TRUSTED COMPUTING GROUP™

TNC EVERYWHERE
Unified Security

TNC EVERYWHERE
Unified Security

A day in the life of the TNC-enabled enterprise…

An employee comes to work in the morning. When she badges into the building, the physical access control system publishes her location to a central clearinghouse, the Metadata Access Point (MAP).

The employee authenticates to the enterprise network, and her workstation is checked for compliance with corporate security policies. The policy server provisions appropriate access to network resources for the employee.

A guest visits the company using a laptop compliant with IETF/TNC standards. A health check against the guest endpoint ensures it complies with enterprise security policies before allowing it access to the corporate network.

The guest is placed in a restricted VLAN which provides access to appropriate resources, such as the Internet, but blocks access to the internal corporate subnets. His endpoint health and behavior are monitored throughout the duration of his connection to the network.

A contractor arrives to perform maintenance on a protected system. The contractor successfully authenticates and his endpoint passes the health check; the policy server provisions access only to that system, and he is also monitored.

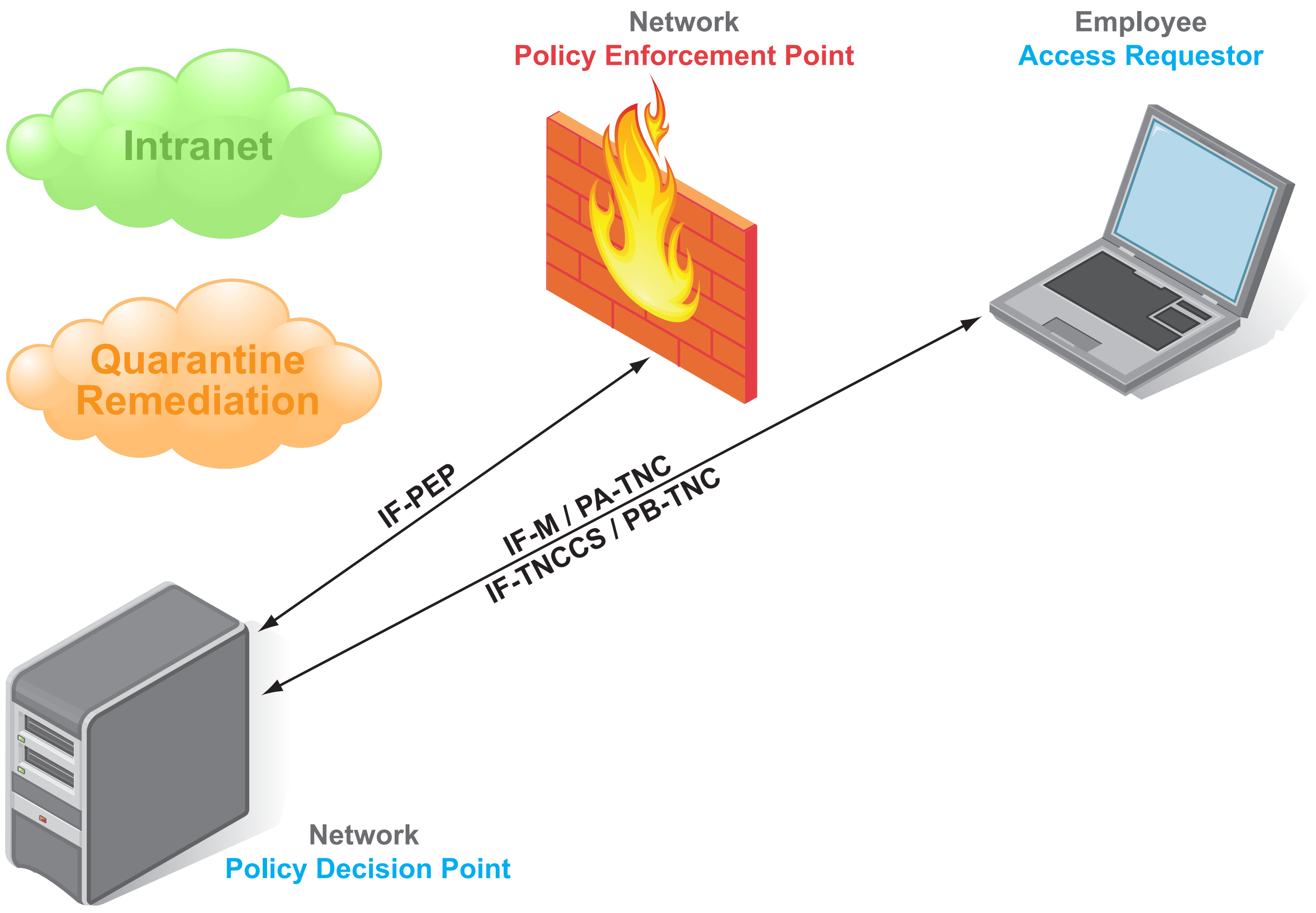
The contractor plugs in an EVDO device and makes a connection to the Internet, in violation of corporate policy. A network leak prevention sensor detects the leak and publishes a policy violation event to the MAP.

