

How Juniper Networks Infrastructure Enables Avaya IP Telephony

Introduction to VoIP Challenges: Security, Performance, and Interoperability

The benefits and cost savings of Voice over IP (VoIP) make it an attractive technology for enterprise customers. Voice applications demand a higher level of network performance than 'best effort' data networks. Putting voice on the data network as part of a VoIP implementation creates performance, security, and interoperability concerns on existing data networks.

Voice traffic has more stringent performance requirements than data traffic. Traditional network components are not designed to handle voice and cause degradation of voice quality, create new avenues for security breaches, and impact availability of voice service. According to Infonetics Research, 68% of IP telephony deployments require router upgrades to support voice traffic. Jitter, latency, and packet retransmissions that may be tolerable for data traffic are major issues for voice, causing problems like poor voice quality and inadequate service availability. The data network performance is impacted by the additional voice traffic, affecting applications like email, document transfer, and Web performance.

Putting voice on the data network creates security and interoperability concerns with serious service impacts.

New security risks like toll fraud and eavesdropping are introduced. Additional points of entry are created, exposing the network to threats that compromise corporate data networks. A hacked VoIP system on the data network now provides a back door to the corporate LAN. Security risks range from viruses, worms, and denial of service (DoS) attacks to unauthorized access. Network infrastructure and IP telephony elements not designed to interoperate are another source of service disruption and poor voice quality.

Meeting VoIP Challenges: Secure and Assured Enterprise VoIP

VoIP deployments face challenges in the areas of performance, security, and interoperability. To overcome these challenges, all network infrastructure elements must be optimized to handle voice traffic. Network security and infrastructure elements must protect the entire network from the vulnerabilities introduced by VoIP. IP telephony applications and network infrastructure components must be jointly tested to ensure network security, availability and resiliency. Finally, network infrastructure and IP telephony vendors must commit to making interoperability a priority as new standards are introduced.

Juniper Networks, Inc. and Avaya have combined industry-leading routing, security, and IP telephony

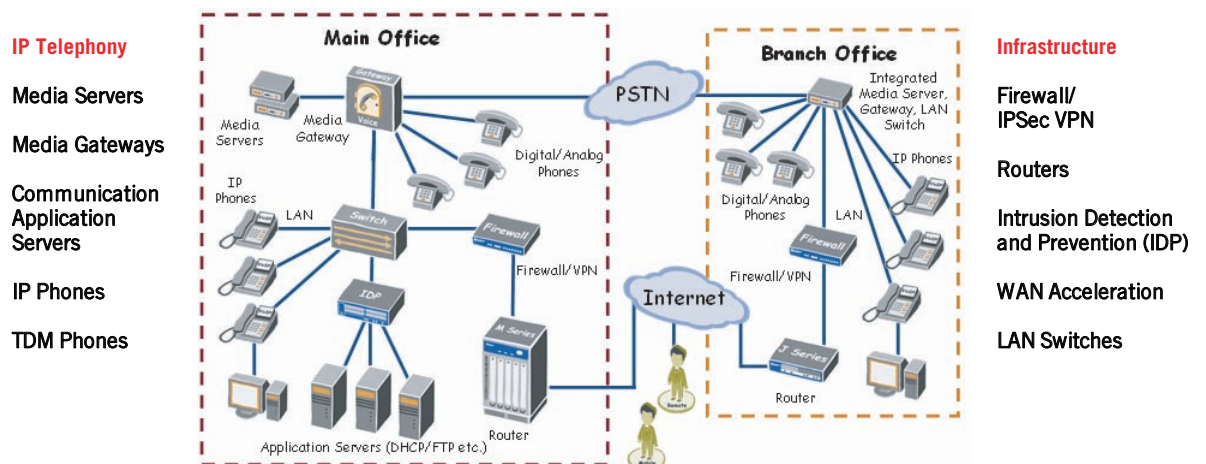


Figure 1—Juniper Networks infrastructure combines with Avaya IP telephony to deliver a complete, best-in-class enterprise VoIP solution.

products to provide an end-to-end IP telephony solution that address these key challenges of performance, security, and interoperability. All Juniper Networks infrastructure elements are capable of handling voice and designed to work with Avaya IP telephony applications to deliver a certified, best-in-class enterprise VoIP solution with security and performance unmatched in the industry (Figure 1).

Pervasive Security to Protect Corporate Assets

Juniper Networks and Avaya work together to provide pervasive security that spans the infrastructure as well as applications. Juniper Networks provides best-in-class network security designed to handle voice and work with Avaya IP telephony products to secure your converged voice and data network. Juniper Networks' ASIC-based security products offer superior performance and security for both voice and data traffic. The Juniper Networks ScreenOS security operating system includes application-level gateways (ALGs) that are voice-aware, recognizing Session Initiation Protocol (SIP) and the Avaya H.323 voice protocol to dynamically open and close firewall pinholes for incoming and outgoing calls only as needed. Traditional firewall solutions – which are not voice-aware – open a range of static ports for voice traffic and leave them open, exposing the network to security threats.

In addition to being voice-aware, Juniper Networks' security products feature innovative, market-leading security technologies such as support for SIP with Network Address Translation (NAT). NAT increases security by concealing a set of host addresses on a private network behind a pool of public addresses, thus securing those hosts from direct targeting in network

attacks. With Juniper Networks security, users send and receive calls through a NAT network while keeping the network secure. Other solutions do not have this capability and require a third-party device to perform this function, increasing both cost and complexity.

Table 1 summarizes some of the Juniper Networks security features that enable Avaya IP telephony.

Assured Service and High Availability to Meet Stringent Voice Requirements

The Juniper Networks and Avaya enterprise VoIP solution is designed to ensure voice quality, reliability, and availability, even when unexpected network events occur. The Juniper Networks infrastructure optimizes and protects voice and data traffic by ensuring transport separation and giving preferential treatment to voice traffic. Juniper Networks' VoIP-specific performance and high availability features provide the following critical benefits:

Performance:

- Ensure that voice gets appropriate priority on the data network to deliver superior IP telephony application performance
- Increase network efficiency by compressing voice packet headers over WAN
- ASIC-based hardware acceleration provides low-latency, low-jitter, high-availability packet transport for high quality voice communications

High Availability:

- Resilient Virtual Private Network (VPN) connectivity ensures that no calls are dropped, even when a failure occurs

Table 1 – VoIP security features and benefits enabling Avaya IP telephony

Security Feature	Benefit
• ALGs with support for SIP and Avaya H.323	• Dynamically opens and closes firewall pinholes as needed for voice traffic, minimizing network security risks
• Zone-based architecture	• Enables segmentation of VoIP network, separating traffic by type in order to apply appropriate policies and optimize access control
• Eavesdropping prevention	• Protects voice calls to ensure privacy of telephone conversations via high-performance VoIP encryption using site-to-site VPNs
• Unauthorized use prevention/ VoIP access control	• Prevents toll fraud and other forms of unauthorized access by employing policy-based access control for SIP and Avaya H.323
• Denial of service (DoS) protection	• Guards against system security breaches that render network services (including VoIP) unavailable to users

- Dynamic routing survives failures by automatically finding alternate routes to ensure IP telephony system availability
- Bi-directional Forwarding Detection (BFD) provides sub-second failure recovery to ensure voice calls are not interrupted if an IP link fails

Compliance Tested and Certified for Seamless Interoperability

Working together, Juniper Networks and Avaya are able to provide industry-leading performance and security for enterprise VoIP at the feature/functional level as well as the solution level. Through this strategic partnership, Juniper Networks and Avaya are able to leverage unique application- and infrastructure-level high availability mechanisms that maximize resiliency and availability without impacting network performance. This joint solution is compliance tested and certified under the Avaya DevConnect program to help ensure seamless interoperability. In addition, the strategic partnership between Juniper Networks and Avaya ensures that interoperability will continue to be a priority as VoIP evolves and new standards are introduced.

- **Custom application-layer gateway (ALG)** – Juniper Networks support for Avaya H.323 ALG enhances network security because it is able to work with the Avaya H.323 protocol to open pinholes for incoming and outgoing calls rather than opening a range of static ports to handle VoIP traffic.
- **Support for Session Initiation Protocol (SIP) anomalies** – Juniper Networks Intrusion Detection and Prevention (IDP) systems protect against known SIP anomalies to provide additional security for Avaya IP telephony applications.
- **Customized WAN Optimization** – Juniper Networks WAN acceleration products work specifically with Avaya IP telephony applications to provide additional bandwidth without incurring additional cost.
- **Support for Avaya IP Softphone** – Juniper Networks secure sockets layer (SSL) VPN products have been tested with Avaya IP Softphone and IPAgent to ensure secure and reliable access for authorized remote users.
- **Avaya DevConnect compliance tested and certified** – Juniper Networks infrastructure and Avaya IP telephony applications have been compliance tested and certified as part of the Avaya DevConnect program.
- **Strategic partnership ensures interoperability moving forward** – The strategic partnership between Juniper Networks and Avaya ensures that interoperability will

continue to be a priority as VoIP evolves and new standards are introduced.

Cost-Effective Implementation and Ongoing Management

Both Juniper Networks and Avaya are committed to an incremental deployment model that enables organizations to leverage their existing infrastructure investments. Juniper Networks' innovative and market-leading security technologies integrate well into the network, allowing for cost-effective deployment, configuration, integration, and ongoing management. The end-to-end enterprise VoIP solution offered by Juniper Networks and Avaya also takes advantage of the strength of Avaya Global Services and certified systems integrators to support all phases of the solution implementation, from design through ongoing management. Together, this means that Juniper Networks and Avaya are dedicated to providing the best Total Cost of Operations for enterprise VoIP customers.

- **Support for entire PDIO model** – Avaya Global Services or your preferred global systems integrators are prepared to handle planning, deployment, integration, and operation (PDIO) of this end-to-end solution from Juniper Networks and Avaya.
- **Smooth migration from TDM to IP telephony applications** – Working together, Juniper Networks and Avaya offer the products, operational scale, and technological expertise to transition your current telecom network to a state-of-the-art converged voice and data network.
- **Best-in-class solutions** – Juniper Networks and Avaya provide a complete, end-to-end enterprise VoIP solution that combines best-in-class network security and performance with IP telephony applications from the global leader in communication systems.
- **Evolve at your own pace** – Juniper Networks Secure and Assured network infrastructure can be deployed incrementally, based on your business needs, helping you to evolve your network over time.

Summary

Enterprises deploying IP telephony are faced with the challenge of creating a converged voice and data network that provides high performance and pervasive security to run the latest communication applications. Together, Juniper Networks and Avaya provide complete, end-to-end enterprise VoIP solutions featuring voice-aware security unmatched in the industry, assured VoIP performance, and proven interoperability. Juniper

Networks and Avaya are committed to cost-effective implementation and ongoing management strategies that enable organizations to leverage their existing infrastructure investments. Enterprises can be confident that the joint solution developed by Juniper Networks

and Avaya will help secure their converged voice and data network and continue to meet their performance and security requirements as their network evolves and as new applications are introduced.

Key Benefits

Juniper Networks Secure and Assured network infrastructure enables high-quality, reliable, and secure Avaya IP telephony communications via the following key features and benefits:

Firewall/ IPSec VPN	SSL VPN	Routing	Intrusion Detection and Prevention (IDP)	WAN Acceleration
<ul style="list-style-type: none"> • ALGs support Avaya H.323 to maximize network security • NAT support simplifies IP telephony implementation and boosts security • Policy-based virtualization enables network segmentation to control resources and enhance VoIP performance 	<ul style="list-style-type: none"> • Supports Avaya IP Softphone and IPAgent • Firewall-friendly SSL transport makes it easier for voice to travel through firewall • Flexible dual-mode transport supports both SSL and IPSec to improve performance for remote users 	<ul style="list-style-type: none"> • Improves bandwidth utilization and VoIP performance via cRTP packet compression • Minimizes latency, jitter, and packet loss to ensure voice and data performance • MPLS support to expedite VoIP traffic 	<ul style="list-style-type: none"> • Protects VoIP servers and clients from worms, Trojans, malware and other emerging threats and vulnerabilities • Protects against wide set of application-layer attacks including SIP- and H.323-based attacks 	<ul style="list-style-type: none"> • Increases existing bandwidth capacity to support VoIP • Improves performance of data components of other telephony applications (messaging, contact center, etc.) • Ensures minimal latency (~2ms) for both voice and data traffic

About Avaya

Avaya delivers Intelligent Communications solutions that help companies transform their businesses to achieve market-place advantage. More than 1 million businesses worldwide, including more than 90 percent of the FORTUNE 500®, use Avaya solutions for IP Telephony,

Unified Communications, Contact Centers and Communications Enabled Business Processes. Avaya Global Services provides comprehensive service and support for companies, small to large. For more information visit the Avaya Web site: <http://www.avaya.com>.

AVAYA
INTELLIGENT COMMUNICATIONS
avaya.com