ASA 8.3 Problema: MSS superato - I client HTTP non possono passare ad alcuni siti Web

Sommario

Introduzione

In questo documento viene descritto un problema che si verifica quando alcuni siti Web non sono accessibili tramite un'appliance ASA (Adaptive Security Appliance) con software versione 8.3 o successive.

La versione ASA 7.0 introduce diversi nuovi miglioramenti nella sicurezza, uno dei quali è la verifica della presenza di endpoint TCP conformi al valore MSS (Maximum Segment Size) annunciato. In una normale sessione TCP, il client invia un pacchetto SYN al server, con il valore MSS incluso nelle opzioni TCP del pacchetto SYN. Al ricevimento del pacchetto SYN, il server deve riconoscere il valore MSS inviato dal client e inviare il proprio valore MSS nel pacchetto SYN-ACK. Quando il client e il server sono entrambi a conoscenza del valore MSS dell'altro, nessuno dei due peer deve inviare all'altro un pacchetto più grande del valore MSS del peer.

Èstato rilevato che alcuni server HTTP su Internet non rispettano il valore MSS annunciato dal client. Successivamente, il server HTTP invia al client pacchetti di dati più grandi del valore MSS annunciato. Prima della versione 7.0, questi pacchetti erano autorizzati tramite l'appliance ASA. Con i miglioramenti apportati alla sicurezza nella versione 7.0 del software, questi pacchetti vengono eliminati per impostazione predefinita. Questo documento è stato progettato per aiutare l'amministratore di Cisco Adaptive Security Appliance nella diagnosi del problema e nell'implementazione di una soluzione per consentire ai pacchetti che superano il valore MSS.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

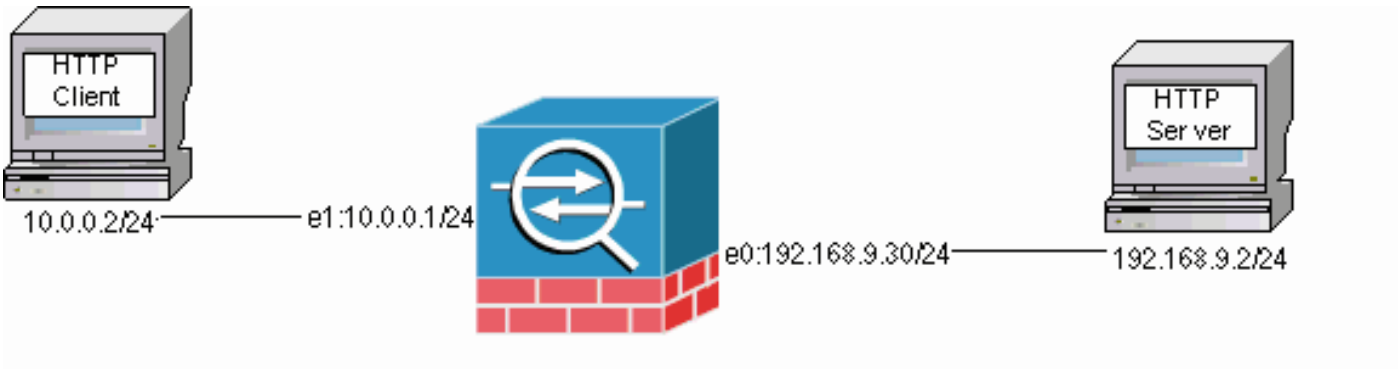
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte nel documento.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione ASA 8.3

Questi comandi di configurazione vengono aggiunti a una configurazione predefinita di ASA 8.3 in modo da consentire al client HTTP di comunicare con il server HTTP.

Configurazione ASA 8.3

```
ASA(config)#interface Ethernet0
ASA(config-if)#speed 100
ASA(config-if)#duplex full
ASA(config-if)#nameif outside
ASA(config-if)#security-level 0
ASA(config-if)#ip address 192.168.9.30 255.255.255.0
ASA(config-if)#exit
ASA(config)#interface Ethernet1
ASA(config-if)#speed 100
ASA(config-if)#duplex full
ASA(config-if)#nameif inside
ASA(config-if)#security-level 100
ASA(config-if)#ip address 10.0.0.1 255.255.255.0
ASA(config-if)#exit
ASA(config)#object network Inside-Network
ASA(config-obj)#subnet 10.0.0.0 255.0.0.0
ASA(config)#nat (inside,outside) source dynamic Inside-Network interface
ASA(config)#route outside 0.0.0.0 0.0.0.0 192.168.9.2 1
```

Risoluzione dei problemi

Se un sito Web non è accessibile tramite l'appliance ASA, attenersi alla seguente procedura per risolvere il problema. È innanzitutto necessario acquisire i pacchetti dalla connessione HTTP. Per raccogliere i pacchetti, è necessario conoscere gli indirizzi IP del server e del client HTTP nonché l'indirizzo IP a cui il client viene convertito quando attraversa l'appliance ASA.

Nella rete di esempio, il server HTTP è indirizzato a 192.168.9.2, il client HTTP è indirizzato a 10.0.0.2 e gli indirizzi del client HTTP sono convertiti in 192.168.9.30 quando i pacchetti escono dall'interfaccia esterna. Per raccogliere i pacchetti, è possibile usare la funzione di acquisizione di Cisco Adaptive Security Appliance (ASA) oppure usare un'acquisizione esterna. Se si intende utilizzare la funzione di acquisizione, l'amministratore può anche utilizzare una nuova funzione di acquisizione inclusa nella versione 7.0 che consente all'amministratore di acquisire i pacchetti scartati a causa di un'anomalia TCP.

Nota: a causa di limitazioni spaziali, alcuni comandi di queste tabelle vanno a capo su una seconda riga.

1. Definire una coppia di elenchi degli accessi che identificano i pacchetti in entrata e in uscita dalle interfacce esterna e interna.
2. Abilitare la funzione di acquisizione per l'interfaccia interna ed esterna. Abilitare anche l'acquisizione per i pacchetti MSS-exceeded specifici per TCP.
3. Cancellare i contatori Accelerated Security Path (ASP) sull'appliance ASA.
4. Abilitare la registrazione dei messaggi trap a livello di debug inviati a un host della rete.
5. Avviare una sessione HTTP dal client HTTP al server HTTP con problemi e raccogliere l'output syslog e l'output di questi comandi quando la connessione non riesce.**show capture-insideshow capture-outsideshow capture mss-captureshow asp dropNota:** per ulteriori informazioni sul messaggio di errore, fare riferimento al messaggio di log del sistema 419001.

Soluzione alternativa

Èpossibile implementare una soluzione ora che l'ASA rifiuta i pacchetti che superano il valore MSS annunciato dal client. Tenere presente che si potrebbe desiderare di non consentire a questi pacchetti di raggiungere il client a causa di un potenziale sovraccarico del buffer sul client. Se si sceglie di consentire i pacchetti tramite l'ASA, procedere con questa procedura di soluzione.

Modular Policy Framework (MPF) è una nuova funzionalità della versione 7.0 che consente l'accesso di questi pacchetti tramite l'appliance ASA. Questo documento non è progettato per descrivere in dettaglio l'MPF, ma suggerisce piuttosto le entità di configurazione utilizzate per risolvere il problema. Fare riferimento alla guida alla configurazione di ASA 8.3 per ulteriori informazioni su MPF.

Una panoramica della soluzione alternativa include l'identificazione del client e dei server HTTP tramite un elenco degli accessi. Una volta definito l'elenco degli accessi, viene creata una mappa delle classi e l'elenco degli accessi viene assegnato alla mappa delle classi. Quindi viene configurata una mappa TCP e viene abilitata l'opzione per consentire i pacchetti che superano il valore MSS. Dopo aver definito la mappa TCP e la mappa classi, è possibile aggiungerle a una mappa dei criteri nuova o esistente. Una mappa dei criteri viene quindi assegnata a un criterio di protezione. Utilizzare il comando **service-policy** in modalità di configurazione per attivare una

mappa dei criteri a livello globale o su un'interfaccia. Questi parametri di configurazione vengono aggiunti all'elenco di configurazione di Cisco Adaptive Security Appliance (ASA) 8.3. Dopo aver creato una mappa dei criteri denominata "http-map1", questa configurazione di esempio aggiunge la mappa delle classi a questa mappa dei criteri.

Interfaccia specifica: Configurazione MPF per consentire pacchetti che superano il valore MSS

```
ASA(config)#access-list http-list2 permit tcp any host 192.168.9.2
ASA(config)#
ASA#configure terminal
ASA(config)#
ASA(config)#class-map http-map1
ASA(config-cmap)#match access-list http-list2
ASA(config-cmap)#exit
ASA(config)#tcp-map mss-map
ASA(config-tcp-map)#exceed-mss allow
ASA(config-tcp-map)#exit
ASA(config)#policy-map http-map1
ASA(config-pmap)#class http-map1
ASA(config-pmap-c)#set connection advanced-options mss-map
ASA(config-pmap-c)#exit
ASA(config-pmap)#exit
ASA(config)#service-policy http-map1 interface outside
ASA#
```

Dopo aver impostato i parametri di configurazione, i pacchetti da 192.168.9.2 che superano il valore MSS annunciato dal client vengono autorizzati tramite l'ASA. È importante notare che l'elenco degli accessi utilizzato nella mappa di classe è progettato per identificare il traffico in uscita verso 192.168.9.2. Il traffico in uscita viene esaminato per consentire al motore di ispezione di estrarre il valore MSS dal pacchetto SYN in uscita. Pertanto, è essenziale configurare l'elenco degli accessi tenendo presente la direzione del SYN. Se è richiesta una regola più pervasiva, è possibile sostituire l'istruzione **access-list** in questa sezione con un'istruzione **access-list** che autorizzi tutto, ad esempio **access-list http-list2 allow ip any** o **access-list http-list2 allow tcp any any**. Inoltre, tenere presente che il tunnel VPN può essere lento se si utilizza un valore elevato di TCP MSS. È possibile ridurre il valore TCP MSS per migliorare le prestazioni.

Questo esempio aiuta a configurare il traffico in entrata e in uscita a livello globale nell'appliance ASA:

Configurazione globale: Configurazione MPF per consentire pacchetti che superano il valore MSS

```
ASA(config)#access-list http-list2 permit tcp any host 192.168.9.2
ASA(config)#
ASA#configure terminal
ASA(config)#
ASA(config)#class-map http-map1
ASA(config-cmap)#match any
ASA(config-cmap)#exit
ASA(config)#tcp-map mss-map
ASA(config-tcp-map)#exceed-mss allow
ASA(config-tcp-map)#exit
ASA(config)#policy-map http-map1
ASA(config-pmap)#class http-map1
ASA(config-pmap-c)#set connection advanced-options mss-map
ASA(config-pmap-c)#exit
ASA(config-pmap)#exit
ASA(config)#service-policy http-map1 global
ASA#
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Ripetere i passaggi della sezione Risoluzione dei problemi per verificare che le modifiche alla configurazione eseguano le operazioni per cui sono state progettate.

Registri di sistema da una connessione riuscita

```
%ASA-6-609001: Built local-host inside:10.0.0.2
%ASA-6-609001: Built local-host outside:192.168.9.2
%ASA-6-305011: Built dynamic TCP translation from inside:10.0.0.2/58798
               to outside:192.168.9.30/1025
%ASA-6-302013: Built outbound TCP connection 13 for outside:192.168.9.2/80
               (192.168.9.2/80) to inside:10.0.0.2/58798 (192.168.9.30/1025)
%ASA-5-304001: 10.0.0.2 Accessed URL 192.168.9.2:/

%ASA-6-302014: Teardown TCP connection 13 for outside:192.168.9.2/80 to
               inside:10.0.0.2/58798 duration 0:00:01 bytes 6938 TCP FINs

!--- The connection is built and immediately !--- torn down when the web content is retrieved.
```

Output di show Commands da una connessione riuscita

```
ASA#
ASA#show capture capture-inside
21 packets captured
   1: 09:16:50.972392 10.0.0.2.58769 > 192.168.9.2.80: S
      751781751:751781751(0)
   win 1840 <mss 460,sackOK,timestamp 110313116 0,nop,wscale 0>

 !--- The advertised MSS of the client is 460 in packet #1. However, !--- with th workaround in place,
packets 7, 9, 11, 13, and 15 appear !--- on the inside trace, despite the MSS>460. 2: 09:16:51.098536
192.168.9.2.80 > 10.0.0.2.58769: S 1305880751:1305880751(0) ack 751781752 win 8192 <mss 1380> 3:
09:16:51.098734 10.0.0.2.58769 > 192.168.9.2.80: . ack 1305880752 win 1840 4: 09:16:51.099009 10.0.0.2.
> 192.168.9.2.80: P 751781752:751781851(99) ack 1305880752 win 1840 5: 09:16:51.228412 192.168.9.2.80 >
10.0.0.2.58769: . ack 751781851 win 8192 6: 09:16:51.228641 192.168.9.2.80 > 10.0.0.2.58769: . ack 7517
win 25840 7: 09:16:51.236254 192.168.9.2.80 > 10.0.0.2.58769: . 1305880752:1305882112(1360) ack 7517818
25840
   8: 09:16:51.237704 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305882112 win 4080
   9: 09:16:51.243593 192.168.9.2.80 > 10.0.0.2.58769: P
      1305882112:1305883472(1360) ack 751781851 win 25840
  10: 09:16:51.243990 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305883472 win 6800
  11: 09:16:51.251009 192.168.9.2.80 > 10.0.0.2.58769: .
      1305883472:1305884832(1360) ack 751781851 win 25840
  12: 09:16:51.252428 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305884832 win 9520
  13: 09:16:51.258440 192.168.9.2.80 > 10.0.0.2.58769: P
      1305884832:1305886192(1360) ack 751781851 win 25840
  14: 09:16:51.258806 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305886192 win 12240
  15: 09:16:51.266130 192.168.9.2.80 > 10.0.0.2.58769: .
      1305886192:1305887552(1360) ack 751781851 win 25840
  16: 09:16:51.266145 192.168.9.2.80 > 10.0.0.2.58769: P
      1305887552:1305887593(41) ack 751781851 win 25840
  17: 09:16:51.266511 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305887552 win 14960
  18: 09:16:51.266542 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305887593 win 14960
```

```
  19: 09:16:51.267320 10.0.0.2.58769 > 192.168.9.2.80: F
      751781851:751781851(0) ack 1305887593 win 14960
  20: 09:16:51.411370 192.168.9.2.80 > 10.0.0.2.58769: F
      1305887593:1305887593(0) ack 751781852 win 8192
  21: 09:16:51.411554 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305887594 win 14960
21 packets shown
ASA#
ASA#
ASA#show capture capture-outside
21 packets captured
   1: 09:16:50.972834 192.168.9.30.1024 > 192.168.9.2.80: S
      1465558595:1465558595(0) win 1840 <mss 460,sackOK,timestamp
      110313116 0,nop,wscale 0>
   2: 09:16:51.098505 192.168.9.2.80 > 192.168.9.30.1024:
      S 466908058:466908058(0) ack 1465558596 win 8192 <mss 1460>
   3: 09:16:51.098749 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466908059 win 1840
   4: 09:16:51.099070 192.168.9.30.1024 > 192.168.9.2.80: P
      1465558596:1465558695(99) ack 466908059 win 1840
   5: 09:16:51.228397 192.168.9.2.80 > 192.168.9.30.1024: .
      ack 1465558695 win 8192
   6: 09:16:51.228625 192.168.9.2.80 > 192.168.9.30.1024: .
      ack 1465558695 win 25840
   7: 09:16:51.236224 192.168.9.2.80 > 192.168.9.30.1024: .
      466908059:466909419(1360 ack 1465558695 win 25840
   8: 09:16:51.237719 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466909419 win 4080
   9: 09:16:51.243578 192.168.9.2.80 > 192.168.9.30.1024: P
      466909419:466910779(1360) ack 1465558695 win 25840
  10: 09:16:51.244005 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466910779 win 6800
  11: 09:16:51.250978 192.168.9.2.80 > 192.168.9.30.1024: .
      466910779:466912139(1360) ack 1465558695 win 25840
  12: 09:16:51.252443 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466912139 win 9520
  13: 09:16:51.258424 192.168.9.2.80 > 192.168.9.30.1024: P
      466912139:466913499(1360) ack 1465558695 win 25840
  14: 09:16:51.258485 192.168.9.2.80 > 192.168.9.30.1024: P
      466914859:466914900(41) ack 1465558695 win 25840
  15: 09:16:51.258821 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466913499 win 12240
  16: 09:16:51.266099 192.168.9.2.80 > 192.168.9.30.1024: .
      466913499:466914859(1360) ack 1465558695 win 25840
  17: 09:16:51.266526 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466914859 win 14960
  18: 09:16:51.266557 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466914900 win 14960
  19: 09:16:51.267335 192.168.9.30.1024 > 192.168.9.2.80: F
      1465558695:1465558695(0) ack 466914900 win 14960
  20: 09:16:51.411340 192.168.9.2.80 > 192.168.9.30.1024: F
      466914900:466914900(0) ack 1465558696 win 8192
  21: 09:16:51.411569 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466914901 win 14960
21 packets shown
ASA#
ASA(config)#show capture mss-capture
0 packets captured
0 packets shown
ASA#
ASA#show asp drop

Frame drop:
```

```
Flow drop:
ASA#

!--- Both the show capture mss-capture and the show asp drop !--- commands reveal that no packets are
dropped.
```

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Avvisi sui prodotti per la sicurezza (comprese le appliance Cisco Adaptive Security (ASA))
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems