



Blocking Skype Communication in Fireware® XTM

Technical Brief

WatchGuard® Technologies, Inc.
Published: January 2011

Introduction

Founded in 2003, Skype has grown rapidly in popularity around the world as a way to communicate for both businesses and consumers. Skype can be used for Instant Messaging (IM), file transfer, Voice over IP (VoIP) calls, including conference calls, and video calls. Skype users download a free Skype client to their local system. Calls to other Skype users are free, but there is a charge to call mobiles and landlines. Some statistics from the Skype website indicate the popularity of the service.

- Skype is responsible for 8% of global international calling minutes.
- Over 20 million users are online at peak times.
- In the third quarter of 2009, Skype users devoted 27.7 billion minutes to Skype calls.
- Over a third of Skype calls are video calls.

Skype communication is encrypted. Unlike other VoIP applications, Skype is based on peer to peer to technology. There is no central infrastructure. The entire Skype directory of users is distributed among all the nodes in the network. Once a user registers with the service and downloads the client, their system could potentially become a node in the network, even if it is not actively making a call. Skype was designed to get around firewalls and it dynamically uses a combination of ports.

Dangers Inherent in Skype

There are several security and productivity concerns that may cause a network administrator to block Skype.

- With all the features and ease of use, bandwidth usage could be excessive.
- Organizations may have policies preventing the use of their systems as supernodes that provide directory information.
- Encryption may not allow regulated organizations to fully track and audit all communication. Some countries have even prohibited the use of Skype.
- Employers may want to restrict time wasting from idle chat and calls.
- File transfer could be used to transfer sensitive data outside the organization.
- Instant messaging can be a source of malware and spam. File transfer could be a source of infection from viruses.

Blocking Skype in Fireware® XTM

Skype blocking was introduced in version 11.2 of Fireware XTM, using a combination of a signature to detect initial login and the blocked sites list to prevent connections to supernodes in the P2P network. Skype blocking is configured as an Application Blocker action, in the Instant Messaging (IM) tab. This feature blocks the initial sign on, and thus all possible forms of communication are blocked. There are no options to allow certain aspects of Skype and to disallow others. Skype servers are detected and dynamically added to the Blocked Sites list with reason as “default packet handling.” If Skype is unchecked to remove it from the blocked site list, it will continue to be blocked for the duration of time that IP addresses remain on the blocked sites list. (The default duration is 20 minutes). With Fireware XTM version 11.4 comes an improved way to block Skype and many other applications.

Application Control — Adds Deeper Inspection Capabilities to XTM

Fireware XTM version 11.4 introduced a new way of managing and controlling applications for WatchGuard XTM 2, 5, 8, and 1050 appliances. Application Control allows administrators to enforce acceptable use policies for users and groups by category, application, and application sub-functions. Application Control actions can be applied to packet filter or proxy policies. Using over 2,300 signatures and behavioral techniques, Application Control gives the administrator real-time and historical visibility into the use of over 1,500 applications on the network. The control and visibility given to the IT pro by WatchGuard Application Control helps organizations enforce acceptable use policies that are mandated by industry regulation, legal and political jurisdictions, corporate goals or culture, and the like.

Skype is one of the most common applications that administrators need to manage. Application Control uses more sophisticated techniques than pattern matching to identify the traffic because Skype traffic is encrypted. The engine looks for behaviors that are typical of Skype applications. You can configure Application Control to block a user login to the Skype network. It is important to understand that Application Control can only block the Skype login process. It cannot block traffic for a Skype client that has already logged in and has an active connection. Here's how to to configure an Application Control action to block user logins to Skype:

1. Select **Subscription Services > Application Control**.
The Application Control Actions page appears.
2. Double-click the Application Control action you want to edit.
3. From the list of applications, select the **Skype** application. To quickly find the Skype application, type "skype" in the search text box.
4. Click **Edit**.



5. Set the action for all behaviors to **Drop**.
6. Click **OK** to save the action for the Skype application.
7. Click **OK** to save the Application Control action.

After you configure the Application Control action to block Skype, you must apply this Application Control action to all policies in your configuration. You can do this when you edit the policy, or on the **Policies** tab of the Application Control dialog box.

Caveats:

Application Control can only block the initial login to Skype. It cannot block traffic for a Skype client that has already logged in and has an active connection. For example:

- If a remote user logs in to Skype when the computer is not connected to your network, and then the user connects to your network while the Skype client is still active, Application Control cannot block the Skype traffic until the user exits and logs out of the Skype application, or restarts the computer.
- When you first configure Application Control to block Skype, any users that are already logged in to the Skype network are not blocked until they exit and log out of the Skype application, or restart their computers.
- An Application Control action that blocks Skype must be applied to all policies. For example, if you have a high precedence policy that allows all DNS, you must configure the DNS policy to use the Application Control action that blocks Skype.
- Skype must be blocked for all users on the network because the Skype peers on the same network that can't get directly out (due to Application Control) will eventually find the local peer on the local network that you have allowed out, and use this to connect to supernodes.

Note that closing the window of the Skype client application does not log out or disconnect a user. The user must explicitly select "Sign Out" from the Skype menu, or right click the icon in the task tray and select "Sign Out."

Skype may also be blocked with some other common configurations of the XTM appliance. Skype communication is not possible when HTTPS deep packet inspection is enabled on the HTTPS proxy. Even if Skype blocking is unchecked in Application Blocker, it is still not possible to enable Skype communication with HTTPS dpi.

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

U.S. SALES:

+1.800.734.9905

INTERNATIONAL SALES:

+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of extensible threat management (XTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. Our newest appliances – the WatchGuard XTM 8 Series and XTM 1050 – provide high performance and fully extensible, enterprise-grade security at an affordable price. WatchGuard extensible content security (XCS) appliances deliver comprehensive email and web traffic protection for security, privacy, and compliance. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2011 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, and Fireware are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part. No. WGCE66693_012611