CONSENTRY NETWORKS

APPLICATION BRIEF

Securing VoIP with ConSentry Networks

Enterprises are increasingly adopting IP telephony as their voice solution. While voice over IP (VoIP) offers many benefits, its use of IP as a transport makes it subject to many of the same vulnerabilities that afflict data networks. Given how mission critical voice service is – and how high people's expectations are for dependability based on traditional phone system operation – IT needs to be aware of these vulnerabilities and take steps to protect the VoIP system.

IP telephony environments are very similar to data environments, so they require similar security measures. For example, most VoIP call managers run on variations of common operating systems, making them vulnerable to viruses, worms, denial of service (DoS) attacks, and other malware. IP phones can also fall victim to targeted attacks as well as be potential launch points for malware. For example, hackers can create attacks that cause VoIP phones to reboot or delete their configuration information, making the phones unusable and crippling the call manager.

VoIP threats can be grouped into two broad categories: attacks that disrupt service availability by bringing down the call manager and attacks that degrade or compromise voice quality, potentially making the VoIP service unusable.

With its focus on LAN security, ConSentry Networks can help IT protect the VoIP infrastructure. ConSentry's LANShield platforms brings together in a single device a comprehensive set of services – including network admission control, full traffic visibility, user access control, and threat control – that can be used to secure any IP-based application or service on the LAN.

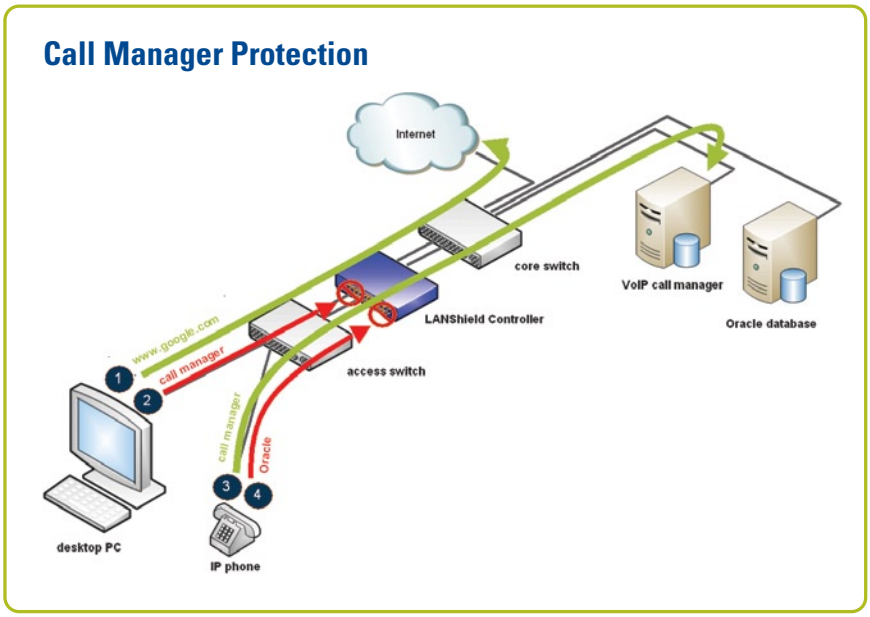
In particular, ConSentry can help protect against:

Attacks that can bring down the call manager

If the VoIP call manager goes down, the enterprise's entire voice system goes down. Hackers can exploit vulnerabilities in the call manager OS and even in the VoIP protocols themselves to launch a DoS or other attack against the call manager. IP phones, including softphones, can even be the launch point for such attacks, which seek to cripple the call manager, often by triggering an overload of call set ups.

ConSentry provides several mechanisms to protect the call manager. First, ConSentry's LANShield platforms can restrict which applications and protocols, even which users and devices, reach the call manager. The LANShield platforms perform stateful deep packet inspection encompassing Layers 2-7, as well as flow-based traffic tracking, allowing for fine-grained access controls. As a result, IT can define policies that ensure only SIP (Session Initiation Protocol) or H.323 traffic reaches the call manager.

This application-based control enables the LANShield platform to protect the call manager from non-SIP exploitations. This protection is especially useful for soft-



LANShield identifies IP phones by MAC address or wildcard and can automatically block traffic destined for the call manager from devices other than IP phones or block traffic from IP phones that are not destined for the call manager.

phones, since their use of a computer platform exposes the VoIP infrastructure to the full range of computer-based threats.

In addition to controls that limit which applications can reach the call manager, ConSentry can also control which devices can access the call manager. For example, MAC-address wildcarding and whitelisting allow IT to define which devices can send traffic to the call manager. With these restrictions in place, the LANShield platform would block any traffic destined for the call manager that was not initiated by one of the authorized IP phones.

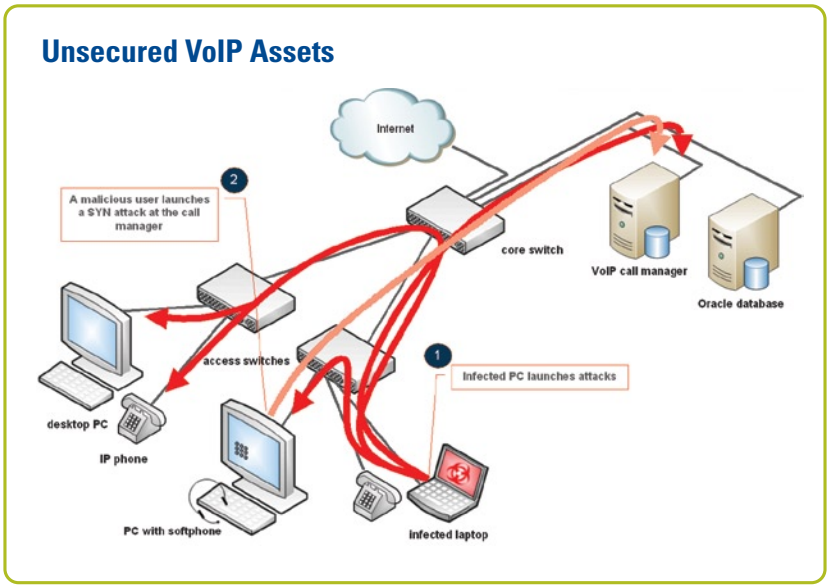
ConSentry also protects the VoIP infrastructure by identifying and blocking the source of DoS attacks. ConSentry's DoS detection algorithm protects against call manager overload by checking whether a user is making too many calls per second to the same destination. And by continued tracking of connection attempts over time, ConSentry is able to accurately identify an attack, curtailing false positives. Based on the policy set by IT, the LANShield platform will block the offending application that's attempting to swamp the call server or shut down a user's traffic altogether.

Attacks that compromise voice quality

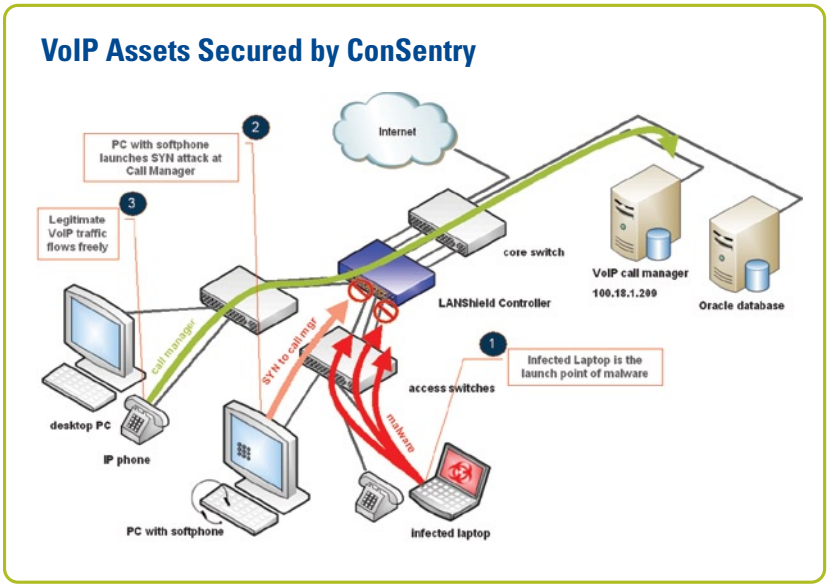
Rather than aiming to take down the call manager, some attacks attempt to disrupt the VoIP system by degrading the voice quality. Viruses, worms, and even some DoS attacks will consume so much bandwidth that VoIP call quality declines, sometimes to the point of rendering the VoIP system unusable. Many such attacks originate in IP phones themselves, requiring a solution that's close to the source – whether a physical phone or desktop.

ConSentry's malware algorithms quickly identify both known and unknown threats and disable the infected device. These application-specific algorithms operate by distinguishing normal behavior from abnormal behavior for individual applications. For example, to detect fast propagating worms, the LANShield platforms track connection attempts, by application, and compare those rates, over time, to typical connection attempt rates. The algorithm triggers when the connection attempt rate exceeds a threshold that varies based on the elapsed time.

Similarly, ConSentry combats "blind" worms by comparing the ratio of attempted to failed connections, over time, and by application; a high failure ratio indicates an attack. These capabilities, coupled with the LANShield platform's close proximity to desktops and its visibility into and control over all user traffic, enables ConSentry to quickly contain malware attacks, including zero-hour attacks.



In an open converged LAN, an infected PC or malicious user can quickly launch attacks to degrade voice quality or disable VoIP assets such as phones and the call manager.



LANShield can identify legitimate SIP or H.323 traffic and block non-VoIP traffic from accessing call manager or malicious traffic from spreading to IP phones.

As with the DoS solution, IT has the flexibility to block all traffic from an infected desktop phone or softphone or block just the malicious application. ConSentry's ability to shut down malicious traffic at the source prevents the bandwidth exhaustion that can make IP telephony conversations unintelligible.

The ConSentry Advantage

In addition to securing the VoIP environment, ConSentry can help simplify a VoIP deployment. For example, the LANShield platforms' visibility into and control over LAN traffic on a per-user, per-application, per-flow basis enables IT to securely separate voice from data traffic, without the need for virtual LANs.

Likewise, ConSentry's role-based provisioning lets IT centrally define voice- and data-related access policies, ensuring consistent, ubiquitous access control. The LANShield platforms' deep packet inspection and fine-grained application controls may eliminate the need for a VoIP-specific firewall in some organizations. And in upcoming releases, ConSentry will support quality of service (QoS) capabilities that will enhance bandwidth utilization and call quality.

ConSentry's comprehensive security capabilities allow IT to secure LAN-based applications and services, including VoIP, as never before.

CONSENTRY™ NETWORKS

Corporate Headquarters
ConSentry Networks
1690 McCandless Drive
Milpitas CA 95035
Phone 408.956.2100 **Fax** 408.956.2199
Toll-Free 866.841.9100
www.consentry.com

Germany
ConSentry Networks
Lyoner Strasse 6 D-605 8
Frankfurt Germany
Phone +49 69 677 33 4
Fax +49 69 677 33 00

United Kingdom
ConSentry Networks
Lakeside House 1, Furzeground Way
Stockley Park, Heathrow, UB11 1BD
Phone +44 (0) 2086 22 3020
Fax +44 (0) 2086 22 3200

Japan
ConSentry Networks
Hibiya Central Bldg. 14F
1-2-9, Nishi Shinbashi, Minato-ku
Tokyo 105-0003 Japan
Phone +813-5532-7630
Fax +813-5532-7373