Web Security Appliance 설계 가이드

목차

소개

이 문서에서는 최적의 성능을 위해 Cisco WSA(Web Security Appliance) 및 관련 구성 요소를 설계하는 방법에 대해 설명합니다.

배경 정보

WSA용 솔루션을 설계할 때 어플라이언스 자체의 컨피그레이션 뿐만 아니라 관련 네트워크 디바이스 및 해당 기능에 대해서도 신중하게 고려해야 합니다.모든 네트워크는 여러 디바이스의 협업이며, 그 중 하나가 네트워크에 올바르게 참여하지 않으면 사용자 경험이 줄어들 수 있습니다.

WSA를 구성할 때 고려해야 하는 두 가지 주요 구성 요소가 있습니다.제공합니다하드웨어는 두 가지 유형으로 제공됩니다.첫 번째는 S170, S380, S680 Series 모델과 같은 물리적 하드웨어 유형과 S160, S360, S660, S370, S670 Series 모델과 같은 기타 EoL(End of Life) 모델입니다.다른 하드웨어 유형은 가상(예: S000v, S100v, S300v Series 모델)입니다.이 하드웨어에서 실행되는 운영 체제(OS)를 *AsyncOS for Web이라고* 하며, 이는 코어의 FreeBSD를 기반으로 합니다.

WSA는 프록시 서비스를 제공하며 모든 트래픽(HTTP, HTTPS 및 FTP(File Transfer Protocol))을 검사, 검사 및 분류합니다. 이러한 모든 프로토콜은 TCP를 기반으로 실행되며 적절한 작동을 위해 DNS(Domain Name System)에 크게 의존합니다.이러한 이유로, 네트워크 상태는 어플라이언스의 적절한 운영과 네트워크의 여러 부분과의 통신에 있어서 엔터프라이즈 제어 내부와 외부 모두에서 매우 중요합니다.

설계

최적의 성능을 위해 WSA 및 관련 구성 요소를 설계하려면 이 섹션에 설명된 정보를 사용하십시오.

네트워크

WSA의 올바른 작동을 위해서는 오류 없이 빠른 네트워크가 필수적입니다.네트워크가 불안정하면

사용자 환경이 저하될 수 있습니다.일반적으로 웹 페이지에 도달하는 데 시간이 더 걸리거나 연결할 수 없을 때 네트워크 문제가 탐지됩니다.초기 성향은 어플라이언스 탓이지만, 일반적으로 잘못된 동작의 네트워크입니다.따라서 네트워크에서 HTTP, HTTPS, FTP, DNS와 같은 상위 레벨 애플리케이션 프로토콜에 가장 적합한 서비스를 제공하는지 확인하기 위해 신중하게 고려하고 감사를 수행해야 합니다.

일반 고려 사항

다음은 최상의 네트워크 동작을 보장하기 위해 구현할 수 있는 몇 가지 일반적인 고려 사항입니다.

- 레이어 2(L2) 네트워크가 안정적인지, 스패닝 트리 작업이 올바른지, 스패닝 트리 계산 및 토폴로지가 자주 변경되지 않는지 확인합니다.
- 사용되는 라우팅 프로토콜은 빠른 컨버전스와 안정성도 제공해야 합니다.OSPF(Open Shortest Path First) 고속 타이머 또는 EIGRP(Enhanced Interior Gateway Routing Protocol)는 이러한 네트워크에 적합합니다.
- WSA에서 항상 두 개 이상의 데이터 인터페이스를 사용합니다.엔드 유저 컴퓨터에 연결되는 것과 아웃바운드 작업에 사용되는 것(업스트림 프록시 또는 인터넷에 연결된 것)을 나타냅니다.이는 TCP 포트 수가 소진되거나 네트워크 버퍼가 가득 찬 경우(특히 내부 및 외부 모두에 단일 인터페이스를 사용하는 경우) 등 가능한 리소스 제한 문제를 제거하기 위해 수행됩니다.
- 보안을 강화하기 위해 관리 전용 트래픽에 관리 인터페이스를 지정합니다.GUI를 통해 이를 실현하려면 **Network(네트워크) > Interfaces(인터페이스)**로 이동하고 **Separate routing (M1 port restricted to appliance management services only)** 확인란을 선택합니다.
- 고속 DNS 서버를 사용합니다.WSA를 통한 트랜잭션에는 하나 이상의 DNS 조회(캐시에 없는 경우)가 필요합니다.느리거나 동작이 잘못된 DNS 서버는 모든 트랜잭션에 영향을 미치며 지연 또는 느린 인터넷 연결로 관찰됩니다.
- 별도의 라우팅 테이블을 사용하는 경우 다음 규칙이 적용됩니다.

