ASA 8.3 e mais atrasado: Monitore e pesquise defeitos problemas de desempenho

Índice

Introdução

Este documento fornece a informação sobre o ASA comanda que você pode se usar para monitorar e pesquisar defeitos o desempenho de uma ferramenta de segurança adaptável de Cisco (ASA).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em uma ferramenta de segurança adaptável de Cisco (ASA) essa versão 8.3 e mais recente das corridas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você trabalhar em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Troubleshooting

A fim pesquisar defeitos problemas de desempenho, verifique as áreas básicas descritas nesta seção.

> Nota: Se você tem a saída do **comando show de** seu dispositivo Cisco, você pode usar o analisador do CLI Cisco (clientes registrados somente) a fim indicar problemas potenciais e reparos. Os determinados comandos de exibição dos suportes de analisador do CLI Cisco. Se você usa o analisador do CLI Cisco, você deve ser um cliente registrado, você deve ser entrado a sua conta de Cisco, e você deve ter o Javascript permitido dentro de seu navegador.

Configurações de velocidade e dúplex

A ferramenta de segurança preconfigured para autodetect os ajustes da velocidade e duplexação em uma relação. Contudo, diversas situações existem que podem fazer com que o processo de auto-negociação falhe, que conduz à velocidade ou as incompatibilidades duplex (bidirecional) (e os problemas de desempenho). Para a infraestrutura de rede de missão crítica, Cisco não codifica manualmente a velocidade e duplexação em cada relação tão lá é nenhuma possibilidade para o erro. Estes dispositivos geralmente não se movem ao redor, assim que se você os configura corretamente, você não deve precisar de mudá-los.

Em todo o dispositivo de rede, a velocidade do link pode ser detectada, mas o duplex deve ser negociado. Se dois dispositivos de rede são configurados à velocidade e duplexação da autonegociação, trocam os quadros (chamados pulsos rápidos de enlace, ou FLP) que anunciam suas capacidades da velocidade e duplexação. Um parceiro de enlace que não esteja ciente, estes pulsos é similar aos quadros regulares do 10 Mbps. Um parceiro de enlace que possa descodificar os pulsos, os FLP contém todos os ajustes da velocidade e duplexação que o parceiro de enlace pode fornecer. A estação que recebe os FLP reconhece os quadros, e os dispositivos concorda mutuamente com os ajustes os mais altos da velocidade e duplexação que cada um pode conseguir. Se um dispositivo não apoia a negociação automática, o outro dispositivo recebe os FLP e as transições ao modo de detecção paralela. A fim detectar a velocidade do sócio, o dispositivo escuta o comprimento dos pulsos, e ajusta então a velocidade em conformidade. O problema elevara com a configuração bidirecional. Porque o duplex deve ser negociado, o dispositivo que é ajustado à autonegociação não pode determinar os ajustes no outro dispositivo, assim ele opta por metade-frente e verso, como exposto no padrão da IEEE 802.3u.

Por exemplo, se você configura a relação ASA para a negociação automática e a conecta a um interruptor que esteja codificado para o 100 Mbps e FULL-frente e verso, o ASA manda FLP. Contudo, o interruptor não responde porque é codificado para a velocidade e duplexação e não participa na negociação automática. Porque não recebe nenhuma resposta do interruptor, as transições ASA no modo de detecção paralela e detectam o comprimento dos pulsos nos quadros que o interruptor manda. Isto é, o ASA detecta que o interruptor está ajustado ao 100 Mbps, assim que ajusta a velocidade da relação em conformidade. Contudo, porque o interruptor não troca FLP, o ASA não pode detectar se o interruptor pode executar FULL-frente e verso, assim

que o ASA ajusta o duplex da relação metade-frente e verso, como exposto no padrão da IEEE 803.2u. Porque o interruptor é codificado ao 100 Mbps e FULL-frente e verso, e o ASA tem apenas negociado automaticamente ao 100 Mbps e metade-frente e verso (como deve), o resultado é uma incompatibilidade duplex (bidirecional) que possa causar problemas sérios de desempenho.

Uma velocidade ou uma incompatibilidade duplex (bidirecional) mais frequentemente são reveladas quando os contadores de erros nas relações na pergunta aumentam. A maioria de erros comuns são quadro, verificações de redundância cíclica (CRC), e runts. Se estes valores incrementam em sua relação, uma incompatibilidade de velocidade/bidirecional ou uma questão de cabeamento ocorrem. Você deve resolver esta edição antes que você continue.

Exemplo

```
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)
```

CPU Utlization

Se você observou a utilização CPU é alta, termina estas etapas a fim pesquisar defeitos:

1. Verifique que o contagem de conexão na **contagem do xlate da mostra** é baixo.
2. Verifique que o bloco de memória é normal.
3. Verifique que o número de ACL é mais alto.
4. Emita o comando dos **detalhes da memória da mostra**, e verifique que a memória usada

pelo ASA é utilização normal.

5. Verifique que as contagens no **CPU hog dos processos da mostra** e na **memória dos processos da mostra** são normais.

6. Alguns hospedam o presente dentro ou fora que a ferramenta de segurança pode gerar o tráfego malicioso ou maciço que pode ser uma transmissão/tráfego multicast e causar a utilização elevada da CPU. A fim resolver esta edição, configurar uma lista de acessos para negar o tráfego entre os anfitriões (End to End) e para verificar o **uso**.

7. Verifique o duplex e apresse ajustes em relações ASA. O ajuste da má combinação com as interfaces remotas pode aumentar a utilização CPU.

   Este exemplo mostra o número mais alto no *erro de entrada* e as *excedentes* devido à má combinação da velocidade. Use o **comando show interface** a fim verificar os erros:

```
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)
```

   A fim resolver esta edição, ajuste a velocidade como o *automóvel à* interface correspondente.

   Nota: Cisco recomenda que você permite o [IP verifica o comando interface do caminho reverso em] todas as relações porque deixará cair os pacotes que não têm um endereço de origem válida, que conduza a menos USO de CPU. Isto aplica-se ao FWSM que enfrenta edições da alta utilização da CPU.
8. Uma outra razão para o uso da alta utilização da CPU pode ser devido a rotas de transmissão múltiplas demais. Emita o comando do [mrouter da mostra] a fim verificar se o ASA recebe rotas de transmissão múltiplas demais.

9. Use o [comando show local-host] a fim ver se a rede experimenta um ataque de recusa de serviço, que possa indicar um ataque do vírus na rede.

10. A alta utilização da CPU pôde ocorrer devido à identificação de bug Cisco CSCsq48636. Refira a identificação de bug Cisco CSCsq48636 (clientes registrados somente) para mais informação.

Nota: Se a solução forneceu acima não resolve a edição, promove a plataforma ASA de acordo com as exigências. Refira a folha de dados do Dispositivos de segurança adaptáveis Cisco ASA série 5500 para obter mais informações sobre das capacidades e das capacidades adaptáveis da plataforma da ferramenta de segurança. Contacte TAC (clientes registrados somente) para mais informações.

Utilização da memória alta

Estão aqui algumas causas possíveis e definições para a utilização da memória alta:

- **Logging de evento:** O logging de evento pode consumir grandes quantidades de memória. A fim resolver esta edição, instale e registre todos os eventos a um servidor interno, tal como um servidor de SYSLOG.
- **Escape de memória:** Um problema conhecido no software da ferramenta de segurança pode conduzir ao consumo da memória alta. A fim resolver esta edição, promova o software da ferramenta de segurança.
- **Eliminação de erros permitida:** A eliminação de erros pode consumir grandes quantidades de memória. A fim resolver esta edição, desabilitação que debuga com o `comando undebug all`.
- **Portas de bloqueio:** As portas de bloqueio na interface externa de uma ferramenta de segurança fazem com que a ferramenta de segurança consuma quantidades elevadas de memória para obstruir os pacotes através das portas especificadas. A fim resolver esta edição, obstrua o tráfego causador na extremidade ISP.
- **Ameaça-detecção:** A característica da detecção da ameaça consiste em níveis diferentes das estatísticas que recolhem para várias ameaças, assim como na detecção de varredura da ameaça, que determina quando um host está executando uma varredura. **Desligue** esta característica para consumir menos memória.

PortFast, canalização, e entroncamento

Àrevelia, muito Switches, tal como os switch Cisco que executam o Catalyst Operating System (OS), é projetado ser dispositivos plug and play. Como tal, muitos dos parâmetros da porta padrão não são desejáveis quando um ASA é obstruído no interruptor. Por exemplo, em um interruptor que execute o OS do catalizador, a canalização do padrão é ajustada ao automóvel, o entroncamento é ajustado ao automóvel, e PortFast é desabilitado. Se você conecta um ASA a um interruptor que execute o OS do catalizador, desabilite a canalização, desabilite o

entroncamento, e permita PortFast.

Canalizar, igualmente conhecida como o Fast EtherChannel ou EtherChannel de Giga, é usada para ligar dois ou mais portas física em um grupo lógico a fim aumentar o throughput geral através do link. Quando uma porta é configurada para o canal automático, manda quadros do Port Aggregation Protocol (PAgP) enquanto o link se torna ativo a fim determinar se é parte de um canal. Estes quadros podem causar problemas se o outro dispositivo tenta à autonegociação a velocidade e duplexação do link. Se canalizar na porta é ajustada ao automóvel, igualmente conduz a um atraso adicional de aproximadamente 3 segundos antes que os começos da porta para enviar o tráfego após o link estejam acima.

> Nota: Nos Catalyst XL Series switch, canalizar não é ajustada ao automóvel à revelia. Por este motivo, você deve desabilitar a canalização em toda a porta de switch que conectar a um ASA.

O entroncamento, igualmente conhecido pelo Inter-Switch Link (ISL) comum ou pelo dot1q dos protocolos de entroncamento, combina as LAN virtuais múltiplas (VLAN) em uma porta única (ou no link). O entroncamento é usado tipicamente entre dois Switches quando ambo o Switches tem mais de um VLAN definido nele. Quando uma porta é configurada para o entroncamento automático, manda quadros do Dynamic Trunking Protocol (DTP) enquanto o link vem acima a fim determinar se a porta a que conecta quer ao tronco. Esses quadros DTP podem provocar problemas com a autonegociação do link. Se o entroncamento é ajustado ao automóvel em uma porta de switch, adiciona um atraso adicional de aproximadamente 15 segundos antes que os começos da porta para enviar o tráfego após o link estejam acima.

PortFast, igualmente conhecido como o começo rápido, é uma opção que informe o interruptor que um dispositivo da camada 3 está conectado fora de uma porta de switch. A porta não espera o padrão 30 segundos (15 segundos a escutar e 15 segundos a aprender); em lugar de, esta ação faz com que o interruptor ponha a porta no estado de encaminhamento imediatamente depois que o link vem acima. É importante compreender que quando você permite PortFast, medindo - a árvore não é desabilitada. Medida - a árvore é ainda ativa nessa porta. Quando você permite PortFast, o interruptor está informado somente que não há um outro interruptor ou hub (dispositivo da camada 2-only) conectado no outro extremo do link. O interruptor contorneia o atraso 30-second normal quando tentar determinar se resultados de um laço da camada 2 se traz acima essa porta. Depois que o link é trazido acima, ainda participa na medida - árvore. A porta manda as unidades de dados do pacote de Bridge (BPDU), e o interruptor ainda escuta BPDU nessa porta. Por estas razões, recomenda-se que você permite PortFast em toda a porta de switch que conectar a um ASA.

> Nota: Os Catalyst OS Releases 5.4 e mais atrasado incluem o **comando set port host <mod>/<port>** que permite que você use um comando único desabilitar a canalização,

desabilitar o entroncamento, e permitir PortFast.

Network Address Translation (NAT)

Sessão de cada sobrecarga NAT ou NAT (PANCADINHA) é atribuída um slot de tradução conhecido como um *xlate*. Estes xlates podem persistir mesmo depois que você faz mudanças ao NAT ordena que influência elas. Isto pode conduzir a uma prostração dos slots de tradução ou do comportamento inesperado ou a ambos pelo tráfego que se submete à tradução. Esta seção explica como ver e xlates claros na ferramenta de segurança.

> Cuidado: Uma interrupção momentânea do fluxo de todo o tráfego através do dispositivo puder ocorrer quando você xlates globalmente claros na ferramenta de segurança.

Prove a configuração ASA para a PANCADINHA que usa o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface externa:

```
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)
```

Trafique que corre através da ferramenta de segurança se submete muito provavelmente ao NAT. A fim ver as traduções que estão no uso na ferramenta de segurança, emita o **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
```

Os slots de tradução podem persistir depois que as mudanças chaves são feitas. A fim cancelar entalhes da tradução atual na ferramenta de segurança, emita o **comando clear xlate**:

```
Ciscoasa#clear xlate
```

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

O comando clear xlate cancela toda a tradução dinâmica atual da tabela do xlate. A fim cancelar uma tradução particular IP, você pode usar o **comando clear xlate** com a palavra-chave **global do [ip address]**.

Está aqui uma configuração da amostra ASA para o NAT:

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

Observe o **xlate da mostra** output para a tradução para 10.2.2.2 interno ao Outside 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
```

Cancele a tradução para o endereço IP global de 10.10.10.10:

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

Neste exemplo, a tradução para 10.2.2.2 interno ao Outside Global 10.10.10.10 é ida:

```
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
```

Syslogs

Os Syslog permitem que você pesquise defeitos edições no ASA. Cisco oferece um servidor de SYSLOG livre para o Windows NT chamado o servidor de SYSLOG do Firewall ASA (PFSS). Você pode transferir o PFSS da página dos downloads do software (clientes registrados somente).

Diversos outros fornecedores, tais como Kiwi Enterprises , oferecem servidores de SYSLOG para diversas plataformas Windows, tais como o Windows 2000 e o Windows XP. A maioria UNIX e de máquinas de Linux têm os servidores de SYSLOG instalados à revelia.

Quando você estabelece o servidor de SYSLOG, configurar o ASA a fim enviar-lhe logs.

Por exemplo:

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

> Nota: Este exemplo configura o ASA para enviar a eliminação de erros (nível 7) e uns Syslog mais críticos ao servidor de SYSLOG. Porque estes logs ASA são os mais verbosos, use-os somente quando você pesquisa defeitos uma edição. Para a operação normal, configurar o nível de registro à advertência (nível 4) ou ao erro (nível 3).

Se você experimenta uma edição com desempenho lento, abra o Syslog em um arquivo de texto e em uma busca para o endereço IP de origem associado com o problema de desempenho. (Se

você usa UNIX, você pode `grep` com o Syslog para o endereço IP de origem.) Verifique para ver se há mensagens que indicam o servidor interno tentado alcançar o endereço IP interno na porta TCP 113 (para o protocolo de identificação, ou a identificação), mas o ASA negou o pacote. A mensagem deve ser similar a este exemplo:

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

Se você recebe esta mensagem, emita o comando service resetinbound ao ASA. O ASA não deixa cair silenciosamente pacotes; em lugar de, este comando faz com que o ASA restaure imediatamente toda a conexão de entrada que for negada pela política de segurança. O server não espera o pacote identificação para cronometrar para fora sua conexão de TCP; em lugar de, recebe imediatamente um pacote da restauração.

SNMP:

Monitorar o desempenho de Cisco ASA que usa o SNMP é o método recomendada para as distribuições de empreendimento. Cisco ASA apoia o Monitoramento de redes com versões de SNMP 1, 2c e 3.

Você pode configurar a ferramenta de segurança para enviar armadilhas a um Network Management Server (NMS), ou você pode usar o NMS para consultar o MIBs na ferramenta de segurança. O MIBs é uma coleção das definições, e a ferramenta de segurança mantém um base de dados dos valores para cada definição. Para obter mais informações sobre disto, refira configurar o SNMP em Cisco ASA.

Todo o MIBs apoiado para Cisco ASA pode ser encontrado na lista de suporte MIB ASA. Desta lista, este MIBs é útil para o monitoramento de desempenho:

- CISCO-FIREWALL-MIB ---- Contém os objetos úteis para o Failover
- CISCO-PROCESS-MIB ---- Contém os objetos úteis para a utilização CPU
- CISCO-MEMORY-POOL-MIB ---- Contém os objetos úteis para objetos da memória.

Consultas de DNS inverso

Se você experimenta o desempenho lento com o ASA, verifique que você tem os registros do ponteiro do Domain Name System (PTR DNS), igualmente conhecidos como registros da pesquisa de DNS reversa, no servidor DNS competente para os endereços externos que o ASA usa. Isto incluem todo o endereço em seu pool da tradução de endereço de rede global (NAT) (ou a interface externa ASA se você sobrecarrega na relação), qualquer endereço estático, e endereço interno (se você não usa o NAT com ele). Alguns aplicativos, tais como o File Transfer Protocol (FTP) e os servidores Telnet, podem usar pesquisas de DNS reversas a fim determinar de aonde o usuário vem e se é um host válido. Se a pesquisa de DNS reversa não resolve, a seguir o desempenho está degradado como os tempos do pedido para fora.

A fim assegurar-se de que um registro PTR exista para estes anfitriões, emita o **comando nslookup de** seu PC ou a máquina Unix; inclua o endereço IP global que você se usa para conectar ao Internet.

Exemplo

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

Você deve receber uma resposta para trás com o nome de DNS do dispositivo atribuído a esse endereço IP de Um ou Mais Servidores Cisco ICM NT. Se você não recebe uma resposta, contacte a pessoa que controla seu DNS a fim pedir a adição de registros PTR para cada um de seus endereços IP globais.

Excedentes na relação

Se você tem uma intermitência de tráfego, os pacotes descartado podem ocorrer se a explosão excede a capacidade de proteção do buffer FIFO no NIC e nos bufferes do anel de recebimento. Permitir frames de pausa para o controle de fluxo pode aliviar esta edição. A pausa (XOFF) e os quadros XON são gerados automaticamente pelo NIC com base em hardware no uso do buffer FIFO. Um frame de pausa é enviado quando o uso de buffer excede a marca da água superior. A fim permitir quadros da pausa (XOFF) para o controle de fluxo, use este comando:

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

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

Refira a possibilidade da interface física e configurar parâmetros dos Ethernet para mais informação.

comandos show

show cpu usage

O comando show cpu usage é usado determinar a carga de tráfego colocada no ASA CPU. Durante tempos do tráfego de pico, a rede aflui, ou os ataques, o USO de CPU podem cravar.

O ASA tem um único CPU para processar uma variedade de tarefas; por exemplo, processa pacotes e as cópias debugam mensagens ao console. Cada processo tem sua própria finalidade, e alguns processos exigem mais processador central - tempo do que outros processos. A criptografia é provavelmente a maioria de processo intensivo de CPU, assim que se seu ASA passa muito tráfego através dos túneis criptografado, você deve considerar um ASA mais rápido, um concentrador VPN dedicado, tal como o VPN3000. O VAC offloads a criptografia e a descriptografia do ASA CPU e executa-a no hardware no cartão. Isto permite que o ASA cifre e decifre o 100 Mbps do tráfego com 3DES (criptografia do 168-bit).

O registro é outro processo que pode consumir grande quantidade de recursos do sistema. Devido a isto, recomenda-se que você desabilita o console, o monitor, e o buffer entrando o ASA. Você pode permitir estes processos quando você pesquisa defeitos um problema, mas desabilita-os para a operação do dia a dia, especialmente se você é executado fora da capacidade de CPU. Igualmente sugere-se que a informações de syslog ou o Simple Network Management Protocol (SNMP) que registram (história de registro) devam ser ajustados ao nível 5 (notificação) ou abaixar. Além, você pode desabilitar o mensagem do syslog específico ID com o **comando no logging message <syslog_id>**.

O Cisco Adaptive Security Device Manager (ASDM) igualmente fornece um gráfico na aba da monitoração que permite que você ver o USO de CPU do ASA ao longo do tempo. Você pode usar este gráfico a fim determinar a carga em seu ASA.

O comando show cpu usage pode ser utilizado para exibir as estatísticas de utilização da CPU.

Exemplo

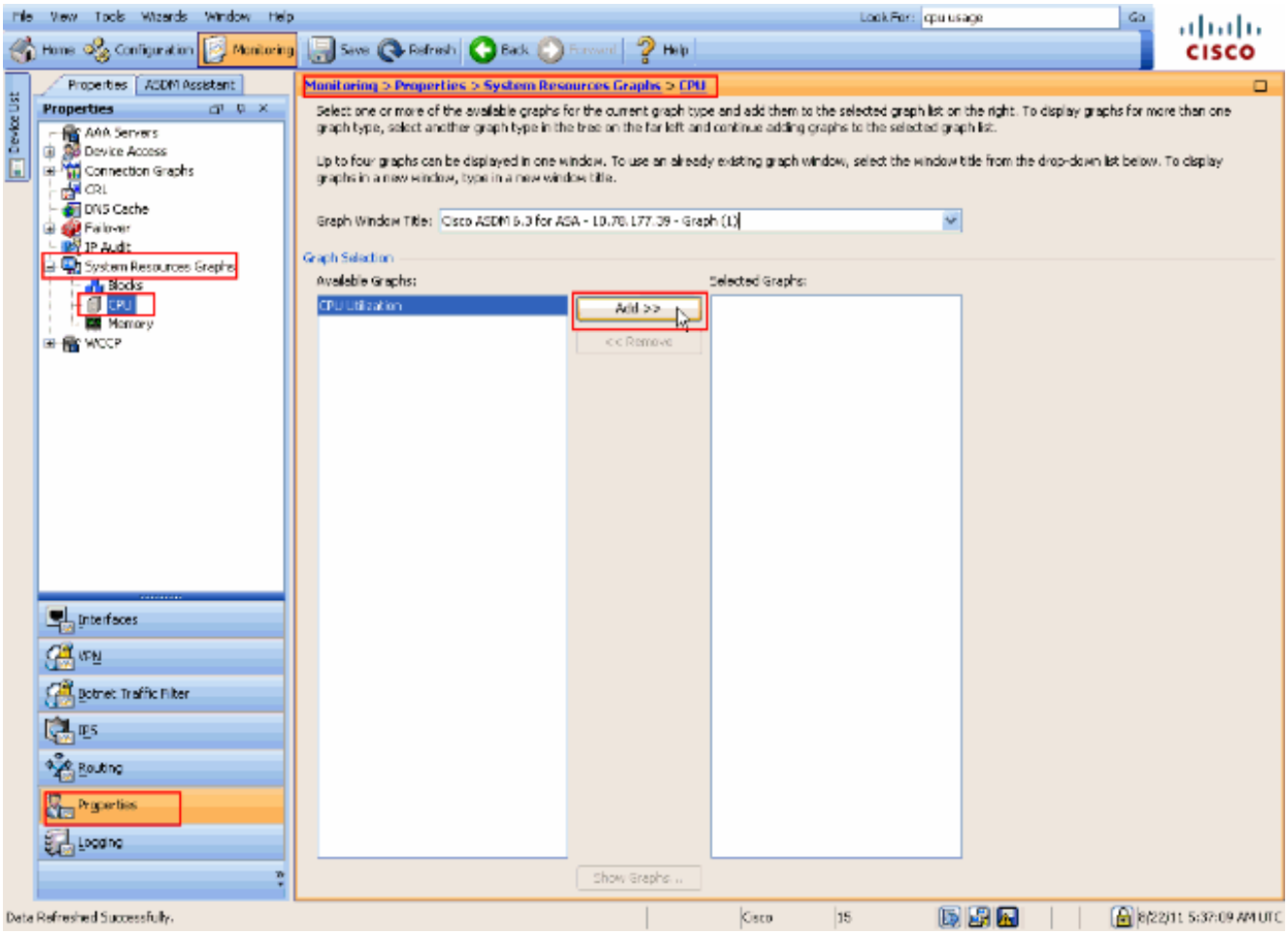
```
Ciscoasa#show cpu usage

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

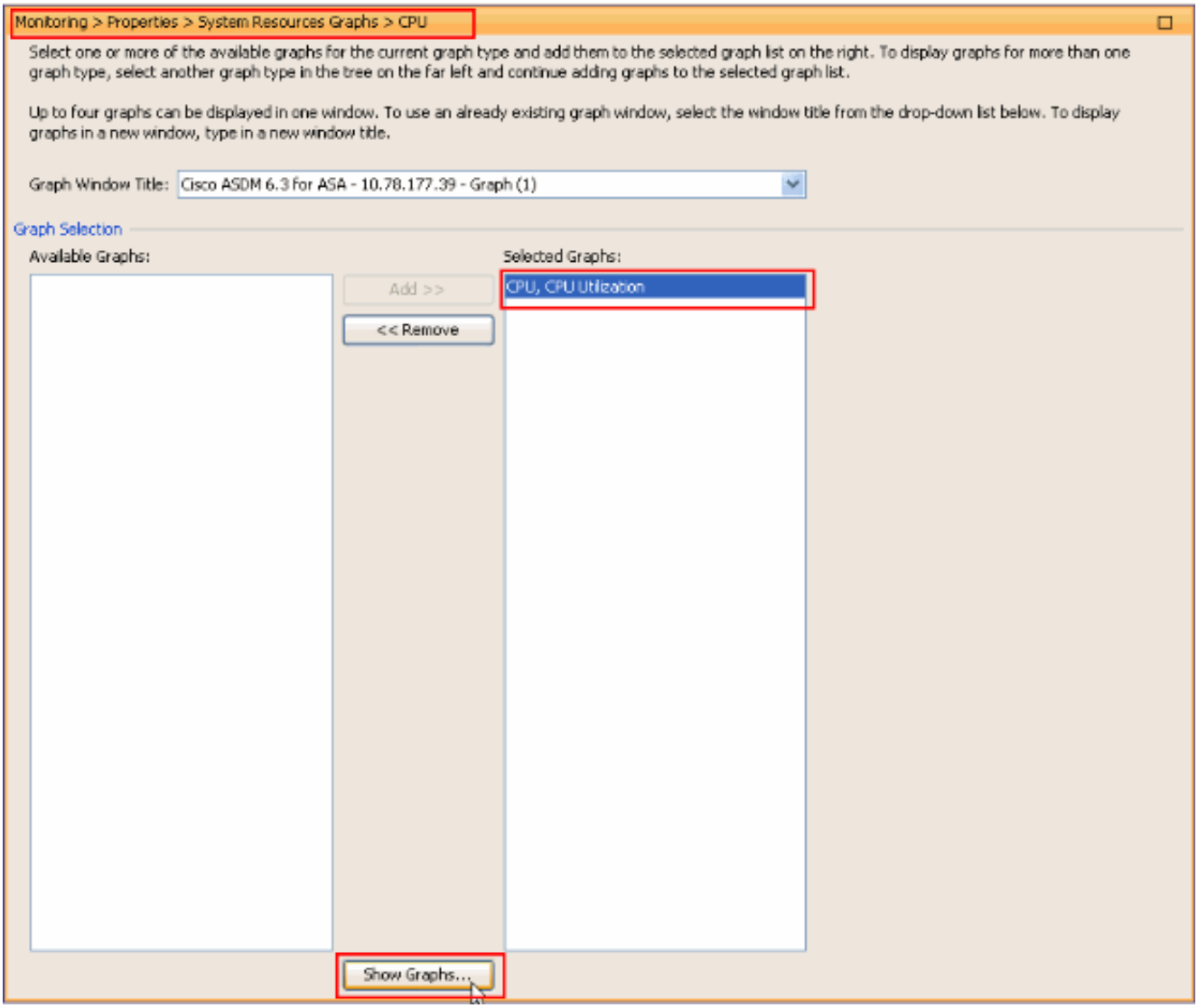
Vendo o USO de CPU no ASDM

Termine estas etapas a fim ver o USO de CPU no ASDM:

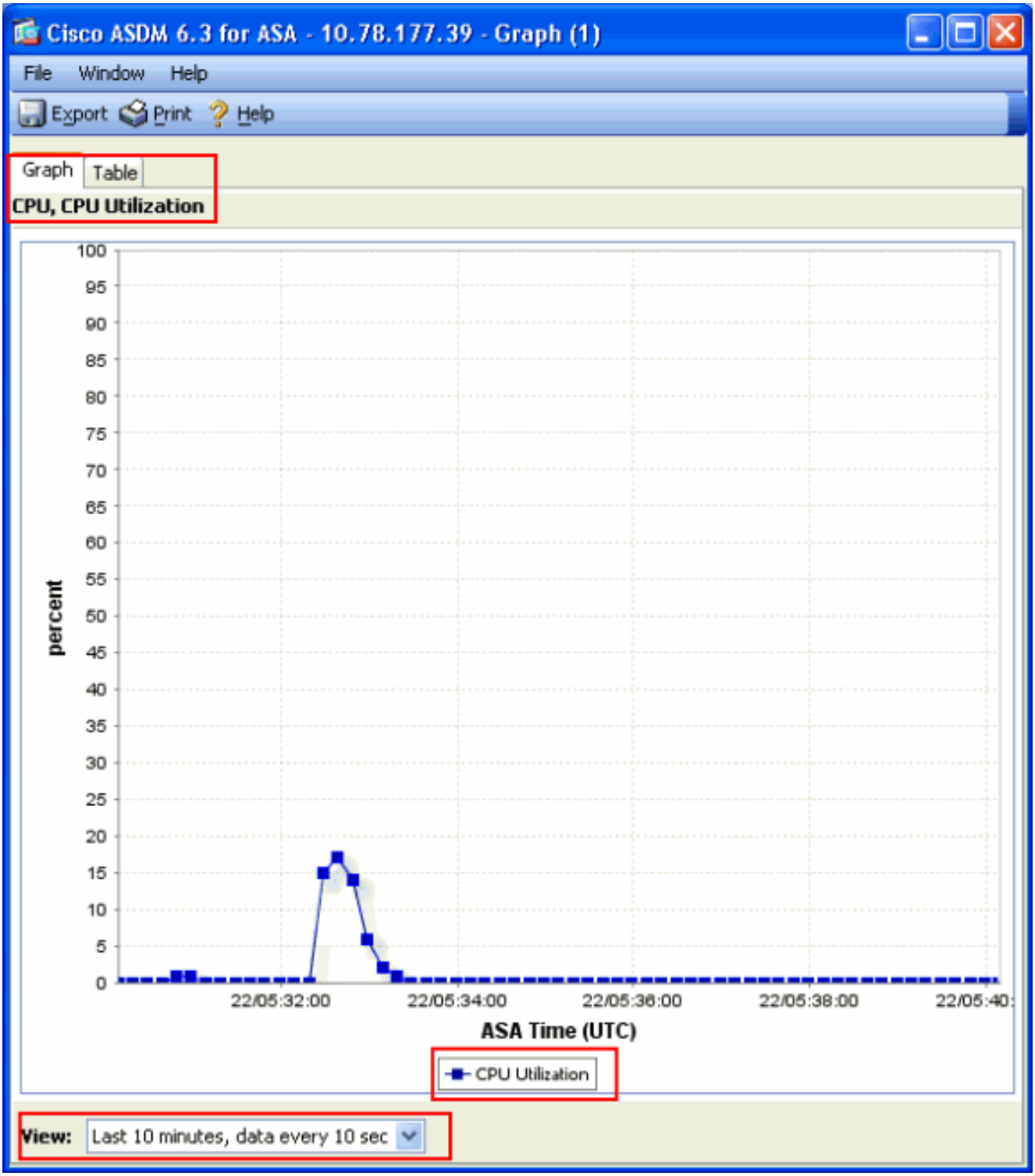
1. Vão à **monitoração > as propriedades > os gráficos dos recursos de sistema > o CPU no** ASDM e escolhem o **título do indicador do gráfico**. Então, escolha os gráficos exigidos da lista de **gráficos disponíveis** e o clique **adiciona** como mostrado.



2. Uma vez que o nome exigido do gráfico é adicionado sob os **gráficos selecionados** secione, clique **gráficos da mostra**.



A imagem seguinte mostra o gráfico do **USO de CPU no** ASDM. As ideias diferentes deste gráfico estão disponíveis e podem ser mudadas selecionando a vista da lista de drop-down da vista. Esta saída pode ser imprimida ou salvar ao computador como necessário.



Descrição da saída

Esta tabela descreve os campos na saída do **uso processador central da mostra**.

Campo	Descrição
Utilização CPU pelos segundos 5	Utilização de CPU durante os últimos cinco segundos
1 minuto	Amostras de uma média de 5 segundos de utilização da CPU no último m

5 minutos	Média de exemplos de 5 segundos de utilização de CPU nos últimos cinc minutos.

show traffic

O comando show traffic mostra quanto tráfego que passa com o ASA durante um período de tempo dado. Os resultados se baseiam no intervalo de tempo desde a emissão do comando. Para resultados precisos, emita o **comando clear traffic** primeiramente e espere então 1-10 minutos antes que você emita o **comando show traffic**. Você poderia igualmente emitir o **comando show traffic** e a espera 1-10 minutos antes que você emita o comando outra vez, mas somente a saída do segundo exemplo é válida.

Você pode usar o **comando show traffic** a fim determinar quanto o tráfego passa com seu ASA. Se você tem interfaces múltiplas, o comando pode ajudá-lo a determinar que relações enviam e recebem a maioria de dados. Para dispositivos ASA com duas relações, a soma do tráfego de entrada e de saída na interface externa deve igualar a soma do tráfego de entrada e de saída na interface interna.

Exemplo

```
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
```

Se você vem perto de ou alcança o throughput taxado em uma de suas relações, você precisa de promover a uma relação mais rápida ou de limitar a quantidade de tráfego em que vai ou fora dessa relação. A falha fazer assim pode conduzir aos pacotes descartado. Como explicado na seção da relação da mostra, você pode examinar os contadores de interface a fim encontrar sobre a taxa de transferência.

show perfmon

O comando show perfmon é usado monitorar a quantidade e os tipos de tráfego que o ASA inspeciona. Este comando é a única maneira de determinar por segundo o número de traduções (xlates) e de conexões (conexão). As conexões são divididas posteriormente em conexões TCP e UDP. Veja a **descrição de Output** para descrições da saída que este comando gerencie.

Exemplo

```
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
```

Descrição da saída

Esta tabela descreve os campos na saída do **perfmon da mostra**.

Campo	Descrição
Xlates	Conversões criadas por segundo
Conexões	Conexões estabelecidas por segundo
Conns TCP	Conexões TCP por segundo
Conns UDP	Conexões UDP por segundo
Acesso URL	URL (Web site) alcançadas por segundo
Req do server URL	Os pedidos enviaram a Websense e ao N2H2 por segundo (exige o comando do **filtro**)
Reparares TCP	Número de pacotes de TCP que o ASA para a frente por segundo
TCPIntercept	Número de pacotes SYN por segundo que excederam ao limite embriônico definido em estático
Reparares HTTP	Número de pacotes destinado à porta 80 por segundo (requer comando fixup protocol
Reparares FTP	Comandos ftp inspecionados por segundo
AAA Authen	Solicitações de autenticação por segundo
Autor AAA	Pedidos de autorização por segundo

Conta AAA	Requisições de contabilização por segundo

show blocks

Junto com o comando show cpu usage, você pode usar o comando show blocks a fim determinar se o ASA está sobrecarregado.

Blocos de Processamento de Pacotes (1550 e 16.384 Bytes)

Quando entra a relação ASA, um pacote está colocado na fila da interface de entrada, passado até o OS, e colocado em um bloco. Para pacotes de Ethernet, os blocos 1550-byte são usados; se o pacote vem dentro em uma placa de Ethernet Gigabit 66 megahertz, os blocos 16384-byte estão usados. O ASA determina se o pacote está permitido ou negado com base no algoritmo de segurança de adaptação (ASA) e processa o pacote completamente à fila de saída na interface externa. Se o ASA não pode apoiar a carga de tráfego, o número de 1550-byte disponível obstrui (ou blocos 16384-byte para 66 megahertz GE) pairos perto de 0 (segundo as indicações da coluna de CNT do comando output). Quando a coluna de CNT bate zero, o ASA tenta atribuir mais blocos, até um máximo de 8192. Se não mais bloco está disponível, o ASA deixa cair o pacote.

Blocos de Failover e Syslog (256 Bytes)

Os blocos de 256 bytes são principalmente usados para mensagens de failover stateful. O ASA ativo gerencie e envia pacotes ao ASA à espera a fim atualizar a tradução e a tabela de conexão. Durante períodos de tráfego intermitente onde as altas taxas de conexões são criadas ou rasgadas para baixo, o número de blocos disponíveis do 256-byte pode deixar cair a 0. Esta gota indica que umas ou várias conexões não estão atualizadas ao ASA à espera. Isto é geralmente aceitável porque a próxima vez em torno da comutação classificada o protocolo trava o xlate ou a conexão que são perdidos. Contudo, se a coluna de CNT para o 256-byte obstrui estadas em ou perto de 0 por períodos de tempo extendido, o ASA não pode prosseguir com a tradução e as tabelas de conexão que são sincronizadas devido ao número de conexões por segundo que o ASA processa. Se isto acontece consistentemente, promova o ASA a um modelo mais rápido.

Os mensagens do syslog mandados do ASA igualmente usam os blocos do 256-byte, mas não são liberados geralmente em tal quantidade que causa uma prostração do pool de bloco do 256-byte. Se a coluna de CNT mostra que o número de blocos do 256-byte está perto de 0, assegure-se de que você não registre na eliminação de erros (nível 7) ao servidor de SYSLOG. Isto é

indicado pela linha de armadilha de logging na configuração ASA. Recomenda-se que você ajusta o registro à notificação (nível 5) ou o abaixa, a menos que você exigir a informação adicional para propósitos de debugging.

Exemplo

```
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
```

Descrição da saída

Esta tabela descreve as colunas na saída dos **blocos da mostra**.

Coluna	Descrição
TAMANHO	E faz sob medida, nos bytes, do pool de bloco. Cada tamanho representa um tipo particular
MAX	Número máximo de blocos disponíveis para o pool de bloco especificado do byte. O número máximo de blocos é cinzelado fora da memória na inicialização. Tipicamente, o número máxi de blocos não muda. A exceção é para o 256- e os blocos 1550-byte, onde a ferramenta de segurança adaptável pode dinamicamente criar mais quando necessária, até um máximo de
BAIXO	Low-water mark. Este número indica o mais baixo número de blocos deste tamanho disponív desde que a ferramenta de segurança adaptável foi posta acima, ou desde que a última limp dos blocos (com o comando clear blocks). Um zero dentro a BAIXA coluna indica um evento precedente onde a memória esteja completa.
CNT	Número atual de blocos disponíveis para esse pool de bloco específico do tamanho. Um zero dentro que a coluna de CNT significa que a memória está completa agora.

Esta tabela descreve os valores da fileira do TAMANHO na saída dos **blocos da mostra**.

Valor do TAMANHO	Descrição
0	Usado por blocos do dupb.
4	Duplica blocos existentes nos aplicativos tais como o DNS, o ISAKMP, a Filtragem URL, o ua o TFTP, e os módulos TCP. Também, este bloco feito sob medida pode ser usado normalme pelo código para enviar pacotes aos direcionadores, etc.
80	Usado no TCP Intercept para gerar pacotes de reconhecimento e para mensagens Hello Messages do Failover.

256	Utilizado para atualizações de failover total, informações de SYSLOG e outras funções TCP. Estes blocos são usados principalmente para mensagens da comutação classificada. A ferramenta de segurança adaptável ativa gerencie e envia pacotes à ferramenta de segurança adaptável à espera para atualizar a tradução e a tabela de conexão. No tráfego intermitente, as altas taxas de conexões são criadas ou rasgadas para baixo, o número de blocos disponíveis pôde deixar cair a 0. Esta situação indica que umas ou várias conexões não estiveram atualizadas à ferramenta de segurança adaptável à espera. O protocolo da comutação classificada trava a tradução ou a conexão faltante a próxima vez. Se a coluna de CNT para o 256-byte obstrui estadas em ou perto de 0 por períodos de tempo extendido, a seguir a ferramenta de segurança adaptável está tendo o problema que mantém a tradução e as tabelas de conexão sincronizadas devido ao número de conexões por segundo que a ferramenta de segurança adaptável está processando. Os mensagens do syslog mandados da ferramenta de segurança adaptável igualmente usam os blocos do 256-byte, mas não são liberados geralmente em tal quantidade para causar uma prostração do pool de bloco do 256-byte. Se a coluna de mostra que o número de blocos do 256-byte está perto de 0, assegure-se de que você não está registrando na eliminação de erros (nível 7) ao servidor de SYSLOG. Isto é indicado pela linha armadilha de logging na configuração adaptável da ferramenta de segurança. Nós recomendamos que você ajusta o registro na notificação (nível 5) ou abaixamo-lo, a menos que você exigir a informação adicional para propósitos de debugging.
1550	Usado para armazenar pacotes de Ethernet para processar através da ferramenta de segurança adaptável. Quando um pacote incorpora uma relação adaptável da ferramenta de segurança, é colocado na fila da interface de entrada, passado até o sistema operacional, e colocado em um bloco. A ferramenta de segurança adaptável determina se o pacote deve ser permitido ou negado com base na política de segurança e processa o pacote completamente à fila de saída na interface externa. Se a ferramenta de segurança adaptável está tendo o problema que prossegue com a carga de tráfego, o número de blocos disponíveis pairará perto de 0 (segundo as indicações da coluna de CNT do comando output). Quando a coluna de CNT é zero, a ferramenta de segurança adaptável tenta atribuir mais blocos, até um máximo de 8192. Se não mais blocos está disponível, a ferramenta de segurança adaptável deixa cair o pacote.
16384	Usado somente para o 64-bit, placas de Ethernet Gigabit 66-MHz (i82543). Veja a descrição 1550 para obter mais informações sobre dos pacotes de Ethernet.
2048	Controle ou guiou os quadros usados para atualizações do controle.

show memory

O comando show memory indica a memória física total (ou RAM) para o ASA, junto com o número de bytes atualmente disponível. A fim usar esta informação, você deve primeiramente compreender como o ASA usa a memória. Quando as botas ASA, ele copiarem o OS do flash em RAM e executarem o OS de RAM (apenas como o Roteadores). Em seguida, o ASA copia a configuração de inicialização do flash e coloca-a em RAM. Finalmente, o ASA atribui RAM a fim criar os poois de bloco discutidos na seção dos blocos da mostra. Uma vez que esta atribuição está completa, o ASA precisa RAM adicional somente se a configuração aumenta em tamanho. Além, o ASA armazena a tradução e as entradas de conexão em RAM.

Durante a operação normal, a memória livre no ASA deve mudar muito pouco, se de todo. Tipicamente, a única vez que você deve ser executado baixo na memória é se você está sob o ataque e os milhares de conexões atravessam o ASA. A fim verificar as conexões, emita o

comando show conn count, que indica a corrente e o número máximo de conexão com o ASA. Se o ASA é executado fora da memória, causa um crash eventualmente. Antes do impacto, você pôde observar mensagens da falha de alocação de memória no Syslog (%ASA-3-211001). Se você é executado fora da memória porque você está sob o ataque, contacte o centro de assistência técnica da Cisco (TAC).

Exemplo

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

Used memory:       228697108 bytes (21%)

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

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

show xlate

O comando show xlate count indica a corrente e o número máximo de traduções com o ASA. Uma tradução é um mapeamento de um endereço interno a um endereço externo e pode ser um mapeamento um a um, tal como o Network Address Translation (NAT), ou um mapeamento many-to-one, tal como a tradução de endereço de porta (PAT). Este comando é um subconjunto do **comando show xlate**, que outputs cada tradução com o ASA. A saída do comando mostra traduções “no uso,” qual refere o número de traduções ativa no ASA quando o comando é emitido; “o mais usado” refere os máximos de traduções que foram considerados nunca no ASA desde que foi posto sobre.

> Nota: Um host único pode ter conexões múltiplas aos vários destinos, mas somente uma tradução. Se a contagem do xlate é muito maior do que o número de anfitriões em sua rede interna, é possível que um de seus host internos esteve comprometido. Se seu host interno foi comprometido, paródias o endereço de origem e envia a pacotes para fora o ASA.

> Nota: Quando a configuração vpnclient é permitida e o host interno manda pedidos DNS, o **comando show xlate** pôde alistar xlates múltiplos para uma tradução estática.

Exemplo

```
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
```

A primeira entrada é uma tradução de endereços da porta TCP para a porta de host (10.1.1.15, 1026) na rede interna à porta de host (192.150.49.1, 1024) na rede externa. A bandeira “r” denota a tradução é uma tradução de endereço de porta. “Eu” bandeiras denoto que a tradução se aplica à endereço-porta interna.

A segunda entrada é uma tradução de endereço de porta UDP para a porta de host (10.1.1.15, 1028) na rede interna à porta de host (192.150.49.1, 1024) na rede externa. A bandeira “r” denota a tradução é uma tradução de endereço de porta. “Eu” bandeiras denoto que a tradução se aplica à endereço-porta interna.

A terceira entrada é uma tradução de endereço de porta ICMP para a host-ICMP-identificação (10.1.1.15, 21505) na rede interna à host-ICMP-identificação (192.150.49.1, 0) na rede externa. A bandeira “r” denota a tradução é uma tradução de endereço de porta. “Eu” bandeiras denoto que a tradução se aplica à endereço-ICMP-identificação interna.

Os campos de endereço interno aparecem como endereços de origem nos pacotes que transversal de mais interface segura a menos interface segura. Inversamente, aparecem como endereços de destino nos pacotes que transversal de menos interface segura a mais interface segura.

show conn count

O comando show conn count mostra a corrente e o número máximo de conexão com o ASA. Uma conexão é um mapeamento de informações de Camada 4 de um endereço interno para um endereço externo. As conexões estão acumuladas quando o ASA recebe um pacote SYN para sessões de TCP ou quando o primeiro pacote em uma sessão de UDP chega. As conexões estão rasgadas abaixo de quando o ASA recebe o pacote ACK final, que ocorre quando o aperto de mão da sessão de TCP se fecha ou quando o intervalo expira na sessão de UDP.

Os contagens de conexão extremamente altas (normal das épocas 50-100) puderam indicar que você está sob o ataque. Emita o **comando show memory** a fim assegurar-se de que o contagem de alta conexão não faça com que o ASA seja executado fora da memória. Se você estiver sob ataque, você pode limitar o número máximo de conexões por entrada estática e também limitar o número máximo de conexões embrionárias. Esta ação protege seus servidores internos, assim que não se tornam oprimidos. Refira referências de comandos do Dispositivos de segurança adaptáveis Cisco ASA série 5500 para mais informação.

Exemplo

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

show interface

O comando show interface pode ajudar a determinar problemas de incompatibilidade bidirecional e problemas de cabo. Pode igualmente fornecer o maior insight se ou não a relação está passada. Se o ASA é executado fora da capacidade de CPU, o número dos blocos 1550-byte paira perto de 0. (olhar nos blocos 16384-byte nos cartões da atuação 66 megahertz.) Um outro indicador é o aumento de “sem bufferes” na relação. A mensagem dos sem bufferes indica que a relação é incapaz de enviar o pacote ao OS ASA porque não há nenhum bloco disponível para o pacote, e o pacote é deixado cair. Se um aumento em níveis do sem buffer ocorre regularmente, emita o **comando show proc cpu** a fim verificar o USO de CPU no ASA. Se o USO de CPU é alto devido a uma carga de tráfego pesado, promova a um ASA mais poderoso que possa segurar a carga.

Quando um pacote entrar em uma interface pela primeira vez, ele será colocado na fila de hardware de entrada. Se a fila de hardware de entrada está completa, o pacote está colocado na fila do software da entrada. O pacote é passado de sua fila de entrada e colocado em um bloco 1550-byte (ou em um bloco 16384-byte em interfaces Gigabit Ethernet 66 megahertz). O ASA então determina a interface de saída para o pacote e coloca o pacote na fila de hardware apropriada. Se a fila de hardware está completa, o pacote está colocado na fila do software de emissor. Se os blocos máximos em qualquer uma das filas do software são grandes, a seguir a relação está passada. Por exemplo, se o 200 Mbps entra o ASA e todos saem uma única relação do 100 Mbps, a fila do software de emissor indica altos números na interface externa, que indica

que a relação não pode segurar o volume de tráfego. Se você experimenta esta situação, promova a uma relação mais rápida.

Exemplo

```
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)
```

Você também deve procurar erros na interface. Se você recebe runts, erros de entrada, CRC, ou erros de frame, é provável que você tem uma incompatibilidade duplex (bidirecional). O cabo pôde ser defeituoso também. Veja ajustes da velocidade e duplexação para obter mais informações sobre das edições frente e verso. Recorde que cada contador de erros representa o número de pacotes que são deixados cair devido a esse erro particular. Se você vê um contador específico que incremente regularmente, o desempenho em seu ASA sofre muito provavelmente, e você deve encontrar a causa de raiz do problema.

Quando você examinar os contadores de interface, note que se a relação é ajustada FULL-frente e verso, você não deve experimentar nenhuns colisões, colisões atrasada, ou pacotes adiados. Inversamente, se a relação é ajustada metade-frente e verso, você deve receber colisões, alguns colisões atrasada, e possivelmente alguns pacotes adiados. O número total de colisões, de colisões atrasada, e de pacotes adiados não deve exceder 10% da soma dos contadores do pacote de entrada e saída. Se suas colisões excedem 10% de seu tráfego total, a seguir o link está utilizado, e você deve promover FULL-frente e verso ou a uma velocidade mais rápida (10 Mbps ao 100 Mbps). Recorde que as colisões do meio de 10% que o ASA deixa cair 10% dos pacotes que atravessam essa relação; cada um desses pacotes deve ser retransmitido.

Refira o **comando interface em** referências de comandos do Dispositivos de segurança adaptáveis Cisco ASA série 5500 para informações detalhadas sobre dos contadores de interface.

show processes

O comando show processes no ASA indica todos os processos ativo que são executado no ASA o comando é executado naquele tempo que. Esta informação é útil a fim determinar que processos recebem demasiado processador central - cronometre e que processos não recebem nenhum processador central - tempo. A fim obter esta informação, emita o **comando show processes** duas vezes; espere aproximadamente 1 minuto entre cada exemplo. Para o processo na pergunta, subtraia o valor de tempo de execução indicado na segunda saída do valor de tempo de execução indicado na primeira saída. Este resultado mostra-lhe quanto processador central - cronometre (nos milissegundos) o processo recebido nesse intervalo do tempo. Note que alguns processos estão programados para ser executado em intervalos particulares, e alguns processos são executado somente quando têm a informação a processar. O processo 577poll tem muito provavelmente o valor de tempo de execução o maior de todos seus processos. Isto é normal porque o processo 577poll vota as interfaces Ethernet a fim considerar se têm algum dados que precisar de ser processado.

> Nota: Um exame de cada processo ASA é fora do âmbito deste documento, mas é mencionado momentaneamente para a integralidade. Refira o comando show processes ASA para obter mais informações sobre dos processos ASA.

Resumo de comandos

Em resumo, use o **comando show cpu usage** a fim identificar a carga que o ASA está abaixo. Recorde que a saída é uma média do corredor; o ASA pode ter uns pontos mais altos do USO de CPU que sejam mascarados pela média do corredor. Uma vez que o ASA alcança o USO de CPU de 80%, a latência com o ASA aumenta lentamente a aproximadamente 90% CPU. Quando o USO de CPU é mais de 90%, o ASA começa deixar cair pacotes.

Se o USO de CPU é alto, use o **comando show processes** a fim identificar os processos que usam a maioria de processador central - tempo. Use esta informação a fim reduzir algum do tempo que é consumido pelos processos intensivos (tais como o registro).

Se o CPU não executa quente, mas você acredita que os pacotes estão deixados cair ainda, use o **comando show interface** a fim verificar a relação ASA para ver se há sem bufferes e colisões, causada possivelmente por uma incompatibilidade duplex (bidirecional). Se os incrementos da contagem do sem buffer, mas o USO de CPU não são baixos, a relação não pode apoiar o tráfego que corre através d.

Se não houver problemas com os buffers, verifique os blocos. Se a coluna de CNT atual na saída dos **blocos da mostra** é próxima a 0 nos blocos 1550-byte (blocos 16384-byte para cartões da atuação 66 megahertz), o ASA deixa cair muito provavelmente pacotes de Ethernet porque é demasiado ocupado. Nesta instância, os aumentos de CPU altos.

Se você experimenta o problema quando você faz novas conexões com o ASA, use o **comando show conn count** a fim verificar o contagem atual de conexões com o ASA.

Se a contagem atual é alta, verifique a **memória da mostra** output a fim assegurar-se de que o ASA não seja executado fora da memória. Se a memória é baixa, investigue a fonte das conexões com o **show conn** ou o **comando show local-host** a fim verificar que sua rede não experimentou um ataque de recusa de serviço.

Você pode usar outros comandos a fim medir a quantidade de tráfego que passa com o ASA. **O comando show traffic** indica os pacotes e os bytes agregados pela relação, e o **perfmon da mostra** quebra o tráfego para baixo nos tipos diferentes que o ASA inspeciona.

Informações Relacionadas

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