INTEROP LABS

6 in a Series

Making NAC Security-Aware with IF-MAP

At Interop Las Vegas 2008, the Trusted Computing Group introduced a new protocol, IF-MAP. The IF-MAP protocol creates a structured way to store, correlate, and retrieve identity, access control, and security posture information about users and devices on a network. Products that implement this new protocol can become more network and security-aware, in a standardized and interoperable way. IF-MAP can be used to solve many architectural problems with current NAC solutions, and offers applicability far beyond the world of NAC.

The Background for IF-MAP

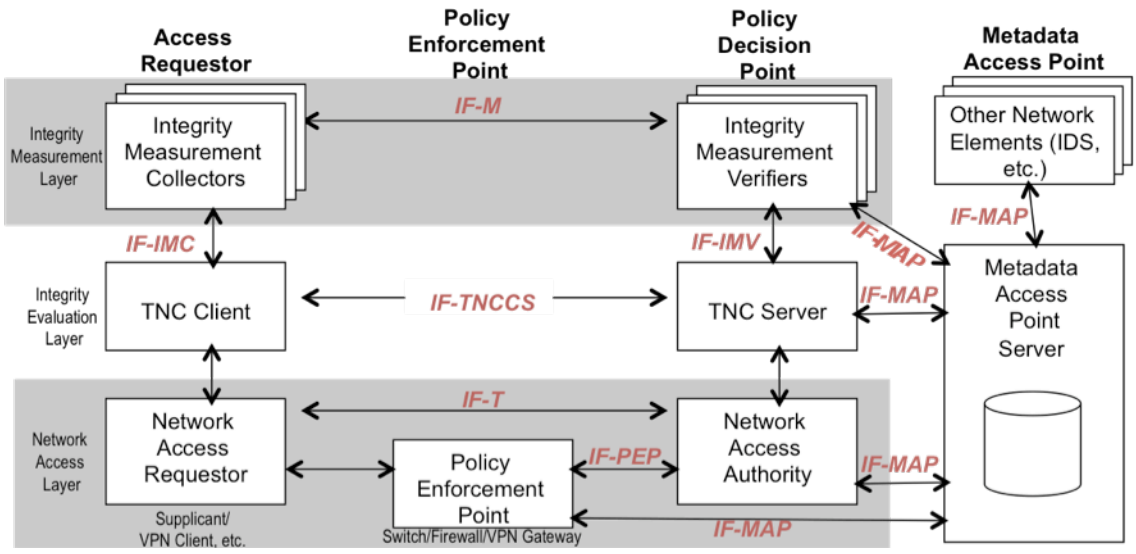
A long-standing difficulty in network security has been the collection, correlation, and searchability of bits of information about users of the network. Many enterprises have tools, ranging from DHCP servers to firewalls to authentication servers to malware scanners, and all of these tools have bits of information about a user or an end-point. However, no single tool usually has the "big picture," an ability to say that a particular MAC address is on some port of some switch with an IP address, an authenticated identity (and access controls) and an end-point security posture. Tools such as Security Information Management products (SIMs/SEMs) have started to make inroads in collecting and correlating the data, but this is generally a new area for network and security products.

The goal of IF-MAP is to create that big picture. IF-MAP collects bits of information from all over the network and links it all together into one single searchable database. A big picture view of systems and security would be an invaluable asset in helping to intelligently apply security policies and proactively protect the network. NAC definitely isn't the only area that could use that big picture---everything and everyone from Intrusion Prevention Systems to firewalls to security auditors and help desks could benefit from greater visibility into the network.

What is IF-MAP?

IF-MAP describes a database service that contains information (metadata) about systems and users currently connected to a network. IF-MAP uses a publish/subscribe model, where all of the network and security applications can participate in updating, and querying, the service (called an IF-MAP server).

