PRODUCT CATEGORY BROCHURE

UNIFIED ACCESS CONTROL

Comprehensive Network Access Control
Using the Network You Have Today

Juniper Networks® Unified Access Control is a comprehensive access control solution that:

- Granularly and dynamically controls end user access based on user identity, device security state, and location information.
- Leverages your existing network infrastructure—from user authentication to access points and switches, to Juniper firewalls and IDP Series appliances—through an open, standards-based architecture.
- Is based on field-tested components being used today in tens of thousands of network deployments worldwide.

In today's high-performance enterprise, the network and applications are no longer separate from the business—they *are* the business. Diverse users—including employees, guests, contractors, and partners—need access to a myriad of network resources and applications, ranging from simple Internet access to sensitive internal data. These same users are increasingly demanding access from a barrage of device types, ranging from personal notebooks and netbooks, to even more sophisticated mobile devices. This dramatic rise in user count and device type significantly increases an organization's potential exposure to malicious behavior. Even the managed devices of trusted users may become unknowingly infected when used to surf the Internet or work remotely—inadvertently becoming a threat when connected directly to the network and serving as a launch pad for attacks. Guest users who may only need an Internet connection can come onto the network with their own unmanaged devices and unknowingly expose sensitive network resources to malware or breach.

Network access control (NAC) is not new. In many instances the term simply serves to unify a number of disparate problems that enterprises have been wrestling with for years. As this category has become more defined, however, a plethora of solutions has emerged, each of which attempts to address access control in a different way. This can make it very difficult to get a clear picture of network access control, and how it functions.

UAC: An Access Control Solution You Can Trust

Juniper Networks Unified Access Control (UAC) combines the best of access control and security technologies while leveraging existing security and network infrastructure investments. UAC incorporates different levels of session-specific policy—including authentication and authorization, roles, and resource policies—to deliver extremely robust access control and security policies that are simple to deploy, maintain, and modify. All policy is created and pushed by the hardened Juniper Networks IC Series Unified Access Control Appliances, the centralized policy servers at the heart of UAC. User identity, device state, and network location can be determined by the dynamically deployable, cross-platform UAC Agent, or Juniper Networks Junos® Pulse, Juniper's integrated, multi-service network client which enables anytime, anywhere connectivity, security, and acceleration, as well as via UAC's agent-less mode—particularly useful in cases where installing a software client is not feasible, such as guest access.

UAC is the industry's only NAC solution that provides full Layer 2 through Layer 7 policy enforcement on the widest possible array of enforcement points. UAC's policies can be enforced at Layer 2 (and beyond) using any vendor's 802.1X-enabled wireless access points or switches (including Juniper Networks EX Series Ethernet Switches) for dynamic virtual LAN (VLAN) assignment, filter/ACL assignment, quality of service (QoS), and more. At Layers 3-7 any Juniper Networks firewall platform, including the Juniper Networks SRX Series Services Gateways, deployed with UAC becomes identity-enabled, leveraging the industry's leading security device families as full NAC enforcers at any scale. Finally, Juniper Networks IDP Series Intrusion Detection and Prevention Appliances deliver role-based, application level policy enforcement providing unparalleled access control and security granularity.

Every Juniper Networks UAC component—including the IC Series UAC Appliances, UAC Agent, Junos Pulse, and enforcement points—is built on open, industry standards and proven security and access control devices, including features from Juniper Networks SA Series SSL VPN Appliances with their legacy of policy management, dynamic endpoint assessment and seamless interaction with existing AAA backbones; Juniper Networks Odyssey Access Client (OAC), the market-leading, enterprise-built 802.1X supplicant; and Juniper Networks SBR Enterprise Series Steel-Belted Radius Servers, the de facto standard in AAA/RADIUS servers.

With Juniper Networks UAC, you can start deploying NAC quickly and simply by installing just a single IC Series UAC Appliance within your network. This allows you to use your existing, vendor-agnostic 802.1X switches or access point, including the Juniper Networks EX Series switches—or any Juniper Networks firewall or IDP Series platform—for policy enforcement. The result is a uniquely adaptable, scalable solution that combines user identity, device security state, and network location to create dynamic, session-specific network and application access control policy for each user—leveraging the network you have in place today.

