White Paper

The Importance of Standards to Network Access Control

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Part Number: 200205-001 Nov 2006

Table of Contents

Introduction

Users today are accessing enterprise networks from anywhere in the world, at any time of day, all via a myriad of access technologies and devices running any number of operating systems, operating environments, and applications.

In this globally dynamic and diverse world, today's network administrator has no idea where a user's managed or unmanaged device has been before it attempts to access the enterprise network. A user's device could be infected with insidious, virulent forms of malware spawned by today's sophisticated, well-funded hacker. A user's device could be acting as a transfer agent for the spread of viruses, spyware, adware, Trojans, worms, bots, rootkits, or other malicious applications, onto the enterprise network or directly to other unsuspecting user devices. The introduction of any of these unwanted infections can put an organization's intellectual property at risk and it can have a serious impact on productivity, significantly increasing costs to the enterprise.

Enter network access control. While there is no universally agreed upon definition for network access control, it is essentially the ability to control network access based on compliance with network policies. The network policies with which compliance is required may include policies based on user identity, device identity, device health, and device location, to name just a few. Network access control can ensure that the appropriate connection is made to the appropriate network in the appropriate manner by both user and device. Network access control can also ensure that users meet authentication policies, that their devices meet authentication and security policies, and that users and devices comply with any other policies set by an organization.

Because of its breadth of capabilities and depth of function, network access control solutions frequently cut across not just the entire enterprise network, but also across a number of internal organizations and functions as well. A network access control deployment spans virtually every IT discipline, from desktop management to desktop security, from network infrastructure to network administration. It may also include individuals and resources involved in regulatory compliance, since network access control addresses several of the organizational requirements for successful compliance with industry and governmental regulations. Like the number and variety of groups that are involved in a network access control decision process, there are a number of user devices and network infrastructure hardware, software, and firmware components that will be affected by the decision as well.

Given the wide ranging nature of network access control, from the number and variety of user devices and infrastructure components directly impacted by its introduction to the number of organizational disciplines involved in any network access control decision process, the decision between a standard or proprietary network access control solution becomes vitally important.

Standard vs. Proprietary Network Access Control

A definition of the word "standard", as found in the Merriam-Webster OnLine Dictionary, is "something established by authority, custom, or general consent as a model or example." Conversely, the word "proprietary", according to the same Merriam-Webster OnLine Dictionary, means "something that is used, produced, or marketed under exclusive legal right of the inventor or maker." These definitions also apply to the world of network technology.

In a technical context, a "standard" is usually defined as a set of guidelines or specifications for interoperability that have been agreed upon, adopted, or approved either universally or by a large group of interested parties. "Open standards" are a set of interoperability guidelines that are publicly available and may be implemented by anyone who chooses to do so. Standards encompass the ideas of many, as well as the concepts of compatibility, interoperability, and agreement.

In the network access control space, there are a variety of solutions available but most network access control solutions are proprietary either in part or in total. And while proprietary network access control solutions may seem attractive in the short run, they can be very costly in the long run.

Virtually any group or organization can declare that their specifications or guidelines are a "standard". However, unless those specifications or guidelines are made available to the public for their general use and adoption without obstruction or restriction, including constricting licensing terms or use fees, they are not truly a "standard". Users need to beware of specifications that appear to be or call themselves "standards" but in reality are proprietary. Restrictions may apply to the use of those specifications that serve the interests of the specification's creator rather than the user.

Similarly, a vendor might successfully entice a large number of companies to adopt a set of private guidelines or specifications, but that does not make those specifications into open standards. Unless a guideline or specification is openly published for public review and use, has been universally accepted or agreed upon by a group of like-minded, interested parties, and is free of use restriction, it is not a standard. It is owned and controlled privately and therefore, by definition, proprietary.

There are many compelling reasons why a standards-based solution for access control should be considered by an organization when determining what network access control solution to select. A standard emphasizes the interoperability between components. Additionally, standards provide interoperability with other technologies and products, ensuring that best-of-breed selections made by the organization will work seamlessly together. Adoption of a proprietary solution, on the other hand, can decrease flexibility and increase total cost of ownership (TCO), limiting the ability to create heterogeneous environments based on best-of-breed technologies, and ultimately limiting selection and choice.

For most organizations, the decision whether to select and implement a standard or proprietary solution will boil down to several key factors:

1. An organization needs to determine what value a given technology, whether standards-based or proprietary, brings to their business. One consideration is whether the solution offers immediate cost savings. Standards are vital for organizations looking to avoid being locked into a single vendor's technology, products, and ongoing support. By using standards-based technologies, organizations need not worry about price increases or other unilateral actions that might be taken by a supplying vendor.
2. A second important consideration is the time, effort, and expense needed to integrate, test, and deploy a selected solution, and whether a standard or proprietary solution aids in decreasing those expenditures. Standards enable technologies to be open and accessible, and typically provide organizations deploying standard technologies with the ability to choose from several different vendors. The impact of this advantage is clearly amplified as the number of interoperable elements within an overall solution increases. Standards-based solutions can decrease total cost of ownership (TCO) and at the same time give organizations the freedom to choose the technologies they wish to use and integrate. The use and implementation of standards equates to value and freedom of choice.
3. Network access control solutions integrate a number of user, device, and network related security and access control technologies. These include Authentication, Authorization, Accounting (AAA), endpoint device integrity and security, network policy management and enforcement, and quarantine and remediation. A network access control solution based on standards seamlessly integrates these technologies and inevitably links the various organizational disciplines responsible for overseeing the implementation of these technologies, including network operations and administration, security operations, desktop management, RADIUS or identity management, and compliance. By selecting

a standards-based network access control solution, organizations can simultaneously integrate several technologies as well as the groups and disciplines crucial to the successful implementation and deployment of those technologies.

4. Access control also has its share of standards and protocols to ensure compatibility and interoperability. Among those standards and protocols are RADIUS, Extensible Authentication Protocols (EAP), and 802.1X. As the IEEE standard for port-based network access control adapted for use in the enterprise space, the 802.1X standard provides a strong framework for authentication, access control, and data privacy. The 802.1X standard has driven and utilizes other standards, including Remote Dial-In User Service (RADIUS) which is a standard client/server security protocol from the IETF that is typically used in authentication servers in 802.1X-based environments. RADIUS provides authentication checks for users or devices. Also, the 802.1X standard utilizes the Extensible Authentication Protocol (EAP) standard which works over a variety of authentication systems and delivers an authentication framework standard for wireless and wired networks. (The importance of the 802.1X standard along with related protocols and standards to access control will be discussed in a separate white paper.)

The only standards-based, open network access control architecture available that conforms to nearly every description of a “standard” is the Trusted Network Connect (TNC), a set of standards-based, open specifications that are constructed on the twin ideals of integrity and identity.

What Is Trusted Network Connect

Trusted Network Connect, or TNC, is the name of a subgroup of the Trusted Computing Group (TCG). It is also the name of the open standard network access control architecture.

The Trusted Computing Group (TCG) is a not-for-profit organization formed in 2003 to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies across multiple platforms, peripherals, and devices. The TCG has approximately 140 members, including component vendors, software developers, systems vendors, and network and infrastructure companies, of which 70 members have participated in and continue to actively participate in the definition and specification of the TNC’s open, standards-based network access control architecture.

The Trusted Computing Group’s Trusted Network Connect (TNC) solution is an open architecture that defines several standard interfaces, indicated by dotted lines in the architecture diagram in Figure 2. These standard interfaces enable components from different vendors to securely operate together, creating an endpoint integrity and network access control solution from existing installed equipment and heterogeneous networks. The TNC architecture is designed to build on established standards and technologies, such as 802.1X, RADIUS, IPsec, EAP, and TLS/SSL.

