IPsec LAN 間トンネルを介した ASA のクライアントレス SSL VPN トラフィックの設定例

内容

概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス (ASA) クライアントレス SSLVPN ポータルへ接続し、IPSec LAN-to-LAN トンネル経由で接続しているリモート ロケーションに配置されているサーバにアクセスする方法を説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- クライアントレス SSL VPN の設定
- LAN-to-LAN VPN 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 9.2(1) を実行している ASA 5500-X に基づいていますが、すべてのバージョンの ASA にも適用されます。

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

。ライブ ネットワークを変更する前に、コマンドを実行した場合に発生する可能性がある影響を理解しておいてください。

背景説明

クライアントレス SSLVPN セッションからのトラフィックが LAN-to-LAN トンネルを通過するときに、2 つの接続があることに注意してください。

- クライアントから ASA への接続
- ASA から宛先ホストへの接続

ASA から宛先ホストへの接続では、宛先ホストに「最も近い」ASA インターフェイスの IP アドレスが使用されます。したがって、LAN-to-LAN 対象トラフィックには、そのインターフェイス アドレスからリモート ネットワークへのプロキシ アイデンティティが含まれている必要があります。

> **注：** ブックマークにスマート トンネルが使用されている場合でも、宛先に最も近い ASA インターフェイスの IP アドレスが使用されます。

設定

この図では、2 つの ASA の間に LAN-to-LAN トンネルがあり、これによりトラフィックが 192.168.10.x から 192.168.20.x へ移動できます。

このトンネルの対象トラフィックを決定するアクセス リストを次に示します。

ASA1

```
access-list l2l-list extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0
```

ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
```

クライアントレス SSLVPN ユーザが 192.168.20.x ネットワーク上のホストと通信しようとすると、ASA1 はそのトラフィックの送信元のアドレスとして 209.165.200.225 を使用します。LAN-to-LAN アクセス コントロール リスト（ACL）には 209.168.200.225 がプロキシ アイデンティティとして含まれていないため、トラフィックは LAN-to-LAN トンネル経由で送信されません。

LAN-to-LAN トンネル経由でトラフィックを送信するには、新しいアクセス コントロール エントリ（ACE）を対象トラフィック ACL に追加する必要があります。

ASA1

```
access-list l2l-list extended permit ip host 209.165.200.225 192.168.20.0
255.255.255.0
```

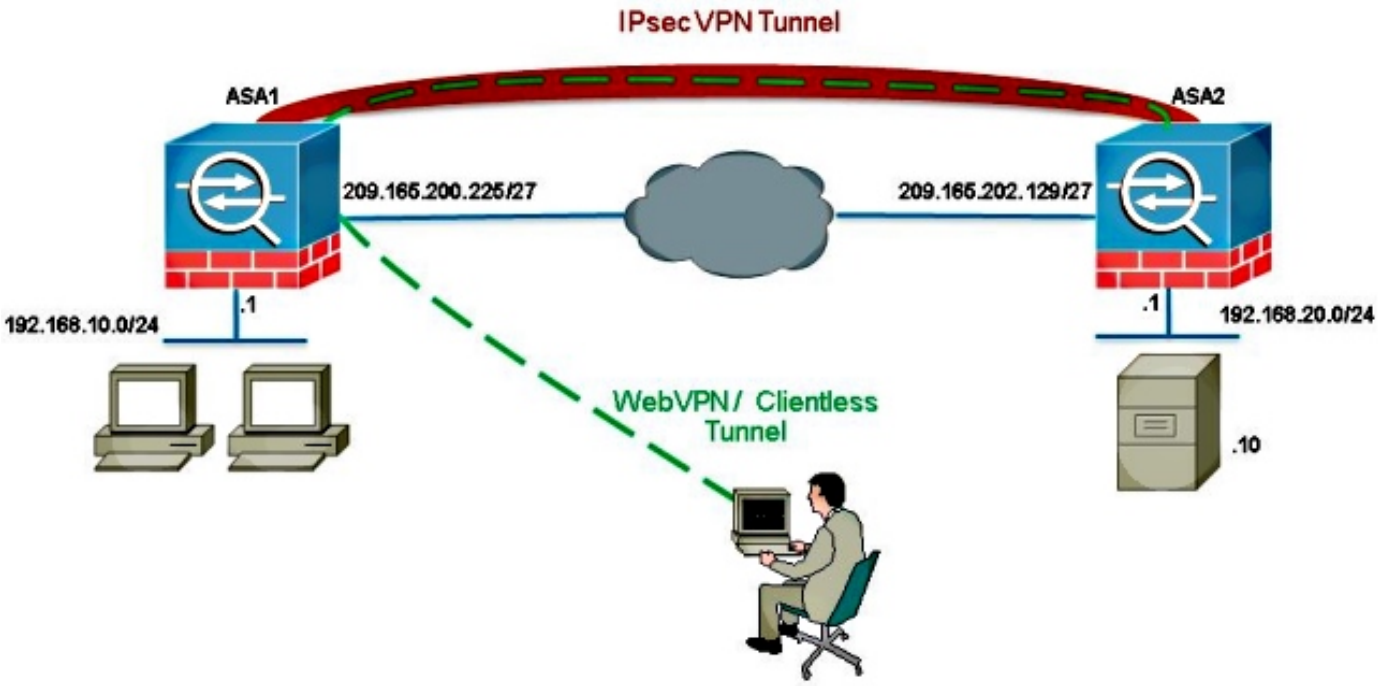
ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 host
209.165.200.225
```

この原則は、クライアントレス SSLVPN トラフィックが、LAN-to-LAN トンネルを通過することが想定されていない場合でも、送出元と同じインターフェイスに **U ターンして戻る必要がある設定に適用されます。**

> **注**：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図



通常、ASA2 はインターネット アクセスを提供するため、192.168.20.0/24 に対するポート アドレス変換（PAT）を実行します。この場合、ASA 2上の192.168.20.0/24からのトラフィックが209.165.200.225に向かう際にPATプロセスから除外されます。除外しない場合、応答はLAN-to-LANトンネルを経由しません。以下に、いくつかの例を示します。

ASA2

```
nat (inside,outside) source static obj-192.168.20.0 obj-
192.168.20.0 destination
static obj-209.165.200.225 obj-209.165.200.225
!
object network obj-192.168.20.0
nat (inside,outside) dynamic interface
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

- **show crypto ipsec sa：このコマンドを使用して、ASA1 プロキシの IP アドレスとリモート ネットワーク間のセキュリティ アソシエーション（SA）が作成されたことを検証します。**クライアントレス SSLVPN ユーザがそのサーバにアクセスすると暗号化カウンタおよび復号カウンタが増加するかどうかを確認します。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

セキュリティ アソシエーションが確立されていない場合は、障害の原因に対して IPSec デバッグを使用できます。

- **debug crypto ipsec <level>**

  注：debug コマンドを使用する前に、「デバッグ コマンドの重要な情報」を参照してください。