ASA 8.3 の問題：MSS の超過 - HTTP クライアントが一部の Web サイトを参照できない

内容

概要

このドキュメントでは、一部の Web サイトがバージョン 8.3 以降のソフトウェアを実行している適応型セキュリティ アプライアンス (ASA) 経由で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 リリースでは、いくつかの新しいセキュリティ拡張機能が導入されました。その 1 つである TCP エンドポイント チェック機能は、アドバタイズされた最大セグメント サイズ (MSS) を厳守します。 通常の TCP セッションでは、クライアントからサーバに SYN パケットが送信される際に、SYN パケットの TCP オプションに MSS が含まれています。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 値を認識して、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 よりも前では、これらのパケットは ASA 経由で許可されていました。7.0 ソフトウェア リリースではセキュリティ機能が強化されており、デフォルトではそのようなパケットは廃棄されます。このドキュメントは、Cisco 適応型セキュリティ アプライアンスの管理者がこの問題を診断したり、MSS 超過パケットを許可するための回避策を実行したりする際に役立つように作成されています。

前提条件

要件

このドキュメントに特有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、8.3 ソフトウェア イメージを実行している 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。

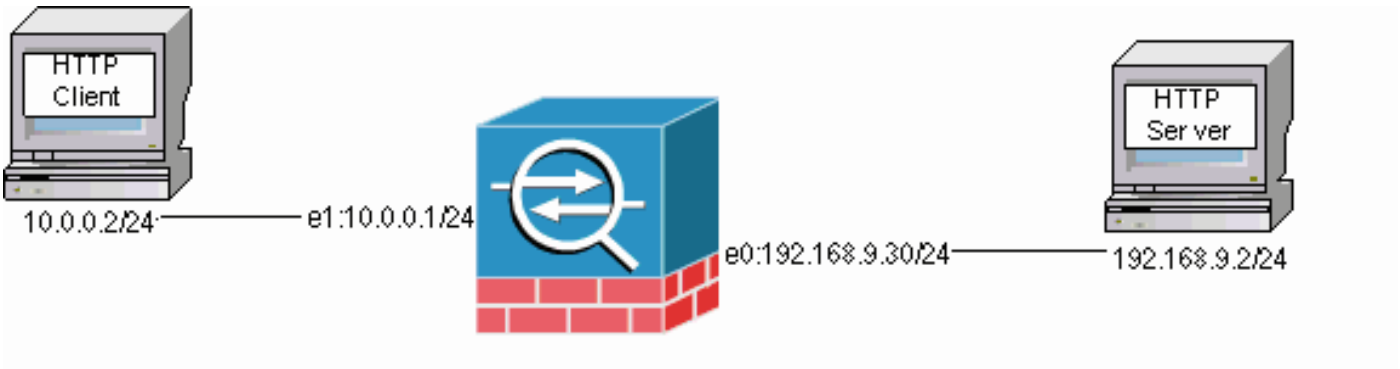
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

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。

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 セットアップを使用します。



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ました。

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
```

トラブルシュート

特定の Web サイトに ASA 経由でアクセスできない場合は、次の手順でトラブルシューティングします。最初に、HTTP 接続からのパケットをキャプチャする必要があります。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 通過時にクライアントが変換される IP アドレスが判明していなければなりません。

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 となっており、パケットが外部インターネットから出るときに HTTP クライアントのアドレスが 192.168.9.30 に変換されます。パケットの収集には、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できます。または、外部のパケット キャプチャを利用することも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：これらの表のコマンドの一部は、スペースの制約により2行に折り返されています。

1. 外部および内部インターフェイスを入出す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. 内部と外部の両方のインターフェイスでキャプチャ機能を有効にします。TCP 固有の MSS 超過パケットのキャプチャも有効にします。
3. ASA の高速セキュリティ パス (ASP) 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 レベルでトラップ syslog を有効にします。
5. HTTP クライアントから問題のある HTTP サーバへの HTTP セッションを開始し、接続に失敗した後、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**メッセージの詳細[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

クライアントからアドバタイズされた MSS 値を超過するパケットが ASA でドロップされることが判明したので、回避策を実行します。ただし、クライアント側でバッファ オーバーランが発生する可能性があるため、そのような超過パケットがクライアントに到達するのを許可しないほうがよい場合もあります。超過パケットが ASA を通過することを許可する場合は、以下の回避策の手順を続行してください。

モジュラ ポリシー フレームワーク (MPF) はリリース 7.0 の新機能で、超過パケットが ASA を通過することを許可するために使用されます。このドキュメントの目的は、MPF について詳しく説明することではなく、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することです。MPF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』を参照してください。

回避策全体には、アクセス リストによる HTTP クライアントと HTTP サーバの識別も含まれます。アクセス リストを定義すると、クラス マップが作成されて、アクセス リストがそのマップに割り当てられます。次に、TCP マップが設定され、MSS 超過パケットを許可するオプションが有効になります。TCP マップとクラス マップが定義された後、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。その後、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、ポリシー マップをグローバルにアクティブ化するか、インターフェイスでアクティブ化します。**これら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](#)」に追加されています。「http-map1」というポリシー マップを作成した後、次の設

定例ではそのポリシーマップにクラスマップが追加されます。

特定のインターフェイス：MSS 超過パケットを許可するための MPF 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#
```

これらの設定パラメータを設定すると、クライアントからアドバタイズされた MSS を超える 192.168.9.2 からのパケットが ASA を通過できるようになります。クラスマップで使用されるアクセスリストは、192.168.9.2への発信トラフィックを識別するように設計されていることに注意してください。発信トラフィックは、インスペクションエンジンが発信SYNパケットからMSSを抽出できるように検査されます。したがって、アクセス リストは必ず SYN の方向で設定する必要があります。より広範囲にわたる規則が必要な場合は、この項の**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。TCP MSS に大きな値を設定すると、VPN トンネルが遅くなる可能性があることに留意してください。TCP MSS の値を低くするとパフォーマンスを向上させることができます

次の例は、ASA のインバウンド トラフィックとアウトバウンド 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。

グローバルに設定：MSS 超過パケットを許可するための MPF 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

この項では、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紹介しています。

「トラブルシューティング」の項の手順を繰り返して、意図したとおりに設定が変更されていることを確認します。

接続に成功した場合の Syslog

```
%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.
```

接続に成功した場合の 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.
> 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.

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
- セキュリティ製品のフィールド通知（Cisco 適応型セキュリティ アプライアンス（ASA）を含む）
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems