ASA 5500 구성의 원격 VPN 클라이언트 로드 밸런싱 예

목차

소개

로드 밸런싱은 Cisco VPN Client가 여러 ASA(Adaptive Security Appliance) 유닛에서 사용자 개입 없이 공유되도록 하는 기능입니다.로드 밸런싱은 사용자가 공용 IP 주소를 항상 사용할 수 있도록 보장합니다.예를 들어 공용 IP 주소를 서비스하는 Cisco ASA가 실패하면 클러스터의 다른 ASA가 공용 IP 주소를 가정합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- ASA에 IP 주소를 할당하고 기본 게이트웨이를 구성했습니다.
- IPsec은 VPN 클라이언트 사용자에 대해 ASA에 구성됩니다.
- VPN 사용자는 개별적으로 할당된 공용 IP 주소를 사용하여 모든 ASA에 연결할 수 있습니다.

적격 클라이언트

로드 밸런싱은 다음 클라이언트에서 시작된 원격 세션에만 적용됩니다.

- Cisco VPN Client(릴리스 3.0 이상)
- Cisco VPN 3002 Hardware Client(릴리스 3.5 이상)
- CiscoASA 5505 - Easy VPN 클라이언트 역할 수행

LAN-to-LAN 연결을 비롯한 다른 모든 클라이언트는 로드 밸런싱이 활성화된 보안 어플라이언스에 연결할 수 있지만 로드 밸런싱에는 참여할 수 없습니다.

사용되는 구성 요소

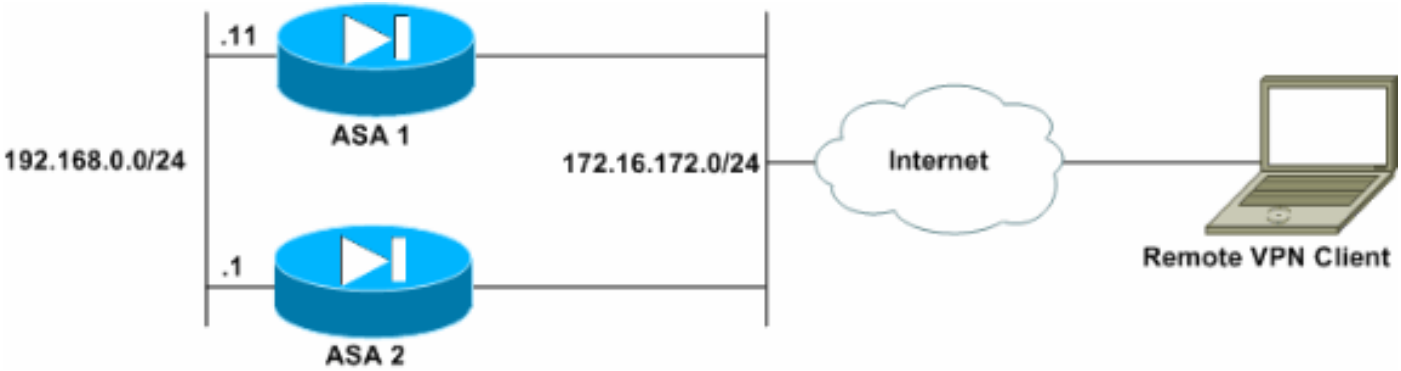
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- VPN Client Software 릴리스 4.6 이상
- Cisco ASA 소프트웨어 릴리스 7.0.1 이상**참고:** 로드 밸런싱 지원을 8.0(2) 버전의 Security Plus 라이센스가 있는 5520 이상 ASA 5510 및 ASA 모델로 확장합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

제한 사항

- VPN 가상 클러스터 IP 주소, UDP(User Datagram Protocol) 포트 및 공유 암호는 가상 클러스터의 모든 디바이스에서 동일해야 합니다.
- 가상 클러스터의 모든 디바이스는 동일한 외부 및 내부 IP 서브넷에 있어야 합니다.

구성

IP 주소 할당

IP 주소가 외부 및 내부 인터페이스에 구성되어 있고 ASA에서 인터넷에 액세스할 수 있는지 확인합니다.

참고: 내부 및 외부 인터페이스에서 ISAKMP가 활성화되어 있는지 확인합니다.이를 확인하려면 **Configuration > Features > VPN > IKE > Global Parameters**를 선택합니다.

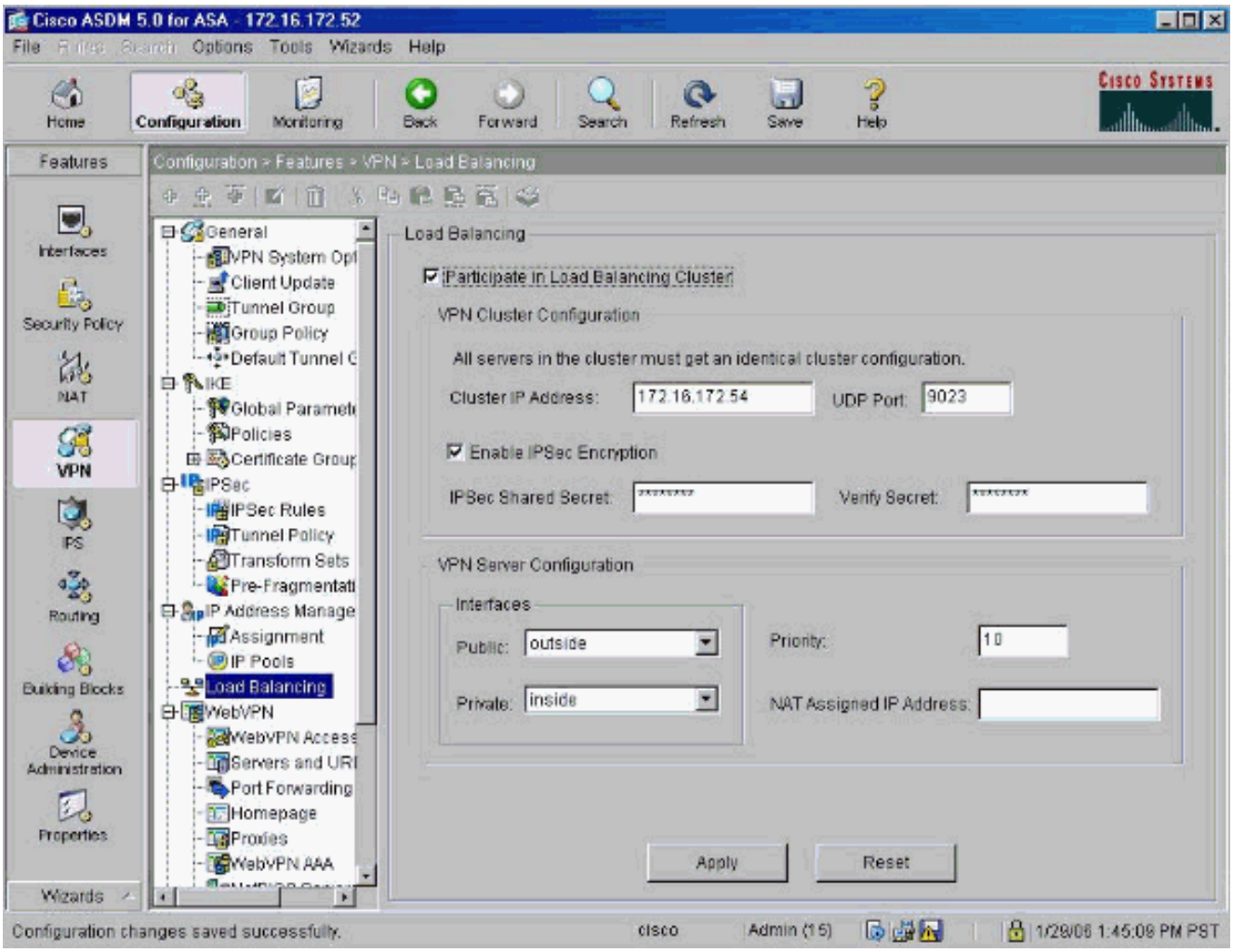
클러스터 구성

이 절차에서는 Cisco ASDM(Adaptive Security Device Manager)을 사용하여 로드 밸런싱을 구성하는 방법을 보여줍니다.

참고: 이 예의 많은 매개변수에는 기본값이 있습니다.

1. Configuration **> Features > VPN > Load Balancing을 선택하고 Participate in Load Balancing Cluster를** 선택하여 VPN 로드 밸런싱을 활성화합니다

.



2. VPN Cluster Configuration(VPN 클러스터 컨피그레이션) 그룹 상자에서 클러스터에 참여하는 모든 ASA에 대한 매개변수를 구성하려면 다음 단계를 완료합니다.Cluster IP Address(클러스터 IP 주소) 텍스트 상자에 클러스터의 IP 주소를 입력합니다.Enable **IPSec Encryption을 클릭합니다**.IPSec 공유 암호 텍스트 상자에 암호화 키를 입력하고 암호 확인 텍스트 상자에 다시 입력합니다.
3. VPN Server Configuration(VPN 서버 컨피그레이션) 그룹 상자에서 옵션을 구성합니다 .Public(공개) 목록에서 수신 VPN 연결을 수락하는 인터페이스를 선택합니다.Private(비공개) 목록에서 전용 인터페이스인 인터페이스를 선택합니다.(*선택* 사항) Priority(우선순위) 텍스트 상자에서 ASA가 클러스터에 가지는 우선순위를 변경합니다.이 디바이스가 NAT를 사용하는

방화벽 뒤에 있는 경우 NAT(Network Address Translation) Assigned IP Address의 IP 주소를 입력합니다.

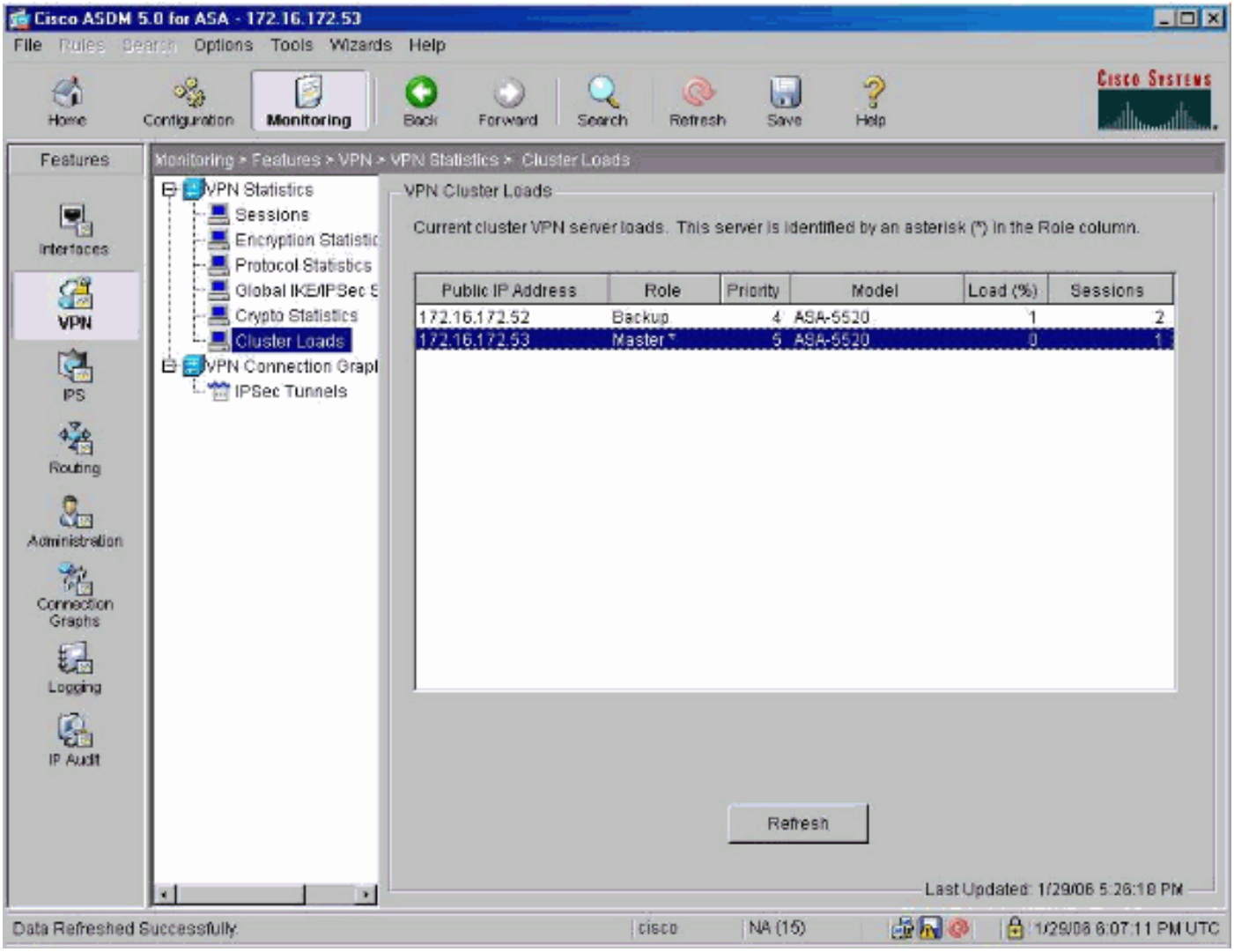
4. 그룹에 속한 모든 ASA에 대해 단계를 반복합니다.

이 섹션의 예에서는 다음 CLI 명령을 사용하여 로드 밸런싱을 구성합니다.

```
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
```

모니터링

Monitoring(**모니터링) > Features(기능) > VPN > VPN Statistics(VPN 통계) > Cluster Loads(클러스터 로드)를 선택하여** ASA에서 로드 밸런싱 기능을 모니터링합니다.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여

show 명령 출력의 분석을 봅니다.

- **show vpn load-balancing** - VPN 로드 밸런싱 기능을 확인합니다.

```
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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug vpnlb 250** - VPN 부하 분산 기능의 문제를 해결하는 데 사용됩니다.

```
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]
```

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조

- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems