TNC and SCAP: an Integrated Solution for Automating Security

September 2010

Trusted Computing Group
3855 SW 153rd Drive, Beaverton, OR 97006
Tel (503) 619-0562 | Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

TNC and SCAP: an Integrated Solution for Automating Security

Detecting and thwarting the threats and vulnerabilities of today's computer systems and networks have challenged technical professionals from numerous companies and government organizations. Today, a combination of standards-based techniques has brought a new level of security and trust to interconnected computing devices and the networks that connect them. Working together, the National Institute of Standards and Technology (NIST) and the Trusted Computing Group (TCG) have integrated the Security Content Automation Protocol (SCAP) developed by NIST and Trusted Network Connect (TNC) standards developed by TCG to provide a powerful combination of automated compliance management and network access and enforcement. Automating and integrating security management with these standards reduces expensive manual intervention and frees security experts to focus on other more complex information security issues.

The SCAP Standards

NIST's SCAP was created as a community effort to create a common set of standards to help express and automate configuration management. The SCAP standards provide a common language for organizations to perform continuous monitoring and assessment of the endpoint population in regards to compliance with required configurations and the existence of known vulnerabilities for the ultimate purpose of minimizing the attack surface of each endpoint. SCAP provides a common language to express standards as well as a common language for evaluating and scoring the compliance with those standards.

Organizations can apply a variety of tools that are SCAP validated by NIST as conforming to the SCAP standards for specific capabilities. Today, over 39 products have at least one form of NIST SCAP validation. SCAP content is also available to the community in the form of security checklists and reference data. Reference data (or benchmarks) provide detailed low-level guidance on setting the security configuration of operating systems and applications. SCAP reference data available from multiple sources including a dictionary of Common Platform Enumeration (CPE) entries, information on Common Vulnerabilities and Exposures (CVE) entries, an Open Vulnerability and Assessment Language (OVAL) database and Common Configuration Enumeration (CCE) entries.

A well-known and broadly applied implementation of the SCAP standards is the Federal Desktop Core Configuration (FDCC). A 2007 Office of Management and Budget (OMB) memo established SCAP as a required standard for measuring compliance for FDCC compliance. NIST certifies tools for the specific role as a FDCC Scanning to audit and assess endpoint systems as compliant with FDCC requirements as expressed in the SCAP standards. The specific configuration requirements in FDCC are expressed using CCE identifiers so organizations can track and document their compliance. Other broadly applied security mandates such as the Federal Information Security Management Act (FISMA) are now being expressed in SCAP.

SCAP gathers hundreds of endpoint configuration items that provide ongoing monitoring of the configuration and compliance health of any organization. Some tools also provide remediation capabilities to return non-compliant configuration settings back to the applied standard. SCAP also includes a Common Vulnerability Scoring System (CVSS) for identifying those machines that are found to have known software vulnerabilities that create known exploits that may be used to infiltrate a machine.

The TNC Architecture and Standards

TCG's TNC architecture integrates security products from different vendors using open standards. As illustrated in Figure 1, the architecture includes several components. The left three components form a classic Network Access Control (NAC) architecture. An Access Requestor (AR) requests access to a protected network. A Policy Decision Point (PDP) obtains information about the AR such as user identity and device health. The PDP then consults policies established by the network owner to decide what access should be granted to the AR, and sends instructions to a Policy Enforcement Point (PEP), which enforces the decision. If conditions change (e.g. the health of the AR improves or degrades), the PDP can send a revised decision to the PEP, increasing or decreasing the AR's network access.

The right two components add a novel capability: Coordinated Security. The PDP sends the information it has obtained to a database called a Metadata Access Point (MAP). Other security systems such as Sensors and Flow Controllers can use this information to improve their operations and share their own information and events with the PDP through the MAP, enabling many kinds of security automation.

Throughout the TNC architecture, open standards are used to connect the different components. This allows products from different vendors to work together easily, leveraging each other's strengths and forming a system that is much more capable than any one component alone. For example, an Intrusion Detection System (IDS) can act as a Sensor, detecting attacks on the network. When the IDS detects an attack, it can publish an event to the MAP. The PDP will be notified immediately if the attack pertains to an AR for which it is responsible. Appropriate action can be taken automatically, such as blocking the attack at its source.

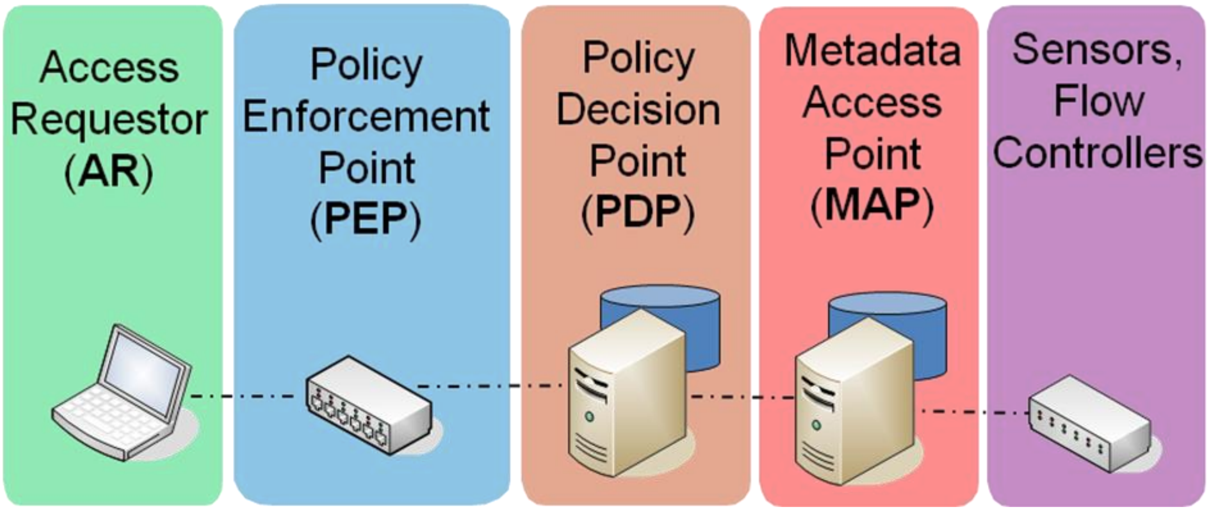
Access Requestor (AR)
Policy Enforcement Point (PEP)
Policy Decision Point (PDP)
Metadata Access Point (MAP)
Sensors, Flow Controllers

Figure 1. The TNC Architecture

Due to space constraints, this is only a very brief outline of the TNC architecture. None of the TNC standards has been identified and few of the benefits of the TNC architecture and standards have been described. For a more complete description, review the other materials available on the TCG web site (http://www.trustedcomputinggroup.org). However, this outline provides the necessary basis for the next section, which describes how the SCAP standards have been integrated into the TNC architecture.

SCAP + TNC = Stronger Security and More Automation

With SCAP's standards for device security management and TNC's complementary set of network capabilities, users can easily achieve a level of security that was very difficult, expensive or impossible to deliver previously.

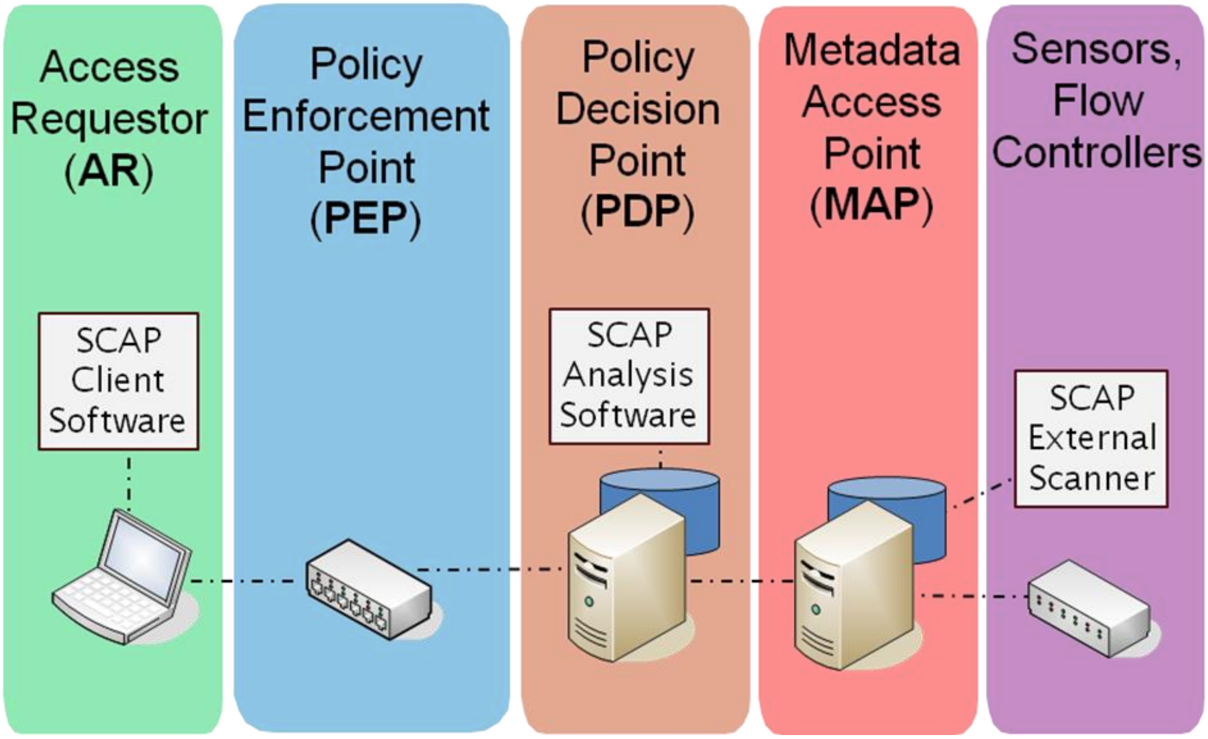
Access Requestor (AR)
Policy Enforcement Point (PEP)
Policy Decision Point (PDP)
Metadata Access Point (MAP)
Sensors, Flow Controllers
SCAP Client Software
SCAP Analysis Software
SCAP External Scanner

Figure 2. TNC and SCAP Together

As seen in Figure 2, existing SCAP products fit easily into the TNC architecture. First of all, SCAP-validated scanners reside on Access Requestors. They can plug into the TNC architecture through the IF-IMC standard. Secondly, SCAP-validated scanner analysis and management components can be connected on the PDP using the TNC's IF-IMV standard. These standards were designed for adding new device checks to the TNC architecture. Finally, external SCAP scanners can function as Sensors, sharing data and alerts about device configuration through the MAP using the TNC's IF-MAP standard. At all three of these interface locations, SCAP provides the user the capability to know what is running on a machine as well as its compliance with required checklists and SCAP-based enterprise policies. TNC adds the capability to automatically perform enforcement based on identity and other criteria as well as the framework to integrate all these different sensors. In short, TNC handles the networking and network integration and SCAP handles the compliance aspects.

Towards Increasingly Trustworthy Computing

Vendors have already demonstrated the ease of implementing SCAP with TNC and customers are deploying this integration, at least in pilots. However, this is just the beginning of the benefits of integrating the NIST and TCG open standards efforts. With the success of this initial collaboration, NIST and TCG will continue to expand the capabilities of SCAP and TNC technologies. This will occur within each organization as before and explore areas for integrating the standards to achieve an even more secure, automated computing and network environment.