Cisco WSA(Web Security Appliance)는 Skype 트래픽을 어떻게 처리합니까?

목차

질문:

Cisco WSA(Web Security Appliance)는 Skype 트래픽을 어떻게 처리합니까?

환경: Cisco WSA, Skype

Skype는 전용 VoIP(Internet Telephony) 네트워크입니다.Skype는 주로 P2P 프로그램으로 작동하므로 중앙 서버와 직접 통신하지 않고 작동합니다.Skype는 다양한 방법으로 연결을 시도하므로 특히 차단하기가 어려울 수 있습니다.

Skype는 다음 기본 설정으로 연결됩니다.

1. 임의의 포트 번호를 사용하여 다른 피어에 UDP 패킷을 직접 연결
2. 임의의 포트 번호를 사용하여 다른 피어에 TCP 패킷 전달
3. 포트 80 및/또는 포트 443을 사용하여 다른 피어에 TCP 패킷을 직접 연결
4. 포트 443에 HTTP CONNECT를 사용하여 웹 프록시를 통해 터널링된 패킷

명시적 프록시 환경에 구축할 경우 방법 1-3은 Cisco WSA에 전송되지 않습니다.Skype를 차단하려면 먼저 네트워크의 다른 위치에서 차단해야 합니다.다음을 사용하여 Skype 단계 1-3을 차단할 수 있습니다.

- 방화벽:NBAR를 사용하여 Skype 버전 1을 차단합니다. 자세한 내용은 http://ciscotips.wordpress.com/2006/06/07/how-to-block-skype/을 참조하십시오.
- Cisco IPS(ASA):Cisco ASA는 시그니처를 통해 Skype를 잠재적으로 탐지하고 차단할 수 있습니다.

Skype가 명시적 프록시를 사용하도록 다시 전환되면 Skype는 HTTP CONNECT 요청에 클라이언트 세부 정보를 의도적으로 제공하지 않습니다(사용자-에이전트 문자도 없음). 따라서 Skype와 유효한 CONNECT 요청을 구별하기가 어렵습니다.Skype는 항상 포트 443에 연결되며 대상 주소는 항상 IP 주소입니다.

예:

연결 10.129.88.111:443 HTTP/1.0
프록시 연결:유지

다음 액세스 정책은 IP 주소 및 포트 443과 일치하는 WSA를 통해 모든 CONNECT 요청을 차단합니다. 이는 모든 Skype 트래픽과 일치합니다.그러나 포트 443의 IP 주소로 터널링하려는 비 Skype 프로그램도 차단됩니다.

Skype 차단 - HTTPS 프록시가 비활성화된 명시적 환경

IP 및 포트 443 트래픽과 일치하도록 사용자 지정 URL 카테고리를 생성합니다.

1. "Security Manager" -> "Custom URL Categories" -> "Add Custom Category"로 이동합니다.
2. "범주 이름"을 입력하고 "고급"을 확장합니다.
3. 정규식 창에서 "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+"를 사용합니다.

액세스 정책에서 이 범주를 거부하도록 설정:

1. "Web Security Manager" -> "Access Policies(액세스 정책)"로 이동합니다.
2. 해당 정책 그룹에 대한 "URL Categories(URL 범주)" 열 아래의 링크를 클릭합니다.
3. "Custom URL Category Filtering(맞춤형 URL 카테고리 필터링)" 섹션에서 새 Skype 카테고리에 대해 "Block(차단)"을 선택합니다.
4. 변경 사항 제출 및 커밋

*참고:*HTTPS 프록시 서비스가 비활성화된 경우에만 명시적 CONNECT 요청을 차단할 수 있습니다!

WSA HTTPS 암호 해독이 활성화된 경우 Skype 트래픽이 순전히 HTTPS 트래픽이 아니므로 (CONNECT 및 포트 443을 사용하더라도) 중단될 수 있습니다. 그러면 WSA에서 502 오류가 생성되고 연결이 삭제됩니다.IP 주소에 대한 실제 HTTPS 웹 트래픽은 계속 작동합니다(WSA에서 해독되지만).

Skype 차단 - HTTPS 프록시가 활성화된 명시적/투명 환경

IP 및 포트 443 트래픽과 일치하도록 사용자 지정 범주를 만듭니다.

1. "Security Manager" -> "Custom URL Categories" -> "Add Custom Category"로 이동합니다.
2. "범주 이름"을 입력하고 "고급"을 확장합니다.
3. 정규식 창에서 "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+"를 사용합니다.

암호 해독 정책에서 이 범주를 암호 해독하도록 설정:

1. "Web Security Manager" -> "Decryption Policies"로 이동합니다.
2. 해당 정책 그룹에 대한 "URL Categories(URL 범주)" 열 아래의 링크를 클릭합니다.
3. "Custom URL Category Filtering(맞춤형 URL 카테고리 필터링)" 섹션에서 새 Skype 카테고리에 대해 "Decrypt(해독)"를 선택합니다.
4. 변경 사항을 제출하고 커밋합니다.

*참고:*Skype 트래픽은 IP로 전송되므로 "분류되지 않은 URL"의 일부로 간주됩니다. 작업이 해독할지 패스스루를 수행하는지에 따라 위와 같은 효과가 발생합니다.