HairPinトラフィックを使用したFTD上のVPNユーザの内部リソースアクセスの設定

内容

お問い合わせ内容

目標は、Cisco Secure Firewall FTDで（Windowsドメインに参加しているサーバに対して）RADIUSを使用してVPN認証が成功した後に、VPNユーザが内部ネットワークリソースにフルアクセスできるようにすることです。

VPNセットアップはすでに動作しています。ユーザはVPNクライアントをダウンロードしてインストールし、正常に認証できます。 この問題では、必要な内部リソースアクセスをVPN経由で許可するために必要なアクセスコントロールとNATルールの設定に焦点が当てられています。

環境

- 製品：Cisco Secure Firewall Firepower(FTD)バージョン7.6.0（CSF1220CXアプライアンスなど）
- 管理：Firepower Management Center(FMC)、クラウド配信FMC(cdFMC)、またはFirepower Device Manager(FDM)
- VPN:Windowsドメインに参加しているサーバー(NPS)に対するRADIUS認証で構成されます
- VPNアドレスプール：192.168.250.1 ~ 192.168.250.200
- ターゲット内部サブネットの例：192.168.95.0/24
- ソフトウェアバージョン：9.22.1（ワークフローで参照）
- 関連インターフェイス：VPN入力の「外部」インターフェイス
- VPN接続上でRDPおよびActive Directoryアクセスが必要

解決策

次の手順では、VPNユーザがCisco FTDの内部リソース（RDPやActive Directoryなど）にアクセスできるようにするために必要な設定の詳細を説明します。 これには、アクセスポリシールールの作成、VPNトラフィックのNAT免除およびヘアピンNATの設定、トラブルシューティングコマンドを使用した設定の検証が含まれます。

ステップ1:アクセスリストエントリを追加して、VPNアドレスプールから内部リソースにアクセスできるようにします。

```
access-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: Default Access Control Policy - Mandat
access-list CSM_FW_ACL_ remark rule-id 268438528: L7 RULE: Permit_VPN_Pool
```

ステップ2:内部リソースがVPNプールにリターントラフィックを送信できるようにするアクセスリストルールを追加します。

```
access-list CSM_FW_ACL_ advanced permit ip any object VPN_Pool
```

必要に応じて、これらのルールを後で強化して特定の送信元と宛先を制限できます。

ステップ3:VPNトラフィックのNAT免除またはヘアピンNATの設定

一般的なアプローチには次の2つがあります。

- ◦ オプションA：内部サブネットへのVPNプールのNAT免除

```
nat (outside,inside) source static VPN_Pool VPN_Pool destination static Net_192.168.95.1-24 Net_192.168
```

- ◦ オプションB：同じインターフェイス上のVPNプールに対するヘアピンNAT(no-proxy-arp)

```
nat (any,any) source static VPN_Pool VPN_Pool no-proxy-arp
```

- ◦ 選択肢C：外部インターフェイスのVPNプールのダイナミックヘアピンNAT

```
nat (outside,outside) dynamic VPN_Pool interface
```

正しい方法は、内部リソースが同じ物理インターフェイス（ヘアピンNATが必要）にあるか、異なるインターフェイス（NAT免除）にあるかによって異なります。

ステップ4:packet-tracerコマンドを使用して、VPNプールから内部リソースへのトラフィックフローをシミュレートし、目的のルール、NAT、およびルートによってトラフィックが許可されているかどうかを確認します。

```
packet-tracer input outside icmp 192.168.250.1 8 0 192.168.95.1
packet-tracer input outside tcp 192.168.250.1 12345 192.168.95.1 80
packet-tracer input inside icmp 192.168.95.1 8 0 192.168.250.1
packet-tracer input inside tcp 192.168.250.1 54321 192.168.95.1 443
--
Phase 5
```

```
ID: 5
Type: ACCESS-LIST
Result: ALLOW
Config: access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any r
Additional Information:  This packet will be sent to snort for additional processing where a verdict wi
Elapsed Time: 0 ns
--
Phase 7
ID: 7
Type: NAT
Result: ALLOW
Config: nat (outside,outside) dynamic VPN_Pool interface
Additional Information: Static translate 192.168.250.1/12345 to 192.168.250.1/12345 Forward Flow based
Elapsed Time: 0 ns
```

注：WebVPNフェーズのパケットトレーサ出力では、外部インターフェイスのVPNトラフィックが「DROP」と表示される場合があります。 これは、外部インターフェイスのプレーンテキストトラフィックでは想定される動作であり、NATの検証に使用できます。

追加メモ：

- Threat Defense UIのパケットキャプチャに着信要求だけが表示される場合があります。 ドロップは観察されないが、トラフィックが内部リソースに到達しない場合は、NATとアクセスリストルールを確認します。
- SSHが使用できない場合、すべてのトラブルシューティングはcdFMCの脅威対策UI機能を使用して実行できますが、コマンドの使用は制限されます。
- エンドツーエンド接続のために、隣接するデバイスで変更が必要になる場合があります。

原因

根本的な原因は、VPNから内部へのトラフィックと内部からVPNへのプールトラフィックに対するアクセスポリシーとNAT設定が不十分であることでした。デフォルト設定では、VPNプールから内部リソースへの双方向通信および内部リソースへの双方向通信は許可されておらず、同じインターフェイスでのトラフィックの入出力に関するヘアピンNAT要件も処理されていませんでした。

関連コンテンツ

- FTDでのNAT免除の設定
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。