

UNIFIED ACCESS CONTROL ADDRESSES HIPAA COMPLIANCE

Preserving the Integrity of Sensitive Patient and Business Data for Today's Health Care Organizations

Challenge

HIPAA requires health care organizations ensure that their networks and applications are secure, and that sensitive patient and business data is protected when in use, during transmission, or when stored. Health care organizations must also provide secure yet pervasive access to networks, applications and data for partners and contractors so they can be productive.

Solution

Juniper Networks Unified Access Control (UAC) reduces network threat exposure, delivers comprehensive control, visibility, and monitoring and decreases access control deployment cost and complexity. UAC extends access control to network traffic, mitigating risks and protecting sensitive corporate assets.

Benefits

- Flexible, secure, standards-based access control that leverages existing network infrastructure and components
- Protects networks, applications and data from unauthorized access, attacks and breaches
- Works with heterogeneous network components including any 802.1X compatible access point and switch, any Juniper firewall/VPN platform, or both

One of the only certainties in today's health care industry is that change is constant. Just as certain as change, though, is the ongoing requirement in health care organizations for robust data and network security. This is especially true given the demands placed on health care organizations by the Health Insurance Portability and Accountability Act (HIPAA), which makes network, application and data protection of paramount importance to the survival of today's health care organizations. Also of major importance is providing caregivers with access to up-to-date, accurate patient information—whenever and wherever it is required.

Add to these factors the importance for health care organizations to ensure that their users—not only employees but guest users including partners and contractors—have quick, simple access to the networked information and applications that they need to do their jobs, and it becomes apparent that health care organizations and their networks require a powerful network access control (NAC) solution. Such a solution must ensure strong authentication, advanced network protection, robust application-level access control, secure guest user access, network visibility and monitoring, and patient data accessibility, security and privacy, while addressing and adhering to regulatory directives such as those imposed by HIPAA.

The Challenge

Increased mobility and the extended enterprise introduce a host of new enterprise security challenges. Health care organizations are particularly susceptible to security breaches, worms, viruses and data leaks because of the sensitive nature of the information traveling over their networks. Confidential patient data—medical, personal and financial—must be protected, not only on the network but also as it is transmitted over wired and wireless LAN (WLAN) connections. Just as crucial is making data easily accessible to and usable by caregivers when needed and appropriate. Any delay in patient information or medical record access could be costly, even life-threatening to a patient.

However, as more mobile and diverse types of users—from health care providers and administrators to contractors and guest users—and their managed and unmanaged devices connect to the network, securing patient data and protecting the network and applications becomes an increasing challenge. Trusted employees working remotely or surfing the web from home or a wireless hotspot with a managed mobile device can inadvertently be infected with malware, such as a worm or trojan horse. And when that safe, known endpoint device reconnects directly to the health care organization's LAN via a wired or wireless connection, it can unknowingly unleash a malware attack, security breach, or other serious issue onto the network and on the data being stored on the network. Then there are contractors and partners who require access to the network, vital health care applications and sensitive patient and staff data using unmanaged devices. They too can unknowingly expose sensitive LAN resources to malware or breach. And, finally, there are guest users who may try to access the health care organization's wireless

network—or even their wired network, via an Ethernet jack in a waiting room, for example—to simply gain Internet access. These users can unintentionally launch a network malware attack, be the point of origination for a security breach, or accidentally stumble across sensitive data stored on or traversing the health care organization's network. For these reasons and more, controlling network and application access is essential to protecting the LAN and its resources in extended enterprises such as those in the health care industry.

In addition to the need for strict access controls are the mandates set forth by HIPAA, which places significant limits and imposes restrictive demands on patient safety, clinical automation, patient record privacy and medical error reduction. In addition to access control, HIPAA governs integrity control, person/entity authentication, transmission security, and information systems activity review. In short, HIPAA requires that health care organizations employ and monitor strict access control and AAA practices on all wired and wireless networks. This is a tall order, especially for networks like those in the health care industry where more and more workers are mobile, endpoint devices are increasingly diverse and may be shared between employees, and security policies are constantly in flux.

To effectively enforce security and access policies and reliably protect sensitive patient and employee data and health care applications from unauthorized users, health care organizations need a comprehensive access control solution. The solution must ensure that only authorized users access the network, enforce strict policy controls, and be able to work within the current network environment without causing disruption or requiring rip-and-replace, forklift upgrades.

Juniper Networks Unified Access Control and HIPAA

Juniper Networks® Unified Access Control (UAC) combines the best of access control and security technologies while enabling enterprises to leverage their existing network investments. For health care organizations, this means cost-effective, reliable protection for all confidential data, regardless of user device, role or location. UAC is a flexible, scalable solution that simplifies the deployment and management of network and application access control, resulting in quicker, cost-effective HIPAA compliance and better overall network security.

Built on the robust security and access control capabilities of widely deployed products such as the market-leading Juniper Networks SA Series SSL VPN Appliances, Odyssey Access Client (OAC), and SBR Enterprise Series Steel-Belted Radius Servers, as well as industry standards such as 802.1X, RADIUS, and EAP, and the open, standards-based specifications and architecture for network access control and endpoint integrity from the Trusted Network Connect (TNC), a work group of the Trusted Computing

Group (TCG), Juniper Networks Unified Access Control addresses vital HIPAA mandates, including:

- Access Control [§ 164.312(a)(1)]
- Integrity Controls [§164.312(e)(2)(i)]
- Person/Entity Authentication [§164.312(d)]
- Transmission Security [§164.312(e)(1)]
- Information Systems Activity Review [§ 164.308(a)(1)(ii)(D)]
- Unique User Identification [§ 164.312(a)(2)(i)]
- Automatic Logoff [§ 164.312(a)(2)(iii)]
- Encryption and Decryption [§ 164.312(a)(2)(iv)]
- Login Monitoring [§ 164.308(a)(5)(ii)(C)]
- Audit Control Standard [§ 164.312(b)]

Unified Access Control Components

Juniper Networks Unified Access Control incorporates three primary elements that together create a standards-based, session-specific access control policy for each user, leveraging existing network infrastructure and components:

Juniper Networks IC Series Unified Access Control Appliances is the hardened centralized policy server at the heart of UAC. Based on Juniper Networks market-leading SA Series SSL VPN Appliances and integrating RADIUS functionality from the well-known Juniper Networks SBR Enterprise Series Steel-Belted Radius Servers, the IC Series can push an agent down to the endpoint device, collect information about the user and their device including its security state from the agent, and serve as the interface with existing enterprise AAA infrastructure. Once user credentials are validated and the device security state established, the IC Series implements the appropriate access policy for each user/session and propagates that policy to enforcement points throughout the network.

The UAC Agent is a dynamically downloaded agent that can be preconfigured, provisioned in real time by the IC Series, installed using Juniper Networks Installer Service or deployed by other means. The UAC Agent collects user credentials and assesses the security state of the endpoint. It provides support for network access at Layer 2 using 802.1X via integrated functionality from the OAC and/or at Layer 3 in conjunction with Juniper firewalls. It includes an integrated, stateful personal firewall for dynamic client-side policy enforcement, as well as specific functionality for devices running the Microsoft® Windows® operating system, including IPsec VPN—enabling strong data encryption from the endpoint to the firewall—and Single Sign On to Active Directory. The UAC Agent also includes Host Checker functionality from the SA Series SSL VPN Appliance, which scans endpoints for a variety of security applications and states, including antivirus, anti-malware and personal firewalls and allows custom checks of

elements such as registry, specific files, processes and port status. It can also perform an MD5 checksum to verify application validity. User authentication, endpoint assessment, and access can also be provisioned via an agent-less mode for instances where software downloads are not practical.

Enforcement Points for UAC include any 802.1X compatible switch—such as Juniper Networks EX Series Ethernet Switches—and wireless access points for Layer 2 enforcement, and/or any Juniper Networks firewall/VPN platform, including Juniper Networks SSG Series Secure Services Gateways and ISG Series Integrated Security Gateways with IDP Series Intrusion Detection and Prevention Appliances, as overlay enforcement points for Layers 3-7 enforcement. Such flexibility enables smaller deployments and delivers investment protection.

Juniper Networks Comprehensive Solution for Standard-based Access Control

UAC incorporates three different levels of session-specific policy, including authentication/authorization, roles and resource policies. Together these different policy types can be used to create extremely fine, granular access control that is easy to deploy, maintain and modify.

When a user with an endpoint device connects to a network with UAC deployed, the IC Series maps the user and device to a role using information collected by the UAC Agent or Host Checker (in agent-less deployments). Once network credentials are submitted, the IC Series combines the credentials and group or attribute information with other data such as endpoint security state and network location. The IC Series features a comprehensive AAA engine for seamless deployment into the most popular authentication settings and data stores.

The IC Series then dynamically maps the user to a role for the session. Role attributes can include session attributes and parameters, and specify restrictions with which the user must comply. This is extremely useful in organizations governed by HIPAA, where security is vital and compliance is mandatory.

Finally, the resource policy that governs network and resource access is assigned. Examples include Layer 2 RADIUS attribute-based policies such as VLAN assignments and/or vendor specific attributes (VSAs), as well as Layer 3 policies that govern access to IP addresses, ports or ranges of policies listed previously. Layer 7 policies, such as intrusion prevention system (IPS) policies or URL filtering, provide additional levels of dynamic threat management. Each policy layer adds granularity to overall access control.

UAC also leverages the capabilities of the IDP Series to deliver broad application traffic visibility, which isolates threats to the user or device level and employs an applicable policy action against the offending user or device via UAC enforcement points, which include any 802.1X compatible access point and/or switch—such as the EX Series Ethernet Switches—and/or any Juniper firewall platform. UAC can also correlate user identity and role information to network and application access, addressing many of the strictures of HIPAA.

Features and Benefits

UAC combines the best of security and access control technologies while leveraging existing enterprise network investments and deployments to deliver dynamic, unique session-specific access control policy for each user based on their identity, device security state, and location, addressing the requirements of regulatory compliance by:

- Protecting the enterprise network from access by unhealthy, non-compliant, and/or malicious endpoint devices
- Maintaining network access control, security and health regardless if endpoint devices are shared, managed, unmanaged, or unmanageable
- Enforcing access and security policies across the network via any new or existing vendor-agnostic, 802.1X-enabled access points or switches, including the EX Series Ethernet Switches, any Juniper firewall/VPN platform, or both, saving time and providing network investment protection
- Granularly controls access to mission critical applications and sensitive data, allowing access by only authorized users and devices
- Employs strong data encryption from the endpoint device to the firewall and into the network, securing and protecting data in transit from external and internal threats
- Dynamically identifies guest users—including contractors and partners—granting them appropriate, differentiated network access as defined by the enterprise
- Coordinated Threat Control isolates threats to the user or device level and applies a suitable policy action against threatening users and/or devices when used in conjunction with the IDP Series, addressing “insider threats”

Secure Good Health for Your Applications and LAN

Flexible, easy to manage and deploy, and built upon field-tested components used in thousands of deployments worldwide, industry standards, and open specifications, UAC is the ideal solution for health care organizations seeking to preserve the integrity of sensitive patient and business data. Caregivers enjoy enhanced user mobility and data access, while health care organizations realize operational efficiencies and simplified HIPAA compliance. The result is improved quality of care, reduced costs, greater protection for sensitive data and applications, and in general, a healthier network infrastructure for wired and wireless LAN connections in health care organizations.

Next Steps

For more information about Juniper Networks UAC, visit www.juniper.net/uac.

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

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

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.