PROTECT YOUR VOIP/SIP SERVERS

Insulating your voice network and its servers from attacks and disruption
Insulating your voice network and its servers from attacks and disruption

The Situation
Did the appeal of voice over IP (VoIP) savings get ahead of your security controls? Has your network been brought down by a VoIP vulnerability? Most organizations fail to realize the security implications of replacing an isolated voice network with a VoIP infrastructure integrated with the rest of their critical network and Internet infrastructures.

Voice over Internet Protocol (VoIP) and Session Initiation Protocol (SIP) both provide a means to establish communication channels over an IP network. You may have a typical voice call one on one with a colleague at work or perhaps a multi-cast conference call where various team members around the world are discussing some new product or service that can change the market. Could sensitive information be discussed in these conversations? Could a hacker eavesdrop on these conversations? Having improper security controls around VoIP/SIP can compromise the voice network and put your organization at risk.

Driving Concerns
Because they enable cost savings over traditional PBX telephony systems, VoIP/SIP servers have been widely adopted in many organizations. A VoIP server is like any server or PC with an Internet connection: it can be the target or unwitting accomplice of a hacker attack.

Many VoIP systems are improperly segmented from the data network. The VoIP and session initiation protocol (SIP) servers themselves are poorly secured against network attacks, network eavesdropping, or denial of service attacks. If someone can access one of these servers, they can move on to other assets around the network in search of data and disruption. Organizations that rely on VoIP systems without a proper security plan in place find themselves at risk of serious network downtime and loss of the critical communication infrastructure connecting employees with the outside world—including customers.

Each organization must account carefully for VoIP and SIP risks including:

- **Denial of Service Attacks (DoS/DDoS).** DoS/DDoS attacks to a VoIP server can bring the data network—as well as the servers that host it—to a crashing halt, with devastating effects on all network and voice traffic
- **SIP Vulnerabilities.** The SIP protocol is used to set up and tear down phone calls. Some SIP Server vulnerabilities can allow attackers to hijack SIP sessions as part of a man in the middle attack. In addition, buffer overflow attacks can target vulnerabilities that exist within the SIP protocol.
- **Malware.** Malware, such as a worm, can spread through open ports on VoIP/SIP Servers, infecting other servers and critical points of the infrastructure
- **Improperly Secured VoIP Servers.** Unpatched software or unnecessary and open ports and services on a VoIP server can allow network attacks that use these servers as a stepping stone to other corporate assets
- **Eavesdropping.** Hackers can intercept VoIP packet streams and interpret phone conversations on the fly, violating confidentiality and leaving your company open to a data loss or regulatory disclosure
- **Unauthorized VoIP server access.** Administrators can inadvertently disrupt servers or compromise their integrity with unapproved software or configuration changes

Security Connected
The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.
Solution Description
You can implement stronger VoIP and SIP security in stages, pursuing a multi-pronged strategy. This approach allows IT security administrators to fine-tune their implementations based on organizational needs. The steps below show the steps to take, from basic to advanced:

• **Malware Protection.** Deploy an antivirus solution that can not only scan for malware in real time, but provide real-time heuristics detection of zero-day malware

• **Protection against Vulnerabilities/Exploits.** McAfee recommends reviewing open ports and running services on VoIP/SIP servers and disabling or closing any unneeded ports and services. This precaution can reduce the risk of attack. In addition, provide basic firewall functionality to block access to typical open ports on VoIP/SIP servers. Intrusion Prevention (IPS) technology on the server can assist in protecting unpatched VoIP/SIP Servers against exploitation. Host IPS technologies have built-in mechanisms that can protect against zero-day vulnerabilities or exploits. This protection can work in either a signature or heuristic based fashion where anomalies are queried to a database to validate whether that action is malicious or benign.

• **Protection against Denial of Service Attacks.** Since VoIP/SIP servers are considered critical communication infrastructure, they are susceptible to denial of service attacks from the network layer as well as buffer overflow exploits at the system layer. Implement intrusion detection and memory protection that can find, analyze, and prevent these types of attacks.

• **Blocking installation and execution of unauthorized applications or processes.** To protect the integrity of VoIP/SIP servers against inadvertent or malicious installation or execution of software, install a whitelisting technology

• **VoIP Server Auditing.** VoIP/SIP servers have a specific purpose. It is recommended that organizations implement a server auditing strategy around these servers. Auditing should include monitoring of changes to operating system, registry, or critical application files. In addition, monitor administrators who have access to these servers and ensure they follow proper change management processes before changes are conducted on this critical infrastructure.

• **Secure the perimeter.** Many organizations choose to segment their VoIP/SIP servers and voice network from the rest of their main IP network. These organizations can benefit from network-based intrusion prevention technology that can continuously monitor the packets that traverse the voice network. This extra layer can filter out any data packets that should not be traveling over the voice network.

Decision Elements
These factors could influence your architecture:
• Are your VoIP Servers centrally managed?
• What operating systems are your VoIP servers running?
• What is your change management process for adding new VoIP servers on the network?
• Is your voice network segmented from the data network?
• Do you allow communication tools on your network such as Skype or Google voice?
• Do you have appliance based VoIP/SIP servers?
**Technologies Used in the McAfee Solution**

McAfee provides several solutions that can help organizations achieve total VoIP/SIP server and network protection. No two VoIP/SIP environments are ever the same, so McAfee offers an array of solutions that can help administrators secure their voice networks and voice servers to meet organization-specific needs. The solution includes advanced technologies such as McAfee® Application Control and McAfee Change Control that can lock down the VoIP/SIP Servers to run only processes that are deemed “trusted.” McAfee VirusScan® Enterprise and McAfee Host Intrusion Prevention help administrators protect their servers from malware and zero-day vulnerabilities through use of signature and heuristics-based detections.

Furthermore, organizations that choose to segment their voice network may want to secure that perimeter with McAfee Network Security Platform (NSP), which has signature and heuristics-based detections for VoIP/SIP vulnerabilities. Some of these mechanisms include detections of DoS/DDoS attacks at the network level. NSP can detect anomalous behavior, perhaps misused or exploited VoIP/SIP protocols, as well as backdoor intrusions into the voice network. Through integration with the reputation systems of McAfee Global Threat Intelligence™, NSP can help organizations profile and block the malicious external IP addresses that are attempting to perform these denial of service attacks. NSP can accomplish this inspection and blocking without introducing any additional latency, a crucial requirement for voice traffic.

The technologies working on the server and in the network can be centrally managed and reported via the McAfee ePolicy Orchestrator® (McAfee ePO™) console. With new visibility into threats and relevant actions, your organization can close the security gaps that exist on the voice network and VoIP/SIP server infrastructure.

McAfee products help insulate your voice network and its servers from attacks and disruption.
McAfee VirusScan Enterprise
McAfee VirusScan Enterprise combines antivirus, antispyware, firewall, and intrusion prevention technologies to stop and remove malicious software on VoIP/SIP servers. McAfee VirusScan Enterprise is available for both Windows and Linux servers.

McAfee VirusScan Enterprise protects VoIP/SIP servers with heuristics and signature based malware detection. In addition, VirusScan Enterprise includes:

• **Access Protection Rules.** Prevents unwanted changes to your VoIP/SIP servers by restricting access to specified ports, files, shares, registry keys, and registry values. In addition, it includes the ability to prevent unauthorized changes to VirusScan Enterprise policies and configurations.

• **Buffer Overflow Protection.** Protection against memory-based exploits that can impact VoIP/SIP servers

• **Global Threat Intelligence (GTI).** McAfee GTI has the ability to provide real time file reputation of suspicious files on a system to determine if that file is malicious

McAfee Application Control
McAfee Application Control lets IT administrators prevent the unauthorized installation of software on VoIP/SIP servers. Administrators define a standard list of which processes and applications are allowed to run, and a dynamic trust model allows controlled, automated updating of this software by trusted updaters. In addition, Application Control can prevent malicious code execution on servers.

• **System protection.** Extends coverage to Java, ActiveX controls, scripts, batch files, and specialty code for greater control over application components

• **Multi-server support.** Application Control has support for Linux, AIX, Solaris, and Windows-based VoIP servers

• **Advanced Memory Protection.** Buffer overflow detection and exploit blocking guard all running processes on VoIP/SIP servers

McAfee Change Control
Hardening VoIP/SIP servers is one of the most effective methods of protecting these servers. However, without proper monitoring and enforcement of any security implementation put in place, changes can be made without your organization's knowledge. Tamper-proof technologies can prevent unauthorized changes to VoIP/SIP servers. McAfee Change Control delivers continuous detection of system-level changes being made across the server and prevents unauthorized changes to critical system files, directories, and configurations. Change Control tracks and validates every modification to the VoIP/SIP server. McAfee Change Control has the ability to integrate with common ticketing systems such as BMC Remedy to log, approve, and monitor change requests for server changes.

McAfee Host Intrusion Prevention
McAfee Host Intrusion Prevention protects VoIP/SIP servers against zero-day vulnerabilities on the server as well as providing comprehensive protection against the most common exploits out today. McAfee Host Intrusion Prevention (Host IPS) also includes full desktop firewall functionality. Host IPS can protect VoIP/SIP servers that are not up to date on patches by blocking exploits triggered from vulnerabilities within the operating system or software used by the VoIP/SIP system. These detections are signature, behavioral, and heuristics-based. These features include enveloping and shielding that protect the VoIP/SIP software processes from executing outside of their own memory space and also stop outside processes attempting to interfere with that memory space.
McAfee Network Security Platform (NSP)
VoIP servers and networks are especially prone to attacks such as eavesdropping, man in the middle, or DoS attacks. An intruder may use these attacks to either disrupt communication services or gather information. McAfee Network Security Platform (NSP) provides intrusion prevention technologies (IPS) that can detect and block these threats before they can cause damage to your VoIP/SIP systems. NSP can help secure the VoIP/SIP server and voice network perimeter by filtering traffic before it reaches the VoIP/SIP servers. NSP includes signatures specific to detection of VoIP vulnerabilities and attacks.

NSP can also analyze traffic through its threat analyzer and assist administrators in determining if there are any anomalies in their voice networks. This can also help administrators decide if rogue devices have connected to the voice network that can pose a risk to the network. NSP can accomplish this protection at wire speed, without introducing any latency to the VoIP/SIP server infrastructure.

McAfee ePolicy Orchestrator (McAfee ePO)
McAfee ePolicy Orchestrator enables the automatic software distribution and policy management of McAfee VirusScan Enterprise, McAfee Host Intrusion Prevention, McAfee Application Control, and McAfee Change Control, as well as reporting for McAfee Network Security Platform.

- McAfee ePO Extension provides the interface for configuration, scheduling, and security reporting for VoIP/SIP servers
- McAfee ePO agent acts as an intermediary between the agents installed on the VoIP/SIP servers and the McAfee ePO console and database
- McAfee ePO itself provides a “single pane of glass” for managing VoIP/SIP server security
- McAfee ePO can provide reporting functionality for network-based appliances

Impact of the Solution
Layered protections will help insulate your VoIP/SIP servers from the malware, vulnerabilities, and attacks that threaten the availability of your critical communication infrastructure.

- McAfee VirusScan Enterprise can reduce the amount of malware that can infect VoIP/SIP servers by scanning files and directories on those servers. Its buffer overflow protection combats memory based exploits that are targeted at VoIP/SIP Servers.
- McAfee Application Control can prevent the installation of unauthorized software on VoIP/SIP servers. Using Application Control, you can harden these servers and the VoIP software by preventing any unauthorized execution of software or other code that could adversely affect functionality or availability.
- McAfee Change Control can prevent unauthorized system changes to the file system, registry, or dll’s of VoIP/SIP servers that lead to unnecessary server downtime
- McAfee Host Intrusion Prevention can assist administrators in protecting servers from vulnerabilities introduced by missing server patches. Furthermore, Host IPS can protect against vulnerabilities that exist within the SIP and VoIP protocols. Host IPS also includes a firewall to prevent malware from spreading over open ports on VoIP/SIP Servers.
- McAfee Network Security Platform can assist in preventing DoS, man in the middle, and eavesdropping attacks at the network layer—before the attack can reach the servers

As your business increases its reliance on a VoIP voice network, these protections will help ensure that network is both available and secured against digital eavesdropping.
Optional Integrations
McAfee Network Security Platform (NSP) has great flexibility in integrating with various McAfee technologies. To help achieve complete protection and visibility for VoIP/SIP Servers, NSP can integrate with McAfee Host Intrusion Prevention at the endpoint. Integrated data can help the administrator correlate events received from both NSP and HIPS. This will provide a complete view of protection both at the network and endpoint level from within the NSP console. In addition, McAfee NSP can integrate with ePO to provide a single reporting console for NSP events and endpoint events using the power of ePO reporting and dashboards by rolling up the data from NSP to the ePO console using a data rollup task with the ePO configuration.

Q&A
What types of executable files can be whitelisted?
McAfee Application Control can whitelist a variety of executables including .exe, .dll, and scripts such as .js, .vbs, and .bat for Windows.

Can McAfee Application Control and McAfee Change Control be tampered with?
McAfee has built controls into both products that prevent users from disabling either McAfee Application Control or McAfee Change Control. This includes users with administrator rights to a server.

What if certain IT administrators need to make changes to servers locked down with McAfee Application Control?
In the Application Control policy, you can leverage your Active Directory to define trusted users, those authorized to make changes to a server. Used in combination with Change Control, the activity conducted by each administrator can be monitored to ensure that no administrator is making system level changes that can have an adverse effect on the VoIP/SIP server.

Does McAfee Network Security Platform need to be deployed in-line on a network?
NSP can be deployed in several ways. If your organization simply wants to monitor but not block any events discovered by NSP, you can simply deploy it in a SPAN or TAP configuration. However, if your organization wants to enforce the full blocking and mitigation functionality, then the device would need to be deployed in-line. All NSP appliances include full Fail-Open Kit support and High Availability configurations.

How is Host Intrusion Prevention different from Application Control?
Host Intrusion Prevention actually compliments Application Control. Application Control is a whitelisting technology where you define what applications/processes are allowed to run and includes advanced memory protection. HIPS can provide signature and behavioral Intrusion Prevention on zero day vulnerabilities as well as provide enveloping and shielding protection against processes running on the VoIP/SIP server. Furthermore, HIPS includes a connection and location aware firewall.

How does McAfee GTI work in McAfee VirusScan Enterprise?
McAfee Global Threat Intelligence file reputation service will perform a DNS Query of a hash of the suspicious item. If that hash matches the GTI checks in the cloud, the appropriate action will take place to either allow or block the malicious entity depending on policy configurations.
Additional Resources
www.mcafee.com/virusscan-enterprise
www.mcafee.com/appcontrol
www.mcafee.com/changecontrol
www.mcafee.com/hips-server
www.mcafee.com/nsp
www.mcafee.com/epo

QuickTip Videos:

White Paper: Making VoIP Secure

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected

About the Author
Joseph Fiorella is a Senior Systems Engineer at McAfee and based in New York City. Joseph has been involved in the information security field for the past 8 years. Since Joseph joined McAfee in 2009, he has been implementing and supporting security technologies for some of the largest Public Sector organizations in the North East. Joseph holds a Bachelor's degree from Pace University, as well as numerous certifications, such as Certified Information Systems Security Professional (CISSP), Security+, and Certified Information Security Manager (CISM). Joseph is an active member of (ISC)2 and the New York Chapter of ISACA. Joseph is currently in the process of completing his Master's Degree at New York University.