如何配置思科网络安全设备和RSA DLP网络以实现互操作？

目录

问题：

如何配置思科网络安全设备和RSA DLP网络以实现互操作？

概述:

本文档提供除《Cisco WSA AsyncOS用户指南》和《RSA DLP网络7.0.2部署指南》之外的其他信息，以帮助客户实现两种产品的互操作。

产品描述：

思科网络安全设备(WSA)是一款强大、安全、高效的设备，可保护企业网络免受基于Web的恶意软件和间谍软件程序的侵扰，这些程序可能危害企业安全并暴露知识产权。网络安全设备通过为标准通信协议（如HTTP、HTTPS和FTP）提供Web代理服务，提供深度应用内容检测。

RSA DLP Suite包含全面的防数据丢失解决方案，通过利用整个基础架构中的通用策略发现和保护数据中心、网络和端点中的敏感数据，客户可以发现和保护企业中的敏感数据。 DLP套件包括以下组件：

- **RSA DLP数据中心**。DLP数据中心可帮助您在数据中心内的任何位置、文件系统、数据库、电子邮件系统和大型SAN/NAS环境中定位敏感数据。
- **RSA DLP网络**。DLP网络监控并强制在网络上传输敏感信息，例如邮件和网络流量。
- **RSA DLP终端**。DLP终端可帮助您发现、监控和控制笔记本电脑和台式机等终端上的敏感信息。

Cisco WSA能够与RSA DLP网络进行互操作。

RSA DLP网络包括以下组件：

- **网络控制器**。维护有关机密数据和内容传输策略的信息的主设备。网络控制器使用策略和敏感内容定义以及初始配置后对其配置的任何更改来管理和更新受管设备。
- **受管设备**。这些设备可帮助DLP网络监控网络传输并报告或拦截传输：
  传感器。传感器安装在网络边界，被动监控离开网络或跨网络边界的流量，分析其是否存在敏感内容。传感器是带外解决方案；它只能监控和报告策略违规。**拦截器**。拦截器也安装在网络边界，它允许您对包含敏感内容的邮件(SMTP)流量实施隔离和/或拒绝。侦听器是内联网络代理，因此可以阻止敏感数据离开企业。**ICAP服务器**。专用服务器设备，允许您对包含敏感内容

的HTTP、HTTPS或FTP流量进行监控或阻止。ICAP服务器与代理服务器（配置为ICAP客户端）一起工作，以监控或阻止敏感数据离开企业Cisco WSA与RSA DLP网络ICAP服务器互操作。

已知限制

Cisco WSA外部DLP与RSA DLP网络的集成支持以下操作：允许和阻止。它尚不支持“修改/删除内容”（也称为密文）操作。

互操作性产品要求

思科WSA和RSA DLP网络的互操作性已通过下表中的产品型号和软件版本进行测试和验证。虽然从功能上讲，此集成可能与型号和软件的不同版本配合使用，但下表是唯一经过测试、验证和支持的组合。强烈建议使用两个产品的最新支持版本。

产品	软件版本
思科网络安全设备(WSA)	AsyncOS版本6.3及更高版本
RSA DLP网络	7.0.2

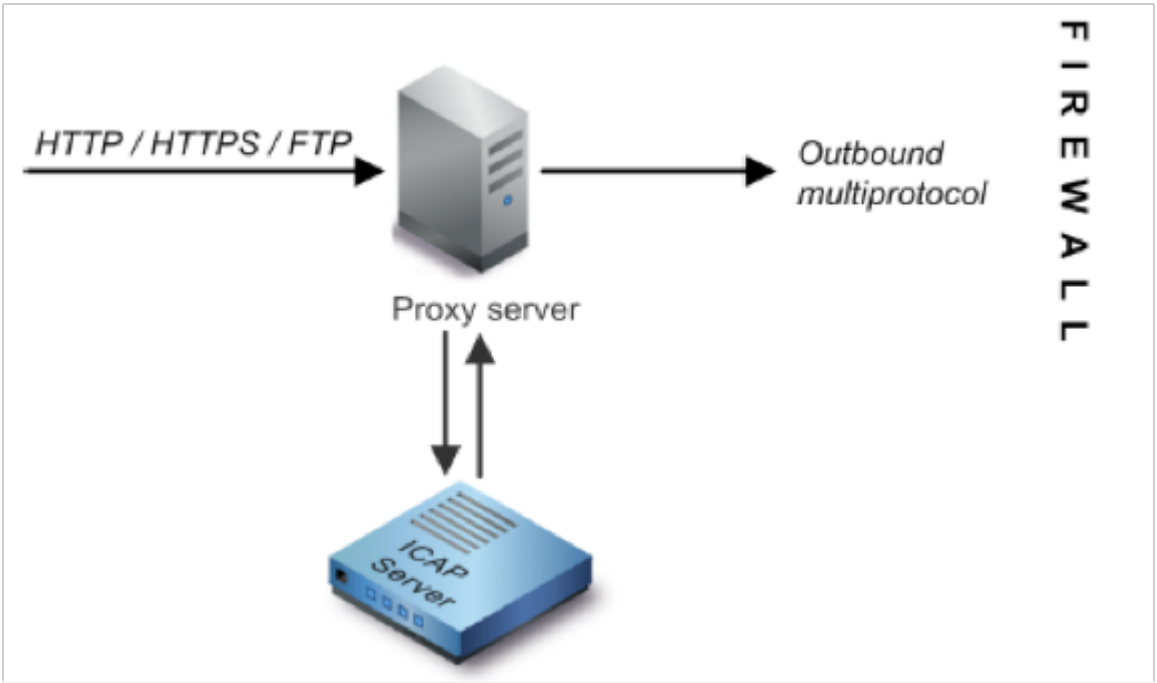
外部DLP功能

使用Cisco WSA的外部DLP功能，您可以将所有或特定的传出HTTP、HTTPS和FTP流量从WSA转发到DLP网络。所有流量都使用互联网控制自适应协议(ICAP)传输。

架构

《RSA DLP网络部署指南》显示了以下用于与代理服务器进行RSA DLP网络间操作的通用架构。此架构不是特定于WSA的，而是适用于与RSA DLP网络互操作的任何代理。

图 1：RSA DLP网络和思科网络安全设备的部署架构



配置思科网络安全设备

1. 在WSA上定义与DLP网络ICAP服务器配合使用的外部DLP系统。有关说明，请参阅随附的WSA用户指南“定义外部DLP系统的用户指南说明”摘要。

2. 创建一个或多个外部DLP策略，这些策略定义WSA发送到DLP网络以进行内容扫描的流量，步骤如下：

- 在“GUI”(GUI)>“Web安全管理器”(Web Security Manager)>“外部DLP策略”(External DLP policies)>“添加策略”(Add Policy)下
- 单击要配置的策略组的*目标*列下的链接
- 在“编辑目标设置”(Edit Destination Settings)部分下，选择定义目标扫描自定义设置(Define Destinations Scanning Custom Settings?)下拉菜单
- 然后，我们可以将策略配置为“扫描所有上传”或扫描上传到自定义URL类别中指定的某些域/站点

配置RSA DLP网络

本文档假设已安装并配置RSA DLP网络控制器、ICAP服务器和企业管理器。

1. 使用RSA DLP Enterprise Manager配置网络ICAP服务器。有关设置DLP网络ICAP服务器的详细说明，请参阅《RSA DLP网络部署指南》。您应在ICAP服务器配置页面上指定的主要参数为： ICAP服务器的主机名或IP地址。在配置页的“常规设置”部分，输入以下信息： 在Server Timeout in Seconds字段中，服务器被视为已超时的时间量(秒)。选择以下选项之一作为On Server Timeout的响应:失效开放。如果要在服务器超时后允许传输，请选择此选项。关闭失败.如果要在服务器超时后阻止传输，请选择此选项。
2. 使用RSA DLP企业管理器创建一个或多个特定于网络的策略，以审核和阻止包含敏感内容的网络流量。有关创建DLP策略的详细说明，请参阅《RSA DLP网络用户指南》或“企业管理器

在线帮助”。 执行的主要步骤如下： 从策略模板库至少启用一个对您的环境和您将监控的内容有意义的策略。在该策略中，设置DLP网络特定策略违规规则，指定网络产品在发生事件（策略违规）时自动执行的操作。设置策略检测规则以检测所有协议。将策略操作设置为“审核并阻止”。

或者，我们可以使用RSA Enterprise Manager自定义在发生策略违规时发送给用户的网络通知。此通知由DLP网络发送，作为原始流量的替代。

测试设置

1. 将浏览器配置为将传出流量从浏览器定向到WSA代理。

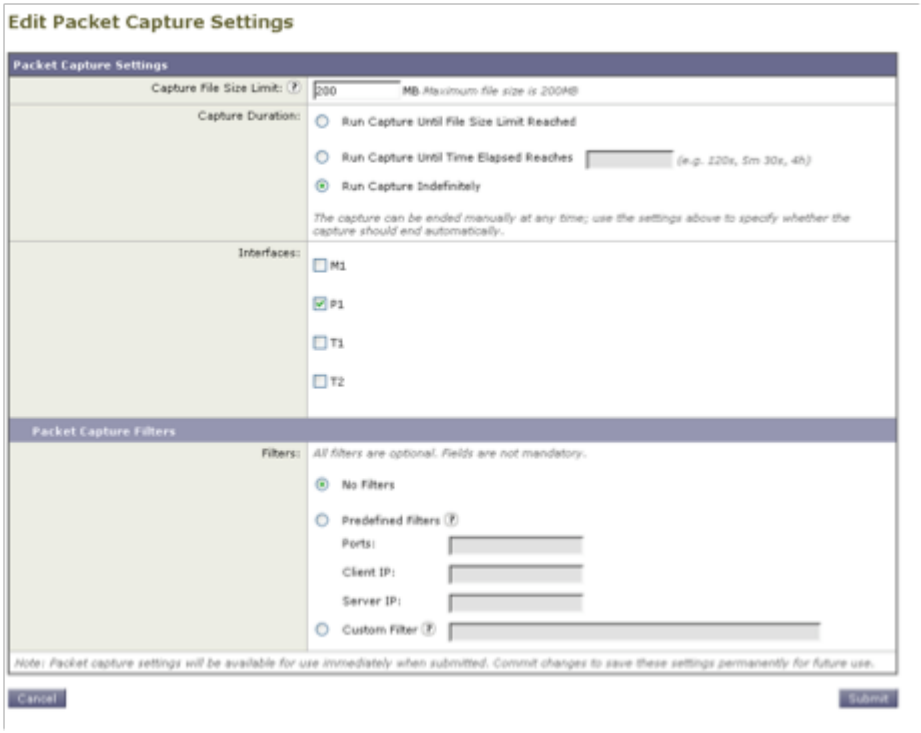
   例如，如果您使用Mozilla FireFox浏览器，请执行以下操作： 在FireFox浏览器中，选择“工**具**”>“**选项**”。系统将显示“选项”对话框。单击“Network(网**络)**”选项卡，然后单击“**Settings(设**置)”。系统将显示Connection Settings对话框。选中**Manual Proxy Configuration**复选框，然后在**HTTP Proxy**字段中输入WSA代理服务器的IP地址或主机名，并输入端**口号3128(**默认值)。再次**单击**“确定”，保存新设置。
2. 尝试上传一些您知道的内容违反了您之前启用的DLP网络策略。
3. 您应在浏览器中看到Network ICAP discard消息。
4. 使用“Enterprise Manager”查看因此违反策略而产生的事件和事件。

故障排除

1. 在网络安全设备上为RSA DLP网络配置外部DLP服务器时，请使用以下值：

   服务器地址:RSA DLP网络ICAP服务器的IP地址或主机名端口：用于访问RSA DLP网络服务器的TCP端口，通常为**1344**服务URL格式：**icap://*<hostname_or_ipaddress>*/srv_conalarm**示例：icap://dlp.example.com/srv_conalarm
2. 启用WSA的流量捕获功能，以捕获WSA代理和网络ICAP服务器之间的流量。这在诊断连接问题时非常有用。为此，请执行以下操作：

   在WSA GUI上，转到用**户界面**右上角的“支持和帮助”菜单。从菜**单中选**择Packet Capture，然后单击Edit **Settings**按钮。系统将显示Edit Capture Settings窗口。



在屏幕的Packet Capture Filters部分，在Server IP（服务器IP）字段中输入Network ICAP服务器的IP地址。单击 Submit 以保存更改。

3. 使用WSA访问日志中的以下自定义字段(在*GUI > System Administration > Log Subscriptions > accesslogs*下)获取详细信息：
   %xp:外部DLP服务器扫描判定(0 = ICAP服务器上没有匹配项；1 =针对ICAP服务器的策略匹配，“ — （连字符）” =外部DLP服务器未启动扫描)

[用户指南定义外部DLP系统说明。]

_