思科網路安全裝置(WSA)如何處理Skype流量？

目錄

問題：

思科網路安全裝置(WSA)如何處理Skype流量？

環境： Cisco WSA、Skype

Skype是一個專有的網際網路電話(VoIP)網路。Skype主要作為點對點程式運行，因此它不會直接與中央伺服器進行通訊。Skype可能尤其難以阻止，因為它將以許多不同的方式嘗試連線。

Skype按以下優先順序連線：

1. 使用隨機埠號將UDP資料包定向到其他對等體
2. 使用隨機埠號將TCP資料包轉發到其他對等體
3. 使用埠80和/或埠443將TCP資料包轉發到其他對等體
4. 使用HTTP CONNECT通過Web代理將資料包通過隧道傳輸到埠443

在顯式代理環境中部署時，方法1-3永遠不會傳送到Cisco WSA。要阻止Skype，必須先從網路中的其他位置阻止它。可以使用以下方式阻止Skype步驟1至3:

- 防火牆：使用NBAR阻止Skype版本1。有關詳細資訊，請訪問 http://ciscotips.wordpress.com/2006/06/07/how-to-block-skype/
- Cisco IPS(ASA):Cisco ASA可能通過簽名檢測和阻止Skype。

當Skype回退到使用顯式代理時，Skype會在HTTP CONNECT請求中故意不提供客戶端詳細資訊（也沒有使用者代理字串）。 這導致難以區分Skype和有效的CONNECT請求。Skype將始終連線到埠443，並且目標地址始終為IP地址。

範例：

連線10.129.88.111:443 HTTP/1.0
Proxy-Connection:keep-alive

以下訪問策略將阻止通過WSA的與IP地址和埠443匹配的所有CONNECT請求。這將匹配所有Skype流量。但是，嘗試通過隧道連線到埠443上的IP地址的非Skype程式也會被阻止。

阻止Skype — 禁用HTTPS代理的顯式環境

建立自定義URL類別以匹配IP和埠443流量：

1. 導航到「安全管理器」 — >「自定義URL類別」 — >「新增自定義類別」。

2. 填寫「類別名稱」並展開「高級」。
3. 在「正規表示式」視窗中使用「[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+」。

在Access Policies（訪問策略）中將此類別設定為deny:

1. 導航到「網路安全管理器」 — >「訪問策略」。
2. 點選相應策略組的「URL類別」列下的連結。
3. 在「自定義URL類別過濾」部分，為新Skype類別選擇「阻止」。
4. 提交並提交更改

*附註：*只有禁用HTTPS代理服務時，才能阻止顯式CONNECT請求！

啟用WSA HTTPS解密後，Skype流量很可能會中斷，因為它不是純HTTPS流量（儘管使用了CONNECT和埠443）。 這將導致WSA生成502錯誤，並且連線將被丟棄。到IP位址的所有真實HTTPS Web流量將繼續有效（儘管將在WSA上解密）。

阻止Skype — 已啟用HTTPS代理的顯式/透明環境

建立自定義類別以匹配IP和埠443流量：

1. 導航到「安全管理器」 — >「自定義URL類別」 — >「新增自定義類別」。
2. 填寫「類別名稱」並展開「高級」。
3. 在「正規表示式」視窗中使用「[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+」。

在「解密策略」中將此類別設定為解密：

1. 導航到「網路安全管理器」 — >「解密策略」。
2. 點選相應策略組的「URL類別」列下的連結。
3. 在「自定義URL類別過濾」部分，為新Skype類別選擇「解密」。
4. 提交並提交更改。

*附註：*由於Skype流量被傳送到IP，因此將被視為「未分類URL」的一部分。 根據操作是解密還是傳遞，會產生與上面相同的效果。