ASA VPN 로드 밸런싱 디렉터 선택 프로세스

목차

소개

이 문서에서는 Cisco 5500-X Series ASA(Adaptive Security Appliance)와의 VPN 로드 밸런싱 시나리오의 디렉터 선택 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 9.2를 실행하는 Cisco ASA 5500-X를 기반으로 합니다.

> **참고:**이 문서는 버전 7.0(1)에서 기능이 처음 도입되었으므로 모든 소프트웨어 버전에도 적용됩니다.

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.

배경 정보

VPN 로드 밸런싱은 가상 클러스터의 디바이스 간에 네트워크 트래픽을 균등하게 분산하기 위해 사용되는 메커니즘입니다.로드 밸런싱은 간단한 배포를 기반으로 합니다.처리량 활용이나 기타 요소

를 고려하지 않습니다.로드 밸런싱 클러스터는 디렉터와 하나 이상의 보조 디바이스로 구성되며 이러한 디바이스는 동일하게 구성할 필요가 없습니다.

로드 밸런싱 알고리즘

다음은 로드 밸런싱 알고리즘의 개요입니다.

- 디렉터 디바이스는 내부 IP 주소의 오름차순으로 정렬된 보조 클러스터 멤버 목록을 유지 관리합니다.
- 부하는 각 보조 클러스터 멤버가 제공하는 정수 백분율(활성/최대 세션 수)로 계산됩니다.
- 디렉터 디바이스는 IPSec/SSL(Secure Sockets Layer) VPN 터널을 로드가 가장 낮은 디바이스로 리디렉션하여 다른 디바이스보다 1% 더 높은 디바이스로 리디렉션합니다.
- 모든 보조 클러스터 멤버가 디렉터 디바이스보다 1% 더 높은 경우에만 디렉터 디바이스가 자체적으로 리디렉션됩니다.

다음은 디렉터 1개와 보조 클러스터 멤버 2개가 있는 예입니다.

- 모든 노드는 0% 로드로 시작하고 모든 백분율은 가장 가까운 1/2%로 반올림됩니다.
- 모든 멤버에 디렉터 디바이스보다 1% 높은 로드가 있는 경우 디렉터 디바이스가 연결을 수행합니다.
- 디렉터 디바이스에서 연결을 수행하지 않으면 현재 로드 비율이 가장 작은 백업 디바이스에서 세션을 가져옵니다.
- 모든 구성원이 동일한 로드 비율을 갖는 경우 세션 수가 가장 적은 백업 디바이스가 세션을 수행합니다.
- 모든 구성원이 동일한 로드 비율과 동일한 세션 수를 가질 경우 IP 주소가 가장 적은 백업 디바이스가 세션을 수행합니다.

이사 선거 프로세스

VPN 부하 균형 디렉터 선택 프로세스는 네트워크 외부의 클러스터에서 수행됩니다. 외부 네트워크에서 교환되는 데이터 유형은 두 가지입니다.

- 디렉터 검색에 사용되는 클러스터 IP 주소에 대한 ARP(Address Resolution Protocol) 패킷이 교환됩니다.디렉터를 검색하기 위해 클러스터 IP 주소에 대해 전송되는 최대 ARP 패킷 수는 다음과 같습니다.

  (10 - 우선 순위) + 1

  여기서 *우선 순위*는 vpn load-balancing CLI 명령의 **priority** 하위 명령에서처럼 구성됩니다.

- Hello 요청/응답 메시지에 대한 외부의 UDP 패킷이 교환됩니다.포트 번호는 **cluster port load-balancing** 하위 명령에 지정되며 기본값은 **9023입니다**.

예를 들어, 로드 밸런싱 디바이스의 *우선 순위*가 5인 경우 어떤 디렉터 디바이스가 클러스터 IP 주소를 소유하는지 확인하기 위해 최대 6개의 ARP 패킷을 전송하려고 시도합니다.디렉터 디바이스가 탐지되면 ASA는 더 이상 ARP 메시지를 전송하지 않고 UDP Hello 요청을 전송하기 15초 전에 기다립니다.그런 다음 디렉터 디바이스가 UDP Hello 응답으로 응답합니다.

재부팅 시나리오 주의

로드 밸런싱 클러스터에 있는 2개의 ASA가 있는 재부팅 상황:

- 재부팅하기 전에 ASA-1 또는 ASA-2가 디렉터였습니다.
- ASA-1이 재부팅됩니다.
- ASA-2는 이전에 디렉터가 아닌 경우 디렉터가 됩니다.
- ASA-1은 재부팅한 후 클러스터만 멤버로 가입합니다.

로드 밸런싱 알고리즘은 클러스터 디바이스의 외부 인터페이스도 연결된 스위치 컨피그레이션의 영향을 받을 수 있습니다.예를 들어, 스패닝 트리 알고리즘은 스위치에 연결된 디바이스가 재부팅될 때 연결 지연을 일으킬 수 있습니다.

> **팁**:spanning-tree port fast 명령은 프로세스 속도를 높이는 데 도움이 됩니다.

로드 밸런싱이 활성화된 새로 리부팅된 ASA는 스위치의 연결 지연으로 인해 현재 디렉터 디바이스에 연결할 수 없으므로 디렉터 디바이스(디렉터 디바이스가 이미 있는 경우에도)가 되려고 할 수 있습니다.ARP 충돌로 인해 디렉토리 충돌이 탐지되면 MAC(Media Access Control) 주소가 낮은 ASA가 승리하고, MAC 주소가 높은 ASA는 디렉터 디바이스 역할을 중단합니다.

감독 재선거 과정

이사 장치의 재선을 일으키는 두 가지 상황이 있다.

클러스터에서 디렉터 장치 제거

ASA에서 이 기능을 비활성화하면 변경 사항을 알리기 위해 모든 클러스터 멤버에 브로드캐스트 메시지가 전송되고 이전에 설명한 선택 프로세스가 수행됩니다.

디렉터 장치가 클러스터 구성원 hello 메시지에 응답하지 않습니다.

디렉터 디바이스가 클러스터 멤버 Hello 메시지에 응답하지 않으면 ASA 클러스터 멤버가 디렉터가 더 이상 존재하지 않음을 탐지하는 데 약 20초가 걸립니다.Hello 메시지는 5초마다 전송됩니다(구성할 수 없음). 4개의 Hello 메시지 후에 클러스터 멤버가 디렉터 디바이스로부터 응답을 받지 못하면 선택 프로세스가 트리거됩니다.

문제 해결

> **참고:**debug 명령을 사용하기 전에 Cisco의 Debug Commands에 대한 중요 정보 문서를 참조

하십시오.

이러한 debug 명령은 시스템의 문제를 해결하려는 시도에서 유용할 수 있습니다.

- **debug fsm 255** - 이 명령을 사용하여 일반 유한 상태 머신 디버그를 활성화합니다.비활성화하려면 **no debug all** 명령을 입력합니다.
- **debug menu vpnlb 3** - VPN 부하 균형 디버그 추적을 활성화하려면 이 명령을 사용합니다.비활성화하려면 **debug 메뉴 vpnlb 3** 명령을 다시 입력합니다.
- **debug menu vpnlb 4** - VPN 부하 균형 기능 추적을 활성화하려면 이 명령을 사용합니다.비활성화하려면 **debug 메뉴 vpnlb 4** 명령을 다시 입력합니다.

관련 정보

- 로드 밸런싱 이해
- 기술 지원 및 문서 – Cisco Systems