Solution Note: Managing Skype and other VoIP Applications

Balancing the Advantages of Low-Cost VoIP Services With Associated Risks

Introduction

Skype is one of the many consumer-oriented voice over IP (VoIP) applications that have become increasingly popular as Internet access has become ubiquitous and connection speeds have increased. Additional Skype functionality includes video conferencing and instant messaging. According to www.download.com, Skype is the most commonly-downloaded VoIP application, outstripping the nearest competitive offering by more than threefold. The *Application Usage and Risk Report (5th Edition, Spring 2010)* confirms the popularity of VoIP applications as they were found in 90% of the nearly 350 organizations analyzed worldwide. In total, 30 different VoIP applications were detected with the 5 most popular, lead by Skype, shown in the figure below.

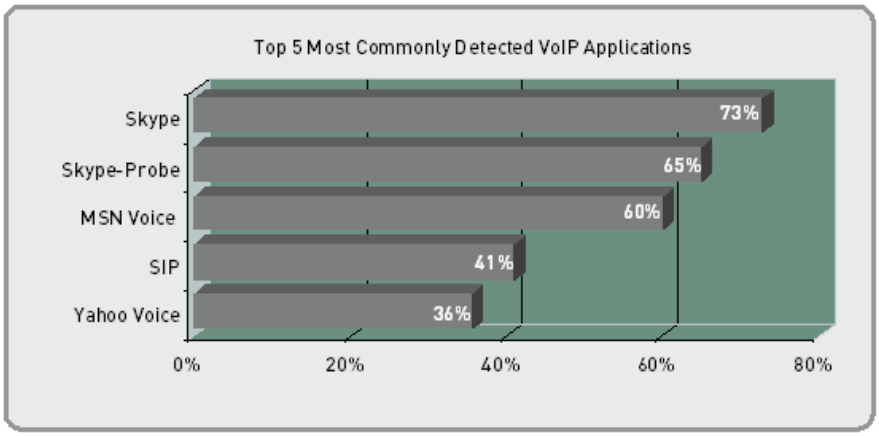

Figure 1: Five most commonly detected VoIP applications.

The dark side of these applications is that they can introduce certain security risks (threat propagation, data loss) because they can easily traverse the firewall, looking like web browsing, hopping from port to port, or using encryption. Out of all of the VoIP applications found, Skype is the most aggressively evasive application, using a combination of proprietary encryption and port hopping (Skype Probe) to gain access to the Internet. Compounding the risks associated with the evasive behavior that Skype and other VoIP applications exhibit is the fact that the additional functionality (instant messaging, video conferencing, file transfer) can introduce regulatory compliance issues and are known threat vectors, capable of delivering exploits, worms and phishing attacks.

The Challenge: Enabling VoIP to the Benefit of Users and the Business

The value of Skype and VoIP applications, for both business and personal use, is clear. They are easy to use and once installed, can simplify communications to friends, family and co-workers at a lower cost, particularly for those who travel frequently and/or internationally. The challenge for IT is to maintain network security while enabling the use of Skype or other VoIP applications. The draconian "block all VoIP" is no longer effective—what if your boss is using it and his calls home while traveling are blocked? A "head in the sand" approach of allowing all is equally inappropriate because it may result in propagation of threats, as well as potential data leakage or compliance issues. Organizations need to follow a systematic process to develop, enable and enforce policies that allow the VoIP use of in a secure manner.

1. **Find out who the business and personal VoIP users are.** Many corporations use VoIP in some way or another already, so a critical step is to determine who the users are and if possible, determine personal vs business usage. Knowing who the users are will allow IT to have a meaningful discussion with the business groups and agree upon the common company goals. Equally important, is that this step can help IT move past the image of "always saying no" and towards the role of business enabler.

2. **Develop a personal VoIP application usage policy.** Once visibility into VoIP for business and personal usage patterns are determined, organizations should engage in discussions around which VoIP applications and which functions should and should not allowed on the network. If an approved VoIP application exists, efforts should be made to encouraged its use. The results of these discussions, including which VoIP applications are or are not allowed should be well documented and shared with users.
3. **Use Technology to Monitor and Enforce Policy.** The outcome of each of these discussions should be documented with an explanation of how IT will apply security policies to enable the secure use of VoIP across the organization.

Documenting and enforcing a policy around VoIP can help organizations improve communications, productivity, and the bottom line while boosting employee morale. An added benefit is that it can help bridge the chasm that commonly exists between the IT department and the business groups.

The Solution: Apply Policy Control Over Usage, Block Threats

Palo Alto Networks next-generation firewalls allow organizations to take a very systematic approach to enabling the secure use of VoIP applications such as Skype, SIP, Yahoo Voice and MSN Voice by determining usage patterns, and then establishing (and enforcing) policies that enable the business objectives in a secure manner.

- **Identify Usage Patterns for Skype and other VoIP applications.** In many cases, VoIP is already in use as part of the network infrastructure. Most commonly, corporate VoIP applications will use SIP, H.323, or SCCP, making them easy to delineate from those that are more commonly used for personal communications. Palo Alto Networks identifies 40 different VoIP applications (see list here), with new variants added on a regular basis via a weekly content update. No matter which VoIP applications are in use, the goal of this phase is to determine who is using Skype or other VoIP applications and for what purpose.
- **Define and Enforce Appropriate Usage Policies.** After determining the usage patterns and business requirements, administrators can apply appropriate usage policies that support the organization's goals and objectives. The ability to delineate which VoIP applications are popular and who is using them means that appropriate enablement policies can be deployed. The identity of the application tied to the user information from enterprise directory services (Active Directory, LDAP, eDirectory) enables administrators to apply policies that go beyond the traditional allow or deny:

  - Allow or deny
  - Allow based on schedule
  - Allow and apply traffic shaping (QoS)
  - Allow certain application functions
  - Allow but scan
  - Decrypt and inspect
  - Allow for certain users or groups
  - Any combination of the above

  Using a policy editor that carries a familiar look and feel, experienced firewall administrators can quickly create a firewall policies that:

  - Allows Skype for all users
  - Allows Skype but applies traffic shaping to ensure it does not rob business critical applications of precious bandwidth.
  - Allows the use of Skype based on a specific schedule.
  - Denies the use or Skype altogether and presents the user with a notification as to why the application has been blocked.

  Allowing the use of Skype can be beneficial to the company so it is important to enable the use while managing the business and security risks.

- **Protect the Network From Attacks Propagated Across Skype and other VoIP applications.** Like many popular applications, Skype has had its share of vulnerability exploits, the most recent of which was an ZBOT variant (TROJ.ZBOT.COC). This exploit was actually addressed in 2009 by an application update, but many users have failed to keep their Skype clients up-to-date. If Skype is in use and continues to be allowed on the network, then policies can be implemented to remind users to keep their clients up-to-date. Due to the fact that Skype uses proprietary encryption, the payload cannot be inspected in transit. However, a secondary layer of protection can be implemented to inspect the HTTP traffic to look for Skype specific exploits traversing the network.

Summary

The response to the use of consumer-oriented applications such as Skype can take one of two forms. Blindly blocking, which may result in lost productivity and business opportunities or blindly allowing, which can expose the business to unnecessary business and security risks. The recommended approach to managing the use of these types of applications is for IT departments to work with the business groups to determine key business requirements and how they can enable the secure use without hindering workflow. With a Palo Alto Networks next-generation firewall, the IT department can achieve the best of both worlds by enabling usage while protecting users and the company from a wide range of business and security risks.