  모든 인터페이스는 기본 *관리* 라우팅 테이블(M1, P1, P2)에 포함됩니다.

  데이터 인터페이스만 *데이터* 라우팅 테이블에 포함됩니다.

  참고:라우팅 테이블의 분리는 인터페이스별로 이루어지는 것이 아니라 서비스별로 이루어집니다.예를 들어, WSA와 Microsoft AD(Active Directory) 도메인 컨트롤러 간의 트래픽은 항상 관리 라우팅 테이블에 지정된 경로를 따르며 이 테이블에서 P1/P2 인터페이스를 가리키는 경로를 구성할 수 있습니다.관리 인터페이스를 사용하는 데이터 라우팅 테이블에 경로를 포함할 수 없습니다.

로드 밸런싱

다음은 최적의 네트워크 동작을 보장하기 위해 구현할 수 있는 로드 밸런싱 고려 사항입니다.

- DNS 순환 - 단일 호스트 이름이 프록시로 사용되지만 DNS 서버에 여러 A 레코드가 있을 때 사용되는 용어입니다.각 클라이언트는 이를 다른 IP 주소로 확인하고 다른 프록시를 사용합니다

.DNS 레코드 변경은 재부팅 시 클라이언트에 반영되므로(로컬 DNS 캐싱) 변경이 필요한 경우 낮은 수준의 안정성을 제공합니다.그러나 최종 사용자에게는 이 사항이 투명하게 표시됩니다.

- PAC(Proxy Address Control) 파일 - 이 파일은 각 URL이 브라우저에 기록된 기능을 기반으로 처리되는 방법을 결정하는 프록시 자동 스크립팅 파일입니다.동일한 URL을 항상 직접 또는 동일한 프록시에 전달하는 기능이 있습니다.

- Auto discovery(자동 검색) - PAC 파일을 얻기 위해 DNS/DHCP 방법을 사용하는 방법을 설명합니다(이전 고려 사항에 설명). 일반적으로 이러한 첫 번째 세 가지 고려 사항은 하나의 솔루션으로 통합됩니다.그러나 Microsoft Office, Adobe 다운로더, Javascripts 및 Flash와 같은 많은 사용자 에이전트가 PAC 파일을 전혀 읽을 수 없는 복잡한 작업입니다.

- WCCP(Web Cache Control Protocol) - 이 프로토콜(특히 WCCP 버전 2)은 여러 WSA 간에 로드 밸런싱을 생성하고 고가용성을 통합하는 강력하고 강력한 방법을 제공합니다.

- 별도의 로드 밸런싱 어플라이언스 - 로드 밸런서를 전용 시스템으로 사용하는 것이 좋습니다.

방화벽

다음은 최적의 네트워크 동작을 보장하기 위해 구현할 수 있는 몇 가지 방화벽 고려 사항입니다.

- 각 소스에서 네트워크 전체에서 ICMP(Internet Control Message Protocol)가 허용되는지 확인합니다.WSA는 ICMP Echo 요청(유형 ⁄⁄ 및 Echo(유형 0)에 따라 달라지며 ICMP Unreliable-fragmentation(유형 3, 코드 4)이 필요한 RFC 1191에 설명된 대로 MTU(Maximum Transition Unit) 검색 메커니즘에 의존하므로 매우 중요합니다. pathmtudiscovery CLI 명령을 사용하여 WSA에서 경로 MTU 검색을 비활성화하면 WSA는 RFC 879에 따라 기본 MTU인 576바이트를 사용합니다. 이는 오버헤드가 증가하고 패킷의 리어셈블리로 인해 성능에 영향을 줍니다.

- 네트워크 내부에 비대칭 라우팅이 없는지 확인합니다.이는 WSA에서 문제가 아니지만, 경로를 따라 발생한 방화벽은 통신 양쪽을 모두 수신하지 못했기 때문에 패킷을 삭제합니다.

- 방화벽의 경우 WSA IP 주소를 위협에서 일반 엔드 컴퓨터 스테이션으로 제외하는 것이 매우 중요합니다.방화벽이 차단될 수 있음
- 너무 많은 연결(일반적인 방화벽 지식 기준)으로 인해 WSA IP 주소.

- 고객 프레미스 디바이스의 WSA IP 주소에 NAT(Network Address Translation)를 사용하는 경우 각 WSA가 NAT에서 별도의 외부 전역 주소를 사용하는지 확인합니다.단일 외부 전역 주소가 있는 여러 WSA에 대해 NAT를 사용하는 경우 다음 문제가 발생할 수 있습니다.

  모든 WSA에서 외부 세상으로 연결되는 모든 연결은 하나의 외부 글로벌 주소를 사용하며, 방화벽에는 리소스가 빠르게 부족합니다.

  해당 단일 목적지로 향하는 트래픽이 급증하면 대상 서버가 이를 차단하고 전체 엔터프라이즈를 이 리소스에 대한 액세스로부터 차단할 수 있습니다.이 리소스는 회사 클라우드 스토리지, Office Cloud 연결 또는 컴퓨터별 안티바이러스 소프트웨어 업데이트와 같은 중요한 리소스입니다.

ID

ID의 모든 구성 요소에 *논리적 AND* 원칙이 적용됩니다.예를 들어 user-agent 및 IP 주소를 모두 구성하면 이 IP 주소*의* user-agent를 의미합니다.사용자 에이전트 *또는* 이 IP 주소를 의미하지 않습니다.

동일한 서로게이트 유형(또는 서로게이트 없음) 및/또는 사용자 에이전트의 인증에 하나의 ID를 사용합니다.

인증이 필요한 각 ID에 Internet Explorer, Mozilla Firefox 및 Google Chrome과 같은 프록시 인증을 지원하는 알려진 브라우저/사용자 에이전트에 대한 사용자 에이전트 문자열이 포함되도록 하는 것이 중요합니다.인터넷 액세스가 필요하지만 프록시/WWW 인증을 지원하지 않는 애플리케이션이 있습니다.

ID는 일치하는 첫 번째 항목에서 끝나는 일치 항목을 검색하여 위쪽에서 아래쪽으로 매칭합니다.따라서 ID *1*과 ID *2*가 구성되어 있고 트랜잭션이 ID 1과 일치하면 ID 2에 대해 검사되지 않습니다.

액세스/암호 해독/라우팅/아웃바운드 악성코드 정책

이러한 정책은 서로 다른 유형의 트래픽에 적용됩니다.

- 액세스 정책은 일반 HTTP 또는 FTP 연결에 적용됩니다.트랜잭션을 수락할지 아니면 삭제할지를 결정합니다.

- 암호 해독 정책은 HTTPS 트랜잭션을 암호 해독, 삭제 또는 전달할지 여부를 결정합니다.트랜잭션이 암호 해독되면 트랜잭션의 연속 부분은 일반 HTTP 요청으로 표시될 수 있으며 액세스 정책과 일치됩니다.HTTPS 요청을 삭제해야 하는 경우 액세스 정책이 아닌 암호 해독 정책에 삭제합니다.그렇지 않으면 삭제된 트랜잭션을 먼저 해독하고 삭제하기 위해 더 많은 CPU 및 메모리를 사용합니다.

- 라우팅 정책은 WSA를 통해 허용된 트랜잭션의 업스트림 방향을 결정합니다.이는 업스트림 프록시가 있거나 WSA가 *커넥터* 모드에 있고 Cloud Web Security 타워로 트래픽을 전송하는 경우에 적용됩니다.

- 아웃바운드 악성코드 정책은 최종 사용자로부터 웹 서버로의 HTTP 또는 FTP 업로드에 대해 적용됩니다.일반적으로 HTTP Post 요청입니다.

각 정책 유형에 대해 *논리적 OR* 원칙이 적용된다는 점을 기억해야 합니다.여러 ID가 참조된 경우 트랜잭션이 구성된 ID와 일치해야 합니다.

더욱 세분화된 제어를 위해 이러한 정책을 사용합니다.정책별로 잘못 구성된 ID는 문제를 생성할 수 있으며, 정책에서 참조된 여러 ID를 사용하는 것이 더 유용합니다.ID는 트래픽에 영향을 주지 않으며, 정책에서 나중에 일치할 트래픽 유형을 식별합니다.

암호 해독 정책은 인증과 함께 ID를 사용하는 경우가 많습니다.이는 잘못되지 않으며 때로는 필요할 때도 있지만, 암호 해독 정책에서 참조되는 인증과 함께 ID를 사용하는 것은 인증이 이루어지도록 하기 위해 암호 해독 정책과 일치하는 모든 트랜잭션이 해독됨을 의미합니다.암호 해독 작업은 삭제 또는 전달될 수 있지만, 인증 ID가 있으므로 나중에 트래픽을 삭제 또는 전달하기 위해 암호 해독이 수행됩니다.이것은 비싸기 때문에 피해야 한다.

일부 컨피그레이션에는 30개 이상의 ID와 30개 이상의 액세스 정책이 포함되어 있으며, 모든 액세스 정책에는 모든 ID가 포함됩니다.이 경우 모든 액세스 정책에서 일치하는 ID는 이 많은 ID를 사용할 필요가 없습니다.어플라이언스 작동에는 영향을 주지 않지만, 문제 해결 시도와 혼동을 초래하며 성능과 관련하여 많은 비용이 듭니다.

맞춤형 URL 범주

맞춤형 URL 카테고리의 사용은 일반적으로 잘못 인식되고 오용되는 WSA의 강력한 툴입니다.예를 들어 ID에 일치하는 모든 비디오 사이트를 포함하는 컨피그레이션이 있습니다.WSA에는 비디오 사이트가 URL을 변경할 때 자동으로 업데이트되는 내장 툴이 있으며, 이는 자주 발생합니다.따라서 WSA에서 URL 카테고리를 자동으로 관리하고 아직 분류되지 않은 특별 사이트에 맞춤형 URL 카테고리를 사용하는 것이 좋습니다.

정규식에 주의하세요.점(.) 및 별표(*)와 같은 특수 문자를 사용하면 CPU가 매우 크고 메모리는 광범위할 수 있습니다.WSA는 모든 정규식을 확장하여 각 트랜잭션과 일치시킵니다.예를 들어, 정규식은 다음과 같습니다.

```
example.*
```

이 표현식은 example.*com* 도메인과 함께 *example*이라는 단어를 포함하는 모든 URL과 일치합니다.정규식에서 *dot* 및 *star*를 사용하지 말고 마지막 수단으로만 사용합니다.

다음은 문제를 생성할 수 있는 정규식의 또 다른 예입니다.

```
www.example.com
```

정규식 필드에서 이 예제를 사용하는 경우 www.example.com뿐만 아니라 www.www3example2com.com*과* 일치합니다. 여기서 점은 *임의의 문자*를 의미하기 때문입니다.www.example.com에만 매칭하려면 점을 이스케이프하십시오.

```
www\.example\.com
```

이 경우 사용자 지정 URL 범주 도메인 내에 이 형식을 포함할 수 있는 경우 정규식 기능을 사용할 이유가 없습니다.

```
www.example.com
```

안티멀웨어 및 평판

둘 이상의 스캐닝 엔진이 활성화된 경우 적응형 스캐닝을 활성화하는 옵션을 고려하십시오.적응형 스캐닝은 WSA의 강력하고 작은 엔진으로, 각 요청을 미리 검사하고 요청을 스캔하기 위해 사용해야 하는 포괄적인 엔진을 결정합니다.이렇게 하면 WSA의 성능이 약간 향상됩니다.