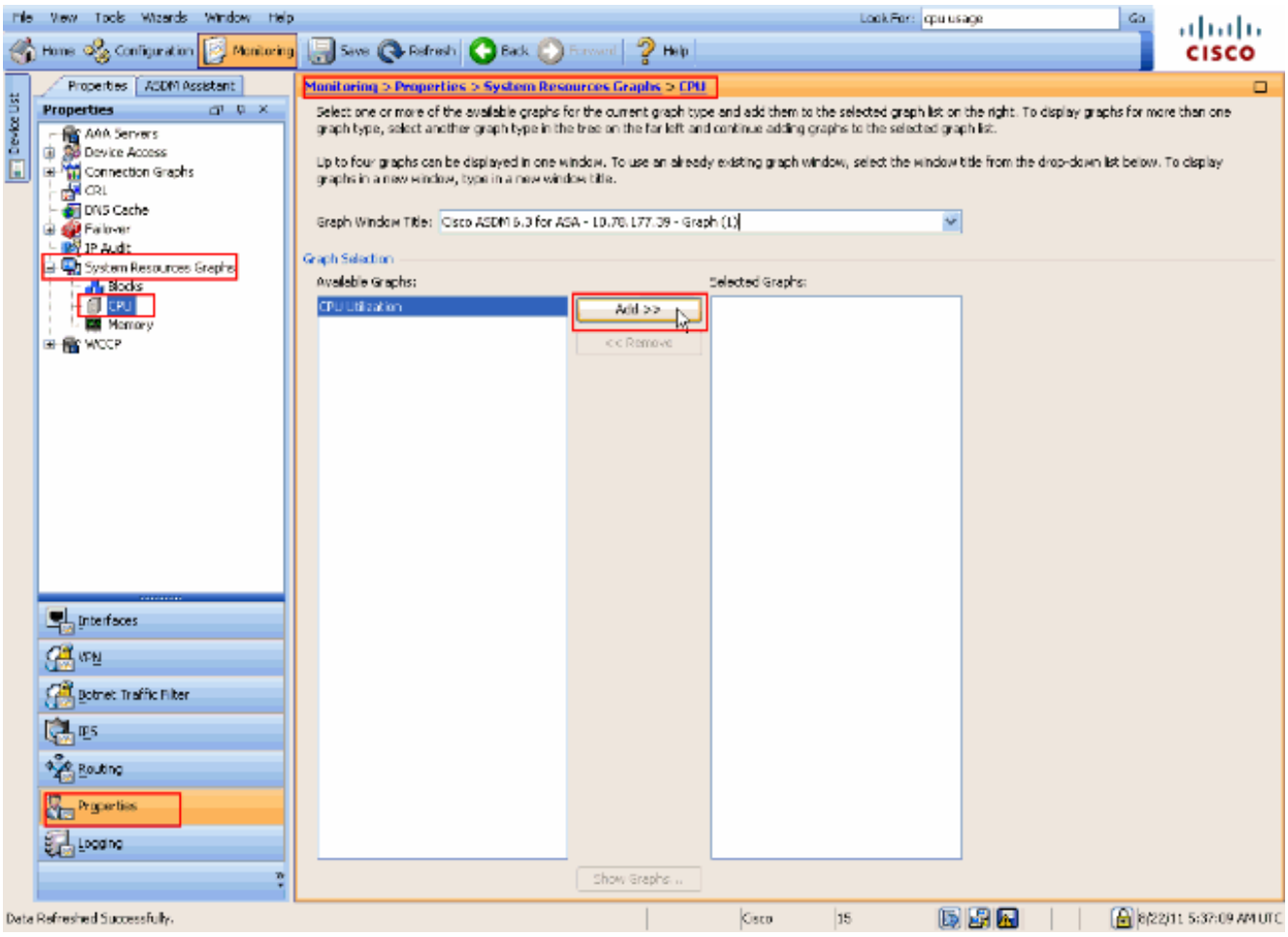
```
Ciscoasa#show cpu usage
```

```
CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

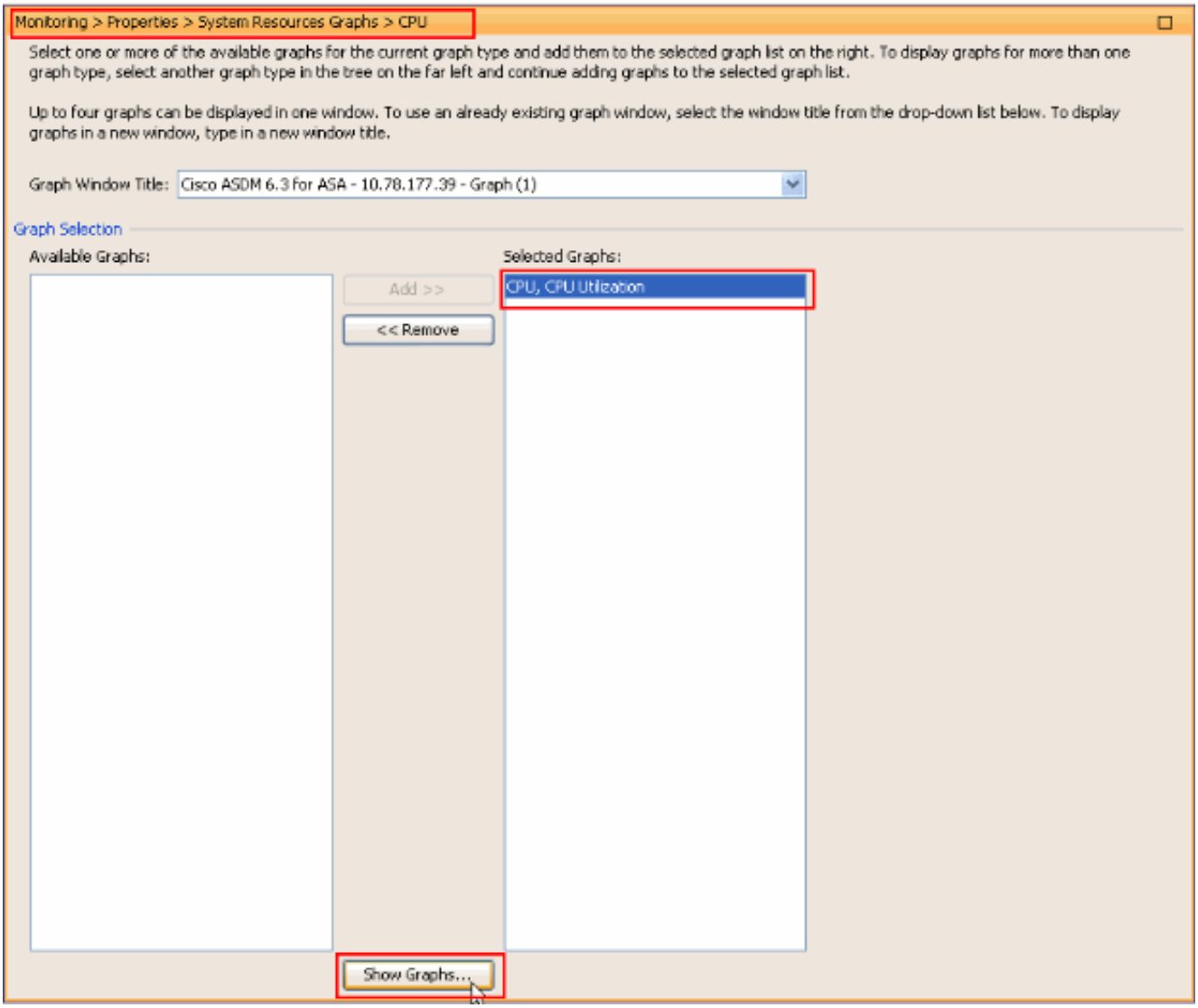
Ver el USO de la CPU en el ASDM

Complete estos pasos para ver el USO de la CPU en el ASDM:

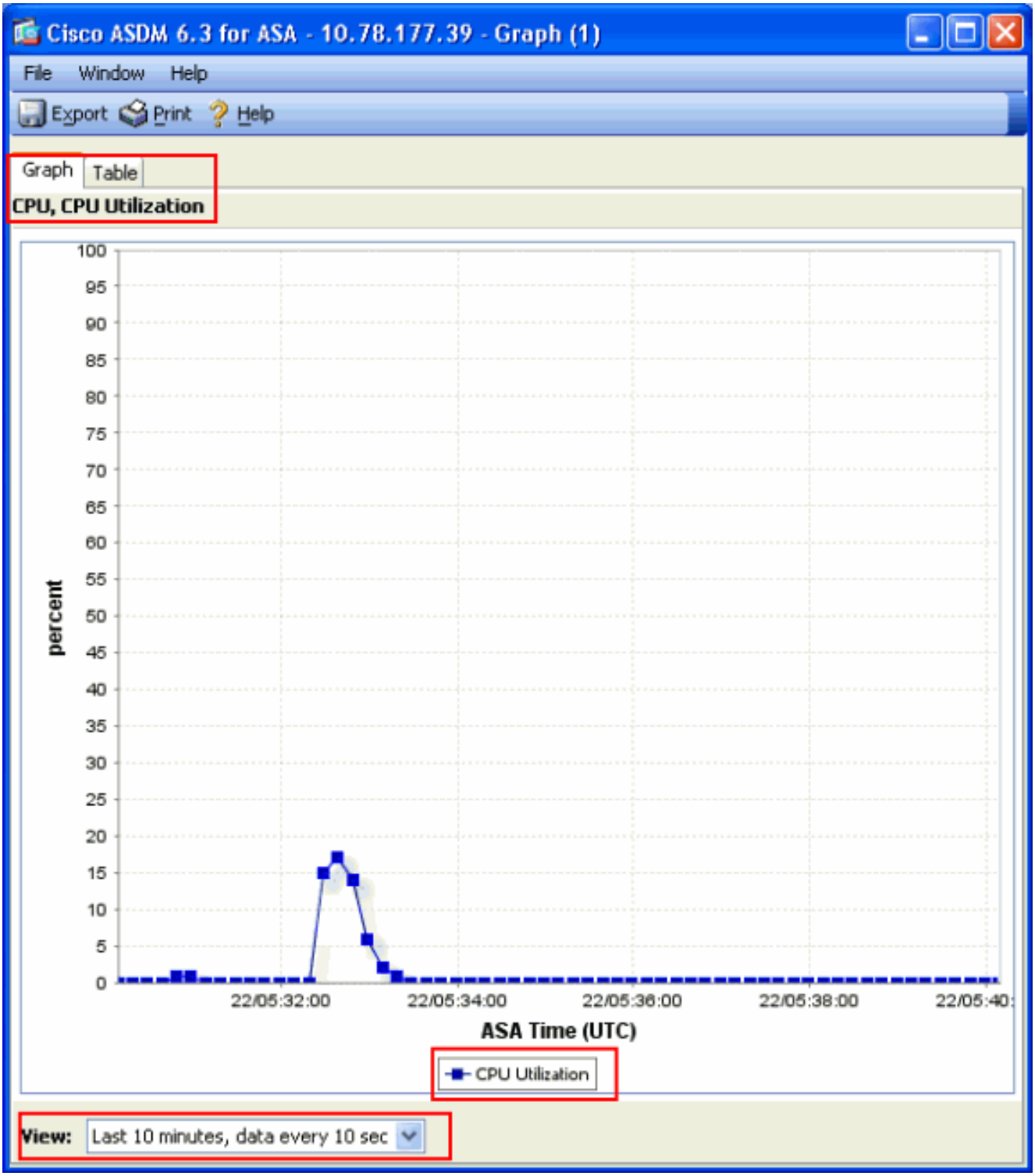
1. Van a **monitorear > las propiedades > los gráficos de los recursos del sistema > el CPU** en el ASDM y eligen el **título de la ventana del gráfico**. Entonces, elija los gráficos requeridos de la lista de **gráficos disponibles** y el tecleo **agrega** como se muestra.



2. Una vez que el nombre requerido del gráfico se agrega bajo **gráficos seleccionados** seccione, haga clic los **gráficos de la demostración**.



La imagen siguiente muestra el gráfico del **USO de la CPU** en el ASDM. Las distintas vistas de este gráfico están disponibles y pueden ser cambiadas seleccionando la visión de la lista desplegable de la visión. Esta salida se puede imprimir o guardar al ordenador como sea necesario.



Descripción del Resultado

Esta tabla describe los campos en el resultado de **show cpu usage**.

Campo	Descripción
Uso de CPU por 5 segundos	Uso de CPU durante los últimos cinco segundos
1 minuto	Promedio de muestras de 5 segundos de utilización de la CPU durante el último

5 minutos	minuto Promedio de muestras de 5 segundos de la utilización de la CPU durante los últ cinco minutos

show traffic

El comando show traffic muestra cuánto tráfico que pasa con el ASA durante un período de tiempo dado. Los resultados se basan en los intervalos de tiempo desde la última vez que se ejecutó el comando.. Para los resultados precisos, ejecute el **comando clear traffic** primero y en luego espere 1 a 10 minutos antes de ejecutar el **comando show traffic**. También ejecute el **comando show traffic** y espere 1 a 10 minutos antes de ejecutar el comando otra vez, pero solamente el resultado de la segunda instancia es válido.

Usted puede utilizar el **comando show traffic** para determinar cuánto pasa el tráfico con su ASA. Si tiene interfaces múltiples, el comando puede ayudarlo a determinar qué interfaces envían y reciben la mayoría de los datos. Para los dispositivos ASA con dos interfaces, la suma del tráfico entrante y saliente en la interfaz exterior debe igualar la suma del tráfico entrante y saliente en la interfaz interior.

Ejemplo:

```
Ciscoasa#show traffic
outside:
        received (in 124.650 secs):
                295468 packets  167218253 bytes
                2370 pkts/sec   1341502 bytes/sec
        transmitted (in 124.650 secs):
                260901 packets  120467981 bytes
                2093 pkts/sec   966449 bytes/sec
inside:
        received (in 124.650 secs):
                261478 packets  120145678 bytes
                2097 pkts/sec   963864 bytes/sec
        transmitted (in 124.650 secs):
                294649 packets  167380042 bytes
                2363 pkts/sec   1342800 bytes/sec
```

Si se aproxima o alcanza el rendimiento nominal en una de sus interfaces, debe actualizar a una interfaz más rápida o limitar la cantidad de tráfico que entra o sale de esa interfaz. Si no lo hace, pueden producirse descartes de paquetes. Como se explica en la sección show interface , puede examinar los contadores de interfaz con el fin de obtener información acerca del rendimiento.

show perform

Utilizan al comando show perfmon de monitorear la cantidad y los tipos de tráfico que el ASA examina. Este comando es la única manera de determinar el número de traducciones (xlates) y de conexiones (conn) por segundo. Las conexiones se vuelven a dividir en conexiones TCP y de protocolo de datagrama de usuario (UDP). Consulte Descripción de Resultados para obtener las descripciones del resultado que este comando genera.

Ejemplo:

```
Ciscoasa#show traffic
outside:
        received (in 124.650 secs):
                295468 packets  167218253 bytes
                2370 pkts/sec   1341502 bytes/sec
        transmitted (in 124.650 secs):
                260901 packets  120467981 bytes
                2093 pkts/sec   966449 bytes/sec
inside:
        received (in 124.650 secs):
                261478 packets  120145678 bytes
                2097 pkts/sec   963864 bytes/sec
        transmitted (in 124.650 secs):
                294649 packets  167380042 bytes
                2363 pkts/sec   1342800 bytes/sec
```

Descripción del Resultado

Esta tabla describe los campos en el resultado **show perfmon** .

Campo	Descripción
Xlates	Traducciones construidas por segundo
Conexiones	Conexiones que se establecen por segundo
TCP Conns	Conexiones TCP por segundo
UDP Conns	Conexiones UDB por segundo
URL Access	URL (sitios web) a los que se accede por segundo
URL Server Req	Las solicitudes enviadas a Websense y al N2H2 por segundo (requiere el comando **filter**)
TCP Fixup	Número de paquetes TCP que el ASA adelante por segundo
TCPIntercept	Cantidad de paquetes SYN por segundo que han excedido el límite embrionario establecid una sentencia estática
HTTP Fixup	Cantidad de paquetes destinados al puerto 80 por segundo (requiere el **comando fixup pro http**)
FTP Fixup	Comandos FTP inspeccionados por segundo

AAA Authen	Solicitudes de autenticación por segundo
AAA Autor	Pedidos de autorización por segundo
AAA Account	Solicitud de cuentas por segundo.

show blocks

Junto con el comando show cpu usage, usted puede utilizar el comando show blocks para determinar si el ASA está sobrecargado.

Bloques de procesamiento de paquetes (1550 y 16384 bytes)

Cuando entra en la interfaz ASA, un paquete se coloca en la cola de la interfaz de entrada, se pasa hasta el OS, y se coloca en un bloque. Para los paquetes Ethernet, se utilizan los bloques 1550 bytes; si el paquete viene dentro en una tarjeta Gigabit Ethernet de 66 MHz, se utilizan los bloques de 16384 bytes. El ASA determina si el paquete está permitido o negado sobre la base del Algoritmo de seguridad adaptable (ASA) y procesa el paquete a través a la cola de salida en la interfaz de salida. Si el ASA no puede soportar la carga de tráfico, el número de 1550-byte disponible bloquea (o los bloques 16384-byte para 66 MHz GE) las libraciones cerca de 0 (tal y como se muestra en de la columna CNT de la salida de comando). Cuando la columna CNT golpea cero, el ASA intenta afectar un aparato más bloques, hasta un máximo de 8192. Si no más de bloques están disponibles, el ASA cae el paquete.

Bloques de conmutación por fallas y Syslog (256 bytes)

Los bloques de 256 bytes se utilizan principalmente para conmutación por error. El ASA activo genera y envía los paquetes al ASA espera para poner al día la traducción y la tabla de conexiones. Durante los períodos de tráfico congestionado donde se crean o se desactivan las altas velocidades de conexiones, el número de bloques disponibles de 256 bytes puede llegar a 0. Este descenso indica que una o más conexiones no están puestas al día al ASA espera. Esto es generalmente aceptable porque la próxima vez el protocolo de stateful failover captura la xlate o la conexión que se pierde. Sin embargo, si la columna CNT para el 256-byte bloquea las estancias en o cerca de 0 por los períodos ampliados, el ASA no puede continuar con la traducción y las tablas de conexiones que se sincronizan debido al número de conexiones por segundo que el ASA procese. Si sucede esto constantemente, actualice el ASA a un modelo más rápido.

Los mensajes de Syslog enviados del ASA también utilizan los bloques del 256-byte, pero no se

liberan generalmente en tal cantidad que cause un agotamiento del agrupamiento de bloques del 256-byte. Si la columna CNT muestra que el número de bloques de 256 bytes está cerca de 0, asegúrese de que no registre en el Debugging (nivel 7) al servidor de syslog. Esto es indicada por la línea de trampa de registro en la configuración ASA. Se recomienda que establezca el registro a la Notificación (el nivel 5) o inferior, a menos que requiera la información adicional para los propósitos de debugging.

Ejemplo:

```
Ciscoasa#show blocks
  SIZE    MAX    LOW    CNT
     4   1600   1597   1600
    80    400    399    400
   256    500    495    499
  1550   1444   1170   1188
 16384   2048   1532   1538
```

[Descripción del Resultado]

Esta tabla describe las columnas en el resultado de **show blocks**.

Columna	Descripción
TAMAÑO	E clasifica, en los bytes, del agrupamiento de bloques. Cada tamaño representa un tipo determ
MÁX	Número máximo de bloques disponibles para el agrupamiento de bloques especificado del byt número máximo de bloques se talla fuera de la memoria en el bootup. Típicamente, el número máximo de bloques no cambia. La excepción está para el 256- y los bloques 1550-byte, donde dispositivo de seguridad adaptante puede crear dinámicamente más cuando está necesitado, h un máximo de 8192.
BAJO	Marca de agua baja. Este número indica el número más bajo de bloques de este tamaño disponibles puesto que el dispositivo de seguridad adaptante fue accionado para arriba, o pues que la última limpieza de los bloques (con el comando clear blocks). Un cero adentro la column BAJA indica un evento anterior donde estaba llena la memoria.
CNT	Número actual de bloques disponibles para ese agrupamiento de bloques específico del tamañ cero adentro que la columna CNT significa que la memoria es llena ahora.

Esta tabla describe los valores de la fila SIZE (TAMAÑO) en el resultado **show blocks** .

Valor SIZE (TAMAÑO)	Descripción
0	Utilizado por los bloques del dupb.
4	Duplica los bloques existentes en las aplicaciones tales como DNS, ISAKMP, Filtrado de URL

	uauth, TFTP, y módulos TCP. También, este bloque clasificado se puede utilizar normalment el código para enviar los paquetes a los drivers, al etc.
80	Utilizado en la Intercepción de tráfico de TCP para generar los paquetes de reconocimiento y los mensajes Hello Messages de la Conmutación por falla.
256	Usado para las actualizaciones de conmutación por error con estado, syslogging y otras func de TCP. Estos bloques se utilizan principalmente para los mensajes de la falla de estado. El dispositivo de seguridad adaptante activo genera y envía los paquetes al dispositivo de segur adaptante espera para poner al día la traducción y la tabla de conexiones. En el tráfico congestionado, donde se crean o se derriban las altas velocidades de las conexiones, el núm de bloques disponibles pudo caer a 0. Esta situación indica que una o más conexiones no fue puestas al día al dispositivo de seguridad adaptante espera. El protocolo de la falla de estado coge la traducción o la conexión que falta la próxima vez. Si la columna CNT para el 256-byte bloquea las estancias en o cerca de 0 por los períodos ampliados, después el dispositivo de seguridad adaptante está teniendo problema que mantiene la traducción y las tablas de conexiones sincronizadas debido al número de conexiones por segundo que el dispositivo de seguridad adaptante esté procesando. Los mensajes de Syslog enviados del dispositivo de seguridad adaptante también utilizan los bloques del 256-byte, pero no se liberan generalmer en tal cantidad para causar un agotamiento del agrupamiento de bloques del 256-byte. Si la columna CNT muestra que el número de bloques del 256-byte está cerca de 0, asegúrese de usted no esté registrando en el debugging (nivel 7) al servidor de Syslog. Esto es indicada po línea de trampa de registro en la configuración adaptante del dispositivo de seguridad. Recomendamos que usted fija el registro en la notificación (el nivel 5) o baja, a menos que us requiera la información adicional para los propósitos de debugging.
1550	Utilizado para salvar los paquetes Ethernet para procesar a través del dispositivo de seguridad adaptante. Cuando un paquete ingresa una interfaz adaptante del dispositivo de seguridad, s coloca en la cola de la interfaz de entrada, se pasa hasta el sistema operativo, y se coloca en bloque. El dispositivo de seguridad adaptante determina si el paquete se debe permitir o nega sobre la base de la política de seguridad y procesa el paquete a través a la cola de salida en interfaz de salida. Si el dispositivo de seguridad adaptante está teniendo problema que contin con la carga de tráfico, el número de bloques disponibles asomará cerca de 0 (tal y como se muestra en de la columna CNT de la salida de comando). Cuando la columna CNT es cero, e dispositivo de seguridad adaptante intenta afectar un aparato más bloques, hasta un máximo 8192. Si no más de bloques están disponibles, el dispositivo de seguridad adaptante cae el paquete.
16384	Utilizado solamente para el 64-bit, placas Gigabit Ethernet 66-MHz (i82543). Vea la descripci para 1550 para más información sobre los paquetes Ethernet.
2048	Controle o dirigió las tramas usadas para las actualizaciones del control.

show memory

El comando show memory visualiza memoria física total (o el RAM) para el ASA, junto con la cantidad de bytes actualmente disponible. Para utilizar esta información, usted debe primero entender cómo el ASA utiliza la memoria. Cuando el ASA inicia, copia el OS del Flash en el RAM y ejecuta el OS del RAM (apenas como el Routers). Después, el ASA copia la configuración de inicio del Flash y la pone en el RAM. Finalmente, el ASA afecta un aparato el RAM para crear a los agrupamientos de bloques discutidos en la sección de los bloques de la demostración. Una vez que esta asignación es completa, el ASA necesita el RAM adicional solamente si la configuración aumenta de tamaño. Además, el ASA salva las entradas de la traducción y de la conexión en el RAM.

Durante el funcionamiento normal, memoria libre en el ASA debe cambiar muy poco, si en absoluto. Típicamente, la única vez que usted debe ejecutarse bajo en la memoria es si usted está bajo el ataque y cientos de miles de conexiones pasan con el ASA. Para marcar las conexiones, publique el **comando show conn count**, que visualiza la corriente y la cantidad máxima de conexiones con el ASA. Si el ASA se ejecuta de la memoria, causa un crash eventual. Antes de la caída, usted puede ser que note los mensajes de la falla de asignación de memoria en el Syslog (%ASA-3-211001). Si se queda sin memoria porque el equipo sufre un ataque, comuníquese con el el Centro de Asistencia Técnica de Cisco (TAC).

Ejemplo:

```
Ciscoasa#
show memory
Free memory:        845044716 bytes (79%)

Used memory:        228697108 bytes (21%)

-------------      ----------------

Total memory:      1073741824 bytes (100%)
```

show xlate

El comando show xlate count visualiza la corriente y el número máximo de traducciones con el ASA. Una traducción es un mapping de una dirección interna a una dirección externa y puede ser un mapping uno a uno, tal como Traducción de Dirección de Red (NAT), o un mapping de varios a uno, por ejemplo la Traducción de Dirección de Puerto (PAT). Este comando es un subconjunto del **comando show xlate**, que hace salir cada traducción con el ASA. La salida de comando muestra las traducciones “funcionando,” cuál refiere al número de traducciones activas en el ASA cuando se publica el comando; “utilizado” refiere a las traducciones máximas que se han considerado nunca en el ASA desde que fue accionado encendido.

> Nota: Un solo host puede tener múltiples conexiones a varios destinos, pero solamente una traducción. Si la cuenta de xlate es mucho más grande que el número de hosts en su red interna, es posible que uno de sus hosts internos se vea comprometido. Si se ha comprometido su host interno, las parodias la dirección de origen y manda los paquetes el ASA.

> Nota: Cuando se habilita la configuración vpnclient y el host interior envía las solicitudes

DNS, el **comando show xlate** puede enumerar xlates múltiples para una traducción estática.

Ejemplo:

```
Ciscoasa#
show xlate count
84 in use, 218 most used
```

```
Ciscoasa(config)#show xlate

3 in use, 3 most used

Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,

       o - outside, r - portmap, s - static

TCP PAT from inside:10.1.1.15/1026 to outside:192.150.49.1/1024 flags ri
idle 62:33:57 timeout 0:00:30
UDP PAT from 10.1.1.15/1028 to outside:192.150.49.1/1024 flags ri
idle 62:33:57 timeout 0:00:30
ICMP PAT from inside:10.1.1.15/21505 to outside:192.150.49.1/0 flags ri
idle 62:33:57 timeout 0:00:30
```

La primera entrada es una traducción de la dirección del puerto TCP para el puerto de host (10.1.1.15, 1026) en la red interna al puerto de host (192.150.49.1, 1024) en la red externa. El indicador “r” significa que la traducción es una Traducción de Dirección de Puerto. Los indicadores "i" significan que la traducción se aplica a address-port interno.

La segunda entrada es una Traducción de Dirección de Puerto UDP para el puerto de host (10.1.1.15, 1028) en la red interna al puerto de host (192.150.49.1, 1024) en la red externa. El indicador “r” significa que la traducción es una Traducción de Dirección de Puerto. Los indicadores "i" significan que la traducción se aplica a address-port interno.

La tercera entrada es una Traducción de Dirección de Puerto ICMP para host-ICMP-id (10.1.1.15, 21505) en la red interna al host-ICMP-id (192.150.49.1, 0) en la the red externa. El indicador “r” significa que la traducción es una Traducción de Dirección de Puerto. Los indicadores "i" significan que la traducción se aplica a la address-ICMP-id interna.

Los campos de la dirección interna aparecen como direcciones de origen en los paquetes que atraviesan la interfaz más segura a la interfaz menos segura. Inversamente, aparecen como la dirección de destino en los paquetes que atraviesan la interfaz menos segura a la interfaz más segura.

show conn count

El comando show conn count muestra la corriente y la cantidad máxima de conexiones con el ASA. Una conexión es una asignación de información de Capa 4 desde una dirección interna a una dirección externa. Se aumentan las conexiones cuando el ASA recibe un paquete SYN para las sesiones TCP o cuando llega el primer paquete en una Sesión UDP. Se derriban las conexiones cuando el ASA recibe el paquete ACK final, que ocurre cuando el apretón de manos de la sesión TCP se cierra o cuando el descanso expira en la Sesión UDP.

Los recuentos de conexiones de la extremadamente alta (50-100 veces normales) pudieron indicar que usted está bajo ataque. Publique el **comando show memory** para asegurarse de que el conteo de conexiones alto no hace el ASA ejecutarse de la memoria. Si está siendo atacado, puede establecer un número máximo de conexiones por entrada estática, y también poner un límite al número de conexiones embrionarias. Esta acción protege sus servidores internos para que no se saturen. Refiera a las referencias de comandos del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 para más información.

Ejemplo:

```
Ciscoasa#show conn count
2289 in use, 44729 most used
```

show interface

El comando show interface puede ayudar a determinar los problemas de discordancia dúplex y los problemas con el cable. También puede comprender mejor si la interfaz está desbordada o no. Si el ASA se ejecuta de la capacidad de CPU, el número de los bloques 1550-byte asoma cerca de 0. (mirada en los bloques 16384-byte en los 66 indicadores luminosos LED amarillo de la placa muestra gravedad menor del carruaje del MHz.) Otro indicador es el aumento de "no hay suficiente buffers" en la interfaz. El ningún mensaje de los buffers indica que la interfaz no puede enviar el paquete al ASA OS porque no hay bloque disponible para el paquete, y se cae el paquete. Si ocurre un aumento en ningunos niveles del buffer regularmente, publique el **comando show proc cpu** para marcar el USO de la CPU en el ASA. Si el USO de la CPU es alto debido a una carga de tráfico intenso, actualice a un ASA más potente que pueda manejar la carga.

Cuando un paquete ingresa primero en una interfaz, se ubica en la cola de hardware de entrada. Si la cola de hardware de entrada está completa, el paquete se coloca en la cola de software de

entrada. El paquete se pasa de su cola de entrada y se coloca en un bloque 1550-byte (o en un bloque 16384-byte en 66 interfaces de Ethernet Gigabite del MHz). El ASA después determina la interfaz de salida para el paquete y coloca el paquete en la cola de hardware apropiada. Si la cola de hardware está llena, el paquete se coloca en la cola de software de salida. Si los bloques máximos en cualquiera de las colas del software son grandes, la interfaz se desborda. Por ejemplo, si el 200 Mbps entra en el ASA y sale todo una sola interfaz del 100 Mbps, la cola del software de salida indica los números altos en la interfaz de salida, que indica que la interfaz no puede manejar el volumen de tráfico. Si experimenta esta situación, actualice a una interfaz más rápida.

Ejemplo:

```
Ciscoasa#show interface
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
 Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
       Input flow control is unsupported, output flow control is unsupported
       MAC address 0013.c480.b2b8, MTU 1500
       IP address 192.168.17.4, subnet mask 255.255.255.0
       311981 packets input, 20497296 bytes, 0 no buffer
       Received 311981 broadcasts, 157 runts, 0 giants
       379 input errors, 107 CRC, 273 frame, 0 overrun, 0 ignored, 0 abort
       0 pause input, 0 resume input
       0 L2 decode drops
       121 packets output, 7744 bytes, 0 underruns
       0 pause output, 0 resume output
       0 output errors, 0 collisions, 1 interface resets
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops, 0 tx hangs
       input queue (blocks free curr/low): hardware (255/249)
       output queue (blocks free curr/low): hardware (255/254)
```

También debe controlar si hay errores en la interfaz. Si recibe los recuentos ignorados, los errores de entrada, los CRC, o los errores de trama, es probable que tenga una discordancia dúplex. El cable pudo ser defectuoso también. Consulte las configuraciones de la velocidad y el dúplex para obtener más información sobre los problemas de dúplex. Recuerde que cada contador de errores representa el número de paquetes que se caen debido a ese error particular. Si usted ve un contador específico que incremente regularmente, el funcionamiento en su ASA sufre muy probablemente, y usted debe encontrar la causa raíz del problema.

Mientras examina los contadores de la interfaz, observe que si la interfaz se configura en dúplex completo, no debe experimentar colisiones, colisiones tardías ni paquetes postergados. Por el contrario, si la interfaz se configura en semidúplex, debe recibir las colisiones, algunas colisiones tardías y posiblemente algunos paquetes postergados. El número total de colisiones, colisiones tardías y paquetes postergados no debe exceder del 10% de la suma de los contadores de paquetes de entrada y de salida. Si sus colisiones exceden el 10% de su tráfico total, entonces el link presenta una utilización excesiva y debe actualizar a dúplex completo o a una velocidad más rápida (10 Mbps a 100 Mbps). Recuerde que las colisiones del medio del 10% que el ASA cae el 10% de los paquetes que pasan a través de esa interfaz; cada uno de estos paquetes deberá

retransmitirse.

Refiera al **comando interface** en las referencias de comandos del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 para información detallada sobre los contadores de la interfaz.

show processes

El comando show processes en el ASA visualiza todos los procesos activos que se ejecutan en el ASA que el comando se ejecuta en ese entonces. Esta información es útil para determinar qué procesos reciben demasiado tiempo de uso de CPU y qué procesos no reciben nada de tiempo de uso de CPU. Para conseguir esta información, ejecute el **comando show processes** dos veces; espere cerca de 1 minuto entre cada vez. Para el proceso en cuestión, reste el valor del tiempo de ejecución visualizado en el segundo resultado del valor del tiempo de ejecución visualizado en el primer resultado. Este resultado le muestra cuánto hora de la CPU (en los milisegundos) el proceso recibido en ese intervalo del tiempo. Observe que algunos procesos están programados para ejecutarse en intervalos determinados, y algunos procesos se ejecutan solamente cuando tienen información para procesar. El proceso 577poll probablemente tenga el valor del tiempo de ejecución más grande de todos sus procesos. Esto es normal porque el proceso 577poll sondea las interfaces de Ethernet para considerar si tienen algunos datos que deben ser procesados.

> Nota: Un examen de cada proceso ASA está fuera del ámbito de este documento, pero se menciona abreviadamente para lo completo. Refiera al comando show processes ASA para más información sobre los procesos ASA.

Resumen de Comandos

En resumen, utilice el **comando show cpu usage** para identificar la carga que el ASA está debajo. Recuerde que el resultado es un promedio del funcionamiento; el ASA puede tener puntos más altos del USO de la CPU que sean enmascarados por la media del funcionamiento. Una vez que el ASA alcanza el USO de la CPU del 80%, el tiempo de espera con el ASA aumenta lentamente al cerca de 90% CPU. Cuando es el USO de la CPU más el de 90%, el ASA comienza a caer los paquetes.

Si el uso de CPU es alto, use el **comando show processes** para identificar los procesos que utilizan el mayor tiempo de CPU posible. Utilice esta información para reducir algo del tiempo que es consumido por los procesos intensivos (tales como registro).

Si el CPU no ejecuta caliente, pero usted cree que los paquetes todavía están caídos, utilice el **comando show interface** para marcar la interfaz ASA para ningunos buffers y colisiones, causada posiblemente por una discordancia dúplex. Si el conteo del no buffer aumenta, pero el uso de la CPU no es bajo, la interfaz no puede soportar el tráfico que la atraviesa.

Si las memorias intermedias están bien, verifique los bloques. Si la columna CNT actual en la salida de los **bloques de la demostración** está cercana a 0 en los bloques 1550-byte (bloques 16384-byte para 66 indicadores luminosos LED amarillo de la placa muestra gravedad menor de la actuación del MHz), el ASA cae muy probablemente los paquetes Ethernet porque está demasiado ocupado. En este caso, el CPU llega a un pico.

Si usted experimenta el problema cuando usted hace las nuevas conexiones con el ASA, utilice el **comando show conn count** para marcar el conteo actual de conexiones con el ASA.

Si la cuenta actual es alta, marque la **memoria de la demostración** hecha salir para asegurarse de que el ASA no se ejecuta de la memoria. Si la memoria es baja, investigue la fuente de las conexiones con el comando **show conn** o el **comando show local-host** para verificar que su red no ha experimentado un ataque de negación de servicio.

Usted puede utilizar otros comandos para medir la cantidad de tráfico que pasa con el ASA. **El comando show traffic** visualiza los paquetes y los bytes globales por la interfaz, y el **perfmon de la demostración** rompe el tráfico abajo en diversos tipos que el ASA examine.

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Soporte Técnico - Cisco Systems