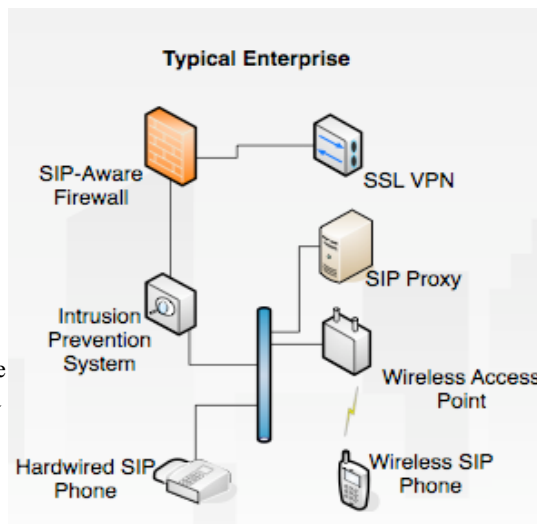


VoIP: Security & Integration

Unless you've hidden under a rock for the last several years, you're well aware of what Voice over IP (VoIP) is, and what it can do for you. VoIP has spread well beyond the technological elite to grandmothers, artists, and--perhaps most critically--normal, non-technology focused enterprises. Unfortunately, this is where the next phase of hard work begins. We now need to take VoIP out of our pilot testbeds and deploy it throughout the network. This means integrating it with your existing security policy and your deployed networks. The InteropLabs (formerly InteropNet Labs or iLabs) has investigated VoIP for much of the last decade, educating Interop attendees on this new and promising technology. In the early years, the focus was on examining the plethora of VoIP protocols, such as H.323, MGCP, Skinny, and SIP. As it became clear that SIP had won over the industry, the iLabs shifted to focusing on basic interoperability, and later, the interoperability of advanced functionality. Now, as real deployments begin to grow, the InteropLabs turn the spotlight to the issues of integration. Specifically, we look at how VoIP using SIP and Security interact, both within the company and for remote users. Additionally, with the overwhelming growth of 802.11 (WiFi) wireless, we would be remiss to not ask the question, "What happens when I try to run VoIP over WiFi?"

As is always the case with the InteropLabs, we've built an example network environment with equipment contributed from the best in the field. To address our VoIP: Security & Integration questions, we've built a number of example enterprises and sets of representative remote users. Each enterprise has various security mechanisms and remote access tools deployed, alongside a wireless infrastructure. The remote users connect via various VPN technologies, transiting a sometimes harsh emulated Internet. Finally, within each enterprise, wireless VoIP users roam with soft clients and wireless handsets. Border security for SIP is not a simple task. The design of the protocol itself forces our firewalls to be smarter. Unlike a simple protocol like HTTP, SIP cannot be enabled with a simple set of fixed rules. Rather, the protocol has dynamic elements that require the firewall to have an Application Layer Gateway (ALG) which actually looks at the SIP message exchanges and permits access on a call by call basis. This problem only becomes worse if you combine it with private address space and NAT. In that case, it's not only necessary to delve deep into the data stream to understand what resources need to be made available, but also to be able to rewrite that data as it transits the NAT boundary. The problems with NAT can reach beyond the border, sometimes requiring additional configuration on equipment within the enterprise. In our lab area, each of our example enterprises is protected by one of these advanced firewalls, with at least one enterprise using NAT.



VoIP: Security & Integration Team

Jim Martin, Netzwert AG

Team Lead

Jed Daniels, IronPort

Educator

Bill Burge, Tactical Networking

Helen Garey, Tactical Networking

Matthew Gast, Trapeze Networks

Jeremy McNamara, The NuFone Network

Doug Moeller, National Technical Systems

David Newman, Network Test, Inc

With Assistance From:

Karl Auerbach, Interworking Labs

John Balogh, Pennsylvania State Univ.

Chien-shun Chu, Juniper Networks

Doug Doolley, Juniper Networks

David Iles, Nortel Networks

Chris McGugan, Symbol Technologies

Craig Johnson, Check Point

Hadriel Kaplan, Acme Packet

Jerish Parapurath, Juniper

Networks

Andy Singer, Check Point

Harsh Singh, Juniper Networks

Eric Thomas, WildPackets

Craig Watkins, Transcend

INTEROP[®] LABS

As part of any rational security policy, it is important not only to implement access control mechanisms such as firewalls, but to also have the ability to detect and stop successful attacks that may initiate from a trusted user or have bypassed border security. To address this, Intrusion Detection/Prevention Systems (IDS/IPS) read deeply into the data stream to identify, and sometimes combat, malicious activity. Like the firewall ALGs, IPSs need to be protocol-aware to be able to discern proper and improper traffic. Recently, IPS vendors have turned their attention to VoIP and SIP, and have produced tools that attempt to keep your VoIP infrastructure safe, despite your users. We've deployed several of these IPS tools throughout our example enterprises.

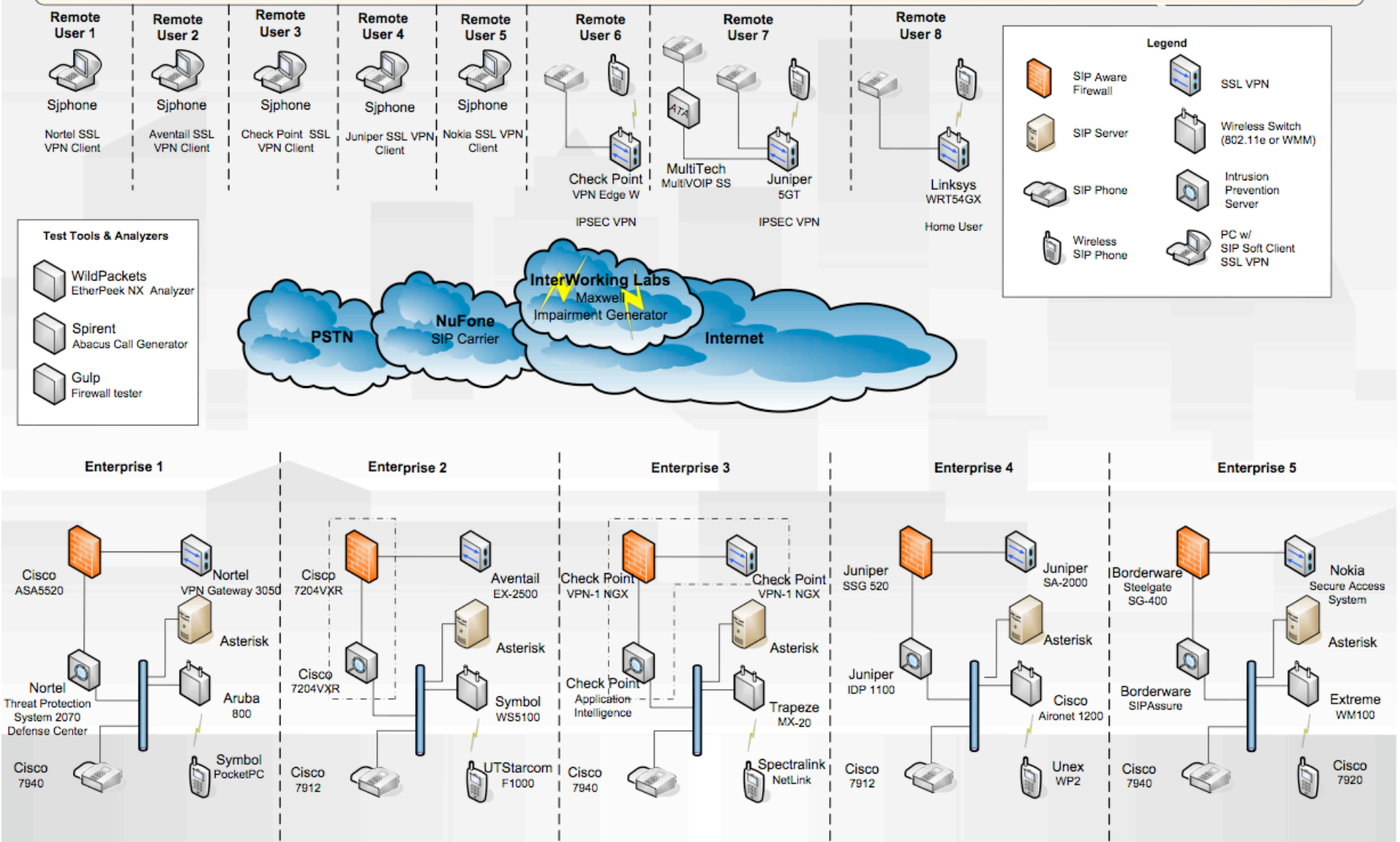
Enterprises have employees everywhere, from the sales person at customer sites to nearly the entire company at home during off hours. When VoIP becomes part of the way you do business, it needs to work securely in all those places too. The latest buzzword in the VPN community is "SSL". While having the ability to greatly ease deployment in general, SSL VPNs bring a particular and interesting challenge to VoIP. The technology underlying VoIP (UDP) and the technology underlying SSL VPNs (TCP) are fundamentally different, particularly with respect to timing and loss. To most engineers, the expectation was that VoIP over SSL VPNs would be significantly worse than VoIP over IPsec or in the clear. However, recent tests have shown just the opposite. By deploying SSL VPNs in each of our example enterprises and having remote VoIP users we're attempting to reproduce or refute these non-intuitive results and examine the necessary considerations for deploying VoIP over an SSL VPN.

VoIP over Wireless at first glance seems like such an easy fit, however, the trick, as always, is in the details. VoIP will work fine over wireless when the wireless environment is perfect, but try to do it in a big enterprise, a trade-show floor, or even your kitchen with the microwave on, and you'll experience how bad it can be. Similar to the SSL VPNs, this comes down to the way that VoIP and wireless interact at a very low level. Enter the 802.11e standard and WiFi Multimedia (WMM). These standards allow voice to be prioritized and treated differently within the wireless domain to ensure high quality. Products that use these standards are just becoming available, and we've got several on hand, deployed alongside traditional (non-WMM) products to demonstrate the impact of these new standards.

Las Vegas 2006

INTEROP[®] LABS

InteropLabs - Las Vegas 2006 - VoIP: Security & Integration



VoIP: Security & Integration Contributors

Aruba Networks
 Aventail
 Borderware
 Checkpoint
 Cisco Systems
 Extreme Networks
 Juniper Networks
 MultiTech
 Nokia
 Nortel Networks
 SpectraLink
 Symbol Technologies
 Trapeze Networks
 Unex
 UTStarcom
 WildPackets

With Assistance From:

American Power Conversion
 Avocent
 Digium
 InterWorking Labs
 IPSwitch
 SJ Labs
 The NuFone Network
 VMWare

INTEROP LABS