# Risoluzione dei problemi del contatore di sovraccarico dell'interfaccia ASA

## Sommario



## Introduzione

Questo documento descrive il contatore di errori di "sovraccarico" e come analizzare i problemi di prestazioni o di perdita di pacchetti sulla rete. Un amministratore potrebbe notare degli errori riportati nell'output del comando **show interface** sull'appliance ASA (Adaptive Security Appliance).

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

## Problema

Il contatore di errori dell'interfaccia ASA "overrun" tiene traccia del numero di volte in cui un

pacchetto è stato ricevuto sull'interfaccia di rete, ma non c'era spazio disponibile nella coda FIFO dell'interfaccia per memorizzare il pacchetto. Il pacchetto è stato quindi scartato. Il valore di questo contatore può essere visualizzato con il comando **show interface**.

Output di esempio che visualizza il problema:

```
ASA# show interface GigabitEthernet0/1
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
Full-Duplex(Full-duplex), 1000 Mbps(1000 Mbps)
Input flow control is unsupported, output flow control is off
MAC address 0026.0b31.0c59, MTU 1500
IP address 10.0.0.113, subnet mask 255.255.0.0
580757 packets input, 86470156 bytes, 0 no buffer
Received 3713 broadcasts, 0 runts, 0 giants
2881 input errors, 0 CRC, 0 frame, 2881 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
905828 packets output, 1131702216 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 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 (255/230)
output queue (blocks free curr/low): hardware (255/202)
```

Nell'esempio di cui sopra, sono stati osservati 2881 sovraccarichi sull'interfaccia dall'avvio dell'ASA o dall'immissione del comando **clear interface** per cancellare manualmente i contatori.

# Cause di sovraccarichi dell'interfaccia

Gli errori di sovraccarico dell'interfaccia sono in genere causati da una combinazione dei seguenti fattori:

- Livello software: il software ASA non estrae i pacchetti dalla coda FIFO dell'interfaccia abbastanza velocemente. In questo modo, la coda FIFO si riempie e i nuovi pacchetti vengono scartati.
- Livello hardware: la velocità con cui i pacchetti entrano nell'interfaccia è troppo elevata, il che fa sì che la coda FIFO si riempia prima che il software ASA possa prelevare i pacchetti. In genere, una frammentazione di pacchetti determina il riempimento della coda FIFO fino alla capacità massima in un breve periodo di tempo.

# Procedure per la risoluzione dei problemi relativi alla causa dei sovraccarichi dell'interfaccia

Per risolvere il problema, procedere come segue:

1. Determinare se l'ASA presenta errori di CPU e se questi contribuiscono al problema. Riduzione dei blocchi prolungati o frequenti della CPU.
2. Comprendere le velocità del traffico di interfaccia e determinare se l'ASA ha una sottoscrizione eccessiva a causa del profilo di traffico.
3. Determinare se il problema è causato da picchi di traffico intermittenti. In questo caso,

implementare il controllo del flusso sull'interfaccia ASA e sulle porte switch adiacenti.

# Cause e soluzioni potenziali

## La CPU sull'appliance ASA è periodicamente occupata per elaborare i pacchetti in arrivo (CPU Hog)

Per elaborare i pacchetti in arrivo, la piattaforma ASA elabora tutti i pacchetti del software e usa i core principali della CPU che gestiscono tutte le funzioni del sistema (ad esempio syslog, connettività di Adaptive Security Device Manager e ispezione delle applicazioni). Se un processo software mantiene la CPU più a lungo del previsto, l'ASA la registra come un evento di blocco della CPU dal momento che il processo ha "bloccato" la CPU. La soglia della CPU è impostata in millisecondi ed è diversa per ogni modello di accessorio hardware. La soglia si basa sul tempo necessario per riempire la coda FIFO dell'interfaccia, data la potenza della CPU della piattaforma hardware e le velocità di traffico potenziale che il dispositivo può gestire.

I blocchi della CPU a volte causano errori di sovraccarico dell'interfaccia sulle appliance ASA single-core, ad esempio 5505, 5510, 5520, 5540 e 5550. I maiali lunghi, che durano 100 millisecondi o più, possono causare soprattutto sovraccarichi del traffico per livelli relativamente bassi e velocità di traffico non bursty. Il problema non ha un impatto altrettanto significativo sui sistemi multi-core, poiché altri core possono estrarre pacchetti da un anello Rx se uno dei core CPU è bloccato da un processo.

Se la durata del maiale supera la soglia del dispositivo, viene generato un syslog con ID 711004, come mostrato di seguito:

```
06 feb 2013 14:40:42: %ASA-4-711004: Attività eseguita per 60 msec, Processo = ssh, PC =
90b0155, Stack chiamate = Feb 06 2013 14:40:42: %ASA-4-711004: Attività eseguita per 60 msec,
processo = ssh, PC = 90b0155, stack di chiamate = 0x090b0155 0x090bf3b6 0x090b3b84 0x090b3f6e
0x090b4459 0x090b44d6 0x08c46fcc 0x09860ca 0x080fad6d 0x080efa5a 0x080f0a1c 0x0806922c
```

Gli eventi di interruzione della CPU vengono inoltre registrati dal sistema. L'output del comando **show proc cpu-hog** visualizza i seguenti campi:

- Processo: il nome del processo che ha eseguito l'hogging della CPU.
- PROC_PC_TOTAL: il numero totale di volte in cui questo processo ha bloccato la CPU.
- MAXHOG - il tempo massimo di esecuzione della CPU osservato per il processo, in millisecondi.
- LASTHOG - Quantità di tempo in millisecondi in cui l'ultimo mazzo ha tenuto in mano la CPU.
- LASTHOG At - Ora dell'ultimo attacco della CPU.
- PC: valore del contatore di programma del processo quando si è verificato il guasto della CPU. (Informazioni per il Cisco Technical Assistance Center (TAC))
- Stack di chiamate: lo stack di chiamate del processo quando si è verificato il blocco della CPU. (Informazioni su Cisco TAC)

Nell'esempio viene mostrato l'output del comando **show proc cpu-hog**:

```
ASA#

show proc cpu-hog
```

```
Process:    ssh, PROC_PC_TOTAL: 1, MAXHOG: 119, LASTHOG: 119
LASTHOG At: 12:25:33 EST Jun 6 2012
PC:         0x08e7b225 (suspend)

Process:    ssh, NUMHOG: 1, MAXHOG: 119, LASTHOG: 119
LASTHOG At: 12:25:33 EST Jun 6 2012
PC:         0x08e7b225 (suspend)
Call stack: 0x08e7b225 0x08e8a106 0x08e7ebf4 0x08e7efde 0x08e7f4c9 0x08e7f546 0x08a7789c
            0x095a3f60 0x080e7e3d 0x080dcfa2 0x080ddf5c 0x0806897c

CPU hog threshold (msec): 10.240
Last cleared: 12:25:28 EST Jun 6 2012
ASA#
```

Il processo ASA SSH ha mantenuto la CPU per 119 ms il 6 giugno 2012 alle 12:25:33 EST.

Se gli errori di sovraccarico su un'interfaccia aumentano continuamente, controllare l'output del comando **show proc cpu-hog** per verificare se gli eventi di sovraccarico della CPU sono correlati a un aumento del contatore di sovraccarico dell'interfaccia. Se gli errori di sovraccarico dell'interfaccia sono causati dai log della CPU, è consigliabile cercare i bug con Bug Toolkit o aprire una richiesta di assistenza in Cisco TAC. L'output del comando **show tech-support** include anche l'output del comando **show proc cpu-hog**.

## Il profilo del traffico elaborato periodicamente sovrascrive l'ASA

A seconda del profilo del traffico, il traffico che attraversa l'appliance ASA potrebbe essere eccessivo e si potrebbero verificare sovraccarichi.

Il profilo di traffico comprende (tra gli altri aspetti):

- Dimensioni pacchetto
- Gap tra pacchetti (velocità pacchetto)
- Protocollo: alcuni pacchetti sono soggetti all'ispezione delle applicazioni sull'appliance ASA e richiedono una maggiore quantità di elaborazione rispetto ad altri pacchetti

Per identificare il profilo del traffico sull'appliance ASA, è possibile usare le seguenti funzionalità:

- NetFlow - L'ASA può essere configurata per esportare i record NetFlow versione 9 in un agente di raccolta NetFlow. Questi dati possono quindi essere analizzati per ottenere ulteriori informazioni sul profilo del traffico.

