ASA 8.3：Cisco セキュリティ アプライアンス経由の接続の確立とトラブルシューティング

内容

概要

Cisco 適応型セキュリティ アプライアンス（ASA）の初期の設定では、デフォルトのセキュリティ ポリシーが適用され、内部から出ることはできますが、外部から入ることはできません。これとは異なるセキュリティ ポリシーを適用する必要があるサイトの場合、外部のユーザは ASA 経由で Web サーバに接続することができます。

Cisco ASA を経由して基本的な接続性を確立したら、ファイアウォールの設定を変更できます。ASA に追加する設定変更はすべて、サイトのセキュリティ ポリシーに準拠している必要があります。

バージョン 8.2 以前の Cisco 適応型セキュリティ アプライアンス（ASA）の同一の設定については、「PIX/ASA：Cisco セキュリティ アプライアンスによる接続の確立とトラブルシューティング』を参照してください。

前提条件

要件

このドキュメントは、Cisco ASA での一部の基本設定がすでに終了していることを前提としています。ASA の初期設定の例については、次のドキュメントを参照してください。

- ASA 8.3(x)：インターネットへの単一の内部ネットワークの接続

- Cisco 適応型セキュリティ アプライアンス（ASA）での PPPoE クライアントの設定

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 以降を稼働する Cisco 適応型セキュリティ アプライアンス（ASA）に基づいています。

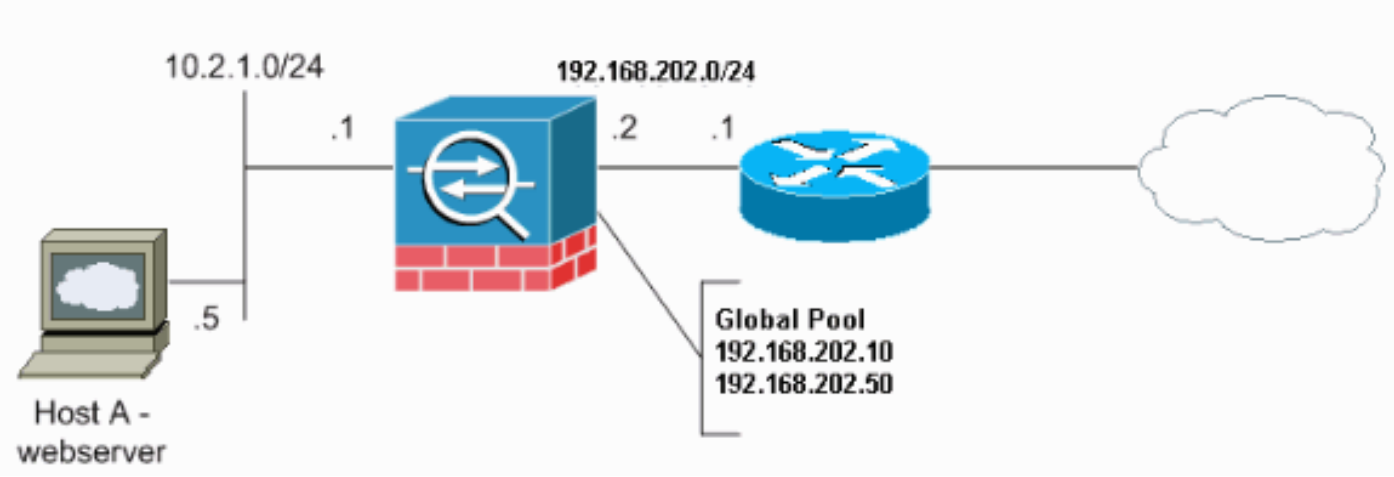
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『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。

ASA を経由した接続性の動作

このネットワークでは、ホストAは10.2.1.5の内部アドレスを持つWebサーバです。Webサーバには192.168.202.5の外部（変換）アドレスが割り当てられます。インターネットユーザがWebサーバにアクセスするには、192.168.202.5をポイントする必要があります。Web サーバの DNS エントリも、そのアドレスである必要があります。インターネットから他の接続はできません。



注：この設定で使用されるIPアドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。これらは、ラボ環境で使用された RFC 1918 のアドレスです。

Cisco ASA を経由した接続性の設定

ASA 経由の接続性を設定するには、次の手順を実行します。

1. IP プールの範囲で、内部サブネットと別のネットワーク オブジェクトを定義するネットワーク オブジェクトを作成します。次のネットワーク オブジェクトを使用して NAT を設定します。

```
object network inside-net
subnet 0.0.0.0 0.0.0.0
```

```
object network outside-pat-pool
range 192.168.202.10 192.168.202.50
nat (inside,outside) source dynamic inside-net  outside-pat-pool
```

