

White Paper

Juniper Networks Unified Access Control (UAC) and EX-Series Switches

Meeting Today's Security Challenges with End-to-End Network
Access Control



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Executive Summary

Network access control (NAC) has become essential for enterprise networks. Changing business practices, regulatory demands and an explosive growth in vulnerabilities are driving enterprises to control who may be admitted to the corporate network and what resources—servers, applications, stored data and the like—they may access. Businesses have essentially begun proactively enforcing corporate access policies because the risks are just too high to simply trust that all users will adhere to security and access policies on their own.

The automation of business processes has increased corporate dependence on network-based information for everything from initial customer contact and order entry to fulfillment and billing. At the same time, the user community has become more diverse and corporate boundaries have become more elastic. Outsourcing and the growing use of contractors mean IT must provide network and application access to a dynamic work force with differing needs and operating from numerous locations. Corporate “outsiders” such as customers and guests have even come to expect Internet access at the very least from waiting areas and conference rooms.

In addition, the adoption of new technologies such as voice over IP (VoIP) and the enterprise LAN’s transformation into a converged communications infrastructure have led to a proliferation of new devices on the network, such as IP phones, security cameras, bar code readers and industrial robots.

Amidst this new era of openness, enterprises must ensure compliance with industry and governmental regulations, and they must demonstrate that they have stringent access controls in place to protect critical, sensitive data ranging from finance and credit card information to patient health records.

These changes in business operations have created security vulnerabilities that are compounded by an explosive growth in malware and breaches. Outbreaks are targeting more devices and are moving more rapidly, and the time between patches and a new threat is shrinking. Given the threats that user mobility brings about, and the diversity of devices that request connection to the network, there’s really no longer a completely “trusted” user or device.

Introduction

In today’s business environment, enterprises need to establish and enforce dynamic, continuous pre- and post-admission network access controls to ensure that users operate within corporate policies. These controls must operate from the LAN edge to the data center and apply to all classes of users and devices. Juniper Networks designed its Unified Access Control (UAC) solution to address this set of challenges. UAC utilizes user identity, device security state and location information to create dynamic, session-specific access controls that are distributed and enforced across the network. As an end-to-end network access control system, the Juniper UAC solution enables enterprises to tackle the most pressing security issues they face, including network protection, guest access control, network visibility and monitoring, application access control that is aligned with roles and responsibilities, and differentiated services based on identity-based quality of service (QoS) control.

Scoping Network Access Control

While there is agreement that there is a need for network access control in enterprises, there is no consensus about what constitutes such a solution. While vendor implementations vary, a robust network access control solution should be able to provision network and application access based on a user’s identity; the role or network groups to which a user has been assigned; the health and/or security state of the user’s device (also referred to as endpoint assessment or host posture); network location; and the network attributes, such as bandwidth, QoS priorities and virtual LAN (VLAN) membership, assigned to a user or device. A network access control solution needs to function dynamically, addressing and modifying user and/or device access based on the authentication and security state.

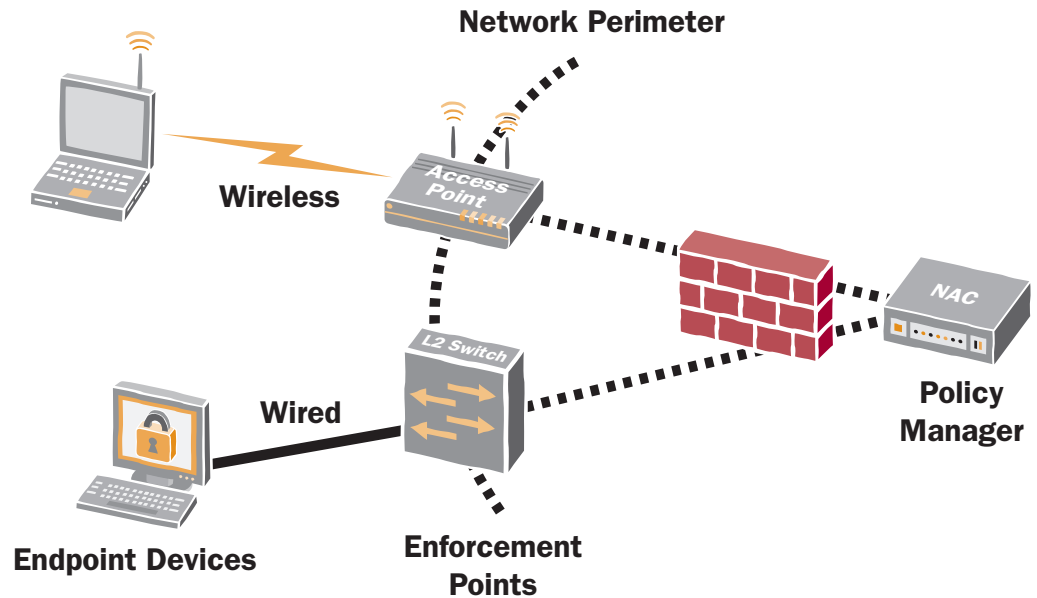


Figure 1: A Typical Network Access Control Environment

A robust network access control solution must address both network admission control and application access control. Pre-admission controls gate whether a user and/or device is allowed onto the network and may include authentication and endpoint assessment. Application access control includes any restrictions on network resources a user or device is allowed to access and use. For example, guest users may be allowed Internet access, but are limited to 1 Mbps of bandwidth; the network access control solution should be able to recognize such users as “guests,” restrict their access to external Internet sites and rate-limit their connection.

The Role of 802.1X and the Importance of Open Architectures and Standards

Network access control vendors, LAN switch makers, access point manufacturers and client software vendors have widely adopted the authentication mechanism defined in the IEEE 802.1X standard for port-based network access control. As a result, many network access control solutions are able to leverage existing RADIUS and back-end identity stores for user and/or device authentication, and can interoperate seamlessly with any 802.1X standard-compliant switch.

The 802.1X standard works in conjunction with the Extensible Authentication Protocol (EAP) standard to provide port-based network access control for both wired and wireless networks. Defined by the Internet Engineering Task Force (IETF), EAP is an authentication framework that ensures the secure passing and validation of network credentials. EAP also allows for the creation of a variety of extensible access protocols, such as tunneled EAP for more flexible, expandable network access and authorization. EAP’s extensibility supports the need for network access control solutions to include more information with the user/device authentication information about and from the user and their device, such as endpoint security and posture validation.

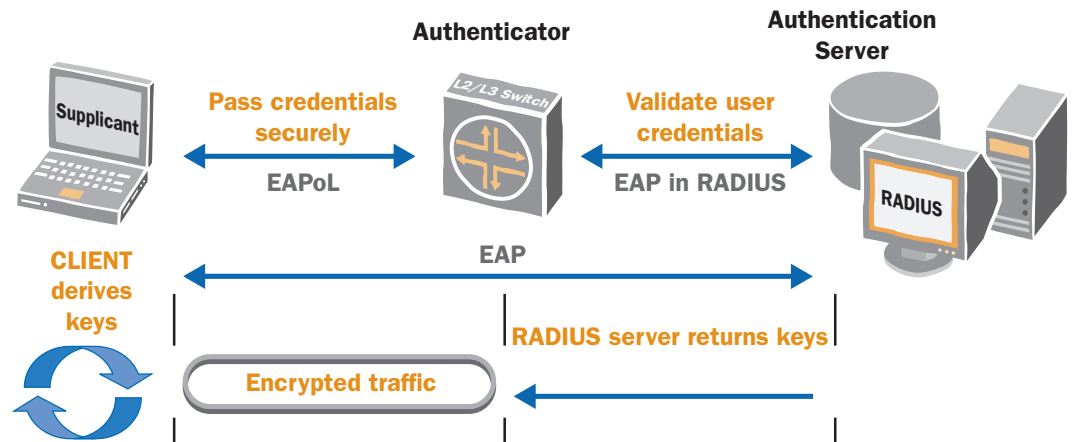


Figure 2: A Typical 802.1X Network Environment

Before admitting an endpoint—whether wired or wireless—to the LAN, the 802.1X-compatible device first authenticates the user and their endpoint. Compliant switches and access points block all traffic from 802.1X clients (also known as “supplicants”) except for EAP until authentication is successful. Once the user enters the necessary authentication data (such as a user name and password or other authentication mechanism), the endpoint communicates an authentication request to the switch, which relays it to an authentication server. If the authentication process succeeds, the LAN switch or wireless access point grants the user and their endpoint network access; if authentication fails, network access is denied. In addition to permitting or denying LAN access, 802.1X switches and access points may place an endpoint in an assigned VLAN, if supported.

This simple “on/off” access control is the strength of the 802.1X standard. The 802.1X standard provides a strong baseline for the admission control portion of network access control. The 802.1X standard ensures interoperability between 802.1X-compliant clients running on endpoints, switches and network access control solutions, allowing enterprises to leverage existing infrastructure whenever possible.

Juniper UAC is based on industry standards, including 802.1X, EAP, RADIUS, IPSec and the Trusted Computing Group’s (TCG) Trusted Network Connect (TNC) standards for endpoint integrity and network access control. By supporting industry standards, Juniper allows enterprises the flexibility to leverage their existing hardware and software infrastructure to implement access control in a flexible, cost-effective manner, delivering a faster, higher return on investment (ROI).

(For more information, read the Juniper Networks white paper “802.1X: Port-Based Authentication Standard for Network Access Control (NAC)” at http://www.juniper.net/solutions/literature/white_papers/200216.pdf.)

The Juniper Networks UAC Solution

Juniper Networks Unified Access Control (UAC) is built on a foundation of industry standards, open specifications, and vast amounts of technology and real-world experience from several of Juniper’s market-leading, industry-proven products, including Juniper Secure Access SSL VPN, Steel-Belted Radius® (SBR), and Odyssey® Access Client (OAC). Juniper UAC integrates this technology and expertise into a solution that seamlessly provides secure guest user access, network and application access control, and network visibility and monitoring end-to-end across the network.

The UAC solution allows enterprises to extend access control to and enforce security from the edge of the network deep into the network’s core and through to the data center. Customers have the option of enabling UAC at Layer 2, using 802.1X; at Layer 3 using an overlay deployment for resource and application access control; or in a mixed mode for complete protection for the network and its resources, applications and data. Access policies are enforced at Layer 2 using any vendor’s 802.1X-enabled wireless access points or switches, at Layers 2-4 with the Juniper Networks new EX-series Ethernet switches, and at Layers 3-7 using any Juniper firewall platform.

In addition, UAC controls network access for managed endpoint devices such as employee laptop and desktop computers; unmanaged devices, such as those used by guests and contractors; and “unmanageable” endpoints such as printers and IP-based security cameras, environmental system controls, bar code readers, and other computing and non-computing devices that are driven by and connected to the network.

By committing to standards and supporting a variety of policy enforcement elements, Juniper empowers organizations to leverage their existing investments in network devices and software to deliver comprehensive access control, eliminating the need for expensive network overhauls or firmware/software upgrades to the network infrastructure. Customers have the flexibility to deploy the complete UAC solution or select components for varying degrees of access control and visibility, phasing in access control as needed at their own pace. It’s entirely up to the individual customer and their access control needs.

The UAC Solution Components

The Juniper UAC solution consists of three basic components: an agent (the UAC Agent), a policy management server (the Infranet Controller) and enforcement points.