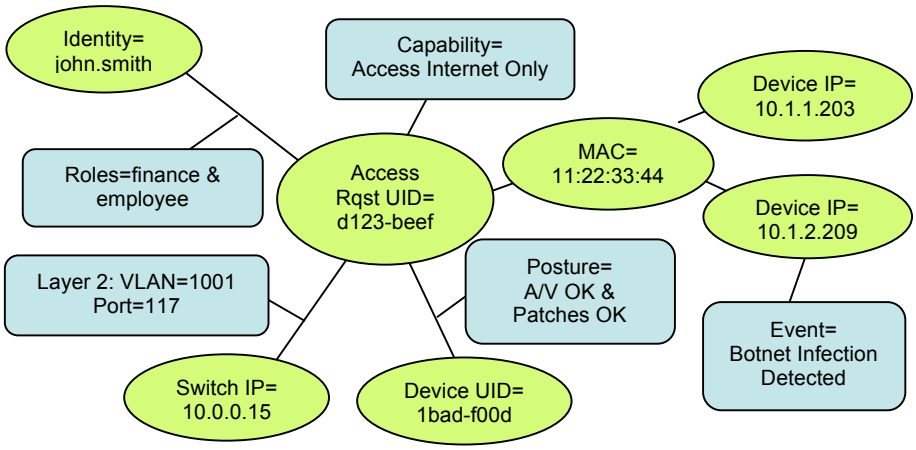
The publish side is pretty straightforward. For example, network applications can publish information to the IF-MAP server about any system connecting to the network, such as a mapping between MAC addresses, IP addresses, and user authentication information. Security applications, like a NAC posture checker, can publish information about the state of end-point security of the system. And other, non-NAC pieces of the network, like Intrusion Detection Systems (IDSes) and vulnerability checkers, can also publish information about systems on the network. The data model in IF-MAP doesn't require that the publisher know exactly what device or user they're talking about. Bits of information can be published to an IF-MAP server with whatever identifying information is available: a MAC address, an IP address, even a port on a switch, and the IF-MAP server stores the information in one large interconnected graph.



The interesting part comes on the subscribe side. Here, a piece of a NAC solution (such as a Policy Decision Point or a Policy Enforcement Point) can subscribe to the IF-

MAP server to learn information about a system as it happens, so that if the state of security of the end system changes, the policy of what that system can do and where it can go can also change.

IF-MAP also supports querying and searching for information with immediate results as an alternative to subscribing to information. The retrieval model (which is also used in the subscription part of the protocol) is very flexible. When specifying a search query, an IF-MAP client can start from any piece of metadata and search from there. For example, a search (or subscription) can ask for the user identity associated with a MAC address, or the end-point security posture associated with a particular port on a switch. The diagram to the right, gives an example of what a piece of the IF-MAP server's database might look like.



In other words, IF-MAP servers, publishers, and subscribers, provide a standards-based way to apply true continuous policy decision-making and enforcement based on the state of end-point security. If a system on the network suddenly starts behaving badly, as the IDS detects that and publishes the information, the NAC part of the network can learn about this and quarantine the user.

What does the IF-MAP Protocol Look Like?

IF-MAP itself is an XML-based protocol with four main operations:

publish, used to create, update, or delete information about a network element;
search, used to retrieve information (immediately) from the database about a network element;
subscribe, used to maintain a list of searches that the IF-MAP client wants to be notified about; and
poll, used by the IF-MAP client to say that they are ready to receive the results of a subscription.

On the wire, IF-MAP uses the SOAP (Simple Object Access Protocol) specification as defined by the W3C as an underlying encapsulation method, typically delivered over an HTTPS transport.

The metadata itself is an extensible part of the IF-MAP specification. While the initial IF-MAP protocol defines a small set of metadata bits of information, there is a clear direction on how the metadata schema can be extended with vendor-specific or application-specific metadata. The initial set of metadata about a network device includes:

Roles and Capabilities	Privileges or accesses granted to a user or device
IP-to-MAC binding	Mapping an IPv4 or IPv6 address to a MAC address
Layer-2 Location	VLAN and port numbers; switch addresses
Security Events	Examples include IDS alerts with a CVE number, botnet or worm infections, behavior or traffic changes, policy violations, or peer-to-peer traffic
Device Attributes	Information similar to what an IMV might provide, such as patch status or firewall policy information
Authentication Information	Who authenticated and how they were authenticated
Access Request information	Someone is trying to log in; what their MAC or IP are

What is the status of IF-MAP?

The IF-MAP protocol was just released, after about 18 months of development within the TCG/TNC. A number of NAC products have prototype implementations of IF-MAP in them, but these were not available in time to be part of the Interop Labs demonstrations. However, the TCG/TNC booth is showing demonstrations of IF-MAP in existing NAC products.