Remote VPN-clienttaakverdeling voor ASA 5500-configuratievoorbeeld

Inhoud

Inleiding

Taakverdeling is de mogelijkheid om Cisco VPN-clients te delen via meerdere adaptieve security applicatie (ASA)-eenheden zonder tussenkomst van de gebruiker. Taakverdeling zorgt ervoor dat het openbare IP-adres in hoge mate beschikbaar is voor gebruikers. Als Cisco ASA bijvoorbeeld dat het openbare IP-adres mislukt, neemt een andere ASA in de cluster bijvoorbeeld het openbare IP-adres aan.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- U hebt IP-adressen op uw ASA's toegewezen en de standaardgateway ingesteld.
- IPsec is ingesteld op ASA’s voor de VPN-clientgebruikers.
- VPN-gebruikers kunnen met alle ASA’s verbinding maken met het gebruik van hun individueel toegewezen openbare IP-adres.

In aanmerking komende clients

De taakverdeling is alleen effectief op afstandssessies die met deze klanten worden geïnitieerd:

- Cisco VPN-client (release 3.0 of hoger)
- Cisco VPN 3002 hardwareclient (release 3.5 of hoger)
- Cisco ASA 5505 wanneer ingesloten in een eenvoudige VPN-client

Alle andere klanten, inclusief LAN-to-LAN verbindingen, kunnen verbinding maken met een security apparaat waarop de taakverdeling is ingeschakeld, maar zij kunnen niet deelnemen aan de taakverdeling.

Gebruikte componenten

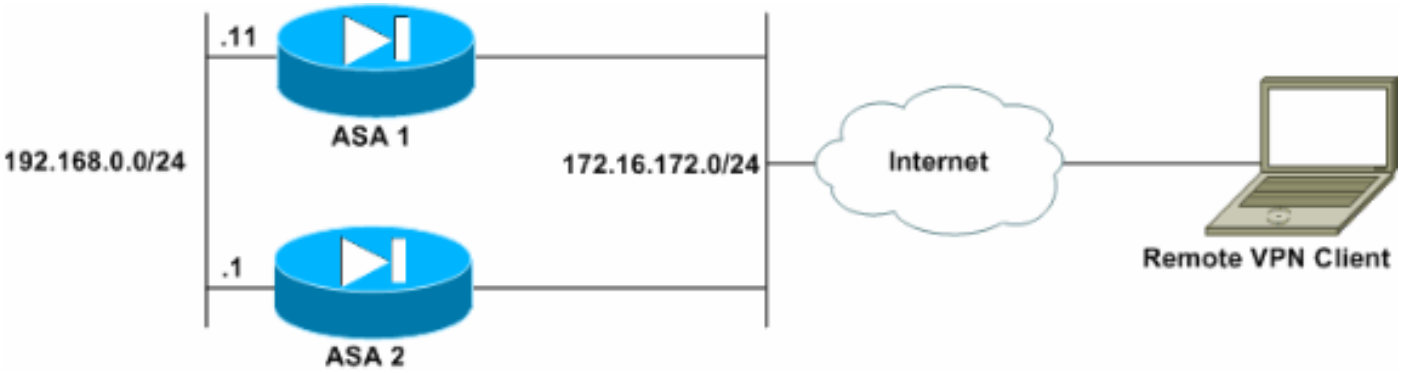
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- VPN-clientsoftwarereleases 4.6 en hoger
- Cisco ASA-softwarereleases 7.0.1 en hogerOpmerking: Uitbreidt de ondersteuning voor taakverdeling voor ASA 5510 en ASA-modellen later dan 5520 die een Security Plus-licentie hebben met de versie 8.0(2).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Beperkingen

- VPN virtueel cluster IP-adres, User Datagram Protocol (UDP)-poort en gedeeld geheim moeten op elk apparaat in de virtuele cluster identiek zijn.
- Alle apparaten in het virtuele cluster moeten aan dezelfde buitenkant en binnen IP-subnetten zijn.

Configuratie

IP-adrestoewijzing

Zorg ervoor dat de IP adressen op de buitenkant en binneninterfaces worden gevormd en u kunt van uw ASA naar het Internet krijgen.

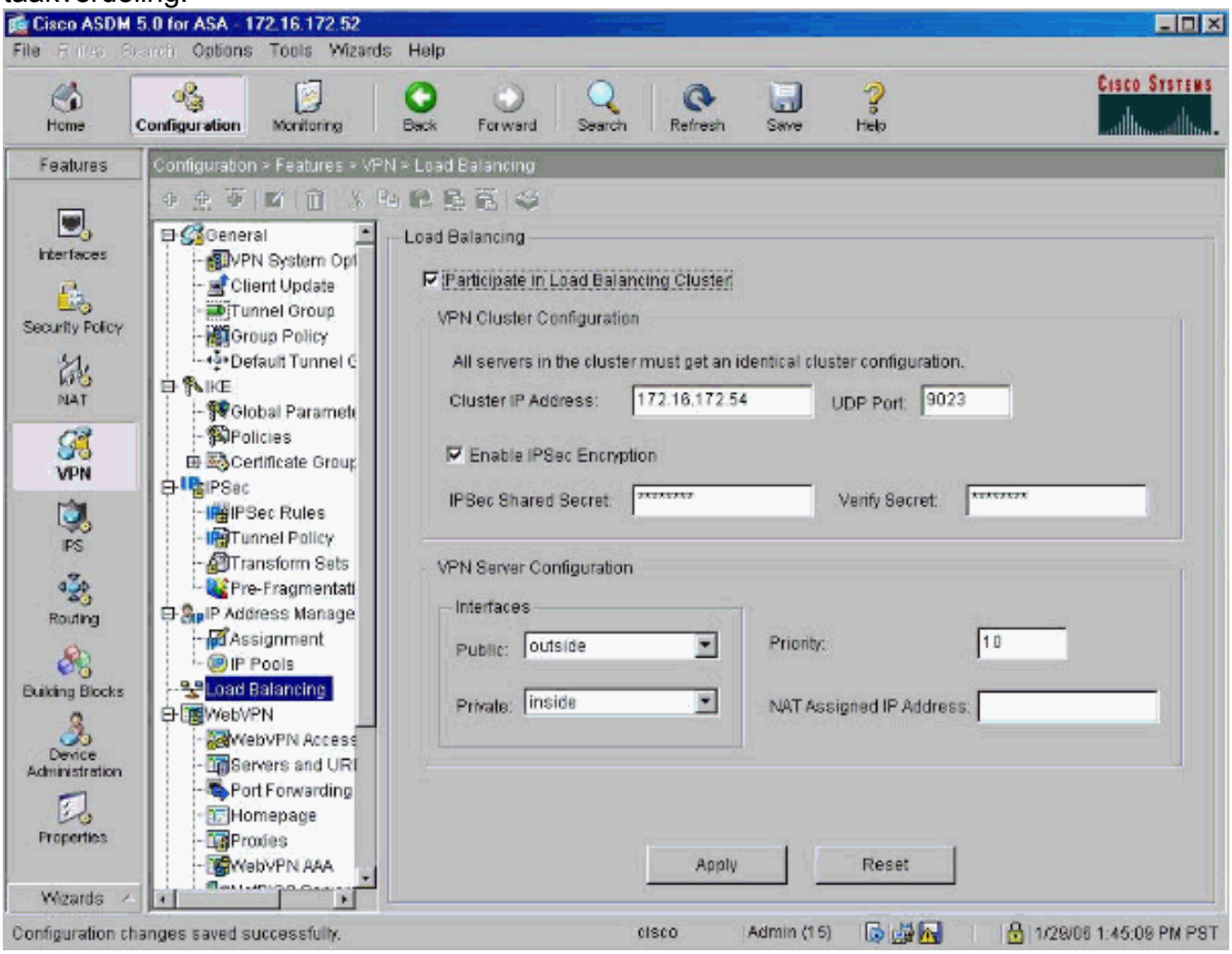
Opmerking: Zorg ervoor dat ISAKMP zowel op de binnen- als buitenkant is ingeschakeld. Selecteer **Configuratie > Functies > VPN > IKE > Mondiale parameters** om dit te verifiëren.

Cluster configuratie

Deze procedure toont hoe u de Cisco Adaptieve Security Devices Manager (ASDM) kunt gebruiken om het taakverdeling te configureren.

Opmerking: Veel parameters in dit voorbeeld hebben standaardwaarden.

1. Selecteer **Configuratie > Functies > VPN > Taakverdeling** en controleer **Deelnemen aan taakverdeling in** VPN-taakverdeling.



2. Voltooi deze stappen om de parameters te configureren voor alle ASA's die deelnemen aan het cluster in het vak VPN Cluster Configuration:Typ het IP-adres van de cluster in het tekstvak Cluster IP-adres.Klik op **IPsec-encryptie inschakelen**.Typ de coderingstoets in het IPSec Shared Security tekstvak en type de applicatie opnieuw in het dialoogvenster

Beveiligde tekst controleren.

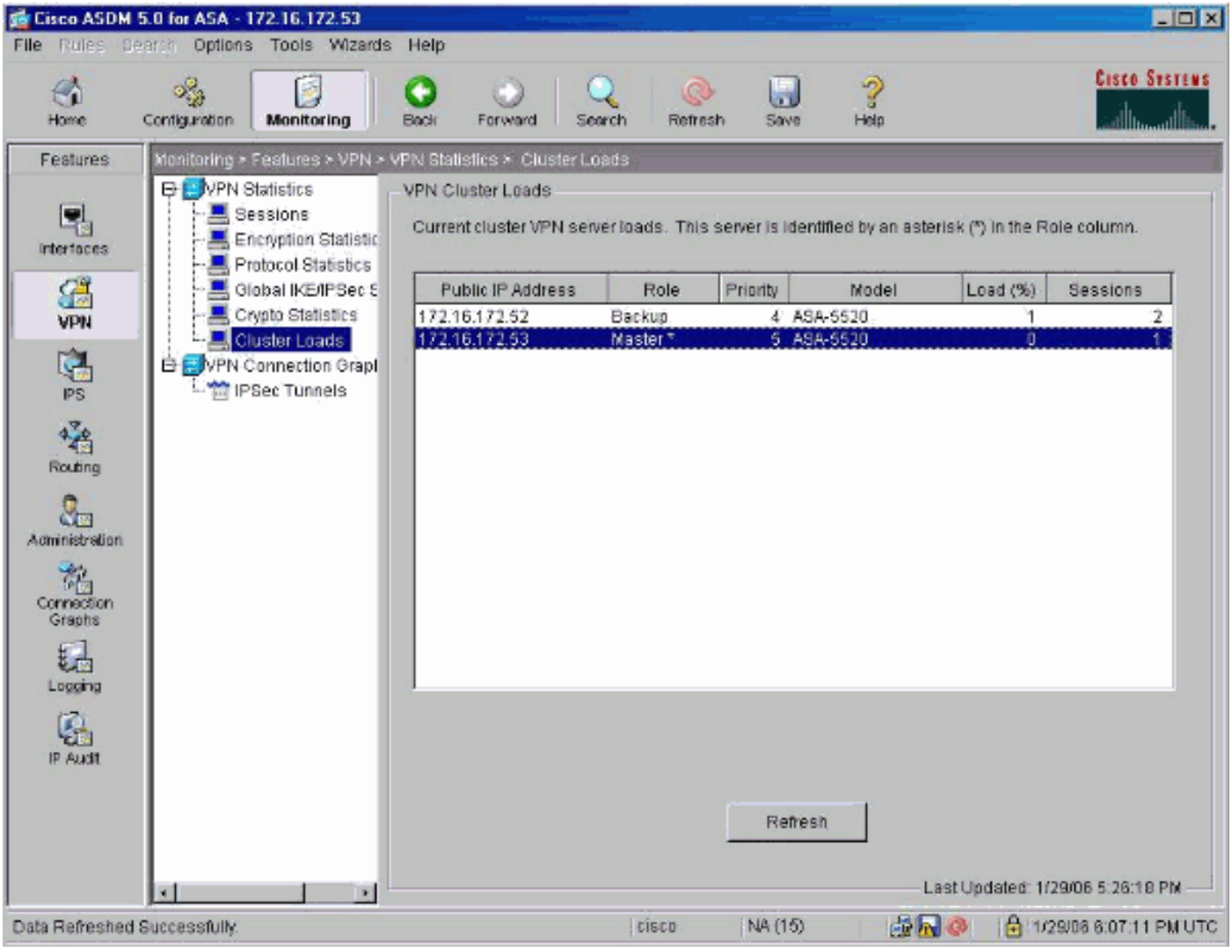
3. Configuratie van de opties in het vak VPN-serverconfiguratie:Selecteer een interface die de inkomende VPN-verbindingen in de openbare lijst accepteert.Selecteer een interface die de particuliere interface in de privélijst is.(*Optioneel*) Wijzig de prioriteit van de ASA in het cluster in het vak Prioritaire tekst.Typ een IP-adres voor het NAT-adres (Network Address Translation) als dit apparaat achter een firewall zit die NAT gebruikt.
4. Herhaal de stappen voor alle deelnemende ASA's in de groep.

Het voorbeeld in deze sectie gebruikt deze CLI-opdrachten om het taakverdeling in te stellen:

```
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
```

Controleren

Selecteer **Controle > Functies > VPN > VPN Statistieken > Cluster Loads** om de taakverdeling op de ASA te controleren.



Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **Toon VPN lading-in-**evenwicht—Verifieert de functie voor het taakverdeling van VPN.

```
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
```

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

Opdrachten voor troubleshooting

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug vpnlb 250**: voor problemen oplossen bij de taakverdeling van VPN.

```
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]
```

Gerelateerde informatie

- Adaptieve security applicaties van Cisco ASA 5500 Series
- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems