PIX/ASA 7.x と IOS： VPN フラグメンテーション

目次

概要

このドキュメントでは、パケットのフラグメンテーションに関連して発生する問題を軽減するのに必要な手順を、順を追って説明しています。 フラグメンテーションの問題の例としては、ネットワーク化されたリソースへの ping は成功していながら、電子メールやデータベースなどの特定のアプリケーションではその同じリソースに接続できない場合が挙げられます。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- VPN ピア間の接続

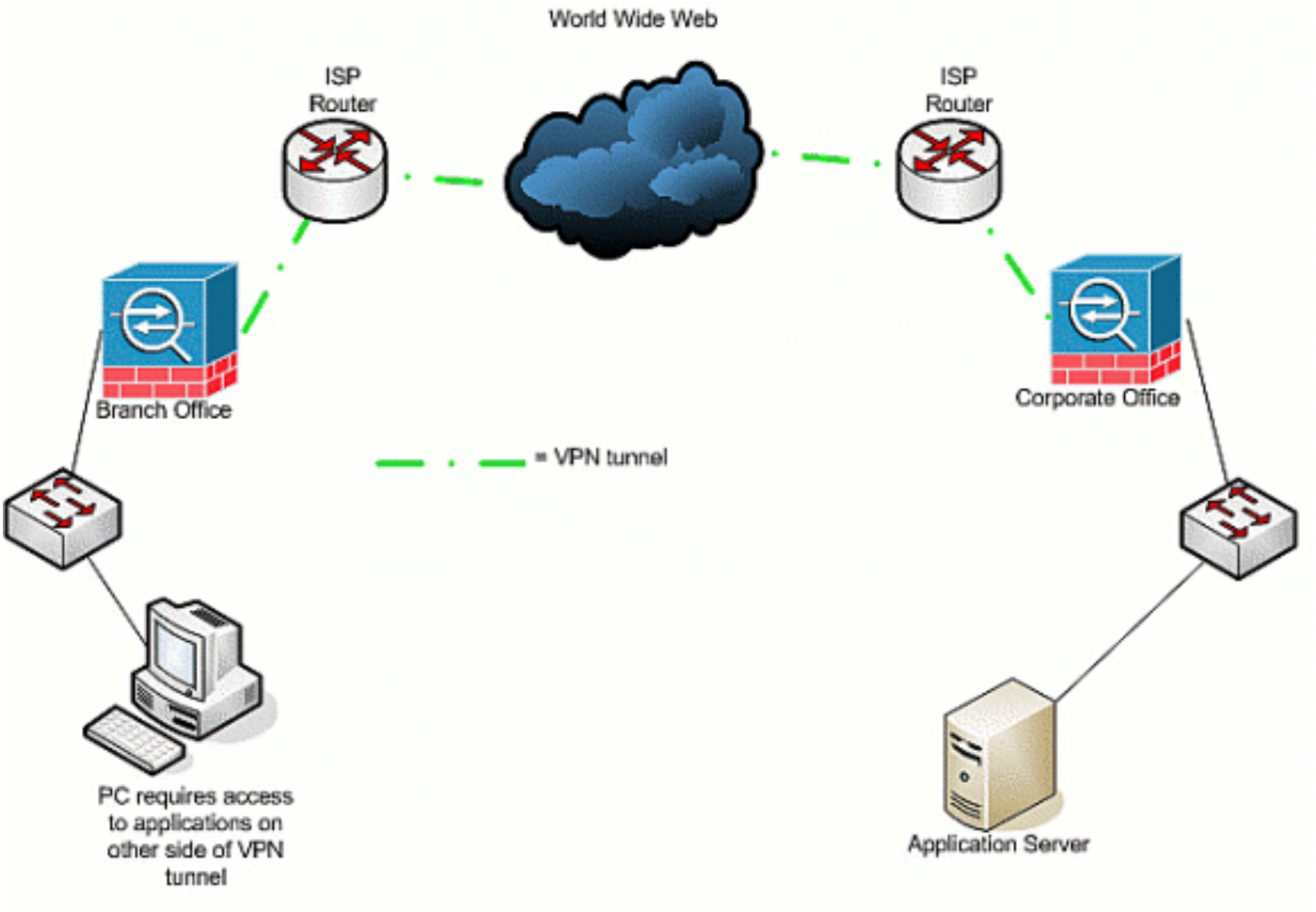
使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではあ

りません。

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。



関連製品

この設定は、次のバージョンのハードウェアとソフトウェアにも使用できます。

- IOS ルータ
- PIX/ASA セキュリティ デバイス

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。

背景説明

IP では、最大 65,536 バイト長の IP パケットがサポートされていますが、大部分のデータリンク レイヤ プロトコルでサポートされているのは、最大伝送ユニット（maximum transmission unit; MTU）と呼ばれる、これより大幅に少ないバイト長です。 特定の種類のデータリンク レイヤ メディアを通過させるためには、サポートされる最大伝送ユニットに基づいて、IP パケットの分割（フラグメント）が必要になる場合があります。 宛先では、このフラグメントを元の完全な IP

パケットに再構成する必要があります。

Protocol	Additional Bytes
ESP (encryption and hash)	56
AH	24+
GRE	24
NAT-T/IPsec over UDP (UDP part)	8
IPsec over TCP (TCP part)	20
L2TP	12
PPTP	48
Outer IP header in IPsec tunnel mode or PPTP/L2TP	20
PPPoE	8

2 つの VPN ピア間でのデータ保護のために VPN を使用すると、元のデータに追加オーバーヘッドが付加され、これにより必然的にフラグメンテーションが発生する可能性があります。 この表には、VPN 接続をサポートするために、保護されたデータへの付加が必要になる可能性のあるフィールドが掲載されています。 複数のプロトコルが必要になる可能性があり、これにより元のパケットのサイズが増加することに注意してください。 たとえば、GRE トンネルを実装し、2 つのシスコ ルータ間で L2L DMVPN IPSEC 接続を使用する場合、 ESP、GRE および外部 IP ヘッダーによる追加のオーバーヘッドが必要です。 トラフィックがアドレス デバイスを通過する際に VPN ゲートウェイへの IP セキュリティ ソフトウェア クライアント接続が用意されている場合、Network Address Translation- Traversal (NAT-T) のためのこの追加オーバーヘッド、さらにはトンネル モード接続のための外側の IP ヘッダーが必要になります。

フラグメンテーションに関連した問題

発信元から宛先へパケットが送信されると、IP ヘッダーの制御フラグ フィールド内に値が入力され、この値が中継デバイスによるパケットのフラグメンテーションを左右します。 制御フラグは 3 ビット長ですが、フラグメンテーションで使用されるのは最初の 2 ビットだけです。 2 番目のビットを 0 に設定すると、パケットのフラグメント化が許可されます。 この値を 1 に設定すると、パケットのフラグメント化は許可されません。 通常、この 2 番目のビットは *Don't Fragment (DF)* ビットと呼ばれます。 3 番目のビットでは、フラグメンテーションが発生した場合に、このフラグメンテーション化されたパケットが最後のフラグメントなのか (0 に設定)、あるいはパケットを構成するフラグメントがさらに存在するのか (1 に設定) が指定されます。

フラグメンテーションが必要な際に、問題を発生させる可能性がある 4 つの領域は次のとおりです。

- フラグメンテーションと再構成を実行する 2 つのデバイスにより、CPU サイクル内の追加のオーバーヘッドとメモリが要求されます。
- 宛先への経路でフラグメントの 1 つが廃棄された場合、パケットを再構成することができず、パケット全体をフラグメント化して再度送信する必要があります。 特に対象のトラフィッ

クがレート制限されている状況では、これによって追加のスループット問題が発生し、許容される制限を超えたトラフィックが発信元から送信されます。
- パケット フィルタリングとステートフル ファイアウォールでは、フラグメントの処理が困難になる可能性があります。 フラグメンテーションが発生すると、最初のフラグメントには外側の IP ヘッダー、TCP、UDP、ESP などの内側のヘッダー、およびペイロードの一部が含まれます。 元のパケットの後続フラグメントによって、外側の IP ヘッダーと連続するペイロードが構成されます。 このプロセスの問題は、特定のファイアウォールではインテリジェントなフィルタリングの判断を行うために、すべてのパケット内部のヘッダー情報を確認する必要があることです。 その情報が欠けていると、最初の 1 つを除くすべてのフラグメントを、誤ってドロップする可能性があります。
- パケットの IP ヘッダー内の発信元では、3 番目の制御ビットを *Don't Fragment* に設定できます。これは、中継デバイスでパケットが受信されてフラグメンテーション処理を行う必要がある場合に、中継デバイスではこれをフラグメンテーション処理できないことを意味します。 この場合、中継デバイスによりパケットが廃棄されます。

主なタスク

フラグメンテーションの検出

デフォルトの最大伝送ユニット値が 1,500 バイトである大部分のネットワークでは、一般的に IP パケットに使用されるイーサネットが使用されます。 フラグメンテーションが発生しているかどうかを検出したり、フラグメンテーションが必要であっても実行できない状況 (DF ビットが設定されている) を検出したりするには、まず VPN セッションを始動します。 次に、フラグメンテーションを検出するには、次の 4 つの手順のいずれかを使用できます。

1. もう一方の端に配置されたデバイスに ping を実行します。 これは、ping によるトンネルの通過が許可されていることを前提にしています。 これに成功したら、同じデバイスのアプリケーションへのアクセスを試行します。 たとえば、Microsoft の電子メール サーバまたはリモート デスクトップ サーバがトンネルの先にある場合、Outlook を開いて電子メールのダウンロードを試行するか、またはサーバへのリモート デスクトップを試行します。 これが実行できない場合で名前解決が適切な場合、フラグメンテーションが問題である可能性が非常に高いといえます。
2. Windows デバイスからは次のように行います。 C:\> **ping -f -l packet_size_in_bytes destination_IP_address**.パケットがフラグメンテーション処理されないように指定するには、**-f** オプションを使用します。 パケットの長さを指定するには、**-l** オプションを使用します。 まず、1,500 のパケット サイズにこれを試してください。 たとえば、**-f -l 1500 192.168.100** で ping を実行します。 フラグメンテーションが必要であるのに実行できない場合、次のようなメッセージが表示されます。 「*Packets need to be fragmented but DF set.*」
3. シスコ ルータで、**debug ip icmp コマンド**を実行して、**拡張 ping コマンド**を使用します。 「*ICMP: dst (x.x.x.x) fragmentation needed and DF set, unreachable sent to y.y.y.y*」 (x.x.x.x は宛先デバイス、y.y.y.y はルータ) と表示された場合、これは、フラグメンテーション処理が必要だが、エコー要求で DF ビットが設定されたので中継デバイスはネクスト ホップへの転送にフラグメンテーション処理ができないことを知らせる中継デバイスからの通知です。 この場合、実行可能になるまで、ping の最大伝送ユニットのサイズを段階的に小さくしていきます。
4. Cisco セキュリティ アプライアンスでは、キャプチャ フィルタを使用します。

ciscoasa(config)#access-list outside_test permit tcp any host 172.22.1.1 eq 80**注:** 発信元を *any* の状態のままにすると、管理者による任意のネットワーク アドレス変換（NAT）の監視が可能になります。ciscoasa(config)#access-list outside_test permit tcp host 172.22.1.1 eq 80 any**注:** 発信元と宛先の情報を入れ換えると、リターン トラフィックをキャプチャすることができます。`ciscoasa(config)# capture outside_interface access-list outside_test interface outside`ユーザは、アプリケーション X を使用して新しいセッションを開始する必要があります。 ユーザが新しいアプリケーション X セッションを開始した後、ASA 管理者は **show capture outside_interface** コマンドを発行する必要があります。

フラグメンテーションの問題に対するソリューション

フラグメンテーションの問題を解決するには、さまざまな方法があります。 このセクションではこれらの方法を説明しています。

方法 1： 静的最大伝送ユニットの設定

静的な最大伝送ユニットの設定によって、フラグメンテーションの問題を解決できます。

1. **ルータでの最大伝送ユニットの変更**：デバイスに手動で最大伝送ユニットを設定する場合、VPN ゲートウェイとして動作するデバイスが、トンネルを介して受信したパケットを保護したり送信したりする前に、受信したパケットをフラグメンテーション処理するように指示されることに注意します。 これは、ルータによってトラフィックが保護されてからフラグメンテーション処理が行われるよりも適切ですが、フラグメンテーション処理はデバイスによって行われます。**警告**： いずれかのデバイス インターフェイスの最大伝送ユニット サイズを変更すると、そのインターフェイスで終了したすべてのトンネルの切断と再構築が発生します。シスコ ルータで **ip mtu コマンド**を使用して、VPN が終端されているインターフェイスの最大伝送ユニット サイズを調整します。
   ```
   router (config)# interface type [slot_#/] port_#
   router (config-if)# ip mtu MTU_size_in_bytes
   ```

2. **ASA/PIX での最大伝送ユニットの変更**：ASA/PIX デバイスで、**mtu コマンド**を使用して、グローバル コンフィギュレーション モードで最大伝送ユニット サイズを調整します。 デフォルトでは、最大伝送ユニット サイズは 1500 に設定されています。 たとえば、*Outside（VPN が終端されているところ）*と名前が付けられたセキュリティ アプライアンス上にインターフェイスが配置されていて、（「フラグメンテーションの検出」セクションに掲載された方式を使用して）フラグメント サイズとして 1380 を使用すると決定した場合には、次のコマンドを使用します。
   ```
   security appliance (config)# mtu Outside 1380
   ```

方法 2： TCP の最大セグメント サイズ

TCP の最大セグメント サイズによって、フラグメンテーションの問題を解決できます。

注: この機能は、TCP だけで機能します。 他の IP プロトコルで IP フラグメンテーションの問題を解決するには、別のソリューションを使用する必要があります。 ルータで ip mtu を設定しても、TCP 3 ウェイ ハンドシェイクでの両エンド ホストの TCP MSS に関するネゴシエーション内容に影響はありません。

1. **ルータでの MSS の変更**通常、TCP トラフィックは大規模なデータの転送に使用されるため、TCP トラフィックでフラグメンテーションが発生します。 TCP では TCP maximum segment size（MSS; 最大セグメント サイズ）と呼ばれる機能がサポートされており、2 台のデバイスによる TCP トラフィックの適切なサイズのネゴシエーションが可能です。 MSS 値は、各デバイスで静的に設定され、想定されるパケットに使用するバッファ サイズを表します。 2 つのデバイスが TCP 接続を確立すると、3 ウェイ ハンドシェイクの間にローカル MSS 値とローカルの最大伝送ユニット値とが比較され、 低い方の値がリモート ピアに送信されます。 次に、交換された 2 つの値の小さい方の値が 2 つのピアによって使用されます。 この機能を設定するには、次を実行します。シスコ ルータでは、VPN が終端されているインターフェイスで **tcp adjust-mss** コマンドを使用します。
```
router (config)# interface type [slot_#/] port_#
router (config-if)# ip tcp adjust-mss MSS_Size_in_bytes
```

2. **ASA/PIX での MSS の変更**最大の TCP セグメント サイズが設定した値を超えず、最大値が指定したサイズ未満ではないことを確認するには、グローバル コンフィギュレーション モードで **sysopt connection コマンド**を使用します。 デフォルト設定を復元するには、このコマンドの no 形式を使用します。 デフォルトの最大値は 1380 バイトです。 デフォルトでは最小値の機能は無効になっています（0 に設定）。デフォルトの最大 MSS 制限を変更するには、次を実行します。
```
security appliance (config)# sysopt connection tcp-mss MSS_size_in_bytes
```

   注: 最大サイズを 1380 より大きく設定する場合、MTU（最大伝送ユニット）のサイズ（デフォルトでは 1500）によってはパケットがフラグメント化する可能性があります。 数多くのフラグメントによって、フラグ ガード機能の使用時にセキュリティ アプライアンスのパフォーマンスが影響される可能性があります。 最小サイズを設定すると、TCP サーバによる数多くの小規模な TCP データ パケットのクライアントへの送信や、サーバとネットワークのパフォーマンスへの影響が回避されます。最小の MSS 制限を変更するには、次を実行します。
```
security appliance (config)# sysopt connection tcp-mss MSS_size_in_bytes
```

   security appliance (config)# sysopt connection tcp-mss minimum MSS_size_in_bytes**注:** MSS を超過するパケット許可するための別の方法の詳細については、『PIX/ASA 7.X の問題：MSS 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』ドキュメントの「MSS を超過したパケットを許可するための MPF の設定」の項を参照してください。

方法 3： パス最大伝送ユニット検出（PMTUD）

PMTUD によって、フラグメンテーションの問題を解決できます。

TCP MSS の主な問題は、フラグメンテーションの発生を回避するために、ルータ上に設定する値を管理者が認識する必要がある点です。 ユーザとリモート VPN の場所の間に複数のパスが存在する場合はこれが問題となる可能性があり、最初のクエリーを実行すると、1 番小さな最大伝送ユニットではなく、2 番目または 3 番目に小さな最大伝送ユニットが最初のクエリー内部のルーティング決定に基づいていることがわかります。 PMTUD を使用すると、フラグメンテーションを回避する IP パケットの最大伝送ユニット値を設定できます。 ICMP メッセージがルータによってブロックされる場合、パス MTU が破損しており、DF ビットが設定されているパケットが廃棄されます。 DF ビットをクリアして、パケットのフラグメント化と送信を許可するには、**set ip df コマンド**を使用します。 フラグメンテーションによってネットワーク上でのパケット転送の速度が低下する可能性がありますが、DF ビットがクリアされるパケットの数を制限するためにアクセス リストを使用できます。

1. 次の 3 つの問題が原因で、PMTUD が機能しないことがあります。中継ルータではパケットの廃棄は可能であるが、ICMP メッセージを返さない。 これはインターネット上ではあまり一般的ではありませんが、ルータが ICMP 到達不能メッセージを返さないように設定されているネットワーク内部では一般的である場合があります。中継ルータでは ICMP 到達不能メッセージを返すことができるが、リターン フローではこのメッセージがファイアウォールによってブロックされる。 これは、より頻繁に発生します。ICMP 到達不能メッセージは発信元に戻るが、発信元ではフラグメンテーション メッセージが無視される。 これは 3 つの問題の中では最も一般的ではありません。1 番目の問題が発生する場合、発信元によって配置された IP ヘッダー内の DF ビットをクリアするか、手動で TCP MSS サイズを調整することができます。 DF ビットをクリアするには、中継ルータによって値が 1 から 0 に変更される必要があります。通常、これはパケットがネットワークを離れる前に、ネットワーク内のルータによって実行されます。 IOS ベースのルータ上でこれを実行する簡単なコード設定を次に示します。

```
Router (config) # access-list ACL_# permit tcp any any
Router (config) # route-map route_map_name permit seq#
Router (config-route-map) # match ip address ACL_#
Router (config-route-map) # set ip df 0
Router (config-route-map) # exit
Router (config) # interface type [slot#/]port #
Router (config-if) # ip policy router-map route_map_name
```

2. **PMTUD トンネルと GRE トンネル**デフォルトでは、ルータはルータ自体が生成する GRE トンネル パケットに対して PMTUD を実行しません。 GRE トンネル インターフェイスに対する PMTUD を有効にして、トンネルを通過するトラフィックの発信元と宛先のデバイスの MTU 調整プロセスにルータを参加させるには、次の設定を使用します。Router (config) # interface tunnel tunnel_#Router (config-if) # tunnel path-mtu-discoverytunnel path-mtu-discovery コマンドを使用すると、ルータの GRE トンネル インターフェイスで PMTUD が有効になります。 オプションの age-timer パラメータでは、（GRE ヘッダーの 24 バイトを差し引いた）検出された最大 MTU サイズのリセットをトンネル インターフェイスが開始するまでの分数を指定します。 タイマーに *infinite* を指定すると、タイマーは使用されません。 min-mtu パラメータでは、最大伝送ユニット値を構成する最小バイト数が指定されます。
3. **PIX/ASA 7.x：Don't Fragment（DF）のクリア**または大規模なファイルやパケットの処理この最大伝送ユニット サイズのエラー メッセージが表示されるため、インターネット、大規模なファイル、またはアプリケーションにトンネルを経由して適切にアクセスすることができない場合があります。

```
PMTU-D packet 1440 bytes greater than effective mtu 1434,
 dest_addr=10.70.25.1, src_addr=10.10.97.55, prot=TCP
```

この問題を解決するには、デバイスの外部インターフェイスから DF ビットを確実にクリアします。 グローバル コンフィギュレーション モードで **crypto ipsec df-bit** コマンドを使用して、IP セキュリティ パケットの DF ビット ポリシーを設定します。

```
pix(config)# crypto ipsec df-bit clear-df outside
```

IP セキュリティ トンネル機能を使用した DF ビットによって、カプセル化されたヘッダーからの Don't Fragment（DF）ビットをセキュリティ アプライアンスでクリア、設定、またはコピーできるかどうかを指定することができます。 IP ヘッダー内部の DF ビットによって、デバイスによるパケットのフラグメント化が許可されるかどうかが判断されます。カプセル化されたヘッダー内で DF ビットを指定するようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec df-bit** コマンドを使用

します。トンネル モード IP セキュリティ トラフィックをカプセル化する際に、DF ビットの clear-df 設定を使用します。 この設定を使用すると、使用可能な最大伝送ユニットのサイズを超えるパケットをデバイスで送信できます。 この設定は、使用可能な最大伝送ユニットのサイズが不明な場合にも適しています。

注: フラグメンテーションの問題が引き続き発生し、パケットが廃棄される場合、オプションとして、**ip mtu tunnel interface** コマンドを使用して手動で最大伝送ユニットのサイズを調整できます。 この場合は、ルータによってパケットが保護される前にフラグメント化されます。 このコマンドは、PMTUD や TCP MSS と組み合せても使用可能です。

確認

現在、この設定に使用できる確認手順はありません。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

トラブルシューティング

VPN 暗号化エラー

IP セキュリティ トンネルがルータと PIX 間に確立されたと仮定します。 パケットが廃棄されたことを示す暗号化エラー メッセージが表示される場合、次の手順を実行して問題を解決します。

1. クライアントからサーバ側にスニファ トレースを実行して、どちらが使用に最適な最大伝送ユニットであるのかを判断します。ping テストも使用できます。

   ```
   ping  -l  1400  192.168.1.1 -f
   ```

   192.168.1.1 はリモート マシンの IP アドレスです。
2. 応答が発生するまで、1400 の値を 20 ずつ下げていきます。**注:** 大部分のインスタンスで機能する、効果的な値は 1300 です。
3. 適切な最大セグメント サイズが判明したら、使用するデバイス用に適当に調整します。PIX ファイアウォール上で、次のコマンドを発行します。

   ```
   sysopt connection tcpmss 1300
   ```

   ルータ側：

   ```
   ip tcp adjust-mss 1300
   ```

RDP と Citrix の問題

問題：

VPN ネットワーク間で ping を実行できますが、Remote Desktop Protocol（RDP）と Citrix の接続がトンネルを介して確立できません。

解決策：

問題は、PIX/ASA の背後にある PC 上の最大伝送ユニットのサイズである可能性があります。 クライアント マシンの最大伝送ユニット サイズを 1300 に設定して、VPN トンネルを介した Citrix 接続の確立を試してみます。

関連情報

- GRE および IP セキュリティでの IP フラグメンテーション、MTU、MSS、および PMTUD の問題の解決
- PIX/ASA 7.0 の問題： MSS 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
- 一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について
- GRE トンネルを使用しているときにインターネットをブラウズできない理由
- テクニカル サポートとドキュメント – Cisco Systems