Challenges
For productivity’s sake, users expect real-time access over almost any device to network resources, applications, and data. This places untold pressure on an organization and its network to ensure controlled, consistent network access independent of access method.

Solution
Juniper Networks provides a secure, comprehensive enterprise-wide access control solution that is fast and simple to deploy, administer, and maintain and that delivers consistent policies and user experience—a requirement for all organizations today.

Benefits
- Enhances network and application security and access protection
- Reduces deployment complexity significantly
- Enables faster, simpler access control deployments
- Delivers substantial administrative time and cost savings
- Provides a faster ROI

In today’s fast-paced, 24x7 global market, employees, customers, partners, and other network users demand pervasive, real-time access to network resources, mission-critical applications, and sensitive data from virtually anywhere, at anytime through nearly any device. This is a requirement by today’s users so that they can simply do their jobs, be productive, and in general, enable their employers—today’s high-performance organizations—to be competitive and successful. These ever-increasing demands, however, place extraordinary pressure on high-performance networks, not to mention those who manage those networks. As the mandate for productivity escalates and the number of employee and non-employee network users explodes, the need for open access to these networks is critical. At the same time, it is imperative that IT managers can administer and provision these open networks through a single management tool.

The Challenge
Today’s high-powered businesses are confronted with many challenges. One challenge they face is to provide their expanding, diverse user population—which includes employees, contractors, partners, customers, even guests—with anytime, anywhere, secure yet pervasive network access. These organizations are also challenged to deliver suitable network credentials and authorization for their growing network of users and to provide them with appropriate, differentiated access to vital networked resources and applications. This enables them to be productive regardless of user location or the endpoint device used. These challenges must be addressed, all the while ensuring that the network and the organization’s resources and sensitive assets remain secure, private, and protected.

Globalization allows organizations to expand beyond traditional corporate boundaries, leveraging resources around the clock and around the world. The number of employees who work while they are mobile or outside of an office environment is increasing. These challenges reinforce and dictate the need for scalable, adaptable anytime, anywhere access control.

Compliance with various industry and governmental regulations and requirements—such as the Sarbanes-Oxley (SOX) Act, Payment Card Industry (PCI) Data Security Standards (DSS), and many others—and the requirement to prove adherence to these regulations are a “must” for any organization today. Organizations must also address secure remote and local network access for off-shoring and outsourcing, business continuity and disaster recovery in today’s volatile world, and protection from the growing specter of insider threats. These factors, alone or in tandem, place an incredible strain on any organization’s network, and in particular its access control solutions. They also place a huge burden on the individuals charged with managing and protecting vital network resources and assets. Secure, comprehensive access control that is fast and simple to deploy, administer, and maintain from a single, centralized location is a must for all organizations, regardless of size and scope.
Unified, Centralized Access Policy Management

Juniper Networks® Unified Access Control (UAC) and Juniper Networks SA Series SSL VPN Appliances, when deployed with Juniper Networks Network and Security Manager (NSM), enable today’s high-performance organizations to centralize the management and provisioning of enterprise-wide access control. This solution allows IT managers to provision and manage access control policies for both Juniper Networks UAC and SA Series appliances centrally rather than use separate management tools for each device. This combination delivers comprehensive, unified security and infrastructure management, significantly reducing the time to configure access control policies, saving administrative time and cost, and enabling quicker, easier remote and local access control deployments.

Juniper Networks NSM delivers enhanced network and security management in a single application across Juniper’s security, access control, routing, and switching devices. It provides device and security policy configuration, comprehensive monitoring, reporting tools, and tools for investigating potential network security threats, all from a single user interface. Businesses can consolidate and simplify management of their network infrastructure. This increases their networks’ security, reduces cost and network management complexity, and allows them to enjoy operational gains and reduces OPEX.