One Network Access Control Solution for All Use Cases

UAC can help you quickly and simply address a number of the use cases and challenges that confront your organization today:

- **Guest Access** – Most organizations demand instant, differentiated access for guest users—which can include partners, contractors, customers, or essentially any user other than an employee. This presents organizations with a unique set of challenges. UAC delivers several different ways to accommodate guest users, depending on your network configuration. If you are using 802.1X infrastructure for enforcement, it's likely that your guests have not installed the full UAC Agent or Junos Pulse. The cross-platform UAC agent-less mode was developed with these guest users in mind. It supports browser-based validation of user credentials and scanning of endpoint devices for posture assessment, including patches and spyware, before user authentication and throughout the user's session. Guests can be dynamically directed to a restricted VLAN for limited access. If your organization is using Juniper Networks firewalls as an overlay enforcement method, you can further control guest access within your network, effectively segmenting sensitive information from unauthorized user access and limiting application access. Access control policies on many Juniper firewalls deliver time-based access restrictions as well as additional Layer 7 unified threat management (UTM) functionality.

  UAC enables guest user accounts to be provisioned for one-time use or with a predefined time limit. Front desk personnel at an organization can be empowered by IT administrators to provision guest user accounts, with a network access expiration of up to eight hours or the duration of a typical business day. Administrators always maintain ultimate control, though, over the provisioning of and maximum time duration allowed guest user accounts.

- **Regulatory Compliance** – Meeting industry and government regulations and requirements, plus the ability to prove adherence to these regulations, is a necessity for organizations today. By deploying UAC, you can meet or surpass regulatory compliance requirements and relieve the stress on your network, your access control resources, and your network and compliance administrators. UAC's ability to ensure that every endpoint device is assessed and checked both pre-admission and post-admission for compliance with your predefined security and access policies—including the state of antivirus, antimalware, personal firewall, and patches—addresses a main requirement of many regulations. UAC also provides industry-leading, dynamic antispyware and antimalware protection for Microsoft Windows endpoint devices attempting network access. UAC's ability to provide secure, encrypted data transport from the endpoint device into and throughout the network—and its robust authentication and authorization capabilities—also help organizations meet regulatory requirements. The identity-enabled profiler within UAC, which correlates user identity and role information to network and application usage, enables you to know who is accessing your network and sensitive applications, when your network and applications are being accessed, what they are accessing, and produces a trail of where the user has been on your network, providing you with a log that is vitally important for regulatory compliance audits.

The IC Series UAC Appliances adopt and leverage the TNC's Interface for Metadata Access Point (IF-MAP) open, standards-based protocol, integrating UAC with vendor-agnostic third-party network and security devices, including devices that collect information about what's happening with your network and applications, and their state. The collected data is reported back to an IC Series appliance, which can serve as a Metadata Access Point (MAP) server, allowing the captured network state data to be leveraged by UAC as it formulates dynamic network and application access control policies and actions. This simultaneously enhances both network and application visibility and security, and helps address even the most stringent industry and government compliance regulations.

- **Insider Threats** – The growing specter of insider threats can cause untold organizational headaches and sleepless nights for you and your administrators. UAC, with its strong authentication and authorization and powerful endpoint device checks, dispels potential insider threats before they even start. By leveraging the robust features and functionality of the Juniper Networks IDP Series appliances as well as specific SRX Series gateways - notably, the SRX3400, SRX3600, SRX5600 and SRX5800 gateways, UAC delivers broad Layer 2-7 visibility into and control of application traffic. This allows you to identify and isolate a threat or misuse at the user or device level, and employ a specific, configurable policy action against the offending user or device—quickly addressing and mitigating insider threats before they launch and misuse before it can become a threat, minimizing network and user downtime and productivity loss. Also, UAC delivers secure, encrypted data transport from the endpoint device into and throughout the network—generally or dynamically by user identity or role—mitigating internal hacking and insider threats.
- **Outsourcing and Off-shoring** – The delivery of secure, distinct network and application access control and protection that addresses the risks associated with outsourcing and off-shoring is a requirement for nearly every organization today. UAC, whether deployed standalone or in concert with Juniper Networks SA Series SSL VPN Appliances secures your network and sensitive data and applications from unwanted intrusion by outsource or off-shore partners and contractors. By utilizing any Juniper firewall platform as enforcement points for UAC, you can effectively segment your network—ensuring that sensitive applications and data are only accessed by authenticated, authorized users that you identify, and no one else. The flexible, robust advanced endpoint device assessment capabilities of UAC, including industry-leading antispyware support, ensures that devices used during outsourcing or off-shoring meet your access control and security policies before they are allowed onto your network.
- **Business Continuity** – With the potential for natural and manmade disasters and pandemics on the rise, your organization's ability to address business continuity and disaster recovery in real time means the difference between business success and failure. UAC handles any disaster by allowing you to deliver the same, secure network access control and application protection you demand and your users expect from a primary or a disaster recovery location. UAC provides licenses that allow your organization to address the dramatic increases in simultaneous user and device access that can be created by a disaster or pandemic.

