ASA 5500 でのリモート VPN クライアント ロード バランシングの設定例

内容

概要

ロード バランシングとは、ユーザが介入することなく、複数の Adaptive Security Appliance (ASA; 適応型セキュリティ アプライアンス) の間で Cisco VPN Client が共有される機能です。ロード バランシングを使用すると、ユーザにとってパブリック IP アドレスの可用性が向上します。たとえば、パブリック IP アドレスを提供する Cisco ASA で障害が発生した場合は、クラスタ内の別の ASA がそのパブリック IP アドレスを引き継ぎます。

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。

- ASA に IP アドレスが割り当てられていて、デフォルト ゲートウェイが設定されている。
- VPN Client ユーザ用の ASA に IPSec が設定されている。
- VPN ユーザは、個別に割り当てられたパブリック IP アドレスを使用してすべての ASA に接続できる。

適格なクライアント

ロード バランシングは、次のクライアントで開始されるリモート セッションでのみ有効です。

- Cisco VPN Client（リリース 3.0 以降）
- Cisco VPN 3002 Hardware Client（リリース 3.5 以降）
- CiscoASA 5505（Easy VPN クライアントとして動作している場合）

その他すべてのクライアント（LAN-to-LAN 接続を含む）は、ロード バランシングがイネーブルになっているセキュリティ アプライアンスに接続できますが、ロード バランシングには参加できません。

使用するコンポーネント

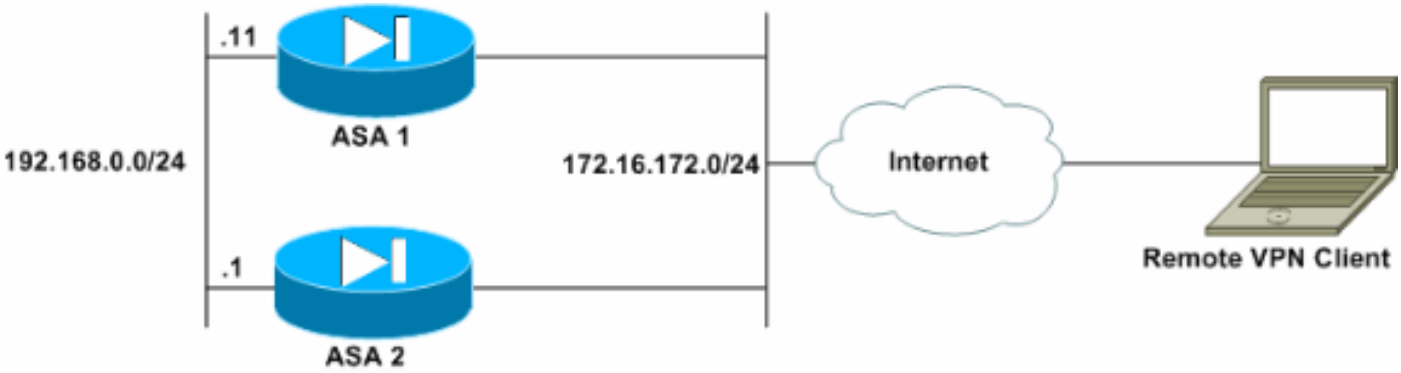
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- VPN Client ソフトウェア リリース 4.6 以降
- Cisco ASA ソフトウェア リリース 7.0.1 以降**注**：8.0(2)バージョンのSecurity Plusライセンスを持つ5520以降のASA 5510およびASAモデルに対して、ロードバランシングのサポートを拡張します。

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。

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 セットアップを使用します。



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。

制約事項

- VPN 仮想クラスタ IP アドレス、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート、および共有シークレットは、仮想クラスタ内のすべてのデバイスでまったく同じである必要があります。

- 仮想クラスタ内のすべてのデバイスは、同じ Outside および Inside の IP サブネットに属している必要があります。

コンフィギュレーション

IP アドレスの割り当て

Outside インターフェイスと Inside インターフェイスに IP アドレスが設定されていること、および ASA からインターネットに到達できることを確認します。

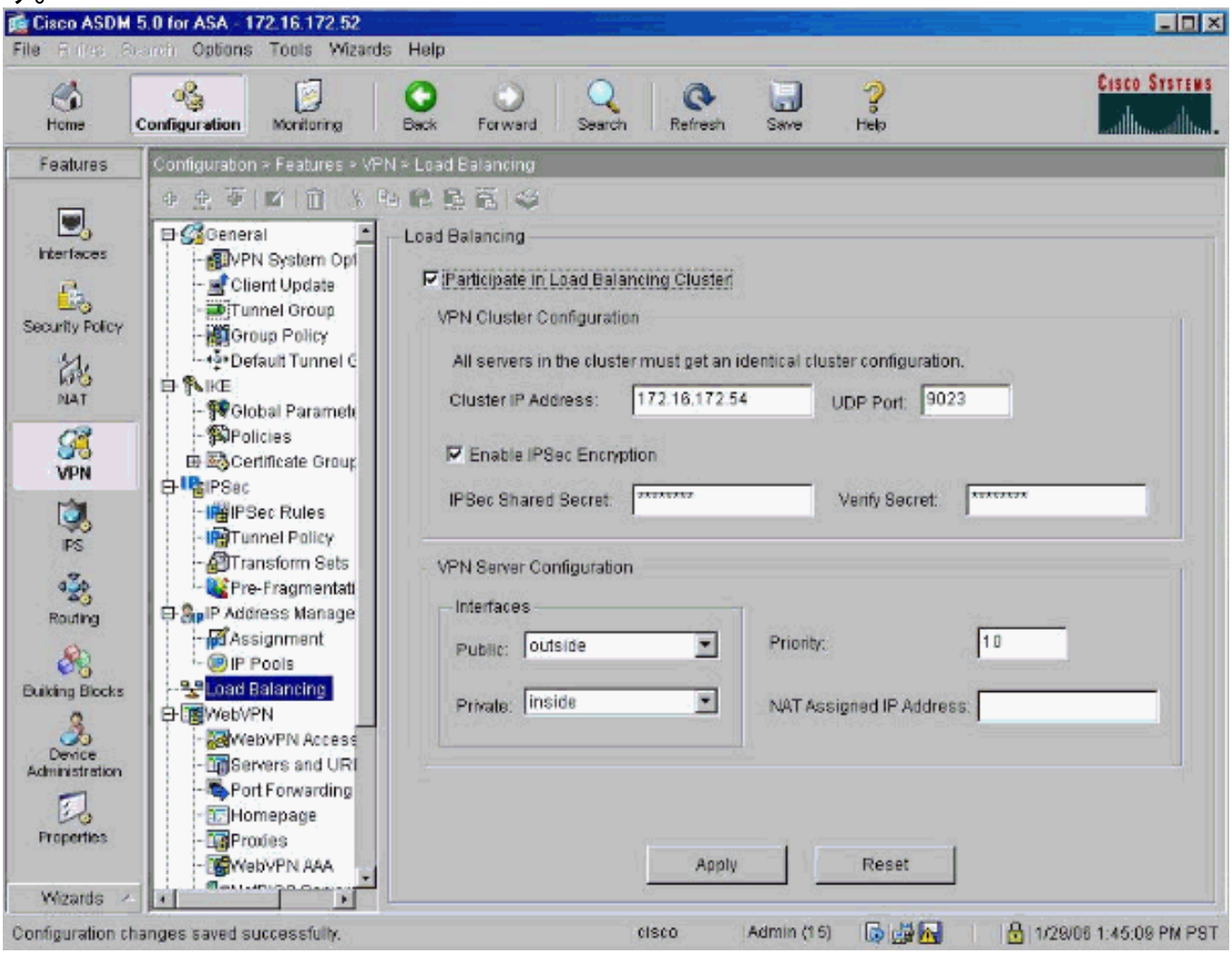
注：内部インターフェイスと外部インターフェイスの両方でISAKMPが有効になっていることを確認します。これを確認するには、**Configuration > Features > VPN > IKE > Global Parameters** の順に選択します。

クラスタの設定

この手順では、Cisco Adaptive Security Device Manager（ASDM）を使用してロード バランシングを設定する方法について説明しています。

注：この例のパラメータの多くはデフォルト値です。

1. **Configuration > Features > VPN > Load Balancing** の順に選択し、**Participate in Load Balancing Cluster** にチェックマークを付けて VPN ロード バランシングをイネーブルにします。



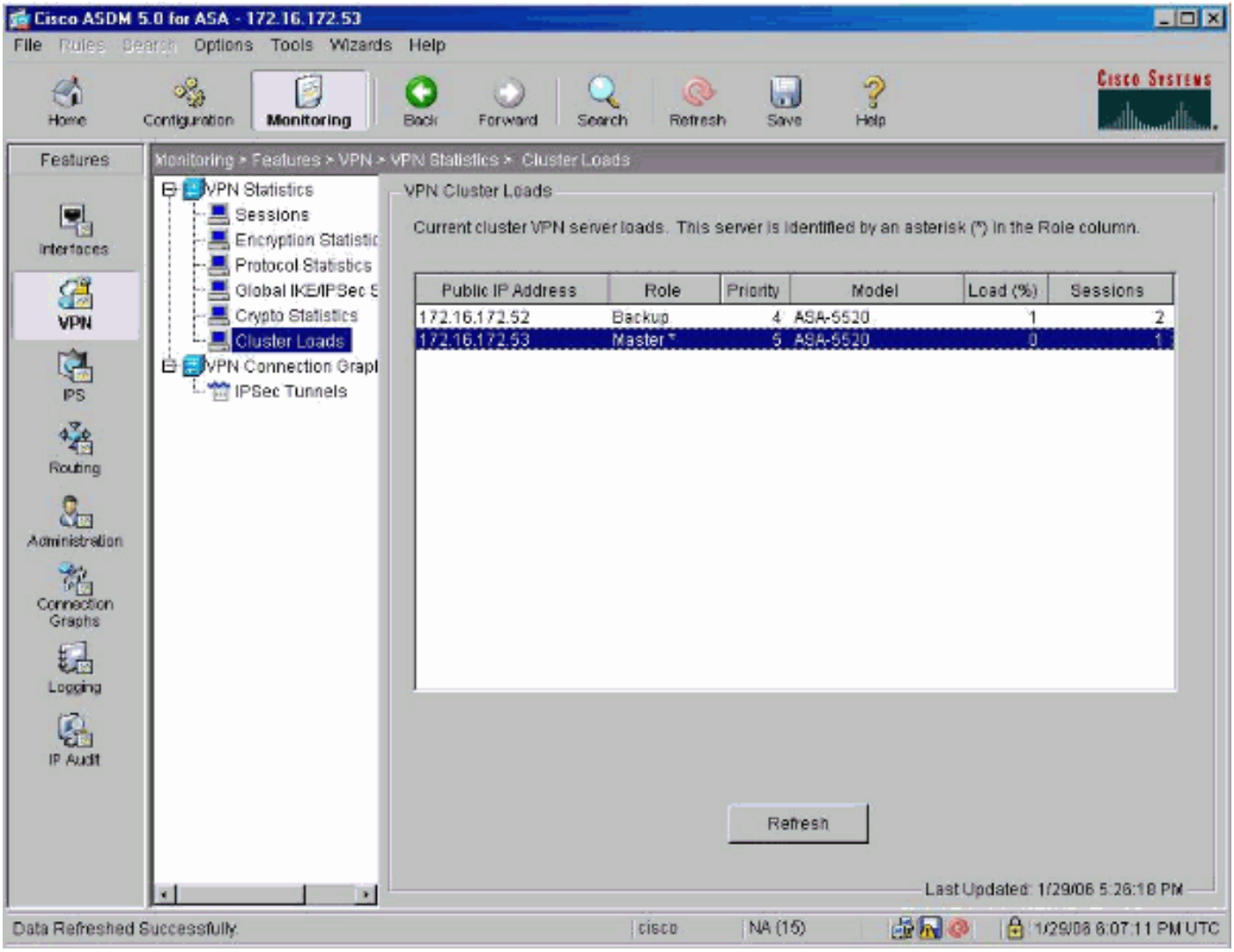
2. VPN Cluster Configuration グループ ボックスで次の手順を実行して、クラスタに参加しているすべての ASA のパラメータを設定します。Cluster IP Address テキスト ボックスにクラスタの IP アドレスを入力します。**Enable IPSec Encryption** にチェックマークを付けます。IPSec Shared Secret テキスト ボックスに暗号化鍵を入力し、Verify Secret テキストボックスに暗号化鍵を再入力します。
3. VPN Server Configuration グループ ボックスで次のオプションを設定します。Public リストで、着信 VPN 接続を受け入れるインターフェイスを選択します。Private リストで、プライベート インターフェイスとして使用するインターフェイスを選択します。（*オプション*）Priority テキスト ボックスで、クラスタ内での ASA の優先順位を変更します。NAT を使用するファイアウォールの背後にこのデバイスが配置されている場合は、Network Address Translation（NAT）Assigned IP Address に IP アドレスを入力します。
4. グループに参加しているすべての ASA で、上記の手順を繰り返します。

このセクションの例では、次の CLI コマンドを使用してロード バランシングを設定します。

```
VPN-ASA2(config)#vpn load-balancing
VPN-ASA2(config-load-balancing)#priority 10
VPN-ASA2(config-load-balancing)#cluster key cisco123
VPN-ASA2(config-load-balancing)#cluster ip address 172.16.172.54
VPN-ASA2(config-load-balancing)#cluster encryption
VPN-ASA2(config-load-balancing)#participate
```

モニタリング

ASA でロード バランシング機能を監視するには、**Monitoring > Features > VPN > VPN Statistics > Cluster Loads** の順に選択します。



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）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show vpn load-balancing**：VPN ロード バランシング機能を確認します。

```
Status: enabled
Role: Backup
Failover: n/a
Encryption: enabled
Cluster IP: 172.16.172.54
Peers: 1

Public IP Role Pri Model Load (%) Sessions
-----------------------------------------------------------
* 172.16.172.53 Backup 5 ASA-5520 0 1
172.16.172.52 Master 4 ASA-5520 n/a n/a
```

トラブルシュート

このセクションは、設定のトラブルシューティングを行う際に参照してください。

トラブルシューティングのためのコマンド

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

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug vpnlb 250**：VPN ロード バランシング機能のトラブルシューティングに使用します。

```
VPN-ASA2#
VPN-ASA2# 5718045: Created peer[172.16.172.54]
5718012: Sent HELLO request to [172.16.172.54]
5718016: Received HELLO response from [172.16.172.54]
7718046: Create group policy [vpnlb-grp-pol]
7718049: Created secure tunnel to peer[192.168.0.11]
5718073: Becoming slave of Load Balancing in context 0.
5718018: Send KEEPALIVE request failure to [192.168.0.11]
5718018: Send KEEPALIVE request failure to [192.168.0.11]
5718018: Send KEEPALIVE request failure to [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718035: Received TOPOLOGY indicator from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
```

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
- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX 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