

GUEST ACCESS MADE EASY

Juniper Networks Unified Access Control and EX Series Ethernet Switches Solve Today's NAC Problems

Table of Contents

Executive Summary	1
Introduction	1
Not All Guests Are Equal	2
Juniper Networks Unified Access Control	2
UAC's Role-Based Access Controls	3
Endpoint Assessment—Or Not	4
Onetime Guest Access—Deployment Scenarios	5
NAC Using EX Series Switches	5
UAC and EX Series Benefits	6
Using Juniper Firewalls and Gateways	6
Contractors and Other “Repeat” Guests—Deployment Scenarios	6
Conclusion	7
About Juniper Networks	7

Table of Figures

Figure 1: Juniper Networks Unified Access Control solution	2
------------------------------------------------------------------	---

Executive Summary

One of the primary reasons enterprises initially deploy network access control (NAC) is to provide guests and contractors with secure network access. Research shows that enterprises expand their use of NAC over time, and industry analysts recommend that businesses implement a comprehensive solution that can grow with their needs. Juniper Networks® Unified Access Control is an open, standards-based network access control solution that gives enterprises the flexibility to implement a range of access controls, from basic to very granular, to accommodate not only employees, but onetime guests, repeat visitors such as contractors and partners, and others.

UAC easily integrates into heterogeneous network environments and ties into existing identity stores, enabling enterprises to leverage their current infrastructure investment to deliver identity-based network and application access control. When combined with Juniper Networks EX Series Ethernet Switches or any Juniper firewall platform, UAC delivers a rich set of identity- and role-based controls, including time, location, and quality of service (QoS) controls, as well as a mirroring option that simplifies compliance reporting. With UAC, enterprises can cost-effectively turn on the right level of access control for their guests today and be well positioned to meet any of tomorrow's access control challenges.

Introduction

The desire to provide network access to employees and visitors alike is a key reason that organizations of all types—from health care, education, and hospitality to government and manufacturing—are deploying NAC solutions. In today's highly connected world, visitors have come to expect businesses to provide Internet access in public spaces such as lobbies and waiting rooms. For their part, enterprises know that it's both a courtesy and good business practice to accommodate guests in this way, and the challenge is to do so without putting business assets at risk or overburdening IT.

According to Gartner, Inc., 80 percent of NAC deployments are installed initially to address guest access control. Some enterprises have already installed gear from different vendors to meet individual use cases; for example, deploying one NAC solution for the visitor waiting in the lobby, and another for contractors, partners, or other non-employees who may need broader access.

Gartner has found that enterprises expand their NAC usage over time—both in terms of scale (the number of endpoint devices supported) and scope (additional use cases, such as visibility into and control over user behavior on the network)¹. Taking a piecemeal approach to NAC is complex and costly, and leaves the enterprise ill equipped to expand its usage beyond a single use case. Consequently, Gartner recommends that enterprises plan for the long term and deploy NAC solutions that not only meet their immediate needs, but also take into consideration their future access control needs and plans.

Juniper Networks Unified Access Control is a comprehensive access control solution that enables enterprises to implement guest access easily, and scales to accommodate more endpoint devices and a range of use cases as NAC usage expands. In UAC, Juniper integrates a robust policy engine and endpoint integrity technology which enterprises can quickly deploy in heterogeneous environments. Likewise, Juniper's intuitive policy management makes it easy to start with the most basic access controls and create more granular controls as needs change.

Juniper's support and adoption of open, industry standards ensures that UAC interoperates in a multivendor environment so that enterprises can leverage their existing infrastructure investments. Standards-based UAC also future-proofs network investments, empowering enterprises to select and deploy best-in-class products that meet their networking needs. Enterprises that are planning a switch upgrade or refresh will find that the combination of UAC and Juniper Networks EX Series Ethernet Switches provides a richer set of guest access controls while lowering the total cost of ownership for NAC. Likewise, pairing UAC with Juniper firewalls and integrated services gateways delivers granular application- and resource-level controls with minimal configuration needed.

Juniper's support for a single management system across its product set means that IT can manage the UAC policy engine, EX Series switches, and other Juniper enforcement points, including Juniper firewall platforms and Juniper Networks IDP Series Intrusion Detection and Prevention Appliances, from a single console, significantly reducing IT overhead while ensuring consistent security across the enterprise.

¹Source: "Magic Quadrant for Network Access Control" Publication Date: 27 March 2009, ID Number: G00166224, authors Lawrence Orans, John Pescatore, Mark Nicolett

Not All Guests Are Equal

Organizations host a variety of guests. Therefore, they need a NAC solution that can accommodate a range of guest types with different levels of access. For the sake of simplicity, guests can be divided into two broad categories: onetime guests and “ongoing” or repeat guests, each with its own access requirements.

Onetime guests are the classic visitor, such as a salesperson or customer who comes on site once or infrequently. Enterprises want to offer these guests temporary Internet access as a courtesy, most often in lobby areas, waiting rooms, and conference rooms. This type of “instant access” is highly restricted, and an NAC solution must ensure that guests gain Internet access only and cannot reach the corporate network.

In contrast, ongoing or repeat guests are users such as contractors, consultants, partners, and vendors who work on site, either for an extended time or periodically. These ongoing guests may be contractors or consultants to whom the enterprise has outsourced a business project or process. To do their job, these guests need access to a specific or limited set of corporate resources in addition to Internet access. Enterprises need a NAC solution that lets them distinguish between these types of guests or non-employees and control precisely what resources they can access.

The ideal NAC solution will also give IT two additional capabilities: a way to easily document what controls are in place and identity-enable those controls so that regulatory requirements can be met; and the option to perform an endpoint assessment of laptops that guests may bring on site. To be effective, an NAC solution must work enterprise-wide; otherwise, wireless networks and open network jacks in places like conference rooms and empty offices will continue to pose a security risk, providing easy, unauthorized access to the corporate network.

Juniper Networks Unified Access Control

UAC is an adaptive, standards-based, simple-to-deploy network access control solution that enterprises can deploy for onetime guest access and easily expand to accommodate ongoing guests as well as employees. Because it is based on standards, UAC interoperates with a range of third-party networking gear and user agents. In addition, UAC fully supports EX Series switches; all Juniper firewall platforms, including the Juniper Networks SRX Series Services Gateways; Juniper’s family of IDP Series Intrusion Detection and Prevention Appliances delivering coordinated threat control; and Juniper Networks STRM Series Security Threat Response Managers for threat analysis and regulatory reporting. As with other Juniper products and solutions, UAC is managed via Juniper Networks Network and Security Manager to ensure that customers benefit from enhanced functionality provided under a single management umbrella.

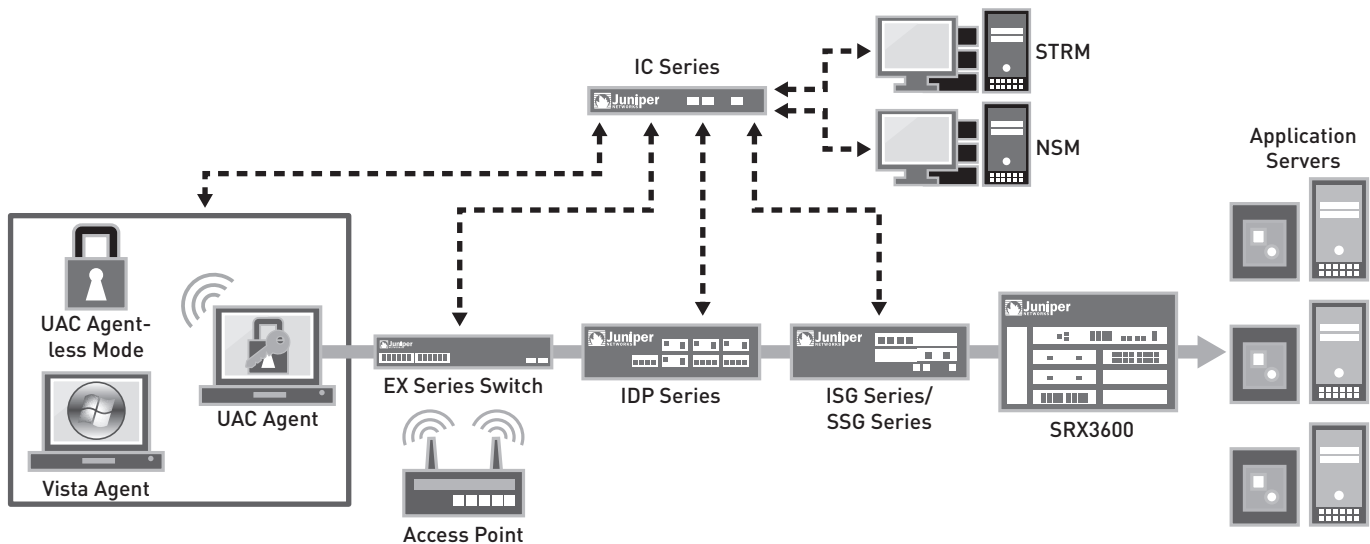


Figure 1: Juniper Networks Unified Access Control solution

UAC has three primary components:

- **Centralized policy management server:** Juniper Networks IC Series Unified Access Control Appliances are the security and access policy engine for UAC, as well as the interface to existing enterprise authentication, authorization, and accounting (AAA) infrastructures. These out-of-band appliances are easy to deploy and enable IT to define access controls and policies centrally. The IC Series distributes these policies to enforcement points—such as the EX Series switches or other vendor-agnostic 802.1X switches and access points, as well as Juniper firewall and integrated services platforms—throughout the network, eliminating the need for IT to configure filters, access control lists (ACLs), or individual policies such as QoS policies on each enforcement point.

In enforcing policies, the IC Series gathers user authentication, endpoint security state, and device location data from endpoints and combines this with customer-defined posture compliance rules, role assignments, and access control rules to deliver dynamic, identity- and role-based policies. The IC Series also correlates information from enforcement points and dynamically responds to changing network conditions in applying access control.

- **Endpoint Agents:** UAC includes agents as well as an agent-less mode, which is ideal for guest access. The UAC Agent is downloadable client software that provides an 802.1X supplicant and gathers host posture information. Juniper also supports third-party user agents, such as Microsoft® Windows® Vista's health agent, via the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) client-server statement of health protocol (TNCCS-SOH).

With UAC's agent-less mode, users sign directly into the IC Series UAC appliance via a captive portal. Agent-less mode supports browser-based validation of network credentials and, like the downloadable UAC Agent, the scanning of devices for posture assessment via Juniper's Host Checker functionality.

The UAC Agent and agent-less mode dynamically capture the user's access request, which reveals various user and device attributes including source IP, media access control (MAC) address, network interface, digital certificate (if one exists), browser type, SSL version, and the results of the endpoint security check performed by the UAC Agent or agent-less mode, if performed. (Endpoint security assessments occur both before user authentication, and throughout the guest user's session, particularly as the endpoint's security state changes.) This set of data is integral to access control and policy enforcement.

- **Enforcement points:** These include Juniper's 802.1X-compliant EX Series Ethernet Switches and any Juniper secure router, firewall, or integrated services gateway, including the SRX Series Services Gateways, Juniper Networks SSG Series Secure Services Gateways, Juniper Networks ISG Series Integrated Security Gateways, ISG Series with Intrusion Detection and Prevention modules, and Juniper Networks NetScreen Security Systems.

Juniper also supports third-party devices as enforcement points, including any 802.1X-enabled wired or wireless access platforms, as well as any network and security devices that support the TNC Interface for Metadata Access Point (IF-MAP) standard.

UAC's Role-Based Access Controls

Juniper Networks Unified Access Control applies access controls based on a user's role, which has numerous advantages for guest access. A user's role is comprised of three pieces of information:



Who: The most important piece of information is *who* the user is—for example, is he or she a onetime guest or ongoing guest (which can be further subdivided into contractor, vendor, partner, and so on as needed)?



Where: Next, *where* the guest is located must be determined—for example, are they in a conference room or lobby with an open wireless access point, or in a cubicle within the campus perimeter with a wired connection?



What: Third, *what* the security state of the endpoint is must be determined—for example, an enterprise may require that ongoing guests have current antivirus software or up-to-date patches and fixes, before being admitted to their network.

Defining roles based on all three parameters and applying role-based controls to guests means that access controls are effective regardless of how guests connect to the network, their location on the network or in the enterprise, or what access method they use, wired or wireless—no more worrying about open jacks or rogue wireless access points. Since role-based access controls factor in location, they can be applied to specific areas such as lobbies, conference rooms, and waiting rooms. Guests who try to access the network from anywhere else can be denied access.

In addition, roles can be configured with session attributes, such as time and bandwidth restrictions. IT could limit onetime access for guests to a four hour block of time, for example, and constrain ongoing guests to network access during business hours. This addresses the critical “when” component to role-based guest network access assessment.

Similarly, IT could limit guests who are accessing the Internet from the lobby to 1 Mbps of bandwidth, while allowing guests in a conference room 10 Mbps of bandwidth since they may be partners, contractors, or others who need to reach and upload or download critical, resource-intensive materials on their own corporate network.

Role-based access control allows for more granular control with less management overhead, eliminating the need to manually configure VLANs on switches or ACLs on firewalls. And because it takes endpoint state into account, and can repeat authentication and endpoint assessment at specified intervals and when an endpoint’s security state or user’s location changes during a session, UAC provides dynamic access privilege management. That is, UAC can make access privileges more or less restrictive based on endpoint and user status changes. For example, if an IDP Series appliance senses anomalous traffic from a guest’s laptop, that information can be communicated to the IC Series appliance, which can revoke that guest’s access privileges or quarantine their traffic.

Endpoint Assessment—Or Not

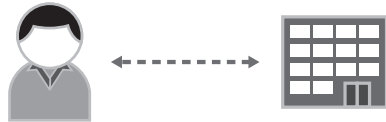
UAC gives enterprises the option to require an endpoint assessment of guest machines, or to forego one. Some organizations may feel that the risk posed by onetime guests is outweighed by the intrusiveness of requiring a host posture check, while repeat guests should be subject to endpoint assessment because of their greater level of access to the corporate network.

Before allowing any access—wireless or wired—to the network, UAC performs a user authentication check; either the UAC agent or agent-less mode submits the user and device credentials to the IC Series policy server, which uses its comprehensive AAA engine to interface with an enterprise’s existing AAA data store to verify the user’s and device’s credentials. At the same time, the IC Series compares the endpoint’s security state against the enterprise’s predefined security policy baseline.

Enterprises may choose not to perform a comprehensive endpoint assessment before granting guest access; to grant access but require the guest to comply with an Acceptable Use Policy; or to provide access only if the endpoint passes a basic integrity check (for example, has current OS patches and fixes as well as up-to-date antivirus software).

Enterprises can also choose from various enforcement actions based on the outcome of the endpoint integrity check. For example, they can deny network access to guests with non-compliant devices. Alternately, enterprises can use UAC to send users and devices that don’t comply with their network admission policies into a quarantine area or network. Working with the EX Series switches or other 802.1X-compatible switches or access points, an IC Series UAC Appliance can transfer non-compliant devices to the appropriate quarantine VLAN. The UAC solution can even remediate non-compliant devices automatically, without user or IT intervention, bringing them into compliance and, if authenticated and authorized, automatically giving them network access, maximizing user productivity while reducing IT costs.

Onetime Guest Access—Deployment Scenarios



Onetime guest access

Enterprises have several alternatives for how to use UAC to implement NAC for onetime guests. These range from bare bones to increasingly granular and span a spectrum of Layer 2 and Layer 3 options. The following section outlines some of the most common approaches.

NAC Using EX Series Switches

Non-role-based access: The most rudimentary way to provide NAC for guests is to implement non-role-based access via Juniper's 802.1X-compatible EX Series switches. Users who don't have an 802.1X supplicant are automatically shunted by the EX Series switch to a default "guest" VLAN. While simple, this approach does require that 802.1X be supported by switches and wireless access points in all locations where guests might access the network. And because guest devices lack 802.1X supplicants, endpoint assessment isn't possible and access controls are limited to simple yes/no access.

Role-based access: There are two ways in which enterprises can implement role-based access with UAC, and customers may choose to implement one or both. In the first method, the guest device is equipped with an 802.1X supplicant/agent. (This can be the UAC Agent or a third-party agent). When the agent attempts to authenticate the guest, naturally the guest won't be in the enterprise identity store. Consequently, the IC Series appliance will identify the guest as "anonymous," place them into the guest role, and apply any appropriate network and resource access policies and controls that IT has defined.

For any 802.1X-compliant switch, these controls include Layer 2 RADIUS attribute-based policies such as VLAN assignment and/or vendor-specific attributes (VSAs). When deployed as part of a UAC solution, EX Series Ethernet Switches, in concert with UAC, support additional controls such as QoS, including guest traffic priority and bandwidth usage (useful if IT wants to throttle guest peer-to-peer traffic, for example); the ability to mirror or copy a traffic flow to another EX Series switch (useful for regulatory and auditing purposes); and the ability to route traffic based on a specified policy (useful if IT wants to funnel guest and contractor traffic through an IPS/IDS platform such as IDP Series Intrusion Detection and Prevention Appliances, before allowing it to reach the Internet or other destinations).

An endpoint assessment of the guest's device may be accomplished if the enterprise enables the guest user to download the UAC Agent from the IC Series; if the guest's device is employing the latest versions of Juniper Networks Odyssey Access Client as a supplicant; or if the device is running the supplicant included with Microsoft Windows Vista or Windows XP Service Pack 3. In the case of a device that downloads the UAC Agent or is running OAC, the endpoint security state and integrity check is conducted by the IC Series (and Juniper's Host Checker). When a device passes the integrity check, the guest user is directed to the appropriate VLAN for users in the guest role. If the device is running the Windows Vista or XP SP3 client, the device is assessed and checked by Windows Security Center (WSC), with the results of the endpoint check relayed to the IC Series appliance so that they may be taken into consideration when UAC formulates and distributes its access decision for the guest's device to its enforcement points.

The second way to support role-based NAC at Layer 2 is via UAC's captive portal, which will be familiar to users who've used this method of wired or wireless network access in hotels and other hot spots. In this scenario, a receptionist or other support person supplies the guest with a user name and onetime password. The guest then inputs the username and onetime password into the captive portal page, enabling the IC Series UAC Appliance, by itself or in conjunction with a local authentication server, to authenticate them as a guest (and, if desired by the enterprise, to ensure that a base level of malware protection is operational on the guest's device), placing the user into the "guest" role. The IC Series UAC Appliance then applies all relevant guest policies.

UAC and EX Series Benefits

The combination of UAC and EX Series switches gives enterprises the flexibility to impose whatever guest policies best meet their needs, such as no access for all guests; access requiring an Acceptable Use Policy; network access requiring a basic level of endpoint integrity (such as an operational, up-to-date antivirus client); access via any 802.1X supplicant, providing only authentication and/or access defined by guest role without posture check; guest access allowed to a specific VLAN and/or the Internet while restricting access to protected corporate resources; or guest access restricted by time, location, and network resource consumption.

Because the Juniper Networks EX Series Ethernet Switches support a rich set of enforcement actions, they can control guest traffic based on the dynamic policies created and propagated by UAC. EX Series switches also support key UAC guest access capabilities such as temporary accounts (which expire after a preset number of hours) and onetime use accounts, as well as the provisioning of guest accounts by non-IT staff (for example, a receptionist).

Using Juniper Firewalls and Gateways

Some organizations may prefer to implement guest access at Layer 3 or higher by using Juniper firewall and services gateway products as overlay enforcement points. A major benefit of this approach is that access controls are applied regardless of whether a guest connects to the network via wired or wireless means, and regardless of 802.1X support within the infrastructure, with no need to restructure and manage VLANs. In addition, access can be very granular, restricting guests to specific gateways, servers, even applications.

In this deployment scenario, guests would log into the network in agent-less mode, using the captive portal. For its part, IT simply points the IC Series policy server at the relevant Internet-facing firewall(s) and/or services gateway(s) and defines the guest policies. The IC Series appliance pushes the policies to the firewalls and/or services gateways, which then limit guests to Internet only access and apply any other policies that have been defined (for example, time, location, QoS, specific resource access, and so on).

The Juniper firewall and services gateway platforms enforce UAC policies by matching filter conditions against Layer 2-4 packet content and taking the appropriate action, such as permitting or denying access to the Internet, a server, or a WAN router based on what IT specifies. In addition, IT can define Layer 3 policies governing access to IP addresses/subnets; Layer 4 ports or ranges to be permitted or denied (enabling guests to go to Internet search engines, but not music download sites, for example); and Layer 7 policies such as IDP policies or URL filtering for additional dynamic threat management.

Contractors and Other “Repeat” Guests—Deployment Scenarios



Repeat guest access

Onetime guest access is a special use case whereby the user is provided Internet access as a courtesy. However, repeat guests such as contractors, consultants, partners, and other “multi-visit” guests generally need access to specific corporate resources and applications to get their job done. Likewise, enterprise security policy may require endpoint assessment for this class of guest since they’re permitted direct access to the corporate network, and not just the Internet. With very little change, UAC can be expanded to accommodate this category of guest user—and all of its sub-categories.

Role-based policies are ideal for repeat guests because they allow IT to distinguish one type of guest from another and apply access controls tailored to that type of guest. For example, IT can provide access to finance resources for guests in the “accounting contractor” role, while restricting guests in the “engineering consultant” category to engineering content and applications.

Organizations can deploy UAC with EX Series switches to provide NAC for repeat guests. Such guests would be placed in the appropriate VLAN based on their role, and any additional location, time, QoS, mirroring, or other policies can be applied. For organizations that rely on VLANs for traffic segmentation, this may be a good option.

Enterprises that want more granular application and resource control, and/or need to accommodate repeat guests who move around the organization (rather than sit in a specific cubicle), may prefer combining UAC with Juniper firewalls or services gateways such as the SRX Series. When UAC is coupled with Layer 3+ devices, access controls and policies follow the guest, regardless of physical location or zone, ensuring that access controls apply enterprise-wide.

Establishing granular controls is straightforward; IT simply points the Juniper firewalls and/or services gateways and the IC Series policy engine at each other and configures whatever access policies are needed. Configuring role-based policies is much easier than defining source-destination filters on firewalls: IT gives the policy a name, indicates whether the action is “allow” or “deny,” and specifies to which resources and roles the policy applies. The firewalls take this information and convert it to the appropriate ACLs.

Juniper has designed UAC to provide powerful access controls without complexity. All IT has to do to apply a policy to one or more guests is simply enable UAC authentication for an individual guest or class of guests, making firewall filters specific to users and roles. For repeat or ongoing guests, this approach offers the greatest flexibility in applying network access control with minimal management overhead.

Conclusion

Enterprises benefit from a single, comprehensive NAC solution that can accommodate onetime guests, repeat visitors such as contractors and partners, employees, and future use cases as they emerge. Juniper Networks Unified Access Control is an integrated, easy-to-use solution that enables enterprises to cost-effectively turn on the right level of access control for their guests today and be well positioned to meet tomorrow’s access control challenges.

Juniper’s support for standards gives enterprises the flexibility to leverage their existing network and security infrastructure when deploying UAC. However, when UAC is combined with Juniper Networks EX Series Ethernet Switches, enterprises benefit from a richer set of role-based access controls, including time, location, and QoS controls, as well as a mirroring option that simplifies compliance reporting.

Likewise, when UAC is coupled with any Juniper firewall platform and SRX Series Services Gateways, enterprises can implement granular controls to constrain where and when repeat guests, such as contractors and partners, access the network and what applications and resources they can reach. And when deployed in a network with both EX Series Ethernet Switches (or other existing 802.1X-compatible switches and/or 802.1X-enabled access points) and any Juniper firewall platform and/or SRX Series device, UAC delivers superior granularity of access control and security policies for guests—as well as anyone attempting network access. UAC is easily configured and managed via NSM, along with Juniper network and security products, so enterprises benefit from streamlined management and low operational overhead.

With UAC, enterprises have a flexible guest access solution that readily accommodates any new and future NAC requirements.

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

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
Airsides Business Park
Swords, County Dublin,
Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

Copyright 2009 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. JUNOSe is a trademark of Juniper Networks, Inc. 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.

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

