

Überwachung und Fehlerbehebung bei ASA-Leistungsproblemen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Fehlerbehebung bei Leistungsproblemen](#)

[Geschwindigkeits- und Duplexeinstellungen](#)

[CPU-Auslastung](#)

[Hohe Speicherauslastung](#)

[PortFast, Channel und Trunking](#)

[Network Address Translation \(NAT\)](#)

[Syslogs](#)

[SNMP](#)

[Umgekehrte DNS-Suche](#)

[Befehle anzeigen](#)

[CPU-Verwendung anzeigen](#)

[Datenverkehr anzeigen](#)

[Perfmon anzeigen](#)

[Blöcke anzeigen](#)

[Arbeitsspeicher anzeigen](#)

[Xlate anzeigen](#)

[Anzahl der Verbindungen anzeigen](#)

[show interface](#)

[Prozesse anzeigen](#)

[Befehlszusammenfassung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Befehle zur Überwachung und Fehlerbehebung der Leistung einer Cisco Adaptive Security Appliance (ASA) beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einer Cisco Adaptive Security Appliance (ASA) mit Version 8.3 und höher.


Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions \(Technische Tipps von Cisco zu Konventionen\)](#).

Fehlerbehebung bei Leistungsproblemen

Um Leistungsprobleme zu beheben, überprüfen Sie die in diesem Abschnitt beschriebenen grundlegenden Bereiche.

 **Hinweis:** Wenn Sie die Ausgabe des `show` Befehls von Ihrem Cisco Gerät erhalten haben, können Sie den [Cisco CLI Analyzer](#) verwenden, um potenzielle Probleme und Korrekturen anzuzeigen. Der Cisco CLI Analyzer unterstützt bestimmte `show` Befehle. Wenn Sie den Cisco CLI Analyzer verwenden, müssen Sie ein registrierter Cisco Benutzer sein, sich bei Ihrem Cisco Konto



anmelden und JavaScript in Ihrem Browser aktivieren.

Geschwindigkeits- und Duplexeinstellungen

Die Sicherheits-Appliance ist so vorkonfiguriert, dass sie die Geschwindigkeit und die Duplexeinstellungen einer Schnittstelle automatisch erkennt. Es gibt jedoch verschiedene Situationen, die dazu führen können, dass der automatische Verhandlungsprozess fehlschlägt, was zu Geschwindigkeits- oder Duplexdiskrepanzen (und Leistungsproblemen) führt. Bei geschäftskritischen Netzwerkinfrastrukturen führt Cisco manuell eine Hardcodierung der Geschwindigkeit und des Duplexmodus auf jeder Schnittstelle durch, sodass keine Fehlerwahrscheinlichkeit besteht. Da sich diese Geräte im Allgemeinen nicht bewegen, müssen Sie sie nicht ändern, wenn Sie sie richtig konfigurieren.

Die Verbindungsgeschwindigkeit kann auf jedem Netzwerkgerät gemessen werden, es muss jedoch eine Duplexverbindung hergestellt werden. Wenn zwei Netzwerkgeräte so konfiguriert sind, dass sie Geschwindigkeit und Duplex automatisch aushandeln, tauschen sie Frames aus (so genannte Fast Link Pulses oder FLPs), die ihre Geschwindigkeit und Duplexfunktionen angeben. Für einen nicht bewussten Verbindungspartner ähneln diese Impulse regulären 10-Mbit/s-Frames. Um die Impulse dekodieren zu können, enthalten die FLPs alle Geschwindigkeits- und Duplexeinstellungen, die der Link-Partner zur Verfügung stellen kann. Die Station, die die FLPs empfängt, bestätigt die Frames, und die Geräte vereinbaren die höchste Geschwindigkeit und die Duplexeinstellungen, die jeder erreichen kann. Wenn ein Gerät keine automatische Aushandlung unterstützt, empfängt das andere Gerät die FLPs und wechselt in den parallelen Erkennungsmodus. Um die Geschwindigkeit des Partners zu erfassen, hört das Gerät die Länge der Impulse ab und legt dann die Geschwindigkeit basierend auf der Länge fest. Das Problem tritt bei der Duplexeinstellung auf. Da Duplex ausgehandelt werden muss, kann das Gerät, das auf "Automatic Negotiation" (Automatische Aushandlung) eingestellt ist, die Einstellungen für das andere Gerät nicht bestimmen. Daher wird standardmäßig Halbduplex verwendet, wie im Standard IEEE 802.3u angegeben.

Wenn Sie beispielsweise die ASA-Schnittstelle für die automatische Aushandlung konfigurieren und sie mit einem Switch verbinden, der für 100 Mbit/s und Vollduplex hardcodiert ist, sendet die ASA FLPs. Der Switch reagiert jedoch nicht, da er für Geschwindigkeit und Duplex fest codiert ist und nicht an der automatischen Aushandlung beteiligt ist. Da die ASA keine Antwort vom Switch erhält, wechselt sie in den parallelen Erkennungsmodus und erfasst die Länge der Impulse in den vom Switch gesendeten Frames. Das heißt, die ASA erkennt, dass der Switch auf 100 Mbit/s eingestellt ist, und setzt daher die Schnittstellengeschwindigkeit auf dieser Grundlage. Da der Switch jedoch keine FLPs austauscht, kann die ASA nicht erkennen, ob der Switch Vollduplex ausführen kann. Daher setzt die ASA den Schnittstellenduplex auf Halbduplex, wie im IEEE 803.2u-Standard angegeben. Da der Switch auf 100 Mbit/s und Vollduplex hardcodiert ist und die ASA soeben automatisch auf 100 Mbit/s und Halbduplex umgestellt hat (wie dies der Fall ist), ergibt sich eine Duplexungleichheit, die zu schwerwiegenden Leistungsproblemen führen kann.

Eine Geschwindigkeits- oder Duplexungleichheit tritt am häufigsten auf, wenn die Fehlerzähler an den betreffenden Schnittstellen ansteigen. Die häufigsten Fehler sind Frames, zyklische Redundanzprüfungen (CRCs) und Runts. Wenn diese Werte auf Ihrer Schnittstelle inkrementiert werden, tritt entweder eine Geschwindigkeits-/Duplexungleichheit oder ein Verkabelungsproblem auf. Sie müssen dieses Problem lösen, bevor Sie fortfahren.

Beispiel

<#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

CPU-Auslastung

Wenn Sie eine hohe CPU-Auslastung festgestellt haben, führen Sie die folgenden Schritte aus, um eine Fehlerbehebung durchzuführen:

- Stellen Sie sicher, dass die Anzahl der Verbindungen in show xlate count gering ist.
- Überprüfen Sie, ob der Speicherblock normal ist.
- Stellen Sie sicher, dass mehr ACLs vorhanden sind.
- Führen Sie den show memory detail Befehl aus, und überprüfen Sie, ob der von der ASA verwendete Speicher normal verwendet wird.
- Überprüfen Sie, ob die Zählungen in show processes cpu-hog und show processes memory normal sind.
- Jeder innerhalb oder außerhalb der Security Appliance vorhandene Host kann schädlichen oder großen Datenverkehr erzeugen, der Broadcast-/Multicast-Datenverkehr sein und eine hohe CPU-Auslastung verursachen kann. Um dieses Problem zu beheben, konfigurieren Sie eine Zugriffsliste, um den Datenverkehr zwischen den Hosts (End-to-End) abzulehnen, und überprüfen Sie die Nutzung.
- Überprüfen Sie die Duplex- und Geschwindigkeitseinstellungen in den ASA-Schnittstellen. Die Einstellung für Diskrepanzen mit den Remote-Schnittstellen kann die CPU-Auslastung erhöhen.

Dieses Beispiel zeigt die höhere Anzahl an *Eingabefehlern* und *Überläufen* aufgrund der Geschwindigkeitsungleichheit. Verwenden Sie den show interface Befehl, um die Fehler zu überprüfen:

```
<#root>
```

```
Ciscoasa#
```

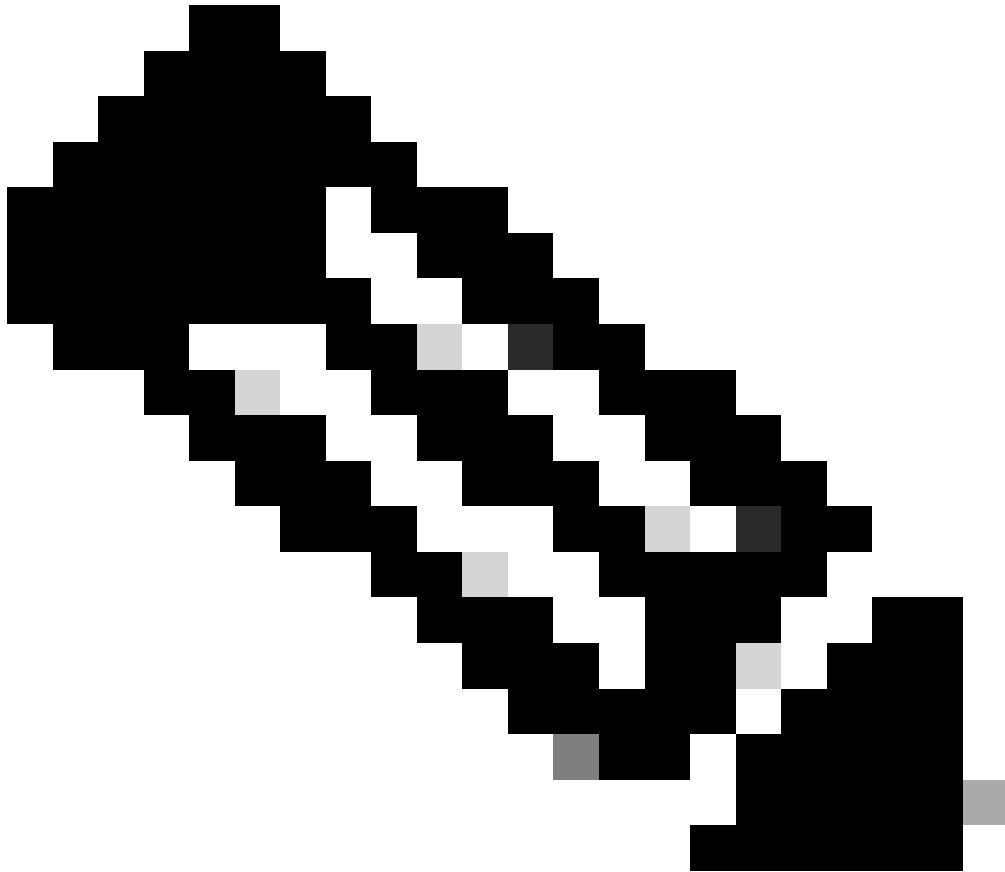
```
sh int GigabitEthernet0/1
```

```
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
```