The MAP notifies the policy server of the policy violation, and the policy server terminates the contractor's access privileges on the network. Comprehensive logging enables the corporate security team to identify what the contractor did and why access was restricted.

At the end of the day, the employee logs out of her PC and badges out to go home. The physical access control system publishes her location to the MAP, and the MAP notifies the policy server that she has left the building.

The policy server provisions a new access policy for the employee's workstation, and the switch reassigns the workstation to a machine VLAN with restricted access for overnight maintenance and upkeep (such as backups or patch management).

TNC interfaces published as IETF RFCs (standards) enable dynamic differentiation & access control enforcement for a wide variety of users in mixed-use environments.



Enterprises are occupied by a wide variety of users, including visitors, partners, contractors, employees, and privileged employees. Networking and security devices from multiple vendors interoperate using TNC-based technology to provide appropriate access for each user based on their identity, endpoint compliance, and role. IETF adoption of TNC specifications ensures industry-wide agreement on standards, providing consistency across products from leading networking and security vendors.

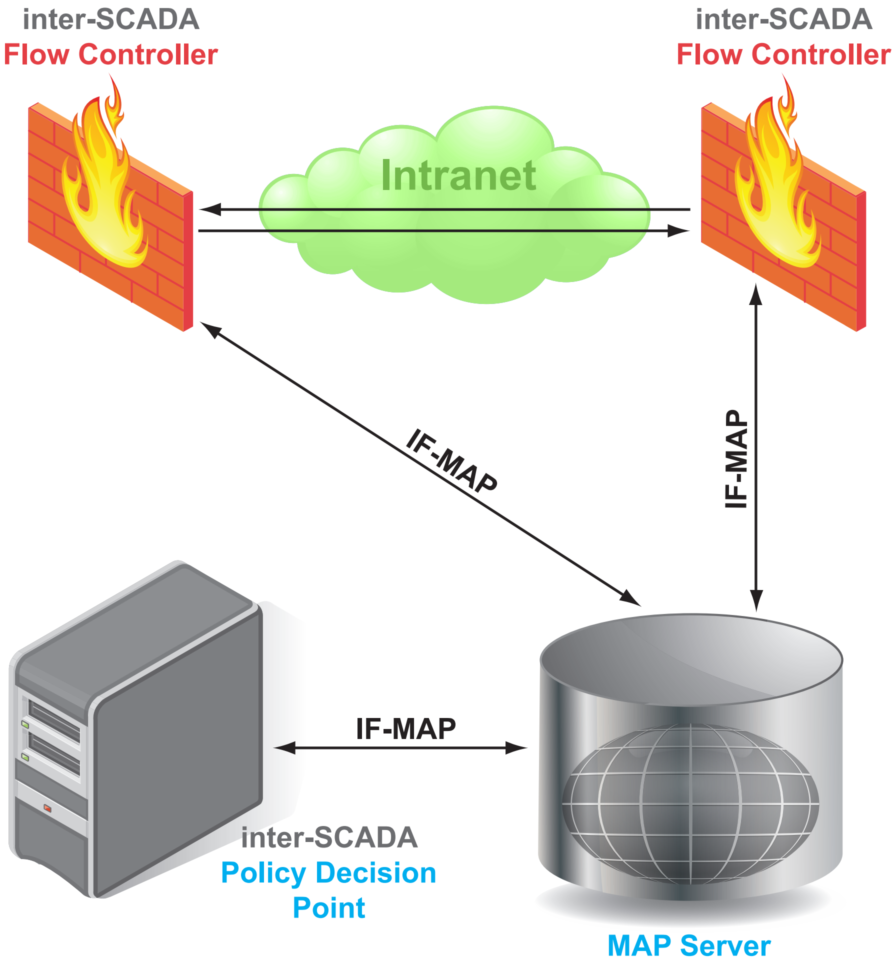
- XSupplicant, an open-source 802.1X client from the OpenSEA Alliance, provides cross-platform support for user authentication and endpoint health checking.

TNC interfaces underlie this intelligent, dynamic, responsive network access control:

- IF-TNCCS (called PB-TNC by the IETF) defines a standard way to perform a health check of a network endpoint such as a laptop computer or printer. If the endpoint is not healthy, it can be fixed or have its network access restricted.
- IF-M (called PA-TNC by the IETF) defines a standard set of health checks that are commonly performed, such as checking firewall status.
- IF-PEP enables provisioning of appropriate access for each user while ensuring consistent access control across wired and wireless connections.

Infoblox®　　JUNIPER® NETWORKS　　LUMETA® Global Network Visibility

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



Interconnectivity of industrial control systems, such as Supervisory Control And Data Acquisition (SCADA) systems, with enterprise IT networks is increasing, driven by considerations from cost to management to monitoring. With this increased access comes increased risk; operating systems that can't be patched due to operational considerations are exposed to infection from indirect connections to untrusted networks, and protocols never designed for security are accessible to attackers. Network security components implementing TNC standards provide isolation and protection.

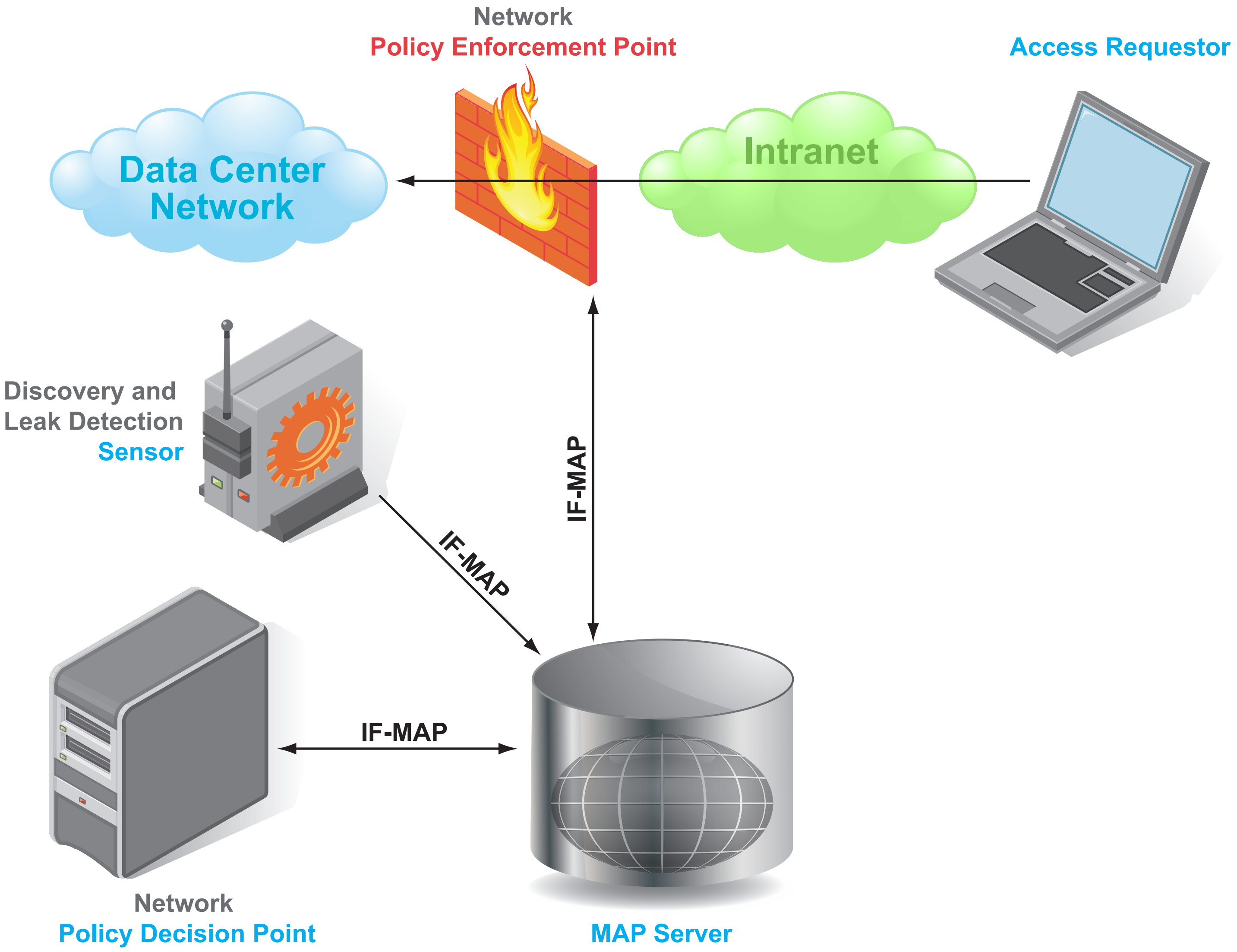
- Provisioning software from The Boeing Corporation acts as a TNC Metadata Access Point (MAP) Client, publishing security policy to be consumed by the Tofino Endboxes.
- The Tofino Security Appliances from Byres Security act as Policy Enforcement Points for the process control network, overlaying the process control network onto an enterprise network and proxying network transport security for Programmable Logic Controllers (PLCs) and Human Machine Interfaces (HMIs).
- The Infoblox NIA acts as a metadata access point (MAP), providing a clearinghouse for information about connected endpoints.

