Supervisión y solución de problemas de rendimiento de ASA

Contenido

Introducción

Este documento describe los comandos que se deben utilizar para monitorear y resolver problemas del rendimiento de un Cisco Adaptive Security Appliance (ASA).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en un Cisco Adaptive Security Appliance (ASA) que ejecuta la versión 8.3 y posteriores.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

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

Solucionar problemas de rendimiento

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

Nota: Si tiene el resultado del show comando de su dispositivo Cisco, puede utilizar el Analizador de Cisco CLI **para mostrar los posibles problemas y soluciones.** El Analizador de Cisco CLI admite ciertos show comandos. Si utiliza el Analizador de Cisco CLI, debe ser un usuario registrado de Cisco, debe haber iniciado sesión en su cuenta de Cisco y debe tener habilitado JavaScript en 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, existen varias situaciones que pueden hacer que el proceso de negociación automática falle, lo que resulta en discordancias de velocidad o dúplex (y problemas de rendimiento). 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 generalmente no se mueven, por lo que si los configura correctamente, no necesita 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 negociar automáticamente la velocidad y el dúplex, intercambian tramas (llamadas impulsos de link rápido o FLP) que anuncian su velocidad y capacidades 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 admite la negociación automática, el otro dispositivo recibe los FLP y pasa al modo de detección en paralelo. Para detectar la velocidad de la pareja, el dispositivo escucha la longitud de los pulsos y, a continuación, establece la velocidad en función de la longitud. El problema surge con la configuración dúplex. Debido a que el dúplex se debe negociar, el dispositivo que está configurado para negociar automáticamente no puede determinar la configuración en el otro dispositivo, por lo que el valor predeterminado es semidúplex, como se indica en el estándar IEEE 802.3u.

Por ejemplo, si configura la interfaz ASA para la negociación automática y la conecta a un switch codificado para 100 Mbps y dúplex completo, el ASA envía los FLP. Sin embargo, el switch no responde porque está codificado para velocidad y dúplex y no participa en la negociación automática. Dado que no recibe respuesta del switch, el ASA pasa al modo de detección en paralelo y detecta la longitud de los pulsos en las tramas que envía el switch. Es decir, ASA detecta que el switch está configurado en 100 Mbps, por lo que establece la velocidad de la interfaz en función de esto. Sin embargo, debido a que el switch no intercambia FLPs, el ASA no puede detectar si el switch puede ejecutar el dúplex completo, por lo que el ASA establece el dúplex de interfaz en semidúplex, como se establece en el estándar IEEE 803.2u. Debido a que el switch está codificado a 100 Mbps y dúplex completo, y el ASA acaba de negociar automáticamente a 100 Mbps y semidúplex (como lo hace), el resultado es una discordancia dúplex que puede causar graves problemas 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:

<#root>

Interface GigabitEthernet0/0 "outside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex), A

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, 774

Utilización de la CPU

Si ha notado que el uso de la CPU es alto, complete estos pasos para resolver problemas:

- Compruebe que el recuento de conexiones en show xlate count es bajo.
- Verifique que el bloque de memoria sea normal.
- Verifique que el número de ACL sea más alto.
- Ejecute el show memory detail comando y verifique que la memoria utilizada por el ASA sea de uso normal.
- Compruebe que los recuentos en show processes cpu-hog y show processes memory son normales.
- 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.
- Verifique la configuración de dúplex y velocidad en las interfaces ASA. La configuración de discordancia con las interfaces remotas puede aumentar el uso de la CPU.

