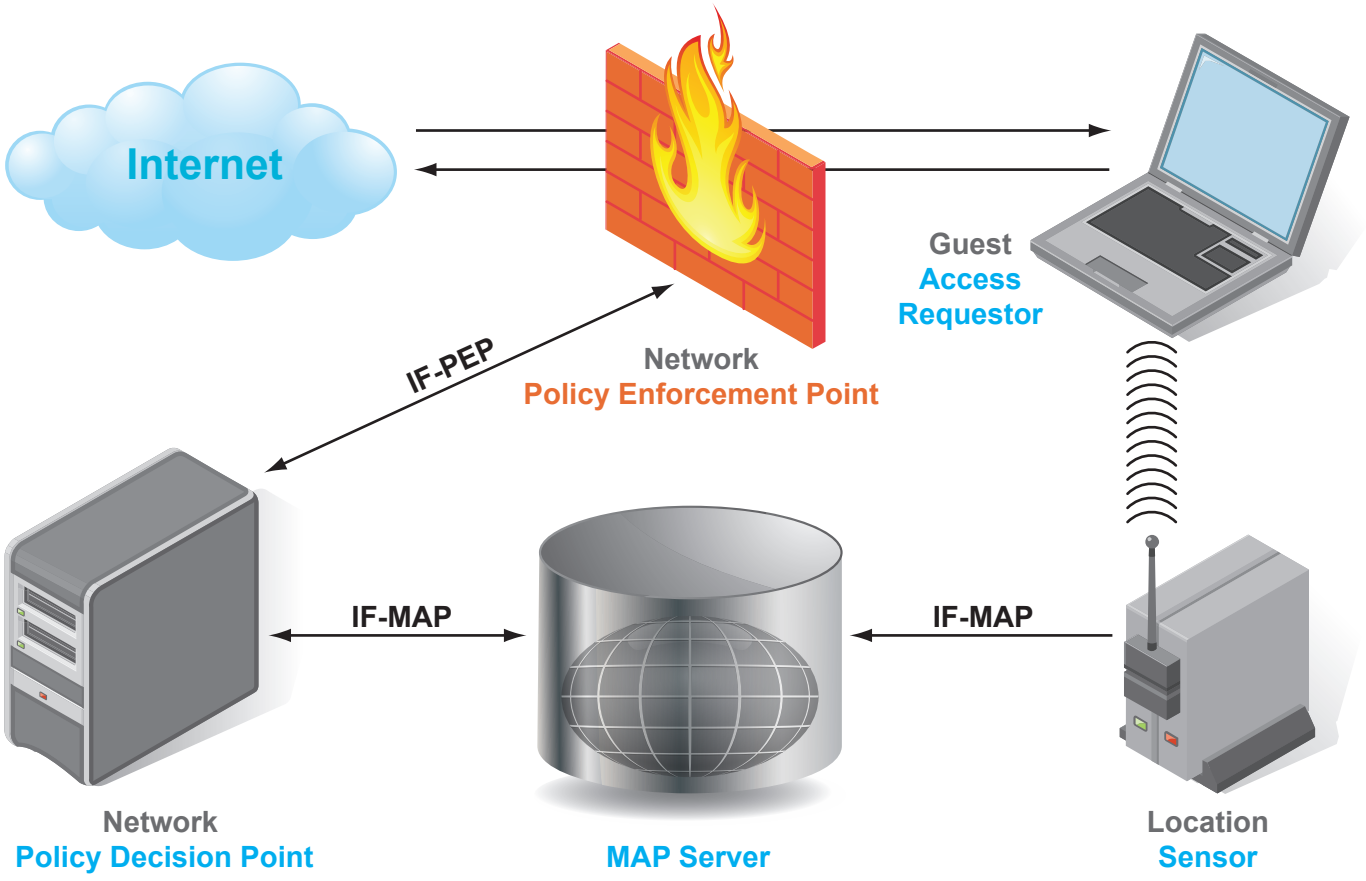
TRUSTED COMPUTING GROUP™

TNC EVERYWHERE

Pervasive Security

Conference Room / Guest Access

TNC interfaces enable dynamic differentiation and access control enforcement for a wide variety of users in mixed-use environments.



- IF-PEP enables provisioning of appropriate access for each user while ensuring consistent access control across wired and wireless connections.
- IF-TNCCS and IF-IMC / IMV enable endpoint integrity checking; implementations can range from a full supplicant to a lightweight dissolving agent.
- The CESP defines mechanisms that enable the application of access controls to endpoints without TNC clients that can't provide identity or endpoint health information.
- IF-MAP enables integration of network intelligence from additional security systems to add a behavioral consideration to the access decision.

enterasys® Secure Networks™

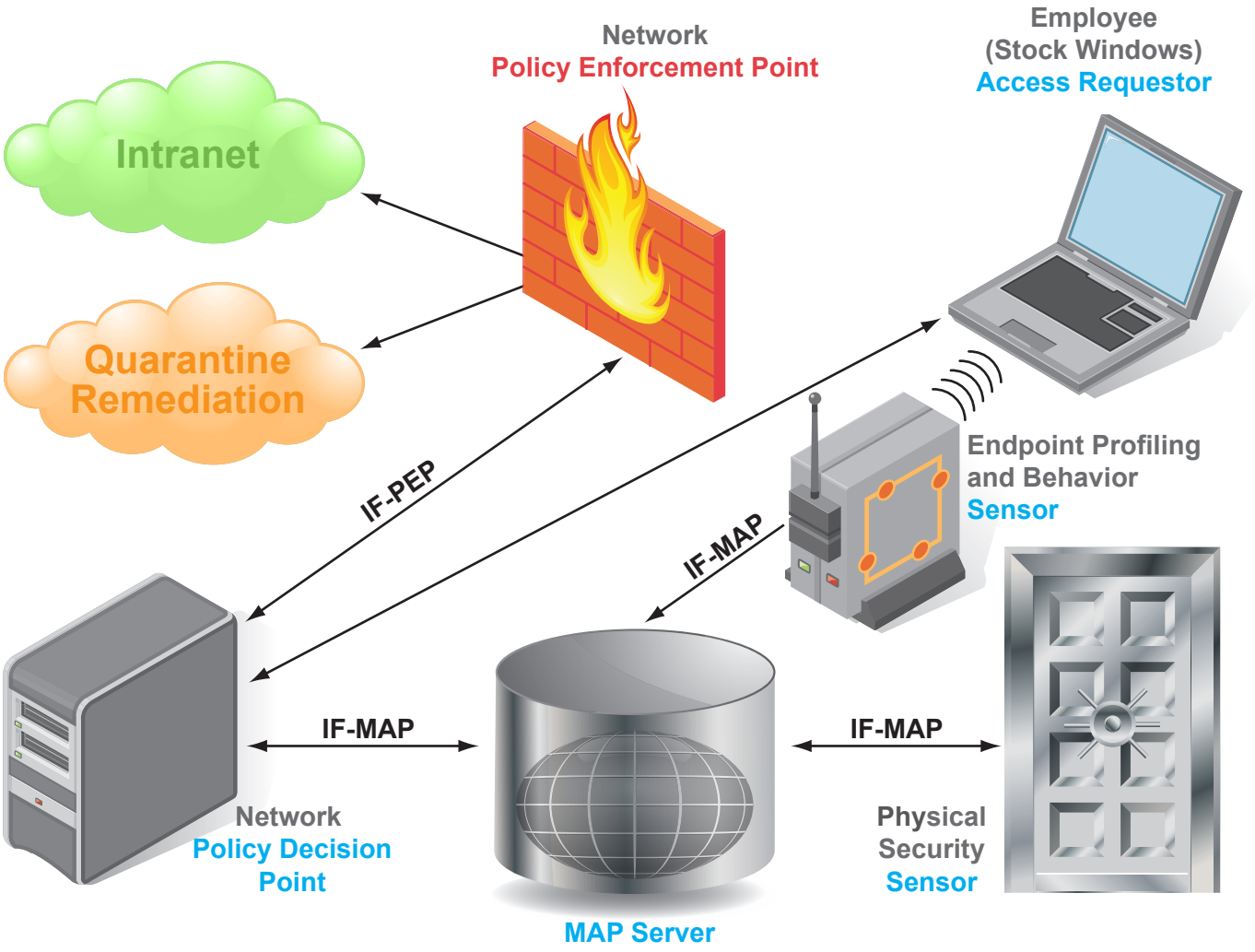
Infoblox®

Juniper® NETWORKS

TRAPEZE NETWORKS

Employee Cubicle

TNC interfaces enable location, identity, endpoint health, and behavior-based access control decisions for users in an enterprise environment, as well as dynamic detection and provisioning of access for unmanaged devices. Integration with physical security controls offers a new dimension of access control intelligence.

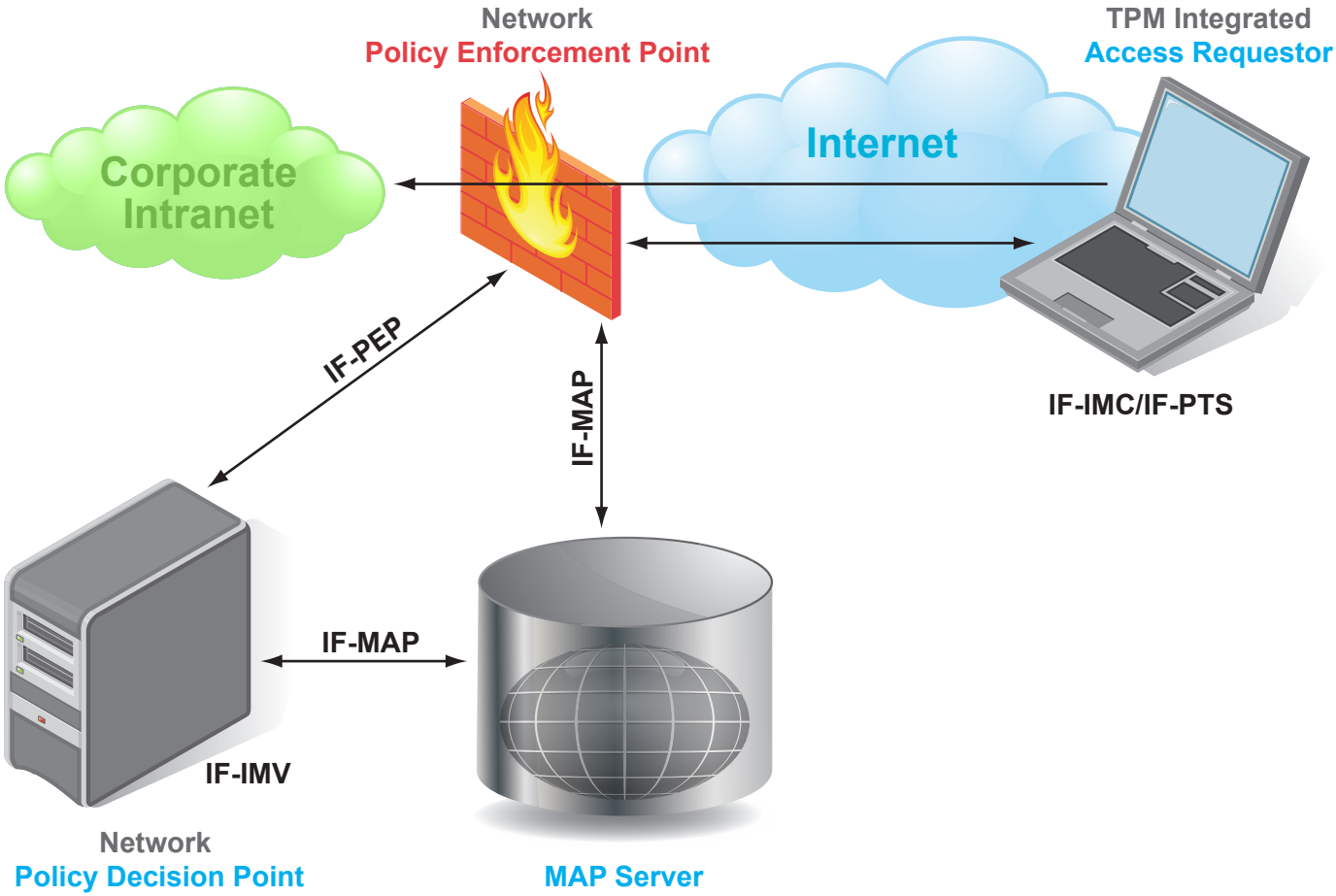


- IF-PEP enables dynamic admission control and port-based network enforcement for both 802.1X authenticated and MAC-authenticated endpoints.
- IF-TNCCS-SOH provides integration between TNC and Microsoft NAP, enabling a NAP Agent to communicate endpoint health information to a TNC PDP without requiring a third-party supplicant.
- The CESP defines mechanisms that ensure the ability to dynamically provision appropriate access for endpoints that lack a TNC client and are unable to authenticate to the network and/or demonstrate compliance with security requirements.
- IF-MAP enables integration of information from additional security systems, adding behavioral intelligence to the access decision for managed and unmanaged endpoints and integrating physical security with network access control.

Great Bay Software Inc.
HIRSCH ELECTRONICS
Infoblox
Juniper NETWORKS
McAfee
Microsoft
ProCurve Networking by HP

Mobile User / Remote Access

TNC interfaces enable consistent user experience and thorough compliance checking for remote users. Optional integration with a TPM provides additional hardware-based assessment to thwart rootkits.



- IF-PTS and TPM integration enable detection of "lying endpoints" that may have been compromised, e.g. by a rootkit, and could be providing inaccurate identity or integrity information.
- IF-MAP enables federation of user session information between the remote access and NAC solutions to facilitate seamless provisioning of access to and through the network.

Infoblox®

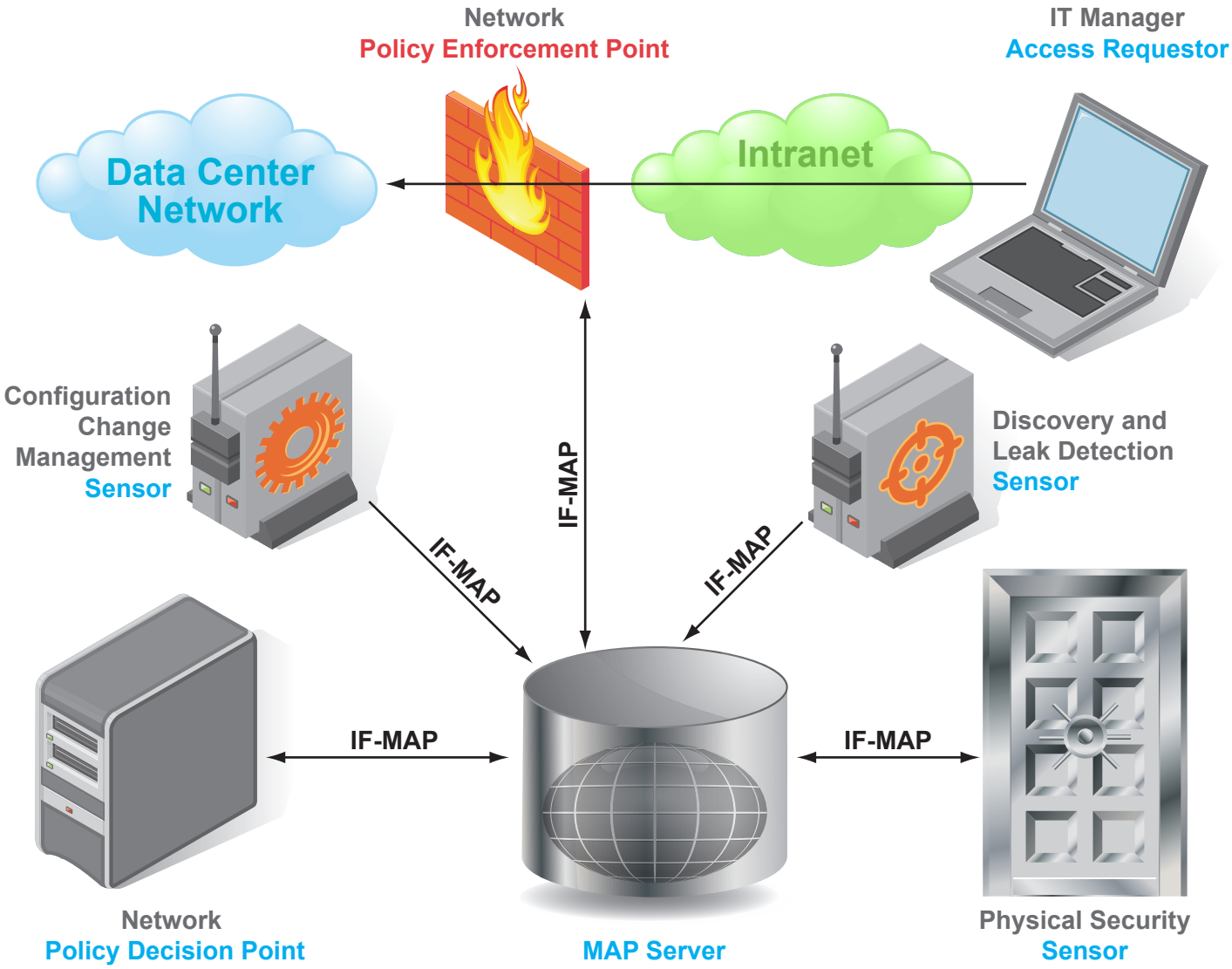
Juniper® NETWORKS

McAfee®

wave®

Data Center / Management

TNC interfaces enable: location, identity, endpoint health, and behavior-based access control decisions for users in an enterprise environment; detection and remediation of illicit activity, such as data leakage by an endpoint or unauthorized changes to network device configurations; and correlation of physical security with network access privileges.

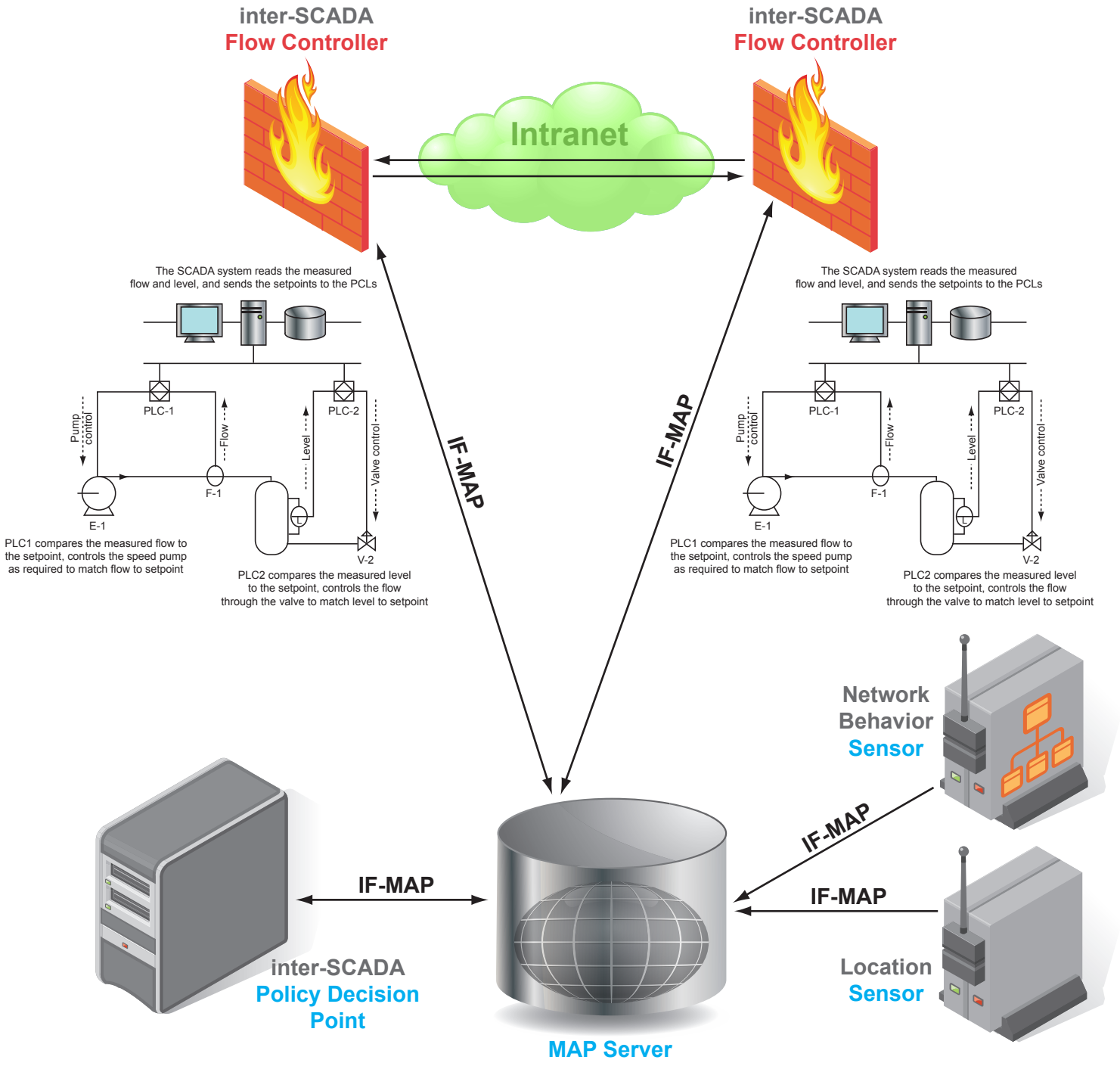


- IF-PEP enables dynamic admission control and assignment of endpoints to the appropriate VLAN.
- IF-MAP enables data leak prevention, configuration management, and correlation of physical access privileges with network access privileges.

enterasys® Secure Networks™ · HIRSCH ELECTRONICS · Infoblox® · Juniper® NETWORKS · LUMETA® · nSolutions Effortless Infrastructure

Industrial Control System (SCADA)

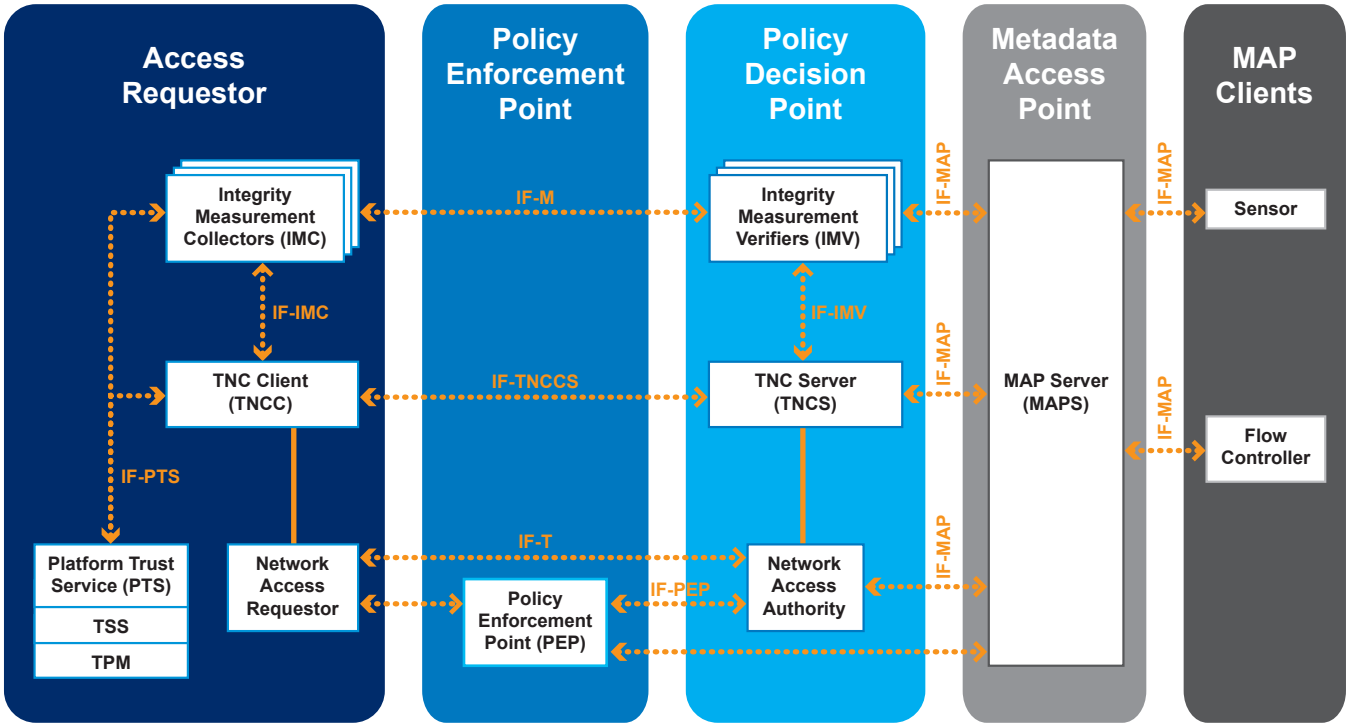
IF-MAP enables dynamic protection for interconnections between a control system network and an enterprise network.



IF-MAP enables coordination of configuration, behavioral, location, and policy information between provisioning applications, policy management and enforcement devices, and network intelligence / visibility components.

BOEING · Great Bay Software Inc. · Infoblox · TOFINO™ · TRAPEZE NETWORKS

TNC Architecture



Elements

Access Requestor (AR): The role of the AR is to seek access to a protected network in order to conduct activities on the network.

Clientless Endpoint (CE): Any endpoint that does not (or cannot) run a TNC client and provide verifiable identity and integrity data.

Policy Enforcement Point (PEP): The PEP is the element which is connected to the AR or CE; the role of the PEP is to enforce the decisions of the PDP regarding network access. Use cases which do not require the PEP include those which conduct network compliance monitoring, suggest remediation recommendations, and exclude direct enforcement.

Policy Decision Point (PDP): The role of the PDP is to perform the decision-making regarding the AR's network access request, in light of the access policies.

Metadata Access Point (MAP): The role of the MAP is to store and provide state information about ARs which may be useful to policy decision making and enforcement. This information includes, but is not limited to, device bindings, user bindings, registered address bindings, authentication status, endpoint policy compliance status, endpoint behavior, and authorization status.

MAP Client (MAPC): The role of the MAP Client is to publish to, or consume from, the MAP state information about ARs and CEs. A MAP Client may both publish and consume state information, and might not be directly connected to the AR or CE.

Trusted Platform Module (TPM): The TPM is a microcontroller that stores keys, passwords and digital certificates. It typically is affixed to the motherboard of a PC and potentially can be used in any computing device that requires these functions. The nature of this silicon ensures that the information stored there is made more secure from external software attack and physical theft. Security processes, such as digital signature and key exchange, are protected through the secure TCG subsystem.

Specifications

IF-IMC / IMV: The interface for integrity measurement verifiers (IF-IMV) and the interface for integrity measurement collectors (IF-IMC) allow TNC clients and servers to load and use plug-in software components from different vendors, enabling easy integration of software from many vendors into a complete TNC implementation.

IF-TNCCS / IF-TNCCS-SOH: The interface for TNC client-server communications (IF-TNCCS) allows TNC clients and servers to exchange integrity measurement data. The interface for TNC client-server communications using the statement of health (IF-TNCCS-SOH) allows TNC servers to easily integrate Microsoft Windows systems and other Network Access Protection clients.

IF-PEP: The interface for Policy Enforcement Points (IF-PEP) enables network hardware from any vendor to serve as a Policy Enforcement Point in a TNC system.

IF-MAP: The interface for Metadata Access Points (IF-MAP) integrates a wide variety of security systems into a cooperative and responsive team, sharing information and alerts.

IF-PTS: The interface for platform trust services (IF-PTS) provides integration with a TPM - a hardware-based cryptographic root of trust - to ensure that TNC components are trustworthy.

CESP: The clientless endpoint support profile (CESP) outlines an approach and enforcement mechanisms to ensure interoperability and enforce compliance in environments where some endpoints lack a TNC Client.