Blue Coat

White Paper

Best Practices for Controlling Skype within the Enterprise >

Introduction

Skype is continuing to gain ground in enterprises as users deploy it on their PCs with or without management approval. As it comes to your organization, should you embrace it and its benefits or attempt to stop its progress?

Skype (rhymes with "ripe") is a proprietary peer-to-peer (P2P) voice over Internet protocol (VoIP) network, founded by the creators of KazAa, the popular peer-to-peer technology. The network is defined by all users of the free desktop software application.

Skype is a public voice over IP (VoIP) application that allows its users to call each other from PC to PC for no charge and set up conference calls between multiple users. It also offers very low cost calls to standard telephones via its technology called Skype-out, calling in to the service (Skype-in), voicemail, instant messaging, file transfer and video calling. Its web site shows that there have been over 250 million downloads worldwide.

It is a very clever piece of technology; the phone service requires very small amounts of bandwidth, all data is encrypted and it can get around attempts to block it from packet-based devices such as firewalls, it even uses other PCs running Skype as the next hop in its communications.

Its benefits are clear to the cost-conscious organization or anyone making calls worldwide. Currently, it is very widely deployed in Asia, a little less in Europe and least in North America – quite possibly a reflection of the relavtive costs of making traditional telephone calls. Skype also shows "presence", so you know when your buddies are at their PC, just like Instant Messager applications from AOL, Yahoo! and MSN.

The drawbacks though, are also similar to IM technologies. Firstly, there's no central log of calls from an organization. The file transfer is peer-to-peer, so doesn't go through the organization's email service for virus-scanning, logging and content control, this means that viruses and spyware can enter while confidential information can leave an organization. The voice and video calls cannot be recorded because the encryption is proprietary, making it impossible to use Skype in an organization that needs to follow financial regulations on communication logging.

> ***Skype usage is continuing to gain ground in enterprises with over 250 million downloads worldwide. Management therefore needs to decide whether the benefits overcome the drawbacks and set appropriate policies within the organization.***

Management therefore needs to decide whether the benefits overcome the drawbacks and set appropriate policies within the organization. If it is decided to block Skype, firewalls need to work in conjunction with proxies to provide a block as firewalls on their own are unable to provide a complete block. It may be decided that specific regions or groups of users are allowed access and this can be achieved by using Blue Coat SG in coordination with firewalls.

Why Block Skype?

Skype is a P2P protocol that intentionally evades network policies and may expose enterprises to security and liability risks. It is difficult to control via traditional means, such as firewalls.

The unauthorized use of Skype in the workplace can cause a number of problems, including the following:

1 Skype file transfers may expose the enterprise network to viruses, spyware or other malicious code.

2 Skype file transfers may also expose enterprises to the risk of confidential information being leaked to outside parties.

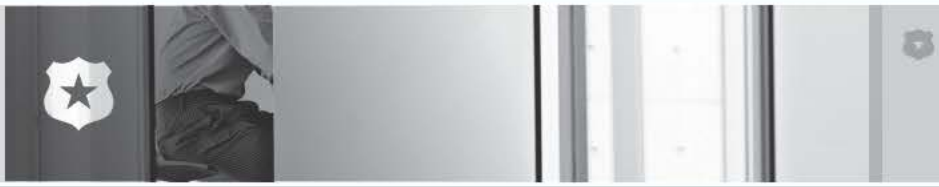
3 As video data is bandwidth-intensive, Skype users can consume a sizeable amount of bandwidth on an enterprise network.

4 Use of Skype PCs as part of a Botnet of PCs to launch denial-of-service and other attacks.

5 Skype users may use its Instant Messaging (IM) functionality to evade enterprise IM controls and send out confidential data

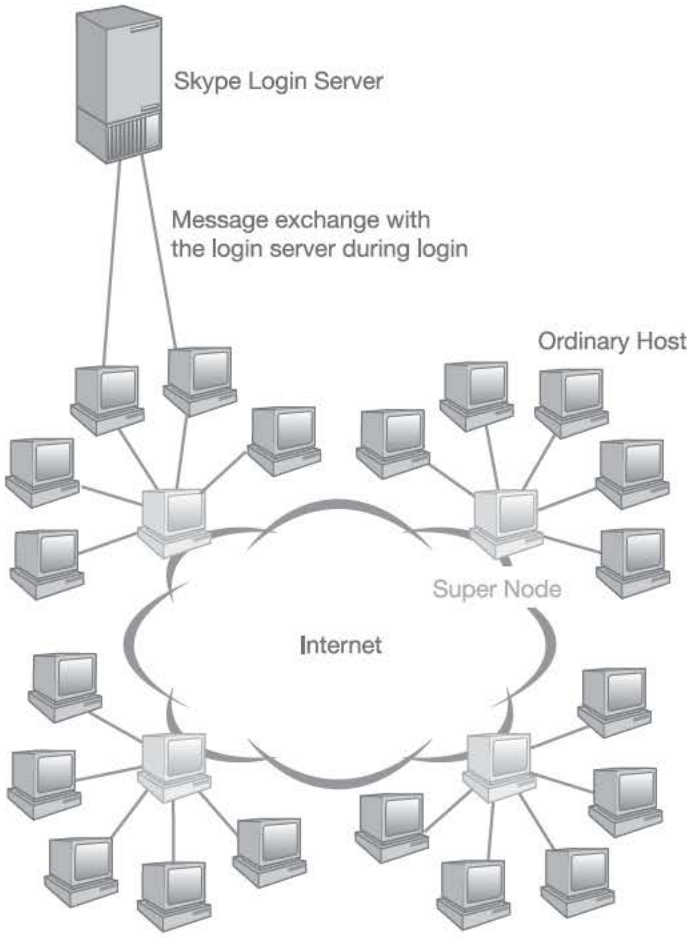
6 All Skype traffic is encrypted using proprietary encryption, so none of the communications can be logged.

As mentioned above, Skype is designed to be hard to block. To date, all the traditional means of blocking unauthorized Skype network use have been unsuccessful. A Tech Brief is available on Blue Coat's web pages that define the full steps to effectively block Skype and give further details on exactly how the technology works.



How Skype Works

When users install and execute a Skype client, Skype tries multiple methods to access a Skype Supernode on the Internet or any of the main Skype login servers. Any PC running Skype that is directly connected to the Internet may be used by the Skype system to become a Supernode. Skype first tries UDP packets directly, then STUN, then TURN – if these fail it uses TCP via previously used Skype port numbers, if this fails it uses TCP over port 80 or port 443, the ports usually used by HTTP and HTTPS traffic.



HOW TO BLOCK SKYPE

To block Skype, IT management needs to use firewalls and Blue Coat SG together. This is a quick overview, full details are in the "Blocking Skype with Blue Coat SG" TechBrief.

STEP 1: BLOCK ALL UNNECESSARY OPEN PORTS ON THE FIREWALL

The first step to control Skype is to ensure that the enterprise firewall is doing its job in blocking all unnecessary ports.

Ideally, an administrator should first begin the firewall configuration by blocking every port on the firewall and then going back and opening only those ports necessary for operation of corporate approved applications.

In addition to allowing only specific ports to be opened (as business dictates), Blue Coat recommends that administrators prohibit high ports from being opened on the firewall.

STEP 2: CREATE WHITE LISTS AT THE FIREWALL OF DEVICES ALLOWED TO COMMUNICATE THROUGH THE FIREWALL.

Organizations should selectively allow access to corporate applications to outside ports through the firewall. The firewall should be configured to allow only appropriate devices to use the open ports; for example allowing just email servers to use port 25 and just the Blue Coat SG to use ports 80 (HTTP) and 443 (HTTPS).

STEP 3: BLOCK DOWNLOADS OF SKYPE EXECUTABLES

Organizations should block access to both the Skype.com domain, as well as downloads of executable content using the Blue Coat SG. It is also recommended that enterprises block downloads of URLs ending with "skype.exe". This will prevent new Skype software from being downloaded to enterprise machines.

STEP 4: INSTALL SSL CONTROLS ON THE BLUE COAT SG

The Blue Coat SG appliances managing application service ports for HTTP (80), RTSP (554), MMS (1755), etc. will drop client connections if the packets sent do not conform to the appropriate protocol. When Skype uses port 80, the protocol used is still Skype's proprietary protocol and does not conform to HTTP and so will be blocked. The Skype application finally attempts to use port 443, if the SSL controls are installed (part of SGOS v4.2) these packets will also be dropped as there is no SSL certificate exchanged between

Skype nodes. Therefore, any attempt to establish a Super-node connection through these service ports will be unsuccessful, as the connection is non-conforming to standards.

If Skype cannot contact a Supernode, the system has blocked Skype from working.

OPTIONAL: ALLOW SKYPE IN SPECIFIC CIRCUMSTANCES

If the organization requires some access to Skype (perhaps certain users or groups or Skype being allowed in certain offices), the checking of SSL certificates by the Blue Coat SG can be ignored. This allows users to access Skype services in specific scenarios.

CONCLUSION

Using Blue Coat Blue Coat SG, enterprises can effectively block the use of Skype. To do so, security administrators must properly configure their firewalls to block open ports that are not needed by the general population of enterprise network users. Blue Coat SG policies can be configured to block downloads of the Skype client onto network machines in the first place. And, with the firewall properly configured, searching attempts are automatically blocked by the Blue Coat SG because the Skype protocol is not recognized as a valid (HTTP conforming) protocol by the appliance.

Blue Coat Systems, Inc. 1.866.30.BCOAT • 408.220.2200
Direct • 408.220.2250 Fax www.bluecoat.com

Copyright© 2007 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Blue Coat Systems, Inc. Specifications are subject to change without notice. Information contained in this document is believed to be accurate and reliable, however, Blue Coat Systems, Inc. assumes no responsibility for its use, Blue Coat is a registered trademark of Blue Coat Systems, Inc. in the U.S. and worldwide. All other trademarks mentioned in this document are the property of their respective owners.