A TNC interface underlies this protection of the interconnection between a process control network and an enterprise network:

- IF-MAP enables coordination of security policy information and certificates between provisioning applications, policy management systems, and enforcement devices.

Infoblox® JUNIPer NETWORKS® LUMETA® Global Network Visibility

TNC interfaces enable location, identity, endpoint health, and behavior-based access control decisions for users in an enterprise environment, along with detection and remediation of illicit activity such as data leakage by an endpoint.



Enterprise environments require a high degree of control over user access to critical application and information resources. Integration of traditional NAC with other security technologies such as data leak prevention can ensure protection not only of the network itself but of the data it contains.

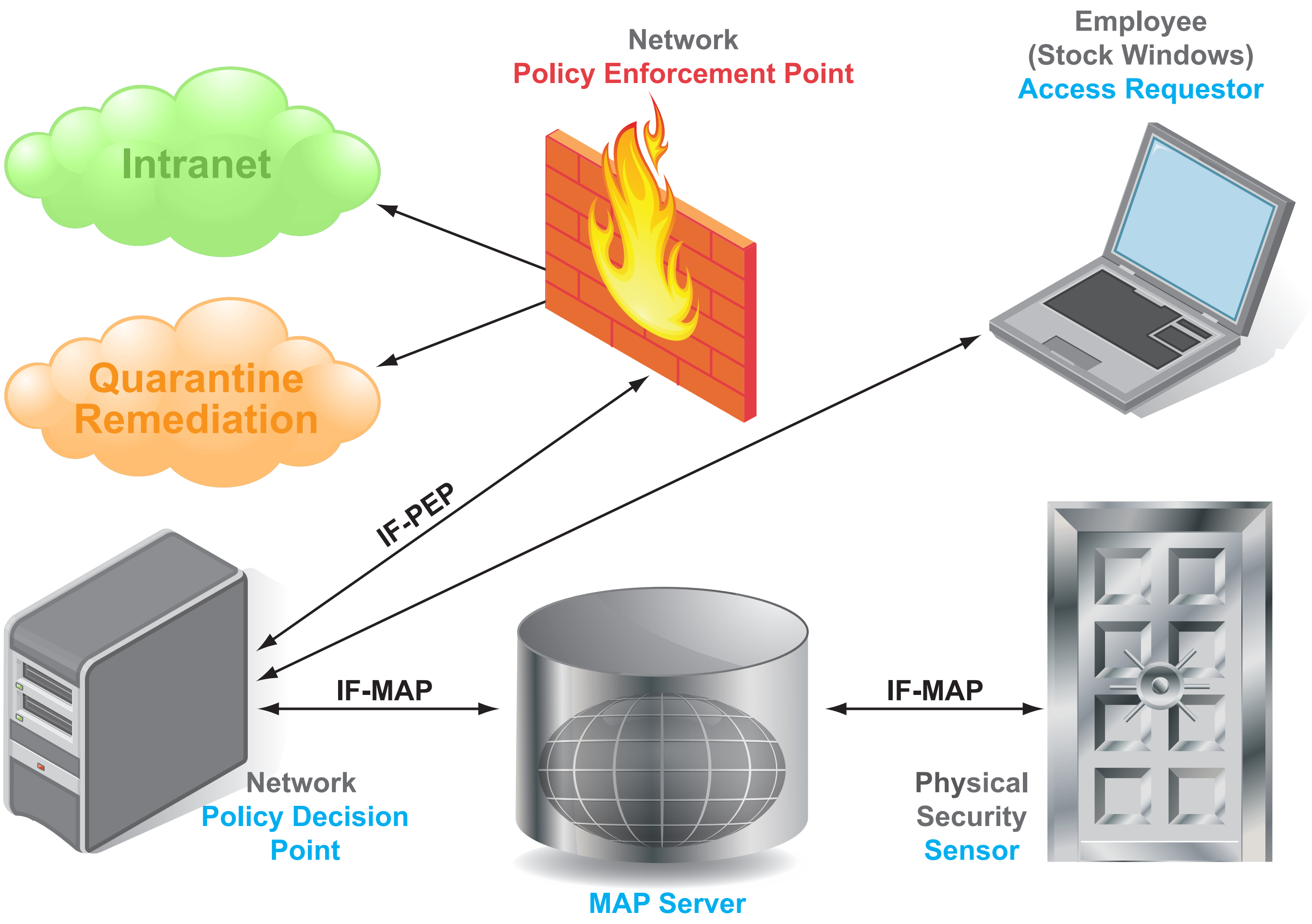
- The Lumeta IPsonar acts as a TNC Metadata Access Point (MAP) Client, detecting network leaks and publishing that information to the TNC Metadata Access Point (MAP); other network devices can use that information to prevent unauthorized "backdoor" Internet connections that bypass network access controls.
- The Juniper Networks IC Series UAC Appliance, the policy management server at the heart of Juniper's Unified Access Control solution, acts as a TNC Policy Decision Point (PDP), providing user authentication and endpoint health checking and provisioning policy to the network devices acting as enforcement points.
- The Infoblox NIA acts as a metadata access point (MAP), providing a clearinghouse for information about connected endpoints.

TNC interfaces underlie this integration of data leak prevention and network access control:

- IF-PEP enables dynamic admission control and assignment of endpoints to the appropriate VLAN.
- IF-MAP enables integration of network intelligence from additional security systems to add a behavioral consideration to the access decision.

Infoblox® JUNIPer NETWORKS® LUMETA® Global Network Visibility

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



Datacenter environments require a high degree of control of both physical and network access to critical resources. Integration with physical security can ensure that only users authorized and physically present in a datacenter location can access the network, mitigating the risks posed by "tailgating" or access gained through social engineering.

