Trusted Network Connect: Securing Networks through Standards-Based Network Access Control and Interoperability

April 20, 2009
Agenda

The Challenges of NAC
A Brief TCG Overview
Introduction to the TNC Architecture and Adoption
How TNC Meets the Challenges of NAC
Deployment Discussion
Hands-on Demonstration
Challenges of NAC

Vendor lock-in
- Proprietary solutions require hardware rip-and-replace

Complexity
- Too many moving parts, both in your network and in the solution

Project scope
- Need to secure thousands of endpoints, hundreds of remote offices, a variety of user communities…

Disruption of business practices
- Confusion, frustration, potential downtime

Support costs
- User impact == helpdesk impact

Uncertain future
- Relatively new technology - where is it going?
TCG: The Big Picture

Applications
- Software Stack
- Operating Systems
- Web Services
- Authentication
- Data Protection

Security Infrastructure

TCG Standards

Desktops & Notebooks

Printers & Hardcopy

Mobile Phones

Networking

Security Hardware

Servers

Storage
Trusted Network Connect (TNC)

Open Architecture for Network Access Control (NAC)
- Completely vendor-neutral
- Strong security through trusted computing

Open Standards for NAC
- Full set of specifications available to all
- Products shipping for more than four years

Work Group of Trusted Computing Group
- Industry standards group
- About 175 member companies in TCG, 75 in TNC-WG
- Includes large vendors, small vendors, customers, etc.
Basic NAC Architecture

- Access Requestor (AR)
- Policy Enforcement Point (PEP)
- Policy Decision Point (PDP)

- VPN

Copyright © 2009 Trusted Computing Group
Integrating Other Security Devices

- Access Requestor (AR)
- Policy Enforcement Point (PEP)
- Policy Decision Point (PDP)
- Metadata Access Point (MAP)
- Sensors, Flow Controllers (MAP Clients)
NAC Challenges - Overcome

Interoperability - work with what you already have
- Vendor-agnostic, multi-vendor support for diverse, heterogeneous networking environments

Reliability - use best-of-breed
- Eliminates vendor lock-in; increases ROI
- Minimizes disruption of business practices

Flexibility - tackle the low-hanging fruit first
- Reduces complexity, cost, deployment time
- Accommodates project scope in phases

Transparency, communication, auto-remediation
- Lower support cost, higher user acceptance

Meet future as well as present needs
- Thorough and open technical review of standards
- Prepares for whatever the future brings
TNC Reality

TNC standards-based products are available

TNC-enabled solutions have been implemented by customers

The number of TNC adopters (vendor and client) continue to grow

TNC-based IETF standards expected to reach RFC status in 2009
Flexible, Standards-based Access Control

Dynamically handles guests, partners, contractors, unmanageable devices
Mitigate threats by controlling access across wired/wireless networks

Centralized validation
Distributed enforcement

Control access to applications
Gain visibility and control for user/device access to network, resources and applications

Leverage other security devices for correlating network threat information to dynamically protect the network

Flexible solution to support access control in distributed networks
Health Check

Access Requestor
- Non-compliant System
  - Windows XP
  - ✔ SP3
  - ❌ AV – Symantec
  - ✔ Firewall

Policy Enforcement Point
- Production Network

Policy Decision Point
- Access Policy
  - Windows XP
  - ✔ SP3
  - ✔ Symantec AV
  - ✔ Firewall

Remediation Network
Behavior Check

Access Requestor

Policy Enforcement Point

Policy Decision Point

Metadata Access Point

Sensors and Flow Controllers (MAP Clients)

Remediation Network

Access Policy
Identity = Behavior

Copyright © 2009 Trusted Computing Group
Behavior Check

Access Requestor

Policy Enforcement Point

Policy Decision Point

Metadata Access Point

Sensors and Flow Controllers (MAP Clients)

Remediation Network

Access Policy
No leaking data

Copyright© 2009 Trusted Computing Group