데이터 센터의 Cisco ASA 5585-X

Cisco® ASA 5500 Series Adaptive Security Appliance 는 하나의 장치에 고급 네트워크 연결 상태 추적 방화벽과 VPN Concentrator 기능을 결합하여 제공합니다. 다중 보안 컨텍스트(가상화된 방화벽과 유사)와 투명한(계층 2) 방화벽 또는 라우팅된(계층 3) 방화벽 운영, 고급 검사 엔진, 침입 방지, IPsec 및 WebVPN 지원 등 많은 고급 기능이 어플라이언스에 포함되어 있습니다.

데이터 센터

해당 섹션에서는 데이터 센터에 방화벽을 구축하는 것과 관련된 비즈니스 요구와 제안된 솔루션의 요구 사항에 대한 설명을 제공합니다. 또한 솔루션에 통합된 다양한 ASA 기술의 개요에 대해서도 설명합니다.

비즈니스 요구: 데이터 센터 방화벽 구축

데이터 센터의 중요성이 그 어느 때보다 기업에 요구되고 있습니다. 데이터 센터에 데이터 서비스가 집중됨에 따라 고성능 및 확장 가능한 네트워크 보안에 대한 요구도 커졌습니다. 이러한 요구의 해결을 위해 Cisco 는 캠퍼스와 데이터 센터의 5Gbps 및 10Gbps 요구를 충족시키는 어플라이언스 ASA 5580 을 출시했습니다. 이제 Cisco 의 ASA 포트폴리오가 더욱 확장되었습니다. 차세대 ASA 5585-X 어플라이언스는 ASA 5500 Series 의 성능 범위를 확장하여, 2Gbps-20Gbps 의 실제 HTTP 트래픽 및 35Gbps 의 대규모 패킷 트래픽을 제공합니다. Cisco ASA 5585-X 는 초당 최대 35 만개의 연결 및 최대 2 백만 개의 초기 동시 연결을 지원합니다. 이후 릴리스에서는 최대 8 백만 개의 동시 연결을 지원할 계획입니다.

Web 2.0 애플리케이션의 출현으로 인해 새로운 장치 유형이 극적으로 증가하였고, 복잡한 콘텐츠의 광범위한 사용에 따라 기존 보안 인프라에 대한 긴장감이 고조되고 있습니다. 오늘날의 보안 시스템은 변화하는 환경에 필요한 빠른 트랜잭션 속도와 심층 있는 보안 정책을 충족하지 못하는 경우가 많습니다. 그 결과 정보 기술 직원은 기본적인 보안 서비스의 제공과 함께 필요한 모니터링, 감사 및 규정 준수 목적을 위해 시스템 생성된 엄청난 수의 보안 이벤트 처리 등 급급해 할 때가 많습니다.

Cisco ASA 5585-X 어플라이언스는 엔터프라이즈 데이터 센터의 많은 트랜잭션과 대기 시간에 민감한 미디어 리치 애플리케이션 보호를 위해 설계되었습니다. 업계 선두의 처리량, 업계에서 가장 빠른 연결 속도, 대규모 정책 구성 및 매우 짧은 대기 시간을 제공하는 ASA 5585-X 는 음성, 비디오, 데이터 백업, 과학 또는 그리드 컴퓨팅, 재무 거래 시스템 등 가장 까다로운 애플리케이션을 다루는 조직의 보안 요구에 매우 적합합니다.

솔루션 요구 사항

Cisco ASA 5585-X 어플라이언스는 사용자와 관리자가 조직 내에서 서로 다른 정책의 보안 도메인 구성을 도와주는 유연하고 경제적인 성능 기반 솔루션을 제공합니다. 사용자는 서로 다른 VLAN 과 관련하여 적절한 정책을 설정할 수 있어야 합니다. 데이터 센터는 데이터 보호를 위해 상태를 추적할 수 있는 방화벽 보안 솔루션을 보유해야 하며 DMZ(비무장 지대) 및 엑스트라넷 서버 팜을 통해 악의적인 트래픽의 필터링을 실시해야 하고 가장 경제적인 비용으로 다중 기가비트 성능을 제공해야 합니다.

Cisco ASA 5585-X 어플라이언스는 액티브/액티브 또는 액티브/스탠바이 토폴로지에서의 배포가 가능하며 탄력성을 높이기 위해 인터페이스 리던던시 등의 추가 기능을 사용할 수 있습니다. 내결함성 및 상태 링크에 별도의 링크가 사용됩니다.

Cisco ASA 5585-X 어플라이언스는 대기업, 데이터 센터 및 서비스 공급자 네트워크를 위한 다중 기가비트 보안 서비스를 제공합니다. 고속 이더넷에서 10 기가비트 이더넷까지의 확장성과 함께 고밀도 구리 및 옵티컬 인터페이스를 통해 업계 경쟁 제품들과는 견줄 수 없는 보안 및 구축 유연성을 지원합니다. 이러한 고밀도 설계로 인해 관리되는 보안 및 인프라 통합 애플리케이션에 필요한 물리적 세그멘테이션의 유지와 보안 가상화의 사용이 가능합니다.

결정

해당 문서에서는 Cisco ASA 5585-X 어플라이언스의 데이터 센터 방화벽 서비스 구축 시의 설계 고려 사항 및 구현 지침에 대한 정보를 제공합니다.

Cisco ASA 기술 개념

보안 정책

방화벽은 외부 네트워크의 사용자가 내부 네트워크에 무단 액세스하는 것을 차단합니다. 방화벽은 또한 내부 네트워크 사이에서도 상호 간 보호가 가능합니다. 인사부 네트워크를 사용자 네트워크로 부터 분리하는 것 등이 그 예입니다. Cisco ASA 어플라이언스에는 다중 보안 컨텍스트 투명한(계층 2) 방화벽 또는 라우팅된(계층 3) 방화벽 운영, 수백 개의 인터페이스 등의 많은 고급 기능들이 포함되어 있습니다. 방화벽에 연결된 네트워크에 대한 기본적인 개념을 설명하면 외부 네트워크는 방화벽 앞에 있으며, 내부 네트워크는 방화벽 뒤에서 보호됩니다. 보안 정책은 이러한 방화벽을 통과해 다른 네트워크에 액세스하려는 트래픽의 유형과 관련 허용여부를 결정합니다. 보안 정책에서 명시적으로 허용하지 않는 한 일반적으로 어떤 트래픽도 방화벽을 통과할 수 없습니다.

Cisco Intrusion Prevention 서비스

Cisco AIP SSP(Advanced Inspection and Prevention Security Services Processor)에는 정확도를 높이기 위해 인라인 침입 방지 서비스가 혁신적인 기술과 결합되어 있습니다. Cisco ASA 5585-X 어플라이언스 내부에 구축된 SSP 는 기타 네트워크 보안 리소스를 통합하고 네트워크 보호를 위한 예방적 접근 방식의 제공을 통해 IPv6 및 IPv4 네트워크를 포괄적으로 보호합니다.

Cisco AIP SSP 에서는 다음과 같은 기능을 통해 더 큰 신뢰로 위협을 차단할 수 있습니다.

- **광범위한 IPS 기능:** 트래픽 경로 또는 프로미스큐어스 모드에서 인라인으로 구축할 수 있는 Cisco AIP SSP 는 Cisco IPS 4200 Series Sensor 에서 사용할 수 있는 모든 IPS 기능을 제공합니다.
- **Global Correlation:** Cisco AIP SSP 는 평판 분석을 추가하고, 위협 노출 기간을 줄이고, 지속적인 피드백을 제공함으로써 기업 경계를 넘어 글로벌 위협 환경에서 실시간 업데이트를 제공합니다.
- **적시의 포괄적인 공격 방지:** Cisco AIP SSP 는 전문화된 IPS 감지 엔진 및 수천 개의 서명을 사용해 수만 개의 알려진 악용 요소 및 더 많은 알려지지 않은 수백만 개의 악용 변종 요소로부터 기업을 보호합니다.
- **제로 데이 공격 방지:** Cisco 이상 감지 기능은 네트워크의 정상적인 동작을 학습한 후 네트워크에서 비정상적 활동이 발견되면 경고함으로써, 서명이 사용하기 전이라도 새로운 위협을 차단하도록 지원합니다.

ASA 어플라이언스 내 트래픽 플로우에 IPS 가 구축되면 어플라이언스의 모든 리던던시 기능이 이러한 플로우로 자동 상속됩니다.

고가용성

Cisco ASA 보안 어플라이언스는 업계에서 가장 탄력적이고 포괄적인 고가용성 솔루션 중 하나입니다. 신속한 장애 조치 및 인터페이스 리던던시와 같은 기능으로 고객은 풀메시(full-mesh) 액티브/스탠바이 및 액티브/액티브 장애 조치 구성을 비롯한 매우 수준 높은 고가용성 구축의 배포가 가능합니다.

이를 통해 고객은 네트워크 기반 공격을 지속적으로 방지하는 한편 연결의 안전한 유지를 통해 오늘날의 비즈니스 요구 사항을 충족시킬 수 있습니다.

액티브/액티브 장애 조치의 경우 두 유닛 모두 네트워크 트래픽의 전달이 가능합니다. 또한 네트워크에 트래픽 공유를 구성할 수도 있습니다. 액티브/액티브 장애 조치는 "다중" 컨텍스트 모드에서 실행되는 유닛에서만 사용할 수 있습니다. 액티브/스탠바이 장애 조치의 경우 한 유닛은 트래픽을 전달하고 다른 유닛은 스탠바이 상태에서 대기하게 됩니다. 액티브/스탠바이 장애 조치는 "단일" 또는 "다중" 컨텍스트 모드에서 실행되는 유닛에서만 사용할 수 있습니다. 두 가지 장애 조치 구성 모두 상태 저장 및 상태 비저장 장애 조치를 지원합니다.

다음 이벤트 중 하나가 발생하면 유닛이 실패할 수 있습니다.

- 유닛에 하드웨어 장애 또는 전력 장애가 있음
- 유닛에 소프트웨어 장애가 있음
- 모니터링한 인터페이스 중 너무 많은 수가 실패함
- 관리자가 CLI 명령 "no failure active"를 사용해 수동 실패를 트리거함

상태 저장 장애 조치가 사용되더라도 장치-장치 장애 조치가 몇몇 서비스 방해를 일으킬 수 있습니다. 몇 가지 예를 들면 다음과 같습니다.

- 불완전한 TCP 3-Way Handshake 를 다시 시작해야 합니다.
- Cisco ASA 소프트웨어 릴리스 8.3 이하에서, 최단 경로 우선 프로토콜(OSPF) 경로가 액티브-스탠바이 유닛에서 복제되지 않습니다. 장애 조치 시 OSPF 인접성을 다시 설정하고 경로를 다시 학습해야 합니다.
- 검사 엔진 상태 대부분이 장애 조치 피어 유닛에 동기화되지 않습니다. 피어 장치에 대한 장애 조치에서 검사 엔진 상태의 손실이 발생합니다.

액티브/스탠바이 장애 조치

액티브/스탠바이 장애 조치에서는 스탠바이 보안 어플라이언스를 사용해 실패한 유닛의 기능을 인수할 수 있습니다. 액티브 유닛이 실패하면 스탠바이 상태로 변경되며, 스탠바이 유닛은 액티브 상태로 변경됩니다. 액티브 상태로 변경된 유닛은 실패한 유닛의 IP 주소(또는 투명한 방화벽을 위해 관리 IP 주소) 및 MAC 주소를 인수하여 트래픽 전달을 시작합니다. 스탠바이 상태가 된 유닛은 스탠바이 IP 주소 및 MAC 주소를 인수합니다. 네트워크 장치에서는 MAC-IP 주소 쌍의 변화가 감지되지 않으므로, 네트워크 어디에서도 ARP(Address Resolution Protocol) 항목의 변경 또는 시간 초과가 발생하지 않습니다.

액티브/스탠바이 장애 조치에서는 다중 컨텍스트 모드의 컨텍스트 기반이 아니라 물리적 유닛 기반에서 장애 조치가 발생합니다. 액티브/스탠바이 장애 조치는 ASA 플랫폼에서 가장 일반적으로 배포되는 고가용성 방법입니다.

액티브/액티브 장애 조치

액티브/액티브 장애 조치는 "다중" 컨텍스트 모드의 보안 어플라이언스에 사용할 수 있습니다. 두 가지 보안 어플라이언스 모두 동시에 네트워크 트래픽을 전달할 수 있으며, 비동기 데이터 플로우를 처리하도록 배포할 수 있습니다. 보안 어플라이언스의 보안 컨텍스트를 장애 조치 그룹으로 나누는 것이 가능합니다. 장애 조치 그룹은 단순히 하나 이상의 보안 컨텍스트로 구성된 논리적 그룹입니다. 보안 어플라이언스에 최대 두 개의 장애 조치 그룹을 생성할 수 있습니다.

장애 조치 그룹은 액티브/액티브 장애 조치에서 장애 조치를 위한 기본 유닛을 형성합니다. 인터페이스 장애 모니터링, 장애 조치 및 액티브/스탠바이 상태는 모두 물리적 유닛에 이상이 있는 것이 아니라 장애 조치 그룹의 특성입니다. 액티브 장애 조치 그룹이 실패하게 되면 스탠바이 상태로 변경되고, 스탠바이 장애 조치 그룹은 액티브 상태가 됩니다. 액티브 상태가 된 장애 조치 그룹은 실패한 장애 조치 그룹 인터페이스의 MAC 및 IP 주소를 인수합니다. 스탠바이 상태가 된 장애 조치 그룹의 인터페이스는 스탠바이 MAC 및 IP 주소를 인수합니다. 이는 물리적 액티브/스탠바이 장애 조치에서 볼 수 있는 것과 유사한 동작입니다.

리던던시 인터페이스

인터페이스 수준의 리던던시는 ASA 어플라이언스에 있는 두 개의 물리적 인터페이스 위에 하나의 논리적 인터페이스를 구성할 수 있다는 개념을 기반으로 합니다. 이 기능은 Cisco ASA 소프트웨어 릴리스 8.0 에서 소개된 바 있습니다.

한 인터페이스는 트래픽 전달을 위한 액티브 인터페이스 역할을 담당합니다. 다른 인터페이스는 스탠바이 상태에 있게 됩니다. 액티브 인터페이스가 실패할 경우 모든 트래픽이 스탠바이 인터페이스로 장애 조치됩니다. 이 기능의 주요 이점은 동일한 물리적 장치 내에서 장애 조치가 발생하므로 장치 수준의 장애 조치가 불필요하게 발생하지 않는다는 것입니다. 이러한 리던던시 인터페이스는 일단 구성하면 물리적 인터페이스처럼 처리됩니다.

액티브 장치의 링크 실패는 장치 수준의 장애 조치를 일으킬 수 있지만 리던던시 인터페이스는 그렇지 않습니다. 데이터 센터 환경에서 풀메시(full-mesh) 토폴로지를 만들기 위해 리던던시 인터페이스를 사용할 경우의 이점은 다음과 같습니다.

- 인터페이스 수준의 장애 조치가 발생할 경우 불완전한 TCP 3-Way Handshake 를 다시 시작할 필요가 없습니다.
- 만약 ASA 어플라이언스에서 동적 라우팅 프로토콜이 사용되는 경우 라우팅 인접성을 다시 설정/다시 학습할 필요가 없습니다.
- 검사 엔진 상태 대부분은 인터페이스 수준의 장애 조치에서는 손실되지 않습니다. 그러나 장치 수준의

장애 조치에서는 손실됩니다. ASA 상태 저장 장애 조치는 세션 데이터 전체를 복제하지는 않으므로 최종 사용자에게 영향이 덜 미칩니다. 예를 들어 MGCP(Media Gateway Control Protocol) 등 일부 음성 프로토콜의 제어 세션은 복제되지 않는데, 장애 조치는 그러한 세션을 중단할 수 있습니다.

인터페이스 리던던시 기능에서는, 두 가지 기본 물리적 인터페이스가 실패한 경우에만(리던던시) 인터페이스가 장애 상태에서 고려될 수 있습니다.

인터페이스 수준 리던던시의 주요 이점은 다음과 같습니다.

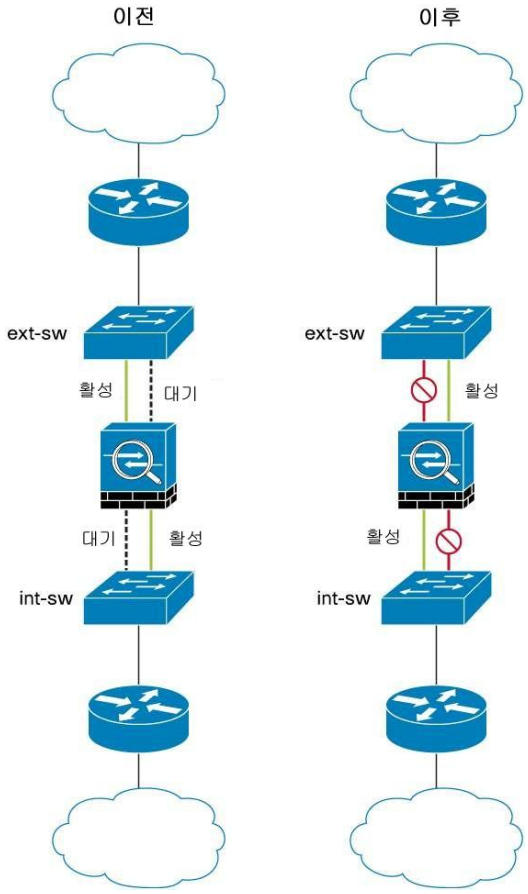
- 장애 조치 환경에서 장치 수준의 장애 조치가 발생할 확률이 줄고, 이에 따라 네트워크/방화벽 가용성이 증가하며 불필요한 서비스/네트워크 중단이 제거됩니다.
- 풀메시(full-mesh) 방화벽 아키텍처가 구축되어 처리량과 가용성이 증가합니다.