How TNC Works

The TNC architecture has been designed to help organizations protect their enterprise networks from viruses, worms, denial of service (DoS) or other malevolent application attacks by allowing them to audit device configurations and impose enterprise security policies before network access has been established. The TNC architecture builds on existing industry standards and defines new open standards as necessary, with an objective of enabling non-proprietary and interoperable solutions to work together within multi-vendor environments.

The TNC’s open specifications encompass the definition of software interfaces and protocols for communication among endpoint security components and between endpoint hosts and networking elements. The Trusted Network Connect architectural framework provides for interoperable solutions from multiple vendors and offers greater choice in selecting the components best suited to meet endpoint integrity and network access control requirements.

802.1X and EAP, IPsec, and RADIUS standards were created to address secure network connectivity. These standards supply a sturdy foundation for extending the network access control process to include host-related security configuration information, and they are widely supported by networking equipment vendors. The wide distribution and implementation of these robust security standards and protocols enable customers to incorporate TNC technology by leveraging existing infrastructure investments without sacrificing interoperability or freedom of choice.

The TNC architecture describes the interaction of various network entities to measure the state of a client system or device attempting to connect to a network, and to communicate that state to other network entities such as systems, appliances and servers. This allows the assessment of the client's compliance to an organization's minimum security policy requirements and a determination of the network's reaction to the request for access.

Solutions based on the TNC open specifications ensure the presence, status, and security level of security applications as well as other applications specified by an organization. TNC-based solutions maintain an organization's access policy by validating the device or user authentication and requiring the establishment of a level of trust before network connection can be allowed. These solutions also provide the option of quarantine and remediation for devices that do not meet minimum security policy requirements, as determined and defined by an organization. This is accomplished by isolating the offending devices and then, if possible or warranted, applying the appropriate remediation procedures to satisfy the organization's defined security policy and provide eligibility for enterprise network access.

TNC Standards-Based Architecture

Typical network access control solution architecture resembles that of standard access control security architecture, such as RADIUS or 802.1X. In the network access control architecture, the enterprise network is guarded by an enforcement point which only grants access to users and devices if they have been approved by the network control server. Many different network devices can function as an enforcement point: an 802.1X access point, a switch or router, a firewall, a VPN gateway, or a specialized endpoint integrity device, to name just a few.

An agent is either preinstalled or downloaded on the user's device. This agent typically uses APIs or plug-ins to collect information about the user device's security state and security products status, and it determines if the user device is clean of any malware or other malicious applications.

The user or device is then authenticated against the organization's enterprise network to ensure that it has been approved for network access. Once authenticated, the information collected about the security state of the user device and the status of its security software is compared against the organization's previously defined network security and access policies. When the user device's profile has been checked against the organization's policies and has been found to be compliant with those policies and any other criteria defined by the organization, the user and their device may be granted access to the enterprise network.

The user or device authentication, the device's security state, the status of the device's security software, compliance with the organization's security and network access policies, and user or device authorization will all determine if the user and device will be granted access to the organization's enterprise network, or if another sort of action such as network access denial, quarantine and remediation should occur.

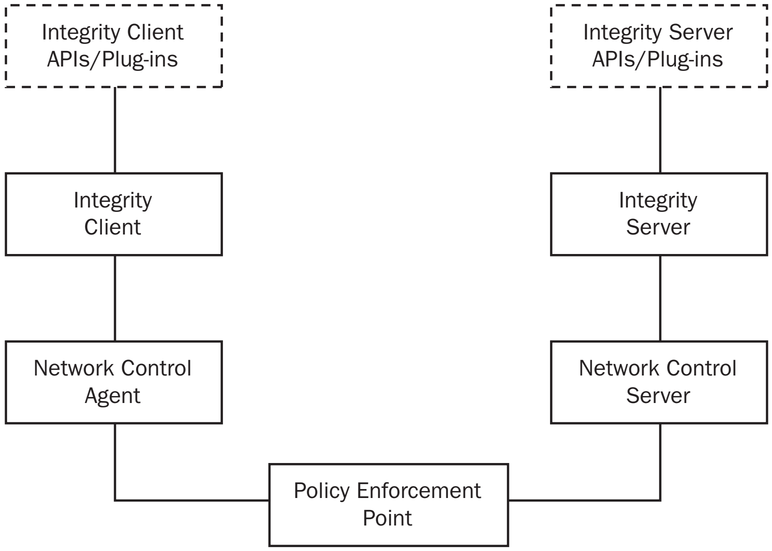

Figure 1 – Typical Network Access Control Architecture & Components

The TNC standards-based open architecture follows a similar pattern. In a TNC-based solution, the client side employs an Integrity Client known as a TNC Client. The TNC Client interfaces with plug-in Integrity Measurement Collectors, or IMCs, which collect status reports on the security of the client device and the state of the security and other software on the device. The TNC Client also interfaces with a Network Access Requestor which manages the underlying network access request protocol (802.1X, IPsec, TLS/SSL, DHCP).

On the server side, a TNC Server acts as an Integrity Server. It interfaces with plug-in Integrity Measurement Verifiers, or IMVs, which evaluate the endpoint's security based on the measurements received from the IMCs and the pre-determined or dynamically applied security policies established by the organization. The TNC Server also interfaces with a Network Access Authority, typically an AAA/RADIUS server, which implements the TNC Server's access control decision and allows or denies endpoint access to the protected network depending on compliance with network security policies.

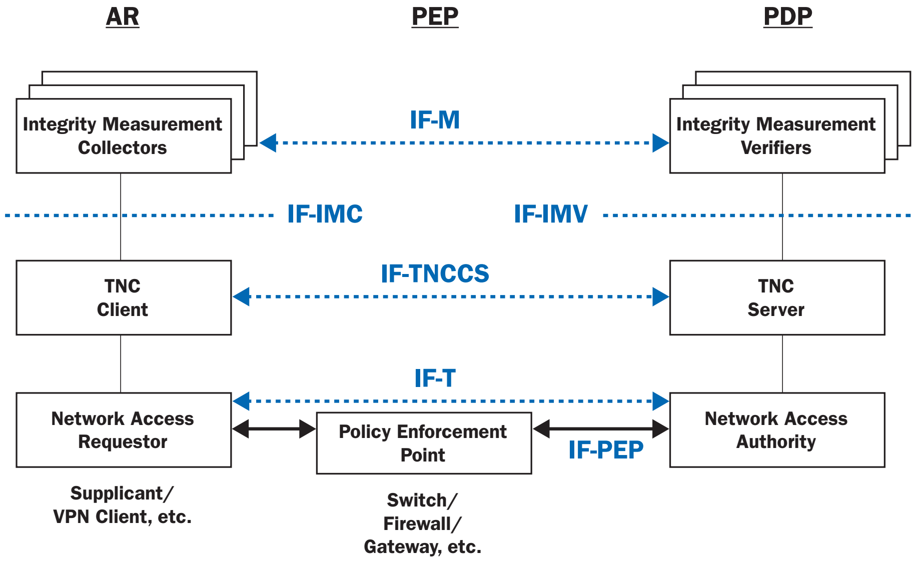

Figure 2 – Trusted Network Connect (TNC) Network Access Control Architecture & Components

The TNC open architecture also provides a solid roadmap for future access control by providing optional support for another TCG standard component, the Trusted Platform Module (TPM). The TPM is a hardware module embedded in a device that enables remote verification of the device's hardware and software integrity. While not a required component of the TNC, by integrating the standards-based TNC architecture with a TPM, the integrity of the endpoint can be established in a more trustworthy manner, immune to any malicious software.

With a way to integrate and address industry standards in hand, and a standards-based, open architecture defined, all that enterprises need is a solution from a trusted, respected industry leader that ties standards and open architecture together, and delivers an endpoint integrity and access control solution for use in mixed, heterogeneous network environments that protects an entire enterprise network and the disparate user devices attempting access. All of this and more is available from Juniper Networks through its Unified Access Control (UAC) solution.

Juniper Networks' Unified Access Control (UAC)

Unified Access Control (UAC) is a comprehensive network access control solution that combines powerful, standards-based user authentication and authorization, identity-based policy control and management, and endpoint security and intelligence to extend access control across the enterprise network.

By incorporating industry standards with well established, industry tested and accepted network and security products, Juniper Networks' UAC solution provides organizations with secure policy compliance, both prior to granting network access and throughout the session lifetime of a user's access to enterprise networks and resources. This approach helps organizations achieve comprehensive, uniform security policy compliance and works very effectively to defeat ever present network threats.

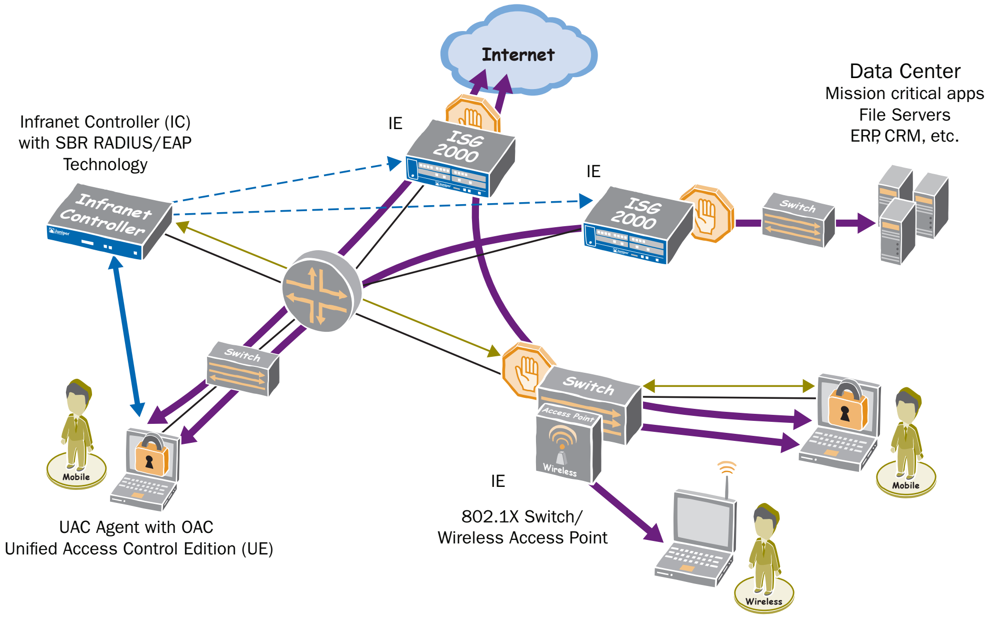

Figure 3 – Juniper's Unified Access Control (UAC) version 2.0

UAC & TNC

Juniper's next version of its Unified Access Control (UAC) network access control solution, version 2.0, enables standards-based secure access control within enterprise LANs. UAC version 2.0 supports the Trusted Network Connect (TNC) open specifications for standards-based application enforcement of security requirements for endpoint devices attempting enterprise network connection.

By supporting the TNC's open architecture specifications, UAC enables organizations to leverage their existing investment in heterogeneous network devices and software. UAC's support of the standards-based TNC network access control architecture specifications further simplifies its ability to be dropped into an existing network environment, securing network and devices quickly and cost effectively, giving the deploying company maximum flexibility and a very high Return-on-Investment (ROI).

UAC further extends its endpoint assessment capabilities by incorporating TNC-conformant antivirus, compliance management, and patch management solutions into its endpoint integrity framework. It also provides support for generic third-party developed TNC security solutions to be easily integrated within the UAC solution's framework. And UAC extends its host checking capabilities to support TNC compliant endpoint device assessment checks for media access control (MAC) addresses and for NetBios systems.

Organizations are now able to implement standards-based access control in a flexible, cost effective manner by exploiting UAC's support for different types of policy enforcement elements and its ability to secure access without incurring expensive network upgrades, or requiring massive software or firmware updates to their network infrastructure.

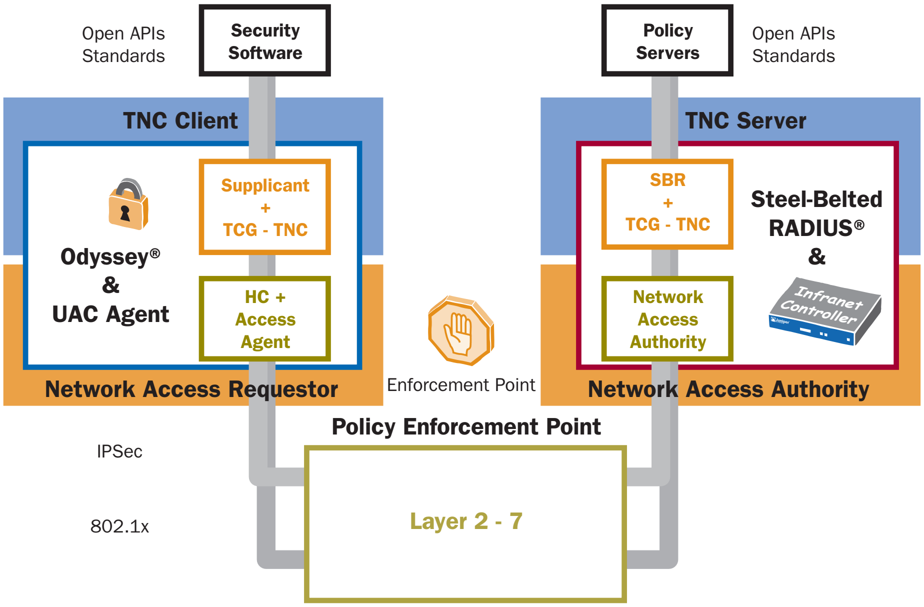

Figure 4 – Juniper's Unified Access Control (UAC) version 2.0 on the TNC Architecture

Juniper's UAC version 2.0 solution provides comprehensive network and endpoint security from network Layer 2 through Layer 7. It is quick and easy to deploy in stable existing networks and flexible for simple deployment on evolving network environments. Because UAC is a standards-based solution that uses and supports the TNC open specifications and industry standards for network access control and endpoint integrity, it ensures multi-vendor interoperability and compatibility, and it offers organizations the ability to choose their network appliances and components and avoid the pitfalls of potentially expensive, restrictive vendor lock-in.

Summary

The pros and cons of proprietary access control solutions should convince organizations to steer clear of solutions that are proprietary or "proprietary standards", and toward solutions based on open standards. Network access control solutions based on standards provide organizations with easy deployment, interoperability, high ROI, and choice. They give organizations the opportunity to select the network infrastructure and software that best meet and adapt to their ever-changing networking needs without fear of constraint or vendor lock-in. The Trusted Network Connect (TNC) network access control standard architectural specifications are published, open, and available online to any vendor, and this provides a superior level of security and assurance.

Incorporating robust, industry tested standards such as 802.1X, RADIUS, and EAP into its open architecture specifications, the TNC offers the highest level of protection required for today's fast paced market, as does Juniper Networks through its adoption and use of the open, standard TNC specifications in its Unified Access Control (UAC) solution.

By using the standards-based TNC architecture as one of its pillars, Juniper Networks' Unified Access Control (UAC) empowers organizations to implement access control in a flexible and cost effective manner within their enterprise LANs. By exploiting UAC's support for various types of policy enforcement elements, and relying on its ability to secure access without requiring expensive network overhauls or complete firmware or software upgrades to network infrastructure, UAC enables organizations to leverage their existing investments in diverse network devices and software for access control. UAC's open, standards-based approach via the TNC architecture and its incorporation of existing industry standards such as 802.1X give organizations vendor-neutral interoperability and provide choice where organizations in the past were limited to use of proprietary solutions. With Juniper Networks' Unified Access Control solution, an organization is free to choose whichever best-of-breed network components and software best suits their business and this represents significant benefits in terms of flexibility, cost, and value.