상호 운용되도록 Cisco Web Security Appliance 및 RSA DLP 네트워크를 구성하는 방법

목차

질문:

상호 운용되도록 Cisco Web Security Appliance 및 RSA DLP 네트워크를 구성하는 방법

개요:

이 문서에서는 고객이 두 제품을 상호 운영할 수 있도록 Cisco WSA AsyncOS 사용 설명서 및 RSA DLP 네트워크 7.0.2 구축 설명서 이외의 추가 정보를 제공합니다.

제품 설명:

Cisco WSA(Web Security Appliance)는 기업 보안을 손상시키고 지적 재산을 노출할 수 있는 웹 기반 악성코드 및 스파이웨어 프로그램으로부터 기업 네트워크를 보호하는 강력하고 안전하며 효율적인 장치입니다.Web Security Appliance는 HTTP, HTTPS 및 FTP와 같은 표준 통신 프로토콜에 대한 웹 프록시 서비스를 제공하여 심층적인 애플리케이션 콘텐츠 검사를 제공합니다.

RSA DLP Suite는 인프라 전반에 걸쳐 공통된 정책을 활용하여 데이터 센터, 네트워크, 엔드포인트에서 중요한 데이터를 검색하고 보호함으로써 기업의 중요한 데이터를 검색하고 보호할 수 있는 포괄적인 데이터 손실 방지 솔루션으로 구성되어 있습니다. DLP 제품군에는 다음 구성 요소가 포함됩니다.

- **RSA DLP 데이터 센터**.DLP Datacenter를 사용하면 데이터 센터, 파일 시스템, 데이터베이스, 이메일 시스템 및 대규모 SAN/NAS 환경에서 중요한 데이터를 찾을 수 있습니다.
- **RSA DLP 네트워크**.DLP 네트워크는 이메일 및 웹 트래픽과 같은 네트워크에서 중요한 정보의 전송을 모니터링하고 적용합니다.
- **RSA DLP 엔드포인트**.DLP 엔드포인트는 랩톱 및 데스크톱과 같은 엔드포인트에서 중요한 정보를 검색, 모니터링 및 제어할 수 있도록 지원합니다.

Cisco WSA는 RSA DLP 네트워크와 상호 운용 가능합니다.

RSA DLP 네트워크에는 다음 구성 요소가 포함됩니다.

- **네트워크 컨트롤러**.기밀 데이터 및 콘텐츠 전송 정책에 대한 정보를 유지 관리하는 기본 어플라이언스입니다.Network Controller는 초기 컨피그레이션 후 컨피그레이션의 변경 사항과 함께 정책 및 민감한 콘텐츠 정의를 사용하여 관리되는 디바이스를 관리하고 업데이트합니다.
- **관리되는 디바이스**.이러한 디바이스는 DLP 네트워크에서 네트워크 전송을 모니터링하고 전송을 보고하거나 차단하는 데 도움이 됩니다.

센서.네트워크 경계에 설치된 센서는 네트워크에서 나가는 트래픽 또는 네트워크 경계를 통과하는 트래픽을 수동적으로 모니터링하여 민감한 콘텐츠가 있는지 분석합니다.센서는 대역외 솔루션입니다.정책 위반을 모니터링하고 보고만 할 수 있습니다.**가로채기**.또한 네트워크 경계에 설치된 가로채기를 사용하면 민감한 콘텐츠가 포함된 이메일(SMTP) 트래픽의 격리 및/또는 거부를 구현할 수 있습니다.인터셉터는 인라인 네트워크 프록시이므로 민감한 데이터가 엔터프라이즈를 떠나는 것을 차단할 수 있습니다.**ICAP 서버**.민감한 콘텐츠가 포함된 HTTP, HTTPS 또는 FTP 트래픽의 모니터링 또는 차단을 구현할 수 있는 특수 목적의 서버 디바이스입니다.ICAP 서버는 프록시 서버(ICAP 클라이언트로 구성)와 함께 작동하여 민감한 데이터가 엔터프라이즈에서 나가는 것을 모니터링하거나 차단합니다.

Cisco WSA는 RSA DLP 네트워크 ICAP 서버와 상호 운용됩니다.

알려진 제한 사항

Cisco WSA External DLP integration with RSA DLP Network는 다음 작업을 지원합니다.허용 및 차단.아직 "Reaction(Reaction)이라고도 하는 Modify/Remove Content(콘텐츠 수정/제거)" 작업을 지원하지 않습니다.

상호 운용성을 위한 제품 요구 사항

Cisco WSA와 RSA DLP 네트워크의 상호 운용 기능은 다음 표에 나와 있는 제품 모델 및 소프트웨어 버전에서 테스트 및 검증되었습니다.기능적으로 말하면 이 통합은 모델 및 소프트웨어의 변형과 함께 작동할 수 있지만 다음 표는 테스트, 검증 및 지원되는 유일한 조합을 나타냅니다.지원되는 최신 버전의 두 제품을 모두 사용하는 것이 좋습니다.

제품	소프트웨어 버전
Cisco WSA(Web Security Appliance)	AsyncOS 버전 6.3 이상
RSA DLP 네트워크	7.0.2

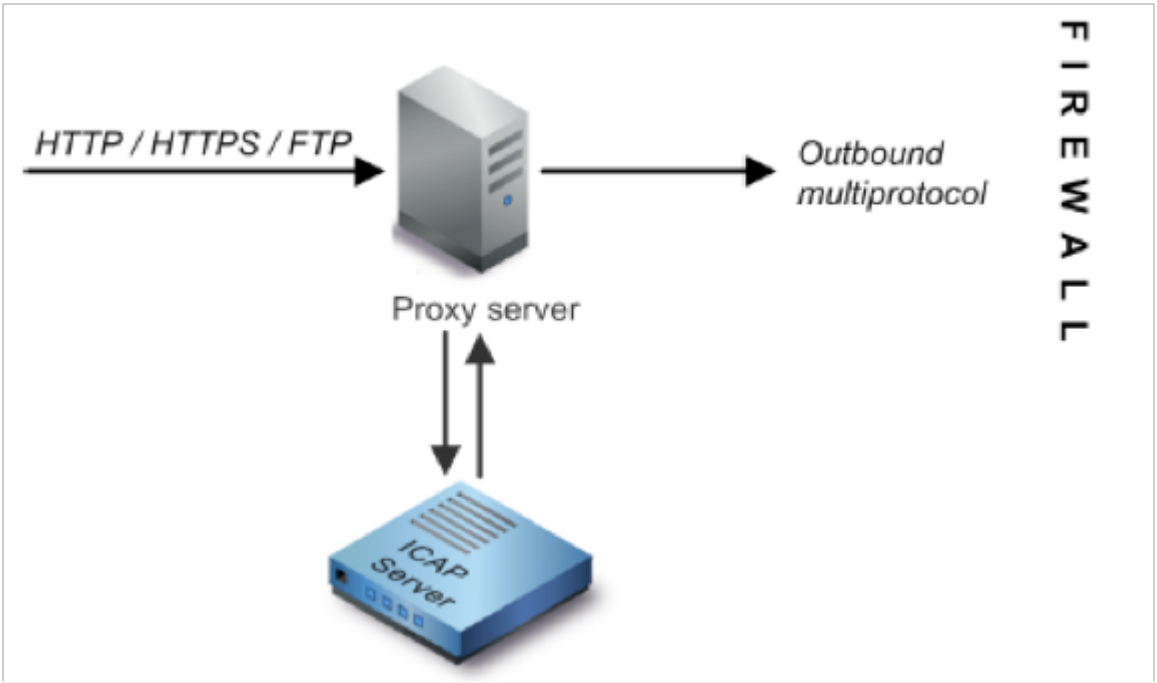
외부 DLP 기능

Cisco WSA의 External DLP(외부 DLP) 기능을 사용하여 WSA에서 DLP 네트워크로 전체 또는 특정 발신 HTTP, HTTPS 및 FTP 트래픽을 전달할 수 있습니다.모든 트래픽은 ICAP(Internet Control Adaptation Protocol)를 사용하여 전송됩니다.

아키텍처

RSA DLP Network Deployment Guide에는 프록시 서버를 사용하는 RSA DLP 네트워크 간 작동을 위한 다음과 같은 일반 아키텍처가 나와 있습니다.이 아키텍처는 WSA에 한정되지 않지만 RSA DLP 네트워크와 상호 작용하는 모든 프록시에 적용됩니다.

그림 1:RSA DLP 네트워크 및 Cisco Web Security Appliance용 구축 아키텍처



Cisco Web Security Appliance 구성

1. DLP 네트워크 ICAP 서버와 함께 작동하는 WSA에서 외부 DLP 시스템을 정의합니다.자세한 내용은 WSA 사용 설명서 "사용자 가이드 지침 외부 DLP 시스템 정의"에서 발췌한 첨부 부분을 참조하십시오.

2. 다음 단계를 사용하여 WSA에서 콘텐츠 검사를 위해 DLP 네트워크에 보내는 트래픽을 정의하는 하나 이상의 외부 DLP 정책을 생성합니다.

- GUI > **Web Security Manager > External DLP policies(외부 DLP 정책) > Add Policy(정책 추가)에서**
- 구성하려는 정책 그룹의 ***Destinations(대상)*** 열 아래의 링크를 클릭합니다.
- 'Edit Destination Settings'(대상 설정 수정) 섹션에서 ?Define Destinations Scanning Custom Settings(대상 검사 사용자 지정 설정 정의)를 선택합니다.드롭다운 메뉴에서
- 그런 다음 'Scan all uploads'(모든 업로드 검사) 또는 맞춤형 URL 카테고리에 지정된 특정 도메인/사이트에 대한 업로드를 스캔하도록 정책을 구성할 수 있습니다.

RSA DLP 네트워크 구성

이 문서에서는 RSA DLP 네트워크 컨트롤러, ICAP 서버 및 Enterprise Manager가 설치 및 구성되어 있다고 가정합니다.

1. RSA DLP Enterprise Manager를 사용하여 네트워크 ICAP 서버를 구성합니다.DLP 네트워크 ICAP 서버 설정에 대한 자세한 지침은 RSA DLP 네트워크 구축 가이드를 참조하십시오.ICAP 서버 컨피그레이션 페이지에서 지정해야 하는 기본 매개변수는 다음과 같습니다. ICAP 서버의 호스트 이름 또는 IP 주소입니다.컨피그레이션 페이지의 **General** Settings(일반 설정) 섹션에 다음 정보를 입력합니다. Server Timeout in Seconds 필드에서 서버가 시간 초과된 것으로 간주되는 시간(초)**입니다**.다음 중 하나를 **서버 시간 초과 시 응답으로 선택합니다.열기 실패**

.서버 시간 초과 후 전송을 허용하려면 이 옵션을 선택합니다.**실패** 닫힘서버 시간 초과 후 전송을 차단하려면 이 옵션을 선택합니다.

2. RSA DLP Enterprise Manager를 사용하여 하나 이상의 네트워크별 정책을 생성하여 민감한 콘텐츠가 포함된 네트워크 트래픽을 감사 및 차단합니다.DLP 정책 생성에 대한 자세한 지침은 RSA DLP 네트워크 사용 설명서 또는 Enterprise Manager 온라인 도움말을 참조하십시오. 수행할 주요 단계는 다음과 같습니다. 정책 템플릿 라이브러리에서 하나 이상의 정책을 활성화하여 사용자 환경과 모니터링할 콘텐츠를 적절하게 활용할 수 있습니다.이 정책 내에서 이벤트(정책 위반)가 발생할 때 네트워크 제품이 자동으로 수행할 작업을 지정하는 DLP 네트워크별 정책 위반 규칙을 설정합니다.모든 프로토콜을 탐지하도록 정책 탐지 규칙을 설정합니다.정책 작업을 "audit and block"으로 설정합니다.

선택적으로 RSA Enterprise Manager를 사용하여 정책 위반이 발생할 때 사용자에게 전송되는 네트워크 알림을 사용자 정의할 수 있습니다. 이 알림은 DLP Network에서 원래 트래픽의 대체 항목으로 전송됩니다.

설정 테스트

1. 브라우저에서 발신 트래픽을 WSA 프록시로 직접 이동하도록 브라우저를 구성합니다.

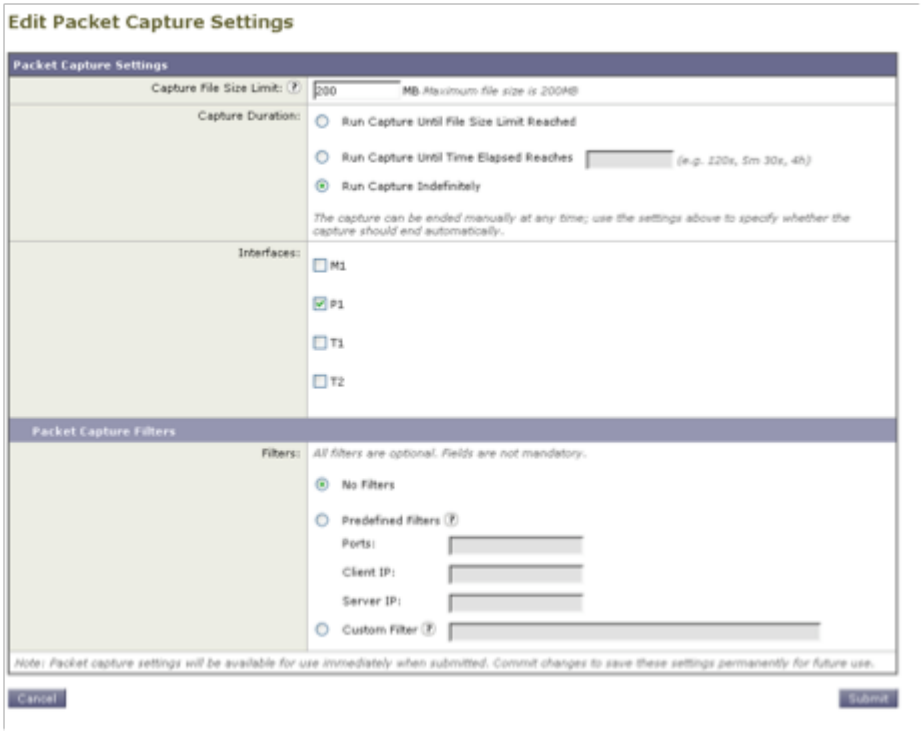
   예를 들어 Mozilla FireFox 브라우저를 사용하는 경우 다음을 수행합니다. FireFox 브라우저에서 **도구 > 옵션**을 선택합니다.옵션 대화 상자가 나타납니다.**네트워크** 탭을 클릭한 다음 **설정**을 클릭합니다.Connection Settings 대화 상자가 나타납니다.Manual **Proxy Configuration(수동 프록시 컨피그레이션**) 확인란을 선택한 다음 **HTTP Proxy** 필드에 WSA 프록시 서버의 IP 주소 또는 호스트 이름과 포트 번호 3128(기본값)을 입력합니다.OK(**확인**)를 클릭한 다음 **OK(확인)**를 다시 클릭하여 새 설정을 저장합니다.
2. 이전에 활성화한 DLP 네트워크 정책을 위반하는 일부 콘텐츠를 업로드하려고 시도합니다.
3. 브라우저에 네트워크 ICAP 폐기 메시지가 표시됩니다.
4. 'Enterprise Manager'를 사용하여 이 정책 위반으로 생성된 결과 이벤트 및 인시던트를 볼 수 있습니다.

문제 해결

1. RSA DLP 네트워크에 대해 Web Security Appliance에서 외부 DLP 서버를 구성할 때 다음 값을 사용합니다.

   서버 주소:RSA DLP 네트워크 ICAP 서버의 IP 주소 또는 호스트 이름포트:RSA DLP 네트워크 서버에 액세스하는 데 사용되는 TCP 포트(일반적으로 **1344)**서비스 URL 형식 :**icap://*<hostname_or_ipaddress>*/srv_conalarm**예:icap://dlp.example.com/srv_conalarm
2. WSA의 트래픽 캡처 기능을 활성화하여 WSA 프록시와 네트워크 ICAP 서버 간의 트래픽을 캡처합니다.이는 연결 문제를 진단할 때 유용합니다.이렇게 하려면 다음을 수행합니다.

   WSA GUI에서 사용자 인터페이스 오른쪽 상단**의 Support and Help**(지원 및 도움말) 메뉴로 이동합니다.메뉴에서 **Packet Capture**를 선택한 다음 Edit **Settings** 버튼을 클릭합니다.Edit Capture Settings 창이 나타납니다.



화면의 **Packet Capture** Filters 섹션에서 Server **IP** 필드에 Network ICAP 서버의 IP 주소를 입력합니다.Submit(**제출**)을 클릭하여 변경 사항을 저장합니다.

3. WSA 액세스 로그(Under ***GUI > System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션)> 액세스 로그***)에서 다음 사용자 지정 필드를 사용하여 자세한 내용을 확인하십시오.
   %XP:외부 DLP 서버 스캐닝 판정(0 = ICAP 서버에 일치하지 않음;1 = ICAP 서버에 대한 정책 일치 및 '-(하이픈)' = 외부 DLP 서버에서 검사를 시작하지 않음

[사용자 설명서 외부 DLP 시스템 정의 지침.]

_