Continuous Assessment Protocols for SACM

draft-hanna-sacm-assessment-protocols-00.txt
NEA Reference Model
from RFC 5209

Posture Collectors

Posture Broker Client

Posture Transport Client

Posture Attribute (PA) protocol

Posture Broker (PB) protocol

Posture Transport (PT) protocols

NEA Client

Posture Validators

Posture Broker Server

Posture Transport Server

NEA Server

November 5, 2012

IETF 85 - SACM Meeting
Basic TNC Architecture

Access Requestor
- Integrity Measurement Collectors (IMC)
- TNC Client (TNCC)
- Network Access Requestor

Policy Enforcement Point
- IF-M
- IF-TNCCS
- Policy Enforcement Point (PEP)

Policy Decision Point
- Integrity Measurement Verifiers (IMV)
- TNC Server (TNCS)
- Network Access Authority

Integrity Measurement Collectors (IMC)
IF-IMC

TNC Client (TNCC)
TNC  Server (TNCS)

Network Access Requestor

http://www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications
NEA With EAP Transport (PT-EAP)

**NEA Client**
- Non-compliant System
  - Windows 7
  - xOSHHotFix 2499
  - xOSHHotFix 9288
  - AV - McAfee Virus Scan 8.0
  - Firewall

**Compliant System**
- Windows 7
  - OSHHotFix 2499
  - OSHHotFix 9288
  - AV - Symantec AV 10.1
  - Firewall

**Policy Enforcement Point**
- Production Network
- Remediation Network
- PA-TNC/PB-TNC/PT-EAP

**Policy Decision Point**
- Windows 7
  - OSHHotFix 2499
  - OSHHotFix 9288
  - AV (one of)
    - Symantec AV 10.1
    - McAfee Virus Scan 8.0
    - Firewall
NEA With TLS Transport (PT-TLS)

Access Requestor

Compliant System
Windows 7
✓ OSHotFix 2499
✓ OSHotFix 9288
✓ AV - Symantec AV 10.1
✓ Firewall

Policy Decision Point

PA-TNC/PB-TNC/PT-TLS

Policy
Windows 7
• OSHotFix 2499
• OSHotFix 9288
• AV (one of)
  • Symantec AV 10.1
  • McAfee Virus Scan 8.0
  • Firewall
SCAP Messages for IF-M

Access Requestor
- Integrity Measurement Collectors (IMC)
  - TNC Client (TNCC)
  - Network Access Requestor

Policy Enforcement Point
- SCAP IF-M
  - IF-IMC
  - IF-TNCCS
  - Policy Enforcement Point (PEP)

Policy Decision Point
- Integrity Measurement Verifiers (IMV)
  - TNC Server (TNCS)
  - Network Access Authority

IF-T

http://www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications
IF-MAP: Secure Dynamic Info Sharing

Access Requestor
- Integrity Measurement Collectors (IMC)
- TNC Client (TNCC)
- Network Access Requestor

Policy Enforcement Point
- IF-M
- IF-T
- Policy Enforcement Point (PEP)

Policy Decision Point
- Integrity Measurement Verifiers (IMV)
- TNC Server (TNCS)

Metadata Access Point
- IF-MAP

Sensors and Flow Controllers
- Sensor
- Flow Controller

http://www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications

November 5, 2012
IETF 85 - SACM Meeting