그림 1 은 인터페이스 리던던시가 사용되고 장치 수준(A/S 또는 A/A) 장애 조치가 없는 ASA 어플라이언스에 대한 간단한 구축 시나리오를 보여줍니다.

이 시나리오에서 ASA 인터페이스 장애가 발생하면 리던던시 인터페이스의 물리적 스탠바이 인터페이스가 액티브 인터페이스 자격을 넘겨받은 이후 보안 어플라이언스가 계속해서 트래픽을 전달하게 됩니다.

이러한 설계는 단일 컨텍스트 모드, 다중 컨텍스트 모드, 라우팅된 방화벽 모드 및 투명한 방화벽 모드에서 지원됩니다.

그림 1. 다음은 리던던시 인터페이스 장애 발생 없이 물리적 인터페이스 장애가 발생한 경우 리던던시 인터페이스의 사용 전후 그림을 보여줍니다.



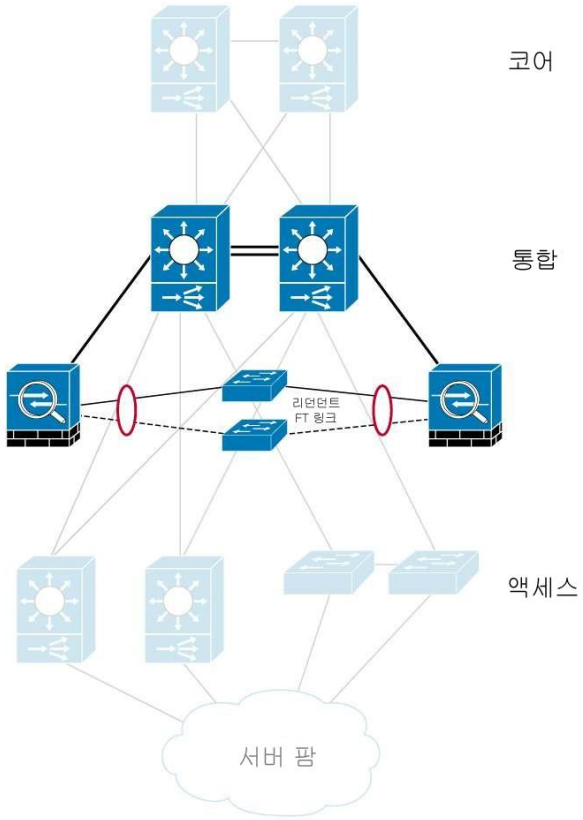
Cisco ASA 5585-X 어플라이언스는 그림 2 에 나와 있듯이 표준 데이터 센터 설계에 적합합니다. VLAN 은 물리적 스위치에서 외부 ASA 어플라이언스로 확장되며, 별도의 스위치에 연결된 상태 링크 및 전용 리던던시 장애 조치를 사용합니다. 이전 섹션에서 설명한 기술들이 결합되어 매우 여유 있는 네트워크 설계가 생성됩니다. ASA 어플라이언스의 다음과 같은 세 가지 주요 기능을 사용하게 됩니다.

- 리던던시 인터페이스
- 액티브/액티브 장애 조치
- 투명한 모드

단일 ASA 어플라이언스를 보안 컨텍스트라고 하는 다중 가상 장치로 분할할 수 있습니다. "다중" 컨텍스트 모드에서는 ASA 어플라이언스에 보안 정책, 인터페이스 및 독립형 장치에서 구성할 수 있는 거의 모든 옵션을 식별하는, 각 컨텍스트에 대한 구성이 포함됩니다. 시스템 구성은 ASA 에 대한 기본 설정을 식별하지만, 네트워크 인터페이스 또는 자체에 대한 네트워크 설정은 포함하지 않습니다. "관리자" 컨텍스트는 다른 모든 컨텍스트와 같지만 하나만 다릅니다. 즉, "관리자" 컨텍스트에 로그인한 사용자는 시스템 관리자 권한을 갖게 되며 "시스템" 및 기타 모든 컨텍스트에 액세스할 수 있습니다.

아키텍처 개요

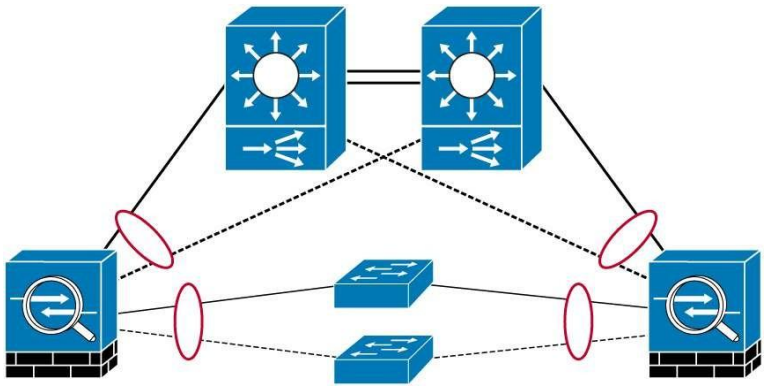
그림 2. 표준 데이터 센터 아키텍처



IPS 서비스를 설계 내의 각 ASA 어플라이언스에 통합하거나, 별도의 독립형 IPS/IDS 를 적용할 수 있습니다. ASA 어플라이언스 내에 IPS 서비스를 통합할 경우의 이점은, IPS 서비스로 검사할 트래픽을 세부적인 제어를 사용해 분류할 수 있다는 것입니다.

방화벽으로 처리할 VLAN 을 담당하는 트렁크 포트를 연결하여, 어그리게이션 계층에서 ASA 5585-X 를 아키텍처에 통합합니다. 필요한 경우 여분의 가용성 수준을 제공하기 위해 어그리게이션 계층에 대해 예비 링크를 구성할 수 있습니다(그림 3). 액티브 장치의 링크 실패는 장치 수준의 장애 조치를 일으킬 수 있지만 리던던시 인터페이스는 그렇지 않습니다.

그림 3. 예비 링크 연결



투명한 또는 라우팅된 방화벽 모드

Cisco ASA 5585-X 는 두 가지 서로 다른 방화벽 모드, 즉 투명한 방화벽 모드와 라우팅된 방화벽 모드를 지원합니다. 라우팅된 방화벽 모드에서 ASA 어플라이언스는 네트워크의 라우터 홉으로 간주됩니다. 투명한 방화벽 모드에서 ASA 어플라이언스는 "스텔스 방화벽"처럼 작동하며 라우터 홉으로 간주되지 않습니다. ASA 어플라이언스는 내부 및 외부 인터페이스에서 동일한 네트워크에 연결됩니다. 공격자에게 방화벽이 보이지 않게 하려는 경우 투명한 모드가 유용합니다. 데이터 센터 설계에서는 ASA 어플라이언스의 액티브/액티브 아키텍처를 지원하기 위해 투명한 모드가 사용됩니다.

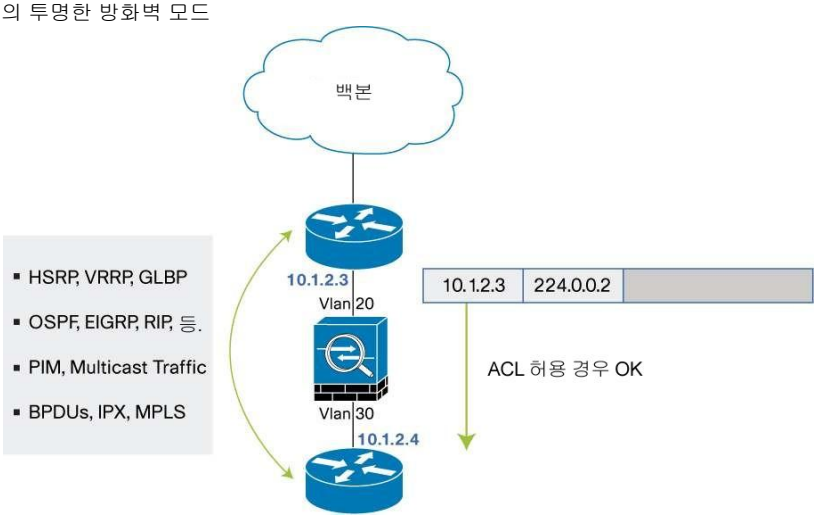
표 1 에서는 두 가지 구축 유형의 기능을 보여줍니다.

표 1. 라우팅된 방화벽 모드와 투명한 방화벽 모드 비교

라우팅됨	자동화
NAT 의 모든 "특성" 사용 가능 데이터 트래픽이 라우팅됨 멀티캐스트 트래픽을 전달하지 않음 컨텍스트 간에 인터페이스 공유 가능	컨텍스트당 두 개의 인터페이스 투명한 모드에 대해 NAT 지원 데이터 트래픽이 브리지됨 멀티캐스트 트래픽 전달 공유

투명한 모드에서 Cisco ASA 5585-X 어플라이언스는 라우터 홉이 아닙니다. ASA 어플라이언스는 내부 및 외부 포트에서 동일한 네트워크를 연결하지만, 각 포트는 서로 다른 VLAN 에 있어야 합니다. ASA 어플라이언스에 동적 라우팅 프로토콜 또는 NAT 가 필요하지 않습니다. 데이터 센터에서 투명 모드를 사용할 경우의 기타 이점에 대해서는 그림 4 에서 설명합니다.

그림 4. 데이터 센터의 투명한 방화벽 모드



- 라우터가 방화벽을 통해 라우팅 프로토콜 인접성을 설정할 수 있습니다.
- HSRP(핫 스탠바이 라우터 프로토콜), VRRP(가상 라우터 장애 복구 프로토콜), GLBP(게이트웨이 부하 균형 프로토콜) 등의 프로토콜은 방화벽을 통과할 수 있습니다. 멀티캐스트 스트림도 방화벽을 가로지를 수 있습니다.
- 비 IP 트래픽도 허용할 수 있지만(사전 구성된 유형은 IPX, MPLS, BPDU), 이더넷 V2/DIX 캡슐화를 사용해야 합니다(검사 없음, 브리징만).

성능 및 확장성

지금까지 방화벽 성능을 결정하는 주요 요소는 Mbps 로 표시되는 처리량이었습니다. 그러나 애플리케이션은 훨씬 더 까다로워져서, 이제 더 오랜 시간 동안 연결 상태를 유지하거나(파일 공유 또는 멀티미디어에서 사용되는 것과 같은 지속적인 연결), 다수의 짧은 라이브 연결을 엽니다(대개 Facebook 과 같은 일반 웹 사이트에서 사용됨).

처리량은 여전히 중요하지만, 동시 연결 관련 기능을 확장하는 새로운 애플리케이션을 처리하고 새 연결을 신속하게 여는 기능을 제공하는 것도 처리량 못지않게 중요해지고 있습니다. Cisco ASA 5585-X 는 이러한 기능을 확장하지만, 초당 연결 속도에서 뛰어난 성능을 제공하고 총 동시 연결 수를 높이는 것에도 특별한 관심을 기울였습니다. Cisco ASA 5585-X 는 매우 짧은 대기 시간 및 병렬 CPU 아키텍처의 고속 전환 백플레인을 사용하여 성능 요구 사항을 해결했습니다.

요약

이 문서에서는 일반 데이터 센터에 대한 요구를 고려하여, 데이터 센터 설계에 Cisco ASA 5585-X 어플라이언스를 사용하는 방법에 대해 설명했습니다. ASA 5585-X 는 설계에 미치는 영향력을 최소화하는 방식으로 데이터 센터에 구축되었고, 이 과정에서 ASA 5585-X 내에 있는 매우 여유 있는 네트워크 설계 및 고가용성 기능이 사용되었습니다.

추가 정보

Cisco ASA 5500 Series Appliance 에 대한 자세한 내용은 http://www.cisco.com/go/asa 를 참조하거나 현재 고객 담당자에게 문의하십시오.

Cisco End-of-Life 정책에 대한 자세한 내용은 다음을 참조하십시오.
http://www.cisco.com/en/US/products/prod_end_of_life.html.

End-of-Life/End-of-Sale 정보를 구독하려면 다음을 참조하십시오.
http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

인쇄지: 미국 C22-624431-00 10/10