TECHNOLOGY FEATURE

NEW STANDARD LAYS THE FOUNDATION FOR COORDINATED, MULTI-VENDOR SECURITY

From Ethernet to HTML, standardization of IT technologies has ultimately led to more choice, greater system interoperability, and lower costs for enterprises. The security market is no exception. Later this year, leading vendors will begin delivering products that support a new security standard that opens the door to powerful, multi-vendor defense-in-depth solutions.

Developed by Trusted Computing Group and dubbed the Interface for Metadata Access Point (IF-MAP), this new standard allows for the dynamic interchange of data among a wide range of networking and security devices. With IF-MAP, systems can share real-time data about policies, status, and behavior for continuous policy decision-making and enforcement based on an endpoint's security state.

As a result, enterprises can implement a multi-vendor security system that delivers coordinated defense-in-depth. IF-MAP gives enterprises greater vendor choice and the flexibility to leverage their investments in existing network and security infrastructure. In addition, IF-MAP enables more robust security by supporting real-time threat response and granular identity-based controls, resulting in less downtime and data loss. And IT will find it easier to define security policies, troubleshoot incidents, and generate compliance reports, reducing operations overhead.

Beyond network access control

IF-MAP builds on and significantly extends the benefits of existing security standards, such as those defined for network access control (NAC). Widespread vendor support for NAC standards, for example, has made it possible for enterprises to combine LAN switches, identity management, and host posture check software from multiple vendors into a solution that best aligns with their needs and budget. Key among NAC standards are the Trusted Computing Group's Trusted Network Connect (TNC) architecture for endpoint security and IEEE 802.1X, which provides port-based access control for wired and wireless networks.

NAC is crucial in protecting corporate assets from unauthorized users and preventing infected devices from connecting to the network. But, like a moat around a castle, NAC is only one piece of a defense-in-depth strategy; it's of little help if a spy slips inside the castle walls or an attacker comes equipped with a trebuchet and long ladders.

IT must contend with a complex security landscape characterized by increasingly sophisticated attacks, regulatory requirements, a proliferation of new and unmanaged network devices, and an increasingly diverse and mobile workforce. Enterprises not only need to control what users do once they're admitted to the network, but also to identify, mitigate, and report on any suspicious activity. The ultimate goal is a security solution that coordinates defenses across the network in real time.

To date, security systems—firewalls, intrusion detection and prevention systems (IDP/IPS), data leakage prevention (DLP), and others—have operated as silos. Except for a few vendor-proprietary implementations, these security platforms have lacked the ability to communicate with one another to coordinate a meaningful threat response.

With the new IF-MAP protocol and extensions to the TNC architecture that

the Trusted Computing Group has defined, enterprises can build a dynamic, multi-vendor defense-in-depth solution.

Groundwork in place: TNC architecture

IF-MAP fits into the TNC architecture, which allows network administrators to audit endpoint configurations and impose enterprise security policies before a network connection is established. In addition, TNC supports access control based on identity, ensuring that only authenticated, authorized systems and users gain access to specific areas of the network based on their locus of responsibility.

TNC architecture enables enterprises to enforce access control policies in a multi-vendor IT environment. Among the functions supported by TNC are: collecting endpoint configuration data; comparing these data against policies set by IT; and

CONTINUED ON PAGE 10

JUNIPER NETWORKS ADAPTIVE THREAT MANAGEMENT SOLUTIONS

SOLUTION-BASED SECURITY THAT WORKS BETTER BECAUSE IT WORKS TOGETHER

From branch office to headquarter locations, Juniper Networks Adaptive Threat Management Solutions reduce security risks through a cooperative security approach. All deployed security elements work together to identify, mitigate, and report on highly sophisticated attacks that evade point security products. An open security architecture provides real-time threat defense with best-in-class, network-wide visibility and control that address security and compliance issues.

Standards-based interoperability allows a shared and open view of network activity—even in a multi-vendor environment. These same standards afford enterprises and service providers the freedom to integrate Juniper Networks devices into their existing infrastructure for a best-in-class approach that's right for their business.

With the introduction of TNC's Interface for Metadata Access Point (IF-MAP) protocol, Juniper once again leads the way in supporting standardized, dynamic data interchange among a variety of networking and security components. IF-MAP support is offered with Unified Access Control (UAC) 3.0 and SA Series SSL VPN appliances version 6.4.

Dual deployment yields unmatched benefits

As integral components of Adaptive Threat Management Solutions, the SA Series SSL VPN appliances, and UAC provide the industry's only coordinated, standards-based, enterprise-wide access control solution. They work in unison to consistently enforce global policies, both locally and remotely, for any user or role—from employees to contractors, partners, offshore workers, and guests. This uniform enforcement reduces the need for IT staff intervention while ensuring real-time security and regulatory compliance.

Coordinated access control also empowers enterprises to get employees online and boost productivity significantly faster than alternative solutions. Employees can gain access with a single, global login, which reduces frustration while minimizing help desk calls and simplifying IT administration.

Additionally, Juniper Networks SA Series and UAC allow for cost-effective growth and the ability to scale access control to tens of thousands of devices and users. They employ a pay-as-you-grow license model, so once the infrastructure is in place, companies can purchase additional licenses on an as-needed basis.

SA Series SSL VPN Appliances—anytime, anywhere access

These market-leading appliances offer secure, remote access solutions for organizations of every size. Using SSL transport, the appliances permit any Web-enabled devices—laptops, PDAs, smartphones, or kiosks—to securely access an organization's resources. SSL eliminates the cost and complexity of installing, configuring, and maintaining client software on each device. What sets the SA Series apart is the ability of these appliances to insist upon a number of preconditions, protecting the network from outside threats common with remote access.

UAC—dynamic, standards-based access control

Juniper Networks UAC combines the best of access control and security technologies, while leveraging existing network investments. It delivers different levels of session-specific policy for extremely robust access control and security policies that are easy to deploy, maintain, and modify. UAC is composed of a centralized, hardened policy management server, a UAC Agent for collecting user credentials and checking endpoint compliance and posture, and UAC enforcement points that can include any 802.1X-compatible access point or switch, or Juniper firewall platform. UAC can enforce access and security policy at Layer 2 using 802.1X, at Layer 3 using an overlay deployment, or at both layers for more granular access control.

For more information about Juniper Networks Adaptive Threat Management Solutions, visit **www.juniper.net/adapt**

IC4500

The IC4500 Unified Access Control Appliance is a next-generation hardened, centralized policy management server delivering superior scalability and performance for mid- to large-size organizations and remote or branch offices.

providing an appropriate level of network access based on level of policy compliance and job function (which may include instructions on how to remediate clients in case of compliance failure).

But the Trusted Computing Group recognized that endpoint admission control is only part of an overall security solution. Consequently, the group expanded the TNC model and defined the IF-MAP protocol to address a major shortcoming in enterprise security—the inability of security devices to share their understanding of network and device capabilities and behavior. Without this "big picture" view, coordinated defense-in-depth isn't possible.

IF-MAP describes a database service and powerful protocol whose publish, subscribe, search, and poll functions enable systems to share data about one another in real time, including policies, status, and behavior information. These additions to TNC architecture give IT a level of visibility into, and control over, network activity that has been out of reach in multi-vendor environments.

Moving beyond NAC, IF-MAP provides a standard way to integrate virtually any security device into TNC architecture. Consequently, a wide range of systems are supported under IF-MAP, including IDP/IPS, DLP, firewalls, DHCP servers, and NAC components such as AAA servers. Let's quickly review TNC architecture before diving into the details of how IF-MAP works.

TNC architecture overview

TNC architecture defines three entities: access requestor (AR), policy enforcement point (PEP), and policy decision point (PDP) (*see Figure 1*). AR is a client or other endpoint, such as a laptop, VPN client, or Web browser initiating an SSL connection; in 802.1X parlance, it would be the 802.1X supplicant. AR includes both client hardware and any software and drivers that implement functions such as authentication and endpoint security assessment (also known as host posture check).

PEP is any device or system, such as a switch, firewall, or VPN gateway, that performs an enforcement action; for example, blocking network access or redirecting a noncompliant client to a remediation server. PEP also controls which level of access an endpoint is granted.

PDP is typically a policy server or other management system that IT uses to define and distribute policies to PEPs. Another function of PDP is to communicate with the authentication server and to pass verification information to ARs.

Building out with IF-MAP extensions

IF-MAP extends the TNC architecture with two additional entities: "metadata" access points, which are network and security devices that support the IF-MAP protocol, and a database server referred to as the MAP server (*see Figure 2*). This database stores information about network security events and objects, including users and devices, as well as relationships among them.

Devices and applications that support IF-MAP can publish information, or "metadata," to the MAP server as well as subscribe to those data. Metadata are an extensible part of the specification, so vendors can extend the metadata schema to encompass application- and vendor-specific characteristics. The standard defines an initial set of metadata that includes device attributes, authentication information, MAC-to-IP address bindings, and Layer 2 location information, such as switch addresses and VLAN and port numbers.

In addition, the IF-MAP standard defines how information about security events can be published to the MAP server. Likewise, information about privileges and access rights granted to users and devices can be

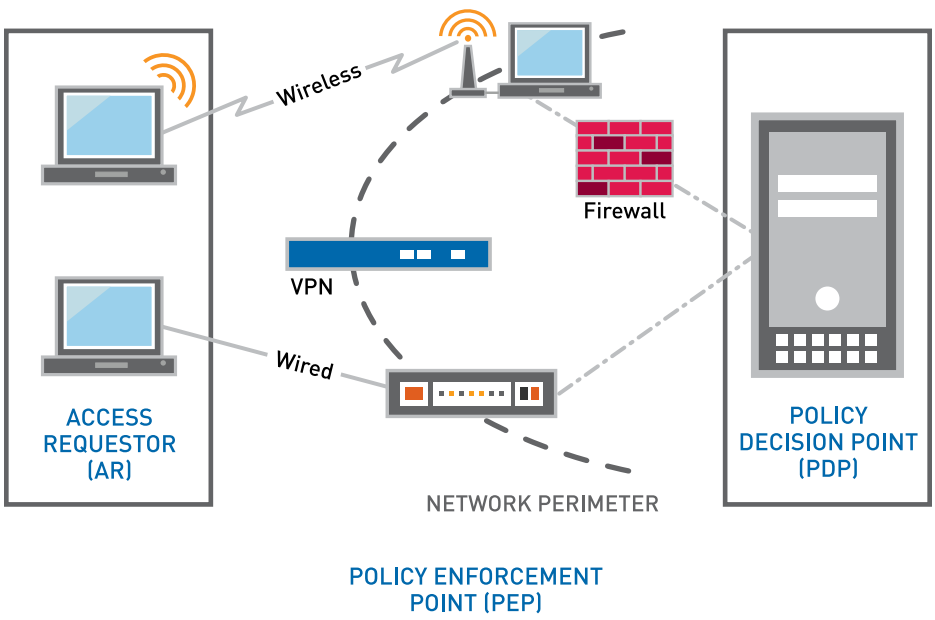

Figure 1: TNC Architecture—from *TNC: Open Standards for Network Access Control*

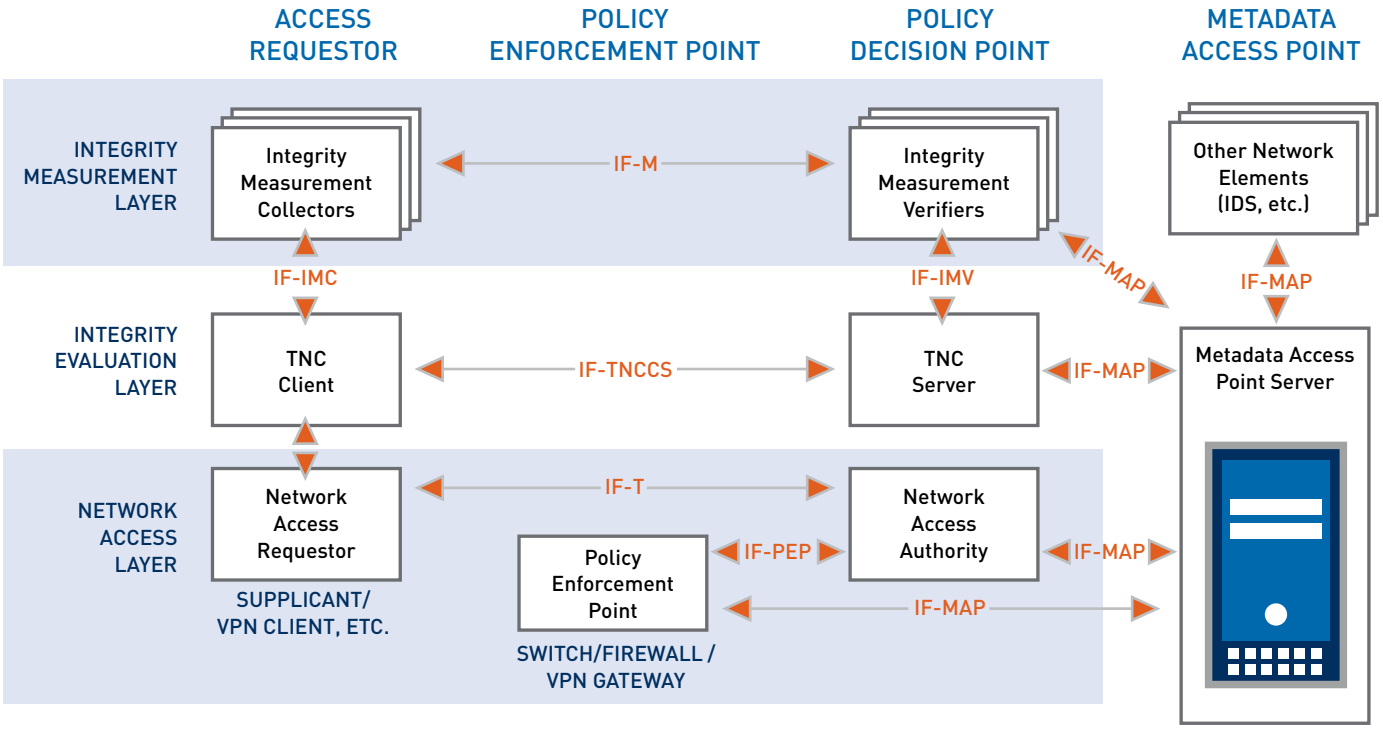

Figure 2: IF-MAP—from *Making NAC Security-Aware with IF-MAP*

published to the MAP server, along with access request information that identifies who is attempting to log into a given system or resource.

The Trusted Computing Group directed TNC to use existing industry standards, such as the Extensible Authentication Protocol (EAP), Transport Layer Security (TLS), and RADIUS, so IF-MAP inherits these characteristics. In addition, TNC architecture operates on top of all commonly used access methods, including VPN-based and dial-up remote access, wireless networks, 802.1X infrastructures, and traditional LAN technologies. For more information about IF-MAP and TNC architecture, see **www.trustedcomputinggroup.org**

IF-MAP in action

By giving network and security systems the ability to share everything from location and address information to state changes, IF-MAP fundamentally changes the way security can be implemented. Security policies can be applied more granularly, based on users and groups, with assessment and control adjusted continuously in response to conditions on the network.

