

Comprehensive Network Access Control Based on the Network You Have Today

Juniper Networks Unified Access Control



You need to control access to your LAN for users such as guests, contractors and your own employees. Juniper Networks Unified Access Control solution will help you meet that need – regardless of the architecture in the network segment you’re concerned about – today.

Juniper Networks Unified Access Control delivers a comprehensive solution that:

- Combines user identity, device security state and location information for session-specific access policy by user.
- Uses the network you already own, including your Authentication, Authorization, Auditing (AAA) infrastructure, any 802.1X-enabled switches or access points and/or any Juniper firewalls.
- Is based on field-tested components being used today in thousands of deployments worldwide.

The Need for Access Control

In today's enterprise, the network is increasingly becoming 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. As access has grown, however, so too has the risk in providing it. Enterprise users may become unknowingly infected when surfing the Internet or working remotely, then bring those infected devices directly into the network. Users accessing the WAN from within the LAN without any access controls can open the enterprise to a host of threats. Guest users who may only need an Internet connection can come onto the network with their own unmanageable devices, and unknowingly expose-sensitive LAN resources to malware.

Controlling access to the network is not new. In many cases the term simply serves to unify a number of disparate problems that enterprises have been wrestling with for some time. As the category has become more defined, however, a plethora of solutions has emerged, each of which attempts to handle access control in a different way. Some common methods include solutions that use DHCP, 802.1X, VLANs, inline devices, firewalls, IPSec gateways and host-based software. Each of these technologies alone can have significant drawbacks, which is why many solutions employ a combination of them. This can make it very difficult to get a clear picture of any one solution and how it functions.

An Access Control Solution You Can Trust

The Juniper Networks Unified Access Control (UAC) v2.0 solution combines the best of access control technologies while leveraging the existing enterprise investments and deployments. All policy is created and pushed by the Infranet Controller, a hardened centralized policy server. User identity, device state and network location can be determined by a dynamically deployable Agent as well as via agentless mode where installing a software client is not feasible. Finally, UAC can enforce policy at Layer 2 using any vendor's 802.1X-enabled switches or wireless access points, at Layers 3-7 using Juniper firewalls, or both. Every component, including the Infranet Controller, UAC Agents and enforcement points is built on field-tested, widely deployed devices, including features from Juniper's Secure Access SSL VPN with its legacy of dynamic endpoint assessment and seamless interaction with the AAA backbone; Juniper Networks Odyssey Access Client (OAC), the market-leading 802.1X supplicant; and Juniper Networks Steel-Belted Radius (SBR), the de facto standard in RADIUS servers. The result is a uniquely flexible solution that combines user identity, device security state information and network location to create a session-specific access control policy for each user using the network that you have in place today.

Juniper Networks Unified Access Control Components in Detail

Juniper's UAC solution incorporates three primary elements that are the result of real-world experience in the access control area (from SSL VPN) as well as the AAA world (OAC and SBR). They include:

- **The Infranet Controller**

- The Infranet Controller is the centralized security policy engine optimized for LAN access control. Based on Juniper's market-leading Secure Access SSL VPN appliances, the Controller can push an agent down to the endpoint, collect information from the agent and act as an interface with your existing enterprise AAA infrastructure. Once user credentials are validated and the security state established, the Controller implements the appropriate access policy for each user/session, and pushes that policy to enforcement points throughout the network.
- The Controller also features integrated RADIUS functionality from SBR, the de facto standard in RADIUS servers. This enables the Controller to support an 802.1X transaction when an endpoint enters the network, and provides a second method of user authentication and policy enforcement.

- **The UAC Agent**

- The UAC Agent is a dynamically downloaded agent that can be provisioned in real time by the Controller, installed using Juniper's Installer Service or deployed by other methods. The Agent serves to collect user credentials, as well as to assess the security state of the endpoint. The UAC Agent includes the means to access the network both at Layer 2 with 802.1X via integrated functionality from the OAC, as well as at Layer 3. These capabilities include an integrated personal firewall for dynamic client-side enforcement of policies, as well as specific functionality for Windows devices that includes IPsec VPN (which enables encryption from the endpoint to the firewall) and Single SignOn to Active Directory. The Agent also includes Host Checker functionality, familiar from thousands of Juniper Secure Access SSL VPN deployments, which enables the administrator to scan endpoints for a variety of security applications/states including, but not limited to, antivirus, malware and personal firewalls. UAC also enables custom checks of elements, such as registry and port status, and can do an MD5 checksum to verify application validity. Deployment is simplified with predefined Host Checker policies, as well as automatic monitoring of AV signature files for the latest definition files for posture assessment.
- Access can also be provisioned in agentless mode, in circumstances where downloads of any software are not practical, such as in guest deployments. Access through agentless mode still includes provisioning of Host Checker, enabling the enterprise to guarantee the security state of all network users.

- **UAC enforcement points**

- While the Infranet Controller and the UAC Agent are somewhat deployment neutral, the choice of enforcement points is often the limiting factor with a network access control solution. Juniper has solved this problem by creating a solution that is as functional with enforcement at Layer 2 as it is at Layers 3-7. For Layer 2 enforcement, UAC can work with any vendor's standards-compliant 802.1X-enabled wired or wireless switching infrastructure. Layer 3-7 enforcement is provided via any Juniper Networks firewall/VPN platform including the Integrated Services Gateway with Intrusion Detection and Prevention and the Secure Services Gateway secure routing platforms. Juniper's wide range of

firewalls offers throughput ranging from 75Mbps to 30Gbps, while some firewalls also support threat management capabilities, including Juniper's Intrusion Detection and Prevention functionality, as well as network-based antivirus, anti-spam and URL filtering capabilities. All of these capabilities can be dynamically leveraged as part of the UAC solution. Customers can use UAC not only to enforce access control policies but also to apply security policies such as deep packet inspection, antivirus and URL filtering on a per user/session basis. This enables the enterprise to unify the application of access and security policies for comprehensive network access and threat control.

Unified Access Control in Action

Instead of simply authenticating users once and providing relatively crude access controls based on network segmentation only, the UAC solution incorporates three different levels of session-specific policy, including authentication/authorization, roles and resource policies. Together these different policy types can be used to create extremely granular access control that is also easy to deploy, maintain and change.

When a device comes onto the network, the first step in a controlled session is for the Infranet Controller to map it to a role. The information required for this mapping is collected by the UAC Agent or via Host Checker in the case of an agentless deployment. The request from the user (in either 802.1X mode or non-802.1X mode, via browser-based agents that are provisioned to the endpoint) reveals a number of different end-user attributes, including source IP, MAC address, network interface (internal versus external), digital certificate if one exists, browser type, SSL version and the results of the endpoint security check. Once credentials are submitted, the Controller features a comprehensive authentication, authorization and accounting engine for seamless deployment into almost all popular AAA settings, including existing RADIUS, LDAP, AD, Netegrity SiteMinder, Certificate/PKI servers and Anonymous Authentication servers.

The Controller then combines the user credentials, and group or attribute information (for example, group membership, if any), with additional information gathered, such as endpoint compliance state and network location. This combination allows the Controller to dynamically map the user to the second step of access control – a role for the session. Role attributes can encompass session attributes/parameters, and can also specify restrictions with which the user must comply before the user can map to a role. These restrictions are extremely useful in settings where security is vital and compliance must be ensured.

The third and final step in access control is the assignment of the resource policy, which governs network and resource access. Some examples include Layer 2 RADIUS attribute-based policies such as VLAN assignments and/or vendor specific attributes, as well as Layer 3 policies that govern access to IP addresses/netmasks, ports or ranges of the above. Layer 7 policies, such as IDP policies or URL filtering, provide additional levels of dynamic threat management.

