Monitoraggio e risoluzione dei problemi di prestazioni dell'ASA

Sommario

Introduzione

In questo documento vengono descritti i comandi da utilizzare per monitorare e risolvere i problemi di prestazioni di una appliance Cisco Adaptive Security (ASA).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, è stata usata una Cisco Adaptive Security Appliance (ASA) con versione 8.3 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Risoluzione dei problemi relativi alle prestazioni

Per risolvere i problemi relativi alle prestazioni, controllare le aree di base descritte in questa sezione.

Nota: se il dispositivo Cisco restituisce i risultati del show comando, è possibile usare Cisco CLI Analyzer per visualizzare i potenziali errori e correggerli. Cisco CLI Analyzer supporta alcuni show comandi. Se si utilizza Cisco CLI Analyzer, è necessario essere un utente Cisco registrato, aver eseguito l'accesso al proprio account Cisco e avere JavaScript abilitato nel browser.

Impostazioni velocità e duplex

L'appliance di sicurezza è preconfigurata per il rilevamento automatico della velocità e delle impostazioni duplex su un'interfaccia. Tuttavia, esistono diverse situazioni che possono causare il fallimento del processo di negoziazione automatica e la conseguente mancata corrispondenza della velocità o del duplex (nonché problemi di prestazioni). Per le infrastrutture di rete mission-critical, Cisco codifica manualmente la velocità e il duplex su ciascuna interfaccia, in modo che non ci siano possibilità di errore. Questi dispositivi in genere non si spostano, quindi se li si configura correttamente, non è necessario modificarli.

Su qualsiasi dispositivo di rete, è possibile rilevare la velocità di collegamento, ma è necessario negoziare il duplex. Se due dispositivi di rete sono configurati per la negoziazione automatica della velocità e del duplex, si scambiano frame (detti Fast Link Pulse o FLP) che ne pubblicizzano la velocità e le funzionalità duplex. Per i partner di collegamento che non sono consapevoli, questi impulsi sono simili ai normali frame a 10 Mbps. Per consentire a un partner di collegamento di decodificare gli impulsi, i file FLP contengono tutte le impostazioni di velocità e duplex che il partner di collegamento può fornire. La stazione che riceve i file FLP riconosce i frame e i dispositivi concordano sulle impostazioni di velocità e duplex più alte possibili per ciascuno di essi. Se un dispositivo non supporta la negoziazione automatica, l'altro dispositivo riceve i pacchetti FLP e passa alla modalità di rilevamento parallelo. Per rilevare la velocità del partner, il dispositivo ascolta la lunghezza degli impulsi e quindi imposta la velocità in base alla lunghezza. Il problema si verifica con l'impostazione duplex. Poiché è necessario negoziare il duplex, il dispositivo impostato per la negoziazione automatica non può determinare le impostazioni sull'altro dispositivo, per impostazione predefinita è half-duplex, come indicato nello standard IEEE 802.3u.

Ad esempio, se si configura l'interfaccia ASA per la negoziazione automatica e la si connette a uno switch hardcoded per 100 Mbps e full-duplex, l'ASA invia pacchetti FLP. Tuttavia, lo switch non risponde perché è hardcoded per la velocità e il duplex e non partecipa alla negoziazione automatica. Poiché lo switch non riceve alcuna risposta, l'ASA passa alla modalità di rilevamento parallelo e rileva la lunghezza degli impulsi nei frame inviati dallo switch. In altre parole, l'ASA rileva che lo switch è impostato su 100 Mbps, quindi imposta la velocità dell'interfaccia su questa base. Tuttavia, poiché lo switch non scambia pacchetti FLP, l'ASA non può rilevare se lo switch può eseguire la modalità full-duplex, quindi imposta l'interfaccia duplex su half-duplex, come indicato nello standard IEEE 803.2u. Poiché lo switch è hardcoded a 100 Mbps e full-duplex e l'ASA ha appena negoziato automaticamente a 100 Mbps e half-duplex (come fa), il risultato è una mancata corrispondenza duplex che può causare gravi problemi di prestazioni.

La mancata corrispondenza della velocità o del duplex viene rilevata più di frequente quando i contatori di errori sulle interfacce in questione aumentano. Gli errori più comuni sono frame, CRC (Cyclic Redundancy Check) e runt. Se questi valori aumentano sull'interfaccia, si verifica una mancata corrispondenza velocità/duplex o un problema di cablaggio. È necessario risolvere il problema prima di continuare.

Esempio

<#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

Utilizzo CPU

Se l'utilizzo della CPU è elevato, completare i seguenti passaggi per risolvere il problema:

- Verificare che il numero di connessioni in show xlate count sia basso.
- Verificare che il blocco di memoria sia normale.
- Verificare che il numero di ACL sia superiore.
- Eseguire il comandoshow memory detail e verificare che la memoria utilizzata dall'ASA sia in uso normale.
- Verificare che i conteggi in show processes cpu-hog e show processes memory siano normali.
- Qualsiasi host presente all'interno o all'esterno dell'appliance di sicurezza può generare traffico dannoso o di massa, che può essere un traffico broadcast/multicast e causare un utilizzo elevato della CPU. Per risolvere questo problema, configurare un elenco degli accessi in modo da negare il traffico tra gli host (end-to-end) e controllare l'utilizzo.
- Verificare le impostazioni duplex e la velocità nelle interfacce ASA. L'impostazione di mancata corrispondenza con le interfacce remote può aumentare l'utilizzo della CPU.

In questo esempio viene mostrato il numero più alto di *errori* di *input* e *sovraccarichi* dovuti a una mancata corrispondenza della velocità. Per verificare gli errori,show interface usare il comando:

<#root>

Ciscoasa#

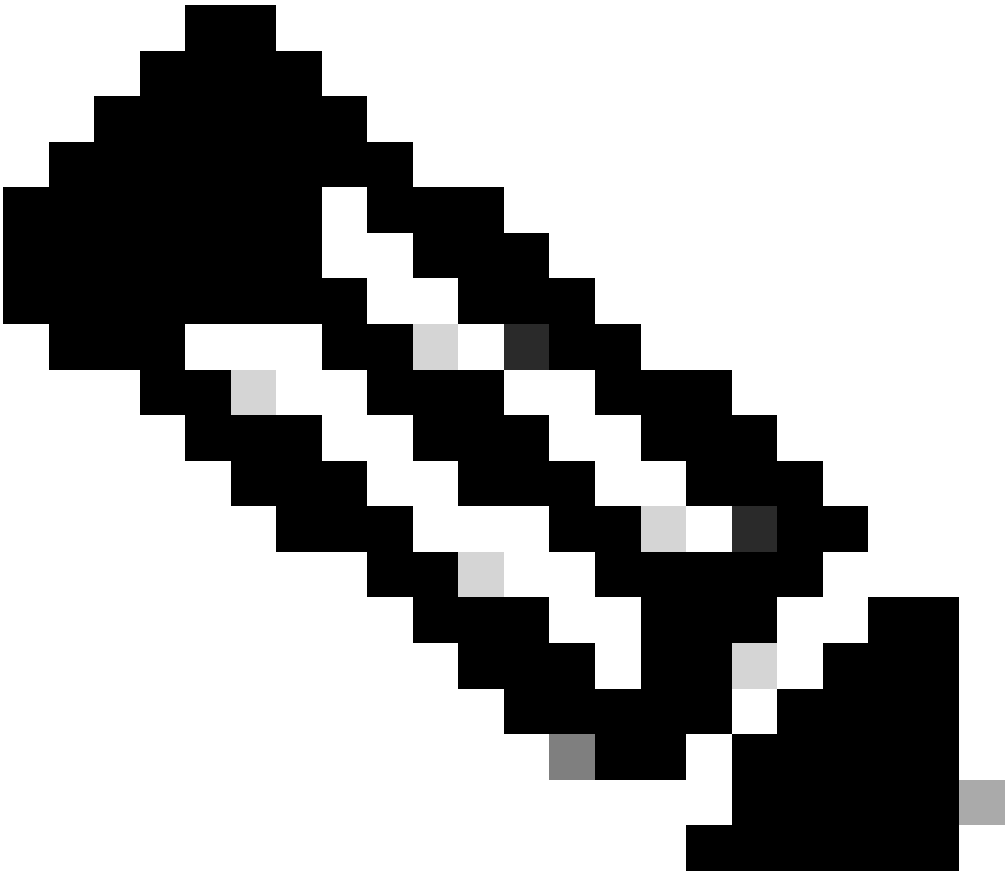
sh int GigabitEthernet0/1

```
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)
```

Per risolvere questo problema, impostare la velocità come *auto* sull'interfaccia corrispondente.



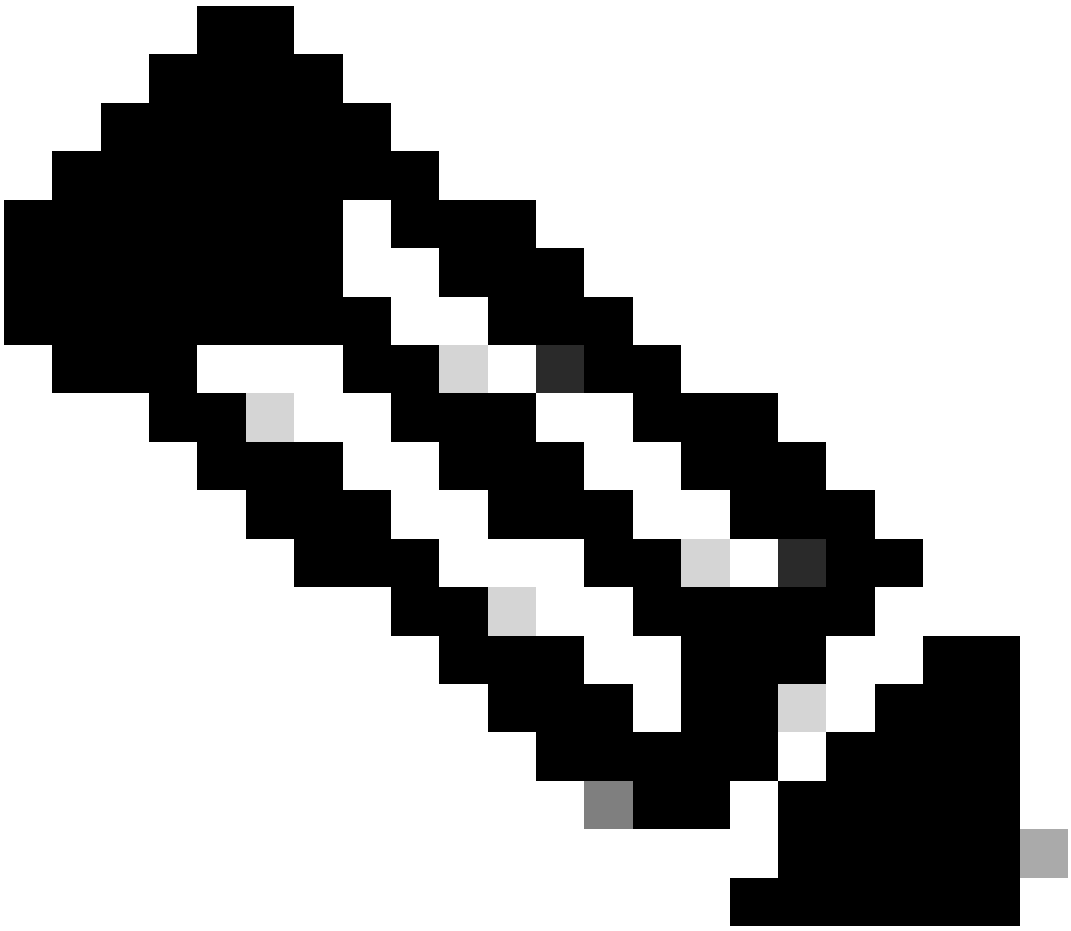
Nota: Cisco consiglia di abilitare il comandoip verify reverse-path interface su tutte le interfacce. In questo modo, i pacchetti che non dispongono di un indirizzo di origine valido verranno eliminati e l'utilizzo della CPU risulterà inferiore. Questo vale per il modulo FWSM quando deve affrontare problemi elevati di CPU.

- Un altro motivo dell'utilizzo elevato della CPU può essere il numero eccessivo di route multicast. Usare il comandoshow mroute per verificare se l'appliance ASA riceve troppe route multicast.

- Utilizzare il show local-host comando per verificare se la rete ha subito un attacco di negazione del servizio, che può indicare un attacco di virus nella rete.

- La CPU può essere elevata a causa dell'ID bug Cisco CSCsq48636. per ulteriori informazioni, fare riferimento all'ID bug Cisco

CSCsq48636.



Nota: solo gli utenti Cisco registrati possono accedere agli strumenti Cisco interni e alle informazioni sui bug.

Nota: se la soluzione fornita in precedenza non risolve il problema, aggiornare la piattaforma ASA in base ai requisiti. Per ulteriori informazioni sulle funzionalità e le capacità di Adaptive Security Appliance Platform, fare riferimento a Cisco Security Modules for Security Appliance. Per ulteriori informazioni, contattare TAC (Cisco Technical Support).

Utilizzo elevato della memoria

Di seguito sono elencate alcune possibili cause e soluzioni per un utilizzo elevato della memoria:

- **Registrazione eventi:** la registrazione degli eventi può occupare grandi quantità di memoria. Per risolvere il problema, installare e registrare tutti gli eventi in un server esterno, ad esempio un server syslog.

- **Perdita di memoria:** un problema noto nel software dell'appliance di sicurezza può causare un consumo elevato di memoria. Per risolvere il problema, aggiornare il software dell'appliance di sicurezza.

- **Debug abilitato:** il debug può richiedere grandi quantità di memoria. Per risolvere il problema, disabilitare il debug con il comando `undebug all`.

- **Blocco delle porte:** il blocco delle porte sull'interfaccia esterna di un accessorio di sicurezza provoca un utilizzo elevato di memoria da parte dell'accessorio di sicurezza per bloccare i pacchetti tramite le porte specificate. Per risolvere il problema, bloccare il traffico in conflitto all'estremità dell'ISP.

- **Threat-Detection:** la funzione di rilevamento delle minacce è composta da diversi livelli di statistiche raccolte per le varie minacce e da un sistema scansionato che determina quando un host esegue una scansione. **Disattivare** questa funzionalità per ridurre il consumo di memoria.

PortFast, Channel e Trunking

Per impostazione predefinita, molti switch, ad esempio gli switch Cisco con sistema operativo Catalyst, sono progettati per essere dispositivi plug-and-play. Di conseguenza, molti parametri della porta predefinita non sono desiderabili quando un'ASA è collegata allo switch. Ad esempio, su uno switch con sistema operativo Catalyst, il channeling predefinito è impostato su Auto, il trunking è impostato su Auto e PortFast è disabilitato. Se si collega un'ASA a uno switch con sistema operativo Catalyst, disabilitare il channeling, disabilitare il trunking e abilitare PortFast.

Il channeling, noto anche come Fast EtherChannel o Giga EtherChannel, viene usato per collegare due o più porte fisiche in un gruppo logico al fine di aumentare la velocità di trasmissione complessiva attraverso il collegamento. Quando una porta è configurata per il channeling automatico, invia i frame PAgP (Port Aggregation Protocol) quando il collegamento diventa attivo per determinare se fa parte di un canale. Questi frame possono causare problemi se l'altro dispositivo tenta di negoziare automaticamente la velocità e il duplex del collegamento. Se il channeling sulla porta è impostato su Auto, si verificherà un ulteriore ritardo di circa 3 secondi prima che la porta inizi a inoltrare il traffico dopo l'attivazione del collegamento.

Nota: sugli switch Catalyst serie XL, il channeling non è impostato su Auto per impostazione predefinita. Per questo motivo, è necessario disabilitare il channeling su tutte le porte dello switch che si connettono a un'ASA.

Il trunking, noto anche con i comuni protocolli di trunking ISL (Inter-Switch Link) o Dot1q, combina più LAN virtuali (VLAN) su una singola porta (o collegamento). Il trunking viene in genere utilizzato tra due switch quando su entrambi gli switch è definita più di una VLAN. Quando una porta è configurata per il trunking automatico, invia frame DTP (Dynamic Trunking Protocol) quando il collegamento viene attivato per determinare se la porta a cui si connette desidera eseguire il trunking. Questi frame DTP possono causare problemi con la negoziazione automatica del collegamento. Se il trunking è impostato su Auto su una porta dello switch, viene aggiunto un ritardo aggiuntivo di circa 15 secondi prima che la porta inizi a inoltrare il traffico dopo l'attivazione del collegamento.

PortFast, nota anche come Fast Start, è un'opzione che informa lo switch che un dispositivo di layer 3 è connesso tramite una porta dello switch. La porta non attende i 30 secondi predefiniti (15 secondi per l'ascolto e 15 secondi per l'apprendimento); al contrario, questa azione determina il passaggio della porta allo stato di inoltro subito dopo l'accensione del collegamento. È importante ricordare che quando si abilita PortFast, lo Spanning Tree non è disabilitato. Lo Spanning Tree è ancora attivo su questa porta. Quando si abilita PortFast, lo switch viene informato solo del fatto che non vi è alcun altro switch o hub (dispositivo di solo livello 2) connesso all'altra estremità del collegamento. Lo switch ignora il ritardo normale di 30 secondi mentre tenta di determinare se un loop di layer 2 genera la porta. Dopo che il link è stato menzionato, partecipa ancora allo Spanning Tree. La porta invia unità BDPU (Bridge Packet Data Unit) e lo switch è ancora in ascolto di BPDU su tale porta. Per questi motivi, è consigliabile abilitare PortFast su qualsiasi porta dello switch che si connette a un'ASA.

Nota: il sistema operativo Catalyst versione 5.4 e successive includono il comando cheset port host <mod>/<port> consente di utilizzare un singolo comando per disabilitare il channeling, disabilitare il trunking e abilitare PortFast.

NAT (Network Address Translation)

A ciascuna sessione NAT o NAT Overload (PAT) viene assegnato uno slot di conversione noto come *xlate*. Tali espressioni possono persistere anche dopo aver apportato modifiche alle regole NAT che li riguardano. Ciò può comportare l'esaurimento degli slot di traduzione o un comportamento imprevisto o entrambi dovuti al traffico che viene tradotto. In questa sezione viene illustrato come visualizzare e cancellare le espressioni sull'appliance di sicurezza.

Attenzione: quando si azzerano gli xlat sul dispositivo di sicurezza, si può verificare un'interruzione momentanea del flusso di tutto il traffico che attraversa il dispositivo.

Esempio di configurazione ASA di una porta che usa l'indirizzo IP dell'interfaccia esterna:

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

Il traffico che attraversa l'appliance di sicurezza passa molto probabilmente a NAT. Per visualizzare le traduzioni in uso sull'appliance di sicurezza, eseguire il comandoshow xlate :

<#root>

Ciscoasa#

show xlate

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

Gli slot di conversione possono essere mantenuti anche dopo aver apportato modifiche importanti. Per cancellare gli slot di conversione correnti sull'appliance di sicurezza, usare il clear xlate comando:

<#root>

Ciscoasa#

clear xlate

<#root>

Ciscoasa#

show xlate

0 in use, 1 most used

Il comandoclear xlate cancella tutta la traslazione dinamica corrente dalla tabella xlate. Per cancellare una particolare traduzione IP, si può usare il comandoclear xlate con la parola chiaveglobal [ip address].

Di seguito è riportato un esempio di configurazione ASA per 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

Osservate l'output dellashow xlate traslazione da 10.2.2.2 a 10.10.10.10 globale esterno:

<#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

Cancella la traduzione dell'indirizzo IP globale 10.10.10.10:

<#root>

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

Nell'esempio, la traduzione di inside 10.2.2.2 verso outside global 10.10.10.10 non è più disponibile:

```
<#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
```

Syslog

I syslog permettono di risolvere i problemi relativi all'appliance ASA. Cisco offre un server syslog gratuito per Windows NT chiamato ASA Firewall Syslog Server (PFSS). È possibile scaricare PFSS da Cisco Technical Support & Downloads.

Diversi altri fornitori, come ad esempio Windows 2000 e Windows XP, offrono server syslog per diverse piattaforme Windows. Per impostazione predefinita, nella maggior parte dei sistemi UNIX e Linux sono installati server syslog.

Quando si configura il server syslog, configurare l'ASA in modo che possa ricevere i log.

Ad esempio:

<#root>

logging on logging host <ip_address_of_syslog_server> logging trap debugging

---

Nota: nell'esempio seguente l'ASA viene configurata in modo da inviare al server syslog il debug (livello 7) e i syslog più critici. Poiché i registri ASA sono i più dettagliati, utilizzarli solo per risolvere il problema. Per il normale funzionamento, configurare il livello di registrazione su Avviso (livello 4) o Errore (livello 3).

Se si verifica un problema di prestazioni lente, aprire il syslog in un file di testo e cercare l'indirizzo IP di origine associato al problema di prestazioni. Se si utilizza UNIX, è possibile `utilizzare` il syslog per ottenere l'indirizzo IP di origine. Verificare la presenza di messaggi che indicano che il server esterno ha tentato di accedere all'indirizzo IP interno sulla porta TCP 113 (per il protocollo di identificazione o il rientro), ma l'ASA ha negato il pacchetto. Il messaggio deve essere simile all'esempio seguente:

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

Se viene visualizzato questo messaggio, inviare il service resetinboundcomando all'appliance ASA. L'appliance ASA non scarta i pacchetti in modo invisibile all'utente, ma reimposta immediatamente tutte le connessioni in entrata negate dal criterio di sicurezza. Il server non attende il timeout della connessione TCP del pacchetto Ident, ma riceve immediatamente un pacchetto di ripristino.

SNMP

Un metodo consigliato per le implementazioni aziendali è monitorare le prestazioni di Cisco ASA con SNMP. Cisco ASA supporta questa funzionalità con il protocollo SNMP versioni 1, 2c e 3.

È possibile configurare l'appliance di sicurezza in modo che invii trap a un Network Management Server (NMS) oppure utilizzare il NMS per sfogliare i MIB sull'appliance di sicurezza. I MIB sono un insieme di definizioni e l'appliance di sicurezza gestisce un database di valori per ogni definizione. Per ulteriori informazioni, consultare la guida alla configurazione di Cisco ASA serie 5500 con CLI, 8.4 e 8.6.

Tutti i MIB supportati per Cisco ASA sono disponibili nell'elenco dei servizi di supporto MIB per ASA. Da questo elenco, questi MIB sono utili per il monitoraggio delle prestazioni:

- CISCO-FIREWALL-MIB: contiene oggetti utili per il failover.
- CISCO-PROCESS-MIB: contiene oggetti utili per l'utilizzo della CPU.
- CISCO-MEMORY-POOL-MIB: contiene oggetti utili per gli oggetti di memoria.

Ricerche DNS inverse

Se le prestazioni dell'appliance ASA sono lente, verificare che nel server DNS autorevole siano presenti record DNS puntatore (DNS), detti anche record di ricerca DNS inversa, per gli indirizzi esterni utilizzati dall'appliance. Sono inclusi tutti gli indirizzi del pool NAT (Network Address Translation) globale (o l'interfaccia esterna ASA se sovraccarica l'interfaccia), tutti gli indirizzi statici e gli indirizzi interni (se non si utilizza NAT con essi). Alcune applicazioni, ad esempio i server FTP (File Transfer Protocol) e Telnet, possono utilizzare ricerche DNS inverse per determinare la provenienza dell'utente e se si tratta di un host valido. Se la ricerca DNS inversa non viene risolta, le prestazioni risulteranno ridotte a causa del timeout della richiesta.

Per verificare l'esistenza di un record PTR per questi host, eseguire il comando dalnslookup computer PC o UNIX e includere l'indirizzo IP globale utilizzato per la connessione a Internet.

Esempio

<#root>

```
% nslookup 192.168.219.25

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

È necessario ricevere una risposta con il nome DNS del dispositivo assegnato a tale indirizzo IP. Se non si riceve una risposta, contattare la

persona che controlla il DNS per richiedere l'aggiunta di record PTR per ogni indirizzo IP globale.

Sovraccarichi sull'interfaccia

Se si verifica un burst di traffico, i pacchetti scartati possono verificarsi se il burst supera la capacità di buffer del buffer FIFO sulla scheda NIC e sui buffer ring di ricezione. Per risolvere il problema, attivare i frame di pausa per il controllo del flusso. I frame di pausa (XOFF) e XON vengono generati automaticamente dall'hardware della scheda NIC in base all'utilizzo del buffer FIFO. Un frame di pausa viene inviato quando l'utilizzo del buffer supera il limite massimo. Per abilitare i frame di pausa (XOFF) per il controllo del flusso, utilizzare questo comando:

<#root>

hostname(config)#

interface tengigabitethernet 1/0

hostname(config-if)#

flowcontrol send on

Comandi show

Mostra utilizzo CPU

Il comandoshow cpu usage viene usato per determinare il carico di traffico sulla CPU dell'ASA. Durante i picchi di traffico, i picchi di rete o gli attacchi, l'utilizzo della CPU può aumentare vertiginosamente.

L'ASA ha una sola CPU per elaborare una varietà di attività; ad esempio, elabora i pacchetti e stampa i messaggi di debug sulla console. Ciascun processo ha un proprio scopo e alcuni processi richiedono più tempo di CPU rispetto ad altri. La crittografia è probabilmente il processo che impiega più tempo la CPU, quindi se l'ASA trasmette molto traffico attraverso i tunnel crittografati, dovete prendere in considerazione un'ASA più veloce, un concentratore VPN dedicato, come VPN 3000. Il VAC scarica la crittografia e la decrittografia dalla CPU dell'ASA e la esegue nell'hardware della scheda. Questo consente all'ASA di crittografare e decrittografare 100 Mbps di traffico con 3DES (crittografia a 168 bit).

La registrazione è un altro processo che può utilizzare grandi quantità di risorse di sistema. Per questo motivo, è consigliabile disabilitare la

registrazione su console, monitor e buffer sull'appliance ASA. È possibile attivare questi processi quando si risolve un problema, ma disattivarli per il funzionamento quotidiano, soprattutto se si esaurisce la capacità della CPU. Si consiglia inoltre di impostare syslog o la registrazione SNMP (Simple Network Management Protocol) (cronologia di registrazione) sul livello 5 (Notification) o su un livello inferiore. Inoltre, è possibile disabilitare gli ID dei messaggi syslog specifici con il no logging message <syslog_id> comando.

Anche Cisco Adaptive Security Device Manager (ASDM) contiene un grafico Monitoring nella scheda che consente di visualizzare l'utilizzo della CPU dell'appliance ASA nel tempo. È possibile usare questo grafico per determinare il carico sull'appliance ASA.

Il **show cpu usage** comando può essere utilizzato per visualizzare le statistiche di utilizzo della CPU.

Esempio

<#root>

Ciscoasa#

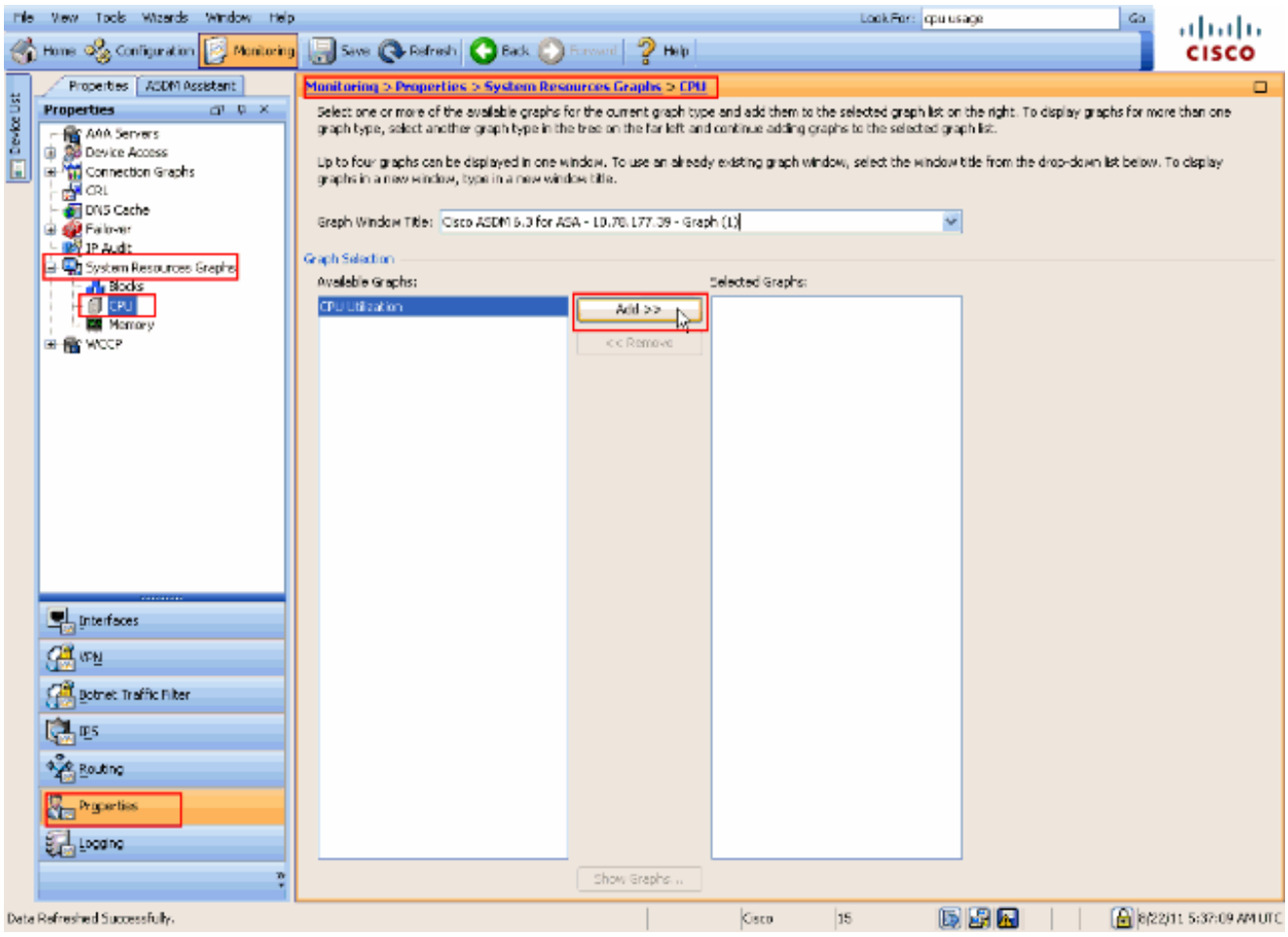
show cpu usage

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

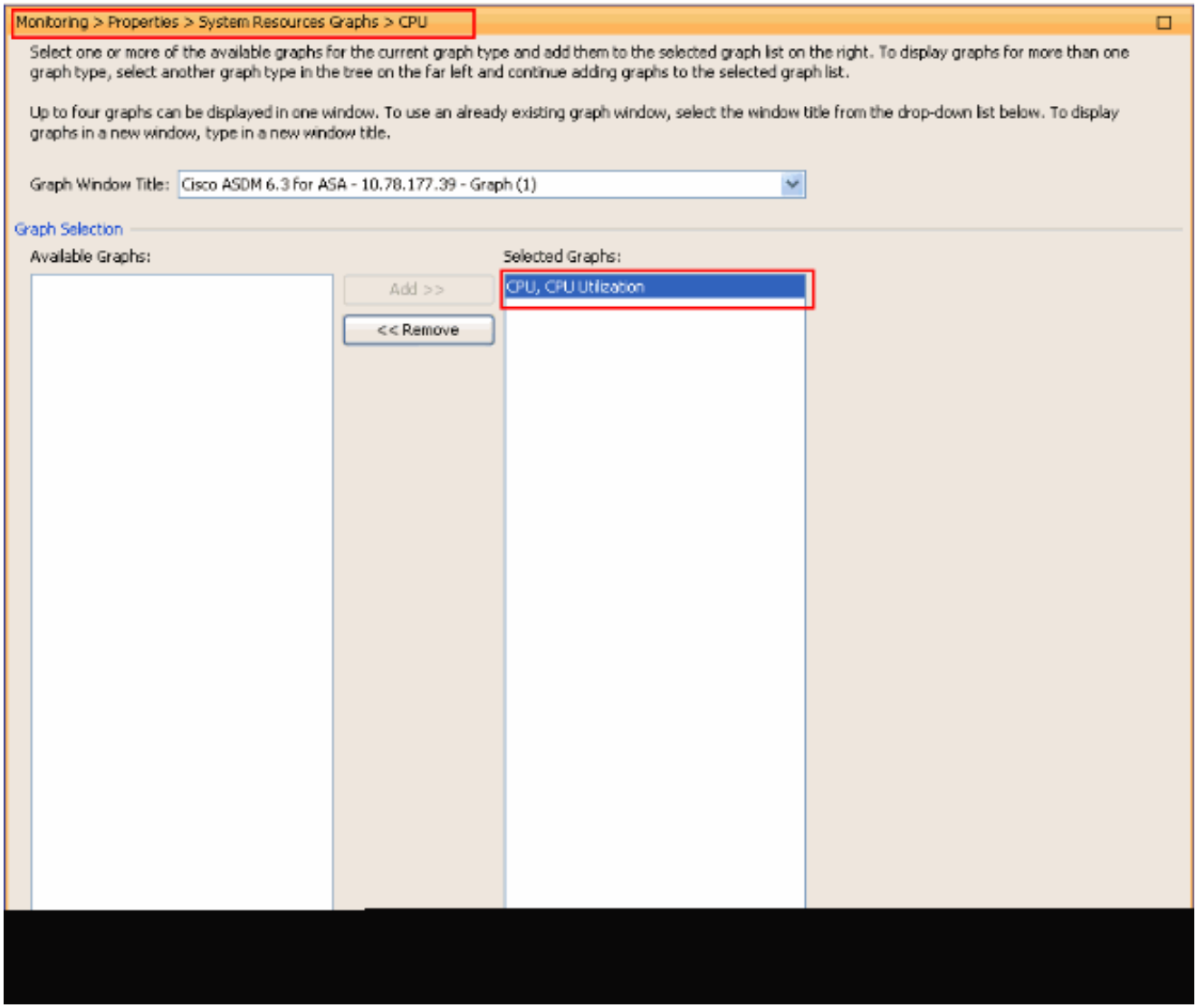
Visualizza utilizzo CPU su ASDM

Per visualizzare l'utilizzo della CPU sull'ASDM, completare la procedura seguente:

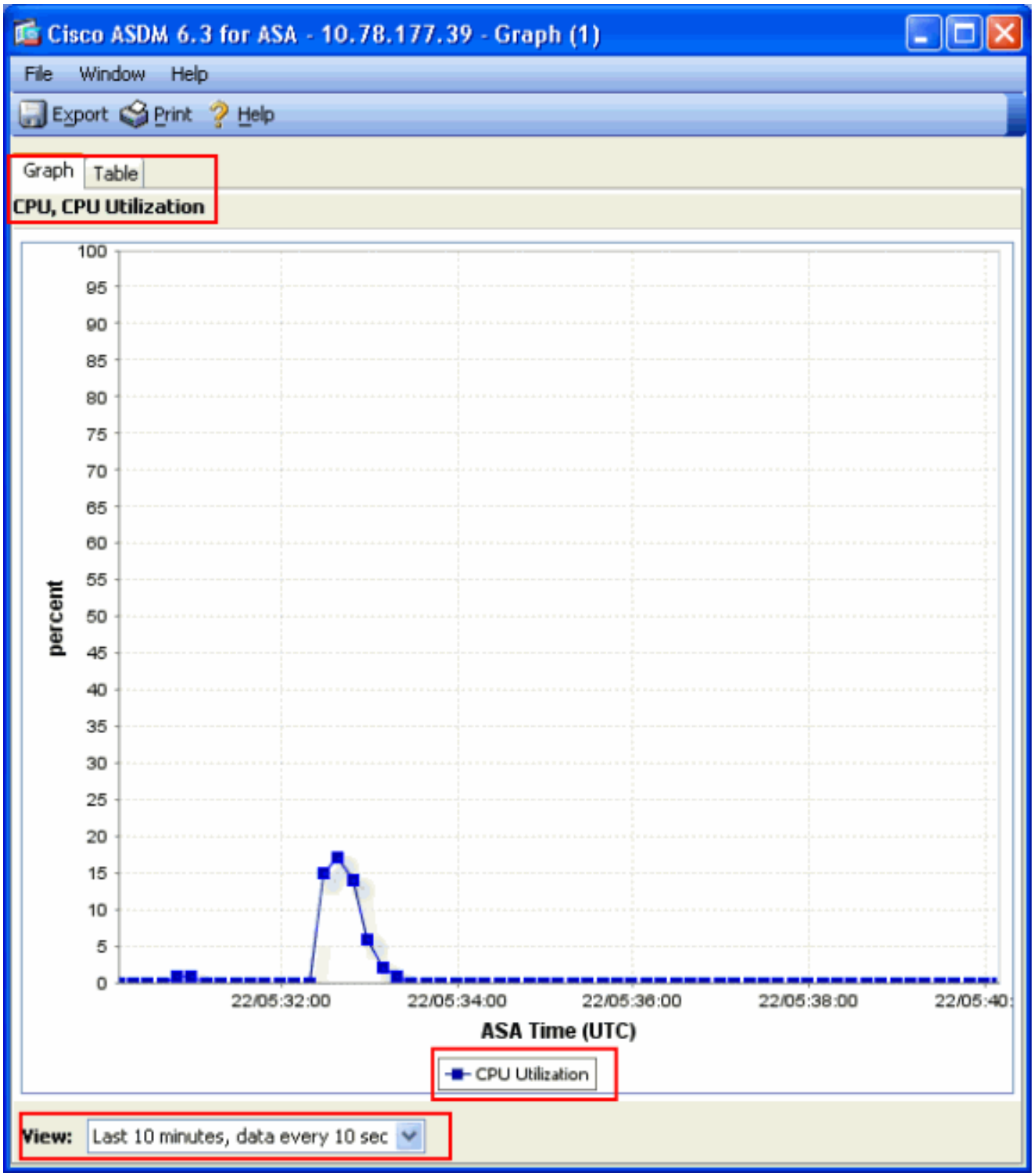
- AndareMonitoring > Properties > System Resources Graphics > CPU a in ASDM e scegliere il **titolo della finestra del grafico**. Quindi, scegliete i grafici desiderati dall'elenco **Grafici disponibili** e fate clic su **Aggiungi** come mostrato.



- Una volta aggiunto il nome del grafico richiesto nella sezione **Grafici selezionati**, fate clic su **Mostra grafici** (**Show Graphs)**.



L'immagine seguente mostra il grafico **Uso CPU** su ASDM. Sono disponibili diverse visualizzazioni di questo grafico che possono essere modificate quando si seleziona la visualizzazione dall'elenco a discesa Vista. È possibile stampare o salvare l'output sul computer in base alle esigenze.



Descrizione dell'output

Questa tabella descrive i campi dell' **show cpu usage** output.

Campo	Descrizione
Utilizzo CPU per 5 secondi	Utilizzo della CPU negli ultimi cinque secondi
1 minuto	Media di 5 campioni di utilizzo della CPU nell'ultimo minuto
5 minuti	Media di campioni di utilizzo CPU di 5 secondi negli ultimi cinque minuti

Mostra traffico

Il comandoshow traffic mostra il traffico che attraversa l'ASA in un determinato periodo di tempo. I risultati si basano sull'intervallo di tempo trascorso dall'ultima esecuzione del comando. Per ottenere risultati accurati, usare prima il **clear traffic** comando, quindi attendere 1-10 minuti prima di usare il show traffic comando. È inoltre possibile eseguire il comando e attendere 1-10 minuti prima di eseguirlo di nuovo,show traffic ma è valido solo l'output della seconda istanza.

È possibile usare il comandoshow traffic per determinare la quantità di traffico che attraversa l'appliance ASA. Se si dispone di più interfacce, il comando consente di determinare quali interfacce inviano e ricevono la maggior parte dei dati. Per gli appliance ASA con due interfacce, la somma del traffico in entrata e del traffico in uscita sull'interfaccia esterna deve essere uguale alla somma del traffico in entrata e del traffico in uscita sull'interfaccia interna.

Esempio

<#root>

Ciscoasa#

show traffic

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

Se il throughput di un'interfaccia è prossimo o raggiunto, è necessario eseguire l'aggiornamento a un'interfaccia più veloce o limitare la quantità

di traffico in entrata o in uscita dall'interfaccia. In caso contrario, i pacchetti potrebbero essere ignorati. Come spiegato nella **show interface**sezione, è possibile esaminare i contatori dell'interfaccia per conoscere il throughput.

Mostra Perfmon

Il comandoshow perfmon viene usato per monitorare la quantità e i tipi di traffico che l'ASA controlla. Questo comando è l'unico modo per determinare il numero di conversioni (xlate) e connessioni (conn) al secondo. Le connessioni sono ulteriormente suddivise in connessioni TCP e UDP (User Datagram Protocol). Per le descrizioni dell'output generato da questo comando, vedere **Descrizione dell'output**.

Esempio

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

Descrizione dell'output

In questa tabella vengono descritti i campi dell'show perfmon output.

Campo	Descrizione
Xlate	Traduzioni create al secondo
Connessioni	Connessioni stabilite al secondo
Conn TCP	Connessioni TCP al secondo
Conn. UDP	Connessioni UDP al secondo
Accesso URL	URL (siti Web) a cui si accede al secondo

Richiesta server URL	Richieste inviate a Websense e N2H2 al secondo (richiede il filter comando)
Correzione TCP	Numero di pacchetti TCP inoltrati dall'ASA al secondo
IntercettaTCP	Numero di pacchetti SYN al secondo che hanno superato il limite embrionale impostato su un pacchetto statico
Correzione HTTP	Numero di pacchetti destinati alla porta 80 al secondo (richiede fixup protocol httpil comando)
Correzione FTP	Comandi FTP ispezionati al secondo
AAA Authen	Richieste di autenticazione al secondo
Autore AAA	Richieste di autorizzazione al secondo
Account AAA	Richieste di accounting al secondo

Mostra blocchi

Insieme al comando,show cpu usage è possibile usare il show blockscomando per determinare se l'ASA è in sovraccarico.

Blocchi pacchetti (1550 e 16384 byte)

Quando arriva all'interfaccia ASA, un pacchetto viene inserito nella coda dell'interfaccia di input, trasmesso al sistema operativo e inserito in un blocco. Per i pacchetti Ethernet, vengono utilizzati i blocchi da 1550 byte; se il pacchetto viene fornito su una scheda Gigabit Ethernet da 66 MHz, vengono utilizzati i blocchi da 16384 byte. L'ASA determina se il pacchetto è autorizzato o rifiutato in base all'algoritmo ASA (Adaptive Security Algorithm) ed elabora il pacchetto attraverso la coda di output sull'interfaccia in uscita. Se l'ASA non può supportare il carico del traffico, il numero di blocchi disponibili da 1550 byte (o blocchi da 16384 byte per il GRE da 66 MHz) rimane vicino a 0 (come mostrato nella colonna CNT dell'output del comando). Quando la colonna CNT raggiunge lo zero, l'ASA cerca di allocare più blocchi, fino a un massimo di 8192. Se non sono disponibili altri blocchi, l'ASA scarta il pacchetto.

Blocchi di failover e syslog (256 byte)

I blocchi da 256 byte vengono utilizzati principalmente per i messaggi di failover stateful. L'appliance ASA attiva genera e invia pacchetti all'appliance ASA in standby per aggiornare la tabella di conversione e connessione. Durante i periodi di traffico bursty in cui vengono create o eliminate elevate velocità di connessione, il numero di blocchi da 256 byte disponibili può scendere a 0. Questo rilascio indica che una o più connessioni non sono aggiornate all'appliance ASA in standby. Questa operazione è in genere accettabile in quanto la volta successiva che il protocollo di failover stateful rileva l'estensione o la connessione perduta. Tuttavia, se la colonna CNT per blocchi di 256 byte rimane uguale o vicina allo 0 per periodi di tempo estesi, l'ASA non può tenere il passo con le tabelle di conversione e di connessione sincronizzate a causa del numero di connessioni al secondo elaborate dall'ASA. Se il problema persiste, aggiornare l'ASA a un modello più veloce.

I messaggi syslog inviati dall'appliance ASA utilizzano anche i blocchi da 256 byte, ma in genere non vengono rilasciati in una quantità tale da causare l'esaurimento del pool di blocchi da 256 byte. Se la colonna CNT indica che il numero di blocchi di 256 byte è vicino a 0, accertarsi di non eseguire il log al Debugging (livello 7) sul server syslog. Ciò è indicato dalla riga di registrazione della trap nella configurazione ASA. È consigliabile impostare la registrazione su Notifica (livello 5) o su un livello inferiore, a meno che non siano necessarie ulteriori informazioni a scopo di debug.

Esempio

<#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
```

Descrizione dell'output

In questa tabella vengono descritte le colonne dell'show blocksoutput.

Colonna	Descrizione
DIMENSIONI	E Dimensioni in byte del pool di blocchi. Ogni dimensione rappresenta un tipo

	particolare
MAX	Numero massimo di blocchi disponibili per il pool di blocchi di byte specificato. Il numero massimo di blocchi viene scomposto nella memoria all'avvio. In genere, il numero massimo di blocchi non cambia. Fanno eccezione i blocchi da 256 e 1550 byte, in cui l'appliance di sicurezza adattiva può creare dinamicamente più elementi quando necessario, fino a un massimo di 8192.
BASSA	Livello minimo. Questo numero indica il numero più basso di blocchi di queste dimensioni disponibili da quando l'appliance Adaptive Security è stata accesa o dall'ultima cancellazione dei blocchi (con il comando cancella blocchi). Uno zero nella colonna LOW indica un evento precedente in cui la memoria era piena.
CNT	Numero corrente di blocchi disponibili per il pool di blocchi di dimensioni specifiche. Uno zero nella colonna CNT indica che la memoria è piena.

In questa tabella vengono descritti i valori della riga SIZE nell'show blocksoutput.

Valore SIZE	Descrizione
0	Utilizzato dai blocchi di copia.
4	Duplica i blocchi esistenti in applicazioni quali DNS, ISAKMP, filtro URL, auth, TFTP e moduli TCP. Inoltre, questo blocco di dimensioni ridotte può essere utilizzato normalmente dal codice per inviare pacchetti ai driver e così via.
80	Utilizzato nell'intercetta TCP per generare pacchetti di conferma e per i messaggi di supporto del failover.
256	Utilizzato per aggiornamenti di failover stateful, registrazione syslog e altre funzioni TCP. Questi blocchi vengono utilizzati principalmente per i messaggi di failover stateful. L'appliance di sicurezza adattiva attiva genera e invia pacchetti all'appliance di sicurezza adattiva in standby per aggiornare la tabella di conversione e di connessione. Nel traffico bursty, dove vengono create o eliminate elevate velocità di connessione, il numero di blocchi disponibili può scendere a 0. Questa situazione indica che una o più connessioni non sono state aggiornate all'appliance di sicurezza adattiva in standby. Il protocollo di

	failover stateful intercetta la traduzione o la connessione persa la volta successiva. Se la colonna CNT per blocchi da 256 byte rimane uguale o vicina allo 0 per lunghi periodi di tempo, Adaptive Security Appliance non riesce a mantenere sincronizzate le tabelle di conversione e di connessione a causa del numero di connessioni al secondo elaborate da Adaptive Security Appliance. I messaggi di syslog inviati dall'appliance di sicurezza adattiva utilizzano anche blocchi da 256 byte, ma in genere non vengono rilasciati in una quantità tale da causare l'esaurimento del pool di blocchi da 256 byte. Se la colonna CNT mostra che il numero di blocchi di 256 byte è vicino a 0, accertarsi di non eseguire il login al server syslog al livello 7 del debug. Ciò è indicato dalla linea di registrazione nella configurazione di adaptive security appliance. È consigliabile impostare la registrazione su Notifica (livello 5) o su un livello inferiore, a meno che non siano necessarie ulteriori informazioni a scopo di debug.
1550	Utilizzato per memorizzare pacchetti Ethernet da elaborare attraverso l'appliance Adaptive Security. Quando un pacchetto entra nell'interfaccia di un'appliance di sicurezza adattiva, viene inserito nella coda dell'interfaccia di input, trasmesso al sistema operativo e inserito in un blocco. L'appliance di sicurezza adattiva determina se il pacchetto deve essere autorizzato o rifiutato in base al criterio di sicurezza ed elabora il pacchetto attraverso la coda di output sull'interfaccia in uscita. Se l'appliance di sicurezza adattiva non riesce a tenere il passo con il carico del traffico, il numero di blocchi disponibili può essere quasi zero (come mostrato nella colonna CNT dell'output del comando). Quando la colonna CNT è pari a zero, l'accessorio Adaptive Security tenta di allocare più blocchi, fino a un massimo di 8192. Se non sono disponibili altri blocchi, il pacchetto viene scartato dall'appliance di sicurezza adattiva.
16384	Utilizzato solo per le schede Gigabit Ethernet a 64 bit e 66 MHz (i82543). Per ulteriori informazioni sui pacchetti Ethernet, vedere la descrizione del modello 1550.
2048	Controllo o frame guidati utilizzati per gli aggiornamenti del controllo.

Mostra memoria

Il comandoshow memory visualizza la memoria fisica (o RAM) totale per l'ASA, insieme al numero di byte attualmente disponibili. Per utilizzare queste informazioni, è necessario anzitutto comprendere come l'appliance ASA usa la memoria. All'avvio, l'ASA copia il sistema operativo dalla memoria flash alla RAM e lo esegue dalla RAM (proprio come i router). Successivamente, l'ASA copia la configurazione di avvio da Flash e la inserisce nella RAM. Infine, l'ASA alloca la RAM per creare i pool di blocchi discussi nella show blocks sezione. Una volta completata l'allocazione, l'ASA ha bisogno di ulteriore RAM solo se la configurazione aumenta. Inoltre, l'ASA memorizza le voci di traduzione e connessione nella RAM.

Durante il normale funzionamento, la memoria libera sull'appliance ASA deve cambiare poco o nulla. In genere, la memoria deve essere insufficiente solo se si è sotto attacco e centinaia di migliaia di connessioni passano attraverso l'appliance ASA. Per controllare le connessioni, usare il comando show conn count show, che visualizza il numero massimo e corrente di connessioni tramite l'appliance ASA. Se la memoria dell'appliance ASA si esaurisce, il sistema si blocca. Prima dell'arresto anomalo del sistema, nel syslog (%ASA-3-211001) vengono visualizzati messaggi di errore relativi all'allocazione della memoria.

Se la memoria è insufficiente a causa di un attacco, rivolgersi al team di supporto tecnico Cisco.

Esempio

<#root>

Ciscoasa#

```
show memory

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

Mostra Xlate

Il comandoshow xlate count visualizza il numero corrente e il numero massimo di conversioni tramite l'appliance ASA. Una traduzione è un mapping tra un indirizzo interno e un indirizzo esterno e può essere un mapping uno-a-uno, ad esempio NAT (Network Address Translation) o molti-a-uno, ad esempio PAT (Port Address Translation). Questo comando è un sottoinsieme del comando stessoshow xlate, che restituisce ciascuna traduzione tramite l'appliance ASA. L'output del comando visualizza le traduzioni "in uso", che si riferiscono al numero di traduzioni attive nell'appliance ASA quando il comando viene emesso. Il valore "most used" (più usato) si riferisce alle massime traduzioni mai viste sull'appliance ASA da quando è stata accesa.

Nota: un singolo host può avere più connessioni a varie destinazioni, ma solo una conversione. Se il numero di host è molto maggiore del numero di host presenti sulla rete interna, è possibile che uno degli host interni sia stato compromesso. Se l'host interno è stato compromesso, falsifica l'indirizzo di origine e invia i pacchetti all'appliance ASA.

Nota: quando la configurazione vpnclient è abilitata e l'host interno invia richieste DNS, il comando può elencare più xlate per una traduzione statica.**Nota**: quando la configurazione vpnclient è abilitata e l'host interno invia richieste DNS, il show xlate comando può elencare più xlate per una traduzione statica.

Esempio

<#root>

Ciscoasa#

show xlate count

 84 in use, 218 most used

<#root>

Ciscoasa(config)#

show xlate

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

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

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

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

La prima voce è una conversione degli indirizzi della porta TCP per la porta host (10.1.1.15, 1026) sulla rete interna verso la porta host (192.168.49.1, 1024) sulla rete esterna. Il flag "r" indica che la traduzione è una Port Address Translation. Il flag "i" indica che la traduzione viene applicata alla porta indirizzo interna.

La seconda voce è una traduzione dell'indirizzo della porta UDP per la porta host (10.1.1.15, 1028) sulla rete interna fino alla porta host (192.168.49.1, 1024) sulla rete esterna. Il flag "r" indica che la traduzione è una Port Address Translation. Il flag "i" indica che la traduzione viene applicata alla porta indirizzo interna.

La terza voce è una traduzione dell'indirizzo della porta ICMP per l'host-ICMP-id (10.1.1.15, 21505) sulla rete interna fino all'host-ICMP-id (192.168.49.1, 0) sulla rete esterna. Il flag "r" indica che la traduzione è una Port Address Translation. Il flag "i" indica che la traduzione si

applica all'indirizzo interno-ICMP-id.

I campi dell'indirizzo interno vengono visualizzati come indirizzi di origine sui pacchetti che attraversano l'interfaccia più protetta fino a quella meno protetta. Viceversa, appaiono come indirizzi di destinazione sui pacchetti che attraversano l'interfaccia meno sicura e passano all'interfaccia più sicura.

Mostra conteggio conn.

Il comandoshow conn count mostra il numero di connessioni correnti e massime attraverso l'appliance ASA. Una connessione è un mapping di informazioni di livello 4 da un indirizzo interno a un indirizzo esterno. Le connessioni vengono costruite quando l'ASA riceve un pacchetto SYN per le sessioni TCP o quando arriva il primo pacchetto in una sessione UDP. Le connessioni vengono interrotte quando l'ASA riceve il pacchetto ACK finale, ossia quando l'handshake della sessione TCP viene chiuso o quando scade il timeout nella sessione UDP.

Un numero di connessioni estremamente elevato (50-100 volte superiore al normale) può indicare un attacco. Per verificare che il numero elevato di connessioni non causishow memory un esaurimento della memoria dell'appliance ASA, eseguire il comando. Se si è sotto attacco, è possibile limitare il numero massimo di connessioni per voce statica e limitare il numero massimo di connessioni embrionali. Questa azione consente di proteggere i server interni, in modo che non risultino sovraccarichi. Per ulteriori informazioni, consultare la guida alla configurazione di Cisco ASA serie 5500 con CLI, 8.4 e 8.6.

Esempio

<#root>

Ciscoasa#

```
show conn count
```

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

show interface

Il comando show interface può aiutare a determinare i problemi di mancata corrispondenza del duplex e i problemi dei cavi. Inoltre, permette di stabilire se l'interfaccia è sovraccarica o meno. Se la capacità della CPU dell'ASA si esaurisce, il numero di blocchi da 1550 byte si avvicina a 0.

(Osservare i blocchi da 16384 byte sulle schede Gig da 66 MHz). Un altro indicatore è l'aumento del numero di "no buffer" sull'interfaccia. Il messaggio no buffer indica che l'interfaccia non è in grado di inviare il pacchetto al sistema operativo ASA perché non è disponibile alcun blocco per il pacchetto, che viene quindi scartato. Se l'aumento dei livelli di buffer non si verifica regolarmente, usare il comandoshow proc cpu per controllare l'utilizzo della CPU sull'appliance ASA. Se l'utilizzo della CPU è elevato a causa di un carico elevato del traffico, aggiornare l'appliance ASA a una versione più potente in grado di gestire il carico.

Quando un pacchetto entra per la prima volta in un'interfaccia, viene inserito nella coda dell'hardware di input. Se la coda hardware di input è piena, il pacchetto viene inserito nella coda software di input. Il pacchetto viene passato dalla coda di input e inserito in un blocco da 1550 byte (o in un blocco da 16384 byte su interfacce Gigabit Ethernet da 66 MHz). L'ASA determina quindi l'interfaccia di output per il pacchetto e inserisce il pacchetto nella coda hardware appropriata. Se la coda dell'hardware è piena, il pacchetto viene inserito nella coda del software di output. Se il numero massimo di blocchi in una delle code software è elevato, l'interfaccia risulta sovraccarica. Ad esempio, se 200 Mbps entrano nell'ASA e tutti escono da una singola interfaccia da 100 Mbps, la coda del software di output indica un numero elevato sull'interfaccia in uscita, che indica che l'interfaccia non può gestire il volume di traffico. In questo caso, eseguire l'aggiornamento a un'interfaccia più veloce.

Esempio

<#root>

Ciscoasa#

```
show interface
```

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

È inoltre necessario verificare la presenza di errori nell'interfaccia. Se si ricevono runt, errori di input, CRC o errori di frame, è probabile che si sia verificata una mancata corrispondenza del duplex. Il cavo può essere difettoso. Per ulteriori informazioni sui problemi del duplex, vedere Impostazioni velocità e duplex. Tenere presente che ogni contatore di errori rappresenta il numero di pacchetti ignorati a causa di un determinato errore. Se si rileva un contatore specifico che aumenta regolarmente, le prestazioni dell'appliance ASA potrebbero risentirne e sarà necessario individuare la causa principale del problema.

Quando si esaminano i contatori dell'interfaccia, notare che se l'interfaccia è impostata su full-duplex, non si devono verificare collisioni, collisioni ritardate o pacchetti differiti. Al contrario, se l'interfaccia è impostata sulla modalità half-duplex, è necessario ricevere le collisioni, alcune collisioni ritardate e possibilmente alcuni pacchetti differiti. Il numero totale di collisioni, collisioni ritardate e pacchetti differiti non deve superare il 10% della somma dei contatori dei pacchetti di input e output. Se le collisioni superano il 10% del traffico totale, il collegamento viene sovrautilizzato e sarà necessario eseguire l'aggiornamento alla modalità full-duplex o a una velocità superiore (da 10 Mbps a 100 Mbps). Tenere presente che le collisioni del 10% indicano che l'ASA scarta il 10% dei pacchetti che passano attraverso l'interfaccia; ciascun pacchetto deve essere ritrasmesso.

Per informazioni dettagliate sui contatori dell'interfaccia, consultare le interface istruzioni in Cisco ASA serie 5500 Adaptive Security Appliance.

Mostra processi

Il comando**show processes** sull'appliance ASA visualizza tutti i processi attivi che vengono eseguiti sull'appliance al momento dell'esecuzione del comando. Queste informazioni sono utili per determinare quali processi ricevono un tempo di CPU eccessivo e quali processi non ricevono alcun tempo di CPU. Per ottenere queste informazioni, eseguire il **show processes** comando due volte; attendere circa 1 minuto tra ciascuna istanza. Per il processo in questione, sottrarre il valore Runtime visualizzato nel secondo output dal valore Runtime visualizzato nel primo output. Questo risultato mostra la quantità di tempo CPU (in millisecondi) ricevuta dal processo in tale intervallo di tempo. Si noti che alcuni processi sono pianificati per l'esecuzione a intervalli specifici e che alcuni processi vengono eseguiti solo quando dispongono di informazioni da elaborare. Il processo di polling 577 ha probabilmente il valore di runtime più elevato tra tutti i processi. Si tratta di un comportamento normale, in quanto il processo di polling 577 esegue un polling delle interfacce Ethernet per verificare se contengono dati da elaborare.

Nota: l'esame di ciascun processo ASA non rientra nell'ambito del presente documento, ma viene brevemente menzionato per completezza. Per ulteriori informazioni sui processi ASA, fare riferimento a ASA 8.3 e versioni successive: monitoraggio e risoluzione dei problemi di prestazioni.

Riepilogo dei comandi

In breve, usare il comandoshow cpu usage per identificare il carico dell'appliance ASA. Tenere presente che l'output è una media continua; l'ASA può avere picchi più alti di utilizzo della CPU mascherati dalla media corrente. Quando l'ASA raggiunge l'80% dell'utilizzo della CPU, la latenza passa lentamente a circa il 90% della CPU. Quando l'utilizzo della CPU è superiore al 90%, l'ASA inizia a scaricare i pacchetti.

Se l'utilizzo della CPU è elevato, utilizzare il **show processes** comando per identificare i processi che utilizzano la maggior parte del tempo CPU. Utilizzare queste informazioni per ridurre parte del tempo necessario per i processi intensivi, ad esempio la registrazione.

Se la CPU non viene eseguita a caldo, ma si ritiene che i pacchetti vengano ancora scartati, usare il comandoshow interface per verificare che l'interfaccia ASA non contenga buffer e collisioni, probabilmente a causa di una mancata corrispondenza del duplex. Se il numero di buffer no aumenta, ma l'utilizzo della CPU non è basso, l'interfaccia non può supportare il traffico che vi scorre.

Se i buffer sono corretti, controllare i blocchi. Se la colonna CNT corrente nell'output delshow blocks comando è vicina a 0 sui blocchi da 1550 byte (blocchi da 16384 byte per schede Gig da 66 MHz), l'ASA probabilmente scarta i pacchetti Ethernet perché è troppo occupata. In questo caso, la CPU raggiunge picchi elevati.

Se si verificano problemi quando si creano nuove connessioni tramite l'appliance ASA, usare il comandoshow conn count per controllare il numero corrente di connessioni tramite l'appliance.

Se il conteggio corrente è alto, controllare l'output delshow memory comando per verificare che la memoria dell'ASA non sia insufficiente. Se la memoria è insufficiente, individuare l'origine delle connessioni con il comando show conn or show local-host per verificare che la rete non abbia subito attacchi di negazione del servizio.

Per misurare la quantità di traffico che attraversa l'ASA, è possibile usare altri comandi. Il **show traffic** comando visualizza i pacchetti e i byte aggregati per interfaccia e suddivide il traffico in diversi tipi,show perfmon ispezionati dall'ASA.

Informazioni correlate

- Cisco ASA serie 5500-X Firewall
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).