如何將思科網路安全裝置和RSA DLP網路配置為互操作？

目錄

問題：

如何將思科網路安全裝置和RSA DLP網路配置為互操作？

概觀:

本文檔提供除《Cisco WSA AsyncOS使用手冊》和《RSA DLP網路7.0.2部署指南》之外的額外資訊，以幫助客戶實現兩種產品的互操作。

產品描述：

思科網路安全裝置(WSA)是一種強大、安全、高效的裝置，可保護企業網路免受可能危害企業安全和洩露智慧財產權的基於Web的惡意軟體和間諜軟體程式的攻擊。Web安全裝置通過為HTTP、HTTPS和FTP等標準通訊協定提供Web代理服務來提供深度應用內容檢測。

RSA DLP套件包括全面的資料丟失防護解決方案，該解決方案使客戶能夠利用整個基礎架構中的通用策略來發現和保護企業中的敏感資料，從而發現和保護資料中心、網路和終端上的敏感資料。DLP套件包括以下元件：

- **RSA DLP資料中心**。DLP資料中心可幫助您定位敏感資料，無論它位於資料中心的哪個位置，在檔案系統、資料庫、電子郵件系統和大型SAN/NAS環境中。
- **RSA DLP網路**。DLP網路監控並強制在網路上傳輸敏感資訊，例如電子郵件和網路流量。
- **RSA DLP終結點**。DLP端點可幫助您發現、監控和控制終端上的敏感資訊，例如筆記型電腦和台式機。

Cisco WSA能夠與RSA DLP網路進行互操作。

RSA DLP網路包括以下元件：

- **網路控制器**。維護機密資料和內容傳輸策略相關資訊的主裝置。網路控制器使用策略和敏感內容定義以及初始配置後對其配置的任何更改來管理和更新受管裝置。
- **受管裝置**。這些裝置幫助DLP網路監控網路傳輸並報告或攔截傳輸：
  感測器。感測器安裝在網路邊界上，被動地監控離開網路或跨越網路邊界的通訊量，分析其是否存在敏感內容。感測器是一種帶外解決方案；它只能監控和報告策略違規。**攔截器**。攔截器還安裝在網路邊界上，允許您對包含敏感內容的電子郵件(SMTP)流量實施隔離和/或拒絕。攔截器是內嵌網路代理，因此可以阻止敏感資料離開企業。**ICAP伺服器**。可用於實施監控或阻止

包含敏感內容的HTTP、HTTPS或FTP流量的特殊用途伺服器裝置。ICAP伺服器與代理伺服器（配置為ICAP客戶端）配合工作，監控或阻止敏感資料離開企業Cisco WSA與RSA DLP網路ICAP伺服器互動操作。

已知限制

Cisco WSA外部DLP與RSA DLP網路整合支援以下操作：允許和阻止。它還不支援「修改/刪除內容」（也稱為密文）操作。

互操作性產品要求

思科WSA和RSA DLP網路的互操作性已經過測試，並使用下表中的產品型號和軟體版本進行了驗證。雖然從功能上說，這種整合可以與型號和軟體的變體一起使用，但下表僅顯示了經過測試、驗證和支援的組合。強烈建議同時使用這兩個產品的最新受支援版本。

產品	軟體版本
思科網路安全裝置(WSA)	AsyncOS 6.3及更高版本
RSA DLP網路	7.0.2

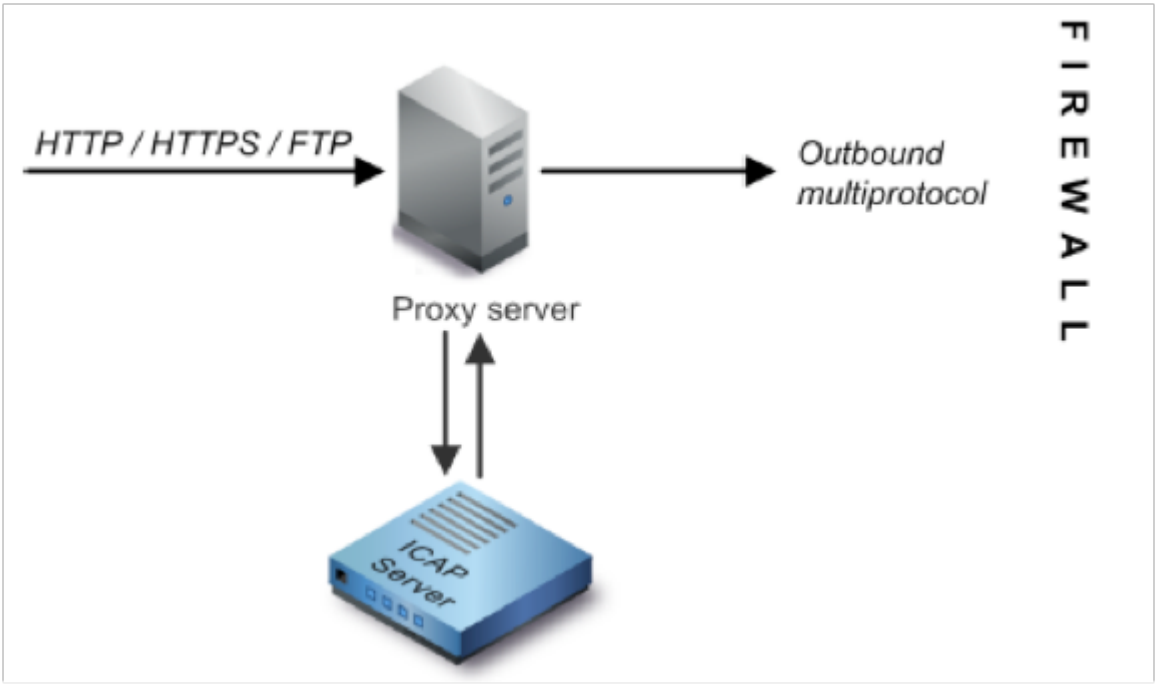
外部DLP功能

使用Cisco WSA的外部DLP功能，可以將所有或特定傳出HTTP、HTTPS和FTP流量從WSA轉發到DLP網路。所有流量均使用網際網路控制適配協定(ICAP)傳輸。

架構

《RSA DLP網路部署指南》顯示了以下通用體系結構，用於與代理伺服器互操作RSA DLP網路。此體系結構不是特定於WSA，但它適用於與RSA DLP網路互動操作的任何代理。

圖1:RSA DLP網路和思科網路安全裝置的部署體系結構



配置思科網路安全裝置

1. 在WSA上定義一個與DLP網路ICAP伺服器配合使用的外部DLP系統。有關說明，請參閱附加的WSA使用手冊「定義外部DLP系統的使用手冊說明」摘錄。

2. 使用以下步驟建立一個或多個外部DLP策略，該策略定義WSA傳送到DLP網路以進行內容掃描的流量：

- 在**GUI > Web Security Manager > External DLP policies > Add Policy**下
- 點選要配置的策略組的***目標***列下的連結
- 在「編輯目標設定」部分下，選擇「定義目標掃描自定義設定」。從下拉選單中
- 然後，我們可以將策略配置為「掃描所有上傳」，或者將上傳掃描到在自定義URL類別中指定的某些域/站點

配置RSA DLP網路

本文檔假設已安裝和配置RSA DLP網路控制器、ICAP伺服器和企業管理器。

1. 使用RSA DLP企業管理器配置網路ICAP伺服器。有關設定DLP網路ICAP伺服器的詳細說明，請參閱《RSA DLP網路部署指南》。您應在ICAP伺服器配置頁面上指定的主要引數包括：ICAP伺服器的主機名或IP地址。在配置頁的**General Settings**部分中，輸入以下資訊： 在**Server Timeout in Seconds**欄位中認為伺服器已超時的**時間(秒)**。選擇以下選項之一作為**伺服器超時**時的響應:**失效開放**。如果要在伺服器超時後允許傳輸，請選擇此選項。**失效關閉**。如果要在伺服器超時後阻止傳輸，請選擇此選項。
2. 使用RSA DLP企業管理器建立一個或多個特定於網路的策略，以稽核和阻止包含敏感內容的網路流量。有關建立DLP策略的詳細說明，請參閱《RSA DLP網路使用手冊》或Enterprise Manager聯機幫助。 要執行的主要步驟如下： 從策略模板庫啟用至少一個對您的環境和要監控的內容有意義的策略。在該策略中，設定DLP網路特定策略違規規則，這些規則指定發生事

件（違反策略）時，網路產品將自動執行的操作。設定策略檢測規則以檢測所有協定。將策略操作設定為「稽核並阻止」。

或者，我們可以使用RSA Enterprise Manager自定義在發生策略違規時傳送給使用者的網路通知。此通知由DLP網路作為原始流量的替代項傳送。

測試設定

1. 將瀏覽器配置為將來自瀏覽器的傳出流量直接轉到WSA代理。

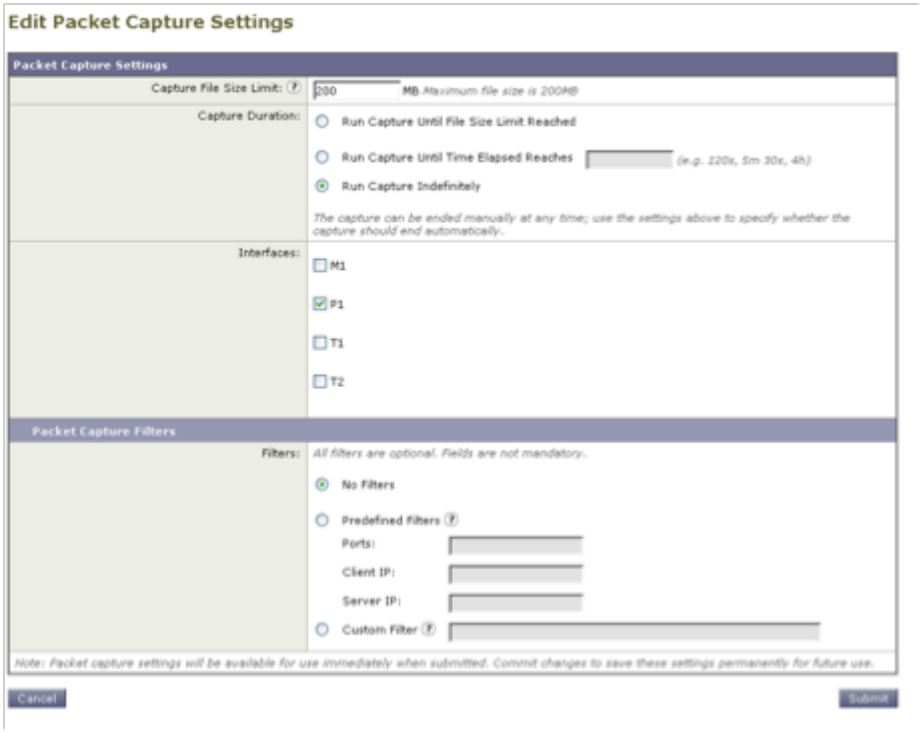
   例如，如果您使用Mozilla FireFox瀏覽器，請執行以下操作： 在FireFox瀏覽器中，選擇**「工具」>「選項」**。此時將顯示「選項」對話方塊。按一下**Network**頁籤，然後按一下**Settings**。出現「Connection Settings（連線設定）」對話方塊。選中**Manual Proxy Configuration**覈取方塊，然後在**HTTP Proxy**欄位中輸入WSA代理伺服器的IP地址或主機名以及埠號3128（預設值）。按一下「**OK**」，然後「**OK**」以儲存新設定。
2. 嘗試上載您知道違反您先前啟用的DLP網路策略的一些內容。
3. 您應在瀏覽器中看到網路ICAP丟棄消息。
4. 使用「Enterprise Manager」可以檢視由此違反策略而建立的結果事件和事件。

疑難排解

1. 在網路安全裝置上為RSA DLP網路配置外部DLP伺服器時，請使用以下值：

   伺服器地址：RSA DLP網路ICAP伺服器的IP地址或主機名連接埠:用於訪問RSA DLP網路伺服器的TCP埠，通常為**1344**服務URL格式：**icap://*<hostname_or_ipaddress>*/srv_conalarm**範例：icap://dlp.example.com/srv_conalarm
2. 啟用WSA的流量捕獲功能以捕獲WSA代理與網路ICAP伺服器之間的流量。這有助於診斷連線問題。為此，請執行以下操作：

   在WSA GUI上，轉到使用者介面右上角的**Support and Help**選單。從選單中選擇**Packet Capture**，然後按一下**Edit Settings**按鈕。此時會顯示「編輯捕獲設定」視窗。



在螢幕的**Packet Capture** Filters部分，在**Server IP**（伺服器IP）欄位中輸入網路ICAP伺服器**的IP**地址。按一下**Submit**儲存更改。

3. 使用WSA訪問日誌中的以下自定義欄位(在***GUI > System Administration > Log Subscriptions> accesslogs***下)***以獲取詳細資訊：***
   %Xp:外部DLP伺服器掃描判定(0 = ICAP伺服器上沒有匹配項；1 =與ICAP伺服器的策略匹配，並且「 — （連字元）」 =外部DLP伺服器未啟動掃描)

使用手冊定義外部DLP系統的說明。