

# Monitorar e solucionar problemas de desempenho do ASA

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Conventions](#)

[Solucionar problemas de desempenho](#)

[Configurações de velocidade e dúplex](#)

[Utilização da CPU](#)

[Alta utilização de memória](#)

[PortFast, canalização e entroncamento](#)

[Tradução de Endereço de Rede \(NAT\)](#)

[Syslogs](#)

[SNMP](#)

[Consultas de DNS inverso](#)

[comandos show](#)

[show cpu usage](#)

[show traffic](#)

[show perfmon](#)

[show blocks](#)

[show memory](#)

[show xlate](#)

[show conn count](#)

[show interface](#)

[show processes](#)

[Resumo de comandos](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve os comandos a serem usados para monitorar e solucionar problemas de desempenho de um Cisco Adaptive Security Appliance (ASA).

# Pré-requisitos

## Requisitos

Não existem requisitos específicos para este documento.

## Componentes Utilizados

As informações neste documento são baseadas em um Cisco Adaptive Security Appliance (ASA) que executa a versão 8.3 e posterior.

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 a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

## Solucionar problemas de desempenho

Para solucionar problemas de desempenho, verifique as áreas básicas descritas nesta seção.

---

 **Observação:** se você tiver a saída do `show` comando do seu dispositivo Cisco, poderá usar o [Cisco CLI Analyzer](#) para exibir problemas potenciais e correções. O Cisco CLI Analyzer suporta determinados show comandos. Se você usa o Cisco CLI Analyzer, deve ser um usuário registrado da Cisco, deve estar conectado à sua conta da Cisco e ter o JavaScript habilitado no seu navegador.

---

## Configurações de velocidade e dúplex

O Security Appliance é pré-configurado para detectar automaticamente as configurações de velocidade e duplex em uma interface. No entanto, existem várias situações que podem fazer com que o processo de negociação automática falhe, o que resulta em incompatibilidades de velocidade ou duplex (e problemas de desempenho). Para infraestruturas de rede de missão crítica, a Cisco codifica manualmente a velocidade e o duplex em cada interface para que não haja chance de erro. Esses dispositivos geralmente não se movem, portanto, se você os configurar corretamente, não precisará alterá-los.

Em qualquer dispositivo de rede, a velocidade do link pode ser detectada, mas o duplex deve ser negociado. Se dois dispositivos de rede forem configurados para negociar automaticamente a velocidade e o duplex, eles trocarão quadros (chamados de Fast Link Pulses, ou FLPs) que anunciam suas capacidades de velocidade e duplex. Para um parceiro de enlace que não está ciente, esses pulsos são semelhantes aos quadros regulares de 10 Mbps. Para que um parceiro de link possa decodificar os pulsos, os FLPs contêm todas as configurações de velocidade e duplex que o parceiro de link pode fornecer. A estação que recebe os FLPs reconhece os quadros e os dispositivos concordam mutuamente sobre as configurações de velocidade e duplex mais altas que cada um pode alcançar. Se um dispositivo não suportar negociação automática, o outro dispositivo recebe os FLPs e faz a transição para o modo de detecção paralela. Para detectar a velocidade do parceiro, o dispositivo escuta o comprimento dos pulsos e, em seguida, define a velocidade com base no comprimento. O problema ocorre com a configuração duplex. Como o duplex deve ser negociado, o dispositivo definido como negociação automática não pode determinar as configurações no outro dispositivo, portanto, ele assume como padrão o half-duplex, conforme declarado no padrão IEEE 802.3u.

Por exemplo, se você configurar a interface ASA para negociação automática e conectá-la a um switch que é codificado para 100 Mbps e full-duplex, o ASA enviará FLPs. No entanto, o switch não responde porque é codificado para velocidade e duplex e não participa da negociação automática. Como não recebe resposta do switch, o ASA faz a transição para o modo de detecção paralela e detecta a duração dos pulsos nos quadros enviados pelo switch. Ou seja, o ASA percebe que o switch está definido como 100 Mbps, portanto, ele define a velocidade da interface com base nisso. No entanto, como o switch não troca FLPs, o ASA não pode detectar se o switch pode executar full-duplex, então o ASA define o duplex da interface como half-duplex, conforme declarado no padrão IEEE 803.2u. Como o switch é codificado para 100 Mbps e full-duplex, e o ASA acaba de negociar automaticamente para 100 Mbps e half-duplex (como ele faz), o resultado é uma incompatibilidade duplex que pode causar graves problemas de desempenho.

Uma incompatibilidade de velocidade ou duplex é revelada com mais frequência quando os contadores de erro nas interfaces em questão aumentam. Os erros mais comuns são quadro, verificações de redundância cíclica (CRCs) e runts. Se esses valores forem incrementados na interface, ocorrerá uma incompatibilidade de velocidade/duplex ou um problema de cabeamento. Você deve resolver esse problema antes de continuar.

### **Exemplo**

<#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

Utilização da CPU

Se você observou que a utilização da CPU está alta, conclua estas etapas para solucionar o problema:

- Verifique se a contagem de conexões no show xlate count está baixa.
- Verifique se o bloco de memória está normal.
- Verifique se o número de ACLs é maior.
- Execute o comando show memory detail e verifique se a memória usada pelo ASA é de utilização normal.
- Verifique se as contagens em show processes cpu-hog e show processes memory são normais.
- Qualquer host presente dentro ou fora do Security Appliance pode gerar o tráfego mal-intencionado ou em massa que pode ser um tráfego de broadcast/multicast e causar a alta utilização da CPU. Para resolver esse problema, configure uma lista de acesso para negar o tráfego entre os hosts (fim a fim) e verifique o uso.
- Verifique as configurações de duplex e velocidade nas interfaces ASA. A configuração incompatível com as interfaces remotas pode aumentar a utilização da CPU.

Este exemplo mostra o número mais alto em *erro de entrada* e *sobrecargas* devido à incompatibilidade de velocidade. Use o show interface comando para verificar os erros:

<#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
```

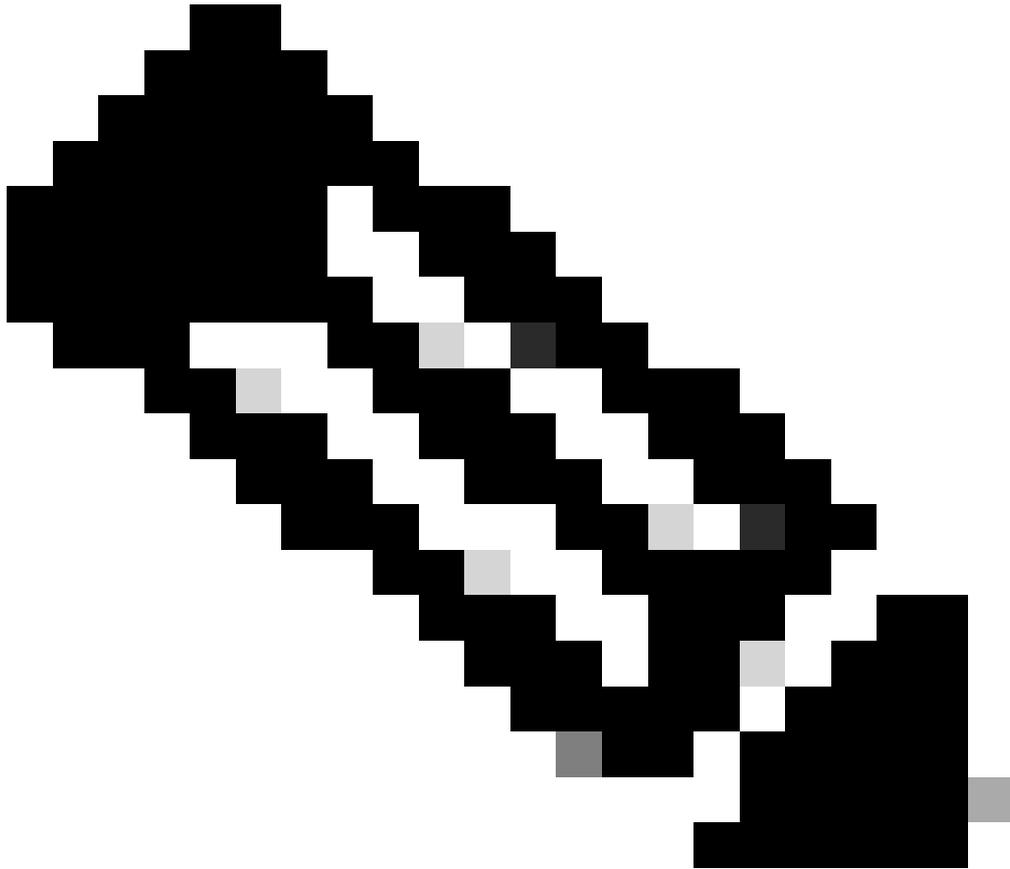
```
7186 input errors, 0 CRC, 0 frame, 7186 overrun
```

```
, 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 esse problema, defina a velocidade como *auto* para a interface correspondente.

---

---

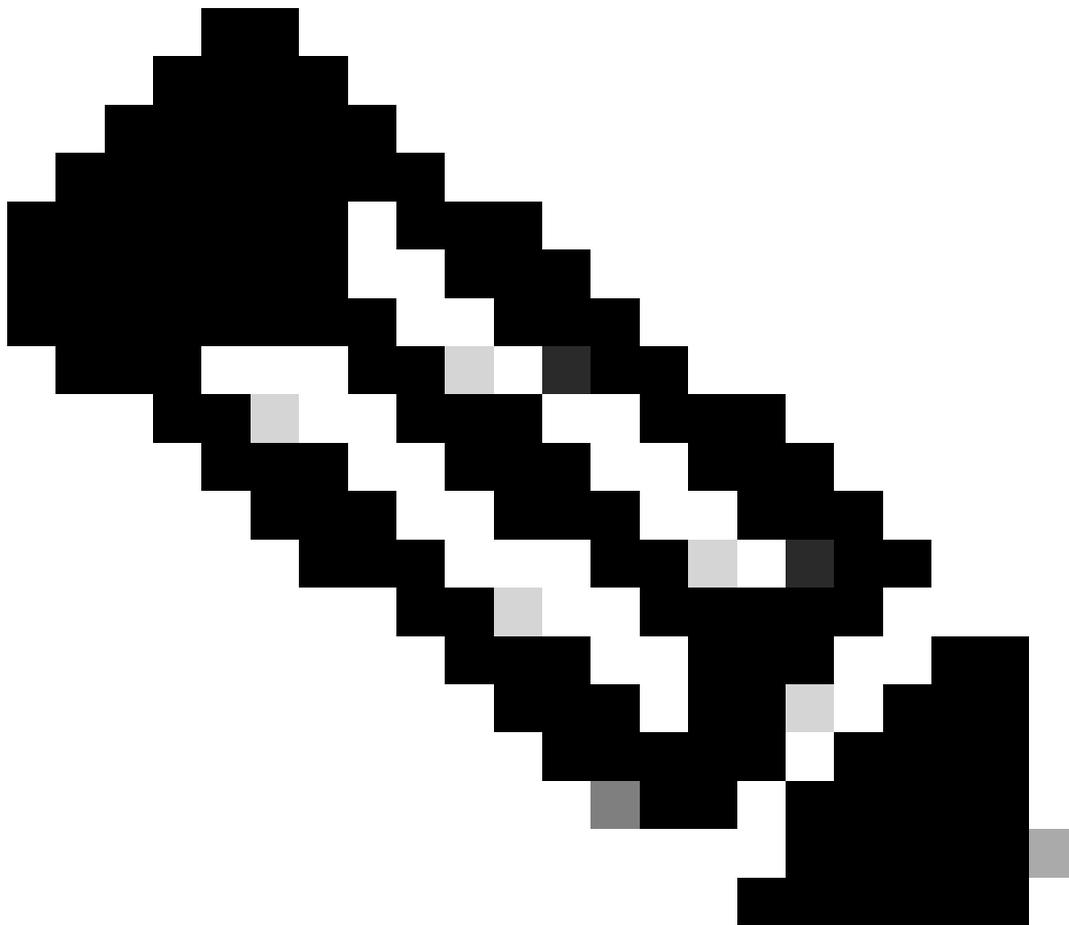


**Observação:** a Cisco recomenda que você habilite o comando `ip verify reverse-path interface` em todas as interfaces. Isso faz com que os pacotes que não têm um endereço de origem válido sejam descartados e resulta em menos uso da CPU. Isso se aplica ao FWSM quando ele enfrenta problemas de alta utilização da CPU.

- 
- Outro motivo para o alto uso da CPU pode ser devido ao excesso de rotas de multicast. Execute o comando `show mroute` para verificar se o ASA recebe muitas rotas multicast.
  - Use o comando `show local-host` para ver se a rede enfrenta um ataque de negação de serviço, o que pode indicar um ataque de vírus na rede.
  - Pode ocorrer alta utilização da CPU devido ao bug da Cisco ID [CSCsq48636](#) . Consulte o bug da Cisco ID [CSCsq48636](#) para obter

mais informações.

---



**Observação:** somente usuários registrados da Cisco podem acessar ferramentas internas da Cisco e informações sobre bugs.

---

 **Observação:** se a solução fornecida anteriormente não resolver o problema, atualize a plataforma ASA com base nos requisitos. Consulte [Cisco Security Modules for Security Appliances](#) para obter mais informações sobre os recursos e capacidades da plataforma Adaptive Security Appliance. Entre em contato com o TAC ([Suporte Técnico da Cisco](#)) para obter mais informações.

---

Alta utilização de memória

Aqui estão algumas causas possíveis e resoluções para alta utilização de memória:

- **Registro de eventos:** O registro de eventos pode consumir muita memória. Para resolver esse problema, instale e registre todos os eventos em um servidor externo, como um Servidor syslog.
- **Vazamento de memória:** um problema conhecido no software do Security Appliance pode levar a um alto consumo de memória. Para resolver esse problema, atualize o software do Security Appliance.
- **Depuração ativada:** A depuração pode consumir grande quantidade de memória. Para resolver esse problema, desabilite a depuração com o comando `undebug all`.
- **Portas de bloqueio:** O bloqueio de portas na interface externa de um Security Appliance faz com que o Security Appliance consuma grandes quantidades de memória para bloquear os pacotes através das portas especificadas. Para resolver esse problema, bloqueie o tráfego ofensivo na extremidade do ISP.
- **Deteção de ameaças:** o recurso de detecção de ameaças consiste em diferentes níveis de estatísticas coletadas para várias ameaças e detecção de ameaças verificadas, que determina quando um host executa uma verificação. **Desative** esse recurso para consumir menos memória.

PortFast, canalização e entroncamento

Por padrão, muitos switches, como os switches da Cisco que executam o sistema operacional Catalyst (OS), são projetados para serem dispositivos plug-and-play. Como tal, muitos dos parâmetros de porta padrão não são desejáveis quando um ASA está conectado ao switch. Por exemplo, em um switch que executa o Catalyst OS, a canalização padrão é definida como Automático, o entroncamento é definido como Automático e o PortFast é desabilitado. Se você conectar um ASA a um switch que executa o Catalyst OS, desative a canalização, desative o entroncamento e ative o PortFast.

