ASA 8.3 の問題： MSS が超過 - HTTP のクライアントがある Web サイトをブラウズできない

目次

はじめに
前提条件
要件
使用するコンポーネント
表記法
設定
ネットワーク図
ASA 8.3 の設定
トラブルシューティング
回避策
確認
関連情報

はじめに

このドキュメントでは、8.3 以降のソフトウェアが稼働する適応型セキュリティ アプライアンス（ASA）を経由する Web アクセスで、一部の Web サイトにアクセスできない場合に発生する問題について説明します。

ASA 7.0 では、いくつかのセキュリティ機能拡張が加えられました。その 1 つである TCP エンドポイントの確認では、アドバタイズされた Maximum Segment Size（MSS; 最大セグメント サイズ）が遵守されます。 通常の TCP セッションでは、クライアントがサーバに SYN パケットを送信する際に、SYN パケットの TCP オプションには MSS が含まれます。 サーバは SYN パケットを受信すると、クライアントから送信された MSS 値を認識し、自身の MSS 値を SYN-ACK パケットで送信します。 クライアントとサーバの両方が互いの MSS を認識すると、いずれのピアもそのピアの MSS よりも大きなパケットを他方に送信しません。

インターネット上にはクライアントがアドバタイズする MSS を受け付けない HTTP サーバがあることが判明しています。 その後、HTTP サーバはアドバタイズされた MSS を超えるデータ パケットをクライアントに送信します。 リリース 7.0 より前では、これらのパケットが ASA 経由で許可されています。 7.0 ソフトウェア リリースではセキュリティの機能拡張により、デフォルトではこのようなパケットは廃棄されます。 このドキュメントでは、この問題の診断と、MSS を超えるパケットを許可するための回避策の実装に役立つ、Cisco 適応型セキュリティ アプライアンス管理者向けの情報を示します。

Cisco 適応型セキュリティ アプライアンス（ASA）の、バージョン 8.2 以前と同じ設定については、「PIX/ASA 7.X の問題： MSS が超過：HTTP クライアントが一部の Web サイトをブラウズできない」を参照してください。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、バージョン 8.3 ソフトウェアが稼働する Cisco 適応型セキュリティ アプライアンス（ASA）に基づくものです。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報について記載しています。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

ASA 8.3 の設定

HTTP クライアントが HTTP サーバと通信できるように、次の設定コマンドが ASA 8.3 のデフォルト設定に追加されています。

ASA 8.3 の設定

```
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
```

トラブルシューティング

特定の Web サイトに ASA 経由でアクセスできない場合のトラブルシューティングは、次の手順で行います。 最初に、HTTP 接続のパケットをキャプチャします。 パケットを収集するには、HTTP サーバとクライアントの関連 IP アドレス、および ASA セキュリティ アプライアンス通過時のクライアントの変換後の IP アドレスを確認する必要があります。

この例のネットワークでは、HTTP サーバのアドレスが 192.168.9.2、HTTP クライアントのアドレスが 10.0.0.2 で、パケットが外部インターネットから送出される際 HTTP クライアントのアドレスが 192.168.9.30 に変換されています。 Cisco 適応型セキュリティ アプライアンス（ASA）のキャプチャ機能を使用して、パケットを収集できます。または、外部パケット キャプチャを使用できます。 キャプチャ機能を使用する場合、管理者はリリース 7.0 に含まれている新しいキャプチャ機能も使用できます。この機能では、TCP の異常により廃棄されたパケットもキャプチャできます。

注: 次の各表のコマンドの中には、スペースの関係上、2 行にわたって表記されているものがあります。

1. 外部インターフェイスと内部インターフェイスで入出力されるパケットを識別する、アクセス リストのペアを定義します。
2. 内部インターフェイスと外部インターフェイスでキャプチャ機能を有効にします。 TCP 特有の MSS 超過パケットのキャプチャも有効にします。
3. ASA で Accelerated Security Path（ASP）のカウンタをクリアします。
4. ネットワーク上のホストに送信されるデバッグ レベルのトラップ syslog を有効にします。
5. HTTP のクライアントから、問題のある HTTP サーバに HTTP セッションを開始し、接続が失敗した後に、syslog の出力と次のコマンドの出力を収集します。**show capture capture-insideshow capture capture-outsideshow capture mss-captureshow asp drop注:** このエラーメッセージについては、「システム ログ メッセージ 419001」を参照してください。

回避策

クライアントから通知された MSS 値を超過するパケットを ASA がドロップしていることがわか

ったので、回避策を実装します。 クライアント側でバッファ オーバーフローが発生する可能性があるため、このようなパケットはクライアントに到達させないほうがよい場合もあります。 これらのパケットを ASA 経由で許可する場合は、次の回避策の手順で続行します。

Modular Policy Framework（MPF）は、リリース 7.0 の新機能で、これらのパケットを ASA 経由で許可するために使用されます。 このドキュメントでは、MPF については詳しく説明しませんが、この問題を回避するために使用する設定エンティティを提示します。 MPF およびこのセクションに記載されているコマンドの詳細については、『ASA 8.3 コンフィギュレーション ガイド』および『ASA 8.3 コマンド リファレンス』を参照してください。

回避策には、アクセス リストによる HTTP クライアントと HTTP サーバの識別が含まれます。 アクセス リストが定義されると、クラス マップが作成され、アクセス リストがクラス マップに割り当てられます。 次に、tcp マップが設定され、MSS を超えるパケットを許可するオプションが有効化されます。 tcp マップとクラスマップが定義されると、それらのマップを新規または既存のポリシーマップに追加できます。 次に、ポリシー マップがセキュリティ ポリシーに割り当てられます。 コンフィギュレーション モードで **service-policy** コマンドを使用して、ポリシーマップをグローバルに、または外部インターフェイスでアクティブ化します。 次の設定パラメータは、Cisco 適応型セキュリティ アプライアンス（ASA）8.3 コンフィギュレーション リストに追加されます。 この設定例では、「http-map1」という名前のポリシーマップの作成後に、そのポリシーマップにクラスマップが追加されています。

特定のインターフェイス： MSS を超過するパケットを許可するための MPF の設定

```
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#
```

設定パラメータが追加されると、クライアントから通知された MSS を超過する 192.168.9.2 からのパケットが ASA 経由で許可されます。 クラスマップで使用されたアクセス リストは、192.168.9.2 へのアウトバウンド トラフィックを識別するためのものである点に注意してください。 アウトバウンド トラフィックが検査され、インスペクション エンジンが発信 SYN パケットから MSS を抽出します。 そのため、SYN パケットの方向でアクセス リストを設定することが必須です。 より広範囲な規則が必要な場合は、このセクションに**アクセス リスト文**を、すべてを許可する**アクセス リスト文**（**access-list http-list2 permit ip any any** や **access-list http-list2 permit tcp any any** など）に置き換えます。 VPN トンネルの通信が遅くなる可能性があるので注意してください。 TCP MSS を低くすると通信効率を上げることができます。

次の例は、ASA の着信トラフィックと発信トラフィックをグローバルに設定する場合に役立ちます。

グローバル設定： MSS を超過するパケットを許可するための MPF の設定

```
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#
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。

「トラブルシューティング」セクションの手順を繰り返し、設定変更により、期待した結果が得られたかどうかを確認します。

接続に成功したときの Syslog

```
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#
```

接続に成功したときの show コマンドの出力

```
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.
```

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- セキュリティ製品に関する Field Notice（Cisco 適応型セキュリティ アプライアンス（ASA））
- Requests for Comments（RFC）