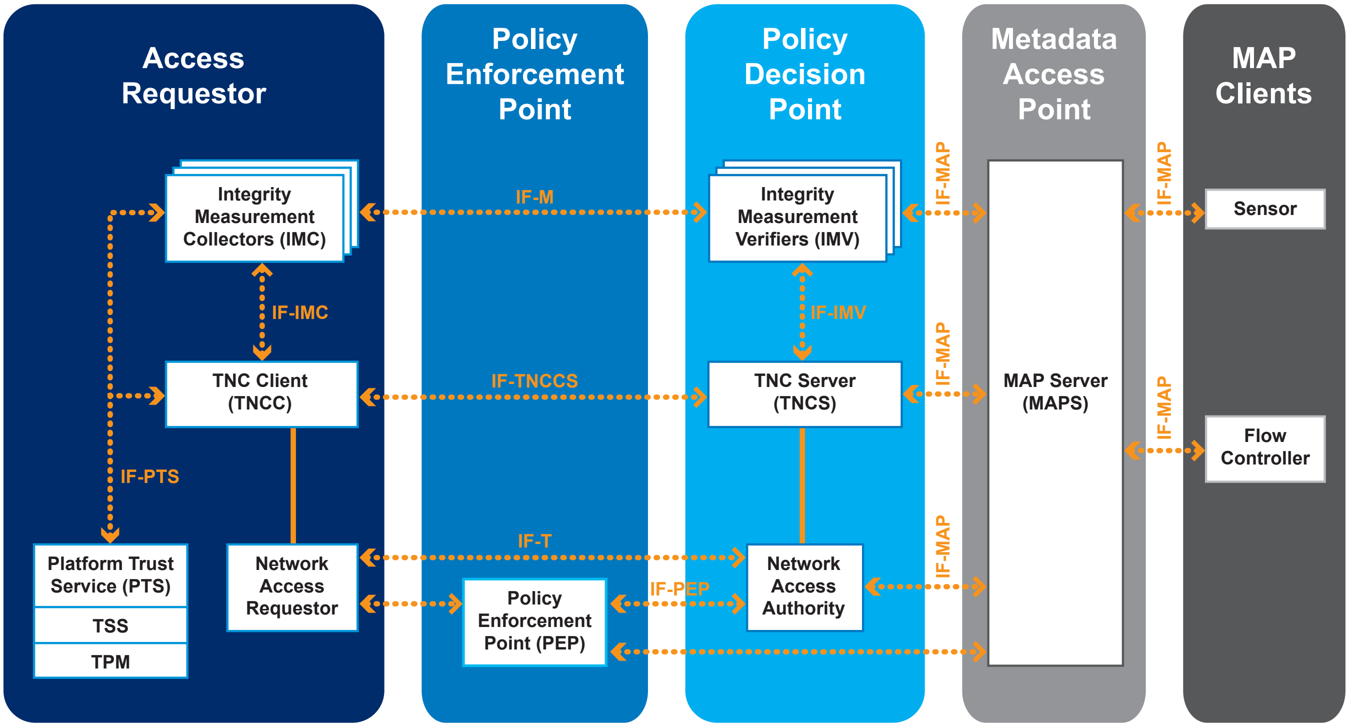
- The Hirsch Velocity Security Management System acts as a MAP Client, publishing information about users' physical badge access to the metadata access point (MAP); other network devices can leverage that information to apply location-based security policies and provision network access only for users physically present in a location.
- The Infoblox NIA acts as a MAP, providing a clearinghouse for information about connected endpoints.
- The Juniper Networks IC Series UAC Appliance, the policy management server at the heart of Juniper’s Unified Access Control solution, acts as a TNC Policy Decision Point (PDP), providing user authentication and endpoint health checking and provisioning policy to the network devices acting as enforcement points.

TNC interfaces underlie this intelligent responsive convergence of physical and network access control:

- IF-PEP enables dynamic admission control and assignment of endpoints to the appropriate VLAN.
- IF-MAP enables integration of network intelligence from additional security systems to add a physical security consideration to the access decision.

Infoblox® JUNIPER NETWORKS® LUMETA® Global Network Visibility

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.

Certification

The TNC certification program covers the IF-IMC, IF-IMV, and IF-PEP specifications. Before receiving TNC certification, products are thoroughly tested for specification compliance and for interoperability with other certified products. TNC certification ensures that products correctly implement the TNC specifications and work together in the enterprise.

TNC Adoption

Access Requestor

McAfee
Microsoft
symantec
IBM
extreme networks
FUJITSU
JUNIPER NETWORKS
StillSecure
wave
Lumension SECURITY

Policy Enforcement Point

ARUBA
extreme networks
enterasys Secure Networks
Microsoft
TRAPEZE NETWORKS
JUNIPER NETWORKS
NORTEL
ProCurve Networking by HP

Policy Decision Point

FUJITSU
Microsoft
IBM
symantec
wave
Q1 Labs
McAfee
JUNIPER NETWORKS
StillSecure
extreme networks
Lumension SECURITY

Metadata Access Point

Infoblox
JUNIPER NETWORKS

Sensors, Flow Controllers

ArcSight
ARUBA
TRAPEZE NETWORKS
JUNIPER NETWORKS
Great Bay Software Inc.
HIRSCH ELECTRONICS
nSolutions Effortless Infrastructure
TOFINO
LUMETA
insightix