

JUNIPER NETWORKS SOLUTIONS FOR HIPAA SECURITY STANDARDS COMPLIANCE

HIPAA Compliance with Remote Access, Security Zones, and Threat Mitigation with Compliance Auditing

Challenge

To secure and prove compliance for sensitive private healthcare information (PHI) while keeping the network open for authorized use.

Solution

Implement a layered security compliance approach with remote access, security zones and threat mitigation with compliance auditing for HIPAA compliance.

Benefits

- Network users are segmented onto multiple security zones to restrict access to sensitive PHI.
- Remote access is granted to authorized users of PHI, while access is denied for those without proper authorization.
- Network based access and actions are logged to provide detailed compliance reporting in support of compliance processes.

Juniper Networks® provides reliable networking solutions for the healthcare market to help customers meet HIPAA compliance requirements while improving patient care and business productivity. Juniper secures healthcare networks, and better enables a productive healthcare environment through secure and scalable remote access, HIPAA security zones and threat mitigation with support for network-based compliance auditing.

HIPAA security standards, although technology agnostic, specifically state required and addressable implementation specifications. Juniper Networks solutions are ideal for addressing many of the security standards requirements and assist HIPAA covered entities in protecting private healthcare information (PHI).

The Challenge

In today's rapidly changing environment, the HIPAA Compliance Officer must frequently evaluate emerging threats to HIPAA compliance and the overall state of compliance for the organization. New workforce enabling technologies, trends in patient care, and network-based threats are placing new demands for solutions to maintain HIPAA compliance (as depicted below). These new technologies, trends, and threats require frequent assessments and enhancements to support HIPAA compliance.

The goal is to keep private healthcare information secure and protected, yet available to those who require and have the authority to access such healthcare information. Given the large number of authorized and non-authorized personnel and contractors within a healthcare organization, this can be a very difficult task. Rigid rules and strict enforcement are required in real-time to simultaneously provide access and protect these sensitive healthcare records.

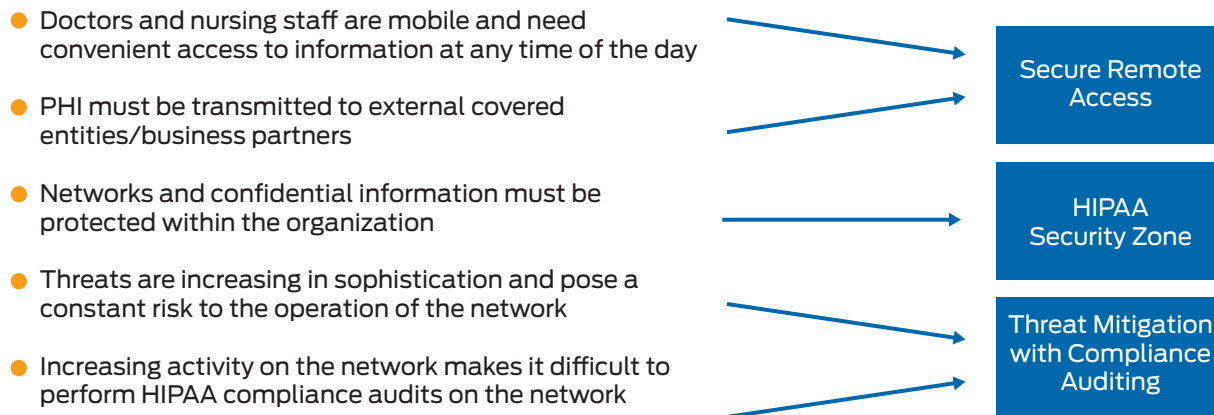


Figure 1: Trends driving HIPAA compliance

Juniper Networks HIPAA Security Standards Compliance Solutions

Juniper has three recommended solutions to help provide HIPAA compliance—remote access, HIPAA security zones, and threat mitigation with compliance auditing.

Remote Access

Extending remote access to the healthcare mobile workforce improves efficiency and patient care. Additionally, remote access has become a critical tool for disaster recovery. By enabling the distributed healthcare enterprise and mobile healthcare workers, Juniper enables healthcare providers to:

- Provide the highest levels of responsive patient care with the network leveraged as a strategic resource to meet these needs.
- Provide VPN access solutions for healthcare workers; enabling remote caregivers to obtain the information they need, when they need it, and to make diagnosis and provide proper care.
- Protect the network as a resource and the privacy and rights of patient private health information PHI.

In figure 2 below, remote access is provided to PHI for HIPAA covered entity partners, branch offices and clinics, healthcare providers working from home offices, and to the data center for record storage. Remote access can be configured not only to encrypt PHI, but also to limit access to applications based upon user and device to provide an additional layer of security.

No one VPN solution is the “right” solution for every unique mobile worker or distributed site situation. Therefore, Juniper is well positioned with a complement of SSL-, IPsec-, and MPLS-based VPN solutions to work with healthcare providers to determine which VPN solution is the best for your unique needs and requirements. Enhanced with user access auditing capabilities, Juniper Networks VPN solutions are ideal for meeting HIPAA compliance requirements.

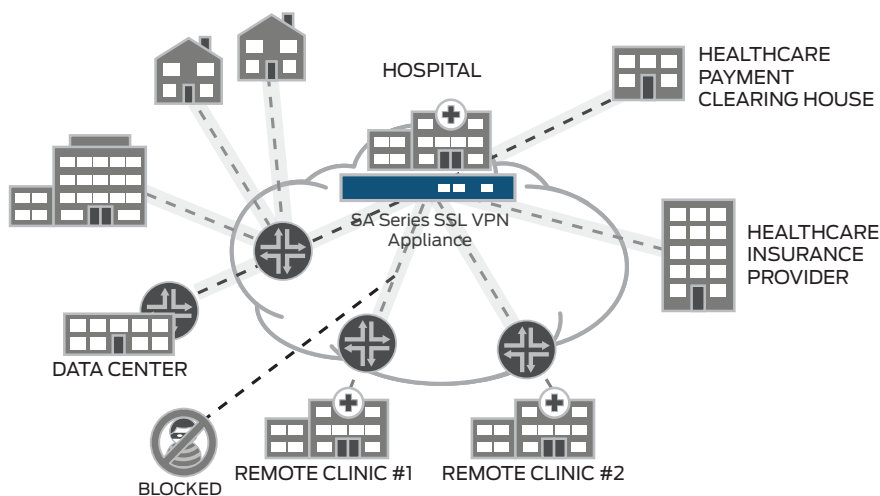


Figure 2: Remote access for HIPAA

HIPAA Security Zones

When deploying HIPAA security zones, the firewall enables the creation of security zones. Security compliance needs dictate use of a firewall that is capable of securing the network up to the application layer (layer 7) with deep packet inspection and protocol anomaly detection. The firewall technology should:

- Support flexible configurations with advanced security capabilities to prevent sophisticated attacks and protect the HIPAA compliance zone from internal as well as external threats.
- Enable virtualization to support multiple zones while consolidating management and lowering total IT network security cost.
- Scale with respect to application and user performance demands to meet the needs of home workers and smaller branch offices as well as the needs of large centralized hospitals.

Juniper Networks provides the level of security and network protection required for HIPAA security zones in a family of firewall solutions that scale to meet the many diverse needs within healthcare. Juniper Networks firewalls can be virtualized, creating multiple zones, while minimizing the cost of deploying multiple firewalls and significantly reducing the cost and time of managing the firewall security.

Juniper Networks firewall solutions can help to provide HIPAA compliance by limiting access to PHI to those who are authorized to access such information. With hardware platforms designed for firewall functionality, the platforms are optimized to protect the network while minimizing delay of critical and real-time applications.

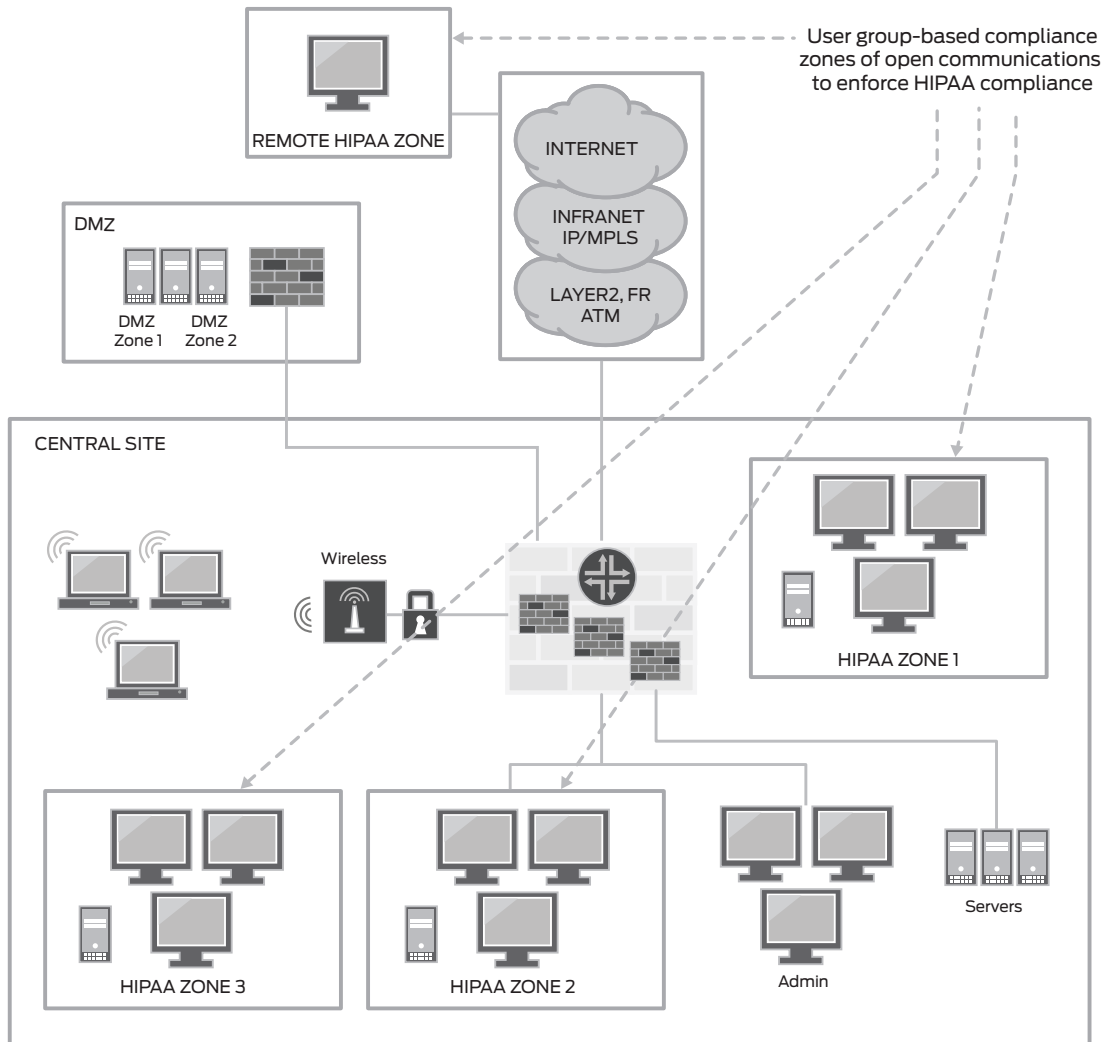
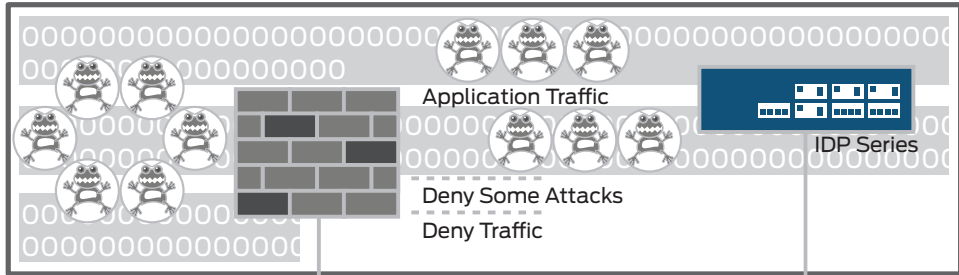


Figure 3: HIPAA security zones

Threat Mitigation with Compliance Auditing

The Juniper Networks IDP Series Intrusion Detection and Prevention Appliances can be deployed to address several of the HIPAA security standards. Specifically, the IDP Series addresses possible external and internal threats, identifies use of unauthorized applications, and provides detailed network-based compliance auditing. The IDP Series must:

- Detect and prevent network-based attacks as they occur with industry leading technology.
- Scale to meet the diverse sets of requirements within healthcare to provide high-end processing throughput while detecting attacks.
- Provide robust audit and reporting capabilities to support the auditing and accountability of compliance.



Firewall blocks most, but not all attacks, and cannot detect unauthorized applications that weaken security

The IDP Series extends a layer of security that the firewall is not able to provide

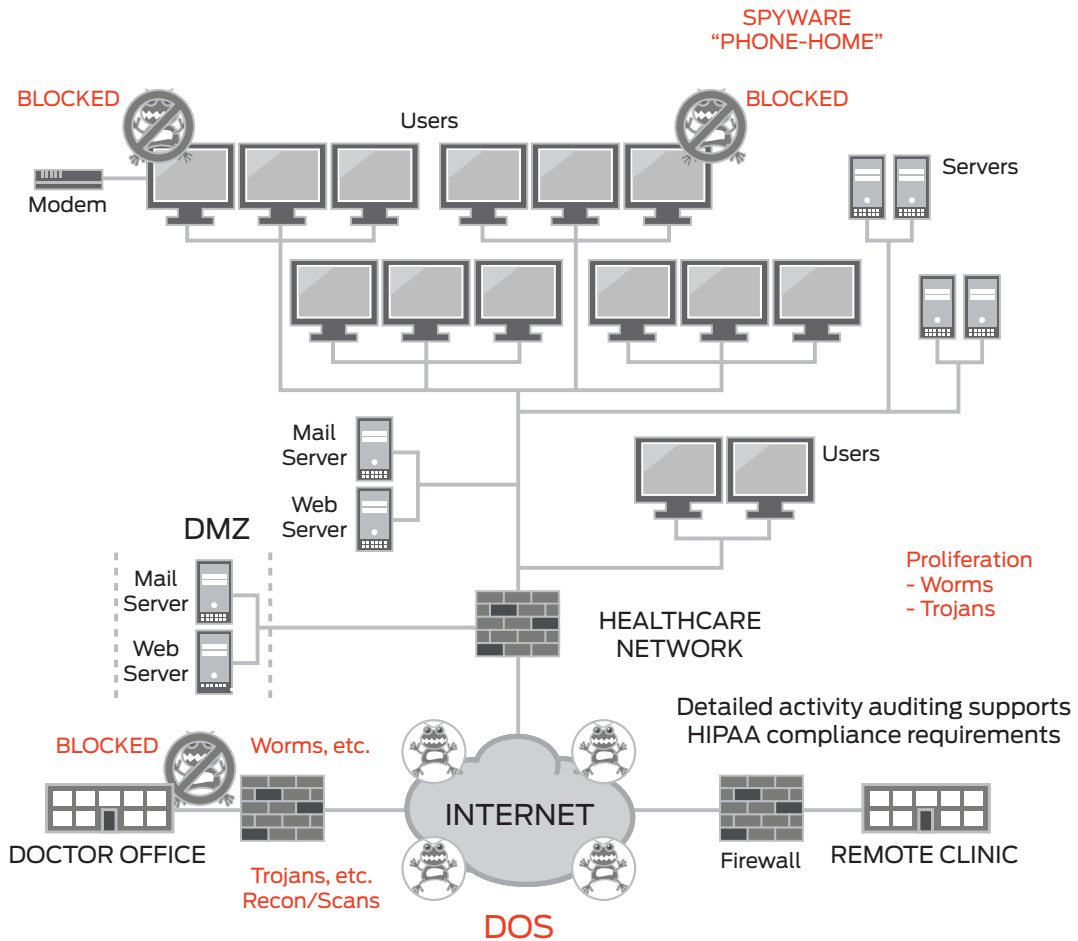


Figure 4: Threat mitigation with compliance auditing

Not only does the IDP Series protect against network-based attacks, but it operates at high speed to minimize latency in the network. In addition to detecting attacks, IDP Series can identify threats while eliminating false positives. The ability to eliminate false positives makes Juniper Networks IDP Series Intrusion Detection and Prevention Appliances operationally efficient to manage and support at any scale in a healthcare provider's network.

For HIPAA-covered entities, an important step in providing compliance is to audit the existing compliance process and improve upon this process to ensure the continual use of best practices. The IDP Series can be very useful in helping covered entities to assess their current state of compliance and to develop and implement process improvements. The detailed auditing capability of the IDP Series provides unique insights to aid in the HIPAA compliance decision-making process.

Features and Benefits

HIPAA security zones segment areas of the network where PHI is stored and transmitted. This segmentation of the network limits access to PHI and is a significant first step towards protecting PHI and meeting HIPAA compliance requirements. This allows HIPAA compliance officers to focus on a smaller portion of the network where PHI is stored and transmitted and can offer a significant reduction in network security investment to meet HIPAA compliance.

Many caregivers are increasingly becoming more mobile as heightened focus is being placed on providing the best possible care. It becomes very challenging to ensure healthcare providers have the proper information they require with the mobility they require. Fortunately, Juniper Networks remote access solution addresses this requirement by providing encryption for PHI transmitted to and from remote care providers with dual token authentication, granular application access and auditing. This remote access solution makes PHI available to those who should have it while preventing access to those who should not have access.

Having firewall based security zones and secure remote access may not necessarily stop someone from attempting to gain unauthorized access to protected PHI. For this reason, threat mitigation with compliance auditing is an essential security layer in providing HIPAA compliance. Juniper's solution can detect attacks and unusual behavior to stop these attacks in real time and provide compliance audit reporting to assist in identifying the source of the attack. This solution can greatly reduce the potential for someone to successfully hack the network and steal protected PHI.

Solution Components

Juniper Networks firewalls are the primary component for providing HIPAA Security Zones. These firewalls can scale from small branch office locations to very large hospitals and data centers. Integrated security solutions such as unified threat management, anti-virus and URL filtering can be integrated into the firewalls.

Juniper Networks SA Series SSL VPN Appliances are the security solution for providing secure remote access to PHI for remote and mobile care givers. This solution is easy to use and cost effectively scales from just a few users to thousands of remote access users. Because of its intuitive interface, little demand is placed upon help desk resources to support large scale deployments.

The IDP Series and Juniper Networks STRM Series Security Threat Response Managers make up the ideal solution to provide attached detection and compliance reporting for HIPAA. The IDP Series can either be deployed integrated within the Juniper Networks ISG Series Integrated Security Gateways or as a standalone platform. The STRM Series add to the ability of the IDP Series to detect abnormal behavior by collecting data from multiple devices across the network.

Solutions for the HIPAA Compliance

Modern healthcare practices and technology enabled trends require the healthcare provider and other covered entities to extend the reach of their network and open it to an increasingly mobile workforce while supporting secure and efficient communications and maintaining HIPAA compliance. As the network perimeter becomes increasingly dynamic, appropriate steps must be taken to ensure the operational quality, reliability, and security of the network. Granular network-based auditing must be enabled to make intelligent choices for HIPAA security standards compliance and to enforce policy.

Juniper enables healthcare providers and other HIPAA covered entities with the best available solutions for providing secure communications with remote and mobile VPN access, enhanced security with HIPAA security zones, and threat mitigation with compliance auditing. These solutions may be deployed as a complement or to provide a significant portion of the HIPAA compliance solution while improving the quality of patient care across the organization. Based upon technology, innovation, and market share, Juniper is a leader in each of the solution categories addressed above and provides the best possible high-performance solution for your organization. For further information regarding HIPAA security standards, please refer to the HIPAA Final Ruling and Code of Federal Regulations.

Next Steps

Contact your Juniper account representative to learn more details about this solution and how it can help you to achieve and maintain proper HIPAA compliance.

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.