

HEALTHCARE SOLUTION PORTFOLIO

Networking and Security best practices
that help healthcare providers improve
quality of care while lowering costs

Healthcare Solution Overview

Healthcare providers continually strive to deliver the highest quality care, make that care easily accessible, and deliver mission critical services at the lowest reasonable cost. To accomplish these goals, innovative healthcare organizations are increasingly leveraging their IT investments. There are several IT initiatives within the healthcare sector where Juniper Networks® can help. For those who deploy them, these initiatives are considered best practices to ensure the quality, safety and authorized availability of vital healthcare information and services. These initiatives include:

1. Security for wireless LAN (WLAN) deployments
2. Multi audience access
3. Data center consolidation and simplification
4. Firewall security upgrades
5. Intrusion prevention systems (IPS) deployments
6. Network-based user authentication
7. Resilient network routing
8. Supporting Electronic Medical Record (EMR) and Patient Health Information (PHI)

Challenges

For healthcare providers, the challenge to provide easily accessible, highest quality care is sometimes at odds with the challenges of containing the cost of care and maintaining the confidentiality of patient health information. For healthcare IT organizations, the challenge is to improve the quality of patient care through the use of innovative technologies, to enable reductions in patient care costs, and to provide security for PHI, limiting access to authorized users only. In short, the quality of patient care is often at odds with the cost of patient care, and authorized access to PHI is often at odds with the obligation to restrict access to only those who are authorized to have such access.

Trends

The growing trend among savvy healthcare IT executives is to leverage IT to create a business advantage by improving the quality of healthcare while reducing the cost of such care. In addition, the network that provides granular access control and heightened network security can ensure that proper access is granted to those with authorized access to PHI, while those without authorization are denied access. This serves to protect the healthcare facility from Health Insurance Portability and Accountability Act (HIPAA) non-compliance and to improve the audit process for HIPAA with granular audit reporting capabilities. Furthermore, IT is effectively leveraged to enhance the quality of patient care, improving the marketability of the healthcare provider while lowering total operating cost to also improve margins for the organization.

Juniper Networks Solution Portfolio for Healthcare

Security for Wireless LAN (WLAN) Deployments

Hospitals and clinics frequently deploy wireless LANs to ensure ubiquitous access throughout the healthcare facility. Patient monitoring, RFID tracking and telemetry may be connected to the wireless network via locators to provide connectivity and location tracking as it is moved from location to location within the facility. Additionally, healthcare providers will often use electronic tablets to transmit healthcare information and to record critical updates. This information can be immediately transmitted over the WLAN from the patient's bedside to the nursing station, or other central aggregation point with instantaneous updates to distributed locations throughout the healthcare system.

Many healthcare providers are turning to the Juniper Networks for access control as they secure their WLAN environment. This solution provides device access to a wireless LAN port and prevents access to the wireless LAN port if authentication fails. A benefit is that the user/device is authenticated before an IP address is provided, which adds to the robustness of security in this network port access solution.

Juniper's access solution for Healthcare consolidate clients into a single client across several devices and throughout the facility. This saves staff training time with one common client to learn, and it lowers ongoing support costs with one client to manage and support across the organization. In addition to providing robust port access control for wireless LANs, Junipers Access Control solution for healthcare can control port access on wired LANs throughout the facility as well. It offers a robust extensible framework (EAP) to exchange network security credentials and is integrated to provide powerful authentication and data privacy capabilities. Juniper's access control for healthcare supports Microsoft windows operating environments as well as Apple environments.

The combination of robust port access security with ease of use and lower support costs makes this an ideal solution for healthcare providers, as they strive to realize improved security with lower than traditional cost throughout their distributed facilities.

Multi-Audience Access

Physician, patient and additional partner portals are easy to create, deploy and support with Juniper Networks solutions for healthcare. Enhanced security is provided through access controls based on the user and device accessing the network. HIPAA and PCI requirements can be enforced with specific access rights to patient health and other information. Furthermore, a cache cleaner ensures that confidential information is not left on remote devices being used to access the network. Physicians may be granted access to confidential medical records while patients are granted access to a portal for scheduling appointments or other services that would otherwise be requested over the telephone or in writing.

These types of portals improve authorized and granular access control and serves to automate various requests for information while enhancing network security. The added security for remote access combined with the ability to consolidate remote access to a single solution serves to enhance user satisfaction, provider access to critical information, and lower total cost for healthcare providers.

Healthcare Data Center Consolidation and Simplification

Data center consolidation and simplification projects serve to lower cost and provide better infrastructure and security for confidential information. Both benefits can be achieved by reducing multiple complex data centers to a simple optimized deployment with fewer layers and boxes to manage and control. However, when data centers are consolidated from a large number down to a much smaller number, several IT issues must be considered. Traditional architectures that have stayed unchanged for over 10 years employ excessive switching layers, largely to work around low performance and low-density characteristics of the devices used in those designs. This growth in the number of devices also introduces new untested operating systems to the environment.

Juniper's leading data center consolidation solution includes Juniper Networks EX Series Ethernet Switches, MX Series 3D Universal Edge Routers, SRX Series Services Gateways, WXC Series Application Acceleration Platforms, and Network and Security Manager (NSM) and STRM Series Security Threat Response Managers. The EX Series Ethernet switches combine Virtual Chassis technology with wire-rate 10 Gigabit Ethernet performance, thereby reducing the number of networking devices and interconnections. The MX Series perform complex edge routing which can also provide intra data center stateful routing and failover. The SRX Series Services Gateways consolidate security appliances with distinct functions into a highly integrated, multifunction platforms that results in simpler network designs, improved application performance – and a reduction of space, power, and cooling requirements. The WXC Series Application Acceleration Platforms help with business continuity and disaster recovery planning by optimizing existing bandwidth during storage-area network synchronization between primary data centers and disaster recovery sites. STRM Series provides collaboration and cooperation between multi-vendor security & routing devices to root out stealthy and sophisticated attacks that evade point security products. NSM provides a single portal with end-to-end visibility across the data center for security, switching and routing infrastructure.

Firewall Security Upgrades

Modern firewalls are migrating to include Unified Threat Management (UTM) capabilities. These capabilities include antivirus, anti-spam, URL filtering, and intrusion prevention systems (IPS). By consolidating UTM within the firewall, healthcare IT staff can reduce the cost of deploying and maintaining a complex layered security architecture. In addition, this consolidation can serve to streamline purchasing, support and maintenance contracts for IT security solutions, adding to the savings in terms of administration and contract processing costs.

Although there are many benefits in consolidating threat management capabilities into a single platform, the obvious concern is that the IT staff may be forced to compromise on the quality of the solution in any one area (for example, sub-optimal throughput performance within the firewall hardware to support a high quality and properly integrated IPS implementation). Juniper's security solutions have been designed for full utilization of the integrated UTM capabilities without a degradation in performance. Additionally, Juniper has integrated best-in-class third-party solutions for UTM, so that healthcare IT staff are not forced into a single vendor deployment.

Intrusion Prevention Systems (IPS) Deployments

As data networking threats have migrated to the application layer, IPS is an increasingly essential layered security solution for the well protected organization. The Juniper Networks Security Solutions provide the most comprehensive intrusion prevention system with proactive security measures that identify, mitigate and report on security breaches in real-time. These methods include both signature-based detection and protocol anomaly detection. Given this comprehensive set of detection methods, the IDP Series can detect intrusions for which signatures have not yet been written.

Given the importance of security and compliance in all branches of the healthcare system and the fact that increasingly security risks are emerging from within the organization as opposed to outside of the organization, an IPS solution is a business necessity for today's healthcare provider. This solution is also an ideal and effective addition to ensure HIPAA and PCI compliance, as any solid compliance process must include effective auditing and reporting. Juniper's security solution, provides granular visibility and an audit trail to ensure and improve upon compliance and is typically a fundamental element of the network security audit process for HIPAA and PCI.

Network-based User Authentication

The Juniper Networks user authentication solutions are the industry-leading and de facto standard for RADIUS to provide Authentication, Authorization and Accounting (AAA) services. RADIUS is an essential building block of any robust network access control solution. Additionally for healthcare, should a network security breach occur, the accounting capabilities enabled by the solution can help to identify the source of the security breach almost instantaneously. Where a large number of diverse users have access to the network such as within healthcare provider environments, the solution enhances fundamental and necessary network security by providing granular access and control..

Resilient Network Routing

The requirements for resiliency in healthcare networks are an absolute requirement. Perhaps in no other industry vertical is the network, its applications and data as life critical as in healthcare. Routing infrastructure has become complex, is vulnerable to attack and can be overwhelmed at times, negatively impacting the entire organization. Juniper's routing platforms with Juniper Networks Junos® operating system are fundamentally designed to be highly resilient and stable to support life critical operations associated with the healthcare vertical. The most frequent reason for a network outage is a mis-configuration caused by human error. Junos OS is enhanced with commit commands and configuration role-back capabilities to greatly reduce the potential for human error and to quickly recover from such errors should they occur. Security is enhanced with a hardened OS that can withstand attacks and allow administrators to address them in real-time. The fundamental design in terms of hardware, software and design methodology allows Juniper to bring to market routing platforms and new software releases that are robust and highly stable to support life critical operations.

Supporting Electronic Medical Record (EMR) and Private Health Information (PHI)

Network access control (NAC) is an emerging IT solution category and an ideal solution for providing network access control for EMR and PHI. Juniper's solution for network access control is Juniper Networks Unified Access Control (UAC). UAC with the Juniper Networks provides coordinated network access and dynamic policy to firewalls acting as enforcement points on the network. UAC can grant policy-based access to EMRs and PHI on a per-user or per-device basis. Should security parameters change on the device accessing the network, UAC can dynamically address these changes and enforce the appropriate policy. By architecturally integrating RADIUS and 802.1X solutions (as discussed above), Juniper provides a comprehensive and robust access control solution, one that is scalable and can be cost-effectively deployed in the most sensitive areas such as a data center or across an entire healthcare organization.

Solution Planning, Implementation, and Deployment

Juniper has a professional services organization well versed in the healthcare vertical as well as partners allied to healthcare to assist in architecting and deploying these or other best practice solutions. As these solutions often have a significant level of integration with the existing healthcare providers IT infrastructure and systems unique to the industry, specialized experience is often necessary and greatly valued. Juniper's market leading solutions and experience in providing these and other solutions for healthcare providers, combined with the expertise of our partners who specialize in providing solutions across the healthcare industry, set Juniper apart from others in the industry.

Summary—Helping Healthcare Enjoy the Benefits of Networking Best Practices

Juniper is a leader in healthcare networks providing the infrastructure and security necessary to run a life critical network without sacrificing network performance or the security of private health information. The organization can support the changing healthcare landscape of more users accessing more applications from more devices over a more distributed footprint. Through the thoughtful use of IT innovation, today's healthcare providers have the opportunity to enhance the quality and accessibility of the care provided to patients with cost-effective solutions that increase staff efficiency and keep sensitive information secure and compliant.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

 Printed on recycled paper