

# TACKLING THE TOP FIVE NETWORK ACCESS CONTROL CHALLENGES

---

Juniper Networks Unified Access Control and EX Series Ethernet Switches

Network Utilities (Systems) Limited  
Liberty House, 516 Walton Road,  
West Molesey, Surrey KT8 2QF

Tel: +44 (0)20 8783 3800  
Fax: +44 (0)20 8783 3810  
Email: [sales@netutils.com](mailto:sales@netutils.com)  
Web: [www.netutils.com](http://www.netutils.com)

## Table of Contents

Executive Summary .....	1
Introduction .....	1
Gaining Control with Juniper Networks Unified Access Control .....	2
Network Protection .....	2
Guest Access .....	4
Network Visibility and Monitoring .....	5
Application Access Control .....	6
Identity-Based QoS Control .....	7
Conclusion .....	8
About Juniper Networks .....	9

## Table of Figures

Figure 1: Juniper Networks Unified Access Control solution working in concert with Juniper Networks EX Series Ethernet Switches, firewall devices, and IDP Series .....	3
Figure 2: Juniper Networks Unified Access Control and guest user access .....	5
Figure 3: Juniper Networks Unified Access Control provides network visibility and monitoring suitable for regulatory compliance .....	6
Figure 4: Juniper Networks Unified Access Control provides powerful application access controls, enabling enterprises to segment their network and address regulatory compliance .....	7
Figure 5: Juniper Networks Unified Access Control and EX Series Ethernet Switches enable QoS policies to be defined and enforced against multiple levels of network traffic .....	8

## Executive Summary

Numerous factors are driving enterprises to control who's admitted to the corporate network and what resources—servers, applications, stored data—they're allowed to access.

Business trends such as mobility, outsourcing and the blurring of corporate network boundaries mean enterprises must provide network and application access to company “insiders” such as employees as well as “outsiders” that include guest users, partners and contractors. IT must open the network to a dynamic workforce, while at the same time protecting critical assets from the vulnerabilities that openness and user mobility bring. In addition, to comply with industry and governmental regulations, enterprises must prove that they have stringent controls in place to restrict access to credit card information, patient health records and other sensitive data.

Technology trends—particularly the move to converge multiple services onto a single IP infrastructure—are also driving the need for network access control. The adoption of IP-based telephony (IPT), videoconferencing and other video services spurred initial deployments of converged networks; emerging unified communications services and applications are helping to drive the next wave of deployments. At the same time, enterprises are connecting everything from security cameras, badge readers, industrial robots, bar code readers, building automation systems and even vending machines to the corporate network. This proliferation of devices and traffic types can pose severe network resource consumption and security challenges.

Juniper Networks® Unified Access Control can help enterprises tackle the range of network and application access problems they face. In this document we explore five common networking challenges that enterprises face—network protection, guest user access, network visibility and monitoring, application access control, and identity-based Quality of Service (QoS)—and discuss how UAC can be used to address each.

## Introduction

Juniper Networks Unified Access Control, built on a foundation of industry standards and market-leading Juniper security products, consists of three tightly integrated network access control components: an endpoint agent (UAC Agent), a policy management server (IC Series UAC Appliance), and enforcement points. An agent-less mode is also available for situations where providing an agent is not feasible.

At the heart of UAC is the IC Series UAC Appliance, a centralized policy management server that is the security and access policy engine for UAC. It also acts as the interface to existing enterprise AAA infrastructures. IT can define pre- and post-admission, access control and security policies centrally within UAC's IC Series. UAC then takes care of the rest, automating the download of endpoint agents or providing agent-less support by role, checking user authentication and device security state against predefined policies, distributing access control policies to enforcement points, and performing other tasks—even automatically remediating non-compliant endpoints. The IC Series UAC Appliance also leverages the policy management capabilities and AAA interface of Juniper's award-winning, market-leading SSL VPN platforms.

UAC supports most device types, including managed, unmanaged and “unmanageable” devices. (For more information, read the white paper “Juniper Networks UAC and EX Series Switches: Meeting Today's Security Challenges with End-to-End Network Access Control” at [www.juniper.net/us/en/local/pdf/whitepapers/2000266-en.pdf](http://www.juniper.net/us/en/local/pdf/whitepapers/2000266-en.pdf))

For managed devices such as employee laptops, desktop computers and other devices, and/or those enterprise users who require a full or lightweight client, UAC provides the UAC Agent. The UAC Agent is a downloadable software client that gathers user/device identity data and host posture information and assesses the endpoint's security state. The UAC Agent leverages functionality from Juniper's enterprise-built, widely-deployed 802.1X supplicant, Juniper Networks Odyssey Access Client, as well as the Juniper Host Checker, an integral component in the thousands of Juniper SSL VPN deployments.

For unmanaged devices such as those used by guests and contractors, UAC provides an agent-less mode which supports browser-based validation of network credentials as well as posture assessment via Host Checker.

Unified Access Control also supports unmanageable devices—such as networked printers, cash registers, bar code scanners, VoIP handsets, and other non-computing devices that may be connected to and accessing the corporate network—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 solutions, 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.

The UAC solution also supports multiple enforcement points. At the network edge, any 802.1X-enabled wireless or wired access platform, including Juniper Networks EX Series Ethernet Switches, can act as an enforcement point. The EX Series Ethernet Switches, including the Juniper Networks EX3200 Ethernet Switches and Juniper Networks EX4200 Ethernet Switches with Virtual Chassis technology, deliver complete Layer 2/Layer 3 Ethernet connectivity solutions for data center, campus and branch-office environments. Juniper specifically designed the EX Series to support a rich set of enforcement actions; every port on the EX3200 and EX4200 switches acts as an enforcement point, controlling traffic based on the dynamic policies created and propagated by UAC.

Deeper in the network, Juniper also supports all of its firewall/VPN appliances as enforcement points, including the Juniper Networks SSG Series Secure Services Gateways, ISG Series Integrated Security Gateways with IDP Series Intrusion Detection and Prevention Appliances, and NetScreen 5000 Series Security Systems.

UAC is extremely flexible, enabling phased deployments. UAC leverages and supports existing network infrastructure and components, rather than requiring a major network overhaul in order to achieve compatibility or gain complete network access control. UAC also allows for selective accessibility, empowering enterprises to determine the authorization and network access levels available to each user and/or role.

UAC's access policies are enforced at Layer 2 through any 802.1X-enabled wireless access point or switch; at Layers 2-4 with the new Juniper Networks EX Series Ethernet Switches; and at Layers 3-7 using any Juniper firewall/VPN platform. Deployments can also be implemented in a mixed mode—blending all enforcement types and supported network layers—for complete end-to-end network, resource application and data protection.

## Gaining Control with Juniper Networks Unified Access Control

The best way to communicate the power and flexibility of UAC is to illustrate how it addresses the key access control challenges that enterprises face: network protection, guest access control, network visibility and monitoring, application access control, and identity-based QoS control.

### Network Protection

Given the diversity of users and devices accessing the enterprise LAN today, the critical role that the network plays with respect to business operations, and the acceleration and sophistication of malware attacks and security breaches, protecting the network is of paramount importance. UAC automatically ties user/device identity and role information to network and application access and authorization, thereby enabling customers to create granular security and access control policies. The combination of UAC with EX Series switches in particular provides coordinated network protection that begins at login with pre-admission controls and continues throughout a user or device's session.

- **Pre-Admission Control:** Before allowing any access—wireless or wired—to the network, UAC performs a user authentication and endpoint assessment check to ensure that users are authenticated and devices are operating in accordance with corporate policy. UAC can quarantine users and devices that don't comply with the enterprise's predefined network admission policies and, working with the EX Series and/or other 802.1X-compatible switches or access points, either transfer non-compliant devices to the appropriate quarantine VLAN or deny network access altogether. The UAC solution can even remediate non-compliant devices automatically, without user or IT intervention, to minimize downtime and reduce help desk calls. With its support for managed, unmanaged and unmanageable devices, the UAC solution can prevent unauthenticated, unauthorized users and non-compliant, unauthorized devices from accessing the network.

