

JUNIPER NETWORKS UNIFIED ACCESS CONTROL AND EX SERIES ETHERNET SWITCHES

A Comprehensive Standards-Based Solution for Network Access Control

Challenge

Some enterprises believe that deploying network access control can be complex, costly and time consuming. Yet a comprehensive 802.1X-based network access control solution addresses many of these challenges.

Solution

Juniper Networks Unified Access Control and Juniper Networks EX Series Ethernet Switches are deployed together, they create a complete 802.1X standards-based network access control environment. The interoperable UAC and EX Series provide powerful pre- and post-admission access control and enforcement, protecting the network, applications and sensitive data.

Benefits

- Protects the network, applications and data from unauthenticated access, attacks and breaches
- Provides the freedom to select and work across diverse network components including other 802.1X compatible switches and Juniper Networks firewalls/VPNs
- Eases network access control deployment
- Delivers added value
- features and interoperability
- A single vendor to work with and to address support if necessary

As businesses today move toward greater mobility and an increased emphasis on outsourcing, enterprises are pressed to employ a more mobile workforce, expand their use of outside contractors, and sustain an increasing number of vendors and partners. All of these users, as well as guest users require network and application access, which places tremendous stress on the enterprise network, its resources and enterprise IT staff. Network and application access needs to be pervasive yet robust and secure. Yet as the demands and availability of network and application access increase, so do the risks to the network, applications and the enterprise's sensitive data.

Network access control is a necessity for today's high-performance enterprise network since it mitigates the risk and manages the threat threshold for enterprises and their networks. Network access control manages access to the network and its applications based on user and/or device compliance against a series of enterprise-defined network and security policies. Criteria for network and security policies include user identity, device identity, device health, device security state and/or network location, to name a few. Policies to be enforced may include users and their devices adhering to and maintaining a baseline of device security state or other criteria defined by the enterprise and ensuring the network and application access and authority of specific users and user roles. A network access control solution can ensure that access is allowed only to authorized corporate resources and all corporate authentication and security policies are met by both user and device before network access and during a network session.

The Challenge

Some enterprises today are concerned that deploying network access control can be complex, costly and time consuming. These enterprises often fear that network and business disruptions could upset their management. They are also concerned that return on investment (ROI) is outweighed by the time and cost of deploying network access control. Network administrators are looking for solutions that address these challenges and protect their network and application integrity, while providing the flexibility to evolve, remain non-disruptive to business operations, and leverage existing network infrastructure investments.

- Selecting network access control based on industry standards accomplishes this. Standards are vital for enterprises, allowing them to:
 - Avoid single vendor lock-in, which provides immunity to price increases and enables technologies to be open and accessible
 - Increase ROI by leveraging existing networking infrastructure components
 - Freely select network infrastructure and technology
 - Ease integration with diverse technologies

Network access control requires a secure, strong and flexible framework for authentication, access management, network security and data privacy. The 802.1X standard, the Institute of Electrical and Electronics Engineers (IEEE) standard for port-based network access control delivers that, and:

- Robust pre-admission and post-admission control enforcement
- A resilient authentication process
- Interoperability with new or existing heterogeneous network components
- Simplicity and speed in the deployment and integration of 802.1X standards-based components

A comprehensive 802.1X-based network access control solution addresses the challenges faced by administrators and their networks by protecting the network, delivering ease and flexibility of deployment, leveraging existing network components, and ensuring network and application integrity. The solution also allows freedom of choice for network components and policy enforcement.

Juniper Networks Comprehensive Solution for Standards-Based Access Control

Juniper Networks® UAC deployed with Juniper Networks EX Series Ethernet Switches delivers a complete 802.1X standards-based network access control environment. The interoperable UAC and EX Series deliver a seamless and single solution that provides powerful pre- and post-admission access control management and enforcement, protecting sensitive corporate data from unauthenticated access, attacks and breaches. The integrated UAC and EX Series also provide enterprises the freedom to select and work with diverse network components including, in the case of UAC, existing or new 802.1X compatible switches and Juniper Networks firewalls. The combined solution avoids the pitfalls usually faced with single-vendor solutions while providing the benefits of working with one vendor for a comprehensive solution including easier and quicker deployment, added value features and interoperability, and one company to contact for support.

UAC combines user identity and device security state information with network location to create a unique, session-specific access control policy for each user. UAC is based on industry standards including 802.1X, Extensible Authentication Protocol (EAP), RADIUS, IPsec, and the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) standards for endpoint integrity and network access control. Its foundation includes field-tested components, including Juniper Networks SA Series SSL VPN Appliances, Odyssey Access Client, and SBR Series Steel-Belted Radius Servers that are used today in thousands of deployments worldwide and which enable UAC to leverage your existing

network environment. With UAC, policy enforcement can be enabled at Layer 2 using the 802.1X standards, or at Layer 3 using an overlay deployment with Juniper Networks firewalls. It can also be provisioned in mixed mode using 802.1X for network admission control and Layer 3 for resource access control. UAC reduces network threat exposure, delivers comprehensive control, visibility, and monitoring to surpass regulatory compliance, and decreases access control deployment cost and complexity, while delivering flexibility for phased deployments. UAC extends access control to network traffic by implementing policy enforcement deeper into your network's core and outward to its edge, which mitigates risks and protects sensitive corporate assets.

The EX Series, which includes the EX3200 and EX4200, combines the high availability (HA) and carrier-class reliability of modular systems with the economics and flexibility of stackable platforms. This delivers a scalable solution for data center, campus and branch office environments. By offering a full suite of Layer 2 and Layer 3 switching capabilities, the EX Series Ethernet Switches satisfy a variety of high-performance applications including Gigabit Ethernet aggregation deployments. A single 24-port or 48-port EX Series Ethernet Switch can be deployed initially. Yet as requirements grow, Juniper's Virtual Chassis technology which is available on the EX4200 allows EX Series Ethernet Switches to be interconnected over a 128 gigabit per second (Gbps) backplane and managed as a single device. This provides a scalable, pay-as-you-grow solution for expanding networks. All EX Series Ethernet Switches include HA features such as redundant, hot-swappable internal power supplies and field-replaceable, multi-blower fan trays to ensure maximum uptime. Each EX Series switch includes an integrated ASIC-based packet-forwarding engine, the EX-PFE, while an integrated Route Engine (RE) based on existing, field-proven Juniper technology delivers all control plane functionality. This brings the same level of carrier-class performance and reliability to the EX Series that Juniper routers bring to the world's largest service provider networks. The EX Series also leverages the same modular Juniper Networks Junos® operating system as Juniper's router products, ensuring a consistent implementation and operation of each control plane feature across the entire Juniper infrastructure.

EX Series and UAC combined together create a comprehensive 802.1X network access control solution that delivers rich policy enforcement capabilities. The EX Series is deployed as enforcement points within a UAC environment, utilizing the 802.1X standard for port level access control and Layer 2 to Layer 4 policy enforcement. The user's identity, device posture and location are used by UAC to determine network admission. If UAC grants network access, it will propagate that information to the EX Series, which will assign the user to a specific VLAN based on their authorization level. When deployed together, the EX Series and UAC can enforce and set user-based quality of service (QoS)

policies for the prioritization of data, voice and video traffic. Also, UAC and EX Series switches can mirror user traffic to a central location for logging, monitoring or threat detection by intrusion prevention systems like the market-leading Juniper Networks IDP Series Intrusion and Detection Prevention Appliances. UAC also leverages the capabilities of the IDP Series to deliver broad

application traffic visibility, which isolates threats to the user or device level and employs an applicable policy action via the EX Series against the offending user or device. UAC can also correlate user identity and role information to network and application access, which better addresses regulatory compliance.

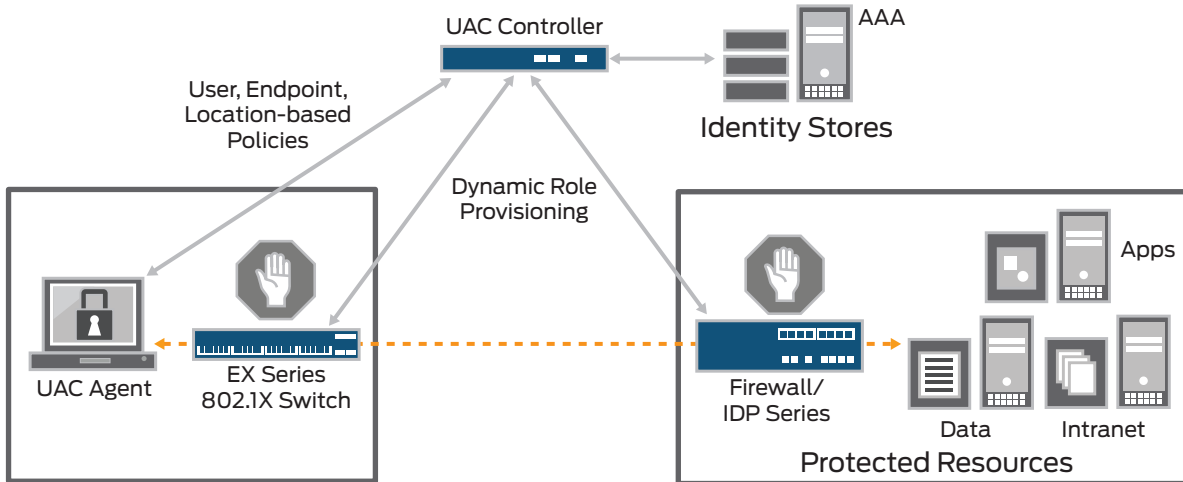


Figure 1: Juniper Networks comprehensive 802.1X network access control solution with UAC and EX Series

Features and Benefits

Together, EX Series Ethernet Switches and UAC deliver a comprehensive 802.1X standards-based network access control solution that:

- Provides rich policy enforcement capabilities
- Uses the 802.1X standard for port level access control and Layer 2 to Layer 4 policy enforcement for robust network admission control
- Enforces user-based QoS policies that enable data, voice and video traffic to be prioritized
- Mirrors user traffic to a central location for logging, monitoring or threat detection by IPS products such as the IDP Series
- Isolates threats to the user or device level and applies a suitable policy action against threatening users and/or devices, when used in conjunction with the IDP Series

Solution Components

Combining the flexibly deployed, best-in-class UAC with the carrier-class reliability of EX Series Ethernet Switches enables organizations to quickly and easily deploy a network access control solution that delivers the performance, availability and operational simplicity to meet the demands of today's high-performance enterprises.

Summary

When deployed together, UAC and EX Series Ethernet Switches provide a complete 802.1X standards-based network access control environment, delivering a seamless solution with powerful pre and post-admission access control and enforcement. UAC interoperating with EX Series enables you to single source a complete, standards-based, best-in-class NAC solution. This also allows you to enjoy value added features when the products are deployed together as well as economies of scale for support and service and the evolution of a complete access control environment. An integrated access control solution of UAC and EX Series gives you the freedom to work with and choose diverse network components. This allows you to avoid vendor lock-in and delivers simple and flexible deployment options, while providing added value features and a single source for support.

Next Steps

For more information on UAC, please go to www.juniper.net/uac. For more information on EX Series Ethernet Switches, please go to www.juniper.net/switching. Or contact your Juniper Networks representative for more information.

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

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

Copyright 2010 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. 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.