

# Controlling Skype

## Introduction to Skype

With the large deployment of broadband technologies, many Internet users are always connected to the Internet. Skype offers a free Internet telephony service. It allows subscribers to make voice calls – at no cost – to other Skype subscribers using the Skype client. Skype is based on P2P (Peer to Peer) technology.

This technical brief shows administrators how to block Skype traffic using ProxySG.

## How Skype Works

There are three steps involved in a Skype communication.

- 1 Logging in
- 2 User search.
- 3 Call establishment and tear-down.

Figure: i-1, Skype Network shows a typical Skype network.

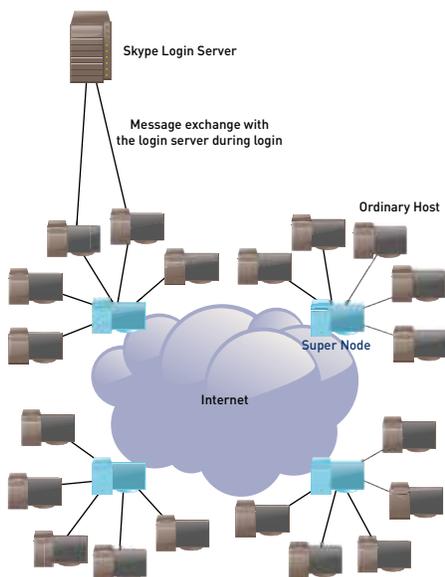


Figure i-1. Skype Network

### Skype Log-in

When users install and execute a Skype client, the client tries to figure out whether it is behind a Network Address Translation (NAT) device, such as a firewall. Because UDP (User Datagram Protocol) packets have trouble traversing NAT firewalls, UDP uses a technique called STUN (Simple Traversal of UDP through NAT) to determine what kind of NAT device it is behind.

If the NAT is a Full Cone, Restricted Cone or Port Restricted NAT, the Skype client obtains the IP address and port information that outside applications can use to send UDP packets to the client. If the NAT is a Symmetrical NAT (which is typical in large enterprises), the Skype client cannot obtain this IP address and port information because NAT maps each unique IP address and port number pair to a different, externally visible IP address and port number pair.

Because STUN is not useful for symmetrical NAT installations, Skype uses a relay traversal technique called Traversal Using Relay NAT (TURN). TURN is less desirable for Skype, since relaying adds a significant amount of latency to the communication. However, it does allow Skype to work.

Once it has sorted out the NAT issues, the Skype client tries to log in by sending UDP packets to a supernode peer from its local supernode list. The supernode list has IP addresses and port numbers of supernodes that are waiting to service the client. If the list is empty, the Skype client tries to log in directly to the Skype log-in server. After logging in, the supernode list gets refreshed.

If the transmission of UDP packets is restricted at the firewall, the Skype client tries to connect using TCP port numbers provided in the supernode list. If connection through TCP over the given ports does not work, the Skype client tries connecting using TCP over port 80 and 443, respectively – hoping that the firewall will interpret the Skype traffic as HTTP/HTTPS traffic and allow it through.

## User Search

Skype uses Global Index technology to search Skype users. Skype claims that their search functionality is distributed and is guaranteed to find a user if they exist and have logged in during last 72 hours. Search results are cached at intermediate nodes.

## Call Establishment and Tear-down

Call signalling is always carried over TCP. For users not present in buddy lists, call placement is equal to a user search plus call signalling. If the caller is behind portrestricted NAT and the recipient is on a public IP address, signalling and media flow happens through an online public IP Skype node, which forwards signalling to the recipient over TCP and routes media over UDP.

If both users are behind port-restricted NAT networks and UDP-restricted firewalls, both caller and recipient Skype clients exchange signalling over TCP with another online Skype node, which also forwards media between caller and recipient.

As you can see, identifying Skype traffic is difficult, since it uses random IP addresses and ports to connect to the Skype network and may even use open well known ports on firewalls to connect.

## How to Block Skype Using ProxySG

There are four steps involved in blocking Skype communication.

