



Trusted Network Connect IF-MAP Announcement FAQ April 2008

Q. What is TCG announcing?

A. TCG is announcing a major addition to the Trusted Network Connect (TNC) architecture. The existing architecture (released in 2004) defined open standards for Network Access Control (NAC). TCG is now extending the TNC architecture by adding two new architectural components and a new standard protocol (IF-MAP). These additions extend the TNC architecture to support standardized, dynamic data interchange among a wide variety of networking and security components, enabling customers to implement multi-vendor systems that provide coordinated defense-in-depth.

Q. Why has TCG decided to extend the capabilities of TNC beyond typical NAC functions?

A. Today's security systems – such as firewalls, intrusion detection and prevention systems, endpoint security systems, data leak protection systems, etc. – operate as “silos” with little or no ability to “see” what other systems are seeing or to share their understanding of network and device behavior. This limits their ability to support coordinated defense-in-depth. In addition, current NAC solutions are focused mainly on controlling network access, and lack the ability to respond in real-time to post-admission changes in security posture or to provide visibility and access control enforcement for unmanaged endpoints. By extending TNC with IF-MAP, the TCG is providing a standard-based means to address these issues and thereby enable more powerful, flexible, open network security systems.

Q. What does IF-MAP include?

A. IF-MAP is a standard client/server protocol for accessing a Metadata Access Point (i.e. IF-MAP server). The IF-MAP server has a database for storing information about network security events and objects (users, devices, etc.). The IF-MAP protocol defines a powerful publish/subscribe/search mechanism and an extensible set of identifiers, and data types.

Q. What is “metadata”, anyway?

A. In the context of IF-MAP, “metadata” is any shared, real time data about network devices, policies, status, behavior and relationships between various systems (e.g. security events, network identity, and network location).

Q. What can people do with IF-MAP?

A. The IF-MAP 1.0 specification supports many use cases. The following are two examples:

- An intrusion detection system with an IF-MAP client publishes an alert to an IF-MAP server (“IP address 10.10.100.24 is sending anomalous traffic”); A firewall that subscribes to information involving 10.10.100.24 receives a notification from the IF-MAP server, triggering an automatic response
- A Security Event Manager (SEM) system queries an IF-MAP server to find the aggregate associations between the IP address and MAC published by the DHCP server, the user name published by the RADIUS server, and the hostname published by the DNS server.

Since IF-MAP is extensible, more use cases may be supported in the future.

Q. What are the benefits of IF-MAP for customers?

A. They can implement more effective, integrated security systems gaining the following benefits:

- Coordinated security response across multiple products from multiple vendors, spanning the range of products from endpoint security to AAA, NAC, IDS/IPS, Data Loss Prevention, firewalls, etc.
- Stronger security with lower operating costs since sensors (e.g. IDS) can be tied automatically into flow controllers (e.g. firewalls), reducing the need for human intervention and accelerating security responses.
- Fewer false alarms (and therefore lower operating costs) since sensors can tune their detection algorithms based on user and machine identity and role
- Customer choice and flexibility, leading to lower initial costs. No need to buy all security products from one vendor to get coordinated, integrated security
- Simpler, more intuitive policies based on user identity and role instead of IP address
- More comprehensible incident reports from sensors since they can include user identity
- Easier integration of data from multiple vendors and devices into security event management (SEM) and other logging and reporting systems.

Q. What are the benefits of IF-MAP for product vendors and resellers?

A. Using open standards to integrate security products provides many benefits over a single-vendor approach or custom integrations:

- Easily integrate products from multiple vendors (or all from one) to meet customer needs and build solutions
- Quickly respond to emerging threats by integrating products as needed
- Extensible schema allows for easy support for vendor-specific data

Q. How is IF-MAP different from other management protocols like SNMP and syslog?

A. IF-MAP provides an integrated, real-time view of security that allows products to work together in a coordinated manner to grant access as appropriate while identifying and responding to threats in real time. Existing network management protocols including syslog and SNMP are static. Each device reports events but the data is not integrated.

Still, syslog and SNMP can play a valuable role with IF-MAP if a Security Event Manager (SEM) or similar device is used to distill the information gathered with syslog and SNMP and feed it into the MAP database. Also, some flow controllers use SNMP to grant or restrict access.

Q. Does IF-MAP use any standard access protocol?

A. Yes, it is based on SOAP.

Q. How is IF-MAP secured?

A. As a critical component of the network security infrastructure, maintaining the security of IF-MAP is essential. Every IF-MAP request is encrypted and authenticated with the industry standard TLS (Transport Layer Security) protocol. Only authorized IF-MAP clients are allowed to access the MAP database and fine-grained access controls may be employed.

Q. What about privacy?

A. Metadata stored in a MAP database may include privacy-sensitive information such as user identity. However, this metadata is purely optional. Depending on regulations, customs, or contractual obligations, it may be necessary to omit some metadata or restrict access and is possible to do so.

Q. Is IF-MAP a required part of the TNC architecture?

A. No, it's optional. Customers can continue to use their existing TNC systems. If they want to add an IF-MAP server, they can do so at any time.

Q. Will IF-MAP implementations require a TPM?

A. As with other TNC specifications, this one can operate in an environment of clients with OR without TPMs. Clients with TPMs offer more security against attacks including rootkits.

Q. How does metadata get into the MAP database?

A. The database is automatically populated by IF-MAP clients. For example, a NAC server might add information about who has logged into the network, from which endpoint, and how healthy the endpoint is. An Intrusion Detection System or Data Leakage Prevention system might add information about that endpoint's behavior.

Q. Must there be hardware changes or upgrades to implement the new protocol?

A. No. IF-MAP can be enabled with a software update from vendors.

Q. Who has implemented these specifications?

A. As with all TCG specifications, IF-MAP is open for anyone to implement. Since the specifications have just been released, there are no shipping products yet. Arcsight, Aruba, Infoblox, Juniper Networks, Lumeta and nSolutions are demonstrating IF-MAP at Interop 2008. We anticipate that products and open source implementations will start appearing by early next year. Of course, IF-MAP is vendor-neutral. Multiple vendors will implement IF-MAP servers and clients.

Q. Will there be open source implementations of the IF-MAP specification?

A. We anticipate that as with other TNC specifications, there will be open source support. For example, the National Center for Data Mining at the University of Illinois at Chicago is implementing an open source IF-MAP stack for client and server implementations. A list of open source support for TCG is available at https://www.trustedcomputinggroup.org/groups/tpm/TCG_Open_Source_Resources_and_References_jan_08_updated.pdf