- SNMP - utilizzare il monitoraggio SNMP per tenere traccia delle velocità di traffico dell'interfaccia ASA, della CPU, delle connessioni e delle velocità di conversione. Le informazioni possono quindi essere analizzate per comprendere lo schema di traffico e il suo cambiamento nel tempo. Provate a determinare se c'è un picco di velocità che è correlato a un aumento dei sovraccarichi e la causa di quel picco di traffico. In alcuni casi, il TAC indica che i dispositivi della rete non si comportano correttamente (a causa di una configurazione errata o di un'infezione da virus) e generano periodicamente un'inondazione del traffico.

## Burst di pacchetti intermittenti Sovrascrivi la coda FIFO dell'interfaccia ASA

Una frammentazione di pacchetti che arrivano sulla scheda NIC potrebbe causare il riempimento del FIFO prima che la CPU possa estrarre i pacchetti. Di solito non si può fare molto per risolvere questo problema, ma è possibile mitigarlo usando le funzionalità QoS nella rete per risolvere i picchi di traffico o controllare il flusso sull'appliance ASA e sulle porte degli switch adiacenti.

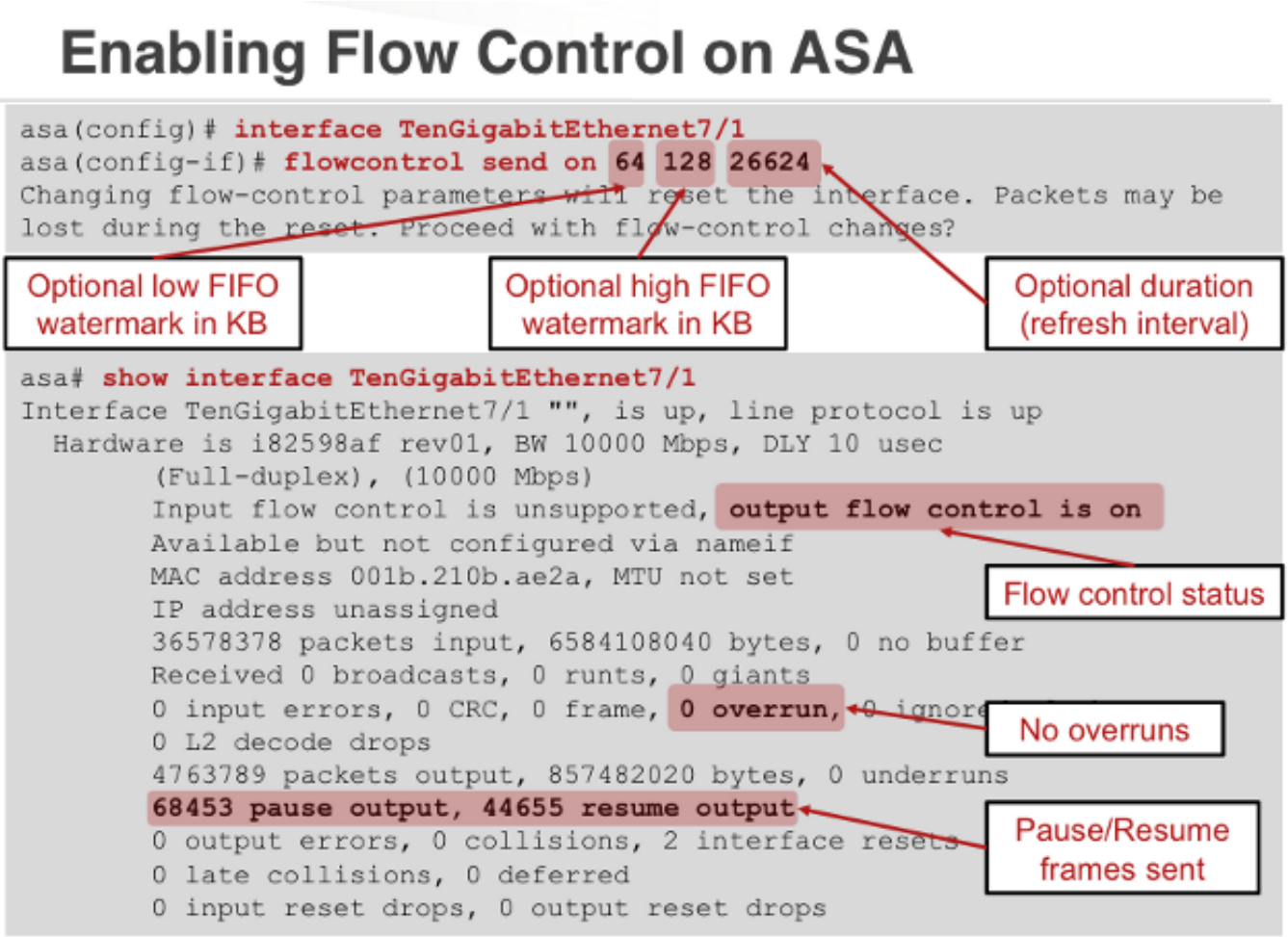
Il controllo del flusso è una funzione che consente all'interfaccia dell'ASA di inviare un messaggio al dispositivo adiacente (ad esempio una porta switch) per istruirlo a interrompere l'invio del traffico per un breve periodo di tempo. Lo fa quando il FIFO raggiunge un certo livello d'acqua. Dopo aver liberato la porta FIFO, la scheda NIC ASA invia un frame di ripristino e la porta dello switch continua a inviare il traffico. Questo approccio funziona bene perché le porte switch adiacenti hanno in genere più spazio di buffer e possono eseguire un processo migliore di buffering dei pacchetti in trasmissione rispetto alle porte ASA nella direzione di ricezione.

Èpossibile provare a abilitare le clip sull'appliance ASA per rilevare i micro-burst del traffico, ma in genere questa operazione non è utile in quanto i pacchetti vengono scartati prima di poter essere elaborati dall'appliance e aggiunti all'acquisizione in memoria. Uno sniffer esterno può essere utilizzato per catturare e identificare l'esplosione del traffico, ma a volte lo sniffer esterno può essere sopraffatto dallo scoppio.

## Abilita controllo del flusso per ridurre i sovraccarichi dell'interfaccia

La funzione di controllo del flusso è stata aggiunta all'ASA nella versione 8.2(2) e successive per le interfacce 10GE e nella versione 8.2(5) e successive per le interfacce 1GE. La capacità di abilitare il controllo del flusso sulle interfacce ASA con sovraccarico si dimostra una tecnica efficace per prevenire il rischio di perdita dei pacchetti.

Per ulteriori informazioni, consultare la funzione di controllo del flusso nella guida di riferimento dei comandi di Cisco ASA serie 5500, versione 8.2.




*(Diagramma da Cisco Live Presentation BRKSEC-3021 di Andrew Ossipov)*

Notare che "controllo del flusso di uscita attivato" significa che l'ASA invia frame di pausa del controllo del flusso dall'interfaccia ASA verso il dispositivo adiacente (lo switch). "Il controllo del flusso di ingresso non è supportato" significa che l'ASA non supporta la *ricezione* di frame di controllo del flusso dal dispositivo adiacente.

Configurazione di esempio del controllo del flusso:

```
interface GigabitEthernet0/2

flowcontrol send on

 nameif DMZ interface
 security-level 50
 ip address 10.1.3.2 255.255.255.0
!
```

# Informazioni correlate

- ASA 8.3 e versioni successive: Monitoraggio e risoluzione dei problemi relativi alle prestazioni
- Presentazione di Cisco Live "Maximizing Firewall Performance" - Questa presentazione descrive l'architettura delle varie piattaforme ASA e include informazioni sulle prestazioni e il tuning. Per accedere alla presentazione, accedere a Ciscolive!365 e cercare il numero di presentazione BRKSEC-3021.
- Cisco TAC Security Podcast Episodio 7 "Monitoring Firewall Performance" - Questo podcast offre una descrizione delle tecniche e dei metodi per monitorare le prestazioni del firewall e identificare i problemi relativi alle prestazioni.
- Documentazione e supporto tecnico – Cisco Systems