가상 어플라이언스를 제외하도록 Cisco ASA 차단 기능 구성

목차

소개

이 문서에서는 위협 탐지 구성 요소에서 가상 어플라이언스를 제외하도록 Cisco ASA를 구성하는 방법에 대해 설명합니다. Cisco ASA 위협 탐지 구성 요소는 DNS 및 기타 프로토콜에서 패킷 검사를 수행합니다. Umbrella는 이 기능이 Virtual Appliance와 충돌하지 않도록 다음 ASA 컨피그레이션 변경을 권장합니다.

- 이 문서에 설명된 대로 가상 어플라이언스를 위협 탐지 '차단' 기능에서 제외합니다.
- 이 문서에서 다루는 DNS 암호화(DNScrypt)를 허용하기 위해 DNS 패킷 검사에서 가상 어플라이언스를 제외합니다. Cisco ASA 방화벽이 DNScrypt를 차단합니다.

위협 감지 '차단' 기능

'차단' 기능이 활성화된 경우 ASA는 위협 탐지 규칙을 트리거하는 소스 IP 주소를 완전히 차단할 수 있습니다. 자세한 내용은 Cisco 문서를 참조하십시오. ASA 위협 탐지 기능 및 컨피그레이션.

가상 어플라이언스는 일반적으로 매우 많은 수의 DNS 쿼리를 Umbrella DNS 확인기로 전송합니다. 리졸버에 연결하는 데 로컬 문제가 있는 경우(예: 일시적인 네트워크 중단/지연) 이러한 쿼리는 실패할 수 있습니다. 전송되는 쿼리 수가 너무 많기 때문에, 작은 비율의 실패도 ASA가 가상 어플라이언스를 차단합니다. 이는 일정 기간 동안 완전한 DNS 중단으로 이어집니다.

가상 어플라이언스 제외

참고: 이 문서의 명령은 지침으로만 참조되며 프로덕션 환경을 변경하기 전에 Cisco 전문가와 상담하는 것이 좋습니다.

CLI를 통해:

- 어플라이언스 IP가 차단되지 않도록 제외하려면 다음 명령을 실행합니다. **no shun**

ASDM 인터페이스를 통해:

- Configuration(컨피그레이션) > Firewall(방화벽) > Threat Detection(위협 탐지) 창을 선택합니다.
- 어플라이언스 IP 주소를 차단에서 제외하려면 'Networks excluded from shun' 필드에 주소를 입력합니다. 쉼표로 구분하여 여러 주소 또는 서브넷을 입력할 수 있습니다.

어플라이언스가 '차단'되었는지 확인

이러한 단계를 따르지 않으면 어떤 상황에서는 어플라이언스가 '차단'되어 DNS 가동 중단이 발생할 수 있습니다.

가상 어플라이언스에 외부 연결이 없는 경우 Cisco ASA 콘솔은 다음과 같이 이벤트를 기록합니다.

4|2014년 6월 6일 14:00:42|401004: 차단된 패킷: 인터페이스 내부의 192.168.1.3 ==> 208.67.222.222
4|2014년 6월 6일 14:00:42|401004: 차단된 패킷: 인터페이스 내부의 192.168.1.3 ==> 208.67.222.222

현재 차단된 IP 주소 목록을 보려면 ASA에서 다음 명령을 실행합니다. **show shun**

현재 차단된 IP 주소를 즉시 지우려면 ASA에서 다음 명령을 실행합니다. **clear shun**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.