Proxy Server/Application Layer Firewall

Samsung VoIP Applications and Proxy Servers

With the wide spread release and deployment of VoIP applications in the market place today, the ever increasing need to understand and work with existing IT infrastructures is an on going endeavor. One of the fastest growing applications in the VoIP market today is the use of IP Phones in remote locations. To take full advantage of this technology all types of network connections and infrastructures such as the Internet are used. The use of the Internet for applications like VoIP can be great advantage to any organization looking to enhance there communications. However when deploying this type of a solution there are many issues that need to be addressed, one such issue is the use of a Proxy server. While the use of these servers has diminished over the past few years they are still being used and deployed for specific applications. It is important to realize the potential issues that could arise from a VoIP deployment on a network that uses a Proxy Server as the single entry point to the Internet.

This document will help to explain the functions of a Proxy Server/Application Layer Firewall and it's functionality with VoIP connections.

Application Layer Firewall's are considered third-generation firewall technology that evaluates network packets for valid data at the application layer before allowing a connection. It examines the data in all network packets at the application layer of the OSI mode and maintains complete connection state and sequencing information. In addition, an application layer firewall can validate other security items that only appear within the application layer data, such as user passwords and service requests.

Most application layer firewalls include specialized application software and proxy services. Proxy services are special-purpose programs that manage traffic through a firewall for a specific service, such as HTTP or FTP. Proxy services are specific to the protocol that they are designed to forward, and they can provide increased access control, careful detailed checks for valid data, and generate audit records about the traffic that they transfer.

This architecture analyzes the complete command set for a single protocol in application space. In addition, proxy services can analyze the data of a packet to provide additional security checks as well as to provide value-added services, such as URL filtering and user authentication.

Each application proxy requires two components that are typically implemented as a single executable; a proxy server and a proxy client. A proxy server acts as the end server for all connection requests originated on a trusted network by a real client. That is, all communication between internal users and the Internet passes through the proxy server rather than allowing users to communicate directly with other servers on the Internet. An internal user, or client, sends a request to the proxy server for connecting to an external service, such as FTP or Telnet. The proxy server evaluates the request and decides to permit or deny the request based on a set of rules that are managed for the individual network service. Proxy servers understand the protocol of the service that they are evaluating, and therefore, they only allow those packets through that comply with the protocol definitions. They also enable additional benefits, such as detailed audit records of session information, user authentication, and caching.

A proxy client is part of a user application that talks to the real server on the external network on behalf of the real client. When a real client requests a service, the proxy server evaluates that request against the policy rules defined for that proxy and determines whether to approve it. If it approves the request, the proxy server forwards that request to the proxy client. The proxy client then contacts the external server on behalf of the client (hence the term "proxy") and proceeds to relay requests from the proxy server to the external server and to relay responses from the external server to the proxy server. Likewise, the proxy server relays requests and responses between the proxy client and the user (real client).

Note A proxy service has three distinct modes of operation: **proxy server**, **proxy client**, and **protocol analysis**. A proxy server forwards approved client requests to the external server, and when it receives an approved reply, it forwards it to the user (real client).

Proxy services never allow direct connections, and they force all network packets to be examined and filtered for suitability. Instead of communicating directly with the real service, a user communicates to the proxy server (because the user's default gateway is set to point to the proxy server on the firewall). The same is true from the perspective of the external service communicating with a user. The proxies handle all communications between the user and the external service.

A proxy service sits transparently between a user on the internal network and the requested service on the external network such as HTTP or FTP requests. That is, from the user's perspective, the user is dealing directly with the external network. From the external network’s perspective, it is dealing directly with a user on the proxy server (instead of the user's real computer).

Proxy services are implemented on top of the firewall host's network stack and operate only in the application space of the operating system. Consequently, each packet must pass through the low-level protocols in the kernel before being passed up the stack to application space for a thorough inspection of the packet headers and packet data by the proxies. Then, the packet must travel back down to the kernel, and then back down the stack for distribution. Because each packet in a session is subject to this process, proxy services are notoriously slow.

Like circuit level firewalls, application layer firewalls can perform additional checks to ensure that a network packet has not been spoofed, and they often perform network address translation.

Proxy services have *several key advantages*:

- Proxy services understand and enforce high-level protocols, such as HTTP and FTP.
- Proxy services maintain information about the communications passing through the firewall server. They provide partial communication-derived sate information, full application-derived state information, and partial session information.
- Proxy services can be used to deny access to certain network services, while permitting access to others.
- Proxy services are also capable of processing and manipulating packet data.
- Proxy services do not allow direct communications between external servers and internal computers, so the names of internal computers do not have to be made known to external computers. In other words, proxy services shield internal IP addresses from the external world.
- By providing transparency, proxies provide users with the appearance that they are communicating directly with external servers.
- Proxy services can route internal services, as well as external-to-internal requests, elsewhere (for example, they can route services to an HTTP server on another computer).

- Proxy services can provide value-added features, such as HTTP object caching, URL filtering, and user authentication.

- Proxy services are good at generating audit records, allowing administrators to monitor attempts to violate the firewall's security policies.

Proxy services also have some disadvantages. These *disadvantages include the following*:

- Application level firewalls cannot provide proxies for UDP, RTP, RTCP and other VoIP services from related protocol families.

- Support for VoIP applications is typically not supported.

- Proxy services require you to replace the native network stack on the firewall server.

- Because the proxy servers listen on the same port as network servers, you cannot run network servers (Microsoft IIS, Apache, FTP, etc...) on the firewall server.

- Proxy services introduce performance delays. Inbound data has to be processed twice, by the application and by its proxy (for example, the Internet e-mail application talks to the proxy e-mail agent, which in-turn talks to a LAN e-mail application).

- Generally, a new proxy must be written for each protocol that you want to pass through the firewall, and therefore, the number of available network services and their scalability is limited. Usually a lag of six months or more exists from when the application is available and when its proxy is available, meaning users must wait for mission-critical applications to be available to them.

- Proxy services often require modifications to clients or client procedures, thus adding a task to the configuration process.

- Proxy services are vulnerable to operating-system and application-level bugs. Most packet filter firewalls do not rely extensively on operating system support mechanisms; however, they do generally rely on device drivers, etc. Most application layer firewalls require extensive support from the operating system to operate correctly, as an example support typically comes from NDIS, TCP/IP, WinSock, Win32, MFC's and the standard C library. If a security relevant bug appears in any of these libraries, it can have undesirable effects on the security of the firewall server.

- Application layer firewalls overlook network packet information that is contained in lower layers. If the network stack is not performing correctly, then some of the information used to perform security checks that the application layer firewalls request using standard calls from operating system libraries could return incorrect information.

- Proxies may require additional passwords or other validation procedures that introduce delays and frustrate users.

For an example of proxy servers, please refer to the following list.

- Microsoft Proxy Server 2.0
- WinGate
- AllegroSurf

In summary the use of Proxy Servers or any form of Application Layer Firewall's that are not designed specifically for VoIP applications typically cannot be used as the primary gateway for a VoIP installation.

A VoIP application can be designed to go around the Proxy Server and utilize the router or another firewall as its primary gateway to the external network, effectively bypassing all of the issues with this type of a technology.

If you need further design assistance with an application that is use Proxy servers please contact Samsung Professional Services or send an email to BCS.NDF@samsung.com

Due to the limitations of Proxy Servers Samsung does not endorse nor recommend the use of them for any VoIP or CTI related applications.