NSM provides consistent monitoring and network device management across Juniper’s portfolio of network, security, and access control products, including:

- Juniper Networks SA Series SSL VPN Appliances
- UAC Policy Management Servers
- Juniper Networks EX Series Ethernet Switches
- Juniper Networks family of firewall platforms, including the Juniper Networks SSG Series Secure Services Gateways and ISG Series Integrated Security Gateways
- Juniper Networks IDP Series Intrusion Detection and Prevention Appliances
- Juniper Networks J Series Services Routers

NSM delivers efficient network-wide policy control and centralized management—and it enables policy changes to be implemented across a network, mitigating threats. It also complements the Juniper Networks STRM Series Security Threat Response Manager, enabling the versioning of policies, complete with policy rollback capabilities. It also supports a full set of management functions through its schema-based management architecture, delivering extensibility. And, through its role-based administration, NSM secures, protects, and delivers network-wide device management and control.

SA Series appliances are Juniper’s market-leading secure remote access appliances that offer full-featured flexibility. They use SSL transport, the secure access protocol built into every standard Web browser. By using SSL, the SA Series appliances eliminate the need for preinstalled client software on every device and the incumbent cost and complexity of installation, configuration, and maintenance associated with traditional IPsec VPN remote access solutions. It also allows any Web-enabled device to securely access an organization’s resources. The temporary VPN connections—via SSL that browsers establish—also eliminate the firewall and Network Address Translation (NAT) issues of traditional IPsec VPN remote access products. The browser-based approach of the SSL VPN appliances also allow mobile users access to corporate network resources securely through a number of devices such as PDAs, smartphones, Internet kiosks, or even their own computer in a hotel room.

SA Series appliances authenticate each user’s identity and verify the security and posture of the endpoint device requesting access before network access is granted. They check the posture of the requesting device, scan for malware, verify operation of endpoint security software—such as antivirus and personal firewalls—and examine the device’s IP address, browser type, and digital certificates, using the results to grant or deny access based on corporate security policies. They continue to check policy compliance of the user and device throughout the network session. Should the user or device posture change and become non-compliant, SA Series appliances can modify access permissions as well. Secure Access appliances provide security for enterprise tasks, with options for increasingly stringent levels of access control to protect even the most sensitive applications and data. They deliver best-in-class security, performance, reliability, and ease of management. SA Series appliances enable organizations to deploy differentiated remote access to resources based on user roles and groups. SA Series appliances can be deployed from the largest, most complex enterprise remote access environments, to smaller businesses that place a high value on network security.

UAC is Juniper’s standards-based, comprehensive local network access control solution. It combines user identity, device security state, and network location information to create a unique, dynamic access control policy, per user and per session. It incorporates different levels of session-specific policy, including authentication/authorization, roles, and resource policies to create extremely granular access control that is easy to deploy, maintain, and modify. Policies can change dynamically as the endpoint or network environment changes. All policy is created and pushed by the Juniper Networks UAC hardened, centralized policy management server. The UAC Agent—which determines and captures user identity, device state, and network location—can be dynamically downloaded by the UAC Controller to an endpoint device, or be deployed in several other ways. Juniper Networks UAC also offers an agent-less mode for instances where installing a software client is not feasible, such as with guest user access. Endpoint devices that attempt LAN connection are scanned for a variety of security applications and states, including antivirus, anti-malware, and personal firewalls. UAC also enables custom checks of elements such as registry and port status, and it can perform an MD5 checksum to verify application validity. The UAC Controller utilizes the information gathered by the UAC Agent (or in agent-less mode) to create dynamic policies that are propagated to network enforcement points across the distributed network.
Juniper Networks UAC can enforce policy at Layer 2 using any vendor-agnostic 802.1X-enabled wireless access point or switch, including the Juniper Networks EX3200 and EX4200 Ethernet Switches; at Layers 3 through 7 using any Juniper firewall platform, including the SSG Series and ISG Series; or both for greater access control granularity. It can also be provisioned in mixed mode, using 802.1X for network admission control and a Layer 3 overlay deployment for resource access control. UAC offers best-in-class performance and scalability. It can integrate the capabilities of the IDP Series to deliver broad application traffic visibility, mitigating insider threats. Juniper Networks UAC reduces threat exposure, delivers comprehensive access control, visibility, and monitoring, and centralizes policy management. It can also integrate the capabilities of the IDP Series to deliver broad application traffic visibility, mitigating insider threats. Juniper Networks UAC reduces threat exposure, delivers comprehensive access control, visibility, and monitoring, and centralizes policy management.

By deploying SA Series appliances and UAC together, with NSM to manage access control devices and policies, high-powered organizations can enjoy a substantial administrative time and cost savings. They can also ensure that consistent network access policies are deployed and enforced uniformly across their network, securing access from remote and local users. With this combined solution, organizations can create common configuration templates that can be shared between SA Series appliances for remote network access control and UAC for local network access control. This sharing of configuration templates for remote network access (SSL VPN) and local network access (UAC) enables a consistent access control experience for users, regardless of their means of network access. This interoperability between, and sharing of, remote and local network access policies cuts ongoing administrative costs by substantially reducing policy configuration time for remote and LAN-based access. The ability for SA Series appliances and UAC to share user and device information also allows for the seamless enablement of access control policies across an entire network. This leads to quicker, easier global access control deployments, faster ROI and stronger network and application access protection. It also enables organizations to deliver uniform remote and local access control policy implementation and enforcement across the distributed network. NSM, deployed with SA Series appliances and UAC, together provide high-powered organizations with a comprehensive means to secure and control their network access, regardless of how a user or device attempts access.

**Features and Benefits**

NSM deployed with SA Series appliances and UAC enables Juniper Networks to deliver the industry’s most robust, comprehensive unified security and infrastructure management solution, which:

- Offers enhanced network and security management functions in a single application for Juniper’s security, access control, routing and switching devices
- Provides centralized provisioning of enterprise-wide access control
- Extends standards-based access control—simplifying rollout and deployment, reducing cost and administration

**Juniper’s Centralized Access Policy Management Solution Components**

Juniper Networks delivers the first comprehensive, unified security and infrastructure management solution, centralizing access control policies and policy management in a single application:

- Network and Security Manager (NSM) is a powerful, centralized management solution that controls the entire device life cycle for Juniper Networks firewall/IPsec VPN platforms; SA Series appliances; UAC policy management servers; J Series routers; IDP Series; and EX Series switches. NSM handles the basic setup and network configuration with local and global security policy deployment for these products.
- SA Series appliances extend clientless secure access to companies of all sizes, from small to medium businesses (SMBs) that need access for remote/mobile employees to large global deployments that need to provide remote and/or extranet access for employees, partners, and customers from a single platform. Enhanced access methods enable the enterprise to dynamically provision access by purpose for virtually any application, including those that are jitter or latency sensitive.
- UAC combines user identity, device security state and network location information for session-specific access policy by user, leveraging existing network infrastructure. The standards-based UAC reduces threat exposure, delivers comprehensive control, visibility, and monitoring, and decreases access control deployment costs and complexity.

![Image: Centralized Policy Management with Juniper Networks NSM, SA Series and UAC](image-url)
Summary – Centrally Managing Policies

Organizations and their administrators struggle with the challenge of balancing secure, controlled access to their networks against ensuring that their mission-critical applications and sensitive data remain protected and private, even with the growing requirement to provide anytime/anywhere, pervasive network and application access to an onslaught of users and devices. These same organizations must also address critical issues such as outsourcing and off-shoring, business continuity, and insider threats. They must address industry and governmental regulations and associated audits, proving their compliance with and adherence to regulations. Delivering secure, comprehensive, consistent access control policies and policy enforcement enterprise-wide, regardless of network access method is a necessity for today’s high-powered organizations.

Juniper Networks, through the deployment of NSM, its market-leading SA Series appliances for remote network access, and its comprehensive LAN-based NAC solution—UAC—delivers the first comprehensive unified security and infrastructure management solution, centralizing access control policies and policy management in a single application. Juniper Networks’ solution for centralized access control policies and policy management eases administrative burden, maximizes efficiencies, reduces configuration and deployment cost, time, and complexity, and ensures a consistent user experience, which further reduces cost and increases user productivity.

Next Steps

For more information on Juniper Networks Network and Security Manager (NSM) please go to: www.juniper.net/nsm.

For more information on Juniper Networks SA Series appliances, please go to: www.juniper.net/sa-series.

For more information on Juniper Networks Unified Access Control, please go to: www.juniper.net/uac.

For pricing and ordering information for any of the mentioned Juniper Networks products, please contact your Juniper Networks sales representative at 1-866-298-6428 or an authorized Juniper Networks reseller.

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.