FWSM： 間違った xlate によるトラフィック障害のトラブルシューティング

目次

概要
前提条件
要件
使用するコンポーネント
表記法
症状
論理トポロジ
関連コンフィギュレーション
確認された動作
トリガ
解決策
正しくないルーティング コンフィギュレーションを解決する
same-security-traffic permit intra-interface をディセーブルにする
正しくないインターフェイスに到着したパケットをドロップする（ACL または uRPF）
xlate-bypass をイネーブルにする
要約
関連情報

概要

ファイアウォール サービス モジュール（FWSM）のパケット処理の設計が原因で、間違ってルーティングされたパケットによって作成された xlate により、ファイアウォールを経由する接続でトラフィックの障害が発生する可能性があります。 インバウンド パケットの出力インターフェイスを選択する場合、FWSM は、最初に、インバウンド パケットの宛先 IP が、その NAT 変換（xlate）テーブルでインバウンド インターフェイスの xlate の既存のグローバル IP/ネットワークに一致するか確認します。 一致が検出されると、出力インターフェイスは、xlate エントリの ローカル インターフェイスに基づいて選択されます。ファイアウォールは、出力インターフェイスの決定にルーティング テーブルを使用しません。

FWSM は、デフォルトでは、いずれかのインターフェイスで受信される、許可された任意のパケットの送信元 IP の xlate エントリを構築します。 パケットがネットワークを介して（何らかの理由で）誤ってルーティングされ、FWSM の不正インターフェイスの着信側に到着すると、これを反映する xlate が構築されます。 この場合、xlate テーブルのエントリは、ルーティング テーブルのエントリを上書きするので、対象宛先でトラフィック障害が発生します。

このドキュメントでは、この問題の症状および原因、診断方法、問題を防ぐための解決策について説明します。

前提条件

要件

FWSM に関する基本的な知識があることが推奨されます。

使用するコンポーネント

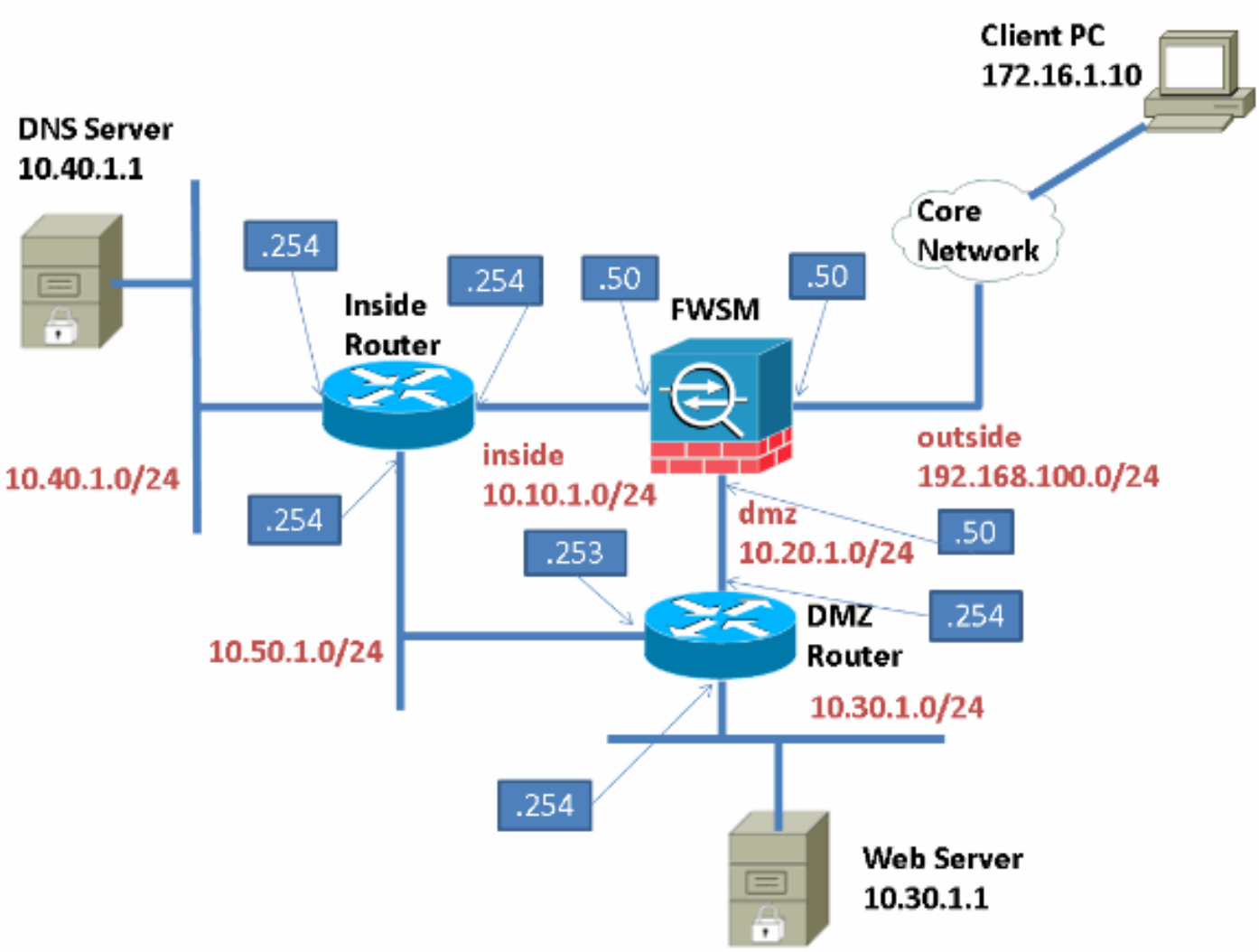
このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

症状

論理トポロジ



関連コンフィギュレーション

```
interface Vlan1
 nameif outside
 security-level 0
 ip address 192.168.100.50 255.255.255.0
!
interface Vlan10
 nameif inside
 security-level 100
 ip address 10.10.1.50 255.255.255.0
!
interface Vlan20
 nameif dmz
 security-level 50
 ip address 10.20.1.50 255.255.255.0
!
same-security-traffic permit intra-interface
access-list outside_in extended permit tcp any host 10.30.1.1 eq www
access-list inside_in extended permit ip any any
access-group inside_in in interface inside
access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.100.254
route dmz 10.30.1.0 255.255.255.0 10.20.1.254
```

確認された動作

172.16.1.10 のクライアント PC から 10.30.1.1 の Web サーバへの接続は失敗します。

外部インターフェイスのパケット キャプチャは、FWSM のインターフェイスに到着するクライアント PC からの TCP SYN を示します。

```
FWSM# show capture outside
3 packets seen, 3 packets captured
   1: 13:58:09.280752960 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
   2: 13:58:12.280755950 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
   3: 13:58:18.280761960 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
3 packets shown
```

dmz インターフェイスのパケット キャプチャは、ファイアウォールから発信されるパケットは示しません。

```
FWSM# show capture dmz
0 packet seen, 0 packet captured
0 packet shown
```

FWSM の接続テーブルにエントリは構築されません。syslog は、クライアントまたはサーバ IP アドレスに関連する情報を示しません。

トリガ

基本レベルでは、この問題の原因は、誤ってルーティングされたパケットにより構築された FWSM の xlate テーブルのエントリです。 FWSM のパケット処理の設計のため、ファイアウォールは、ルーティング テーブルの前に xlate テーブルをチェックして、出力インターフェイスを決定します。 その結果、パケットが既存の xlate と一致すると、エントリがルーティング テーブルでリストされているエントリと競合する場合でも、そのエントリに基づいて出力インターフェイスが選択されます。 つまり、xlate テーブルは、ルーティング テーブルより優先されます。

この問題を診断するには、**show xlate debug** コマンドの出力をチェックします。

```
FWSM# show xlate debug
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       o - outside, r - portmap, s - static
3 in use, 3 most used
NAT from inside:10.30.1.1 to outside:10.30.1.1 flags Ii idle 0:00:00 timeout 3:00:00 connections
0
NAT from inside:10.30.1.1 to inside:10.30.1.1 flags Ii idle 0:00:07 timeout 3:00:00 connections
0

NAT from dmz:10.30.1.1 to outside:10.30.1.1 flags Ii idle 0:00:10 timeout 3:00:00 connections 0
```

注: show xlate の debug キーワードは重要です。 このキーワードを使用しない場合、xlate エントリに、エントリが関連付けられているインターフェイス名が含まれません。

xlate テーブルは、Web サーバに構築されている xlate が 3 つあることが示されます。 1 つめの xlate は、**内部**インターフェイスと**外部**インターフェイス間で構築されます。 2 つめの xlate は、ヘアピニングまたは U ターン xlate として**内部**インターフェイスで構築されます。 3 つめの xlate は、**dmz** と**外部**インターフェイス間で構築されます。 I フラグは、これがアイデンティティ xlate であり、IP が実際には変換されないことを示します。

エントリにリストされる 1 つめのインターフェイスは、IP が実際に存在するとされる「リアル」または「ローカル」インターフェイスです。 2 つめにリストされるインターフェイスは、IP が変換される「マップされた」または「グローバル」インターフェイスです。 これらの xlate はいずれも正しくありません。 これは、Web サーバ (10.30.1.1) が実際には **dmz** インターフェイスの後ろにあるためです。 3 つめの xlate は、このネットワーク設計では正しい xlate です。

テーブルに最初にリストされる xlate が原因で、接続障害が発生します。 クライアントの TCP SYN パケットが 10.30.1.1 を宛先とする外部インターフェイスに到着すると、FWSM は、xlate テーブルをチェックして、最初のエントリとマッチングします。 このエントリは、パケットが**内部**インターフェイスから出力することを示します。これは正しくなく、パケットは吸い込まれます。

デフォルトでは、FWSM は、明示的に設定された NAT ルールと一致しない任意のトラフィックにアイデンティティ xlate を自動的に構築します。 このため、パケットが正しくないインターフェイスに間違って到着すると、xlate が構築されます。 特にこの場合、10.30.1.1 から送信されたパケットは、予期されている **dmz** インターフェイスに到着せずに、**内部**インターフェイスの着信側に到着しました。

最初の xlate (**内部 > 外部**) は、Web サーバが存在しない IP アドレス (10.199.199.1) を ping しようとしたときに構築されました。 エコー要求は、デフォルト ゲートウェイ (DMZ ルータ) を宛先とする Web サーバから送信されました。 DMZ ルータはスタティック ルートに従ってパケットを内側のルータに向けて転送しました。

```
S       10.0.0.0/8 [1/0] via 10.50.1.254
```

10.199.199.0/24 ネットワークは実際には存在しないので、内部ルータは、そのデフォルト ルートに従い、パケットを FWSM の**内部**インターフェイスに送信します。

```
S*   0.0.0.0/0 [1/0] via 10.20.1.50
```

同様に、FWSM には、宛先ネットワークのルートがありません。 そのため、出力インターフェイスとして外部インターフェイスを選択して、アイデンティティ xlate を**内部 > 外部**から構築します。

```
S    0.0.0.0 0.0.0.0 [1/0] via 192.168.100.254, outside
```

2 つめの xlate (**内部 > 内部**) は、内部ルータの 10.40.1.254 インターフェイスがリンク フラップにより一時的にダウンし、Web サーバが DNS サーバにアクセスしようとしたときに構築されました。 DNS 要求は、デフォルト ゲートウェイ (DMZ ルータ) を宛先とする Web サーバから送

信されました。 DMZ ルータはスタティック ルートに従ってパケットを内側のルータに向けて転送しました。

```
S       10.0.0.0/8 [1/0] via 10.50.1.254
```

ただし、10.40.1.0/24 ネットワークに接続される内部ルータのインターフェイスは一時的にダウンし、このネットワークに直接接続されているルートは欠落しました。 そのため、ルーティング テーブルで一致するルートは、FWSM へのデフォルトのルートだけでした。

```
S*   0.0.0.0/0 [1/0] via 10.20.1.50
```

パケットは、FWSM の**内部**インターフェイスにルーティングされました。 FWSM のルーティング テーブルは、10.40.1.0/24 の宛先ネットワークが同じ**内部**インターフェイスの後ろにあることを示していました。

```
S    10.40.1.0 255.255.255.0 [1/0] via 10.10.1.254, inside
```

same-security-traffic permit intra-interface コマンドがイネーブルのため、FWSM は、U ターン xlate を構築できます。

要約すると、最初の xlate は、次のことに基づいてトリガされました。

- DMZ ルータで構成されたブロード 10.0.0.0/8 ルート
- FWSM の内部インターフェイスで構成された **permit ip any any ACL**

2 つめの xlate は、次のことに基づいてトリガされました。

- 内部ルータのフラッピング インターフェイス
- FWSM で構成された **same-security-traffic permit intra-interface**

解決策

この問題にはさまざまな解決策があります。 通常、テーブルから xlate を削除すると、xlate が再構築されるまで、トラフィックは動作を再開します。 これは、**clear xlate** コマンドを使用して完了できます。 次に、例を示します。

```
FWSM# clear xlate interface inside local 10.30.1.1 global 10.30.1.1
```

注: 削除された xlate を使用している接続は切断されます。

完了したら、xlate が繰り返されないようにします。 通常、間違った FWSM インターフェイスにトラフィックが到着しないように環境のルーティング コンフィギュレーションを修正することをお勧めします。 FWSM は、これらの問題に対応する構成オプションをいくつか提供します。

正しくないルーティング コンフィギュレーションを解決する

このソリューションでは、ネットワーク環境を注意して計画し、よく理解する必要があります。 上記の最初の例では、DMZ ルータの 10.0.0.0/8 ルートは、/8 ネットワーク全体が 10.50.1.253 インターフェイス外にないので、技術的には正しくありません。 ただし、次のいくつかのオプションがあります。

- 10.50.1.0/24 ネットワークをまとめて削除し、FWSM を介してすべてのトラフィックをルーティングする。 これにより、内部および DMZ ネットワーク間のセグメンテーションおよびセキュリティを改善できます。
- 10.40.1.0/24 のみで DMZ のスタティック ルートを設定し、10.0.0.0/8 ルートを削除する。

- 内部および DMZ ルータ間でダイナミック ルーティング プロトコルを使用し、実在するネットワークのみを正しくアドバタイズする。

ルーティング コンフィギュレーションを調整するたくさんの方法がありますが、目的は、特定のホストから送信されるトラフィックが、1 つの FWSM インターフェイスだけに到着できるようにすることです。

same-security-traffic permit intra-interface をディセーブルにする

same-security-traffic permit intra-interface コマンドを使用すると、FWSM が、インターフェイスでトラフィックを U ターンまたはヘアピニングできます。 つまり、パケットは、送信時と同じインターフェイスのファイアウォールに入ることができます。 この機能は、デフォルトでディセーブルにされ、ほとんどの FWSM 設計で役に立ちません。 FWSM は VLAN インターフェイスを使用するので、同じ VLAN にあるトラフィックは、FWSM により処理されません。

前述の 2 つめの例では、**same-security-traffic permit intra-interface** コマンドにより、パケットは**内部**インターフェイスで発信および着信できます。 **same-security-traffic permit intra-interface** をディセーブルにすることで、この動作を防ぎ、xlate が構築されるまでパケットをドロップできます。

```
FWSM(config)# no same-security-traffic permit intra-interface
```

正しくないインターフェイスに到着したパケットをドロップする（ACL または uRPF）

前述のいずれの例でも、xlate は、Web サーバから送信されたパケットが誤って**内部**インターフェイスに到着したときに構築されました。 問題を解決するには、FWSM を設定して、間違ったインターフェイスに到着するパケットをドロップできます。

FWSM では、トラフィックを送受信するには、すべてのトラフィックが ACL で許可される必要があります。 そのため、この機能は、各インターフェイスで該当する発信元ネットワークからのトラフィックを許可だけで実行できます。 前述の例では、**内部**インターフェイスは、すべての IP トラフィックを許可します。

```
access-list inside_in extended permit ip any any
```

ただし、10.10.1.0/24 および 10.40.1.0/24 サブネットからのトラフィックを許可するように変更する必要があります。

```
access-list inside_in extended permit ip 10.10.1.0 255.255.255.0 any

access-list inside_in extended permit ip 10.40.1.0 255.255.255.0 any
```

環境によっては、FWSM を介して送受信する異なるネットワークのサイズまたはスケール、あるいはこれらの両方により、適したオプションでない場合があります。 ただし、この機能は、Unicast Reverse Path Forwarding（uRPF）と呼ばれる機能を使用するだけ実行できます。

uRPF 機能がイネーブルの場合、FWSM は、すべての接続の最初のパケットの送信元 IP アドレスをルーティング テーブルと比較します。 検出されたルートが、パケットが到着したインターフェイスと一致しない場合、RPF 障害によりそのパケットはドロップされます。

前述の例では、FWSM には、**dmz** インターフェイスを使用して 10.30.1.0/24 ネットワークに到達するスタティック ルートがあります。 そのため、uRPF が**内部**インターフェイスでイネーブルにされている場合、**内部**インターフェイスに誤って到着する Web サーバ（10.30.1.1）から送信されたパケットはドロップされます。

uRPF をイネーブルにするには、**ip verify reverse-path** コマンドを対象の各インターフェイスに適用します。 次に、例を示します。

```
FWSM(config)# ip verify reverse-path interface inside
```

xlate-bypass をイネーブルにする

上記のいずれの例でも、xlate は、Ii フラグを使用して作成されます。 これらのフラグは、xlate がハイ セキュリティ (i) インターフェイスから発信されたアイデンティティ変換 (I) であることを示します。 デフォルトでは、FWSM は、明示的な NAT/PAT ルールと一致しない任意のトラフィックでこれらの xlate を構築します。 この動作をディセーブルにするには、**xlate-bypass** コマンドは、FWSM 3.2(1) 以降でイネーブルにできます。

```
FWSM(config)# xlate-bypass
```

この機能を使用すると、FWSM は、最初にアイデンティティ xlate を構築しません。 そのため、前述の例のトラフィックは、xlate テーブル エントリにより正しくないインターフェイスにリダイレクトされません。 ただし、トラフィックは、変換されない FWSM を介して送受信されます。

要約

パケットの出力インターフェイスを決定する場合、FWSM は、ルーティング テーブルを参照する前に xlate テーブルを参照します。 このパケットが既存の xlate と一致する場合、出力インターフェイスは、xlate の関連インターフェイスに基づいて選択されます。 これは、ルーティング テーブルで矛盾がある場合も発生します。 このように、xlate テーブルは、ルーティング テーブルより優先されます。

FWSM はデフォルトですべての新しい接続に xlate エントリを構築するので、誤ってルーティングされたパケットにより FWSM が xlate を構築する場合、トラフィック障害が発生します。 前述のように、この問題が発生する可能性は多くありますが、いずれの場合も、正しくないインターフェイスで受信されるパケットが原因です。 このドキュメントでは、次の可能性のある問題について説明しました。

- ブロード ルーティング構成が、誤った方向にパケットを送信する
- FWSM が、間違った送信元ネットワークからのトラフィックを許可するように構成される
- FWSM が、トラフィックをヘアピニング/U ターンするように構成される

間違った xlate により失敗する接続で接続を素早く復元するには、**clear xlate** コマンドを使用してエントリを削除します。 このドキュメントでは、これらの xlate が繰り返されないようにするための解決策についていくつか提供しました。

- 固有なルートを使用して、正しくないルーティング コンフィギュレーションを解決する
- same-security-traffic permit intra-interface をディセーブルにする
- ACL または uRPF を使用して、正しくないインターフェイスに到着するパケットをドロップする
- xlate-bypass をイネーブルにする

関連情報

- コマンド リファレンス： ip verify reverse-path
- コマンド リファレンス： xlate-bypass

- テクニカルサポートとドキュメント - Cisco Systems