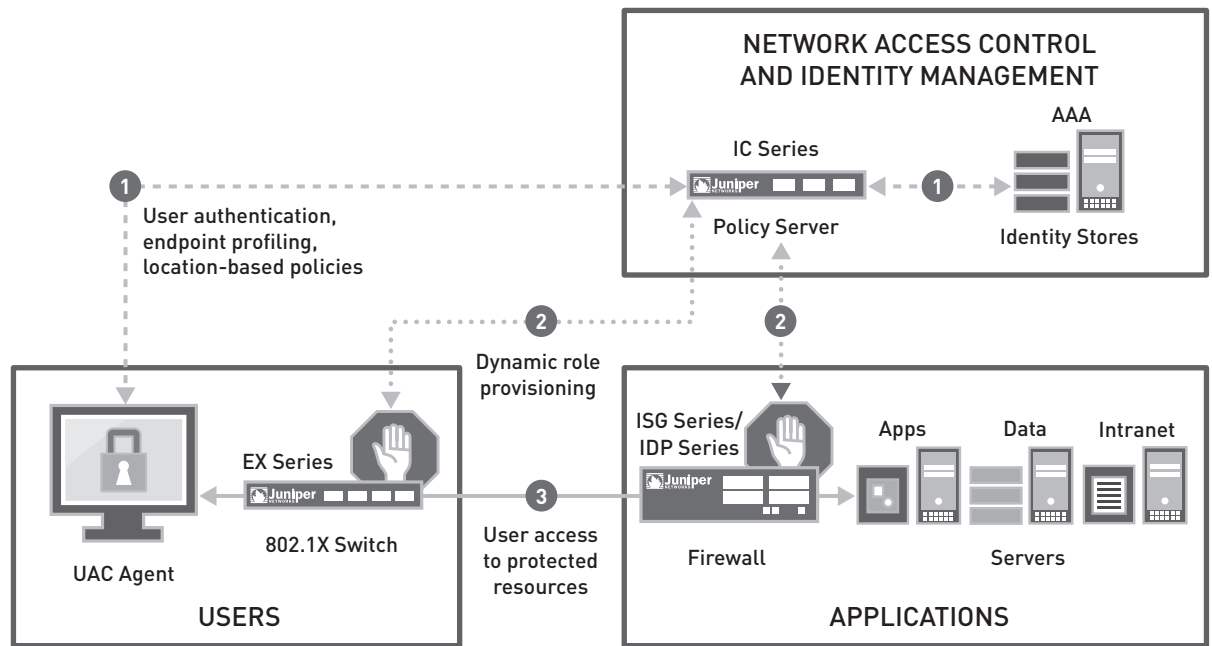


Figure 1: Juniper Networks Unified Access Control solution working in concert with Juniper Networks EX Series Ethernet Switches, firewall devices, and IDP Series

The UAC solution can automatically identify the user and/or device, as well as their assigned roles, at login time. When a user or device attempts to access the network, the UAC Agent can be pre-configured and dynamically downloaded to the user's endpoint device from the IC Series UAC Appliance based on the specified role. The UAC Agent dynamically captures the user's access request, which reveals various user and/or device attributes including source IP, 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 Host Checker (in agent-less mode). The UAC Agent submits the user and/or device credentials and the endpoint security status to the IC Series, which uses its comprehensive AAA engine to verify the user's credentials based on the authentication data it extracts from an enterprise's existing AAA data stores. The IC Series also compares the endpoint's security state against the enterprise's predefined security policy baseline. The IC Series then combines the user's credentials and group or attribute information with the other information gathered such as endpoint compliance state and network location, and dynamically maps the user to a role that defines the access rights for their network session.

Role attributes can encompass session attributes and parameters. They can also specify restrictions with which the user must comply—such as limiting login to designated business hours—before they are mapped to a role. After this initial compliance and role mapping step, the IC Series assigns resource policies which govern network and resource access. Examples of resource policies include Layer 2 RADIUS attribute-based policies such as VLAN assignments and/or vendor specific attributes (VSAs); Layer 3 policies governing access to IP addresses/subnets; Layer 4 ports or ranges to be permitted or denied; and Layer 7 policies such as IDP Series policies or URL filtering for additional dynamic threat management.

Pre-admission controls protect the enterprise network and its assets by preventing unauthenticated and/or unauthorized users from gaining access, and by restricting access for authorized users based on network admission policies. For example, employees in the "customer service" role can be limited to logging onto the network only during normal business days and hours. In addition, pre-admission posture assessment ensures that users with non-compliant devices—for example, students who haven't updated their laptop's antivirus software definitions since leaving for Spring Break—cannot infect the network with malware when they attempt to reconnect to the network.

- **Post-Admission Control:** Through its fully integrated components, UAC can track each network session and dynamically coordinate threat and access control based on information it receives from its enforcement points, including the EX Series. Consider the case of an employee who either inadvertently—by picking up malware surfing the Internet while on the road—or intentionally attempts to launch a zero day worm attack on the corporate network.

When the employee attempts to reconnect to the corporate LAN, they and their device are admitted to the network since they are a known, authorized user whose laptop anti-malware software is up-to-date and has all of the current patches and fixes required by the company's endpoint security and network admission policies. However, once the user attempts to access a server in the data center and the worm attempts to launch its attack, an IDP Series appliance identifies the suspicious traffic and/or anomalous behavior. The IDP Series then reports the threat to the IC Series, which correlates the threat to a specific user and/or device. What happens next depends on the enterprise's particular policy.

For instance, the IC Series UAC Appliance could communicate to the appropriate EX Series or other 802.1X-enabled device to take a configurable policy action against the employee and the device that the IC Series has identified as the source of the suspicious traffic. The IC Series can notify the EX Series switch to restrict the user's or device's access to the network. Alternately, the IC Series could signal the EX Series switch to redirect the user's session to a quarantine server. To minimize the chance of spreading the malware to other devices on the network, the UAC solution could also employ policy-based routing to specify a "safe" path for directing traffic to the quarantine server. Or, the IC Series could instruct the switch to disable the user's session entirely.

Once the offending device has been quarantined and remediated, UAC will automatically re-authenticate the user's credentials and reassess their endpoint's security state. If the credentials are authenticated and the device is deemed within policy, UAC will enable the user and their device to safely reconnect to the LAN.

To further protect the network, UAC ensures that users are only allowed access to their specific role-related resources. For example, once back on the LAN, say the user—who is in sales—attempts to review purchase orders stored on the finance server in the data center. Because his or her role does not permit that level of access, UAC signals the appropriate enforcement point—such as a Juniper firewall—to block the request. In this way, UAC applies application access control (discussed later in this white paper) to specific applications and data on the network, ensuring that only those users who have defined authority access rights can reach protected, sensitive data.

Similarly, enterprises can use the EX Series switches' QoS capabilities to help protect the network. For example, IT can define a bandwidth policy in UAC allocating IP phones up to 300 Kbps of bandwidth. This policy has a dual purpose: not only does it ensure that the phones have sufficient bandwidth to deliver good quality voice, it also acts as a security mechanism by alerting IT if an IP phone begins consuming more than its allocated bandwidth—an indication that it may have been spoofed or hacked.

Based on corporate policy, the EX Series could either shut down the port or redirect the suspicious traffic to a quarantine server or other device for further analysis. In either case, the IP phone would be prevented from consuming excessive bandwidth or otherwise disrupting network operations. At the very least, an EX Series would limit the phone's bandwidth usage, preventing potentially malicious traffic from blasting across the network to overwhelm server resources. In addition, IT would be informed of the problem so that they can further investigate if trouble continues.

## Guest Access

Guest user access continues to be a major challenge for enterprises. Wireless networks and open jacks in conference rooms and waiting areas make it easy for nearly anyone, including those with malicious intent, to connect to the corporate network. IT needs a way to dynamically differentiate guests from "authorized" users such as employees, and control where guests can go on the network and what resources they can access. Since IT has no control over a guest's endpoint device, an access control solution must be non-intrusive and require little—or no—IT intervention.

UAC provides an agent-less mode for such situations. When a guest attempts to access the network, they are redirected from an EX Series or other 802.1X-compatible edge switch directly to the IC Series UAC Appliance, which checks the user's credentials and performs a host posture assessment. The guest cannot be authenticated, but UAC can assign them to a guest role and apply access restrictions based on controls and policies predefined by the corporation.

Depending on corporate policy, guests who fail the posture check can be denied network access, or a policy can be created that ensures that all guest traffic is inspected by the antivirus software in a deployed Juniper firewall, adding Layer 7 application protection without making any changes to the guest's device. As with other endpoints assessed by Host Checker, guest devices are scanned for posture compliance at login and their security state is also monitored throughout the user session.

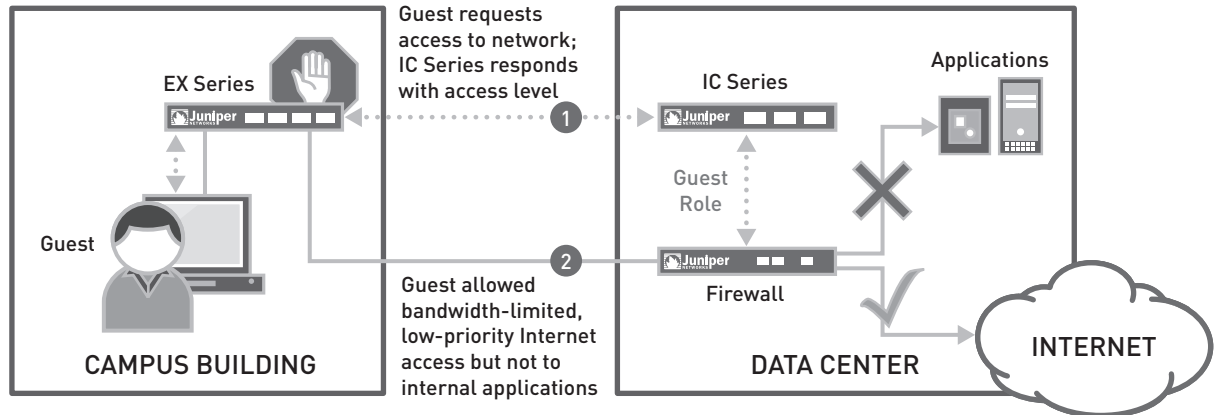


Figure 2: Juniper Networks Unified Access Control and guest user access

Once guests and their devices are identified, checked and placed into a guest role, a variety of corporate-defined policies can be applied. The flexible UAC solution can impose guest access policies such as no access at all for 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 client/supplicant, providing only authentication and/or access defined by the guest role without device posture check; or guest access allowed to a specific VLAN and/or the Internet while restricting access to protected corporate resources.

For example, all guests can be placed into a specific VLAN which only provides access to the Internet. To avoid any impact on other network users, the UAC solution can restrict guests attempting network access from the company lobby to 1 Mbps of bandwidth, while guests attempting access from a conference room could be allowed 10 Mbps of bandwidth since they may be partners, contractors, vendors or other users who need to access critical, resource-intensive materials on their own corporate network.

By utilizing UAC in agent-less mode, interoperating in many cases with the EX Series, IT is assured that guest users attempting network access are identified, their devices checked to ensure compliance with corporate policy, and their access to the network gated appropriately no matter where or how they connect to the enterprise network.

## Network Visibility and Monitoring

Information assets are an enterprise's crown jewels. Protecting intellectual property from misappropriation and threat is crucial. In addition, industry and governmental regulations require that enterprises control access to sensitive information such as patient records, card holder data and financial records.

Having visibility into who is accessing what on the network is a prerequisite to controlling access to applications, data and other resources. Visibility and monitoring are also vital to proving to auditors and regulatory bodies that the required access controls are in place and working.

Enterprises can use UAC in several ways to gain visibility into network traffic. One option is for IT to deploy either a standalone IDP Series appliance or an ISG Series device with IDP in front of the application servers. The IDP Series work in conjunction with the IC Series to correlate user identity and role information with network and application usage, enabling enterprises to audit and log network and application use in accordance with regulatory requirements. The UAC solution, in conjunction with IDP Series and the Juniper Networks Network and Security Manager (NSM), provides fine-grained usage information in a clear, easy-to-understand format; detailed logs include such information as user roles, the status of endpoint compliance to security policies, the resources that users attempt to access and the resources actually accessed.

IT also has the option to mirror traffic from particular users to an IDP Series, protocol analyzer, compliance server or other specialized device. For example, to create an audit trail of transactions by users authorized to handle credit card data, IT could configure a generic routing encapsulation (GRE) tunnel from the EX Series serving those users to a compliance server connected to an EX Series switch in the data center. Similarly, if IT wants visibility into the activity of guests or other users with unmanaged devices, their traffic could be mirrored to an IDP Series or other device for monitoring and logging.

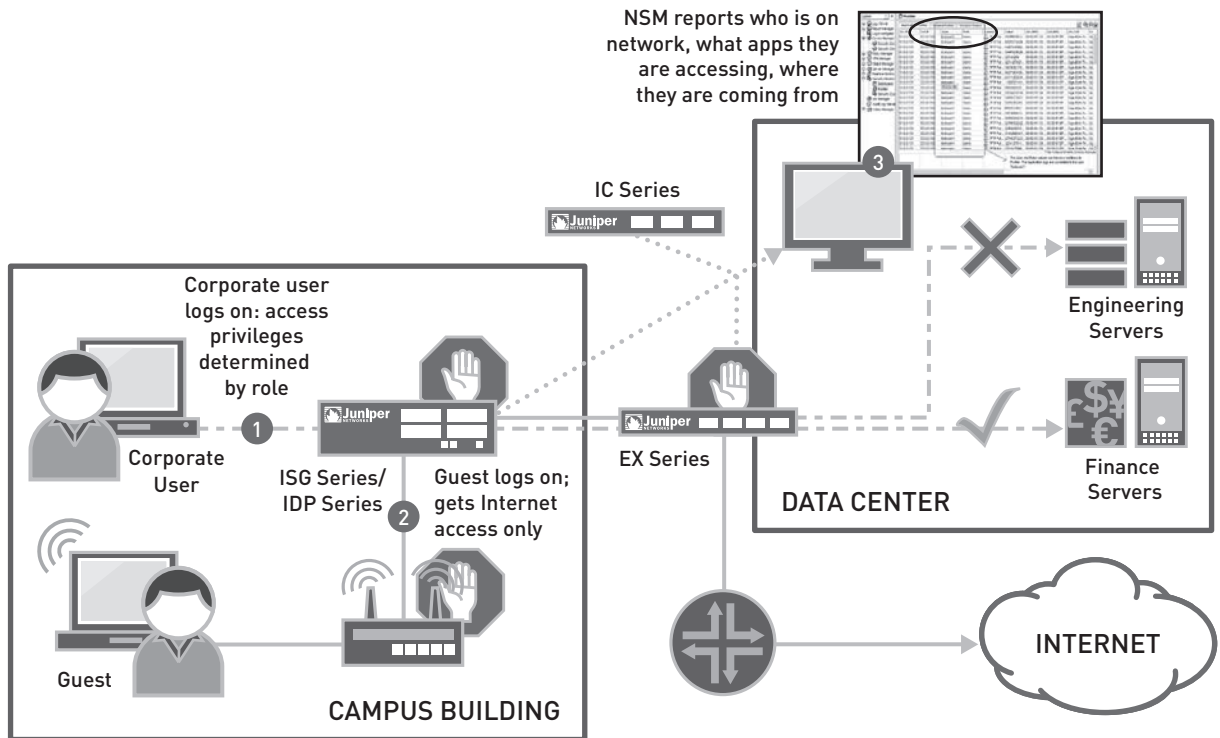


Figure 3: Juniper Networks Unified Access Control provides network visibility and monitoring suitable for regulatory compliance

## Application Access Control

Applications are the engine that drives business processes, and accidental or malicious use or abuse of applications and the data they contain poses a significant risk for enterprises. If applications and/or data are compromised, enterprises can suffer revenue loss, damage to their reputation, regulatory penalties and other consequences.

To comply with federal and industry regulations, for example, enterprises must have a means to ensure that only authorized users have access to servers and storage devices containing sensitive data. That may mean segmenting these servers and storage devices from the rest of the network and/or strictly gating who can use which applications or access certain stored data. Enterprises need a solution that lets them control application access and usage for each user without creating headaches for users or IT.

UAC leverages Juniper's firewall platforms, IDP Series and EX Series to provide granular application access control along with single sign-on. By placing a Juniper firewall/IDP Series such as the ISG Series with IDP in front of application servers, IT can easily control which users have access to which applications and when. IT simply defines application access policies within the IC Series which pushes these policies out to Juniper firewall/VPN platforms to enforce. Users need only authenticate once to the UAC solution, rather than to each application they use. IT benefits from having a single application identity management system to configure and manage, as well as a consistent set of access controls to apply rather than administering numerous application-specific systems and controls. Also, via the IDP Series, the corporation can track and identify users and devices accessing the application servers, providing the necessary data to address regulatory compliance audits.

Enterprises can define application access controls as broadly or as tightly as needed, including restricting specific user groups from attempting to access certain application servers and/or data repositories. For instance, the IC Series can push policies to the EX Series that restrict access to specific switch ports to only predefined, authorized users.

With UAC, enterprises can define policies that grant all employees access to specific applications, while access to other, more sensitive application servers is gated by a user's role. For example, a salesperson may be provided access to sales-oriented applications and servers, but not be allowed to access the finance servers.

IT can also restrict access based on location or time of day. For example, graduate nursing students at a university hospital may be granted access to clinical systems and patient data only when accessing those resources from the clinic; they would not have access to those servers and data from their dormitory or classrooms.

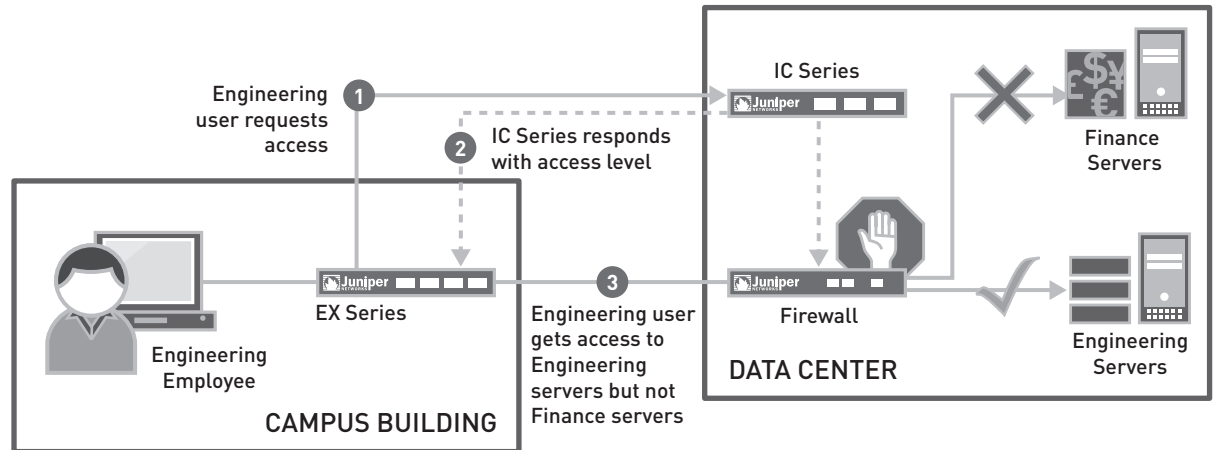


Figure 4: Juniper Networks Unified Access Control provides powerful application access controls, enabling enterprises to segment their network and address regulatory compliance

## Identity-Based QoS Control

Data is no longer the only traffic running over enterprise networks. Voice and video traffic already share the LAN with traditional data in many organizations, prompting IT to begin using QoS mechanisms in switches and routers to ensure good performance for non-data applications. As unified communications applications and services become more widely available and adopted, the need for QoS will only grow. Unfortunately, implementing QoS mechanisms can be complex and tedious, requiring IT to manually configure individual network devices.

UAC simplifies QoS implementation by providing a centralized place for IT to define identity-based QoS policies. Within the IC Series, IT can define QoS policies based on user credentials, network location and/or device posture. The IC Series then pushes these policies to appropriate enforcement points. When EX Series are used as UAC enforcement points, the IC Series will activate QoS access control lists (ACLs) in the switches to enforce bandwidth limiting, traffic prioritization, traffic marking and traffic scheduling. QoS policies are applied dynamically, per user or device session, regardless of the user's or device's location or the type of endpoint a user might use to access the network (for example, desktop computer, laptop or PDA).

For example, QoS policies can be applied to devices such as IP phones to ensure that they have a high-priority, low-latency connection with dedicated bandwidth. When an 802.1X-enabled IP phone authenticates to the network, the IC Series can send a policy to the appropriate EX Series 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.

Similarly, as enterprises roll out unified communications, IT can prioritize certain applications over others, providing medium priority handling for Instant Messaging (IM) versus low priority for voicemail, for example. In addition, enterprises may want to apply QoS policies to specific users or roles—for example, giving finance users high-priority handling for all ERP transactions. Enterprises also have the option to impose bandwidth restrictions on guests and other "low priority" users.

By reducing the complexity of implementing QoS controls, the UAC solution enables enterprises to gain more control over how their network is utilized, including utilization by specific users and devices. Network resources are therefore applied more efficiently and application performance is more consistent and predictable. As a result, enterprises benefit from more intelligent network operation while reducing operational overhead.

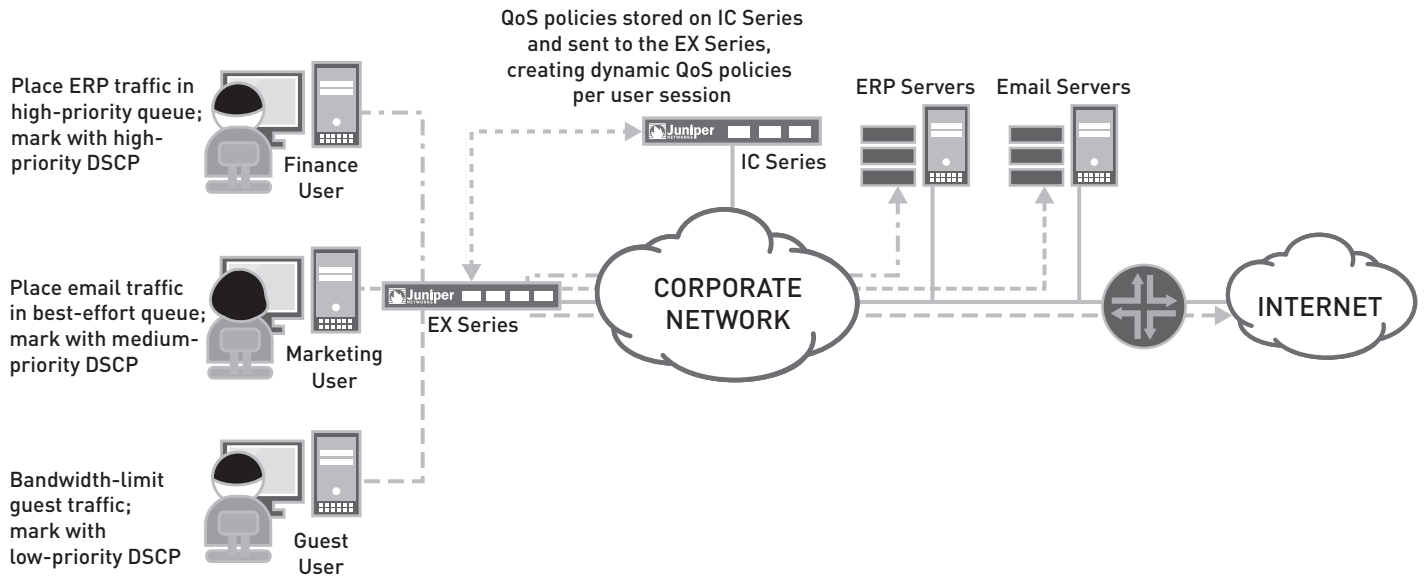


Figure 5: Juniper Networks Unified Access Control and EX Series Ethernet Switches enable QoS policies to be defined and enforced against multiple levels of network traffic

## Conclusion

Enterprises face numerous challenges in today's business climate. Selecting and deploying a comprehensive network access control solution doesn't have to be one of them. Operating end-to-end across the network, Juniper Networks Unified Access Control provides the visibility, protection and control that enterprises need to tackle the most pressing security and access control issues they face.

UAC combines user identity, device security state and location information to create dynamic, session-specific network and application access controls. The UAC solution ensures that only authenticated users and devices that initially comply—and maintain compliance—with network and security policies throughout their network session gain and retain access to the network and its resources, applications and sensitive data.

By tightly integrating the three core components of network access control—endpoint agent, policy management server and enforcement points—Juniper delivers coordinated, scalable access control and threat mitigation without the complexity of other solutions on the market. Building on industry standards and an open, standards-based architecture, the Juniper solution ensures seamless interoperability with new and existing network and security infrastructure components, leveraging them to extend end-to-end access control deep into the network, enabling a flexible, phased deployment.

With the UAC solution, an enterprise can quickly and easily deploy to address a broad spectrum of access control challenges and regulatory compliance 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](http://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  
Airside 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. "Engineered for the network ahead" and JUNOSe are trademarks 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.

