Esempio di configurazione di ASA 5500 con bilanciamento del carico dei client VPN remoti

Sommario

Introduzione

Il bilanciamento del carico è la capacità di condividere i client VPN Cisco su più unità ASA (Adaptive Security Appliance) senza l'intervento dell'utente. Il bilanciamento del carico garantisce che l'indirizzo IP pubblico sia a elevata disponibilità per gli utenti. Ad esempio, se l'appliance Cisco ASA che serve l'indirizzo IP pubblico ha esito negativo, un'altra appliance ASA nel cluster assume l'indirizzo IP pubblico.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Gli indirizzi IP sono stati assegnati alle appliance ASA e il gateway predefinito è stato configurato.
- IPsec è configurato sulle appliance ASA per gli utenti VPN Client.
- Gli utenti VPN possono connettersi a tutte le appliance ASA usando l'indirizzo IP pubblico assegnato singolarmente.

Clienti idonei

Il bilanciamento del carico è valido solo per le sessioni remote avviate con questi client:

- Cisco VPN Client (versione 3.0 o successiva)
- Cisco VPN 3002 Hardware Client (versione 3.5 o successiva)
- Cisco ASA 5505 quando funziona come client Easy VPN

Tutti gli altri client, incluse le connessioni LAN a LAN, possono connettersi a un'appliance di sicurezza su cui è abilitato il bilanciamento del carico, ma non possono partecipare al bilanciamento del carico.

Componenti usati

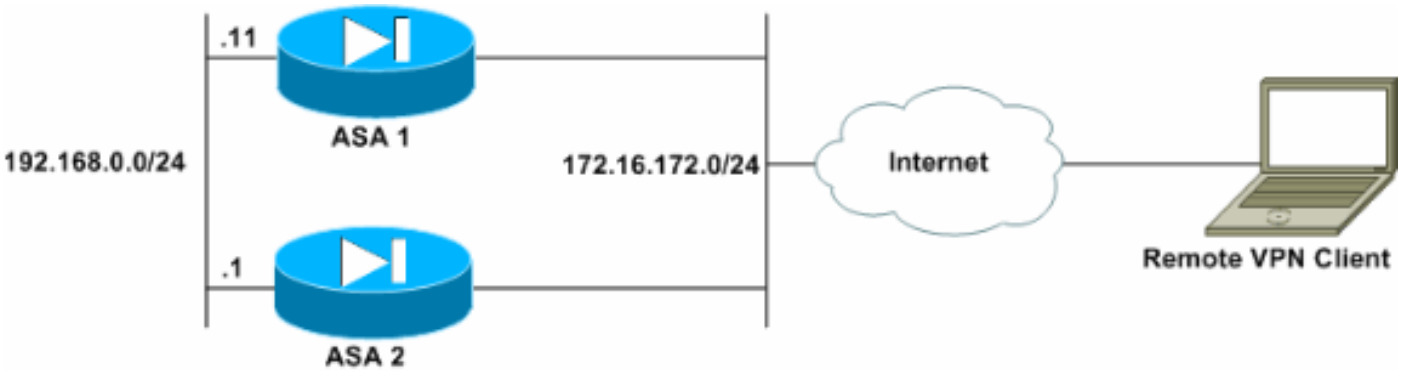
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software VPN Client release 4.6 e successive
- Software Cisco ASA versione 7.0.1 e successive**Nota:** estende il supporto del bilanciamento del carico ai modelli ASA 5510 e ASA successivi alla versione 5520 con licenza Security Plus con versione 8.0(2).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Restrizioni

- L'indirizzo IP del cluster virtuale VPN, la porta UDP (User Datagram Protocol) e il segreto condiviso devono essere identici in tutti i dispositivi del cluster virtuale.

- Tutti i dispositivi nel cluster virtuale devono trovarsi nella stessa subnet IP esterna e interna.

Configurazione

Assegnazione indirizzo IP

Verificare che gli indirizzi IP siano configurati sulle interfacce esterna e interna e che l'appliance ASA sia in grado di accedere a Internet.

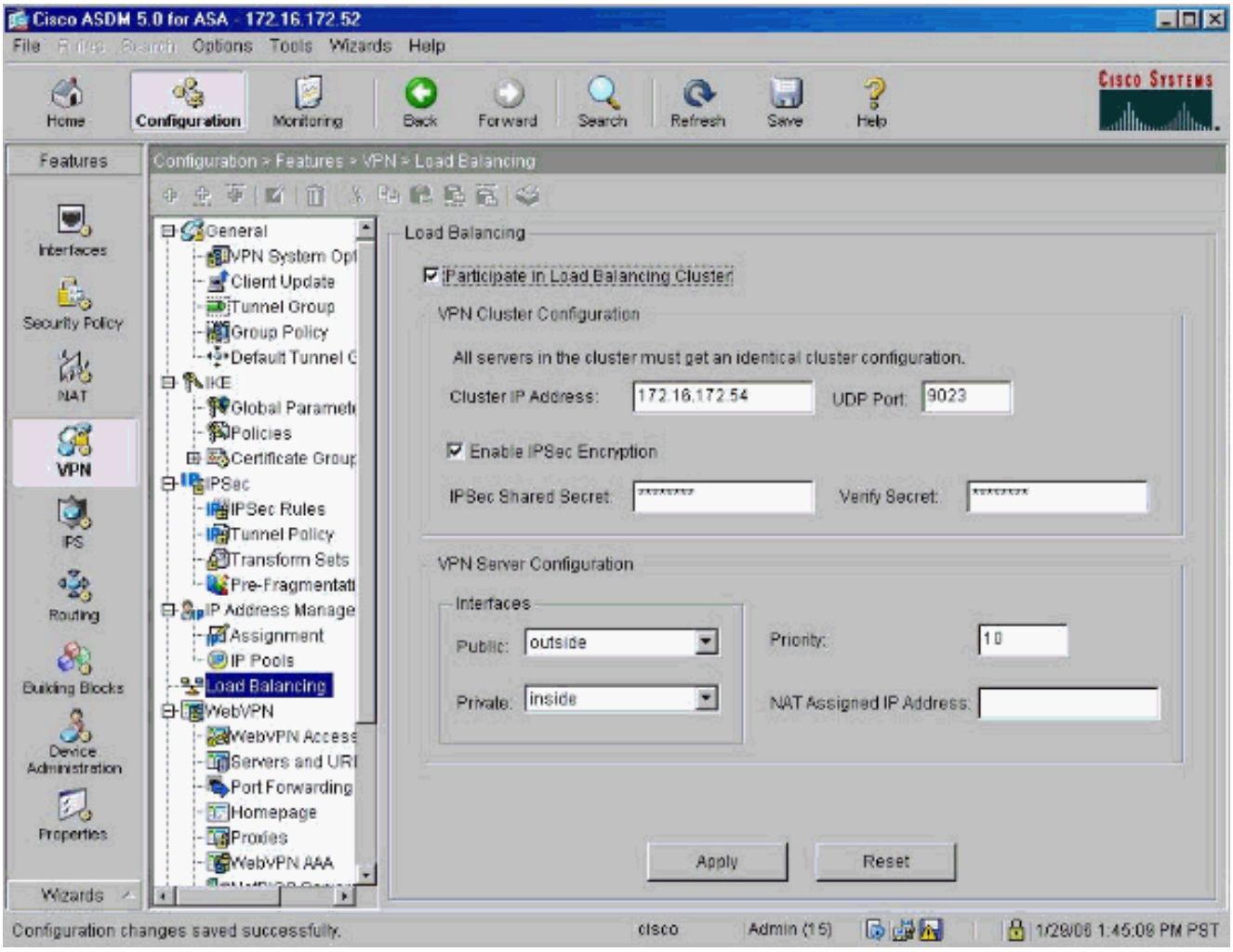
Nota: verificare che ISAKMP sia abilitato sia sull'interfaccia interna sia su quella esterna. Per verificare questa condizione, selezionare **Configurazione > Funzionalità > VPN > IKE > Parametri globali**.

Configurazione cluster

In questa procedura viene mostrato come utilizzare Cisco Adaptive Security Device Manager (ASDM) per configurare il bilanciamento del carico.

Nota: molti dei parametri di questo esempio hanno valori predefiniti.

1. Selezionare **Configurazione > Funzionalità > VPN > Bilanciamento del carico**, quindi selezionare **Partecipa al cluster di bilanciamento del carico** per abilitare il bilanciamento del carico della
VPN.



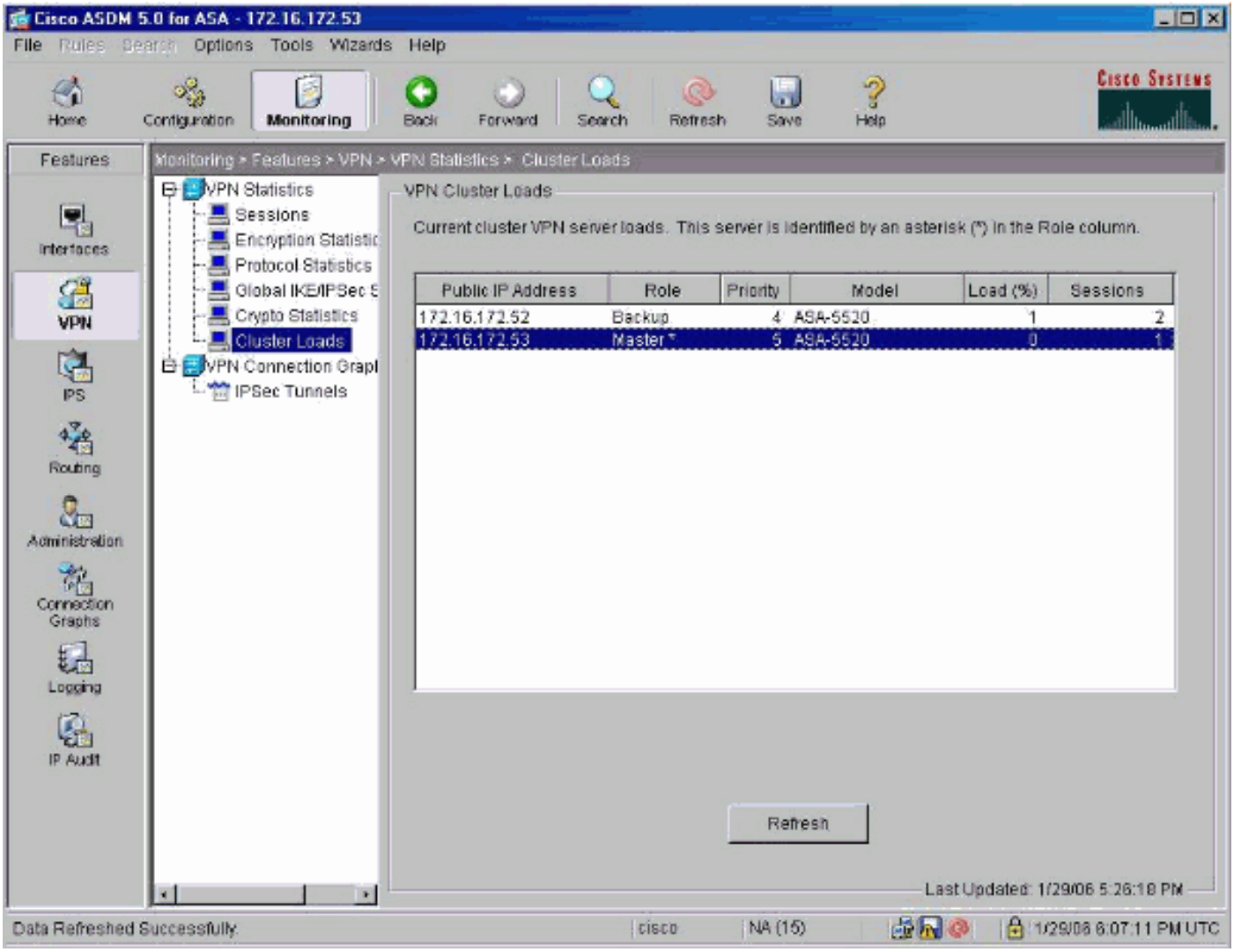
2. Completare la procedura seguente per configurare i parametri di tutte le appliance ASA che partecipano al cluster nella casella di gruppo Configurazione cluster VPN:Digitare l'indirizzo IP del cluster nella casella di testo Indirizzo IP cluster.Fare clic su **Attiva crittografia IPSec**.Digitare la chiave di crittografia nella casella di testo Segreto condiviso IPSec e digitarla nuovamente nella casella di testo Verifica segreto.
3. Configurare le opzioni nella casella di gruppo Configurazione server VPN:Selezionare un'interfaccia che accetti le connessioni VPN in ingresso nell'elenco Pubblico.Selezionare un'interfaccia che corrisponda all'interfaccia privata nell'elenco Private.(*Facoltativo*) Modificare la priorità dell'ASA nel cluster nella casella di testo Priorità.Digitare un indirizzo IP per l'indirizzo IP assegnato NAT (Network Address Translation) se il dispositivo è protetto da un firewall che utilizza NAT.
4. Ripetere i passaggi su tutte le appliance ASA che partecipano al gruppo.

L'esempio in questa sezione utilizza i seguenti comandi CLI per configurare il bilanciamento del carico:

```
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
```

Monitoraggio

Selezionare **Monitoraggio > Funzionalità > VPN > Statistiche VPN > Carichi cluster** per monitorare la funzione di bilanciamento del carico sull'appliance ASA.



Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show vpn load-balancing**: verifica la funzione di bilanciamento del carico 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
```

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug vpnlb 250**: utilizzato per risolvere i problemi relativi alla funzionalità di bilanciamento del carico della 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]
```

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems