Remote-VPN-Client-Lastenausgleich auf ASA 5500 - Konfigurationsbeispiel

Inhalt

Einführung

Beim Lastenausgleich können Cisco VPN-Clients ohne Benutzereingriff auf mehrere Adaptive Security Appliance (ASA)-Einheiten verteilt werden. Durch Lastenausgleich wird sichergestellt, dass die öffentliche IP-Adresse für Benutzer hochverfügbar ist. Wenn beispielsweise die Cisco ASA, die die öffentliche IP-Adresse bereitstellt, ausfällt, übernimmt eine andere ASA im Cluster die öffentliche IP-Adresse.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Sie haben auf Ihren ASAs IP-Adressen zugewiesen und das Standard-Gateway konfiguriert.
- IPsec wird auf den ASAs für die VPN-Client-Benutzer konfiguriert.
- VPN-Benutzer können mithilfe ihrer individuell zugewiesenen öffentlichen IP-Adresse eine Verbindung zu allen ASAs herstellen.

Qualifizierte Kunden

Der Lastenausgleich ist nur bei Remote-Sitzungen wirksam, die mit diesen Clients initiiert wurden:

- Cisco VPN Client (Version 3.0 oder höher)
- Cisco VPN 3002 Hardware Client (Version 3.5 oder höher)
- Cisco ASA 5505 als Easy VPN-Client

Alle anderen Clients, einschließlich LAN-zu-LAN-Verbindungen, können eine Verbindung zu einer Sicherheits-Appliance herstellen, auf der der Lastenausgleich aktiviert ist, sie können jedoch nicht am Lastenausgleich teilnehmen.

Verwendete Komponenten

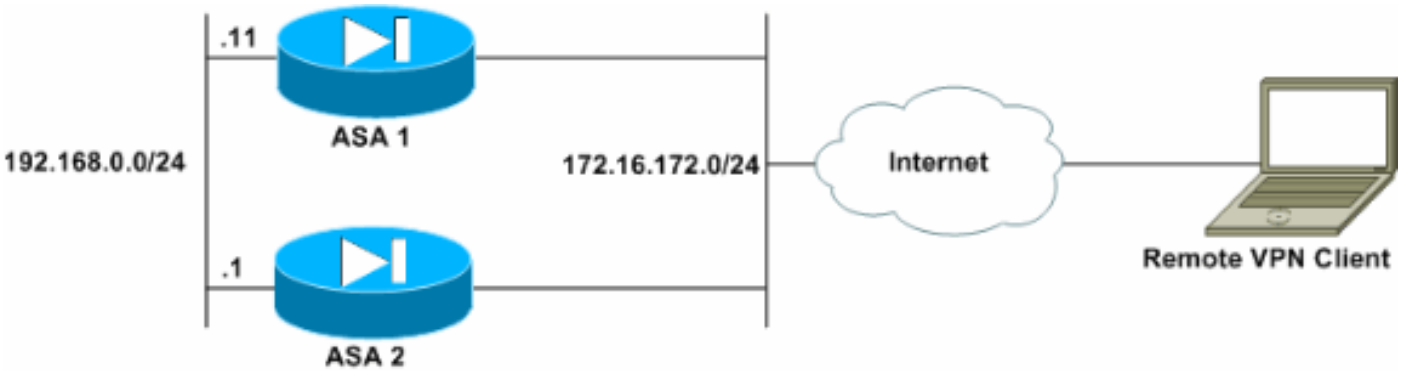
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- VPN Client Software Version 4.6 und höher
- Cisco ASA Software Release 7.0.1 und höher**Hinweis:** Erweitert die Load Balancing-Unterstützung auf ASA 5510- und ASA-Modelle später als 5520, die über eine Security Plus-Lizenz mit der Version 8.0(2) verfügen.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Einschränkungen

- Die IP-Adresse des virtuellen VPN-Clusters, der UDP-Port (User Datagram Protocol) und der gemeinsam verwendete geheime Schlüssel müssen auf jedem Gerät im virtuellen Cluster

identisch sein.
- Alle Geräte im virtuellen Cluster müssen sich in denselben externen und internen IP-Subnetzen befinden.

Konfiguration

IP-Adressenzuweisung

Stellen Sie sicher, dass die IP-Adressen auf der Außen- und der Innenschnittstelle konfiguriert sind, und Sie können von Ihrer ASA aus auf das Internet zugreifen.