A canalização, também conhecida como Fast EtherChannel ou Giga EtherChannel, é usada para ligar duas ou mais portas físicas em um grupo lógico para aumentar o throughput geral através do link. Quando uma porta é configurada para canalização automática, ela envia quadros de Protocolo de Agregação de Portas (PAgP - Port Aggregation Protocol) quando o link se torna ativo para determinar se ela faz parte de um canal. Esses quadros podem causar problemas se o outro dispositivo tentar negociar automaticamente a velocidade e o duplex do link. Se a canalização na porta estiver definida como Automática, isso também resultará em um atraso adicional de aproximadamente 3 segundos antes que a porta comece a encaminhar o tráfego depois que o link estiver ativo.

---

 **Observação:** nos Catalyst XL Series Switches, a canalização não é definida como Automática por padrão. Por esse motivo, você deve desativar a canalização em qualquer porta do switch que se conecte a um ASA.

---

O entroncamento, também conhecido pelos protocolos de entroncamento comuns Inter-Switch Link (ISL) ou Dot1q, combina várias LANs virtuais (VLANs) em uma única porta (ou link). O entroncamento geralmente é utilizado entre dois Switches quando ambos têm mais de uma VLAN definida. Quando uma porta é configurada para entroncamento automático, ela envia quadros de Dynamic Trunking Protocol (DTP) quando o link é ativado para determinar se a porta à qual ela se conecta deseja fazer o entroncamento. Esses quadros de DTP podem causar problemas com a negociação automática do link. Se o entroncamento estiver definido como Automático em uma porta de switch, ele adicionará um atraso adicional de aproximadamente 15 segundos antes que a porta comece a encaminhar o tráfego depois que o link estiver ativo.

O PortFast, também conhecido como Fast Start, é uma opção que informa ao switch que um dispositivo de Camada 3 está conectado a partir de uma porta de switch. A porta não aguarda o padrão de 30 segundos (15 segundos para escutar e 15 segundos para aprender); em vez disso, essa ação faz com que o switch coloque a porta no estado forwarding imediatamente após o link ser ativado. É importante entender que quando você habilita o PortFast, o spanning tree não é desabilitado. A árvore de abrangência ainda está ativa nessa porta. Quando você habilita o PortFast, o switch é informado apenas de que não há outro switch ou hub (dispositivo somente de Camada 2) conectado na outra extremidade do link. O switch ignora o atraso normal de 30 segundos enquanto tenta determinar se um loop de Camada 2 resultará se ativar essa porta. Depois que o link é ativado, ele ainda participa do spanning tree. A porta envia BPDUs (unidades de dados de pacote de ponte) e o switch ainda escuta BPDUs nessa porta. Por esses motivos, é recomendável habilitar o PortFast em qualquer porta de switch que se conecte a um ASA.

---

 **Observação:** as versões 5.4 e posteriores do Catalyst OS incluem o `set port host <mod>/<port>` comando que permite usar um único comando para desativar a canalização, desativar o entroncamento e ativar o PortFast.

---

## Tradução de Endereço de Rede (NAT)

Cada sessão de NAT ou de Sobrecarga de NAT (PAT) recebe um slot de conversão conhecido como *xlate*. Esses *xlates* podem persistir mesmo depois que você faz alterações nas regras de NAT que os afetam. Isso pode levar a uma redução dos slots de conversão ou a um comportamento inesperado ou a ambos pelo tráfego que passa pela conversão. Esta seção explica como exibir e limpar extratos no Security Appliance.

---

 **Cuidado:** uma interrupção momentânea do fluxo de todo o tráfego através do dispositivo pode ocorrer quando você limpa globalmente os *xlates* no Security Appliance.

---

Exemplo de configuração ASA para PAT que usa o endereço IP da interface externa:

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

O tráfego que flui pelo Security Appliance provavelmente passa pelo NAT. Para visualizar as conversões que estão em uso no Security Appliance, emita o comando `show xlate` :

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

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

Os slots de tradução podem persistir após as principais alterações. Para limpar os slots de conversão atuais no Security Appliance, execute o comando `clear xlate`:

```
<#root>
```

```
Ciscoasa#
```

```
clear xlate
```

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

```
0 in use, 1 most used
```

O comando `clear xlate` limpa toda a conversão dinâmica atual da tabela `xlate`. Para limpar uma tradução IP específica, você pode usar o comando `clear xlate` com a palavra-chave global [ip address].

Aqui está um exemplo de configuração ASA 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 a saída `show xlate` da conversão de 10.2.2.2 interno em 10.10.10.10 global externo:

```
<#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
```

Limpe a conversão para o endereço IP global 10.10.10.10:

```
<#root>
```

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

Neste exemplo, a conversão de 10.2.2.2 para 10.10.10.10 global externo foi removida:

```
<#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
```

Syslogs

Os Syslogs permitem que você solucione problemas no ASA. A Cisco oferece um Servidor syslog gratuito para Windows NT chamado ASA Firewall Syslog Server (PFSS). Você pode baixar o PFSS do [Suporte técnico e downloads da Cisco](#).

Vários outros fornecedores, como o, oferecem servidores syslog para várias plataformas Windows, como Windows 2000 e Windows XP. A maioria das máquinas UNIX e Linux tem servidores syslog instalados por padrão.

Quando você configura o Servidor syslog, configure o ASA para enviar logs para ele.

Por exemplo:

```
<#root>
```

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

---

 **Observação:** este exemplo configura o ASA para enviar Debugging (nível 7) e syslogs mais críticos para o Servidor syslog. Como esses logs do ASA são os mais detalhados, use-os somente quando solucionar um problema. Para operação normal, configure o nível de registro para Aviso (nível 4) ou Erro (nível 3).

---

Se ocorrer um problema de desempenho lento, abra o syslog em um arquivo de texto e procure o endereço IP de origem associado ao problema de desempenho. (Se você usa UNIX, pode **grep** através do syslog para o endereço IP de origem.) Verifique as mensagens que indicam que o servidor externo tentou acessar o endereço IP interno na porta TCP 113 (para Identification Protocol ou Ident), mas o ASA negou o pacote. A mensagem deve ser semelhante a este exemplo:

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

Se você receber essa mensagem, emita o `service resetinbound` comando para o ASA. O ASA não descarta pacotes silenciosamente; em vez disso, esse comando faz com que o ASA redefina imediatamente qualquer conexão de entrada que seja negada pela política de segurança. O servidor não espera que o pacote Ident exceda o tempo limite de sua conexão TCP; em vez disso, ele recebe imediatamente um pacote de redefinição.

## SNMP

Um método recomendado para as implantações empresariais é monitorar o desempenho do Cisco ASA com SNMP. O Cisco ASA suporta isso com as versões 1, 2c e 3 do SNMP.

Você pode configurar o Security Appliance para enviar interceptações a um Network Management Server (NMS) ou pode usar o NMS para procurar as MIBs no Security Appliance. As MIBs são um conjunto de definições e o Security Appliance mantém um banco de dados de valores para cada definição. Para obter mais informações sobre isso, consulte o [Guia de Configuração do Cisco ASA 5500 Series com CLI 8.4 e 8.6](#).

Todas as MIBs suportadas para o Cisco ASA podem ser encontradas na lista de suporte MIB do ASA. Nessa lista, esses MIBs são úteis quando você monitora o desempenho:

- CISCO-FIREWALL-MIB ---- contém objetos úteis para failover.
- CISCO-PROCESS-MIB ---- Contém Objetos úteis para Utilização da CPU.
- CISCO-MEMORY-POOL-MIB ---- Contém objetos úteis para objetos de memória.

#### Consultas de DNS inverso

Se o desempenho do ASA estiver lento, verifique se você tem registros de DNS PTR (Domain Name System Pointer), também conhecidos como registros de pesquisa de DNS reverso, no servidor DNS autoritativo para os endereços externos que o ASA usa. Isso inclui qualquer endereço no pool NAT (Network Address Translation) global (ou a interface externa ASA, se você sobrecarregar a interface), qualquer endereço estático e o endereço interno (se você não usar a NAT com eles). Alguns aplicativos, como os servidores de FTP e Telnet, podem usar pesquisas de DNS reverso para determinar de onde o usuário vem e se ele é um host válido. Se a pesquisa de DNS reverso não resolver, o desempenho será degradado à medida que o tempo da solicitação se esgotar.

Para garantir que exista um registro PTR para esses hosts, emita o comando `nslookup` do seu PC ou máquina UNIX; inclua o endereço IP global que você usa para se conectar à Internet.

#### Exemplo

```
<#root>
```

```
% nslookup 192.168.219.25  
10.219.133.198.in-addr.arpa name = www.cisco.com.
```

Você deve receber uma resposta de volta com o nome DNS do dispositivo atribuído a esse endereço IP. Se você não receber uma resposta, entre

em contato com a pessoa que controla seu DNS para solicitar a adição de registros PTR para cada um de seus endereços IP globais.

## Overruns na Interface

Se você tiver uma intermitência de tráfego, os pacotes descartados poderão ocorrer se a intermitência exceder a capacidade de buffer do buffer FIFO na placa de rede e nos buffers do anel de recepção. Se você ativar os quadros de pausa para o controle de fluxo, esse problema poderá ser aliviado. Os quadros Pause (XOFF) e XON são gerados automaticamente pelo hardware da placa de rede com base no uso do buffer FIFO. Um quadro de pausa é enviado quando o uso do buffer excede a marca d'água superior. Para habilitar os quadros de pausa (XOFF) para controle de fluxo, use este comando:

```
<#root>
```

```
hostname(config)#
```

```
interface tengigabitethernet 1/0
```

```
hostname(config-if)#
```

```
flowcontrol send on
```

comandos show

```
show cpu usage
```

O comando `show cpu usage` é usado para determinar a carga de tráfego colocada na CPU do ASA. Durante horários de pico de tráfego, surtos de rede ou ataques, o uso da CPU pode aumentar.

O ASA tem uma única CPU para processar uma variedade de tarefas; por exemplo, ele processa pacotes e imprime mensagens de depuração no console. Cada processo tem sua própria finalidade e alguns processos exigem mais tempo de CPU do que outros. A criptografia é provavelmente o processo com maior uso da CPU, portanto, se o seu ASA passar muito tráfego por túneis criptografados, você deverá considerar um ASA mais rápido, um concentrador VPN dedicado, como o VPN 3000. O VAC descarrega a criptografia e a descryptografia da CPU ASA e a executa no hardware da placa. Isso permite que o ASA criptografe e descryptografe 100 Mbps de tráfego com 3DES (criptografia de 168 bits).

O registro é outro processo que pode consumir grande quantidade de recursos do sistema. Por isso, é recomendável desabilitar o console, o monitor e o registro de buffer no ASA. Você pode habilitar esses processos ao solucionar um problema, mas desabilitá-los para a operação diária, especialmente se ficar sem capacidade de CPU. Também é sugerido que o registro de syslog ou do protocolo de gerenciamento de rede simples (SNMP - Simple Network Management Protocol) (histórico de registro) deve ser definido como nível 5 (Notificação) ou inferior. Além disso, você pode desativar IDs de mensagens de syslog específicos com o no logging message <syslog\_id> comando.

O Cisco Adaptive Security Device Manager (ASDM) também fornece um gráfico na Monitoring guia que permite exibir o uso da CPU do ASA com o tempo. Você pode usar esse gráfico para determinar a carga em seu ASA.

O **show cpu usage** comando pode ser usado para exibir estatísticas de utilização da CPU.

### Exemplo

```
<#root>
```

```
Ciscoasa#
```

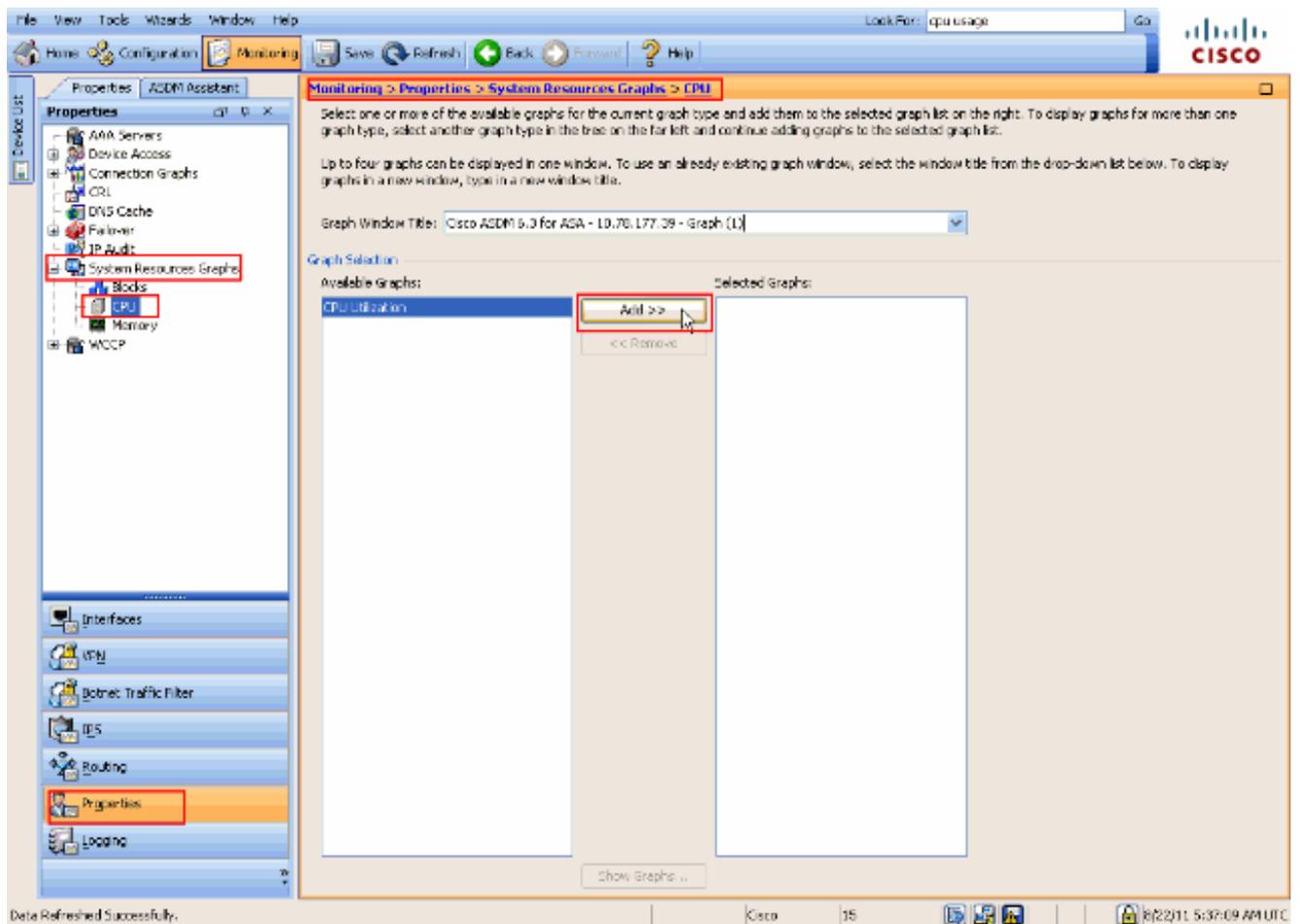
```
show cpu usage
```

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

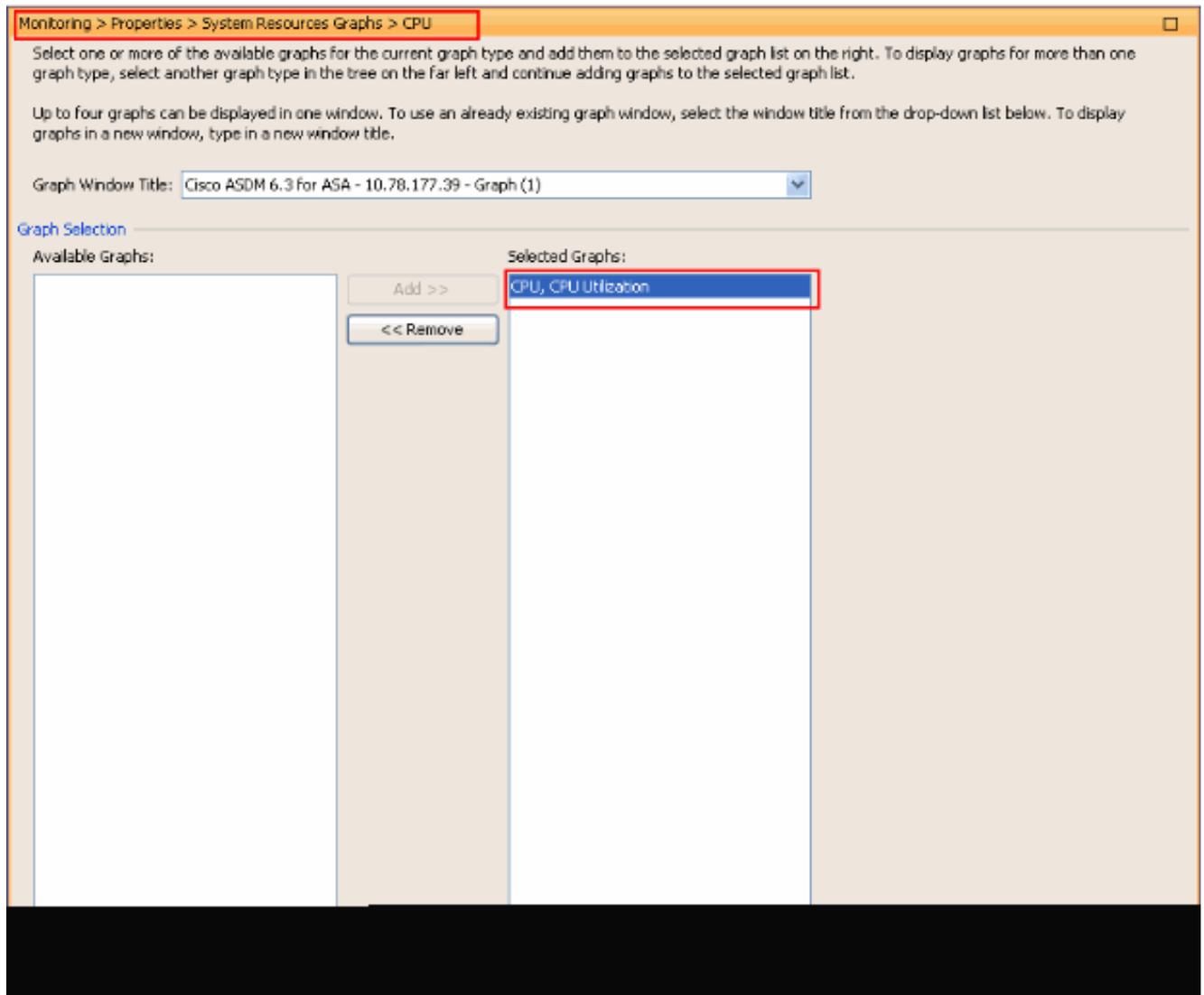
### Exibir Uso da CPU no ASDM

Conclua estes passos para exibir o uso da CPU no ASDM:

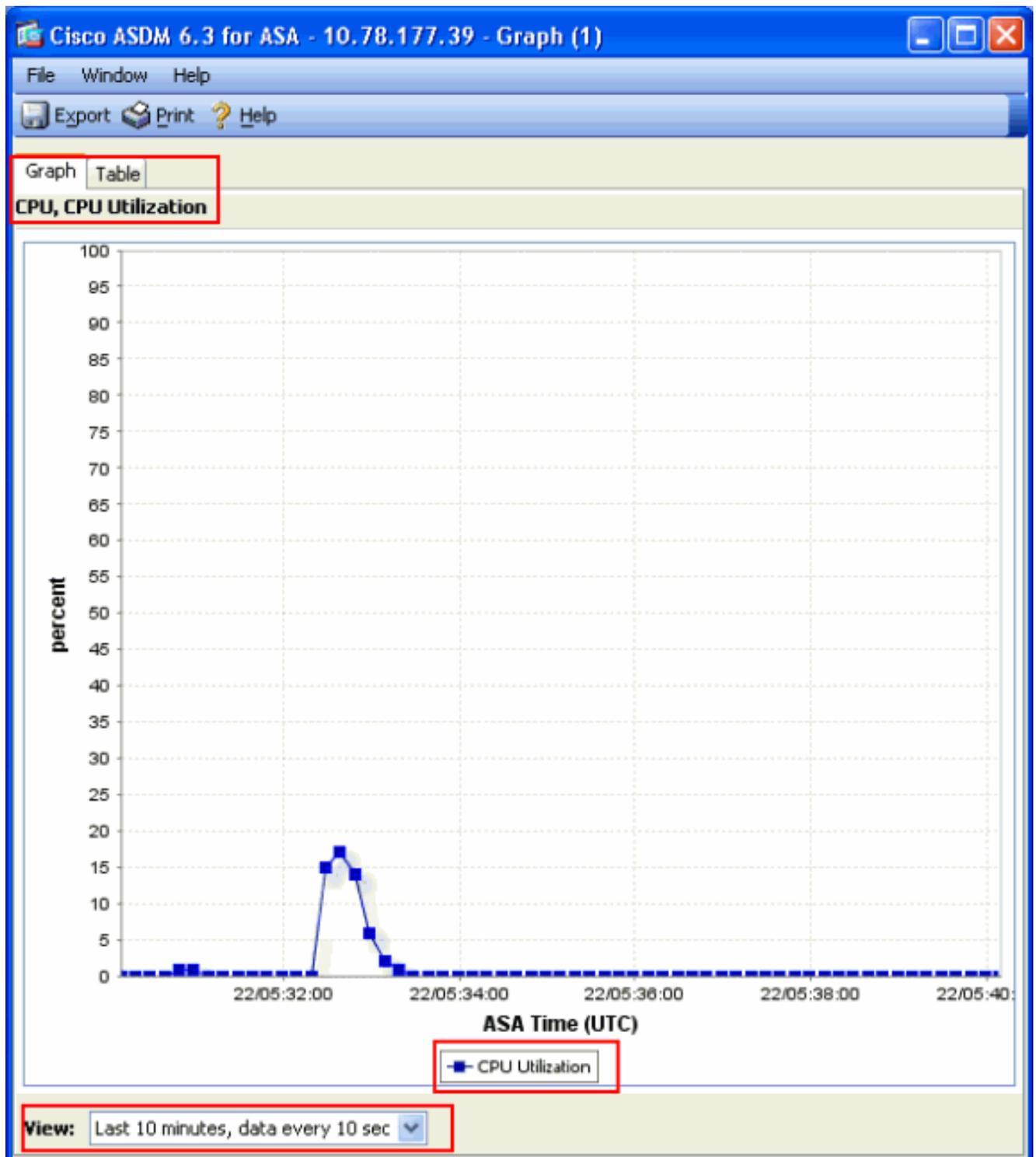
- Vá para Monitoring > Properties > System Resources Graphics > CPU no ASDM e escolha o **Título da Janela Gráfico**. Em seguida, escolha os gráficos necessários na lista **Gráficos disponíveis** e clique em **Adicionar** conforme mostrado.



- Depois que o nome do gráfico necessário for adicionado na seção **Gráficos selecionados**, clique em **Mostrar gráficos**.



A próxima imagem mostra o gráfico **CPU Usage** no ASDM. Diferentes exibições desse gráfico estão disponíveis e podem ser alteradas quando a exibição na lista suspensa Exibir é selecionada. Essa saída pode ser impressa ou salva no computador conforme necessário.



#### Descrição da saída

Esta tabela descreve os campos na **show cpu usage** saída.

Campo	Descrição
Utilização da CPU por 5 segundos	Utilização de CPU durante os últimos cinco segundos
1 minuto	Amostras de uma média de 5 segundos de utilização da CPU no último minuto
5 minutos	Média de exemplos de 5 segundos de utilização de CPU nos últimos cinco minutos.

show traffic

O comando `show traffic` mostra a quantidade de tráfego que passa pelo ASA durante um determinado período. Os resultados se baseiam no intervalo de tempo desde a emissão do comando. Para obter resultados precisos, emita o comando **clear traffic** primeiro e, em seguida, aguarde de 1 a 10 minutos antes de emitir o `show traffic` comando. Você também pode emitir o comando `show traffic` e esperar de 1 a 10 minutos antes de emitir o comando novamente, mas apenas a saída da segunda instância é válida.

Você pode usar o comando `show traffic` para determinar a quantidade de tráfego que passa pelo ASA. Se você tiver várias interfaces, o comando poderá ajudá-lo a determinar quais interfaces enviam e recebem mais dados. Para dispositivos ASA com duas interfaces, a soma do tráfego de entrada e saída na interface externa deve ser igual à soma do tráfego de entrada e saída na interface interna.

### Exemplo

```
<#root>
```

```
Ciscoasa#
```

```
show traffic
```

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

Se você se aproximar ou alcançar o throughput classificado em uma de suas interfaces, precisará atualizar para uma interface mais rápida ou

limitar a quantidade de tráfego que entra ou sai dessa interface. Se isso não for feito, os pacotes podem ser descartados. Como explicado na **show interface** seção, você pode examinar os contadores de interface para descobrir o throughput.

show perfmon

O comando `show perfmon` é usado para monitorar a quantidade e os tipos de tráfego que o ASA inspeciona. Esse comando é a única maneira de determinar o número de conversões (xlates) e conexões (conn) por segundo. As conexões são divididas posteriormente em conexões TCP e User Datagram Protocol (UDP). Consulte **Descrição da saída** para obter descrições da saída gerada por esse comando.

### Exemplo

```
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
```

### Descrição da saída

Esta tabela descreve os campos na `show perfmon` saída.

Campo	Descrição
Xlates	Conversões criadas por segundo
Conexões	Conexões estabelecidas por segundo
Conns TCP	Conexões TCP por segundo
Conexões UDP	Conexões UDP por segundo
Acesso à URL	URLs (sites) acessados por segundo

Solicitação de servidor de URL	Solicitações enviadas à Websense e N2H2 por segundo (requer <code>filter</code> comando)
Correção de TCP	Número de pacotes TCP encaminhados pelo ASA por segundo
InterceptaçãoTCPI	Número de pacotes SYN por segundo que excederam ao limite embriônico definido em um estático
Correção de HTTP	Número de pacotes destinados à porta 80 por segundo (requer <code>fixup</code> <code>protocol http</code> comando)
Correção de FTP	Comandos FTP inspecionados por segundo
AAA Authen	Solicitações de autenticação por segundo
Autor AAA	Solicitações de autorização por segundo
Conta AAA	Requisições de contabilização por segundo

`show blocks`

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

#### **Blocos de pacotes (1550 e 16384 bytes)**

Quando ele entra na interface ASA, um pacote é colocado na fila da interface de entrada, passado para o SO e colocado em um bloco. Para pacotes Ethernet, os blocos de 1550 bytes são usados; se o pacote vier em uma placa Gigabit Ethernet de 66 MHz, os blocos de 16384 bytes serão usados. O ASA determina se o pacote é permitido ou negado com base no ASA (Adaptive Security Algorithm) e processa o pacote para a fila de saída na interface de saída. Se o ASA não puder suportar a carga de tráfego, o número de blocos de 1550 bytes disponíveis (ou blocos de 16384 bytes para GE de 66 MHz) passa perto de 0 (como mostrado na coluna CNT da saída do comando). Quando a coluna CNT atingir zero, o ASA tentará alocar mais blocos, até um máximo de 8192. Se não houver mais blocos disponíveis, o ASA descartará 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 gera e envia pacotes para o ASA em espera para atualizar a tabela de conversão e conexão. Durante períodos de tráfego intermitente em que altas taxas de conexões são criadas ou interrompidas, o número de blocos de 256 bytes disponíveis pode cair para 0. Essa queda indica que uma ou mais conexões não estão atualizadas para o ASA em standby. Isso é geralmente aceitável porque na próxima vez em que o protocolo de failover stateful detecta o xlate ou a conexão que é perdida. No entanto, se a coluna CNT para blocos de 256 bytes permanecer em ou perto de 0 por longos períodos, o ASA não poderá acompanhar as tabelas de conversão e conexão que estão sincronizadas devido ao número de conexões por segundo que o ASA processa. Se isso acontecer de forma consistente, atualize o ASA para um modelo mais rápido.

As mensagens de syslog enviadas do ASA também usam os blocos de 256 bytes, mas geralmente não são liberadas em uma quantidade que cause uma redução do pool de blocos de 256 bytes. Se a coluna CNT mostrar que o número de blocos de 256 bytes está próximo a 0, certifique-se de não registrar em Depuração (nível 7) no Servidor syslog. Isso é indicado pela linha de armadilha de registro na configuração do ASA. É recomendável definir o registro como Notificação (nível 5) ou inferior, a menos que você precise de informações adicionais para fins de depuração.

### Exemplo

```
<#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
```

### Descrição da saída

Esta tabela descreve as colunas na show blocks saída.

Coluna	Descrição
TAMANHO	E Tamanho, em bytes, do pool de blocos. Cada tamanho representa um tipo

	específico
MAX	Número máximo de blocos disponíveis para o pool de blocos de bytes especificado. O número máximo de blocos é gravado fora da memória na inicialização. Normalmente, o número máximo de blocos não é alterado. A exceção é para os blocos de 256 e 1550 bytes, onde o aplicativo de segurança adaptável pode criar dinamicamente mais quando necessário, até um máximo de 8192.
BAIXO	Marca de água baixa. Esse número indica o menor número de blocos desse tamanho disponíveis desde que o aplicativo de segurança adaptável foi ligado ou desde a última limpeza dos blocos (com o comando clear blocks ). Um zero na coluna LOW indica um evento anterior em que a memória estava cheia.
CNT	Número atual de blocos disponíveis para esse pool de blocos de tamanho específico. Um zero na coluna CNT significa que a memória está cheia agora.

Esta tabela descreve os valores da linha SIZE na show blocks saída.

Valor do TAMANHO	Descrição
0	Usado por blocos dupb.
4	Duplica blocos existentes em aplicativos como DNS, ISAKMP, filtragem de URL, uauth, TFTP e módulos TCP. Além disso, esse bloco do tamanho pode ser usado normalmente pelo código para enviar pacotes aos drivers, e assim por diante.
80	Usado na interceptação TCP para gerar pacotes de confirmação e mensagens de saudação de failover.
256	Usado para atualizações de failover stateful, registro de syslog e outras funções TCP. Esses blocos são usados principalmente para mensagens de failover stateful. O aplicativo de segurança adaptável ativo gera e envia pacotes ao aplicativo de segurança adaptável em standby para atualizar a tabela de conversão e conexão. No tráfego intermitente, onde altas taxas de conexões são criadas ou interrompidas, o número de blocos disponíveis pode cair para 0. Essa situação indica que uma ou mais conexões não foram atualizadas para o aplicativo de segurança adaptável em

	<p>espera. O protocolo de failover stateful detecta a conversão ou a conexão perdida na próxima vez. Se a coluna CNT para blocos de 256 bytes permanecer igual a ou próximo a 0 por períodos prolongados, o aplicativo de segurança adaptável se esforçará para manter as tabelas de conversão e conexão sincronizadas devido ao número de conexões por segundo que o aplicativo de segurança adaptável processa. As mensagens de syslog enviadas do aplicativo de segurança adaptável também usam blocos de 256 bytes, mas geralmente não são liberadas nessa quantidade para causar uma redução do pool de blocos de 256 bytes. Se a coluna CNT mostrar que o número de blocos de 256 bytes está próximo a 0, certifique-se de não estar registrando em Depuração (nível 7) no Servidor syslog. Isso é indicado pela linha logging trap na configuração do aplicativo de segurança adaptável. Recomendamos que você defina o registro em Notificação (nível 5) ou inferior, a menos que precise de informações adicionais para fins de depuração.</p>
1550	<p>Usado para armazenar pacotes Ethernet a serem processados por meio do aplicativo de segurança adaptável. Quando um pacote entra em uma interface do aplicativo de segurança adaptável, ele é colocado na fila da interface de entrada, passado para o sistema operacional e colocado em um bloco. O aplicativo de segurança adaptável determina se o pacote deve ser permitido ou negado com base na política de segurança e processa o pacote para a fila de saída na interface de saída. Se o aplicativo de segurança adaptável se esforçar para acompanhar a carga de tráfego, o número de blocos disponíveis poderá pairar próximo a 0 (como mostrado na coluna CNT da saída do comando). Quando a coluna CNT é zero, o aplicativo de segurança adaptável tenta alocar mais blocos, até um máximo de 8192. Se não houver mais blocos disponíveis, o aplicativo de segurança adaptável descartará o pacote.</p>
16384	<p>Usado apenas para as placas Gigabit Ethernet (i82543) de 64 bits e 66 MHz. Consulte a descrição para 1550 para obter mais informações sobre pacotes Ethernet.</p>
2048	<p>Quadros de controle ou guiados usados para atualizações de controle.</p>

show memory

O comando `show memory` exibe a memória física total (ou RAM) para o ASA, juntamente com o número de bytes atualmente disponíveis. Para usar essas informações, você deve primeiro entender como o ASA usa a memória. Quando o ASA é inicializado, ele copia o SO da Flash para a RAM e executa o SO da RAM (assim como os roteadores). Em seguida, o ASA copia a configuração de inicialização do Flash e a coloca na RAM. Finalmente, o ASA aloca a RAM para criar os conjuntos de blocos discutidos na seção `show blocks`. Uma vez concluída essa alocação, o ASA precisará de RAM adicional somente se a configuração aumentar em tamanho. Além disso, o ASA armazena as entradas de conversão e conexão na RAM.

Durante a operação normal, a memória livre no ASA deve mudar muito pouco, se for o caso. Normalmente, a única vez que você precisa ficar com pouca memória é se estiver sob ataque e centenas de milhares de conexões passarem pelo ASA. Para verificar as conexões, execute o comando `show conn count`, que exibe o número atual e máximo de conexões através do ASA. Se o ASA ficar sem memória, ele acabará travando. Antes do travamento, você pode observar mensagens de falha de alocação de memória no syslog (%ASA-3-211001).

Se você ficar sem memória porque está sendo atacado, entre em contato com a equipe do [Suporte Técnico da Cisco](#).

## Exemplo

```
<#root>
```

```
Ciscoasa#
```

```
show memory
```

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

```
show xlate
```

O comando `show xlate count` exibe o número atual e máximo de conversões por meio do ASA. Uma conversão é um mapeamento de um endereço interno para um endereço externo e pode ser um mapeamento um para um, como a Conversão de Endereço de Rede (NAT), ou um mapeamento muitos para um, como a Conversão de Endereço de Porta (PAT). Esse comando é um subconjunto do comando `show xlate`, que gera a saída de cada conversão através do ASA. A saída do comando mostra conversões "em uso", que se refere ao número de conversões ativas no ASA quando o comando é emitido; "mais usado" se refere às conversões máximas que já foram vistas no ASA desde que ele foi ligado.

---

 **Observação:** Um único host pode ter várias conexões para vários destinos, mas apenas uma conversão. Se a contagem `xlate` for muito maior que o número de hosts na rede interna, é possível que um dos hosts internos tenha sido comprometido. Se o seu host interno foi comprometido, ele falsifica o endereço de origem e envia pacotes pelo ASA.

---

---

 **Observação:** quando a configuração do `vpnclient` é ativada e o host interno envia solicitações DNS, o comando `show xlate` pode listar vários `xlates` para uma conversão estática.

---

## Exemplo

```
<#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
```

A primeira entrada é uma Conversão de Endereço de Porta TCP para host-porta (10.1.1.15, 1026) na rede interna para host-porta (192.168.49.1, 1024) na rede externa. O flag "r" indica que a conversão é uma Conversão de endereço de porta. Os flags "i" indicam que a conversão se aplica à porta de endereço interna.

A segunda entrada é uma Conversão de Endereço de Porta UDP para host-porta (10.1.1.15, 1028) na rede interna para host-porta (192.168.49.1, 1024) na rede externa. O flag "r" indica que a conversão é uma Conversão de endereço de porta. Os flags "i" indicam que a conversão se aplica à porta de endereço interna.

A terceira entrada é uma ICMP Port Address Translation para o host-ICMP-id (10.1.1.15, 21505) na rede interna para o host-ICMP-id (192.168.49.1, 0) na rede externa. O flag "r" indica que a conversão é uma Conversão de endereço de porta. Os flags "i" indicam que a conversão se aplica ao endereço-ICMP-id interno.