For example, applications such as a security event manager or policy server can query the IF-MAP database for the association among MAC addresses, IP addresses, user names published by the authentication server, and hostnames in the DNS server. Being able to track activity by user and hostname, rather than by IP and MAC addresses, simplifies policy creation, compliance tracking, and troubleshooting. As a result, IT can more easily restrict and monitor access to credit card processing systems; allow the engineering group, but no other users, to run BitTorrent; and pinpoint which user attempted unauthorized access to the finance server.

A major plus for IT is that the IF-MAP database is automatically populated by IF-MAP clients. For example, a NAC system can instantly update the database with information about users who have logged onto the network, the types of endpoints they're using, and the security status of those endpoints.

IF-MAP allows for synergies among security platforms that to date were possible only with single-vendor solutions, if at all. For example, a firewall that has subscribed to information about endpoints can pick up an alert published by an IDS about anomalous traffic coming from a particular endpoint. Based on the policies in place, the firewall could automatically block that traffic and/or trigger the NAC system to quarantine the user.

Several leading vendors active in the trusted computing group have already begun shipping products that include IF-MAP server and client support.

Because IF-MAP is implemented in software, enterprises may need only a software upgrade from their security vendors to begin taking advantage of the continuous post-admission assessment and control that IF-MAP enables.

Choice and expanded security options

The Trusted Computing Group's focus on defining standards for heterogeneous networking environments yields numerous financial and security benefits for enterprises. By implementing systems that support IF-MAP, enterprises can expect:

Greater choice and flexibility

- Enterprises can use their favorite virus scanning software, firewalls, and other security and networking gear with the assurance that they'll work together. Because IF-MAP is implemented in software, enterprises have the opportunity to leverage their existing equipment, eliminating the need to rip and replace gear to get advanced security capabilities.
- Enterprises have the flexibility to buy pieces of a defense-in-depth solution as needs arise and budgets allow, leading to lower initial costs.
- Standards tend to drive competition; enterprises get sophisticated functionality at a reasonable cost because they can avoid vendor lock-in.

Stronger security, less disruption

- Building on TNC standards, IF-MAP enables a coordinated security response across products from multiple vendors, including AAA, NAC, IDP/IPS, DLP, firewalls, and other security and network systems.
- IF-MAP will allow enterprises to build a defense-in-depth solution capable of continuous policy decision-making and enforcement based on the real-time information, which will accelerate security response time.
- Stronger security will reduce data loss, compliance violations, and downtime, whether these result from accidental or malicious action or malware infection.
- IF-MAP makes it much easier for enterprises to implement identity-based security across their networks. The network is better protected because access controls can be more finely tuned to individual users and groups and then modified based on the information shared among network and security devices.

Streamlined management and lower operations costs

- IF-MAP will lower operations costs by automating threat response and reducing the need for human intervention.
- Because policies can be tied to user identity and role instead of IP addresses, IT will find policy definition more intuitive, resulting in more robust policies and fewer mistakes.
- IT will benefit from more comprehensible incident reports from firewalls and other devices since these will be able to include user identity information. As a result, troubleshooting will be streamlined, which boosts system uptime and user productivity.
- IF-MAP also will make it easier for security event management (SEM) and other reporting/logging systems to integrate data from multiple vendors' devices. IT will be able to get a more accurate "big picture" of network activity than is currently possible, including data necessary for compliance reporting.

Delivering on the promise

As one IT director noted, IF-MAP represents a revolution in security functionality, not just an evolution. IF-MAP has the potential to deliver powerful new security capabilities, streamline IT's job, and give enterprises greater flexibility in building a defense-in-depth solution.

As with any standard, it will take time for IF-MAP support to become ubiquitous. Enterprises can help drive adoption of IF-MAP—and their own deployment of dynamic, cooperative defense-in-depth solutions—by purchasing products that implement it and demanding that security and networking vendors support it. Enterprises that begin planning for IF-MAP now will be well positioned to reap its benefits as additional products come to market. VEER

For more information about securing your network, view a cyber crime Webcast at **www.juniper.net/us/en/dm/secure**