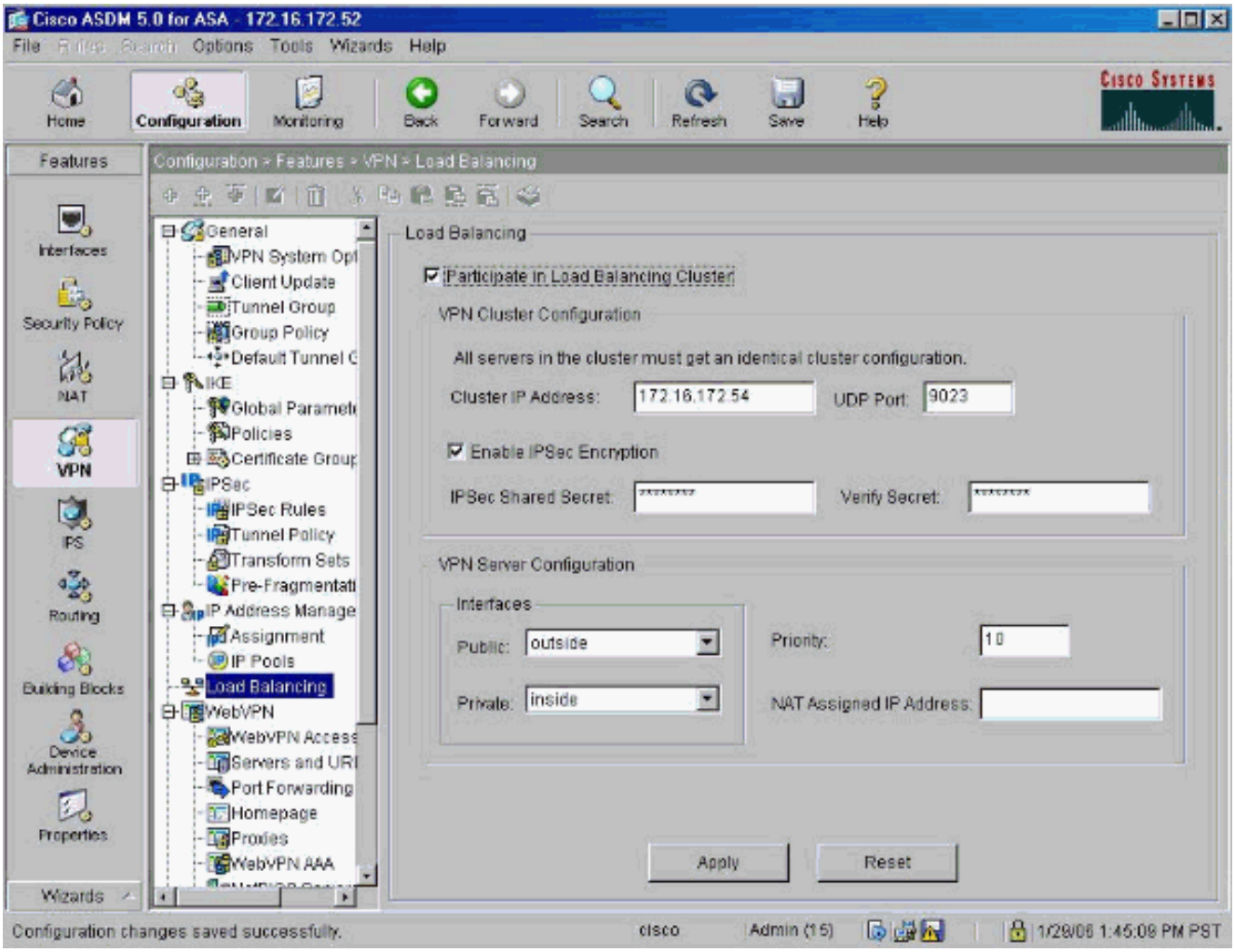
Hinweis: Stellen Sie sicher, dass ISAKMP sowohl für die interne als auch für die externe Schnittstelle aktiviert ist. Wählen Sie **Konfiguration > Funktionen > VPN > IKE > Globale Parameter**, um dies zu überprüfen.

Clusterkonfiguration

Dieses Verfahren zeigt, wie Sie mit dem Cisco Adaptive Security Device Manager (ASDM) Load Balancing konfigurieren.

Hinweis: Viele der Parameter in diesem Beispiel haben Standardwerte.

1. Wählen Sie **Configuration > Features > VPN > Load Balancing aus**, und aktivieren Sie **Participate in Load Balancing Cluster (Am Load Balancing-Cluster teilnehmen)**, um den VPN-Lastenausgleich zu
aktivieren.



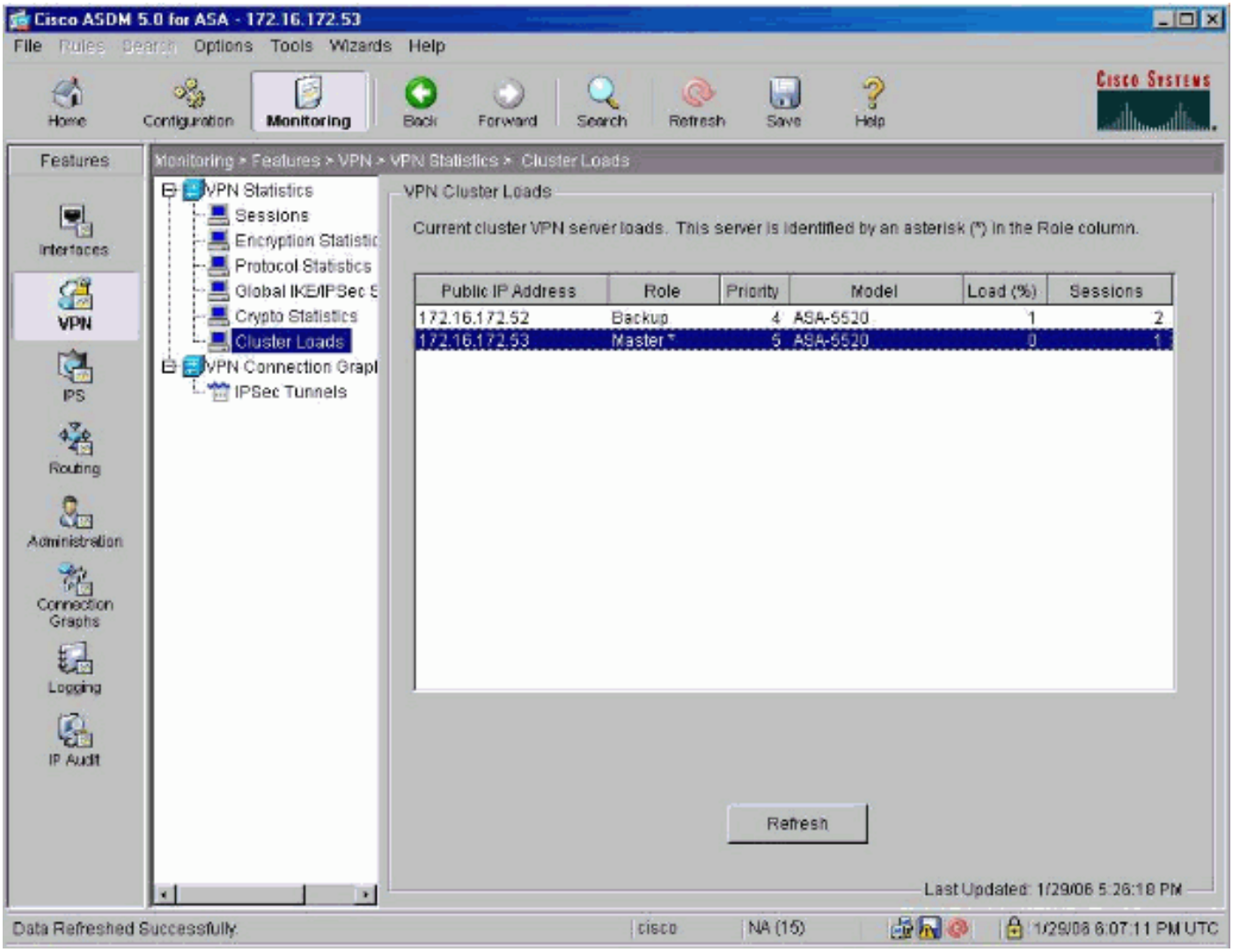
2. Gehen Sie wie folgt vor, um die Parameter für alle ASAs zu konfigurieren, die im Feld "VPN-Cluster-Konfiguration" am Cluster teilnehmen:Geben Sie die IP-Adresse des Clusters in das Textfeld IP-Adresse des Clusters ein.Klicken Sie auf **IPSec Encryption aktivieren**.Geben Sie den Verschlüsselungsschlüssel in das Textfeld IPSec Shared Secret ein, und geben Sie ihn erneut in das Textfeld Verify Secret ein.
3. Konfigurieren Sie die Optionen im Feld "VPN Server Configuration" (Konfiguration des VPN-Servers):Wählen Sie eine Schnittstelle aus, die die eingehenden VPN-Verbindungen in der öffentlichen Liste akzeptiert.Wählen Sie in der Liste Privat eine Schnittstelle aus, die die private Schnittstelle ist.(*Optional*) Ändern Sie die Priorität, die die ASA im Cluster im Textfeld "Priorität" hat.Geben Sie eine IP-Adresse für die Network Address Translation (NAT) Assigned IP Address (Zugewiesene IP-Adresse) ein, wenn sich dieses Gerät hinter einer Firewall befindet, die NAT verwendet.
4. Wiederholen Sie die Schritte für alle teilnehmenden ASAs in der Gruppe.

Im Beispiel in diesem Abschnitt werden die folgenden CLI-Befehle zum Konfigurieren des Load Balancing verwendet:

```
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
```

Überwachung

Wählen Sie **Monitoring > Features > VPN > VPN Statistics > Cluster Loads** aus, um die Lastverteilungsfunktion auf der ASA zu überwachen.



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show vpn load-balancing** - Überprüft die VPN Load Balancing-Funktion.

```
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
```

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug vpnlb 250** - Dient zur Fehlerbehebung bei der VPN-Lastenausgleichsfunktion.

```
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]
```

Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems