如何配置思科Web安全工具和RSA DLP网络兼容？

目录

问题：

如何配置思科Web安全工具和RSA DLP网络兼容？

概述：

本文提供在思科WSA AsyncOS用户指南和RSA DLP网络7.0.2部署指南之外的额外信息帮助客户兼容两产品。

产品描述：

思科Web安全工具(WSA)是保护公司网络以防止基于Web的恶意软件和间谍软件程序能减弱公司安全和曝光知识产权的一个稳健，安全，高效设备。Web安全工具通过提供Web代理服务提供深刻的应用程序内容检验为标准的通信协议例如HTTP、HTTPS和FTP。

RSA DLP套件包括在企业中使客户通过有效利用在基础设施间的普通政策发现和保护敏感数据发现和保护敏感数据在datacenter，在网络和在终端的一全面的数据丢失预防解决方案。 DLP套件包括以下组件：

- **RSA DLP Datacenter**。DLP Datacenter帮助您找出敏感数据，不管哪里位于datacenter，在文件系统、数据库、电子邮件系统和大SAN/NAS环境。
- **RSA DLP网络**。DLP网络监控器和强制执行敏感信息发射关于网络的，例如电子邮件和Web流量。
- **RSA DLP终端**。DLP终端帮助您发现，监控和控制关于终端的敏感信息例如膝上型计算机和桌面。

思科WSA有能力与RSA DLP网络兼容。

RSA DLP网络包括以下组件：

- **网络控制器**。维护关于机要数据和内容传输策略的信息的主要设备。网络控制器管理并且更新有策略的受管理设备，并且与其中任一一起的敏感内容定义变成他们的配置在初始配置以后。
- **受管理设备**。这些设备帮助DLP网络监控器网络发射并且报告或者拦截发射：
  传感器。安装在网络边界，传感器被动地监控离开网络或超过网络边界的流量，分析它对于敏感内容出现。传感器是一带外解决方案;它能只监控并且报告策略违反。**拦截机**。并且安装在网络边界，拦截机允许您实现的电子邮件(SMTP)流量检疫并且/或者拒绝包含敏感内容。拦截机

是一个轴向网络代理并且能阻塞从留下企业的敏感数据。**ICAP服务器**。专用允许您实现监听或阻塞包含敏感内容的HTTP、HTTPS或者FTP流量的服务器设备。ICAP服务器与代理服务器一起使用(配置作为ICAP客户端)监控或阻塞从留下企业的敏感数据

思科WSA与RSA DLP网络ICAP服务器兼容。

已知限制

与RSA DLP网络的思科WSA外部DLP集成支持以下操作：准许并且阻塞。它不支持“修改/删除使”(也呼叫Redaction)操作满意。

互通性的产品需求

思科WSA和RSA DLP网络的互用性用产品模式和软件版本测试并且验证在下表里。当功能发言此集成可能与变化一起使用到型号和软件时，下表代表唯一的测试的，验证的和支持的组合。严格推荐使用两产品最新的支持的版本。

产品	软件版本
思科Web安全工具(WSA)	AsyncOS版本6.3 &上述
RSA DLP网络	7.0.2

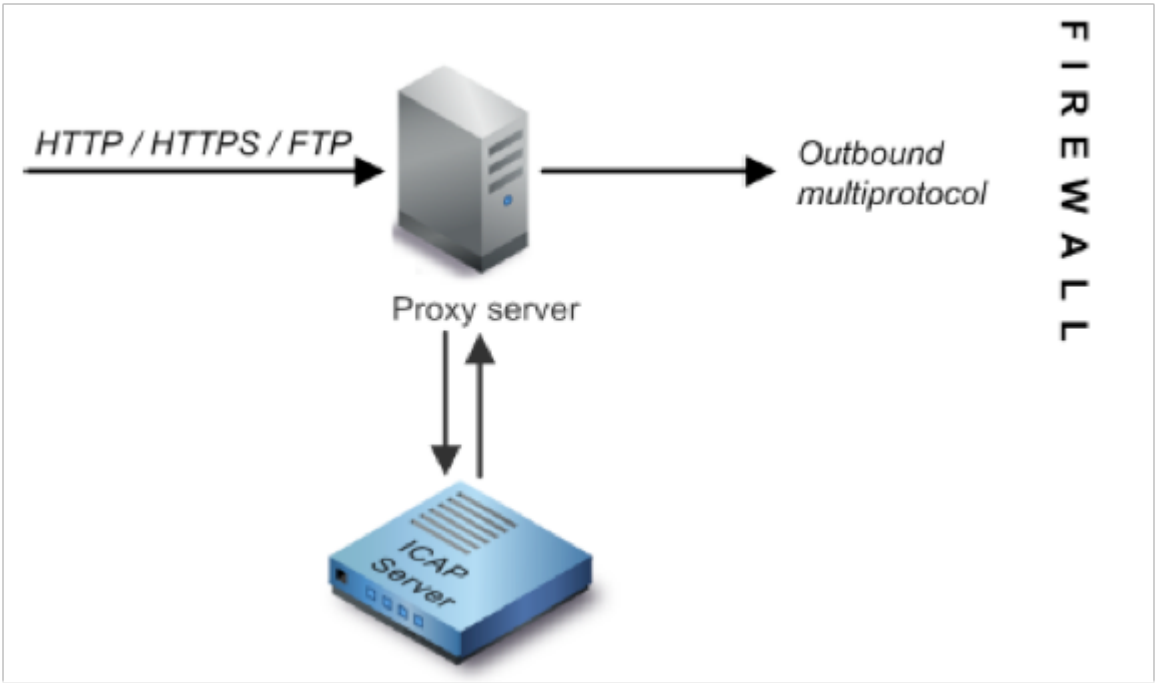
外部DLP功能

使用思科WSA，您的外部DLP功能能转发所有或特定流出的HTTP、HTTPS和FTP流量从WSA到DLP网络。使用互联网控制适应协议(ICAP)，所有流量转接。

体系结构

RSA DLP网络部署指南显示兼容的RSA DLP网络以下通用的体系结构用代理服务器。此体系结构不是特定对WSA，然而适用于与RSA DLP网络兼容的所有代理。

图 1：RSA DLP网络和思科Web安全工具的部署体系结构



配置思科Web安全工具

1. 定义在与DLP网络ICAP服务器一起使用的WSA的外部DLP系统。关于说明，请参阅摘自WSA用户指南“用户指南说明的附加的部分定义外部DLP系统”。

2. 创建使用下面的步骤，定义了流量WSA发送对内容扫描的DLP网络的一个或更多外部DLP策略：

- 下面**GUI > Web安全经理>外部DLP策略>**Add**策略**
- 单击链路在您要配置的策略组的目的地列下
- 在下‘编辑目的地设置部分，选择？定义扫描自定义设置的目的地？从下拉菜单
- 我们能然后配置策略‘扫描所有加载’或扫描加载到在自定义URL类别/站点指定的某些域

配置RSA DLP网络

本文假设， RSA DLP网络控制器、ICAP服务器和企业管理器安装并且配置。

1. 请使用RSA DLP企业管理器配置网络ICAP服务器。关于关于设置您的DLP网络ICAP服务器的更多的指导信息，参考RSA DLP网络部署指南。您在ICAP Server Configuration页应该指定的主要参数是： ICAP服务器的主机名或IP地址。在配置页的**一般**设置部分，请输入以下信息：在秒钟，在后服务器的时间**在秒钟**字段视为计时了在**服务器超时**。选择其中一以下作为答复**在服务器超时**：**出故障开放**。如果要在服务器超时以后，允许发射请选择此选项。**关闭的失败**。如果希望到街区传输在服务器超时以后，请选择此选项。
2. 请使用RSA DLP企业管理器创建一个或更多网络细节的策略审计和阻塞包含敏感内容的网络流量。对于创建的DLP策略更多的指导信息，参考RSA DLP网络用户指南或企业Manageronline帮助。 实行的主要步骤下列： 从策略模板库enable (event)有您的环境和内容的意义您至少的一项策略监控。在该策略内，指定操作网络产品的设置的DLP网络细节的策略违反规则将自动地实行，当事件(策略违反)发生。设置策略检测规则检测所有协议。设置策略

操作“审计和阻塞”。

*随意地*我们能使用RSA企业管理器定制发送给用户的网络通知，当策略违反发生时。 此通知通过DLP网络发送作为原始流量的一更换。

测试设置

1. 配置您的浏览器处理从您的浏览器的流出流量去直接地WSA代理。

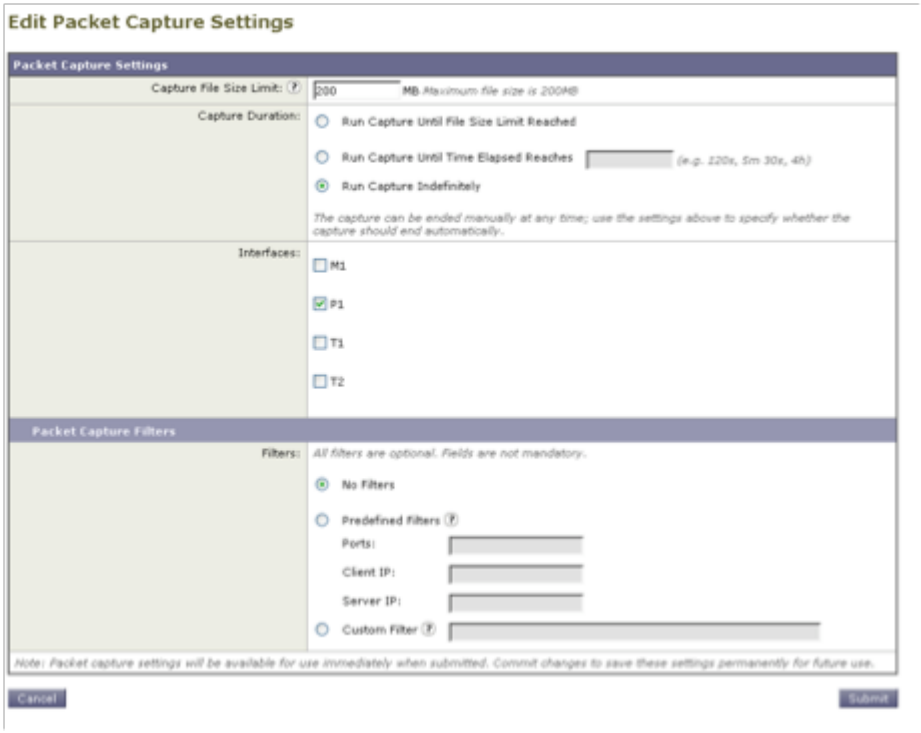
   例如，如果使用Mozilla Firefox浏览器，请执行以下： 在Firefox浏览器中，请选择**Tools>选项**。选项对话出现。点击**Network选项**，然后点击**设置**。连接设置对话出现。选择**手工代理配置**复选框，然后进入WSA代理服务器的IP地址或主机名在**HTTP代理**字段和端口号3128 (默认)的。再点击OK键，然后**好**保存新的设置。
2. 尝试上传您知道是违反DLP网络策略您以前启用的某内容。
3. 您应该看到在浏览器的网络ICAP丢弃消息。
4. 请使用‘企业管理器’查看由于策略的此侵害，创建的发生的事件和事件。

排除故障

1. 当配置在Web安全工具的一个外部DLP服务器RSA DLP网络的时，请使用以下值：

   服务器地址:RSA DLP网络ICAP服务器的IP地址或主机名波尔特：用于的TCP端口访问RSA DLP网络服务器，典型地**1344**服务URL格式：**icap:// *<主机名_or_ipaddress>/srv_conalarm*示例：**icap://dlp.example.com/srv_conalarm
2. 启用捕获WSA的功能流量捕获WSA代理和网络ICAP服务器之间的流量。当诊断连通性问题时，这是有用。要执行此，请执行以下：

   在WSA GUI，请去**支持和Help菜单**在用户界面的右上。选择从菜单的**数据包捕获**，然后点击**EDIT SETTINGS按钮**。Settings窗口编辑的捕获出现。



在屏幕的**数据包捕获**过滤器部分，请在**服务器IP**字段输入网络ICAP服务器的IP地址。单击 Submit 以保存更改。

3. 请使用以下自定义字段在WSA访问日志(在*GUI >System Administration >日志订阅> accesslog下*)获得更多信息：
   %Xp ：外部DLP服务器扫描判决(0 =在ICAP服务器的没有匹配;1 = ICAP服务器的策略匹配和‘- (连字符)’ =扫描未由外部DLP服务器启动)

[定义外部DLP系统的用户指南说明。](#)