- 1 Create a firewall policy that denies clients from going directly to the Internet.
- 2 Allow only the ProxySG to connect to the Internet for HTTP, HTTPS and FTP services.
- 3 Install SGOS 5 with an SSL license (please contact your account manager to purchase this optional license)
- 4 Verify the policy as described in “Verifying Skype Request Blocking” on page i-7.

Because direct client traffic is blocked on the firewall, the Skype client cannot use the Skype ports to access the Internet. The Skype client will then attempt to use HTTP or HTTPS to connect to the Skype service. These requests will be intercepted by the ProxySG. By default, Skype-over-HTTP is blocked by the ProxySG because the ProxySG inspects all HTTP traffic to ensure that it conforms to standards-based HTTP protocols and Skype traffic does not conform. Skype then attempts to use HTTPS over port 443. The ProxySG will block this traffic by default (assuming the ProxySG SSL license is installed) because the ProxySG blocks all traffic on port 443 that does not contain a valid Secure Sockets Layer (SSL) certificate.

The ProxySG will block all HTTPS traffic that does not have a valid SSL certificate (Secure Sockets Layer certificate). This will affect other port 443 traffic that does not use SSL certificates (such as some peer-to-peer applications).

### Verifying Skype Request Blocking

To verify the policy has been installed, attempt to run a Skype client. If the policy has been installed correctly, you should see a screen similar to that show in Figure i-2.



Figure i-2. Skype Connection Error Message

You can also verify that Skype requests are blocked by checking the event log. When skype fails to connect, the event log will contain messages similar to the following:

```
2009-07-14 16:54:56-00:00UTC "SSL Proxy failed while processing CLIENT HELLO(error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol)" 0 310000:1 ..\ssl_proxy\sslproxy_worker.cpp:2729
```

```
2009-07-14 16:54:56-00:00UTC "SSL Proxy failed while processing CLIENT HELLO(error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol)" 0 310000:1 ..\ssl_proxy\sslproxy_worker.cpp:2729
```

## Setting User Policies to Allow Skype

The default policy that checks port 443 traffic for a valid SSL certificate can be made conditional. Using this method, you can block Skype for some users and not for others. The policy conditions are defined using CPL (Content Policy Language). Using CPL, you can use various parameters to allow or disallow Skype traffic (for example, user, IP address, time of day). A common scenario might be to allow Skype for a small subset of users and disallow it for everyone else. The following CPL allows Skype for authenticated users Bobby.Small, Arthur.Dent, and Bob.Kent; all other users are blocked.

```
<proxy>
condition=allowed_skype detect_protocol(none)
define condition skype
request.header.user-agent!="\" http.method=CONNECT url.port=443
end
define condition allowed
user="Bobby.Small"
user="Arthur.Dent"
user="Bob.Kent"
end
define condition allowed_skype
condition=allowed condition=skype
end
```

**Note:** *installation of this policy may result in a VPM compilation warning. This will be an error in the next major release. The user based policy can be changed to IP based to avoid this issue.*

### How to Install the conditional Skype CPL

The following procedure describes how to download and install the Skype CPL that allows you to block Skype for some users and not for others, as described above.

- 1 Download the file skype\_cpl.txt, which is available at this address:  
[http://techlabs.bluecoat.com/policy/skype\\_cpl.txt](http://techlabs.bluecoat.com/policy/skype_cpl.txt)
- 2 Save the file to your desktop or other convenient location.
- 3 Modify the policy to meet your requirements. The user names must be changed.
- 4 Using the ProxySG Management Console, open the Policy Files window; select Configuration > Policy > Policy Files.
- 5 Open the Install Local File from drop-down menu, select Text Editor, and then click Install. A browser window displays the Edit and Install the Local Policy File page.
- 6 Open the skype\_cpl.txt file and copy the text.
- 7 Return to the Edit and Install the Local Policy File page and paste the contents of the skype\_cpl.txt file at the end of the local policy file on your ProxySG.
- 8 Click Install. A page displays in the browser telling you whether the installation was successful. If necessary, correct any errors in the file and re-install it.