외부 ESA-클라우드 SMA 동기화

목차

[소개](#)
[Q. 외부 ESA에서 클라우드 SMA로, 클라우드 ESA에서 외부 SMA로 어떤 연결이 허용됩니까?](#)

소개

Q. 외부 ESA에서 클라우드 SMA로, 클라우드 ESA에서 외부 SMA로 어떤 연결이 허용됩니까?

A. 보안 전용 포트 25 및 587이 데이터 센터의 CES 어플라이언스로 인바운드될 수 있습니다.데이터 센터로부터의 아웃바운드 연결은 제한되지 않으므로 모든 관련 서비스 포트가 허용됩니다.

참고:External(외부)은 Cisco 데이터 센터에서 호스팅되지 않는 모든 애플리케이션을 가리킵니다.

SMA는 SSH 포트 22를 사용하여 연결을 설정하여 ESA와 동기화합니다. 즉, SMA에서 연결이 초기화되므로 클라우드 SMA는 CES 데이터 센터 외부의 ESA와 동기화할 수 있습니다.

SMA와 ESA 간에 관리되는 중앙 집중식 서비스는 다음과 같습니다.

1. 보고(SMA에서 설정된 포트 22 연결을 통해 검색)

2. 메시지 추적(설정된 포트 22 연결을 통해 SMA에서 검색)

3. 스팸 격리(ESA에서 SMA로 포트 6025를 통해 전송)

4. 정책, 바이러스 및 전파 확산 격리(ESA에서 포트 7025를 통해 SMA로 전송)

데이터 센터 내의 SMA에서 SSH 포트 22 연결이 초기화되면 인터넷에서 데이터 센터로 반환 트래픽이 다시 허용되므로 보고 및 메시지 추적 서비스가 작동합니다.

스팸 쿼런틴 및 정책, 바이러스 및 Outbreak 격리 연결은 ESA에서 SMA로, 인터넷에서 데이터 센터로 열리지 않는 포트를 통해 초기화되므로 이 두 중앙 집중식 서비스가 작동하지 않습니다.

요약하자면, 외부 ESA 또는 ESA는 지원되는 보고 및 메시지 추적 서비스만 사용하여 클라우드 SMA와 동기화할 수 있습니다.

그 반대는 전혀 지원되지 않습니다.이는 클라우드 ESA가 외부 SMA와 동기화됩니다.포트 22의 SMA에서 동기화가 초기화되어 연결이 설정되고 포트 22가 인터넷에서 데이터 센터로 허용되지 않으므로 연결이 실패할 수 있습니다.모든 아웃바운드 포트가 열려 있으므로 포트 6025의 스팸 격리 서비스 및 포트 7025의 정책, 전파 확산 및 바이러스 격리 서비스에 대한 트래픽은 클라우드 ESA에서 외부 SMA로 전송할 수 있지만 초기 SSH 연결은 설정되지 않으므로 나머지 기능이 차단됩니다.