2. インターネット ユーザがアクセスする内部ホストに、スタティックな変換アドレスを割り当てます。

```
object network obj-10.2.1.5
  host 10.2.1.5
  nat (inside,outside) static 192.168.202.5
```

3. **access-list コマンドを使用して、Cisco ASA 経由で外部ユーザがアクセスできるようにします。access-list コマンドでは、常に変換アドレスを使用します。**

```
access-list 101 permit tcp any host 192.168.202.5 eq www
  access-group 101 in interface outside
```

ARP ブロードキャスト トラフィックの許可

セキュリティ アプライアンスは、Inside インターフェイスと Outside インターフェイスで同じネットワークに接続します。トランスペアレント ファイアウォールはルーティングされたホップではないので、既存のネットワークに簡単に導入できます。IP の再アドレッシングは必要ありません。IPv4 トラフィックは、アクセス リストなしで、高いセキュリティ インターフェイスから低いセキュリティ インターフェイスに、透過ファイアウォールを自動的に通過することを許可されます。Address Resolution Protocol (ARP; アドレス解決プロトコル) は、アクセス リストなしで、両方向に透過ファイアウォールの通過を許可されます。ARP トラフィックは、ARP インスペクションによって制御できます。低いセキュリティ インターフェイスから高いセキュリティ インターフェイスに移動するレイヤ 3 トラフィックの場合は、拡張アクセス リストが必要です。

注：トランスペアレントモードのセキュリティアプライアンスは、Cisco Discovery Protocol(CDP)パケットやIPv6パケット、または0x600以上の有効なEtherTypeを持たないパケットを渡しません。たとえば、IS-ISパケットを渡すことはできません。Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) は例外でサポートされます。

許可された MAC アドレス

次の宛先 MAC アドレスは、透過なファイアウォールを通過することが許可されています。このリストにない MAC アドレスはドロップされます。

- FFFF.FFFF.FFFF に等しい TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ~ 0100.5EFE.FFFF の IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ~ 3333.FFFF.FFFF の IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD に等しい BPDU マルチキャスト アドレス
- 0900.0700.0000 ~ 0900.07FF.FFFF の Appletalk マルチキャスト MAC アドレス

ルータ モードで通過を許可されないトラフィック

ルータ モードでは、あるタイプのトラフィックは、アクセス リストで許可されていたとしても、セキュリティ アプライアンスを通過できません。ただし、透過ファイアウォールは、拡張アクセ

ス リスト（IP トラフィックの場合）または EtherType アクセス リスト（IP トラフィック以外の場合）を使用して、ほとんどすべてのトラフィックの通過を許可できます。

たとえば、透過ファイアウォールを通してルーティング プロトコルの隣接関係を確立できます。拡張アクセス リストに基づいて、Open Shortest Path First（OSPF）、Routing Information Protocol（RIP; ルーティング情報プロトコル）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）の各トラフィックの通過を許可できます。同様に、ホットスタンバイ ルータ プロトコル（HSRP）や仮想ルータ冗長プロトコル（VRRP）などのプロトコルは、セキュリティ アプライアンスを通過できます。

IP 以外のトラフィック（AppleTalk、IPX、BPDU、MPLS など）は、EtherType アクセス リストを使用して、通過を許可されるように設定できます。

透過型ファイアウォール上で直接サポートされない機能の場合、上流および下流のルータによって機能がサポートされるように、トラフィックの通過を許可することができます。たとえば、拡張アクセス リストを使用すると、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）トラフィック（サポートされない DHCP リレー機能の代わりに）や、IP/TV によって作成されるもののようなマルチキャスト トラフィックを許可できます。

接続性に関する問題のトラブルシューティング

インターネット ユーザが Web サイトにアクセスできない場合は、次の手順に従ってください。

1. 設定アドレスが正しく入力されていることを確認します。有効な外部アドレス正しい内部アドレス外部 DNS が保持する変換アドレス
2. outside インターフェイスでエラーが発生していないかどうかを確認します。Cisco セキュリティ アプライアンスは、インターフェイスの速度とデュプレックス モードを自動検出するように事前設定されています。ただし、自動ネゴシエーション処理が失敗する可能性のある状況がいくつか存在します。その結果、速度またはデュプレックス モードの不一致（およびパフォーマンスの問題）が発生します。 ミッション クリティカルなネットワーク インフラストラクチャの場合、シスコがインターフェイスごとに速度とデュプレックス モードを手動でハードコーディングするため、エラーが発生する可能性はありません。これらのデバイスは通常、固定されています。そのため、適切に設定すれば、変更する必要はありません。**例：**

   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex full
   asa(config-if)#speed 100
   asa(config-if)#exit
   ```

   状況によっては、速度とデュプレックス モードの設定をハードコーディングすると、エラーが発生する場合があります。そのため、次の例に示すように、自動検出モードのデフォルト設定に、インターフェイスを設定する必要があります。**例：**

   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex auto
   asa(config-if)#speed auto
   asa(config-if)#exit
   ```

3. ASA またはヘッドエンド ルータのインターフェイスを通してトラフィックが送受信されない場合は、ARP の統計をクリアしてみてください。

   ```
   asa#clear arp
   ```

4. スタティック変換が有効になっているかどうか確認するには、**show run object および show run static コマンドを使用します。例：**

```
object service www
service tcp source eq www
object network 192.168.202.2
host 192.168.202.2
object network 10.2.1.5
host 10.2.1.5
object service 1025
service tcp source eq 1025
nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www
```

このシナリオでは、Outside の IP アドレスが、Web サーバのマッピングされる IP アドレスとして使用されます。

```
nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www
```

5. Web サーバのデフォルト ルートが ASA の内部インターフェイスを指していることを確認します。
6. show xlate コマンドを使用して変換テーブルを調べ、変換が作成されたかどうかを確認します。
7. 拒否が発生しているかどうかをログ ファイルで調べるには、**logging buffered コマンドを使用します**（変換アドレスを捜し、拒否の有無を調べます）。
8. capture コマンドを使用します。

```
access-list webtraffic permit tcp any host 192.168.202.5

capture capture1 access-list webtraffic interface outside
```

注：このコマンドは、大量の出力を生成します。トラフィックの負荷が大きい場合は、ルータがハングまたはリロードする可能性があります。

9. パケットが ASA に到達した場合は、ASA から Web サーバへのルートが正しいことを確認します（ASA 設定で **route コマンドをチェックします）。**
10. プロキシ ARP が無効になっているかどうかを確認します。ASA 8.3 で **show running-config sysopt コマンドを発行します。**ここでは、プロキシ ARP を **sysopt noproxyarp outside コマンドで無効にしています。**

```
ciscoasa#show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt noproxyarp outside
sysopt connection permit-vpn
```

プロキシ ARP を再び有効にするには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
ciscoasa(config)#no sysopt noproxyarp outside
```

ホストは、同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信するときは、そのデバイスの MAC アドレスを知っている必要があります。ARP は、IP アド

レスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは ARP 要求を送信し、その IP アドレスの所有者を尋ねます。 IP アドレスを所有するデバイスが応答し、「I own that IP address;here is my MAC address」というメッセージを返します。プロキシ ARP は、背後にあるホストに代わって ARP 要求に応答することを、セキュリティ アプライアンスに許可します。セキュリティ アプライアンスは、ホストのスタティック マッピング アドレスに対する ARP 要求に応答します。セキュリティ アプライアンスは、自分の MAC アドレスで要求に応答した後、IP パケットを適切な内部ホストに転送します。たとえば、このドキュメントのダイアグラムでは、Web サーバのグローバル IP アドレス 192.168.202.5 に対して ARP 要求が行われると、セキュリティ アプライアンスは自分の MAC アドレスで応答します。この状況でプロキシARPが有効でない場合、セキュリティアプライアンスの外部ネットワーク上のホストは、アドレス192.168.202.5に対するARP要求を発行してWebサーバに到達できません。**sysoptコマンドの詳細については、コマンドリファレンスを参照してくだ**さい。

11. すべての設定が正しくてもユーザが Web サーバにアクセスできない場合は、Cisco テクニカル サポートでサービス リクエストをオープンしてください。

Error Message - %ASA-4-407001:

一部のホストはインターネットに接続できず。syslog が「`Error Message - %ASA-4-407001:Deny traffic for local-host interface_name:inside_address, license limit of number exceededsyslog`表示されます。この問題の解決方法を次に説明します。

このエラー メッセージは、使用中のライセンスのユーザ限度をユーザの数が超えると出力されます。このエラーを解消するには、ライセンスをアップグレードしてユーザの数を増やします。ユーザのライセンスは、必要に応じて 50、100、または無制限に設定できます。

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