레이어 4 트래픽 모니터는 트래픽을 어떻게 차단합니까?

질문:

Layer 4 Traffic Monitor는 미러링된 트래픽만 수신하는 경우 트래픽을 어떻게 차단합니까?

환경:

레이어 4 트래픽 모니터 - 의심스러운 트래픽을 차단하도록 구성된 L4TM

해결책:

Cisco WSA(Web Security Appliance)에는 모든 네트워크 포트(TCP/UDP 0-65535)에서 의심스러운 세션을 차단할 수 있는 L4TM(Layer 4 Traffic Monitor) 서비스가 내장되어 있습니다.

이러한 세션 트래픽을 모니터링하거나 차단하려면 TAP(Test Access Port) 디바이스를 사용하거나 네트워크 디바이스에 미러 포트(Cisco 디바이스의 SPAN 포트)를 구성하여 WSA로 리디렉션해야 합니다.L4TM 인라인 모드는 아직 지원되지 않습니다.

트래픽은 원래 세션에서 어플라이언스로 미러링된(복사)이지만 WSA는 TCP 세션을 종료하거나 UDP 세션에 대해 ICMP "호스트 도달 불가" 메시지를 전송하여 의심스러운 트래픽을 차단할 수 있습니다.

TCP 세션의 경우

WSA L4TM이 서버로 또는 서버에서 패킷을 수신하고 트래픽이 차단 작업과 일치하면 L4TM은 시나리오에 따라 TCP RST(재설정) 데이터그램을 클라이언트나 서버에 보냅니다.TCP RST 데이터그램은 TCP RST 플래그가 1로 설정된 일반 패킷일 뿐입니다.

RST의 수신자가 먼저 이를 검증한 다음 상태를 변경합니다.수신기가 LISTEN 상태이면 무시됩니다.수신기가 SYN-RECEIVED 상태이고 이전에 LISTEN 상태였던 경우 수신자는 LISTEN 상태로 돌아갑니다. 그렇지 않은 경우 수신자는 연결을 중단하고 CLOSED 상태로 이동합니다.수신기가 다른 상태에 있으면 연결이 중단되고 사용자에게 알리고 CLOSED 상태로 이동합니다.

고려해야 할 두 가지 사례가 있습니다(두 경우 모두 사용자/클라이언트가 방화벽 뒤에 있는 경우).

첫째, 의심스러운 패킷이 방화벽 외부에서 내부 네트워크의 클라이언트로 이동하는 경우입니다.RST가 서버로 전송되며 이 경우 일반적으로 RST를 전달하지는 않지만 RST가 클라이언트에서 실제로 제공되었다고 판단되므로 세션이 종료됩니다.이 경우 RST의 소스 IP는 클라이언트의 스푸핑된 IP가 됩니다.클라이언트가 세션을 종료합니다.

두 번째 경우는 패킷이 내부 네트워크의 클라이언트에서 수신되고 외부 서버(방화벽 외부)로 이동하는 경우입니다. 그런 다음 RST가 클라이언트로 전송되고 RST 소스 IP가 서버의 스푸핑 IP가 됩니다.

UDP 세션의 경우

의심스러운 트래픽이 UDP 세션에서 온 경우 WSA에서 유사한 동작을 수행하지만 TCP RST를 보내는 대신 L4TM은 ICMP 호스트 연결 불가 메시지(ICMP 유형 3 코드 1)를 클라이언트나 서버에 전송합니다.그러나 이러한 경우에는 ICMP 메시지에 호스트가 연결할 수 없으므로 패킷을 전송할 수 없다고 명시되어 있으므로 IP 스푸핑은 없습니다.이 경우 소스 IP는 WSA의 IP가 됩니다.

이러한 RST 및 ICMP 패킷은 구축에 따라 데이터 라우팅 테이블을 사용하여 WSA에서 M1, P1 또는 P2를 통해 전송됩니다.