Os campos de endereço interno aparecem como endereços de origem em pacotes que passam da interface mais segura para a interface menos segura. Por outro lado, eles aparecem como endereços de destino em pacotes que passam da interface menos segura para a interface mais segura.

```
show conn count
```

O comando `show conn count` mostra o número atual e máximo de conexões através do ASA. Uma conexão é um mapeamento de informações de Camada 4 de um endereço interno para um endereço externo. As conexões são criadas quando o ASA recebe um pacote SYN para sessões TCP ou quando chega o primeiro pacote em uma sessão UDP. As conexões são interrompidas quando o ASA recebe o pacote ACK final, que ocorre quando o handshake da sessão TCP é fechado ou quando o tempo limite expira na sessão UDP.

Contagens de conexões extremamente altas (50 a 100 vezes o normal) podem indicar que você está sob ataque. Execute o comando `show memory` para garantir que a alta contagem de conexões não faça com que o ASA fique sem 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. Essa ação protege seus servidores internos, para que eles não fiquem sobrecarregados. Consulte o [Guia de Configuração do Cisco ASA 5500 Series com o CLI, 8.4 e 8.6](#) para obter mais informações.

### Exemplo

```
<#root>
```

```
Ciscoasa#
```

```
show conn count
```

```
2289 in use, 44729 most used
```

```
show interface
```

O comando [show interface](#) pode ajudar a determinar problemas de incompatibilidade duplex e problemas de cabo. Ele também pode fornecer mais informações sobre se a interface está ou não sobrecarregada. Se o ASA ficar sem capacidade de CPU, o número de blocos de 1550 bytes passa para perto de 0. (Examine os blocos de 16384 bytes nas placas Gig de 66 MHz.) Outro indicador é o aumento de "sem buffers" na interface. A mensagem no buffers indica que a interface não pode enviar o pacote para o ASA OS porque não há bloco disponível para o pacote

e o pacote é descartado. Se um aumento nos níveis sem buffer ocorrer regularmente, execute o comando `show proc cpu` para verificar o uso da CPU no ASA. Se o uso da CPU for alto devido a uma carga de tráfego pesada, atualize para um ASA mais potente que possa lidar com 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 estiver cheia, o pacote será colocado na fila de software de entrada. O pacote é passado de sua fila de entrada e colocado em um bloco de 1550 bytes (ou em um bloco de 16384 bytes em interfaces Gigabit Ethernet de 66 MHz). Em seguida, o ASA determina a interface de saída do pacote e coloca o pacote na fila de hardware apropriada. Se a fila de hardware estiver cheia, o pacote será colocado na fila de software de saída. Se o máximo de blocos em qualquer uma das filas de software for grande, a interface estará sobrecarregada. Por exemplo, se 200 Mbps chegam ao ASA e todos saem de uma única interface de 100 Mbps, a fila de software de saída indica números altos na interface de saída, o que indica que a interface não pode lidar com o volume de tráfego. Se você passar por essa situação, atualize para uma interface mais rápida.

### Exemplo

```
<#root>
```

```
Ciscoasa#
```

```
show interface
```

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

Você também deve verificar se há erros na interface. Se você receber runts, erros de entrada, CRCs ou erros de quadro, é provável que haja uma incompatibilidade duplex. O cabo também pode estar com defeito. Consulte [Configurações de velocidade e duplex](#) para obter mais informações sobre problemas de duplex. Lembre-se de que cada contador de erro representa o número de pacotes que são descartados devido a esse erro específico. Se você vir um contador específico que é incrementado regularmente, o desempenho no seu ASA provavelmente será afetado, e você deverá encontrar a causa raiz do problema.

Ao examinar os contadores de interface, observe que se a interface estiver definida como full-duplex, você não deverá experimentar colisões, colisões tardias ou pacotes adiados. Por outro lado, se a interface estiver definida como half-duplex, você deverá receber colisões, algumas colisões atrasadas e, possivelmente, alguns pacotes adiados. O número total de colisões, colisões atrasadas e pacotes adiados não deve exceder 10% da soma dos contadores dos pacotes de entrada e saída. Se suas colisões excederem 10% do tráfego total, o link estará superutilizado e você deverá atualizar para full-duplex ou para uma velocidade mais rápida (10 Mbps a 100 Mbps). Lembre-se de que colisões de 10% significam que o ASA descarta 10% dos pacotes que passam por essa interface; cada um desses pacotes deve ser retransmitido.

Consulte o interface comando em [Cisco ASA 5500 Series Adaptive Security Appliances Command References](#) para obter informações detalhadas sobre os contadores de interface.

show processes

O comando **show processes** no ASA exibe todos os processos ativos que são executados no ASA no momento em que o comando é executado. Essas informações são úteis para determinar quais processos recebem muito tempo de CPU e quais processos não recebem tempo de CPU. Para obter essas informações, execute o **show processes** comando duas vezes; aguarde cerca de 1 minuto entre cada instância. Para o processo em questão, subtraia o valor de Tempo de Execução exibido na segunda saída do valor de Tempo de Execução exibido na primeira saída. Esse resultado mostra quanto tempo de CPU (em milissegundos) o processo recebeu nesse intervalo de tempo. Observe que alguns processos são programados para execução em intervalos específicos e alguns processos são executados somente quando há informações a serem processadas. O processo de pesquisa 577 provavelmente tem o maior valor de tempo de execução de todos os seus processos. Isso é normal porque o processo 577poll sonda as interfaces Ethernet para ver se elas têm dados que precisam ser processados.

---

 **Observação:** um exame de cada processo ASA está fora do escopo deste documento, mas é mencionado brevemente para ser completo. Consulte [ASA 8.3 e posterior: Monitorar e solucionar problemas de desempenho](#) para obter mais informações sobre os processos do ASA.

---

Resumo de comandos

Em resumo, use o comando **show cpu usage** para identificar a carga sob a qual o ASA está. Lembre-se de que a saída é uma média em execução; o ASA pode ter picos mais altos de uso da CPU que são mascarados pela média em execução. Quando o ASA atinge 80% de uso da CPU, a latência através do ASA aumenta lentamente para cerca de 90% da CPU. Quando o uso da CPU é superior a 90%, o ASA começa a descartar pacotes.

Se o uso da CPU for alto, use o **show processes** comando para identificar os processos que usam a maior parte do tempo da CPU. Use essas informações para reduzir parte do tempo consumido pelos processos intensivos (como o registro).

Se a CPU não funcionar quente, mas você acreditar que os pacotes ainda são descartados, use o comando **show interface** para verificar se a interface ASA não tem buffers e colisões, possivelmente causados por uma incompatibilidade bidirecional. Se a contagem de nenhum buffer aumentar, mas o uso da CPU não for baixo, a interface não poderá suportar o tráfego que flui por ela.

Se não houver problemas com os buffers, verifique os blocos. Se a coluna CNT atual na saída **show blocks** próxima a 0 nos blocos de 1.550 bytes (blocos de 16384 bytes para placas Gig de 66 MHz), o ASA provavelmente descartará pacotes Ethernet porque está muito ocupado. Nesse caso, a CPU atinge um pico alto.

Se você tiver problemas ao fazer novas conexões através do ASA, use o comando `show conn count` para verificar a contagem atual de conexões através do ASA.

Se a contagem atual for alta, verifique a saída `show memory` para garantir que o ASA não fique sem memória. Se a memória for insuficiente, investigue a origem das conexões com o comando `show conn` or `show local-host` para verificar se a rede não sofreu um ataque de negação de serviço.

Você pode usar outros comandos para medir a quantidade de tráfego que passa pelo ASA. O **show traffic** comando exibe os pacotes agregados e bytes por interface, e o comando `show perfmon` divide o tráfego em diferentes tipos que o ASA inspeciona.

#### Informações Relacionadas

- [Firewalls Cisco ASA 5500-X Series](#)
- [Suporte técnico e downloads da Cisco](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.