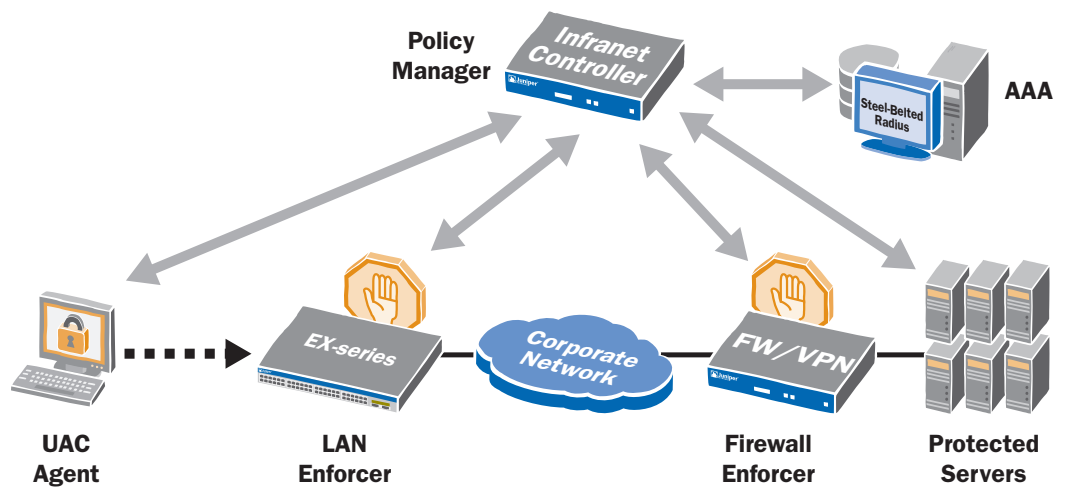


Figure 3: The Juniper Unified Access Control (UAC) Solution.

- **The UAC Agent:** The Juniper UAC Agent, a downloadable software client, serves as an 802.1X supplicant and includes the ability to gather host posture information. Operating in concert with the Infranet Controller, the UAC's policy management engine, the UAC Agent collects user credentials and assesses the endpoint's security state via its integrated Host Checker functionality, including integrated patch assessment technology. Host Checker scans endpoints for a variety of security applications, including antivirus, anti-malware and personal firewalls, and verifies the status and state of those applications. Patch assessment technology inspects endpoints for operating system information and application level, updates and hot fixes. Endpoint integrity checking occurs before user authentication and throughout the user session; access rights can be changed if there are changes in the security state or the endpoint device's policy adherence.

Since the UAC Agent is dynamically downloaded from the Infranet Controller, it is very easy to adopt and deploy; there is no need to manually install and maintain clients on every user device.

For circumstances where software downloads aren't practical, such as guest access, Juniper provides an agent-less mode. In this mode, users sign in directly to the Infranet Controller via a captive portal, similar to accessing a Wi-Fi network in a hotel, local coffee shop or other hotspot. UAC's agent-less mode supports browser-based validation of network credentials and scanning of devices for posture assessment via Juniper Host Checker functionality, both before user authentication and throughout the guest user's session.

Some devices, such as printers, cash registers, bar code scanners and VoIP handsets, cannot accept any kind of agent and are typically referred to as "unmanageable" devices. Juniper supports network access control for unmanageable devices via Media Access Control (MAC) addresses and RADIUS. UAC uses MAC address authentication via RADIUS in combination with MAC address white listing and black listing to dynamically identify devices as unmanageable. Once identified, UAC can deny or permit network access and assign unmanageable devices to an appropriate VLAN. Alternately, UAC can interoperate with and leverage existing asset discovery, profiling solutions or profile stores via Lightweight Directory Access Protocol (LDAP) interfaces, obtaining a device's true identity and using any returned profiles or attributes to map the device to the appropriate VLAN for network access. This saves customers time and money by allowing them to leverage existing policy and profile stores to control network access for their unmanageable devices.

- **Infranet Controller:** At the heart of the Juniper UAC solution is the Infranet Controller, a centralized policy management server that is the security and access policy engine for UAC as well as the interface to existing enterprise AAA infrastructures. The Infranet Controller can push the UAC Agent to endpoint devices (or collect information in agent-less mode), gathering user authentication data and determining endpoint security state and location. The Infranet Controller combines this collected information with corporate-defined compliance rules, implements the appropriate access policy for each user/session, and propagates that policy to enforcement points throughout the network. The Infranet Controller also correlates information it receives from enforcement points and dynamically responds to evolving network conditions by changing a user's access rights if the user violates policy.

IT benefits from the ability to define access controls and policies centrally on the Infranet Controller and distributing them to enforcement points throughout the network, eliminating the need to configure filters, access control lists (ACLs) or individual policies such as QoS policies on each enforcement point. Authentication and endpoint assessment can be repeated at specified intervals during a session to ensure dynamic policy management and enforcement, including remediation for non-compliant users or devices.

- **UAC Enforcement Points:** Enforcement points control access to the network and its resources based on policies created on and provisioned by the Infranet Controller. At the network edge, Juniper Networks EX-series Ethernet switches act as enforcement points, as do any 802.1X-enabled wired or wireless access platforms from other vendors. (The enforcement capabilities of the EX-series switches are detailed in the next section.)

Within the network core and data center, Juniper supports all of its firewall/VPN appliances as enforcement points, including the Secure Services Gateway (SSG) appliances, Integrated Security Gateway (ISG) devices with Intrusion Detection and Prevention (IDP) modules, and NetScreen platforms. At Layers 3-7, the Juniper firewall products act as overlay enforcement points. The basic Juniper NetScreen firewall platforms enforce controls by matching filter conditions against Layer 2-4 packet content and taking the appropriate action, such as permitting or denying access to a server or WAN router.

Some Juniper firewall/VPN platforms support the company’s Unified Threat Management (UTM) security features, which include Intrusion Prevention System (IPS) functionality as well as network-based antivirus, anti-spam and URL filtering capabilities. UAC can dynamically leverage all of these capabilities, applying deep packet inspection, antivirus and URL filtering on a per-user, per-session basis to deliver comprehensive access and threat control.

Operating together, 802.1X-compatible devices, like the Juniper EX-series switches, and Juniper firewall/VPN platforms provide complete Layer 2-7 visibility and control, allowing customers to gain insight into network traffic, unify access and security controls, and define policies at the level of granularity they require. For additional flexibility, enterprises have the option to use UAC enforcement points in transparent mode, which requires no changes to the network infrastructure. Enforcement points can also be set up in audit mode so that IT gains visibility into network traffic without applying enforcement actions.

Juniper IDP platforms, and firewalls with integrated IDP such as the ISG appliances, can also provide broad Layer 2-7 visibility into network traffic. When deployed and implemented together, the Infranet Controller, enforcement points such as the Juniper EX-series switches, and the Juniper standalone IDP platforms can work in concert to isolate a network threat down to the user or device level and apply an appropriate, specific policy action against the offending device to quickly address and mitigate network threats, minimizing network and user downtime.

The EX-series Enforcement Advantage

Juniper designed UAC to interoperate with 802.1X-compliant enforcement points. Therefore, the Infranet Controller is capable of instantiating a broad array of policies and associated enforcement actions on any 802.1X LAN switch. Unfortunately, many of the switches on the market today do not support the range of enforcement actions that UAC makes possible.

In developing its new family of EX-series Ethernet switches, Juniper made the ability to support a rich set of enforcement actions across all of its switch platforms a specific design goal. Consequently, every port on the EX 3200 and EX 4200 series switches acts as an enforcement point, controlling traffic based on the dynamic policies created and propagated by UAC. Working in conjunction with UAC, each EX-series switch supports the following enforcement actions:

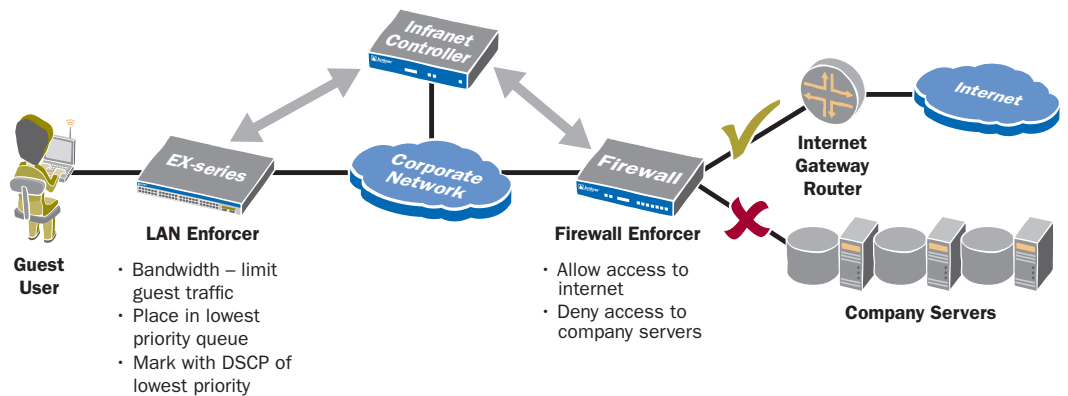


Figure 4: For Guest Access to the Network, the Juniper UAC Solution Provides Differentiated, Secure Access to Services on a Per-User Basis.

- **Admission control:** The EX-series switches will permit or deny network access based on policies developed and distributed by UAC, including those policies based on user authentication status, endpoint posture compliance, user/device role and other policies. The EX-series switches provide standards-based 802.1X port-level access control.
- **VLAN assignment:** An EX-series switch will assign an endpoint to a VLAN based on user/device identity, role or other policy parameter.
- **Bandwidth limiting:** EX-series switches can constrain an endpoint to a specified maximum bandwidth based on policy created on and distributed by UAC, protecting network resources from over-consumption. Bandwidth limiting can be applied to every session an endpoint initiates (for example, a VoIP phone); by user identity or role (for example, guest users are rate limited to 1 Mbps while employees have unlimited bandwidth); by destination (for example, limit traffic to/from the Internet to 10 Mbps); or other parameters.
- **Traffic marking:** EX-series switches can apply QoS markings to traffic to ensure consistent handling throughout the network or within specific portions of the enterprise LAN. An EX-series switch will identify incoming traffic, match it against a QoS policy list, and mark it for appropriate handling by subsequent network devices. Marking can be based on user/device identity or role, traffic type or other parameter. All EX-series switches support IEEE 802.1p marking at Layer 2 and IETF Differentiated Services (DiffServ) Code Point (DSCP) and IP Precedence marking at Layer 3.
- **Traffic scheduling and prioritization:** EX-series switches can queue and service traffic based on its priority setting. All Juniper EX-series switches provide eight queues per port and support 7,000 access control list (ACL) entries per switch, giving enterprises the flexibility to accommodate numerous classes of traffic and define very granular QoS policies.

For example, when an 802.1X-enabled IP phone authenticates to the network, the Infranet Controller can send a policy to the appropriate EX-series switch indicating it should give highest priority handling to traffic on that particular switch port. The port will mark the traffic and put it into a strict priority queue. All of this is done dynamically, eliminating the need for IT to configure QoS policies manually on each switch. Similarly, as enterprises roll out unified communications, IT can prioritize certain applications over others, providing medium priority handling for instant messaging versus low priority for voicemail, for example.
- **Policy-based routing:** Based on a specified policy created on the Infranet Controller, EX-series switches can forward traffic from one or more ports via a particular route. Enterprises can use this capability to ensure that IP telephony traffic is always forwarded over the lowest-latency path, for example. IT can also use this feature to route guest and contractor traffic through an IDP before allowing it to reach the Internet or other destinations.
- **Traffic mirroring:** Using Generic Routing Encapsulation (GRE) tunneling, an EX-series switch is able to mirror or copy a traffic flow to another EX-series switch. Enterprises can use this enforcement action in a number of ways. For example, for regulatory and auditing purposes, IT may define a policy in UAC whereby all finance or credit-card related transactions are mirrored to a compliance server. Similarly, IT could define a policy to mirror certain users' traffic to an IDP or protocol analyzer in order to learn where those users go on the network and what applications and resources they use. Such information can be useful in refining access control policies or for tracking potentially suspicious users.

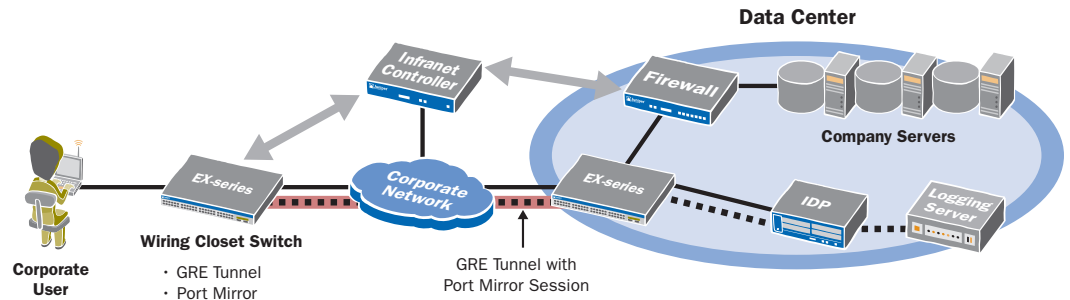


Figure 5: For Visibility into User Sessions, the Juniper UAC Solution and EX-series Switches Can Dynamically Mirror Traffic to an Intrusion Prevention Device in the Data Center.

UAC in Action: Simplifying Deployments and Operations

With UAC, Juniper has tightly integrated the three main network access components—endpoint agent, policy server and enforcement points—so that IT can enforce corporate access policy. Consequently, there’s no need for IT to manage a standalone admission control product, individually configure firewalls with security policies, and define access and QoS policies for each LAN switch. IT can define admission and access control policies centrally within the Infranet Controller, and the UAC solution automates the rest, including the downloading of endpoint agents and even automatically remediating non-compliant endpoints.

By combining user identity, device security state and location information, UAC is able to enforce dynamic, session-specific access controls based on customer-defined policies. The Juniper UAC solution delivers complete end-to-end network access control, enabling enterprises to address the key network access control issues they face, including network protection, guest access control, network visibility and monitoring, application access control and identity-based QoS control. (For more information on how enterprises can use the Juniper Networks UAC solution to meet common network access control challenges, see the Juniper Networks whitepaper “Tackling the Top Five Network Access Control Challenges with the Juniper Networks UAC Solution” at http://www.juniper.net/solutions/literature/white_papers/200265.pdf.)

Conclusion

Network access control is a necessity for today’s high-performance enterprise network. The Juniper Networks Unified Access Control solution addresses the full range of access control challenges by providing dynamic network and application access controls that operate across the entire network, from edge to data center.

Juniper has taken the complexity out of network access control deployment while delivering comprehensive visibility, protection and control. Through its support for open standards, Juniper enables enterprises to take advantage of the UAC solution in their heterogeneous environment and deploy network access control in a staged fashion. At the same time, the tight integration of the UAC components, including the Juniper EX-series switches, provides coordinated, end-to-end access control that’s more scalable and easier to use than other NAC solutions on the market.

The Juniper UAC solution ensures that only authenticated users and devices that comply with network and security policies gain access to the network and authorized resources. It lets enterprises monitor and control network and application access based on a variety of parameters, including user and/or device identity, location, and compliance with network and security policies. With the Juniper UAC solution, enterprises are able to address even the most pressing network access and security issues they face—quickly, simply and completely.

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 HEADQUARTERS
AND SALES HEADQUARTERS FOR
NORTH AND SOUTH AMERICA**
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

**EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS**
Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Aldlestone
Surrey, KT15 2PG, U.K.
Phone: 44.(0).1372.385500
Fax: 44.(0).1372.385501

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978.589.5800
Fax: 978.589.0800

ASIA PACIFIC REGIONAL SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

Copyright 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

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