Skype is an excellent VoIP and IM program and many people just love it because of its easiness and quality, but when it comes to a corporate world, a lot of things must be considered. Do we ready to give bandwidth for a non-business traffic? Do we completely trust skype developers? What about data leakage prevention - can we control data exchange inside skype protocol?

Usually, the answer to most of these questions is "no, we don't and we can't". So the next step is finding the right tool for the right job - blocking skype.

Talking about Cisco devices and taking a quick glance at CCO give us several options - IOS Flexible Packet Matching, IOS NBAR, IPS and may be ASA also. It seems we have enough options to be sure "at least one of them will do the job". After some reseach and testing I'm ready to give you the short answer NO ONE. But there is a long answer yet :-)

An author of some article about skype security said that skype developers are pretty clever guys so they didn't tie skype communication with specific TCP or UDP ports or specific destinational IPs. Moreover all data exchange is encrypted and control channels are made via HTTPS. So the key question is whether we able to distinguish skype traffic among others.

The quick conclusion is that we can't block skype with traditional corporate network security devices - IOS firewalls, ASA, IPSes because we can't distinguish Skype traffic from any other.

I did some googling and found three methods of blocking skype:

1) Using specific signature, i.e. TCP pattern which matches some skype packets during login procedure. This method was described here and uses 0x7030100 TCP pattern. It also used in cisco IOS FPM feature , but as far as I remember from my experiments it blocks only skype registration traffic. As soon as user managed to get skype registered (e.g. via another connection) FPM doesn't catch it anymore

2) Using proxy-server and "man-in-the-middle" approach so we can to classify initial SSL-handshake of skype via specific requests (false positives are still possible).

3) Using statistical methods in some commercial products for ISP (such as SCE).

But there is one more method to consider. One of my favorite ideas I've heard from Cisco is "Let's turn corporate desktop in a service point". That's the point (*pardon moi*) where Cisco Security Agent (or any other proactive HIPS) comes to play. With CSA we could easily block Skype or any other IM even in portable version. It is possible to block execution, prevent network access, etc. for any application. Once just out of curiosity my colleague blocked Kaspersky antivirus.

All features of CSA is subject of another article but behind clear benefit of blocking some unwanted application lays more complex concept. We have only two options in modern corporate network. Whether we control the cloud named "corporate desktops" or not. Whether we allow users to run and install new application or not. An eventually whether we allow chaos to absorb that corporate resource or not.

Update: I found that Cisco claims that IOS NBAR feature could catch Skype version 3 traffic. Hmm, I think I need to give it another try