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

<#root>

Ciscoasa#

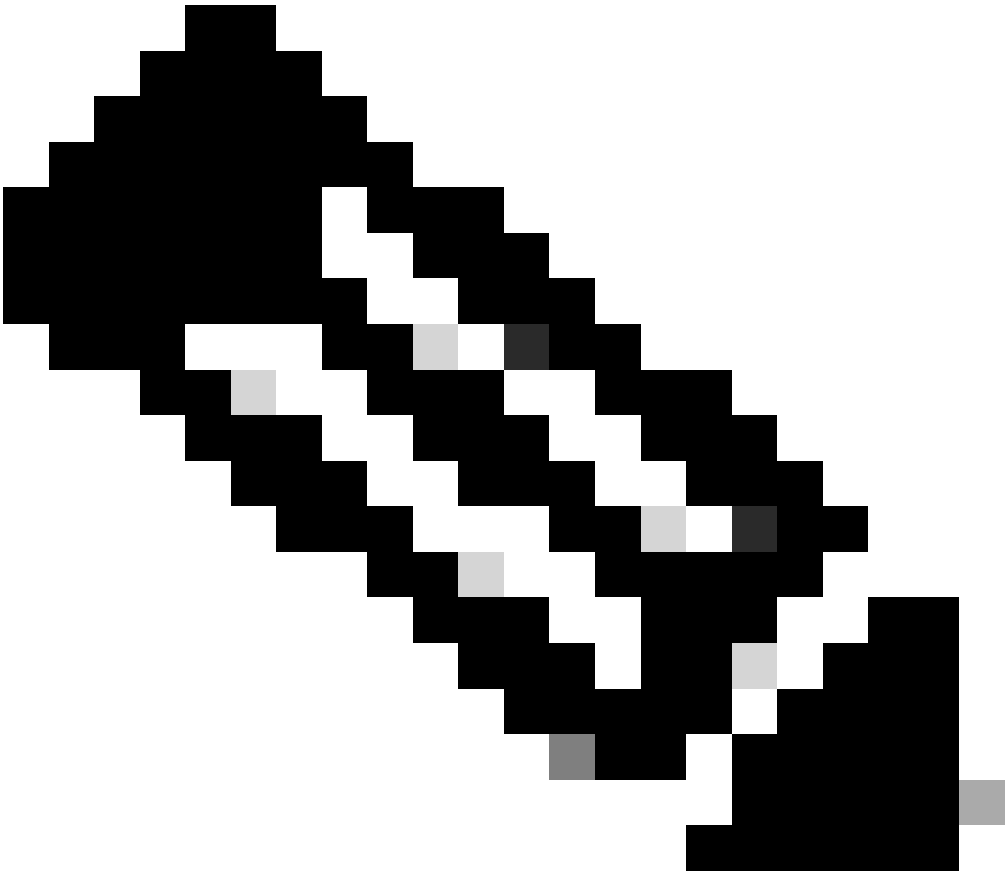
sh int GigabitEthernet0/1

```
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.*



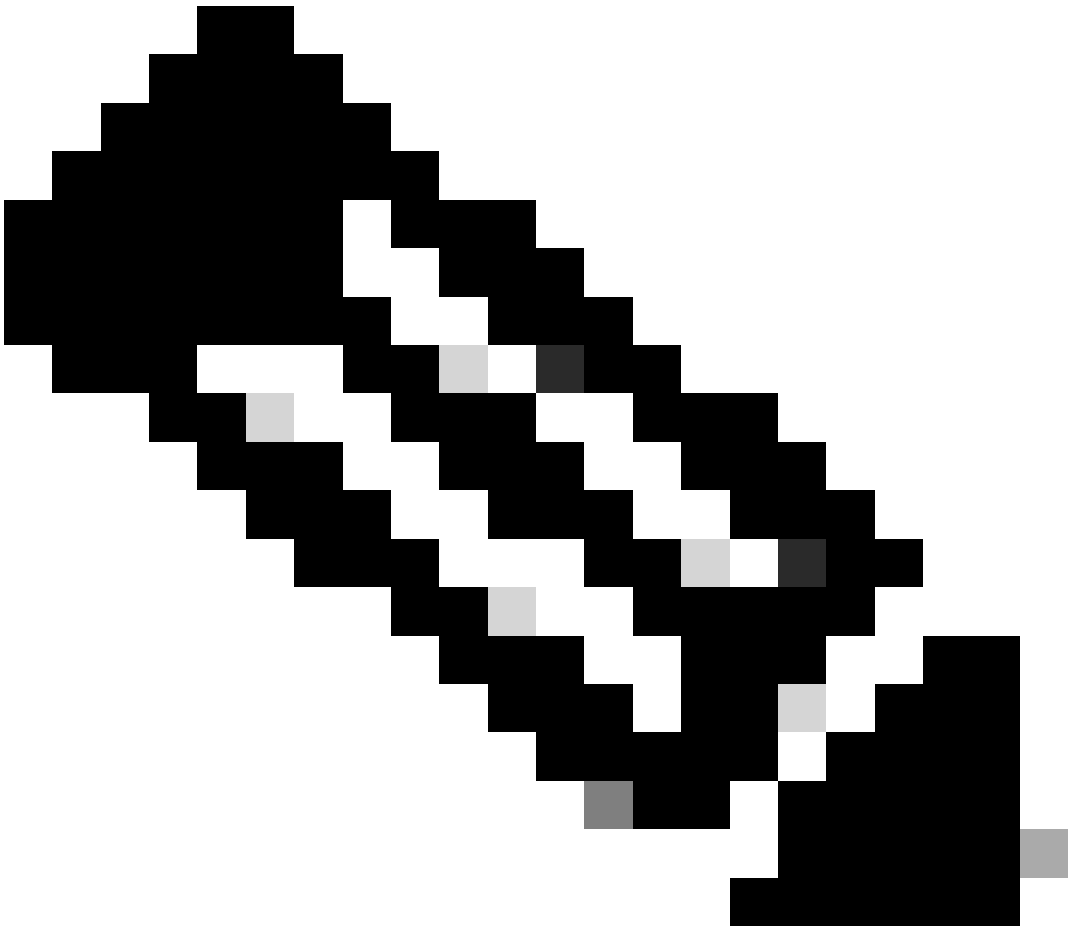
Nota: Cisco recomienda que habilite el ip verify reverse-path interface comando en todas las interfaces. Esto hace que los paquetes que no tienen una dirección de origen válida sean descartados y resulta en un menor uso de la CPU. Esto se aplica al FWSM cuando se enfrenta a problemas de CPU altos.

- Otro motivo del uso de CPU elevado puede ser la existencia de demasiadas rutas multicast. Ejecute el show mroute comando para verificar si ASA recibe demasiadas rutas multicast.

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

- La CPU alta puede ocurrir debido al ID de bug de Cisco CSCsq48636 . Consulte Cisco bug ID CSCsq48636 para obtener más

información.



Nota: Solo los usuarios registrados de Cisco pueden acceder a las herramientas internas de Cisco y a la información de errores.

Nota: si la solución proporcionada anteriormente no resuelve el problema, actualice la plataforma ASA en función de los requisitos. Consulte Módulos de Seguridad de Cisco para Dispositivos de Seguridad para obtener más información sobre las capacidades y capacidades de la Plataforma Adaptive Security Appliance. Póngase en contacto con el TAC (Soporte técnico de Cisco) para obtener más información.

Uso de Memoria Intensivo

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

- **Registro de eventos:** el registro de eventos puede consumir grandes cantidades 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 provocar un elevado consumo de memoria. Para resolver este problema, actualice el software del dispositivo de seguridad.

- **Depuración habilitada:** la depuración puede consumir grandes cantidades de memoria. Para resolver este problema, inhabilite el debugging con el comando undebug all.

- **Bloqueo de puertos:** el bloqueo de puertos en la interfaz externa de un dispositivo de seguridad hace que el dispositivo de seguridad consuma una 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.

- **Detección de amenazas:** La función de detección de amenazas consta de diferentes niveles de estadísticas recopiladas para las distintas amenazas y de la detección de amenazas analizadas, que determina cuándo un host realiza un análisis. **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 de puerto predeterminados no son deseables cuando un ASA está conectado al switch. Por ejemplo, en un switch que ejecuta Catalyst OS, la canalización predeterminada se configura en al Automática, y PortFast se inhabilita. Si conecta un ASA a un switch que ejecuta Catalyst OS, inhabilite la canalización, inhabilite el trunking 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 negociar automáticamente la velocidad y el 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 está configurada en Auto de forma predeterminada. Por esta razón, debe inhabilitar la canalización en cualquier puerto de switch que se conecte a 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 causar 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 ponga el puerto en estado de reenvío inmediatamente después de que el link se active. 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 habilite PortFast en cualquier puerto de switch que se conecte a un ASA.

Nota: Catalyst OS releases 5.4 y posteriores incluyen el set port host <mod>/<port> comando que le permite utilizar un solo comando para inhabilitar la canalización, inhabilitar el 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: se puede producir una interrupción momentánea del flujo de todo el tráfico a través del dispositivo cuando borra xlates globalmente en el dispositivo de seguridad.

Configuración de ejemplo de ASA para PAT que utiliza la dirección IP de la interfaz externa:

object network OBJ_GENERIC_ALL subnet 0.0.0.0 0.0.0.0 nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface

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

<#root>

Ciscoasa#

show xlate

```
 5 in use, 5 most used Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice NA
```

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

<#root>

Ciscoasa#

clear xlate

<#root>

Ciscoasa#

show xlate

0 in use, 1 most used

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

Aquí hay una configuración de ASA de ejemplo para NAT:

object network inside-net subnet 0.0.0.0 0.0.0.0 object network outside-pat-pool range 10.10.10.10 10.10.10.100 nat (inside,outside) source dynamic inside

Observe el show xlate resultado de la traducción para el interior de 10.2.2.2 al exterior global 10.10.10.10:

<#root>

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:

<#root>

```
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:

```
<#root>
```

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 registros del sistema le permiten resolver problemas en el ASA. Cisco ofrece un servidor syslog gratuito para Windows NT denominado Servidor Syslog de firewall ASA (PFSS). Puede descargar PFSS del Soporte técnico y descargas de Cisco.

Varios otros proveedores, como ofrecen servidores syslog para varias 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 configure el servidor syslog, configure el ASA para enviarle registros.

Por ejemplo:

<#root>

logging on logging host <ip_address_of_syslog_server> logging trap debugging

Nota: Este ejemplo configura el ASA para enviar la depuración (nivel 7) y los syslogs más críticos al servidor syslog. Dado que estos registros de ASA son los más detallados, utilícelos únicamente cuando resuelva 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). Verifique si hay mensajes que indiquen que el servidor externo intentó acceder a la dirección IP interna en el puerto TCP 113 (para el protocolo de identificación o identificación), pero el ASA denegó el paquete. El mensaje debe ser similar a este ejemplo:

%ASA-2-106001: Inbound TCP connection denied from 10.64.10.2/35969 to 192.168.110.179/113 flags SYN

Si recibe este mensaje, ejecute el service resetinboundcomando para ASA. El ASA no descarta paquetes silenciosamente; en cambio, este comando hace que el ASA reinicie inmediatamente cualquier conexión entrante que sea denegada por la política de seguridad. El servidor no espera a que el paquete Ident agote el tiempo de espera de su conexión TCP; en su lugar, recibe inmediatamente un paquete de restablecimiento.

SNMP (Protocolo de administración de red simple)

Un método recomendado para las implementaciones empresariales es supervisar el rendimiento de Cisco ASA con SNMP. Cisco ASA es compatible con SNMP versiones 1, 2c y 3.

Puede configurar el dispositivo de seguridad para que envíe capturas a un servidor de administración de red (NMS) o puede utilizar el NMS para examinar las MIB del dispositivo de seguridad. Las MIB son una colección de definiciones y el dispositivo de seguridad mantiene una base de datos de valores para cada definición. Para obtener más información sobre esto, consulte la Guía de configuración de Cisco ASA serie 5500 con CLI, 8.4 y 8.6.

Todos los MIBs soportados para Cisco ASA se pueden encontrar en la Lista de Soporte de MIB ASA. De esta lista, estas MIB son útiles cuando se monitorea el rendimiento:

- CISCO-FIREWALL-MIB ---- Contiene objetos útiles para la conmutación por fallo.
- CISCO-PROCESS-MIB ---- Contiene objetos útiles para la utilización de la CPU.
- CISCO-MEMORY-POOL-MIB ---- Contiene objetos útiles para objetos de memoria.

Búsquedas de DNS inverso

Si experimenta un rendimiento lento con el ASA, verifique que tenga registros de puntero del sistema de nombres de dominio (DNS PTR), también conocidos como registros de búsqueda de DNS inverso, en el servidor DNS autorizado para las direcciones externas que utiliza el ASA. Esto incluye cualquier dirección del conjunto de traducción de direcciones de red (NAT) global (o la interfaz externa de ASA si se sobrecarga en la interfaz), cualquier dirección estática y la dirección interna (si no utiliza NAT con ellas). Algunas aplicaciones, como el protocolo de transferencia de archivos (FTP) y los servidores Telnet, pueden utilizar 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 existe un registro PTR para estos hosts, ejecute el nslookup comando desde su PC o equipo UNIX; incluya la dirección IP global que utiliza para conectarse a Internet.

Ejemplo:

<#root>

```
% nslookup 192.168.219.25

 10.219.133.198.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.

Sobrecarga en la Interfaz

Si tiene una ráfaga de tráfico, los paquetes perdidos pueden ocurrir si la ráfaga excede la capacidad de almacenamiento en búfer del búfer FIFO en la NIC y los búferes de anillo de recepción. Si habilita las tramas de pausa para el control de flujo puede aliviar este problema. Las tramas de pausa (XOFF) y XON son generadas automáticamente por el hardware de NIC en función del uso del búfer FIFO. Se envía una trama de pausa cuando el uso del búfer excede la marca de agua alta. Para habilitar las tramas de pausa (XOFF) para el control de flujo, utilice este comando:

<#root>

hostname(config)#

interface tengigabitethernet 1/0

hostname(config-if)#

flowcontrol send on

Comandos show

show cpu usage

El show cpu usage comando se utiliza para determinar la carga de tráfico colocada en la CPU ASA. Durante tráfico máximo, sobrecargas de red o ataques, puede producirse un pico en el uso de CPU.

El ASA tiene una sola CPU para procesar una variedad de tareas; por ejemplo, procesa paquetes e imprime mensajes de depuración 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 el proceso más intensivo de la CPU, por lo que si su ASA pasa mucho tráfico a través de túneles cifrados, debe considerar un ASA más rápido, un concentrador VPN dedicado, como el VPN 3000. El VAC descarga el cifrado y el descifrado de la CPU ASA y lo realiza en el hardware de la tarjeta. Esto permite al ASA cifrar y descifrar 100 Mbps de tráfico con 3DES (cifrado de 168 bits).

Registrarse es otro proceso que puede consumir enormes cantidades de recursos del sistema. Debido a esto, se recomienda que inhabilite el registro de la consola, el monitor y el buffer en 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 recomienda que el registro de syslog o del protocolo simple de administración de red (SNMP) (historial de registro) se establezca en el nivel 5 (Notificación) o inferior. Además, puede inhabilitar los ID de mensajes de syslog específicos con el no logging message <syslog_id> comando.

Cisco Adaptive Security Device Manager (ASDM) también proporciona un gráfico en la Monitoring ficha que permite ver el uso de CPU del ASA a lo largo del tiempo. Puede utilizar este gráfico para determinar la carga en su ASA.

El **show cpu usage** comando se puede utilizar para mostrar las estadísticas de uso de la CPU.

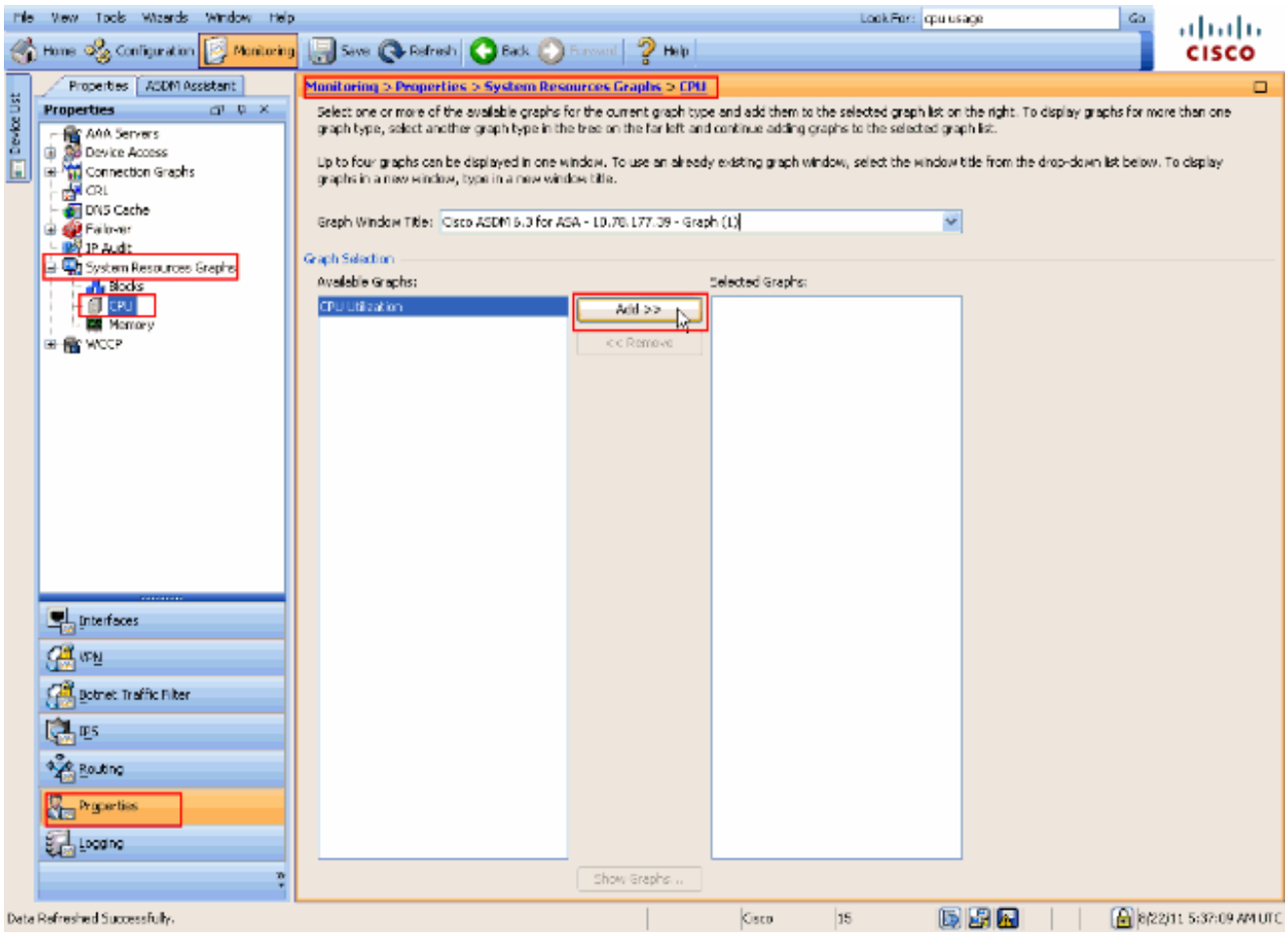
Ejemplo:

```
<#root>

Ciscoasa#

show cpu usage

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

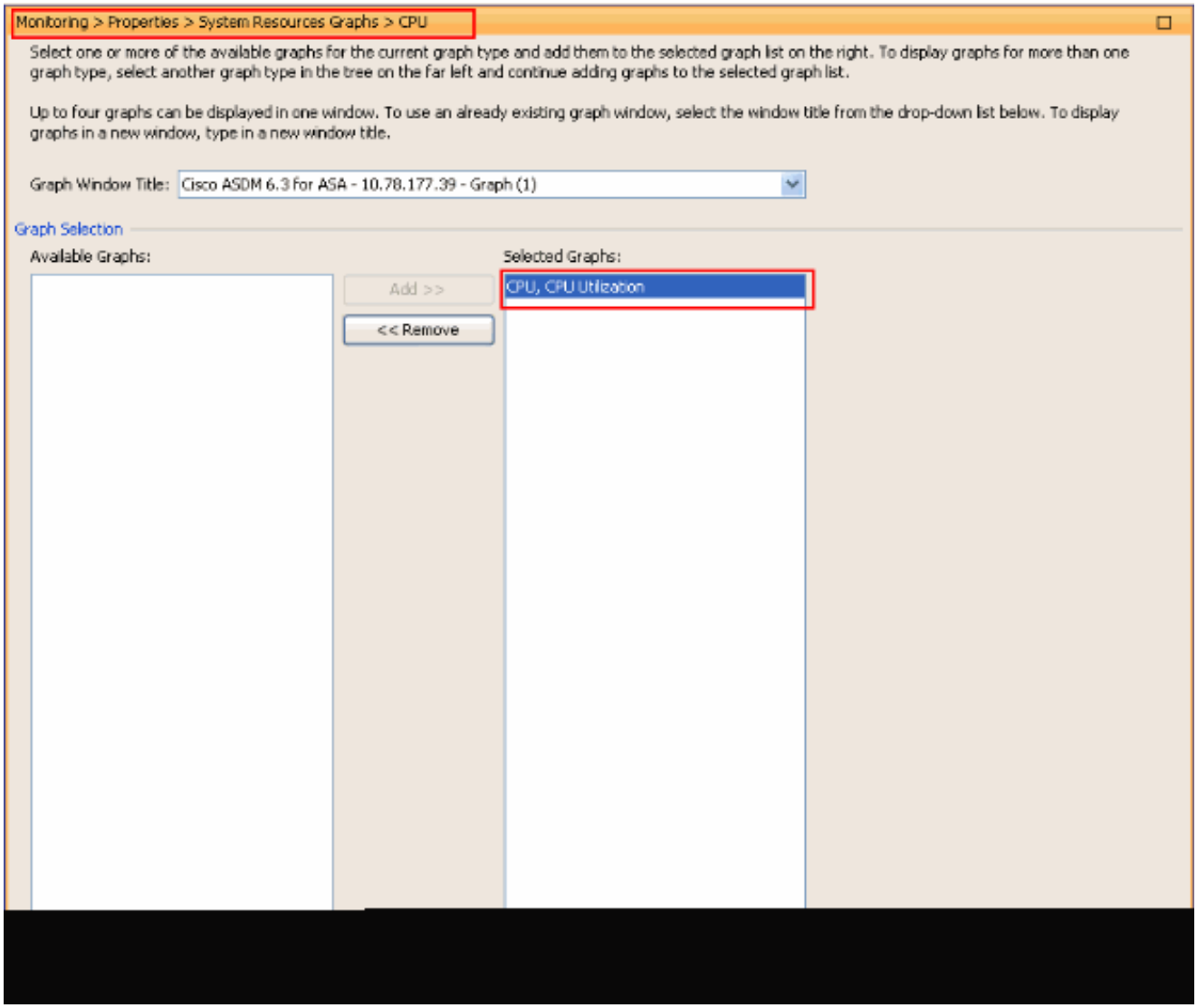
Ver uso de CPU en ASDM

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

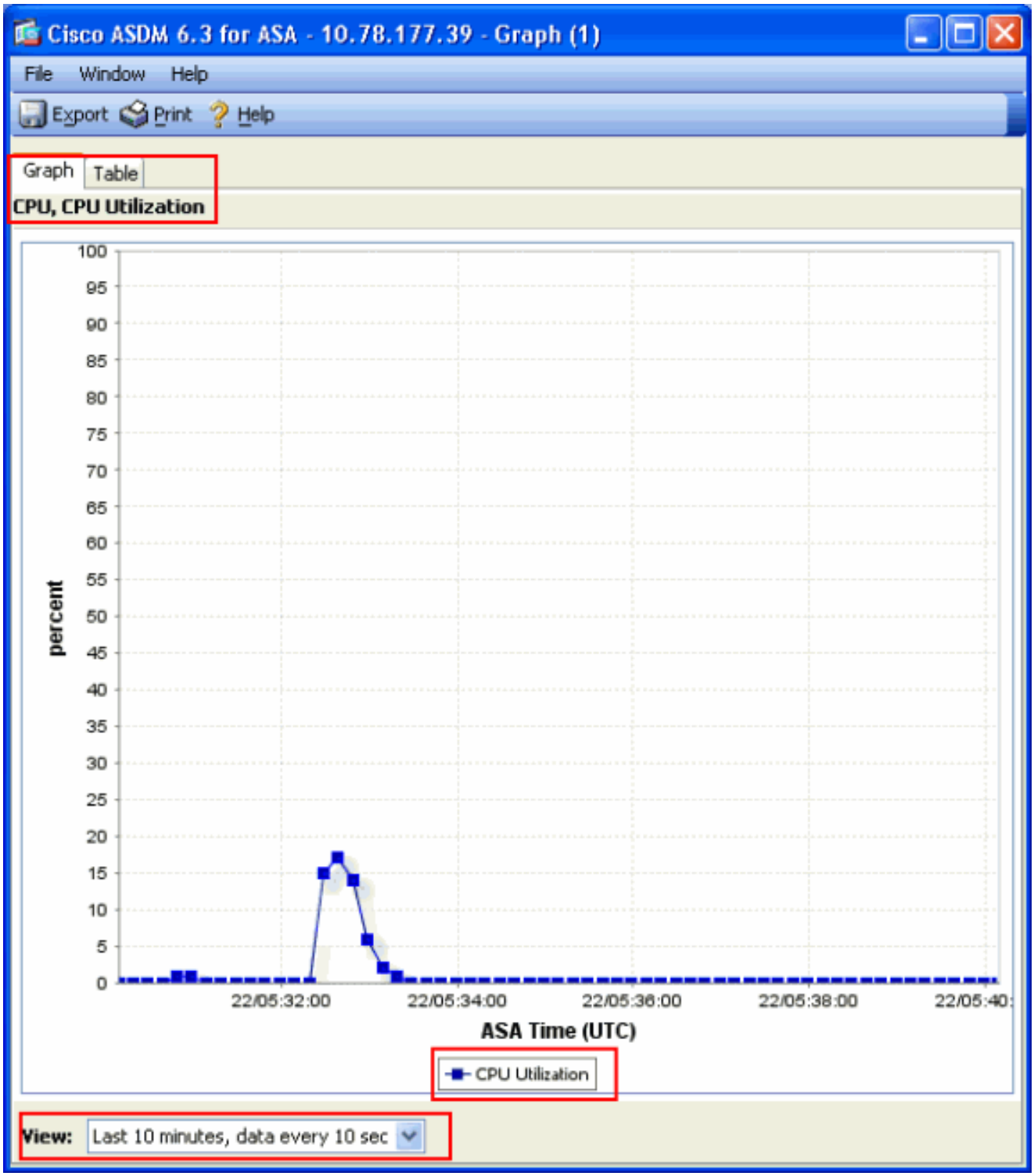
- Vaya a Monitoring > Properties > System Resources Graphics > CPU en ASDM y elija el título de la **ventana gráfica**. A continuación, elija los gráficos necesarios de la lista de **Gráficos disponibles** y haga clic en **Agregar** como se muestra.



- Una vez agregado el nombre de gráfico necesario en la sección **Gráficos seleccionados**, haga clic en **Mostrar gráficos**.



La siguiente imagen muestra el gráfico **Uso de CPU** en el ASDM. Hay disponibles diferentes vistas de este gráfico que se pueden cambiar cuando se selecciona la vista de la lista desplegable Vista. Este resultado se puede imprimir o guardar en el equipo según sea necesario.



Descripción del Resultado

En esta tabla se describen los campos del **show cpu usage** resultado.

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

show traffic

El show traffic comando muestra la cantidad de tráfico que pasa a través del ASA durante un período de tiempo determinado. Los resultados se basan en los intervalos de tiempo desde la última vez que se ejecutó el comando.. Para obtener resultados precisos, ejecute el **clear traffic** comando primero y, a continuación, espere entre 1 y 10 minutos antes de ejecutar el show traffic comando. También puede ejecutar el show traffic comando y esperar de 1 a 10 minutos antes de volver a ejecutarlo, pero sólo es válida la salida de la segunda instancia.

Puede utilizar el show traffic comando para determinar cuánto tráfico pasa a través de su ASA. Si tiene interfaces múltiples, el comando puede ayudarlo a determinar qué interfaces envían y reciben la mayoría de los datos. Para dispositivos ASA con dos interfaces, la suma del tráfico entrante y saliente en la interfaz externa debe ser igual a la suma del tráfico entrante y saliente en la interfaz interna.

Ejemplo:

<#root>

Ciscoasa#

```
show traffic

 outside: received (in 124.650 secs): 295468 packets 167218253 bytes 2370 pkts/sec 1341502 bytes/sec tr
```

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 **show interface** sección, puede examinar los contadores de la interfaz para obtener información sobre el rendimiento.

show perform

El show perfmon comando se utiliza para monitorear la cantidad y los tipos de tráfico que el ASA inspecciona. 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:

PERFMON STATS Current Average Xlates 18/s 19/s Connections 75/s 79/s TCP Conns 44/s 49/s UDP Conns 31/s 30/s URL Access 27/s 30/s URL Serve

Descripción del Resultado

En esta tabla se describen los campos del show perfmon resultado.

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	Solicitudes enviadas a Websense y N2H2 por segundo (requiere filter comando)
TCP Fixup	Número de paquetes TCP que el ASA reenvía por segundo
TCPIntercept	Cantidad de paquetes SYN por segundo que han excedido el límite embrionario establecido en una sentencia estática
HTTP Fixup	Número de paquetes destinados al puerto 80 por segundo (requiere fixup protocol http comando)
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 show cpu usage comando, puede utilizar el show blocks comando para determinar si el ASA está sobrecargado.

Bloques 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 al sistema operativo y se coloca en un bloque. Para los paquetes Ethernet, se utilizan los bloques de 1550 bytes; si el paquete entra en una tarjeta Gigabit Ethernet de 66 MHz, se utilizan los bloques de 16384 bytes. El ASA determina si el paquete está permitido o denegado en función del algoritmo de seguridad adaptable (ASA) y procesa el paquete a través de la cola de salida en la interfaz saliente. Si el ASA no puede soportar la carga de tráfico, el número de bloques de 1550 bytes disponibles (o bloques de 16384 bytes para 66 MHz GE) permanece cercano a 0 (como se muestra en la columna CNT del resultado del comando). Cuando la columna CNT llega a cero, ASA intenta asignar más bloques, hasta un máximo de 8192. Si no hay más bloques disponibles, ASA descarta 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 paquetes al ASA en espera para actualizar la tabla de traducción y conexión. Durante los períodos de tráfico en ráfagas en los que se crean o desactivan altas velocidades de conexiones, el número de bloques de 256 bytes disponibles puede descender a 0. Esta caída indica que una o más conexiones no se actualizan al ASA en 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 los bloques de 256 bytes permanece en 0 o cerca de 0 por períodos de tiempo extendidos, el ASA no puede mantenerse al día con las tablas de traducción y conexión que se sincronizan debido al número de conexiones por segundo que el ASA procesa. Si esto sucede de manera consistente, actualice el ASA a un modelo más rápido.

Los mensajes de Syslog enviados desde ASA también utilizan los bloques de 256 bytes, pero generalmente no se liberan en tal cantidad que cause una disminución del conjunto de bloques de 256 bytes. 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 se indica mediante la línea de trampa de registro en la configuración ASA. Se recomienda que establezca el registro en Notificación (nivel 5) o inferior, a menos que necesite información adicional para la depuración.

Ejemplo:

```
<#root>

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 1
```

Descripción del Resultado

En esta tabla se describen las columnas del show blocks resultado.

Columna	Descripción
TAMAÑO	E Tamaño, en bytes, del conjunto de bloques. Cada tamaño representa un tipo

	determinado
MAX	Número máximo de bloques disponibles para el conjunto de bloques de bytes especificado. El número máximo de bloques se extraen de la memoria durante el arranque. Típicamente, el número máximo de bloques no cambia. La excepción es para los bloques de 256 y 1550 bytes, donde el appliance de seguridad adaptativa puede crear más dinámicamente cuando sea necesario, hasta un máximo de 8192.
BAJO	Marca de agua baja. Este número indica el número más bajo de bloques de este tamaño disponibles desde que se encendió el dispositivo de seguridad adaptable o desde la última limpieza de los bloques (con el comando clear blocks). Un cero en la columna LOW indica un evento anterior en el que la memoria estaba llena.
CNT	Número actual de bloques disponibles para ese conjunto de bloques de tamaño específico. Un cero en la columna CNT significa que la memoria está llena ahora.

En esta tabla se describen los valores de fila SIZE del show blocks resultado.

Valor SIZE (TAMAÑO)	Descripción
0	Usado por bloques dupb.
4	Duplica bloques existentes en aplicaciones como DNS, ISAKMP, filtrado de URL, uauth, TFTP y módulos TCP. Además, este bloque de tamaño se puede utilizar normalmente por el código para enviar paquetes a los controladores, y así sucesivamente.
80	Se utiliza en la intercepción TCP para generar paquetes de reconocimiento y para mensajes hello de failover.
256	Se utiliza para actualizaciones de conmutación por fallo con estado, registro de syslog y otras funciones TCP. Estos bloques se utilizan principalmente para los mensajes de conmutación por fallas stateful. El appliance de seguridad adaptativa activo genera y envía paquetes al appliance de seguridad adaptativa en espera para actualizar la tabla de traducción y conexión. En el tráfico en ráfagas, en el que se crean o desactivan altas velocidades de conexiones, el número de bloques

	disponibles puede descender a 0. Esta situación indica que una o más conexiones no fueron actualizadas al dispositivo de seguridad adaptable en espera. El protocolo Stateful Failover detecta la traducción o conexión perdida la próxima vez. Si la columna CNT para bloques de 256 bytes permanece en 0 o cerca de 0 durante períodos de tiempo prolongados, el appliance de seguridad adaptativa se esfuerza por mantener sincronizadas las tablas de traducción y conexión debido al número de conexiones por segundo que procesa el appliance de seguridad adaptativa. Los mensajes de Syslog enviados desde el dispositivo de seguridad adaptable también utilizan bloques de 256 bytes, pero generalmente no se liberan en tal cantidad para causar una disminución del conjunto de bloques de 256 bytes. Si la columna CNT muestra que el número de bloques de 256 bytes está cerca de 0, asegúrese de que no está registrando en Debugging (nivel 7) en el servidor syslog. Esto se indica mediante la línea de trampa de registro en la configuración del dispositivo de seguridad adaptable. Recomendamos que establezca el registro en Notificación (nivel 5) o inferior, a menos que necesite información adicional para la depuración.
1550	Se utiliza para almacenar paquetes Ethernet para procesar a través del dispositivo de seguridad adaptable. Cuando un paquete entra en una interfaz de dispositivo de seguridad adaptable, se coloca en la cola de la interfaz de entrada, se pasa al sistema operativo y se coloca en un bloque. El dispositivo de seguridad adaptable determina si el paquete se debe permitir o denegar en función de la política de seguridad y procesa el paquete a través de la cola de salida en la interfaz saliente. Si al dispositivo de seguridad adaptable le resulta difícil mantenerse al día con la carga de tráfico, el número de bloques disponibles puede situarse cerca de 0 (como se muestra en la columna CNT del resultado del comando). Cuando la columna CNT es cero, el dispositivo de seguridad adaptable intenta asignar más bloques, hasta un máximo de 8192. Si no hay más bloques disponibles, el dispositivo de seguridad adaptable descarta el paquete.
16384	Sólo se utiliza para las tarjetas Gigabit Ethernet de 64 bits y 66 MHz (i82543). Consulte la descripción de 1550 para obtener más información sobre los paquetes Ethernet.
2048	Tramas guiadas o de control utilizadas para las actualizaciones de control.

show memory

El show memory comando muestra la memoria física total (o RAM) para el ASA, junto con el número de bytes actualmente disponibles. Para utilizar esta información, primero debe entender cómo el ASA utiliza la memoria. Cuando se inicia ASA, copia el sistema operativo de la memoria Flash en la memoria RAM y ejecuta el sistema operativo desde la memoria RAM (al igual que los routers). A continuación, ASA copia

la configuración de inicio de Flash y la coloca en la RAM. Finalmente, ASA asigna RAM para crear los agrupamientos de bloques que se describen en la show blocks sección. Una vez completada esta asignación, el ASA necesita RAM adicional solo si el tamaño de la configuración aumenta. Además, ASA almacena las entradas de traducción y conexión en RAM.

Durante el funcionamiento normal, la memoria libre en el ASA debe cambiar muy poco, si es que cambia. Normalmente, la única vez que debe quedarse sin memoria es si sufre un ataque y cientos de miles de conexiones pasan a través de ASA. Para verificar las conexiones, ejecute el show conn count comando, que muestra el número actual y máximo de conexiones a través del ASA. Si el ASA se queda sin memoria, finalmente se bloquea. Antes del desperfecto, puede observar mensajes de falla de asignación de memoria en el syslog (%ASA-3-211001).

Si se queda sin memoria debido a un ataque, póngase en contacto con el equipo de soporte técnico de Cisco.

Ejemplo:

<#root>

Ciscoasa#

```
show memory

Free memory: 845044716 bytes (79%) Used memory: 228697108 bytes (21%) ------------- ---------------- T
```

show xlate

El show xlate count comando muestra el número actual y máximo de traducciones a través del 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 show xlate comando, que genera cada traducción a través del ASA. El resultado del comando muestra las traducciones "en uso", que se refiere al número de traducciones activas en el ASA cuando se ejecuta el comando; "más utilizadas" se refiere a las traducciones máximas que se han visto en el ASA desde que se encendió.

Nota: Un solo host puede tener varias conexiones a varios destinos, pero solo 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 su host interno se ha visto comprometido, falsifica la dirección de origen y envía paquetes a través del ASA.

Nota: Cuando la configuración vpnclient está habilitada y el host interno envía solicitudes DNS, el show xlate comando puede enumerar múltiples xlates para una traducción estática.

Ejemplo:

<#root>

Ciscoasa#

show xlate count

84 in use, 218 most used

<#root>

Ciscoasa(config)#

show xlate

3 in use, 3 most used Flags: D - DNS, d - dump, I - identity, i - inside, n - no random, o - outside,

TCP PAT from inside:10.1.1.15/1026 to outside:192.168.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30

UDP PAT from 10.1.1.15/1028 to outside:192.168.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30

ICMP PAT from inside:10.1.1.15/21505 to outside:192.168.49.1/0 flags ri idle 62:33:57 timeout 0:00:30

La primera entrada es una Traducción de Dirección del puerto TCP para el puerto de host (10.1.1.15, 1026) en la red interna al puerto de host (192.168.49.1, 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 (192.168.49.1, 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 (192.168.49.1, 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 show conn count comando muestra el número actual y máximo de conexiones a través del ASA. Una conexión es una asignación de información de Capa 4 desde una dirección interna a una dirección externa. Las conexiones se crean cuando ASA recibe un paquete SYN para las sesiones TCP o cuando llega el primer paquete en una sesión UDP. Las conexiones se interrumpen cuando el ASA recibe el paquete ACK final, que ocurre cuando el intercambio de señales de la sesión TCP se cierra o cuando el tiempo de espera expira en la sesión UDP.

Recuentos de conexiones extremadamente altos (50-100 veces superiores a lo normal) pueden indicar que está siendo atacado. Ejecute el show memory comando para asegurarse de que el conteo de conexiones alto no haga que el ASA se quede sin 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. Consulte Guía de Configuración de Cisco ASA 5500 Series con CLI, 8.4 y 8.6 para obtener más información.

Ejemplo:

<#root>

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 de cable. También puede comprender mejor si la interfaz está desbordada o no. Si el ASA se queda sin capacidad de CPU, el número de bloques de 1550 bytes permanece cerca de 0. (Observe los bloques de 16384 bytes en las tarjetas Gig de 66 MHz.) Otro indicador es el aumento de "no hay suficiente buffers" en la interfaz. El mensaje no buffers indica que la interfaz no puede enviar el paquete al sistema operativo ASA porque no hay ningún bloque disponible para el paquete y el paquete se descarta. Si no se produce un aumento en los niveles de memoria intermedia regularmente, ejecute el show proc cpu comando para verificar el uso de la CPU en el ASA. Si el uso de la CPU es alto debido a una carga de tráfico pesada, 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 de 1550 bytes (o en un bloque de 16384 bytes en interfaces Gigabit Ethernet de 66 MHz). El ASA luego 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 200 Mbps entran al ASA y todos salen de una sola interfaz de 100 Mbps, la cola del software de salida indica números altos en la interfaz saliente, lo que indica que la interfaz no puede manejar el volumen de tráfico. Si experimenta esta situación, actualice a una interfaz más rápida.

Ejemplo:

<#root>

Ciscoasa#

show interface

```
 Interface GigabitEthernet0/1 "inside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000
```

También debe comprobar la interfaz en busca de errores. 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 también puede ser defectuoso. 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 ve un contador específico que aumenta regularmente, el rendimiento en su ASA probablemente se resienta, y debe encontrar la causa raíz del problema.

Mientras examina los contadores de interfaz, tenga en cuenta que si la interfaz está configurada en dúplex completo, no debe experimentar ninguna colisión, colisión tardía o paquetes diferidos. Por el contrario, si la interfaz está configurada en semidúplex, debe recibir colisiones, algunas colisiones tardías y posiblemente algunos paquetes postergados. El número total de colisiones, colisiones tardías y paquetes diferidos no debe exceder el 10% de la suma de los contadores de paquetes de entrada y 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 10% significan que ASA descarta el 10% de los paquetes que pasan a través de esa interfaz; cada uno de estos paquetes debe ser retransmitido.

Consulte el interface comando en Referencias de Comandos de Cisco ASA 5500 Series Adaptive Security Appliances para obtener información detallada sobre los contadores de la interfaz.

show processes

El **show processes** comando en el ASA muestra todos los procesos activos que se ejecutan en el ASA en el momento en que se ejecuta el comando. 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 obtener esta información, ejecute el **show processes** comando dos veces; espere aproximadamente 1 minuto entre cada instancia. 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 muestra cuánto tiempo de CPU (en milisegundos) recibió el proceso en ese intervalo de 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 alcance de este documento, pero se menciona brevemente para completar. Consulte ASA 8.3 y versiones posteriores: Monitoreo y Troubleshooting de Problemas de Rendimiento para obtener más información sobre los procesos de ASA.

Resumen de Comandos

En resumen, utilice el show cpu usage comando para identificar la carga que el ASA está bajo. Recuerde que el resultado es un promedio en ejecución; el ASA puede tener picos más altos de uso de CPU que están enmascarados por el promedio en ejecución. Una vez que el ASA alcanza el 80% de uso de la CPU, la latencia a través del ASA aumenta lentamente a aproximadamente el 90% de la CPU. Cuando el uso de la CPU es superior al 90%, el ASA comienza a descartar paquetes.

Si el uso de la CPU es alto, utilice el **show processes** comando para identificar los procesos que utilizan más tiempo de la CPU. Utilice esta información para reducir parte del tiempo que consumen los procesos intensivos (como el registro).

Si la CPU no funciona en caliente, pero cree que los paquetes aún se descartan, utilice el show interface comando para verificar la interfaz ASA para que no haya buffers ni colisiones, posiblemente causados 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 show blocks salida está cerca de 0 en los bloques de 1550 bytes (bloques de 16384 bytes para las tarjetas Gig de 66 MHz), el ASA probablemente descarta paquetes Ethernet porque está demasiado ocupado. En este caso, el CPU llega a un pico.

Si experimenta problemas cuando realiza nuevas conexiones a través del ASA, utilice el show conn count comando para verificar el conteo actual de conexiones a través del ASA.

Si el conteo actual es alto, verifique la show memory salida para asegurarse de que ASA no se quede sin memoria. Si la memoria es baja, investigue el origen de las conexiones con el comando show conn o show local-host para verificar que su red no ha experimentado un ataque de negación de servicio.

Puede utilizar otros comandos para medir la cantidad de tráfico que pasa a través del ASA. El **show traffic** comando muestra los paquetes y bytes agregados por interfaz, y show perfmondivide el tráfico en diferentes tipos que el ASA inspecciona.

Información Relacionada

- Cisco Firewall ASA Serie 5500-X
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).