# Edição ASA 8.3: MSS excedido - Os clientes HTTP não podem consultar a alguns Web site

## Índice



## Introdução

Este documento descreve um problema que ocorre quando alguns sites não são acessíveis por meio de um mecanismo de segurança adaptável (ASA) que executa a versão 8.3 ou posterior do software.

A liberação ASA 7.0 introduz diversos aprimoramentos de segurança novos, um de que é uma verificação para os pontos finais de TCP que aderem ao máximo anunciado do tamanho do segmento (MSS). Em uma sessão de TCP normal, o cliente envia um pacote SYN ao servidor com o MSS incluído dentro das opções de TCP do pacote SYN. O servidor, após receber o pacote SYN, deverá reconhecer o valor do MSS enviado pelo cliente e, então, enviar seu próprio valor de MSS no pacote SYN-ACK. Quando o cliente e o servidor estiverem cientes do MSS de cada um, nem o peer deverá enviar um pacote para outro que seja maior do que o MSS desse peer.

Um descoberta foi realizada que há alguns servidores HTTP na Internet que não honram o MSS que o cliente anuncia. Subsequentemente, o servidor HTTP envia pacotes de dados ao cliente que é maior que o MSS anunciado. Antes da liberação 7.0, estes pacotes foram permitidos com o ASA. Com o aprimoramento da segurança incluído na versão 7.0 do software, estes pacotes foram reduzidos por padrão. Este documento é projetado ajudar ao administrador adaptável da ferramenta de segurança de Cisco no diagnóstico deste problema e na aplicação de uma ação alternativa a permitir os pacotes que excedem o MSS.

Refira a edição PIX/ASA 7.X: MSS excedido - Os clientes HTTP não podem consultar a alguns sites para a mesma configuração na ferramenta de segurança adaptável de Cisco (ASA) com versões 8.2 e anterior.

# Pré-requisitos

## Requisitos

Não existem requisitos específicos para este documento.

## Componentes Utilizados

A informação neste documento é baseada em uma ferramenta de segurança adaptável de Cisco (ASA) esse software da versão 8.3 das corridas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Refira as convenções dos dicas técnicas da Cisco para obter informações sobre das convenções de documento.

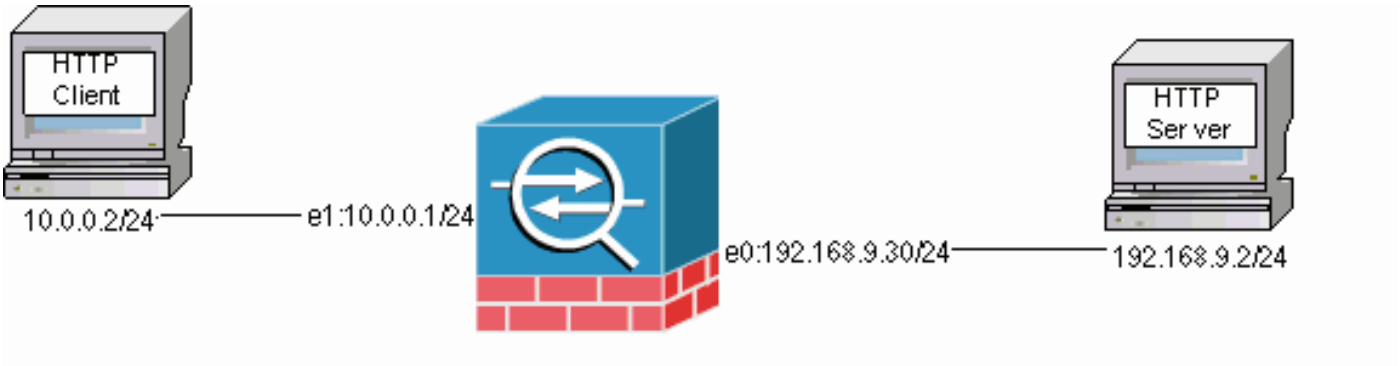
# Configurar

Esta seção apresenta informações para configurar as características que este documento descreve.

**Nota:** Use a Command Lookup Tool (apenas para clientes registrados) para obter informações adicionais sobre os comandos que este documento usa.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:




## Configuração ASA 8.3

Estes comandos configuration são adicionados a uma configuração padrão ASA 8.3 a fim permitir que o cliente HTTP comunique-se com o Server do HTTP.

| Configuração ASA 8.3 |
| --- |
| ASA(config)#**interface Ethernet0** ASA(config-if)#**speed 100**<br>ASA(config-if)#**duplex full** ASA(config-if)#**nameif outside**<br>ASA(config-if)#**security-level 0** ASA(config-if)#**ip address 192.168.9.30 255.255.255.0** ASA(config-if)#**exit**<br>ASA(config)#**interface Ethernet1** ASA(config-if)#**speed 100**<br>ASA(config-if)#**duplex full** ASA(config-if)#**nameif inside**<br>ASA(config-if)#**security-level 100** ASA(config-if)#**ip address 10.0.0.1 255.255.255.0** ASA(config-if)#**exit**<br>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**<br>ASA(config)#**route outside 0.0.0.0 0.0.0.0 192.168.9.2 1** |

# Troubleshooting

Se um Web site particular não é acessível com o ASA, termine estas etapas para pesquisar defeitos. Você precisa primeiramente de capturar os pacotes da conexão de HTTP. A fim recolher os pacotes, os endereços IP de Um ou Mais Servidores Cisco ICM NT relevantes do Server do HTTP e o cliente precisam de ser conhecidos, assim como o endereço IP de Um ou Mais Servidores Cisco ICM NT que o cliente está traduzido a quando atravessa o ASA.

Na rede de exemplo, o Server do HTTP é endereçado em 192.168.9.2, o cliente HTTP é endereçado em 10.0.0.2, e os endereços do cliente HTTP estão traduzidos a 192.168.9.30 enquanto os pacotes saem da interface externa. Você pode usar a característica da captação da ferramenta de segurança adaptável de Cisco (ASA) a fim recolher os pacotes, ou você pode utilizar uma captura de pacote de informação externo. Se você pretende usar a característica da captação, o administrador pode igualmente utilizar uma característica nova da captação incluída na liberação 7.0 que permite que o administrador capture os pacotes que são deixado cair devido a uma anomalia de TCP.

**Nota:** Alguns dos comandos no envoltório destas tabelas a uma segunda linha devido às limitações espaciais.

1. Defina um par de Listas de acesso que identificam os pacotes como ele ingresso e saída a parte externa e as interfaces internas.
2. Permita a característica da captação para ambos a interface interna e externa. Igualmente permita a captação para pacotes MSS-excedidos TCP-específicos.
3. Cancele os contadores acelerados do trajeto da Segurança (ASP) no ASA.
4. Permita a informações de syslog da armadilha a nível de debug enviado a um host na rede.
5. Inicie uma sessão de HTTP do cliente HTTP ao Server do HTTP problemático, e recolha as saídas de SYSLOG e a saída destes comandos depois que a conexão falha.**mostre a captação captação-dentro demostre a captação-parte externa da captaçãomostre a mss-captação da captaçãomostre a gota aspNota:** Refira o mensagem de Log de sistema 419001 para obter mais informações sobre deste Mensagem de Erro.

# Solução

Execute uma ação alternativa agora que você sabe que o ASA deixa cair os pacotes que excedem o valor MSS anunciado pelo cliente. Mantenha na mente que você não pôde querer permitir que estes pacotes alcancem o cliente devido a um buffer potencial passado no cliente. Se

você escolhe permitir estes pacotes com o ASA, continue com este procedimento de solução.

A estrutura de política modular (MPF) é uns novos recursos na liberação 7.0 que é usada para permitir estes pacotes com o ASA. Este documento não é projetado detalhar inteiramente o MPF mas sugere um pouco as entidades de configuração usadas para trabalhar em torno do problema. Refira o manual de configuração ASA 8.3 e o manual de referência de comando ASA 8.3 para obter mais informações sobre do MPF e de algum dos comandos alistados nesta seção.

Uma vista geral à ação alternativa inclui a identificação do cliente HTTP e dos server através de uma lista de acessos. Uma vez que a lista de acessos é definida, um mapa da classe está criado e a lista de acessos é atribuída ao mapa da classe. Um mapa TCP é configurado então e a opção para permitir os pacotes que excedem o MSS é permitida. Uma vez que o mapa TCP e o mapa da classe são definidos, você pode adicionar-lo a um mapa novo ou da política existente. Um mapa de política é atribuído então a uma política de segurança. Use o **comando service-policy no** modo de configuração ativar globalmente um mapa de política ou em uma relação. Estes parâmetros de configuração são adicionados à ferramenta de segurança adaptável de Cisco (ASA) lista de 8.3 configurações. Depois que você cria um mapa de política nomeado "http-map1," esta configuração de exemplo adiciona o mapa da classe a este mapa de política.

**Relação específica: Configuração MPF para permitir os pacotes que excedem o 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#
```

Uma vez que estes parâmetros de configuração são no lugar, os pacotes de 192.168.9.2 que excedem o MSS anunciado pelo cliente estão permitidos com o ASA. É importante notar que a lista de acessos usada no mapa da classe está projetada identificar o tráfego de saída a 192.168.9.2. O tráfego de saída é examinado para permitir que o motor da inspeção extraia o MSS do pacote SYN que parte. Consequentemente, é imperativo configurar a lista de acessos com o sentido do SYN na mente. Se uma regra mais patente é exigida, você pode substituir a **instrução de lista de acesso n**esta seção com uma **instrução de lista de acesso** que permita tudo, tal como a **licença IP da lista de acesso http-list2 alguma** ou **licença tcp da lista de acesso http-list2 alguma**. Igualmente recorde que o túnel VPN pode ser lento se um grande valor de TCP MSS é usado. Você pode reduzir TCP MSS para melhorar o desempenho.

Este exemplo ajuda a configurar globalmente o tráfego de entrada e de saída no ASA:

**Configuração global: Configuração MPF para permitir os pacotes que excedem o 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#
```

# Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

Repita as etapas na seção da pesquisa de defeitos a fim verificar que as alterações de configuração fazem o que são projetadas fazer.

**Syslog de uma conexão bem sucedida**

```
%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.
```

**Saídas do comando show de uma conexão bem sucedida**

```
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 10.0.0.2.58769 > 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 751781851 win 25840 7:
09:16:51.236254 192.168.9.2.80 > 10.0.0.2.58769: .
1305880752:1305882112(1360) ack 751781851 win 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.
```

## Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Field Notice de produto de segurança (que incluem a ferramenta de segurança adaptável de Cisco (ASA))
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems