

Application Note

VoIP Protection with Juniper Networks IDP

Walt Shaw
Product Management
Security Products Group



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 350082-001 June 2006

Introduction

As solutions and products based on VoIP increase in popularity, they present security teams with a fundamental challenge of how to protect an Internet communication that is becoming more ubiquitous in its usage and, as a result, more open to abuse and exploits. Security experts agree that like any communication format that is reliant on Internet protocol and increasing in its usage, VoIP will increasingly fall prey to hackers, attacks, worms, and vulnerabilities native to the application. The increasing attacks and vulnerabilities open the VoIP solution up to eavesdropping, identity theft, fraud and denial of service. A proof point of this trend is the number of attacks that target existing protocols such as HTTP, FTP, SMTP, peer-to-peer and instant messaging—attacks increased significantly as each protocol became widely used.

According to the META Group's "IP Telephony Security" (2005), the potential threats to VoIP include:

- Endpoints and servers (including voice gateways, IP phones, and call control servers) may be targets of attacks initiated from the IP network.
- Endpoints and servers may be infected with worms, trojans and viruses that can degrade the IP Telephony service or even propagate themselves to servers in the data network, leading to damaged data storage.
- Malicious attacks may lead to significant changes in routing protocols and other configuration information.

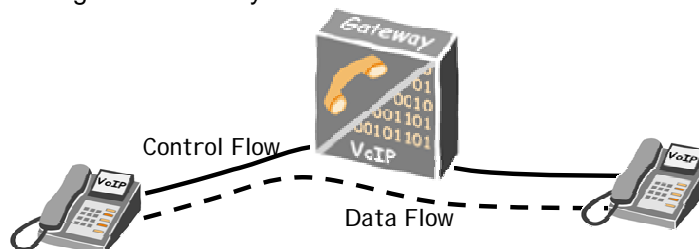
VoIP attacks carry significant ramifications in that the VoIP components are part of the data network so an attack on a call manager can conceivably disable the phone system as well as the data network. Security administrators must consider offerings that address the growing need for VoIP protection at both the application and network layers.

VoIP Traffic Flow

VoIP protocols are slightly different than other protocols in that they have two components:

1. The control flow comprised of SIP, H.225 (for H.323), MGCP, etc
2. The data flow or "media" comprised of RTP and RTCP

The control flow sets up the VoIP call signaling between the IP Phones or "endpoints" (residing at end-user location) and the call manager or proxy (residing at service provider or HQ/central location). Once this handshake is established and determined to be valid and allowed by the security policy, then the media (or voice data) can flow through. While the control flow represents a small portion of the overall VoIP traffic, it is where most of the potential threats would reside since the control flow is where the logic and policy enforcement take place. Any attack in the data flow, where it is converted to sound at the endpoint, would be relatively innocuous. Besides detecting control flow attacks with stateful signatures, IDP also provides protocol anomaly detection. Protocol anomaly defends against future attacks that exploit the underlying vulnerability of the SIP protocol and therefore offers greater zero-day coverage to these as-yet unknown attacks



VoIP Protection with Juniper Networks IDP

Juniper Networks IDP includes several VoIP specific attack detection mechanisms designed specifically to protect VoIP from attacks at both the control and data flow layer.

- **Stateful signatures:** Juniper Networks IDP 4.0 currently provides stateful signatures that protect against a number of exploits that target Skype, SIP, H.323, as well as vendor-specific VoIP phones.
- **Protocol Anomaly:** Juniper Networks IDP 4.0 delivers protocol anomaly protection for two of the most VoIP protocols, SIP and H.225 (the signaling and control protocol for H.323). IDP detects attempts to use the VoIP protocol in ways not meant or designed to be used, and provides coverage against the potential underlying vulnerabilities. The end result is it provides zero-day coverage for future unknown SIP and H.225 attacks. The Juniper Networks IDP protocol decodes for SIP and H.225 will also allow administrators to create custom attack objects unique to their communication network for attack detection and prevention as well as user compliance. Some of the attack objects for detection and prevention included in IDP today are:
 - **SIP: Non-standard method** – This signature detects a SIP (Session Initiation Protocol) request containing a method not defined in the RFC
 - **SIP: Wrong version** – SIP version should be present in the specified place and be equal to "SIP/2.0"
 - **SIP: No colon after the command** – SIP command should be followed by the colon
 - **SIP: Method overflow** – SIP request containing a method name that is too long
 - **SIP: Unknown header** – The header is not specified in RFCs
 - **SIP: Chunk length overflow** - Content-length field is too big
 - **SIP: Wrong content length** – Content length doesn't match the specified in the packet
 - **SIP: Max-forwards are too big** – Max-forwards value should be 70 as recommended
 - **H.225: Unknown command** – Detects an unknown protocol H.225 RAS (registration, administration, and status) message
 - **H.225: No protocol ID** – Identifies malformed or absent protocol ID

Optimization of IDP VoIP Protection on the ISG Series with IDP

All IDP SIP and H.225 protection (signatures, anomaly engine, etc) is available on all Juniper IDP platforms. However, on the ISG 1000 and ISG 2000 with IDP systems, this protection is delivered with firewall-like throughput and latency through intelligent, policy-based traffic management.

On the ISG 1000 and ISG 2000 with IDP, the security policy would dictate that the control flow – where a VoIP threat usually resides – would be delivered to the security module with IDP for application layer threat inspection, while the data flow (which does not have attacks) is delivered directly to the ISG 1000 and ISG 2000 ASIC for access control and DoS protection. Since the data flow being sent through the ASIC comprises the bulk of VoIP traffic, overall performance is optimized and latency reduced due to this intelligent routing of traffic straight through the ASIC.

Summary

VoIP represents a significant cost savings to businesses and as such, is expected to become more widely deployed in coming years. Increasing number of attacks targeting the VoIP protocols are expected as the number of VoIP deployments increase. With Juniper Networks security products, security administrators can be assured that their VoIP networks are protected from attack at both the network layer (control) and the application layer (data or media).