ASA CSC Security Services Module은 HTTP 트래픽의 프록시 역할을 어떻게 합니까?

목차

소개

이 문서에서는 Cisco ASA CSC(Content Security and Control) Security Services Module이 HTTP 트래픽에 대한 프록시 서버 역할을 하는 방법에 대해 설명합니다.

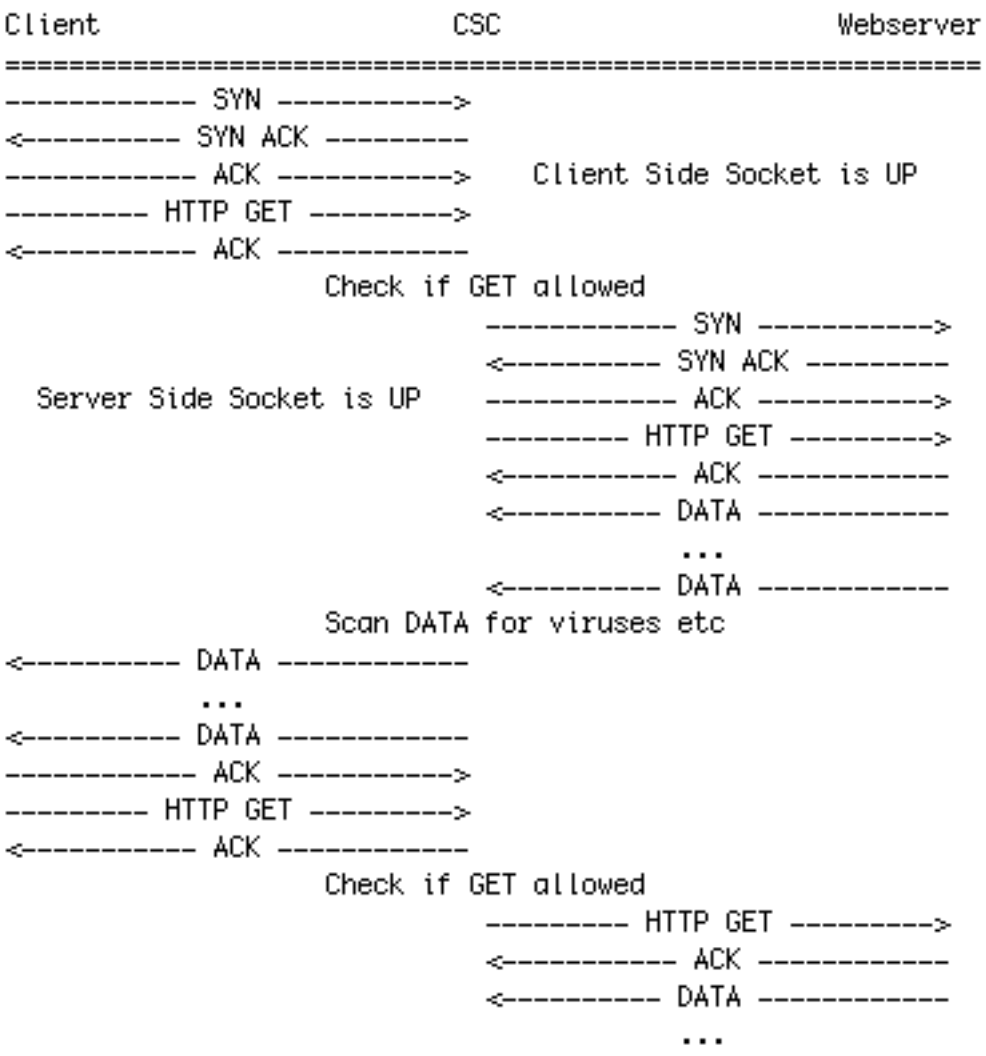
문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

Q. ASA CSC Security Services Module은 HTTP 트래픽에 대한 프록시 역할을 어떻게 합니까?

A. CSC 모듈을 통해 HTTP 연결을 설정하는 단계를 이해하면 다른 문제(예: 페이지 오류 및 성능 문제)를 이해하는 데 도움이 됩니다.

1. 사용자가 사이트에 연결을 시도하면 해당 브라우저는 해당 사이트의 IP 주소로 SYN 패킷을 전송합니다.
2. 프록시 역할을 하는 CSC 모듈은 사이트를 대신하여 SYN 패킷을 인터셉트하고 SYN-ACK로 응답합니다.
3. CSC 모듈이 프록시 역할을 하고 ACK로 응답하며 클라이언트 시스템과 CSC 모듈 HTTP 프록시 엔진 간에 연결이 형성되는 것을 모르는 웹 브라우저입니다.**참고:** 이 연결의 처음 절반은 CSS(Client Side Socket)라고 합니다.
4. 이때 브라우저에서는 사이트로의 연결이 작동 중인 것으로 간주하여 HTTP GET 요청을 보냅니다.
5. HTTP GET 요청은 CSC 모듈에서 처리됩니다.즉, URL 차단/필터링/WRS 설정에 대해 확인됩니다.요청이 허용되면 CSC 모듈은 사이트의 웹 서버에 대한 연결을 설정하기 시작합니다.
6. HTTP 프록시 엔진은 소스 IP 주소 및 소스 포트가 있는 TCP SYN 패킷을 보냅니다. 이 패킷은 클라이언트가 CSS에서 수신한 대로 웹 서버로 보낸 것으로 생각하는 원래 TCP SYN과 일치합니다. 웹 서버는 SYN ACK로 응답하고 HTTP 프록시 엔진은 ACK로 응답합니다.이때 SSS(Server-Side Socket)가 작동합니다.
7. HTTP 프록시 엔진은 클라이언트의 HTTP GET을 웹 서버로 전송하고 웹 서버는 콘텐츠로 응답합니다.
8. 이 콘텐츠는 스캔/점검됩니다.깨끗하면 콘텐츠가 클라이언트로 다시 전달됩니다.
9. 클라이언트에서 모든 웹 서버에 대한 다른 웹 요청에도 동일한 단계가 반복됩니다.

클라이언트 브라우저는 실제로 사이트에 연결하지 않습니다.CSC 모듈과 연결되며, 이 모듈에서는 이 이미지에 표시된 대로 사이트로 간주됩니다.



관련 정보

- 기술 지원 및 문서 – Cisco Systems