

# SOLUTION BRIEF



VoIP PROTECTION

**Top  
Layer**<sup>™</sup>

*perfecting the art of network security*

## Introduction

Organizations increasingly rely on the Internet to increase operational effectiveness at a time when global communications represents new opportunities for all organizations.

Most enterprises implementing Voice over IP (VoIP) are primarily concerned about voice quality, latency, and interoperability. All are fundamental quality-of-service considerations that companies need to deal with before they can even begin justifying the move to VoIP.

In the specific case of service providers, a VoIP network must keep customers satisfied by ensuring the end-user experience of a phone call over the IP network is at least equivalent to traditional phone service a.k.a. the Public Switched Telephone Network (PSTN).

For enterprises to realize the cost savings and service providers to operate a successful business, VoIP deployments must:

- Guarantee PSTN-like delivery, uptime and Quality-of-Service (QoS)
- Optimize handling of lost or out-of-order voice packets
- Provide guaranteed access to emergency services (911)

However, corporations and service providers that are implementing VoIP technologies in a bid to cut communications costs also face risks associated with cyber crime activities that must be addressed proactively. VoIP technologies can be targeted in a similar way to traditional network resources since voice phone calls are converted into IP packets allowing transmission across the Internet. While worms, viruses, and hacker exploitation are likely attacks, the most critical and common attacks that will cause maximum disruption are hijacking of VoIP sessions or Denial-of-Service (DoS) attacks for extortion purposes.

Hijacking of VoIP services is compelling to a criminal, who is intent on reselling phone services for a profit. From the enterprise or service provider's perspective they will see a spike in bandwidth usage that will cause legitimate calls to be dropped and increased costs due to bandwidth charges. In the case of enterprises that share VoIP and application data, the problem can be of greater concern since bandwidth constraints will likely cause a slowdown or even worse, obstruct all services. For Service Providers, the result can be equally damaging with irate customers and loss of revenue.

Since 2002, a new technology has emerged to address these complex threats - network Intrusion Prevention Systems (IPS). The diverse spectrum of solutions offered by IPS vendors to perform the advanced protection of VoIP networks can be confusing in the eyes of organizations looking to deploy IPS in their network. While many vendors mislead customers into believing that signature-based solutions should be the primary concern, the majority of industry attacks and concerns are based on massive call volumes due to hijacked sessions. Only Top Layer Networks has an IPS solution robust enough to protect against these types of VoIP attacks. In addition, the Top Layer IPS solution applies a multi-staged defense for stopping network and application threats and emerging exploits. An IPS system that cannot handle large rate-based attacks, in effect making it "DoS-able" cannot be considered as offering VoIP protection.

### **Understanding the Problem – VoIP Call Hijacking**

VoIP networks treat voice as another form of data but use sophisticated voice-compression algorithms to ensure optimal bandwidth utilization. Securing packetized voice traffic on such networks is not any different from securing any data traffic on an IP network.

When employing VoIP networks, private branch exchanges (PBX) are replaced by server-based IP PBXs that often run on standard operating systems. Hijacking or hacking of these systems could result in loss of services, quality degradation and even worse, the loss or compromise of potentially sensitive data.

When VoIP is used to communicate externally, VoIP gateways convert data packets from the IP network into voice before sending them over a public switched telephone network. These gateways can be subjected to DoS attacks and overrun, similar to today's traditional network firewalls. In addition, these gateways can be hacked into by malicious attackers in order to make free telephone calls. Due to the extra call volume provided by VoIP technology, a hacker breaking into a VoIP data stream has access to a lot more calls than through traditional telephone tapping. The trick to protecting against this lies in making sure that only authorized users are permitted to make and receive VoIP calls in addition to controlling the call volume on a per user or client basis. This ensures that reasonable call levels are always maintained, thus preventing uncontrolled hijacking.

One other area of concern in protecting VoIP data networks is simply keeping up-to-date with patches for the latest vulnerabilities. With the creation time of exploits of vulnerabilities in applications, operating

systems and devices closing, the challenge is for administrators to patch hundreds of servers and desktops before any damage has occurred.

## **Understanding the Problem – VoIP Rate-Based Attacks**

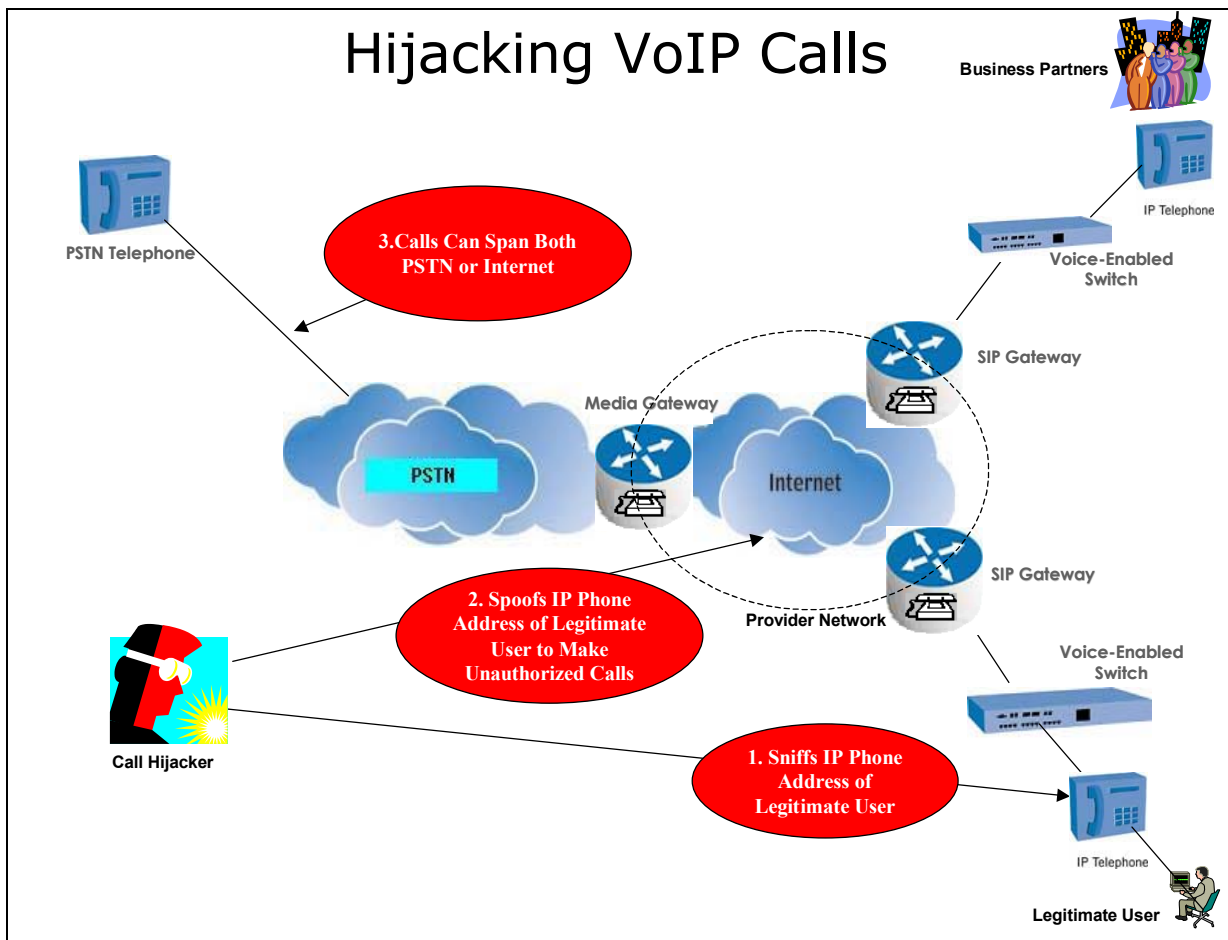
Cyber attacks that impact the performance and availability of the VoIP services are the most common form of attack. Distributed Denial of Service (DDoS) is an attack designed to render a computer or network incapable of providing normal services. The most common DDoS attacks will target the computer's network bandwidth or connectivity. A website DDoS attack is executed by flooding the VoIP gateway with so many requests that it becomes unavailable for normal use. If an innocent user makes normal call request during a DDoS attack, the requests may fail completely, or the quality of the call may be degraded to make voice communications unusable. DDoS attacks can take advantage of thousands of computers, which simultaneously launch hundreds of thousands of requests at the target VoIP infrastructure.

DDoS attacks are very hard to stop because of the large number of randomly distributed attacking sources, which renders conventional protection mechanisms useless. Connectivity attacks are equally devastating, as the web requests are legitimate in format, but overwhelming in volume.

A larger financial issue is when malicious users may hijack or spoof legitimate VoIP accounts and flood a VoIP network with such a high volume of calls, that all available network resources are consumed and can no longer process call requests from legitimate users.

VoIP protocols all rely on TCP and UDP as transport mediums and hence also vulnerable to any low level attacks such as malicious IP Fragmentation, spoofing (UDP), TCP RST window brute forcing, or a variety of IP protocol anomalies which may cause unpredictable behavior in some VoIP services. On SIP-based VoIP networks, as calls are hijacked, DoS conditions can be created by sending a "CANCEL" or "BYE" message to either call participant.

In addition, VoIP networks also rely on DNS and/or DHCP infrastructure for resolving hostnames and IP addresses. If these resources are attacked, the VoIP network will fail to properly handle calls.



## Protecting VoIP with Three Dimensional Protection (3DP)

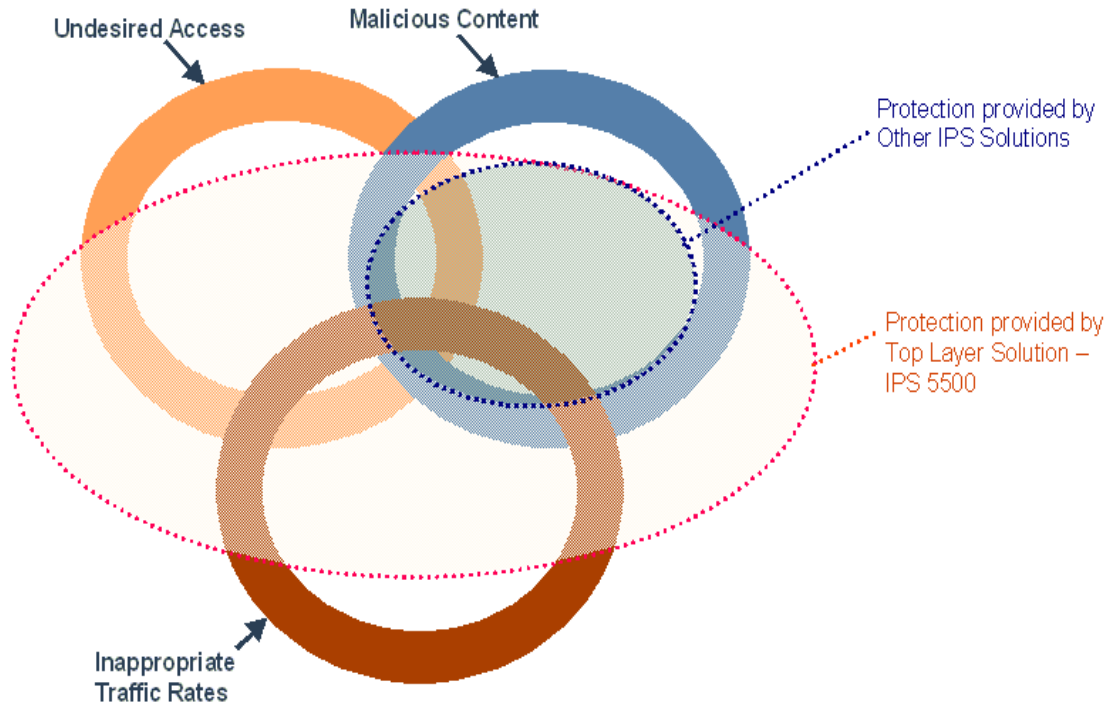
The Industry experts classify network security risks into three major threat categories:

- Malicious content in network traffic, including exploits of Microsoft vulnerabilities, worms, Spyware and other malware;
- Undesired access to networks or systems, including unauthorized or illegal access;
- Rate-based attacks on the infrastructure, such as SYN Floods, and other Denial of Service attacks.

In order to address these three major threat categories, an effective solution needs to comprise three protection mechanisms. These include:

- Content-based IPS protection;
- Stateful firewall filtering;
- And rate-based attack mitigation.

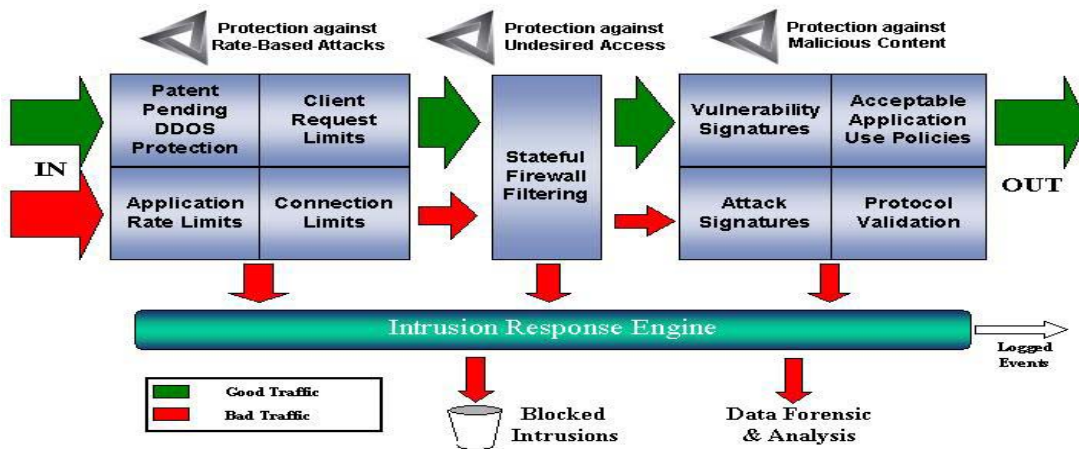
**Figure 1: Top Layer Networks' 3DP Protection**



**The Integrated Solution: Top Layer's IPS 5500**

In order to best combat the threats posed by undesired access, malicious content, and rate-based attacks (and complex hybrid attacks that use multiple elements of these to circumvent static, one-dimensional security tools), enterprises should select and deploy a network IPS solution that addresses all three in an integrated, mutually-reinforcing fashion – as Top Layer Networks does with its “Three Dimensional Protection” approach.

**Top Layer Networks' 3DP Architecture**



## Customer Case Study

A provider of VoIP services wanted to protect their VoIP (e.g. SIP, H.323, MGCP) Gateway infrastructure and network infrastructure from possible overload, abuse, and attack (hijacking) from the VoIP legitimate and malicious users.

Top Layer Networks was the ONLY vendor able to provide the right IPS solution to solve the provider's needs through:

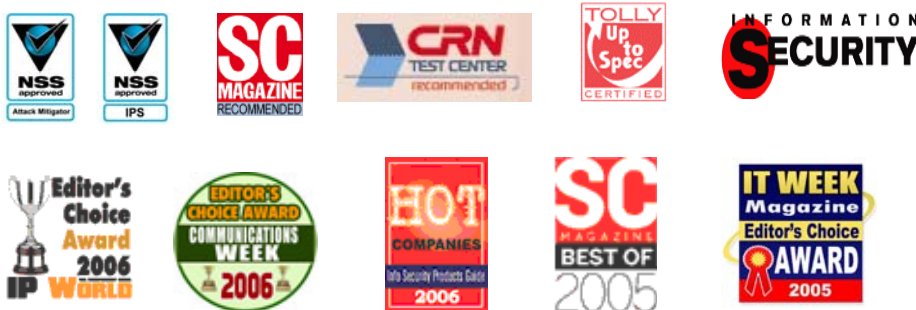
- Limiting the total number of TCP connections to the SIP/MGCP/H.323 Gateway/Proxy infrastructure
- Limiting the total number of TCP Connections from each caller and in total over all callers
- Limiting the total amount of SIP/MGCP/H.323 Control Channel Traffic that can reach the SIP/MGCP/H.323 Gateway/Proxy infrastructure
- Limiting the rate at which VoIP callers can initiate calls via SIP/MGCP/H.323 Control Channel Traffic

Through these mechanisms, Top Layer was able to optimize the providers VoIP service offering, reduce the amount of needed infrastructure and improve call quality and end user experience.

## Next Steps

To find out more about how the IPS 5500 can help protect your network, call Top Layer at 1 508-870-1300, email [info@TopLayer.com](mailto:info@TopLayer.com) or locate your local sales office at [http://www.toplayer.com/content/contact\\_us/offices/index.jsp](http://www.toplayer.com/content/contact_us/offices/index.jsp)

*The IPS 5500 has won the most awards:*



Top Layer Networks, 2400 Computer Drive, Westboro, MA 01581

Phone: 508-870-1300, Fax: 508-870-9797, <http://www.TopLayer.com/>