



NAC and Internet Protocol Telephony

Securing Enterprise Voice-Over-IP Environments

By Grant Hartline

As IP Telephony proliferation grows by leaps and bounds, its attractiveness as a target also increases.

It's an old adage. As the acceptance of any new technology grows, so does its appeal as a target of attack. So it is with the technologies that use Internet Protocol networks to deliver enterprise-wide voice services. Once solely the domain of innovators and early adopters, IP Telephony, also known as Voice-Over-IP or "VoIP", has experienced rapid growth in acceptance as a viable technology for businesses looking to provide more effective, cost-reduced worldwide voice services. This presents a double-edged sword for IT and security departments needing to support their respective businesses. On the one hand, a single worldwide network, including a unified directory structure and a unified messaging store, stands to reduce operating and support expenses significantly. On the other, the real-time nature of voice delivery makes its security and availability critical to business acceptance.

Network Access Control (NAC) solutions extend a virtual perimeter around all network connection points, providing an overall protection fabric that extends throughout the enterprise. It is reasonable to assume that this protection model should be extensible to support IP Telephony segments, providing the same level of compliance assurance and threat prevention in a single management console. Yet, problems remain.

Challenges posed by IP Telephony

As the deployment of IP Telephony increases and NAC solutions continue to evolve, organizations must grapple with how their chosen NAC solutions fit into an environment that provides IP Telephony services to users. In general, these environments pose three challenges for NAC vendors.

First, an IP Telephony segment is populated with a set of embedded OS devices that do not lend themselves to agent-based solutions of any sort, or even to the paradigm of pre-admission compliance. Even if the call control server runs on a general-purpose OS, the phones themselves do not. So a NAC solution deployed to protect either the network-level gear serving the segment or the devices

within the segment (or a combination of both) must be able to do so without the deployment of device-based agents—whether persistent or transient.

To protect the network at large, NAC vendors must develop means to protect IP Telephony. Leaving one aspect of the network vulnerable threatens the entire system.

Second, the latency and jitter sensitivity of IP Telephony (and real-time media delivery generally) demands that whatever protection is provided to the telephony segments is provided without the injection of additional latency or jitter. Combined with a general high packet rate and low bit rate, this tends to make inline deep packet inspection unworkable. Certainly, the need to secure the IP telephony environment exists, but it cannot be accomplished in a way that interferes with the foundational real-time media delivery.

Third, the physical connection methodology of the majority of IP Telephony environments makes switch port-level control unusable, since the physical connection from the wiring closet is to the phone handset, with the general computing device (PC) connected serially downstream of the phone. Using switch port manipulation to drive endpoints into a quarantine VLAN when the switch port itself is a trunk carrying both voice and data is simply not practical, and would result in significantly higher help desk costs.

Mirage Networks, with its unique combination of out-of-band deployment and comprehensive endpoint quarantine, provides the answer. The Mirage NAC solution gives administrators the capability to define and apply an IP Telephony oriented NAC policy that combines reasonable admission checks (MAC Address, MAC/IP Combination, OS, Service Port, connection method, etc.) with a highly robust post-admission threat prevention engine. Leveraging Mirage's security fabric, administrators can then apply this policy to all IP Telephony segments worldwide, regardless of geographical placement.

Deploying a NAC solution at level 2 eliminates the need to integrate with unique switches and operating systems.

Solving the above systemic problems is all well and good, but NAC vendors should also leverage their visibility model to provide additional value to enterprises with IP Telephony environments in play. In conjunction with Avaya's DevConnect program, Mirage Networks engineered and tested a set of IP Telephony policies designed to provide base level protection for any IP Telephony environment. These policies are available out of the box to any Mirage customer, and provide a valuable starting point to truly securing enterprise voice-over environments.

Enterprises that are evaluating NAC solutions have some choices to make when they deploy, or plan to implement, IP Telephony. One choice is to secure the data portions of the network as a project separate and apart from securing the voice. At first glance, this path is appealing, since it means that NAC evaluators must simply make choices that don't explicitly interfere with the operation and stability of voice delivery (such as port level control of ports that serve phones).

However, just as an enterprise-wide voice implementation stands to drive directory structure and messaging store choices, so it should also drive NAC vendor selection. Enterprises that use real-time application delivery generally, and IP Telephony in particular, are encouraged to quiz their selected NAC vendors on their respective plans. At a minimum, vendor plans should include no architectural incompatibility between the workings of the NAC solution and the operational availability and integrity of the IP Telephony solution. Ideally, vendor plans should include specific compatibility with and support for IP Telephony, which means going farther to extend the reach and promise of NAC to provide voice segments the same kinds of proactive compliance and protection that are provided to the data segments.

Summary

In summary, IP Telephony imposes specific requirements on NAC solutions. Enterprises who have deployed IP Telephony, or who have plans to do so, should ensure that the requirements to support and protect the voice environment are included in their search for a strategic NAC vendor. They should seek products from those available today that protect IP Telephony and data infrastructure equally, and allow traffic to pass without added latency.