IC4500

IC6500/6500 FIPS

Juniper Networks UAC Components

UAC incorporates three primary elements that are the result of Juniper's real-world experience in the access control and security areas as well as authentication.

These elements include:

The IC Series Unified Access Control Appliances

The IC Series UAC Appliances are UAC's centralized policy management engine optimized for LAN access control. The IC Series can dynamically deliver, install, and upgrade the UAC Agent or Junos Pulse on the endpoint device. The IC Series also collects user authentication (integrating with your existing AAA infrastructure), endpoint security state, and location information from the UAC Agent or Junos Pulse. (The IC Series can gather this same information through UAC's agent-less mode.) Once user credentials are validated and the device security state established, the IC Series dynamically implement the appropriate access policy for each user per session, and push that policy to UAC enforcement points throughout your distributed network.

But, if a user should attempt unauthorized network access via a web browser, UAC allows your administrators the option of redirecting the user to an IC Series appliance for authentication. Once the user logs in to the IC Series appliance with the appropriate credentials, the IC Series appliance redirects the web browser back to the network resource from which it was originally redirected. This captive portal process empowers you to force users to login to an IC Series appliance before they can reach a desired resource within the network, providing your enterprise with further network protection.

The IC Series also supports an 802.1X transaction when a device attempts to connect to your network, and provides another means of user authentication and policy enforcement. Through UAC's adoption of the TNC's standards-based IF-MAP protocol, the IC Series not only can perform their standard access control function, but also serve as a MAP server, integrating with third-party network and security devices that collect data on the state and status of the network, user, and endpoint device. These third-party devices provide the IC Series with their collected network, application, and user state and status data, enabling UAC to leverage this information as part of its access control process.

The UAC Agent, Junos Pulse and UAC Agent-less Mode

The UAC Agent is a cross-platform, dynamically downloadable agent that can be provisioned using a variety of automated and offline delivery mechanisms to meet an organizations software distribution needs. The UAC Agent collects user and device credentials, and provides both Layer 2 (via 802.1X) and Layer 3+ (via firewall enforcement and dynamic IPsec) user-specific access. The UAC Agent's capabilities include an integrated personal firewall for dynamic client-side policy enforcement, as well as specific functionality for Microsoft® Windows® devices that includes IPsec VPN as an optional secure transport to enable encryption from the endpoint to the firewall, and single sign-on (SSO) to Microsoft Active Directory.

UAC also incorporates Junos Pulse, Juniper's integrated, multi-service network client which enables anytime, anywhere connectivity, security and acceleration with a simplified user experience. Junos Pulse may be deployed as the end user client for Juniper's multi-service, interoperable Junos Pulse gateways, including the IC Series Unified Access Control

Appliances, delivering dynamic, granular identity- and role-based network access control. You will be able to select a dynamic download of Junos Pulse or the UAC Agent from your IC Series appliance. Junos Pulse operates like the UAC Agent. Easy to deploy and manage with virtual plug-and-play connectivity, Junos Pulse enables safe, protected cloud and network access for a diverse user audience over a variety of devices. Junos Pulse leverages the existing 802.1X supplicant native to Microsoft Windows 7, Windows Vista and Windows XP to deliver Layer 2 access control. And, just like the UAC Agent, Junos Pulse delivers Layer 3 authentication and IPsec tunneling with Juniper firewalls and SRX Series Services Gateways when deployed as the client for UAC.

The UAC Agent and Junos Pulse also include Host Checker endpoint assessment functionality. This enables devices attempting network connection to be scanned for a variety of security applications and states—including antivirus, antimalware, personal firewalls, and patches. Both the UAC Agent and Junos Pulse also include industry-tested, dynamic antispyware and antimalware protection for Microsoft Windows endpoint devices, scanning device memory for spyware and providing automatic remediation, if necessary. The UAC Agent and Junos Pulse automatically monitor antivirus and antispyware signature and patch files for the latest definition files for posture assessment. The UAC Agent also leverages installed SMS to automatically check an endpoint device upon network connection attempt for application or operating system patch updates, enabling automatic patch remediation, if needed. UAC's Host Checker also enables custom checks of elements such as registry and port status, and can perform an MD5 checksum to verify application validity. The UAC Agent supports the most popular enterprise computing platforms, including support for Apple® Mac OS® operating system software, delivering wired and wireless Layer 2 and Layer 3 authentication and endpoint integrity to Apple Macintosh® users. Junos Pulse supports Microsoft Windows XP, Windows Vista and Windows 7.

Network access control can also be provisioned in UAC agent-less mode for circumstances where software downloads are not practical, such as guest access. Access through UAC agent-less mode still includes provisioning of Host Checker, as well as antispyware and antimalware protection, enabling an organization to guarantee the security state of all network users and their devices prior to network connection and during their network session. Network access via the UAC Agent or by UAC agent-less mode can be dynamically linked to user or device identity, or to the user's role.

UAC Enforcement Points

The choice of enforcement points can often be a limiting factor for a NAC solution. Juniper Networks has solved this problem by creating a solution that is as functional with policy enforcement at Layer 2 as it is at Layers 3-7.

For Layer 2 policy enforcement, UAC works with any vendor's 802.1X-enabled wired or wireless infrastructure—including the Juniper Networks EX2200, EX3200, EX4200 and EX8200 Ethernet Switches that provide standards-based 802.1X port-level access control and Layer 2-4 policy enforcement based on user identity, location, and/or device. When used in conjunction with UAC, the EX2200, EX3200, EX4200, and EX8200 can also apply QoS policies or mirror user traffic to a central location for logging, monitoring, or threat detection with intrusion prevention systems (IPS) such as the market-leading Juniper Networks IDP Series and IPS capabilities with SRX Series gateways.

UAC's Layer 3-7 enforcement is delivered through any Juniper Networks firewall/VPN platform, including the ISG Series Integrated Security Gateways, the SSG Series Secure Services Gateways, and the SRX Series Services Gateways. Juniper Networks J Series Services Routers may also serve as Layer 3 UAC enforcers, providing Source IP enforcement. Some Juniper Networks firewalls also support UTM capabilities—including Juniper Networks IDP functionality, as well as network-based antivirus, antispam, antiadware, antiphishing, and Web filtering capabilities—which can be dynamically leveraged as part of UAC to enforce and unify access control and security policies on a per user and per session basis. This enables you to deliver comprehensive network access and threat control.

UAC is the first NAC solution to deliver full Layer 7 policy enforcement, leveraging the deep packet, application level threat intelligence of standalone IDP Series appliances as policy enforcement points, ushering in a new era of granularity and control for NAC. Through this integration, application-specific IDP Series policy rules can be enforced based on a user's identity and role, as determined by UAC. Policies can also be defined to control time of day and bandwidth restrictions per application or per role.

Solution Planning, Implementation, and Deployment

Instead of simply authenticating users once and providing access control based only on network segmentation, UAC incorporates different levels of session-specific policy and policy types to create extremely granular access control that is easy to deploy, maintain, and change.

- When users and their devices attempt network access, the first step in a UAC-controlled session is for the IC Series to map the user to a role. The information required for role mapping is collected by the UAC Agent, Junos Pulse, or via UAC's agent-less mode. The connection request from users and their devices reveals a number of different end user attributes, including source IP, Media Access Control (MAC) address, network interface (internal versus external), digital certificate, browser type, SSL version, and the results of UAC's Host Checker's endpoint security check. Once user or device credentials have been submitted, the IC Series' comprehensive AAA engine enables seamless deployment into almost all popular AAA settings—including existing RADIUS, LDAP, and Microsoft Active Directory servers, among others.
- The IC Series then combines the user/device credentials and group or attribute information (for example, group membership) with the endpoint compliance state and network location. This combination allows the IC Series to dynamically map users to the second step of access control—a role for their session.
- Each role has, in addition to session attributes/parameters, a set of associated resource policies that govern access to the network. Examples include Layer 2 RADIUS attribute-based policies such as VLAN assignments and/or vendor-specific attributes (VSAs), as well as Layer 3 policies that govern access to IP addresses and netmasks, ports, or ranges of the aforementioned. Also, Layer 7 policies such as IDP policies or URL filtering can provide additional levels of dynamic threat management.

Each successive layer of policy adds more granularity to overall access control. For example, in a combined 802.1X and Layer 3 overlay enforcement environment, UAC can provision a dynamic VLAN assignment along with resource access policies on the UAC enforcement points to fully control user network and application access across the distributed network. At the same time, the level of granularity can be flattened if that level of protection is not required.

Change Your Access Control, Not Your Network

Juniper Networks realizes that the enterprise network is never static. An access control solution must be granular enough to provide the controls needed, but flexible enough to accommodate changing infrastructure and deployments. In addition, the purpose of access control itself can change. As an example, UAC might initially be deployed to provide an additional layer of access control for your wireless LAN (WLAN) but over time might be used to check the endpoint security state of devices attempting to access the wired network to ensure compliance with access policies and minimum acceptable limits. UAC makes it easy to attain both goals with a single deployment. Once the wireless network is secure, that same functionality can be extended to the wired network using the same deployed IC Series appliances and, if deployed, the same UAC Agents or Junos Pulse clients—providing a unified, centrally managed solution for all user access.

While NAC needs to be robust to protect your network, applications, data, and other networked assets, it does not need to be complex to deploy or difficult to administer or use.

One of the biggest roadblocks around deploying access control is the "on or off" dilemma it implies. UAC makes getting around this hurdle easy. All of Juniper's firewalls can be deployed in transparent mode, making it unnecessary to reroute your network. The solution can then be placed in audit mode. This way, you can find out what would have happened had access controls and policies been enforced, without affecting user traffic. In fact, some customers choose to use only audit mode to help them address compliance requirements.

Still another deployment strategy that works particularly well with UAC is the idea of a phased deployment. Because Juniper offers very different modes of enforcement—through vendor-agnostic 802.1X wired switches and wireless access points, through Juniper Networks firewalls and secure routers, or application layer access control with the IDP Series appliances—you can build on the deployment you have today. You may want to enable 802.1X for port-based access control through UAC on a conference room switch, and then add a Juniper firewall or SRX Series gateway to provide network-based access control protecting a server subnet or other critical resource, then roll out 802.1X to employee cubicles and add IPsec enforcement of user traffic going to a protected resource, and then add an IDP Series appliance to deliver role-based, application level access control or an SRX Series gateway with IPS capabilities for Coordinated Threat Control, addressing insider threats and application misuse. The possibilities are as varied as your network environment. UAC is adaptable, scalable, and ensures secure, flexible access control deployments.

UAC is built to address change simply and quickly. Should you want to provide an additional method of enforcement, there is no need to change anything about your UAC deployment but the policies themselves. There is no need to redeploy the IC Series appliance or to download a new UAC Agent or Junos Pulse client. New enforcement methods can be added seamlessly.

JUNIPER NETWORKS SERVICE AND SUPPORT

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services/.**

Another dilemma for organizations deploying a NAC solution is the creation, management, and provisioning of security and access policies. Centralized access policy management is achieved when UAC is deployed with Juniper Networks Network and Security Manager (NSM) and SA Series SSL VPN Appliances. Common configuration templates can be created and shared between SA Series appliances for remote access control and IC Series appliances for local or LAN-based access control when deployed in the same network environment along with and managed by NSM. This empowers you to implement and enforce consistent remote and local access control policies across your distributed environment, enabling and simplifying the enterprise-wide deployment of uniform network access control. NSM also delivers a single network management platform that allows you to configure and manage many of the key components of a UAC deployment, including the IC Series, Juniper Networks firewalls, SRX Series gateways, EX Series switches, as well as IDP Series and SA Series appliances.

Also, through its support for the TNC's standards-based IF-MAP protocol, the IC Series appliances share user session data with SA Series appliances, as well as other IC Series appliances to enable "follow-me" policies. This federation of user session data delivers seamless provisioning of SSL VPN sessions into UAC at login. The IC Series-SA Series and IC Series-IC Series federation in UAC enables users' access via a single login to networked corporate resources protected by uniform access control policies, delivering a consistent user access experience whether users are connecting to the network locally or accessing it remotely.

Summary: Extending and Simplifying NAC

Your NAC solution must extend beyond simple admission and access control. It should leverage and interoperate with existing network investments for quick, simple deployment. It should be based on open, industry standards so that you avoid being locked into a single vendor's solution and appliances. It should simplify rollout, even enable phased deployments, enhance usability—and ease network access administration, provisioning, and management. And, your network access control solution should address the access control challenges you are confronted with daily—including regulatory compliance, insider threats, guest access, outsourcing and off-shoring, and business continuity. Juniper Networks Unified Access Control addresses all of these requirements, challenges, and more.

For more information about comprehensive network access control that uses the network you have today, please contact your Juniper Networks sales representative, Juniper authorized partner, or visit **www.juniper.net/uac**.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at **www.juniper.net.**

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

♻ Printed on recycled paper

1500051-005-EN Sept 2010