Each successive layer of policy can add still more granularity to overall access control, in contrast to some solutions that only have one or two steps in the access control process. For example, in a combined 802.1X and network enforcement environment, UAC can provision a dynamic VLAN assignment along with resource access policies on the Infranet Enforcers to fully control user access throughout the network. At the same time, this level of granularity can be flattened if the customer does not require it or if the level of protection needed does not merit it. Granular policies are easy to set up and maintain, as they can be duplicated, inherited and edited for streamlined administration. Each time there is a need to create new policies based on those in use, administrators may reuse those that have been already set, including: dynamic authentication policies; role definitions; role settings; and resource authorization policies, including multiple resource groupings that can be associated with the same role, and additional roles that can be easily added to existing resource groupings.

One Network Access Control Solution for All Your Users

One of the primary hurdles in deploying access control is determining what user type it is meant to serve. Each comes with its own set of challenges – guest users, for example, probably bring their own device that you cannot manage and may not even be able to check. These users often need very limited access to corporate resources, but frequently get the Internet access they really need via a wireless LAN that can give them a way into your enterprise's most sensitive materials.

Employees present a completely different set of challenges. In this case, you typically can manage the device – when it is on your network. The activities that occur when the device is being used elsewhere, however, can pose a significant challenge. Adding to the complexity is most users don't thoroughly understand the ins-and-outs of security applications and they don't want to learn. They want to be productive wherever they are. Unfortunately, when the unaware user meets today's talented, well-armed attackers, the results can be as devastating as they are unintentional. Additionally, specific groups of users may require access to privileged resources that need to be protected from the general user population.

Finally, there is the problem of contractors. These users present a unique profile in that they may need access to more sensitive resources, but they will often have their own devices. A good way to picture this user group is to picture a group of auditors. These professionals know their business very well but they don't know your network, and they probably don't have device security as a top-of-mind concern.

Juniper's Unified Access Control solution can address each of these user types without overloading your help desk.

There are several different methods to accommodate guest users, depending on how your network is configured. If you are using 802.1X infrastructure as enforcement – for example, in a wireless deployment – it's safe to assume that the guest will neither have your 802.1X supplicant installed, nor will the guest be able to install it. The cross-platform UAC agentless mode was developed specifically for this use case, and supports browser-based validation of user credentials and scanning of endpoints for posture assessment both before user authentication and throughout the user session. The guest can be directed to a very restricted VLAN for limited access. If you are using Juniper firewalls as an additional or alternate enforcement point, you can further control guest access within the network. The flexible UAC solution can support a variety of guest-access policies such as no guest access at all, access requiring an Acceptable Use Policy, access requiring a basic level of endpoint integrity (such as an antivirus client) without an authentication component or open guest access to the Internet while restricting access to protected corporate resources.

Because your employees are probably using managed devices, it is tempting to think that they would be much easier to manage than guest users, but in reality this may not be the case. One consideration is sheer numbers – it is a reasonable expectation that employees will outnumber guests in most typical enterprises. For an access solution to succeed in this environment, it must be capable of being deployed or updated in real time, and it must enable self-remediation to the greatest extent possible. Juniper's UAC solution meets these needs with ease. The UAC agents can be deployed as part of a standard image, using the Juniper Installer Service, or sent down in real time from the network. If you are using 802.1X infrastructure as an enforcement mechanism, the user without the UAC Agent can be sent to a default VLAN to download it. If you are using Juniper firewalls as an additional or alternate enforcement point, the user can be redirected using captive portal technology (the "hotel experience"). Privileged users can be identified by their authentication attributes (username, group membership or extensively customizable LDAP attribute checking) and provisioned additional access to critical resources, subjected to additional endpoint security requirements, and so on.

Accommodating the needs of contractors varies depending on a number of factors, including the sensitivity of the resources that they will need to access and the length of time for which the assignment is scoped. This is another area in which Juniper's experience with dynamic downloads can greatly ease a deployment. The endpoint device can be checked and the UAC Agent deployed, or the deployment can be done in agentless mode, depending upon your infrastructure and what you need the solution to do. Access control policies on the Juniper firewalls can provide time-based access restrictions as well as additional L7 threat management functionality.

Another consideration for all users, regardless of role, is the ability to identify and isolate endpoints that are not in compliance with enterprise security requirements – and to allow the user the ability to self-remediate or, in some cases, to auto-remediate for the user so no action is required on their part. Along with its extensive endpoint compliance checking capability, the UAC solution offers equally customizable remediation handling: restricting users to a remediation VLAN or network segment containing only a remediation server, providing the ability to offer customized instructions specifying exactly what is out of compliance and how to fix it, and remediating for the user where possible and appropriate.

Change Your Network, Not Your Network Access Control

Juniper Networks realizes that the enterprise network is never truly 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 the access control itself can change. One example might be in a wireless deployment. Initially, the UAC solution might be deployed to provide an additional layer of access control to your WLAN, by ensuring that users are authenticated. Over time, however, there may be a desire to check the endpoint security state of users and ensure that they comply with minimum acceptable limits. UAC makes it easy to achieve both goals in a single deployment. Once the wireless network is secure, that same functionality can be extended to the wired network, providing a unified, centrally managed solution for all user access.

One of the biggest roadblocks around deploying access control is the “on or off” dilemma it implies. UAC makes getting around this hurdle easy, particularly if you are using a Juniper firewall as an enforcement point. All Juniper firewalls can be deployed in transparent mode, making it unnecessary to reroute your network. The system can then be placed in Audit mode. You'll find out what would have happened had access controls been in place without affecting user traffic. In fact, some customers choose to use only Audit mode to help them meet compliance requirements.

Still another deployment strategy that works particularly well with UAC is the idea of a phased deployment. The fact is that few networks have an enterprise-wide deployment of both 802.1X infrastructure or Juniper firewalls. Most have some wireless in one segment, firewalls in another, and 802.1X wired switches in still another. While the intent may be to standardize, it is part of the fluid nature of the network that such standard deployments rarely exist in reality. With UAC, however, it doesn't matter. Because Juniper offers two very different modes of enforcement – vendor-agnostic 802.1X wired switches/wireless access points or Juniper firewalls – you can build on the deployment you have today. You may want to enable 802.1X for port-based access control on a conference room switch, and then add a Juniper firewall to provide network-based access control protecting a server subnet or other critical resource, then roll out 802.1X to employee cubes and add IPSec enforcement of user traffic going to the protected resource. The possibilities are as varied as your network environment.

And Juniper UAC is built to change. Should you want to add 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 Infranet Controller or to download new UAC Agent software. New enforcement methods can be added seamlessly.

**CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA**

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100
www.juniper.net

EAST COAST OFFICE

Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

**ASIA PACIFIC REGIONAL
SALES HEADQUARTERS**

Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, 25/F
ICBC Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

**EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS**

Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Addlestone
Surrey, KT15 2PG, U.K.
Phone: 44-(0)-1372-385500
Fax: 44-(0)-1372-385501

Copyright © 2007, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Networks Service & Support

Juniper Networks delivers comprehensive service and support solutions. With our support portfolio, you benefit from the economy and simplicity of a single service solution to maintain your network's day-to-day operation. Key services include the delivery of around the clock technical assistance, online tools, software support, and options for parts delivery and onsite support. You receive the support you need and the value you deserve. For complete details, please visit us at: <http://www.juniper.net/products/services/>.

About Juniper Networks

Juniper Networks develops purpose-built, high-performance IP platforms that enable customers to support many different services and applications at scale. Service providers, enterprises, governments, and research and education institutions rely on Juniper to deliver a portfolio of proven networking, security, and application acceleration solutions that solve highly complex, fast-changing problems in the world's most demanding networks. Additional information can be found at www.juniper.net.

Next Steps

For more information on how your company can benefit from Juniper Networks products, please contact your sales representative or visit: http://www.juniper.net/products_and_services/unified_access_control/index.html

