思科Web安全工具(WSA)把柄Skype流量？

目录

问题：

思科Web安全工具(WSA)把柄Skype流量？

环境：思科WSA， Skype

Skype是所有权互联网电话(VoIP)网络。Skype主要运行作为一个对等程序，因而不与中央服务器直接地联络运行。因为将尝试连接用许多不同的方式， Skype可以是特别难阻塞。

Skype连接下列顺序按首选的顺序：

1. 对使用随机端口的其他对等体的直接UDP数据包编号
2. 对使用随机端口的其他对等体的直接TCP信息包编号
3. 对使用端口80并且/或者端口443的其他对等体的直接TCP信息包
4. 隧道信息包通过使用HTTP的Web代理连接到端口443

当部署在一个明确代理环境，方法1-3不会发送对思科WSA。为了阻塞Skype，必须从网络的另一个位置首先阻塞它。Skype步骤1-3可以阻塞使用：

- 防火墙：请使用NBAR阻塞Skype版本1。更多信息是可用的在 http://ciscotips.wordpress.com/2006/06/07/how-to-block-skype/
- 思科IPS (ASA) ：思科ASA能通过签名潜在查明并阻塞Skype。

当Skype下跌回到使用一个明确代理时， Skype不故意地提供在HTTP连接请求(或者没有用户代理字符串的客户端细节)。这使困难区分在Skype和一个有效连接请求之间。Skype永远将连接到端口443，并且目的地址总是IP地址。

示例：

连接10.129.88.111:443 HTTP/1.0
代理连接：keep-alive

以下访问策略通过匹配IP地址和端口443的WSA将拒绝所有连接请求。这将匹配所有Skype流量。然而，尝试非Skype的程序建立隧道到在端口443的一个IP地址将阻塞。

阻塞Skype -与HTTPS代理的明确环境禁用

创建自定义URL类别匹配IP和端口443流量：

1. 导航给“安全经理” - > “自定义URL类别” - > “添加自定义类别”。

2. 填好“类别名称”并且展开“提前”。
3. 请使用"[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+"在常规表示窗口。

设置此类别拒绝在访问策略：

1. 导航给“Web安全经理” - > “访问策略”。
2. 单击链路在相应的策略组的“URL类别”列下。
3. 在“自定义URL类别过滤”部分，为新的Skype类别请选择"Block"。
4. 提交并且确认更改

注意：如果HTTPS代理服务禁用，明确连接请求可能只阻塞!

当WSA HTTPS解密启用时， Skype流量可能很可能中断，因为它不纯粹地是HTTPS流量(憎恨使用连接和端口443)。这将导致WSA生成的502错误，并且连接将丢弃。对IP地址的所有实时HTTPS Web流量将继续工作(虽然在WSA将解密)。

阻塞Skype -与HTTPS代理的明确/透明环境启用

创建一个自定义类别匹配IP和端口443流量：

1. 导航给“安全经理” - > “自定义URL类别” - > “添加自定义类别”。
2. 填好“类别名称”并且展开“提前”。
3. 请使用"[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+"在常规表示窗口。

设置此类别解密在解密策略：

1. 导航给“Web安全经理” - > “解密策略”。
2. 单击链路在相应的策略组的“URL类别”列下。
3. 在“自定义URL类别过滤”部分，为新的Skype类别请选择"Decrypt"。
4. 提交并且确认更改。

注意：因为Skype流量发送对IP，将考虑作为“Uncategorized URL一部分”。效果和一样上述将发生根据是否操作解密或转接。