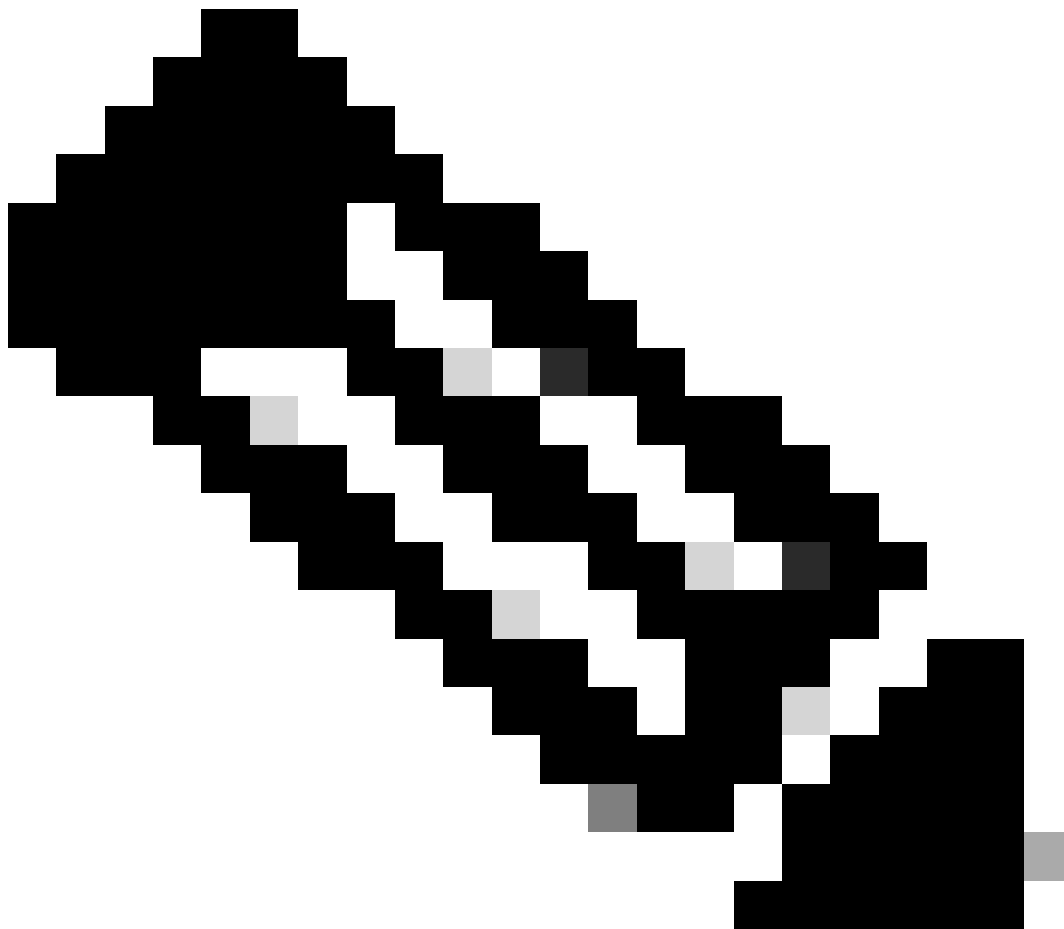
```
, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  121 packets output, 7744 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 1 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops, 0 tx hangs
  input queue (blocks free curr/low): hardware (255/249)
  output queue (blocks free curr/low): hardware (255/254)
```

Um dieses Problem zu beheben, legen Sie für die entsprechende Schnittstelle die *automatische* Geschwindigkeit fest.




Hinweis: Cisco empfiehlt, den `ip verify reverse-path interface` Befehl auf allen Schnittstellen zu aktivieren. Dies führt dazu, dass Pakete ohne gültige Quelladresse verworfen werden, was zu einer geringeren CPU-Auslastung führt. Dies gilt für FWSM, wenn es mit hohen CPU-Problemen konfrontiert ist.

-
- Ein weiterer Grund für die hohe CPU-Auslastung kann auf zu viele Multicast-Routen zurückzuführen sein. Führen Sie den `show mroute` Befehl aus, um zu überprüfen, ob ASA zu viele Multicast-Routen empfängt.
 - Verwenden Sie den `show local-host` Befehl, um festzustellen, ob es im Netzwerk zu einem Denial-of-Service-Angriff kommt, der auf einen Virenangriff im Netzwerk hinweisen kann.
 - Eine hohe CPU-Auslastung kann aufgrund der Cisco Bug-ID [CSCsq48636](#) auftreten. Weitere Informationen finden Sie unter Cisco



Hinweis: Nur registrierte Cisco Benutzer können auf interne Cisco Tools und Fehlerinformationen zugreifen.

 **Hinweis:** Wenn das Problem mit der zuvor bereitgestellten Lösung nicht behoben werden kann, aktualisieren Sie die ASA-Plattform entsprechend den Anforderungen. Weitere Informationen zu den Funktionen und Kapazitäten der Adaptive Security Appliance-Plattform finden Sie unter [Cisco Security Modules for Security Appliances](#). Wenden Sie sich für weitere Informationen an das TAC, ([Cisco Technical Support](#)).


Hier einige mögliche Ursachen und Auflösungen für eine hohe Speichernutzung:

- **Ereignisprotokollierung:** Die Ereignisprotokollierung kann große Mengen an Arbeitsspeicher belegen. Um dieses Problem zu beheben, installieren und protokollieren Sie alle Ereignisse auf einem externen Server, z. B. einem Syslog-Server.
- **Speicherleck:** Ein bekanntes Problem in der Software der Sicherheits-Appliance kann zu einem hohen Speicherverbrauch führen. Aktualisieren Sie die Sicherheits-Appliance-Software, um dieses Problem zu beheben.
- **Debuggen aktiviert:** Das Debuggen kann große Mengen an Arbeitsspeicher beanspruchen. Um dieses Problem zu beheben, deaktivieren Sie das Debuggen mit dem Befehl `undebug all`.
- **Ports blockieren:** Das Blockieren von Ports an der externen Schnittstelle einer Sicherheits-Appliance führt dazu, dass die Security Appliance große Mengen an Speicher benötigt, um die Pakete über die angegebenen Ports zu blockieren. Um dieses Problem zu beheben, blockieren Sie den anstößigen Datenverkehr auf der ISP-Seite.
- **Bedrohungserkennung:** Die Funktion zur Erkennung von Bedrohungen besteht aus verschiedenen Statistikebenen, die für verschiedene Bedrohungen erfasst werden, sowie aus der Erkennung gescannter Bedrohungen, die bestimmt, wann ein Host eine Suche durchführt. **Deaktivieren Sie** diese Funktion, um weniger Speicher zu verbrauchen.

PortFast, Channel und Trunking


Viele Switches, z. B. Cisco Switches mit dem Betriebssystem Catalyst, sind standardmäßig als Plug-and-Play-Geräte konzipiert. Daher sind viele der Standard-Port-Parameter nicht wünschenswert, wenn ein ASA-Gerät an den Switch angeschlossen wird. Beispielsweise ist auf einem Switch, auf dem Catalyst OS ausgeführt wird, das Standard-Channeling auf Auto, Trunking auf Auto und PortFast auf Deaktiviert eingestellt. Wenn Sie eine ASA mit einem Switch verbinden, auf dem Catalyst OS ausgeführt wird, deaktivieren Sie das Channeling, deaktivieren Sie das Trunking, und aktivieren Sie PortFast.

Channeling, auch als Fast EtherChannel oder Giga EtherChannel bezeichnet, wird verwendet, um zwei oder mehr physische Ports in einer logischen Gruppe zu binden, um den Gesamtdurchsatz über die Verbindung zu erhöhen. Wenn ein Port für automatisches Channeling konfiguriert ist, sendet er PAGP-Frames (Port Aggregation Protocol) aus, sobald die Verbindung aktiv wird, um zu bestimmen, ob er Teil eines Kanals ist. Diese Frames können Probleme verursachen, wenn das andere Gerät versucht, die Geschwindigkeit und die Duplex-Einstellungen der Verbindung automatisch auszuhandeln. Wenn Channeling auf dem Port auf Auto (Automatisch) eingestellt ist, führt dies zu einer zusätzlichen Verzögerung von etwa 3 Sekunden, bevor der Port nach dem Herstellen der Verbindung mit der Weiterleitung des Datenverkehrs beginnt.

 **Hinweis:** Auf den Catalyst Switches der XL-Serie ist Channeling nicht standardmäßig auf Auto eingestellt. Aus diesem Grund müssen Sie das Channeling auf jedem Switch-Port deaktivieren, der mit einem ASA-Gerät verbunden ist.

Trunking, auch unter den gebräuchlichen Trunking-Protokollen Inter-Switch Link (ISL) oder Dot1q bekannt, kombiniert mehrere virtuelle LANs (VLANs) auf einem einzelnen Port (oder Link). Trunking wird in der Regel zwischen zwei Switches verwendet, wenn auf beiden Switches mehr als ein VLAN definiert ist. Wenn ein Port für automatisches Trunking konfiguriert ist, sendet er beim Verbindungsaufbau DTP-Frames (Dynamic Trunking Protocol) aus, um zu bestimmen, ob der Port, mit dem er verbunden wird, Trunking verwenden möchte. Diese DTP-Frames können Probleme bei der automatischen Aushandlung der Verbindung verursachen. Wenn Trunking auf einem Switch-Port auf Auto (Automatisch) eingestellt ist, wird eine zusätzliche Verzögerung von etwa 15 Sekunden hinzugefügt, bevor der Port nach dem Herstellen der Verbindung mit der Weiterleitung des Datenverkehrs beginnt.

PortFast, auch als Fast Start bezeichnet, ist eine Option, die den Switch darüber informiert, dass ein Layer-3-Gerät mit einem Switch-Port verbunden ist. Der Port wartet nicht die voreingestellten 30 Sekunden (15 Sekunden zum Abhören und 15 Sekunden zum Lernen), sondern veranlasst den Switch, den Port unmittelbar nach dem Verbindungsaufbau in den Weiterleitungsstatus zu versetzen. Wenn Sie PortFast aktivieren, ist Spanning Tree nicht deaktiviert. Spanning Tree ist auf diesem Port weiterhin aktiv. Wenn Sie PortFast aktivieren, wird der Switch nur darüber informiert, dass kein anderer Switch oder Hub (nur Layer-2-Gerät) am anderen Ende des Links angeschlossen ist. Der Switch umgeht die normale 30-Sekunden-Verzögerung, während er versucht festzustellen, ob sich eine Layer-2-Schleife ergibt, wenn er diesen Port aktiviert. Wenn die Verbindung hochgefahren wurde, ist sie weiterhin Teil von Spanning Tree. Der Port sendet Bridge-Paket-Dateneinheiten (BPDUs), und der Switch wartet weiterhin auf BPDUs an diesem Port. Aus diesen Gründen wird empfohlen, PortFast auf jedem Switch-Port zu aktivieren, der mit einem ASA-Gerät verbunden ist.

 **Hinweis:** Catalyst OS 5.4 und höher enthalten den `set port host <mod>/<port>` Befehl, mit dem Sie das Channeling deaktivieren, Trunking deaktivieren und PortFast aktivieren können.

Network Address Translation (NAT)

Jeder NAT- oder NAT Overload (PAT)-Sitzung wird ein Übersetzungssteckplatz zugewiesen, der als *Xlate* bezeichnet wird. Diese Berechnungen können auch nach dem Ändern der sie betreffenden NAT-Regeln beibehalten werden. Dies kann zu einem Verlust von Übersetzungszeitnischen oder zu unerwartetem Verhalten oder zu beiden durch den zu übersetzenden Datenverkehr führen. In diesem Abschnitt wird erläutert, wie Sie die Xlate-Listen auf der Sicherheits-Appliance anzeigen und löschen.

 **Vorsicht:** Eine vorübergehende Unterbrechung des gesamten Datenverkehrs durch das Gerät kann auftreten, wenn Sie Xlate auf der Sicherheits-Appliance global löschen.

ASA-Beispielkonfiguration für PAT, die die IP-Adresse der externen Schnittstelle verwendet:

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

Datenverkehr, der die Sicherheits-Appliance durchläuft, unterliegt höchstwahrscheinlich einer NAT. Um die auf der Sicherheits-Appliance verwendeten Übersetzungen anzuzeigen, geben Sie den folgenden Befehl ein: `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
```

Die Übersetzungszeiträume können auch nach wichtigen Änderungen beibehalten werden. Führen Sie den folgenden Befehl aus, um die aktuellen Übersetzungssteckplätze auf der Sicherheits-Appliance zu löschen: `clear xlate`:

```
<#root>
```

```
Ciscoasa#
```

```
clear xlate
```

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

0 in use, 1 most used

Der clear xlate Befehl löscht die gesamte aktuelle dynamische Übersetzung aus der Excel-Tabelle. Um eine bestimmte IP-Übersetzung zu löschen, können Sie den clear xlate Befehl mit dem global [ip address] Schlüsselwort verwenden.

Nachfolgend finden Sie eine ASA-Beispielkonfiguration für 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
```

Beachten Sie die show xlate Ausgabe für die Übersetzung von 10.2.2.2 nach 10.10.10.10 global:

```
<#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
```

Löschen Sie die Übersetzung für die globale IP-Adresse 10.10.10.10:

<#root>

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

In diesem Beispiel ist die Übersetzung für inside 10.2.2.2 to outside global 10.10.10.10 nicht mehr vorhanden:

<#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

Syslogs ermöglichen Ihnen die Behebung von Problemen mit der ASA. Cisco bietet für Windows NT einen kostenlosen Syslog-Server an, den ASA Firewall Syslog Server (PFSS). Sie können das PDF-Dokument vom [technischen Support und von den Downloads von Cisco](#) herunterladen.


Mehrere andere Anbieter wie bieten Syslog-Server für verschiedene Windows-Plattformen wie Windows 2000 und Windows XP an. Auf den meisten UNIX- und Linux-Systemen sind standardmäßig Syslog-Server installiert.

Wenn Sie den Syslog-Server einrichten, konfigurieren Sie die ASA so, dass Protokolle an sie gesendet werden.

Beispiele:

<#root>

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

 **Hinweis:** In diesem Beispiel wird ASA so konfiguriert, dass Debugging (Stufe 7) und wichtigere Syslogs an den Syslog-Server gesendet werden. Da diese ASA-Protokolle die umfangreichsten sind, sollten Sie sie nur zur Fehlerbehebung verwenden. Konfigurieren Sie für den Normalbetrieb die Protokollierungsebene auf Warning (Warnung) (Stufe 4) oder Error (Fehler) (Stufe 3).

Wenn ein Problem mit der langsamen Leistung auftritt, öffnen Sie das Syslog in einer Textdatei, und suchen Sie nach der IP-Quelladresse, die mit dem Leistungsproblem verknüpft ist. (Wenn Sie UNIX verwenden, können Sie die Quell-IP-Adresse im Syslog **überprüfen**.) Überprüfen Sie, ob Meldungen vorliegen, die darauf hinweisen, dass der externe Server versucht hat, auf die interne IP-Adresse des TCP-Ports 113 zuzugreifen (für Identification Protocol oder Ident), aber die ASA hat das Paket abgelehnt. Die Nachricht muss dem folgenden Beispiel ähneln:

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

Wenn Sie diese Meldung erhalten, geben Sie den `service resetinbound`-Befehl an die ASA aus. Die ASA verwirft keine Pakete im Hintergrund. Stattdessen veranlasst dieser Befehl die ASA, alle eingehenden Verbindungen, die von der Sicherheitsrichtlinie abgelehnt wurden, sofort zurückzusetzen. Der Server wartet nicht darauf, dass das Ident-Paket seine TCP-Verbindung abläuft, sondern empfängt sofort ein Reset-Paket.

SNMP

Eine empfohlene Methode für Unternehmensbereitstellungen ist die Überwachung der Leistung der Cisco ASA mit SNMP. Die Cisco ASA unterstützt dies mit den SNMP-Versionen 1, 2c und 3.

Sie können die Security Appliance so konfigurieren, dass Traps an einen Network Management Server (NMS) gesendet werden, oder Sie

können das NMS verwenden, um die MIBs auf der Security Appliance zu durchsuchen. MIBs sind eine Sammlung von Definitionen, und die Sicherheits-Appliance verwaltet eine Datenbank mit Werten für jede Definition. Weitere Informationen hierzu finden Sie im [Cisco ASA 5500 Series Configuration Guide with the CLI, 8.4 and 8.6](#).

Alle unterstützten MIBs für Cisco ASA finden Sie in der ASA MIB Support List. Aus dieser Liste sind die folgenden MIBs hilfreich, wenn Sie die Leistung überwachen:

- CISCO-FIREWALL-MIB ---- Enthält Objekte, die für Failover nützlich sind.
- CISCO-PROCESS-MIB ---- Enthält Objekte, die für die CPU-Auslastung nützlich sind.
- CISCO-MEMORY-POOL-MIB ---- Enthält Objekte, die für Speicherobjekte nützlich sind.

Umgekehrte DNS-Suche

Wenn bei der ASA eine langsame Leistung auftritt, stellen Sie sicher, dass Sie im autorisierten DNS-Server für die von der ASA verwendeten externen Adressen DNS-Einträge (Domain Name System Pointer, DNS PTR) haben, die auch als Reverse DNS Lookup-Einträge bezeichnet werden. Dazu gehören alle Adressen in Ihrem globalen NAT-Pool (Network Address Translation) (oder die externe ASA-Schnittstelle, wenn Sie die Schnittstelle überlasten), alle statischen Adressen und internen Adressen (wenn Sie die NAT nicht zusammen mit dieser verwenden). Einige Anwendungen wie FTP (File Transfer Protocol) und Telnet-Server können DNS-Reverse-Lookups verwenden, um zu bestimmen, woher der Benutzer stammt und ob es sich um einen gültigen Host handelt. Wenn die umgekehrte DNS-Suche nicht aufgelöst wird, sinkt die Leistung, wenn die Anforderung abgelaufen ist.

Um sicherzustellen, dass ein PTR-Datensatz für diese Hosts vorhanden ist, geben Sie den nslookup Befehl von Ihrem PC oder UNIX-Computer aus ein. Geben Sie die globale IP-Adresse an, die Sie für die Verbindung mit dem Internet verwenden.

Beispiel

```
<#root>
```

```
% nslookup 192.168.219.25
```

10.219.133.198.in-addr.arpa name = www.cisco.com.

Sie müssen eine Antwort mit dem DNS-Namen des Geräts erhalten, das dieser IP-Adresse zugewiesen ist. Wenn Sie keine Antwort erhalten, wenden Sie sich an die Person, die Ihren DNS kontrolliert, um die Hinzufügung von PTR-Datensätzen für jede Ihrer globalen IP-Adressen anzufordern.

Überläufe auf der Schnittstelle

Bei einem Datenverkehrs-Burst können verworfene Pakete auftreten, wenn der Burst die Pufferkapazität des FIFO-Puffers auf der NIC und den Empfangs-Ringpuffern überschreitet. Wenn Sie Pausen-Frames für die Flusssteuerung aktivieren, kann dieses Problem entschärft werden. Pause (XOFF) und XON-Frames werden automatisch von der NIC-Hardware generiert, basierend auf der FIFO-Puffer-Nutzung. Ein Pausen-Frame wird gesendet, wenn die Puffernutzung die Höchstwassermarke überschreitet. Verwenden Sie den folgenden Befehl, um Pause-Frames (XOFF) für die Flusssteuerung zu aktivieren:

```
<#root>
```

```
hostname(config)#
```

```
interface tengigabitethernet 1/0
```

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

```
flowcontrol send on
```

Befehle anzeigen

CPU-Verwendung anzeigen

Mit show cpu usage diesem Befehl wird die Datenverkehrslast auf der ASA-CPU bestimmt. Während Spitzenzeiten im Datenverkehr, bei Netzwerkspitzen oder Angriffen kann die CPU-Auslastung in die Höhe schnellen.

Die ASA verfügt über eine einzige CPU zur Verarbeitung einer Vielzahl von Aufgaben, z. B. zur Verarbeitung von Paketen und Ausgabe von

Debug-Meldungen an die Konsole. Jeder Prozess hat seinen eigenen Zweck, und einige Prozesse benötigen mehr CPU-Zeit als andere Prozesse. Die Verschlüsselung ist wahrscheinlich der CPU-intensivste Prozess. Wenn Ihre ASA also viel Datenverkehr durch verschlüsselte Tunnel leitet, müssen Sie eine schnellere ASA in Betracht ziehen, einen dedizierten VPN-Konzentrator wie das VPN 3000. Die VAC lagert die Ver- und Entschlüsselung von der ASA-CPU aus und führt sie in der Hardware auf der Karte durch. So kann die ASA 100 Mbit/s Datenverkehr mit 3DES (168-Bit-Verschlüsselung) verschlüsseln und entschlüsseln.

Die Protokollierung ist ein weiterer Prozess, der große Mengen an Systemressourcen beanspruchen kann. Aus diesem Grund wird empfohlen, die Konsolen-, Überwachungs- und Pufferprotokollierung auf der ASA zu deaktivieren. Sie können diese Prozesse aktivieren, wenn Sie ein Problem beheben, sie jedoch für den täglichen Betrieb deaktivieren, insbesondere, wenn Ihnen die CPU-Kapazität ausgeht. Außerdem wird empfohlen, die Syslog- oder SNMP-Protokollierung (Simple Network Management Protocol) (Protokollierungsverlauf) auf die Ebene 5 (Benachrichtigung) oder eine niedrigere Ebene festzulegen. Darüber hinaus können Sie bestimmte Syslog-Meldungs-IDs mit dem `no logging message <syslog_id>` Befehl deaktivieren.

Der Cisco Adaptive Security Device Manager (ASDM) stellt außerdem ein Diagramm auf der Monitoring Registerkarte bereit, mit dem Sie die CPU-Auslastung der ASA im Zeitverlauf anzeigen können. Sie können dieses Diagramm verwenden, um die Belastung Ihrer ASA zu ermitteln.

Der **show cpu usage** Befehl kann verwendet werden, um Statistiken zur CPU-Auslastung anzuzeigen.

Beispiel

```
<#root>
```

```
Ciscoasa#
```

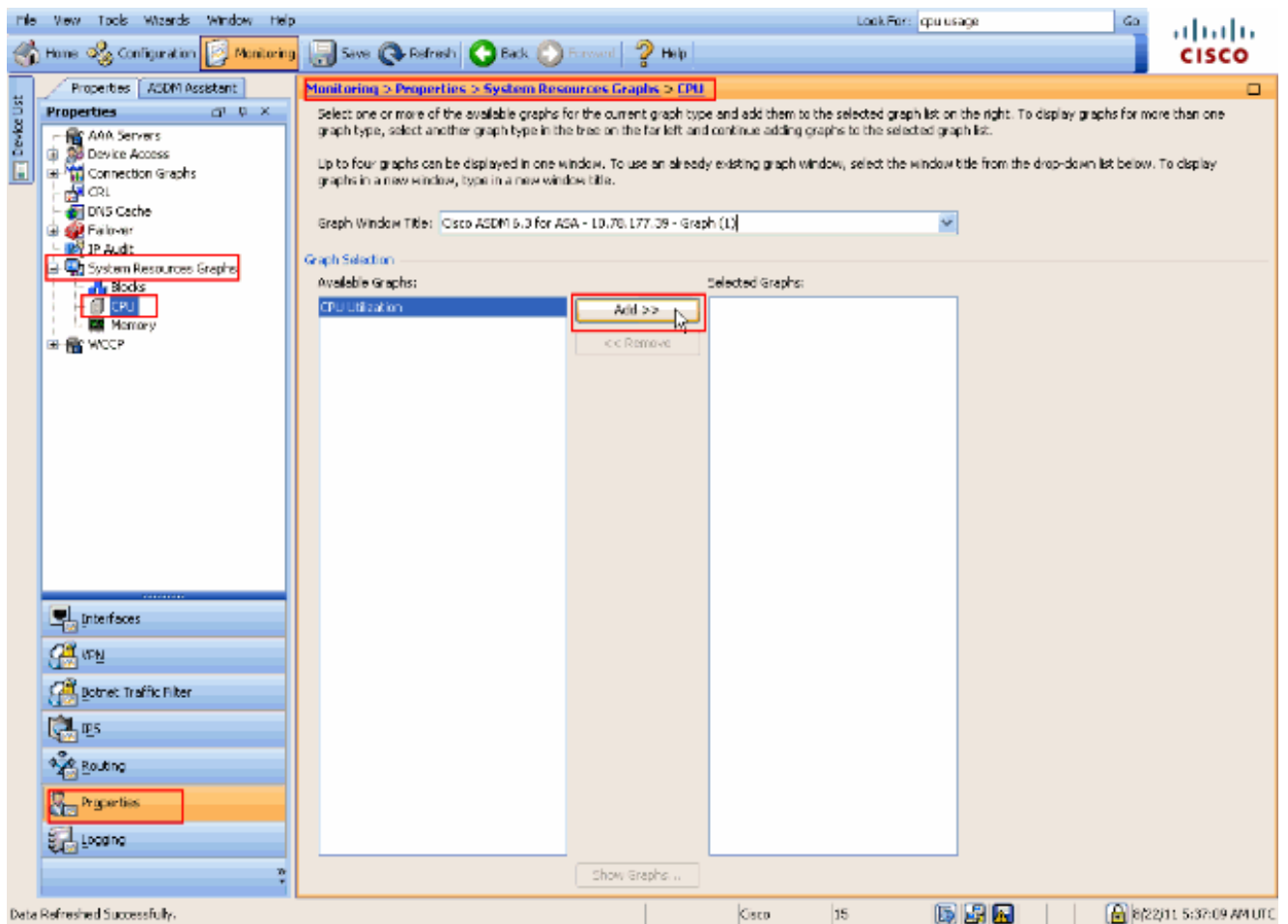
```
show cpu usage
```

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

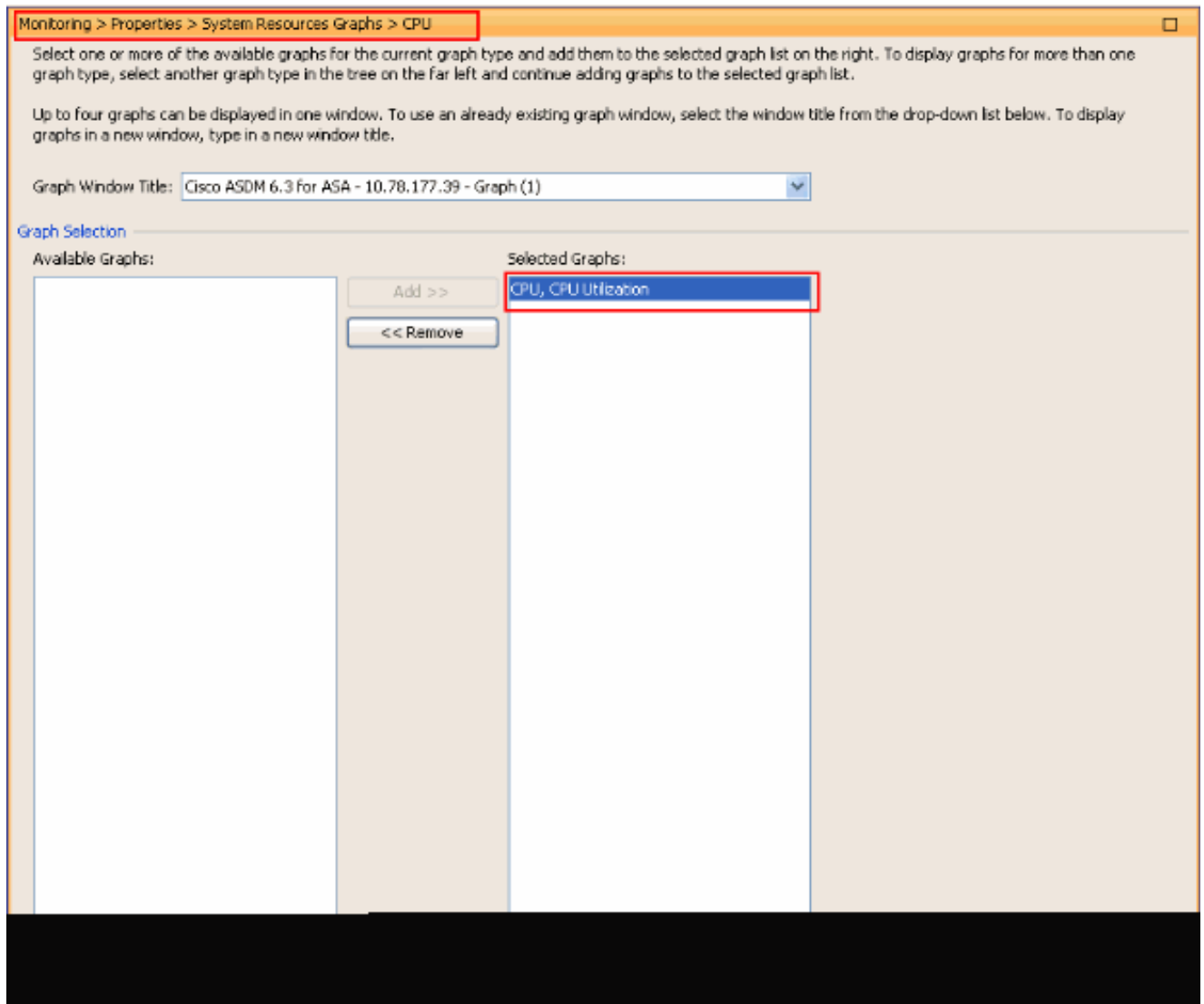
Anzeige der CPU-Auslastung auf ASDM

Gehen Sie wie folgt vor, um die CPU-Auslastung auf dem ASDM anzuzeigen:

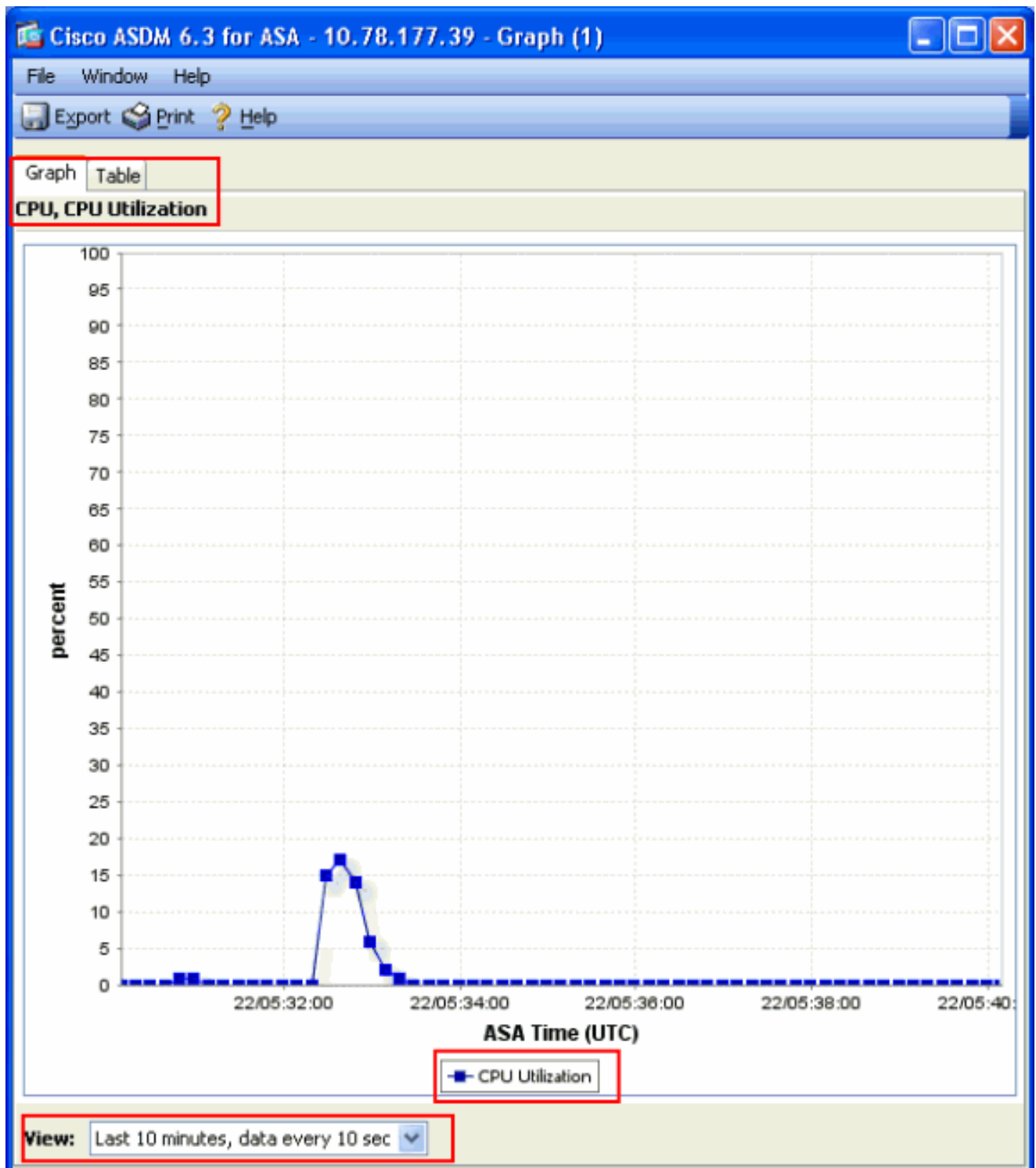
- Gehen Sie zu Monitoring > Properties > System Resources Graphics > CPU in ASDM, und wählen Sie den **Titel des Diagrammfensters aus**. Wählen Sie anschließend die erforderlichen Diagramme aus der Liste der **verfügbaren Diagramme**, und klicken Sie wie dargestellt auf **Hinzufügen**.



- Wenn Sie den gewünschten Diagrammnamen im Abschnitt **Ausgewählte Diagramme** hinzugefügt haben, klicken Sie auf **Diagramme anzeigen**.



Das nächste Bild zeigt das Diagramm zur **CPU-Auslastung** auf dem ASDM. Verschiedene Ansichten dieses Diagramms sind verfügbar und können geändert werden, wenn die Ansicht aus der Dropdown-Liste Ansicht ausgewählt ist. Diese Ausgabe kann bei Bedarf gedruckt oder auf dem Computer gespeichert werden.



Beschreibung der Ausgabe

Diese Tabelle beschreibt die Felder in der **show cpu usage** Ausgabe.

| Feld | Beschreibung |
|-------------------------------|---|
| CPU-Auslastung für 5 Sekunden | CPU-Auslastung in den letzten fünf Sekunden |
| 1 Minute | Durchschnittliche CPU-Auslastung von 5 Sekunden in der letzten Minute |
| 5 Minuten | Durchschnittliche CPU-Auslastung von 5 Sekunden in den letzten fünf Minuten |

Datenverkehr anzeigen

Der `show traffic` Befehl gibt an, wie viel Datenverkehr über einen bestimmten Zeitraum durch die ASA geleitet wird. Die Ergebnisse basieren auf dem Zeitintervall seit der letzten Ausgabe des Befehls. Führen Sie zuerst den **clear traffic** Befehl aus, und warten Sie dann 1-10 Minuten, bevor Sie den `show traffic` Befehl ausführen. Sie können auch den `show traffic` Befehl ausgeben und 1-10 Minuten warten, bevor Sie den Befehl erneut ausgeben, aber nur die Ausgabe der zweiten Instanz ist gültig.

Sie können den `show traffic` Befehl verwenden, um zu bestimmen, wie viel Datenverkehr über Ihre ASA geleitet wird. Wenn Sie über mehrere Schnittstellen verfügen, können Sie mit dem Befehl ermitteln, welche Schnittstellen die meisten Daten senden und empfangen. Bei ASA Appliances mit zwei Schnittstellen muss die Summe des ein- und ausgehenden Datenverkehrs an der externen Schnittstelle der Summe des ein- und ausgehenden Datenverkehrs an der internen Schnittstelle entsprechen.

Beispiel

```
<#root>
```

```
Ciscoasa#
```

```
show traffic
```

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

Wenn Sie den Nenndurchsatz an einer Ihrer Schnittstellen nahezu erreichen, müssen Sie ein Upgrade auf eine schnellere Schnittstelle durchführen oder den ein- und ausgehenden Datenverkehr an dieser Schnittstelle begrenzen. Andernfalls können Pakete verworfen werden. Wie im Abschnitt **show interface** beschrieben, können Sie die Schnittstellenzähler untersuchen, um den Durchsatz zu ermitteln.

Perfmon anzeigen

Der show perfmon Befehl dient zur Überwachung des Datenverkehrs und der Datenverkehrstypen, die von der ASA überprüft werden. Dieser Befehl ist die einzige Möglichkeit, die Anzahl der Übersetzungen (xlates) und Verbindungen (conn) pro Sekunde zu bestimmen. Die Verbindungen werden weiter in TCP- und UDP-Verbindungen (User Datagram Protocol) unterteilt. Unter **Beschreibung der Ausgabe** finden Sie Beschreibungen der Ausgabe, die durch diesen Befehl generiert wird.

Beispiel

```
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
```

Beschreibung der Ausgabe

Diese Tabelle beschreibt die Felder in der show perfmon Ausgabe.

| Feld | Beschreibung |
|------------------|---------------------------------------|
| Xlates | Aufgebaute Übersetzungen pro Sekunde |
| Verbindungen | Pro Sekunde hergestellte Verbindungen |
| TCP-Verbindungen | TCP-Verbindungen pro Sekunde |
| UDP-Verbindungen | UDP-Verbindungen pro Sekunde |

| | |
|-----------------------|--|
| URL-Zugriff | URLs (Websites), auf die pro Sekunde zugegriffen wird |
| URL-Serveranforderung | Anforderungen, die pro Sekunde an Websense und N2H2 gesendet werden (filter Befehl erforderlich) |
| TCP-Fixup | Anzahl der TCP-Pakete, die die ASA pro Sekunde weiterleitet |
| TCPIntercept | Anzahl der SYN-Pakete pro Sekunde, die den embryonalen Grenzwert einer statischen |
| HTTP-Fixup | Anzahl der Pakete, die für Port 80 pro Sekunde bestimmt sind (Befehl erforderlich <code>fixup protocol http</code>) |
| FTP-Fixup | FTP-Befehle, die pro Sekunde überprüft werden |
| AAA Authen | Authentifizierungsanforderungen pro Sekunde |
| AAA-Autor | Autorisierungsanforderungen pro Sekunde |
| AAA-Konto | Buchungsanforderungen pro Sekunde |

Blöcke anzeigen

Zusammen mit dem `show cpu usage` Befehl können Sie den `show blocks` Befehl verwenden, um festzustellen, ob die ASA überlastet ist.

Paketblöcke (1550 und 16384 Byte)

Wenn ein Paket in die ASA-Schnittstelle gelangt, wird es in der Warteschlange der Eingangsschnittstelle platziert, an das Betriebssystem übergeben und in einem Block platziert. Für Ethernet-Pakete werden die 1550-Byte-Blöcke verwendet. Wenn das Paket auf einer 66-MHz-Gigabit-Ethernet-Karte eingeht, werden die 16384-Byte-Blöcke verwendet. Die ASA bestimmt anhand des Adaptive Security Algorithm (ASA), ob ein Paket zulässig ist oder abgelehnt wird, und verarbeitet das Paket bis zur Ausgabewarteschlange an der ausgehenden Schnittstelle. Wenn die ASA die Datenverkehrslast nicht unterstützen kann, bewegt sich die Anzahl der verfügbaren 1550-Byte-Blöcke (oder 16384-Byte-Blöcke für

66-MHz-GE) nahe bei 0 (wie in der CNT-Spalte der Befehlsausgabe gezeigt). Wenn die CNT-Spalte den Wert 0 erreicht, versucht die ASA, weitere Blöcke zuzuweisen, bis zu einem Maximum von 8192. Wenn keine weiteren Blöcke verfügbar sind, verwirft die ASA das Paket.

Failover- und Syslog-Blöcke (256 Byte)

Die 256-Byte-Blöcke werden hauptsächlich für Stateful-Failover-Meldungen verwendet. Die aktive ASA generiert Pakete und sendet diese an die Standby-ASA, um die Übersetzungs- und Verbindungstabelle zu aktualisieren. In Zeiträumen, in denen Spitzenlasten auftreten, bei denen hohe Verbindungsraten erzeugt oder unterbrochen werden, kann die Anzahl der verfügbaren 256-Byte-Blöcke auf 0 sinken. Diese Dropdown-Liste zeigt an, dass mindestens eine Verbindung nicht mit der Standby-ASA aktualisiert wurde. Dies ist in der Regel akzeptabel, da beim nächsten Mal beim Stateful Failover-Protokoll der Xlate oder die Verbindung abgefangen wird, die verloren geht. Wenn die CNT-Spalte für 256-Byte-Blöcke jedoch über längere Zeiträume bei oder nahe 0 bleibt, kann die ASA aufgrund der Anzahl der von der ASA verarbeiteten Verbindungen pro Sekunde nicht mit den Übersetzungs- und Verbindungstabellen mithalten, die synchronisiert werden. Wenn dies konsistent geschieht, aktualisieren Sie die ASA auf ein schnelleres Modell.

Die von der ASA gesendeten Syslog-Meldungen verwenden ebenfalls die 256-Byte-Blöcke, werden aber im Allgemeinen nicht in einer solchen Menge freigegeben, dass der 256-Byte-Block-Pool erschöpft ist. Wenn die CNT-Spalte anzeigt, dass die Anzahl der 256-Byte-Blöcke nahe 0 liegt, stellen Sie sicher, dass Sie sich nicht beim Debuggen (Stufe 7) beim Syslog-Server anmelden. Dies wird durch die Protokollierungs-Trap-Zeile in der ASA-Konfiguration angezeigt. Es wird empfohlen, die Protokollierung auf Benachrichtigung (Stufe 5) oder niedriger festzulegen, es sei denn, Sie benötigen zusätzliche Informationen zum Debuggen.

Beispiel

```
<#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
```

Beschreibung der Ausgabe

Diese Tabelle beschreibt die Spalten in der show blocks Ausgabe.

| Spalte | Beschreibung |
|---------|---|
| GRÖSSE | E Größe des Blockpools in Byte. Jede Größe stellt einen bestimmten Typ dar |
| MAX. | Maximale Anzahl von Blöcken, die für den angegebenen Byteblock-Pool verfügbar sind. Die maximale Anzahl von Blöcken wird beim Systemstart aus dem Speicher entfernt. In der Regel ändert sich die maximale Anzahl von Blöcken nicht. Eine Ausnahme bilden die 256- und 1550-Byte-Blöcke, in denen die Adaptive Security Appliance bei Bedarf dynamisch mehr Pakete erstellen kann, bis zu einem Maximum von 8192. |
| NIEDRIG | Niedrigwasser-Marke. Diese Zahl gibt die niedrigste Anzahl von Blöcken dieser Größe an, die seit dem Hochfahren der Adaptive Security Appliance oder seit dem letzten Löschen der Blöcke (mit dem Befehl clear blocks) verfügbar sind. Eine Null in der Spalte NIEDRIG zeigt ein vorheriges Ereignis an, bei dem der Speicher voll war. |
| CNT | Aktuelle Anzahl der Blöcke, die für diesen spezifischen Größen-Block-Pool verfügbar sind. Eine Null in der CNT-Spalte bedeutet, dass der Speicher jetzt voll ist. |

Diese Tabelle beschreibt die SIZE-Zeileneinträge in der show blocks Ausgabe.

| GRÖSSE Wert | Beschreibung |
|----------------|--|
| 0 | Wird von Dupb-Blöcken verwendet. |
| 4 | Dupliziert vorhandene Blöcke in Anwendungen wie DNS, ISAKMP, URL-Filterung, Authentifizierung, TFTP und TCP-Module. Außerdem kann dieser große Block normalerweise von Code verwendet werden, um Pakete an Treiber usw. zu senden. |
| 80 | Wird im TCP-Intercept zum Generieren von Bestätigungspaketen und für Failover-Hello-Nachrichten verwendet. |
| 256 | Wird für Stateful Failover-Updates, Syslog-Protokollierung und andere TCP-Funktionen verwendet. Diese Blöcke werden hauptsächlich für Stateful Failover-Meldungen verwendet. Die aktive Adaptive Security Appliance generiert Pakete und sendet diese an die Standby Adaptive Security Appliance, um die Übersetzungs- und |

| | |
|-------|---|
| | <p>Verbindungstabelle zu aktualisieren. Bei datenintensivem Datenverkehr, bei dem hohe Verbindungsraten erzeugt oder unterbrochen werden, kann die Anzahl der verfügbaren Blöcke auf 0 sinken. Diese Situation weist darauf hin, dass eine oder mehrere Verbindungen nicht auf die Standby-Adaptive Security Appliance aktualisiert wurden. Das Stateful Failover-Protokoll fängt die verlorene Übersetzung oder Verbindung beim nächsten Mal auf. Wenn die CNT-Spalte für 256-Byte-Blöcke längere Zeit bei oder nahe 0 bleibt, bereitet es der Adaptive Security Appliance aufgrund der Anzahl von Verbindungen pro Sekunde, die die Adaptive Security Appliance verarbeitet, Schwierigkeiten, die Übersetzungs- und Verbindungstabellen zu synchronisieren. Die von der Adaptive Security Appliance gesendeten Syslog-Meldungen verwenden ebenfalls die 256-Byte-Blöcke, werden jedoch im Allgemeinen nicht in einer solchen Menge freigegeben, dass der 256-Byte-Block-Pool erschöpft ist. Wenn die CNT-Spalte anzeigt, dass die Anzahl der 256-Byte-Blöcke nahe 0 liegt, stellen Sie sicher, dass Sie sich nicht beim Debuggen (Stufe 7) beim Syslog-Server anmelden. Dies wird durch die Protokollierungs-Trap-Zeile in der Konfiguration der Adaptive Security Appliance angezeigt. Es wird empfohlen, die Protokollierung auf die Stufe "Notification" (Benachrichtigung) (Stufe 5) oder eine niedrigere Stufe festzulegen, es sei denn, Sie benötigen zusätzliche Informationen zum Debuggen.</p> |
| 1550 | <p>Wird zum Speichern von Ethernet-Paketen verwendet, die über die Adaptive Security Appliance verarbeitet werden sollen. Wenn ein Paket in eine adaptive Sicherheitsanwendungsschnittstelle eintritt, wird es in der Warteschlange der Eingangsschnittstelle platziert, an das Betriebssystem weitergeleitet und in einem Block platziert. Die Adaptive Security Appliance bestimmt anhand der Sicherheitsrichtlinie, ob ein Paket zugelassen oder abgelehnt werden muss, und verarbeitet das Paket bis zur Ausgabewarteschlange an der Ausgangsschnittstelle. Wenn die Adaptive Security Appliance Probleme hat, mit der Datenverkehrslast Schritt zu halten, kann die Anzahl der verfügbaren Blöcke nahe 0 liegen (wie in der CNT-Spalte der Befehlsausgabe gezeigt). Wenn die CNT-Spalte 0 ist, versucht die Adaptive Security Appliance, weitere Blöcke zuzuweisen, bis zu einem Maximum von 8192. Wenn keine Blöcke mehr verfügbar sind, verwirft die Adaptive Security Appliance das Paket.</p> |
| 16384 | <p>Wird nur für 64-Bit-Gigabit-Ethernet-Karten mit 66 MHz verwendet (i82543). Weitere Informationen zu Ethernet-Paketen finden Sie in der Beschreibung für den 1550.</p> |
| 2048 | <p>Control oder Guided Frames werden für Control-Updates verwendet.</p> |

Arbeitsspeicher anzeigen

Der show memory Befehl zeigt den gesamten physischen Speicher (bzw. RAM) für die ASA sowie die Anzahl der derzeit verfügbaren Bytes an.

Um diese Informationen nutzen zu können, müssen Sie zunächst verstehen, wie die ASA den Speicher verwendet. Wenn die ASA bootet, kopiert sie das Betriebssystem von Flash in den RAM und führt es aus dem RAM aus (genau wie Router). Als Nächstes kopiert die ASA die Startkonfiguration aus Flash und legt sie im RAM ab. Schließlich weist die ASA RAM zu, um die im Abschnitt beschriebenen Block-Pools zu erstellen. Nach Abschluss dieser Zuweisung benötigt die ASA nur dann einen zusätzlichen RAM, wenn sich die Größe der Konfiguration erhöht. Darüber hinaus speichert die ASA die Übersetzungs- und Verbindungseinträge im RAM.

Im Normalbetrieb muss sich der freie Speicher auf der ASA nur sehr wenig oder gar nicht ändern. Normalerweise benötigen Sie nur dann wenig Arbeitsspeicher, wenn ein Angriff stattfindet und Hunderttausende von Verbindungen über die ASA verlaufen. Um die Verbindungen zu überprüfen, geben Sie den `show conn count` Befehl ein, der die aktuelle und die maximale Anzahl von Verbindungen über die ASA anzeigt. Wenn der Speicher der ASA erschöpft ist, stürzt sie schließlich ab. Vor dem Absturz werden im Syslog (%ASA-3-211001) Fehlermeldungen zur Speicherzuweisung angezeigt.

Wenn Ihnen aufgrund eines Angriffs der Arbeitsspeicher ausgeht, wenden Sie sich an das [technische Support-Team](#) von [Cisco](#).

Beispiel

```
<#root>
```


```
Ciscoasa#
```

```
show memory
```

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

Xlate anzeigen

Der `show xlate count` Befehl zeigt die aktuelle und die maximale Anzahl von Übersetzungen über die ASA an. Eine Übersetzung ist eine Zuordnung einer internen Adresse zu einer externen Adresse und kann eine Eins-zu-Eins-Zuordnung sein, z. B. Network Address Translation (NAT), oder eine Viele-zu-Eins-Zuordnung, z. B. Port Address Translation (PAT). Dieser Befehl ist eine Teilmenge des `show xlate` Befehls, der jede Übersetzung über die ASA ausgibt. Die Befehlsausgabe zeigt die Übersetzungen "in Verwendung" an. Dies bezieht sich auf die Anzahl der aktiven Übersetzungen in der ASA, wenn der Befehl ausgegeben wird. "meistverwendet" bezieht sich auf die maximalen Übersetzungen, die auf der ASA seit dem Einschalten jemals gesehen wurden.

 **Hinweis:** Ein einzelner Host kann mehrere Verbindungen zu verschiedenen Zielen haben, aber nur eine Übersetzung. Wenn die Anzahl der Xlate-Einträge die Anzahl der Hosts in Ihrem internen Netzwerk deutlich übersteigt, ist es möglich, dass einer Ihrer internen Hosts kompromittiert wurde. Wenn Ihr interner Host kompromittiert wurde, fälscht er die Quelladresse und sendet Pakete an die ASA.



Hinweis: Wenn die vpnclient-Konfiguration aktiviert ist und der interne Host DNS-Anfragen sendet, kann der `show xlate` Befehl mehrere Xlate für eine statische Übersetzung auflisten.

Beispiel

<#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
```

Der erste Eintrag ist eine TCP-Port-Adressumwandlung für den Host-Port (10.1.1.15, 1026) im internen Netzwerk zum Host-Port (192.168.49.1, 1024) im externen Netzwerk. Das "r"-Flag bedeutet, dass die Übersetzung eine Port-Adressumwandlung ist. Die "i"-Flags weisen darauf hin, dass die Übersetzung für den internen Adressport gilt.

Der zweite Eintrag ist eine UDP Port Address Translation für den Host-Port (10.1.1.15, 1028) im internen Netzwerk zum Host-Port (192.168.49.1, 1024) im externen Netzwerk. Das "r"-Flag bedeutet, dass die Übersetzung eine Port-Adressumwandlung ist. Die "i"-Flags

weisen darauf hin, dass die Übersetzung für den internen Adressport gilt.

Der dritte Eintrag ist eine ICMP Port Address Translation für host-ICMP-id (10.1.1.15, 21505) im internen Netzwerk zu host-ICMP-id (192.168.49.1, 0) im externen Netzwerk. Das "r"-Flag bedeutet, dass die Übersetzung eine Port-Adressenumwandlung ist. Die "i"-Flags weisen darauf hin, dass die Übersetzung für die interne Adresse "ICMP-id" gilt.

Die internen Adressfelder werden bei Paketen, die von der sichereren Schnittstelle zu der weniger sicheren Schnittstelle übertragen werden, als Quelladressen angezeigt. Umgekehrt werden sie als Zieladressen auf Paketen angezeigt, die von der weniger sicheren Schnittstelle zur sichereren Schnittstelle übertragen werden.

Anzahl der Verbindungen anzeigen

Der show conn count Befehl zeigt die aktuelle und maximale Anzahl von Verbindungen über die ASA an. Eine Verbindung ist eine Zuordnung von Layer-4-Informationen von einer internen Adresse zu einer externen Adresse. Verbindungen werden aufgebaut, wenn die ASA ein SYN-Paket für TCP-Sitzungen empfängt oder wenn das erste Paket in einer UDP-Sitzung eintrifft. Verbindungen werden getrennt, wenn die ASA das letzte ACK-Paket empfängt. Dies geschieht, wenn der TCP-Sitzungshandshake geschlossen wird oder wenn das Timeout in der UDP-Sitzung abläuft.

Extrem hohe Verbindungszahlen (das 50- bis 100-fache des Normalwerts) können auf einen Angriff hinweisen. Führen Sie den show memory Befehl aus, um sicherzustellen, dass der ASA aufgrund der hohen Anzahl von Verbindungen nicht der Arbeitsspeicher ausgeht. Wenn Sie angegriffen werden, können Sie die maximale Anzahl von Verbindungen pro statischem Eintrag sowie die maximale Anzahl von embryonalen Verbindungen begrenzen. Dadurch werden Ihre internen Server geschützt, damit sie nicht überlastet werden. Weitere Informationen finden Sie im [Konfigurationsleitfaden für die Cisco Serie ASA 5500 mit der CLI 8.4 und 8.6](#).

Beispiel

```
<#root>
```

```
Ciscoasa#
```

```
show conn count
```

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

show interface

Mit dem Befehl [show interface](#) können Sie Probleme mit Duplexdiskrepanzen und Kabelprobleme ermitteln. Sie kann auch weitere Informationen darüber liefern, ob die Schnittstelle überlaufen wurde oder nicht. Wenn der ASA die CPU-Kapazität ausgeht, bewegt sich die Anzahl der 1550-Byte-Blöcke nahe bei 0. (Sehen Sie sich die 16384-Byte-Blöcke auf den 66-MHz-Gig-Karten an.) Ein weiterer Indikator ist die Zunahme von "keine Puffer" auf der Schnittstelle. Die Nachricht no buffers gibt an, dass die Schnittstelle das Paket nicht an das ASA-Betriebssystem senden kann, da kein Block für das Paket verfügbar ist und das Paket verworfen wird. Wenn regelmäßig eine Zunahme der Pufferstufen auftritt, geben Sie den Befehl ein, um die CPU-Auslastung auf der ASA zu überprüfen `show proc cpu`. Wenn die CPU-Auslastung aufgrund einer hohen Datenverkehrslast hoch ist, sollten Sie ein Upgrade auf eine leistungsstärkere ASA durchführen, die die Last bewältigen kann.

Wenn ein Paket zuerst an einer Schnittstelle eingeht, wird es in die Hardware-Eingangswarteschlange gestellt. Wenn die Hardware-Eingabewarteschlange voll ist, wird das Paket in die Software-Eingabewarteschlange gestellt. Das Paket wird aus der Eingangswarteschlange übergeben und in einem 1550-Byte-Block (oder in einem 16384-Byte-Block an 66-MHz-Gigabit-Ethernet-Schnittstellen) platziert. Anschließend bestimmt die ASA die Ausgabeschnittstelle für das Paket und setzt das Paket in die entsprechende Hardware-Warteschlange. Wenn die Hardware-Warteschlange voll ist, wird das Paket in die Ausgabesoftware-Warteschlange gestellt. Wenn die maximalen Blöcke in einer der Softwarewarteschlangen groß sind, wird die Schnittstelle überschrieben. Wenn z. B. 200 Mbit/s an die ASA gesendet werden und alle über eine einzelne 100-Mbit/s-Schnittstelle gesendet werden, weist die Ausgabesoftwarewarteschlange auf hohe Werte an der ausgehenden Schnittstelle hin, was darauf hinweist, dass die Schnittstelle das Datenverkehrsvolumen nicht verarbeiten kann. In diesem Fall sollten Sie auf eine schnellere Schnittstelle aktualisieren.

Beispiel

```
<#root>
```

```
Ciscoasa#
```

```
show interface
```

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


Sie müssen auch die Schnittstelle auf Fehler überprüfen. Wenn Sie Runts, Eingabefehler, CRCs oder Frame-Fehler empfangen, liegt wahrscheinlich eine Duplexungleichheit vor. Das Kabel kann ebenfalls defekt sein. Weitere Informationen zu Duplexproblemen finden Sie unter [Geschwindigkeits- und Duplexeinstellungen](#). Denken Sie daran, dass jeder Fehlerzähler die Anzahl der Pakete angibt, die aufgrund dieses bestimmten Fehlers verworfen wurden. Wenn Sie einen bestimmten Zähler sehen, der sich regelmäßig erhöht, leidet höchstwahrscheinlich die Leistung Ihrer ASA, und Sie müssen die Ursache des Problems finden.

Beachten Sie bei der Überprüfung der Schnittstellenzähler, dass es bei einer Vollduplex-Einstellung der Schnittstelle nicht zu Kollisionen, verspäteten Kollisionen oder zurückgestellten Paketen kommen darf. Wenn die Schnittstelle dagegen auf Halbduplex eingestellt ist, müssen Sie Kollisionen, einige späte Kollisionen und möglicherweise einige zurückgestellte Pakete empfangen. Die Gesamtzahl der Kollisionen, verspäteten Kollisionen und verzögerten Pakete darf 10 % der Summe der Zähler der Eingangs- und Ausgangspakete nicht überschreiten. Wenn Ihre Kollisionen 10 % des gesamten Datenverkehrs überschreiten, ist die Verbindung überlastet, und Sie müssen auf Vollduplex oder eine schnellere Geschwindigkeit (10 Mbit/s bis 100 Mbit/s) aktualisieren. Beachten Sie, dass bei einer Kollision von 10 % die ASA 10 % der Pakete verwirft, die über diese Schnittstelle übertragen werden. Jedes dieser Pakete muss erneut übertragen werden.

interface Detaillierte Informationen zu den Schnittstellenzählern finden Sie unter [Cisco Adaptive Security Appliances Command References \(Befehlsreferenzen](#) für die [Cisco ASA 5500 Serie](#)).

Prozesse anzeigen

Der **show processes** Befehl auf der ASA zeigt alle aktiven Prozesse an, die auf der ASA ausgeführt werden, wenn der Befehl ausgeführt wird. Diese Informationen sind nützlich, um festzustellen, welche Prozesse zu viel CPU-Zeit erhalten und welche keine CPU-Zeit erhalten. Um diese Informationen zu erhalten, geben Sie den **show processes** Befehl zweimal aus. Warten Sie etwa eine Minute zwischen den einzelnen Instanzen. Subtrahieren Sie für den betreffenden Prozess den in der zweiten Ausgabe angezeigten Runtime-Wert von dem in der ersten Ausgabe angezeigten Runtime-Wert. Dieses Ergebnis zeigt an, wie viel CPU-Zeit (in Millisekunden) der Prozess in diesem Zeitintervall empfangen hat. Beachten Sie, dass einige Prozesse in bestimmten Intervallen ausgeführt werden sollen und einige Prozesse nur dann ausgeführt werden, wenn sie über zu verarbeitende Informationen verfügen. Der 577poll Prozess hat höchstwahrscheinlich den größten Runtime Wert aller Ihrer Prozesse. Dies ist normal, da der 577poll-Prozess eine Abfrage an den Ethernet-Schnittstellen durchführt, um festzustellen, ob diese über Daten verfügen, die verarbeitet werden müssen.

 **Hinweis:** Eine Untersuchung der einzelnen ASA-Prozesse wird in diesem Dokument nicht behandelt, wird jedoch der Vollständigkeit halber kurz erwähnt. Weitere Informationen zu den ASA-Prozessen finden Sie unter [ASA 8.3 und höher: Überwachen und Problembehebung](#).

Befehlszusammenfassung

Verwenden Sie den `show cpu usage` Befehl, um die Last zu identifizieren, unter der die ASA steht. Beachten Sie, dass es sich bei der Ausgabe um einen laufenden Durchschnitt handelt. ASA kann höhere Spitzen der CPU-Auslastung aufweisen, die durch den laufenden Durchschnitt maskiert werden. Sobald die ASA eine CPU-Auslastung von 80 % erreicht hat, steigt die Latenz über die ASA langsam auf etwa 90 % der CPU an. Bei einer CPU-Auslastung von mehr als 90 % verwirft die ASA Pakete.

Wenn die CPU-Auslastung hoch ist, verwenden Sie den **show processes** Befehl, um die Prozesse zu identifizieren, die die meiste CPU-Zeit verbrauchen. Verwenden Sie diese Informationen, um den Zeitaufwand für die intensiven Prozesse (z. B. Protokollierung) zu reduzieren.

Wenn die CPU nicht während des Betriebs ausgeführt wird, die Pakete aber dennoch verworfen werden, verwenden Sie den **show interface** Befehl, um die ASA-Schnittstelle auf keine Puffer und Kollisionen zu überprüfen, die möglicherweise durch eine Duplexdiskrepanz verursacht werden. Wenn die Anzahl der Puffer ohne Erhöhung zunimmt, die CPU-Auslastung jedoch nicht niedrig ist, kann die Schnittstelle den Datenverkehr, der sie durchfließt, nicht unterstützen.

Wenn die Puffer in Ordnung sind, überprüfen Sie die Blöcke. Wenn die aktuelle CNT-Spalte in der **show blocks** Ausgabe in den 1550-Byte-Blöcken nahe 0 ist (16384-Byte-Blöcke für 66-MHz-Gigabit-Karten), verwirft die ASA höchstwahrscheinlich Ethernet-Pakete, weil sie zu ausgelastet ist. In diesem Fall sind die CPU-Spitzen hoch.

Wenn bei neuen Verbindungen über die ASA Probleme auftreten, verwenden Sie den **show conn count** Befehl, um die aktuelle Anzahl der Verbindungen über die ASA zu überprüfen.

Wenn die aktuelle Anzahl hoch ist, überprüfen Sie die **show memory** Ausgabe, um sicherzustellen, dass der ASA nicht der Arbeitsspeicher ausgeht. Wenn nicht genügend Arbeitsspeicher vorhanden ist, überprüfen Sie die Verbindungsquelle mit dem Befehl **show conn** oder **show local-host**, um sicherzustellen, dass Ihr Netzwerk keinen Denial-of-Service-Angriff ausgeführt hat.

Sie können andere Befehle verwenden, um die Menge des Datenverkehrs zu messen, der über die ASA geleitet wird. Mit dem **show traffic** Befehl werden die aggregierten Pakete und Bytes pro Schnittstelle angezeigt. Der Befehl **show perfmon** teilt den Datenverkehr in verschiedene Typen auf, die von der ASA geprüft werden.

Zugehörige Informationen

- [Cisco Firewalls der Serie ASA 5500-X](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.