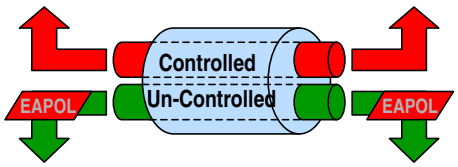
RSACONFERENCE2006

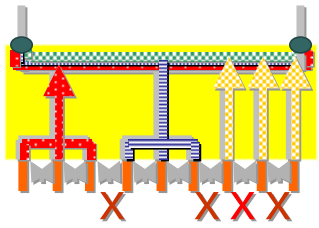
Securing the Endpoint: Deciding Among Different Strategies

Franjo Majstor
CCIE, CISSP
02/14/06 - DEF 201

Technologies Involved - Impact on Strategy Choice

- 802.1x/ EAP
- DHCP, VPN
- RADIUS/Diameter
- IPS/IDS
- PVLAN
- IP<-> MAC @ traceback
- End Node SW





Strategy Challenges

- Client or client-less?
- Easy of deployment vs. feature rich?
- Wait for TNC?
- Interoperable or proprietary?
- Preferred bleeding edge?
- Hybrid solution?
- New protocols, IPv6…?
- …
- ***History of end node <-> infrastructure interaction!***

Backup Slides

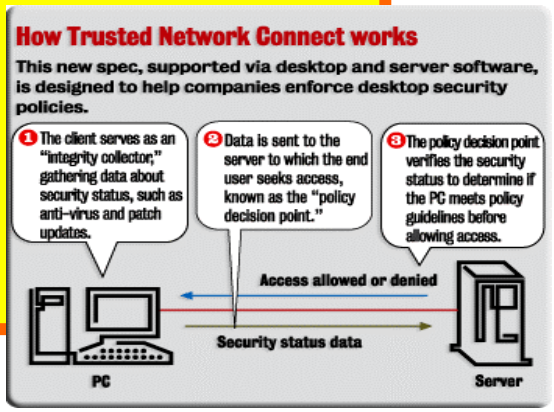
Choices

- **Trusted Network Connect (TNC)**
- **Network Admission Control (NAC)**
- **Network Access Protection (NAP)**
- **Sygate Network Access Control (SNAC)**
- **Automated Quarantine Engine (AQE)**
- **TippingPoint Quarantine Protection (TPQ)**
- **Trusted End System (TES)**
- **Others…**

What is Trusted Network Connect?

The TNC architecture and specifications were developed with a purpose of ensuring the *interoperability* amongst the individual components for the solution provided by different vendors. The aim of the TNC architecture is to provide a *framework* within which consistent and useful specifications can be developed to achieve a *multi-vendor* network standard that provides the following 4 features:

- ***Platform Authentication***
- ***Endpoint Policy Compliance***
- ***Access Policy***
- ***Assessment, Isolation,*** *[Remediation]*

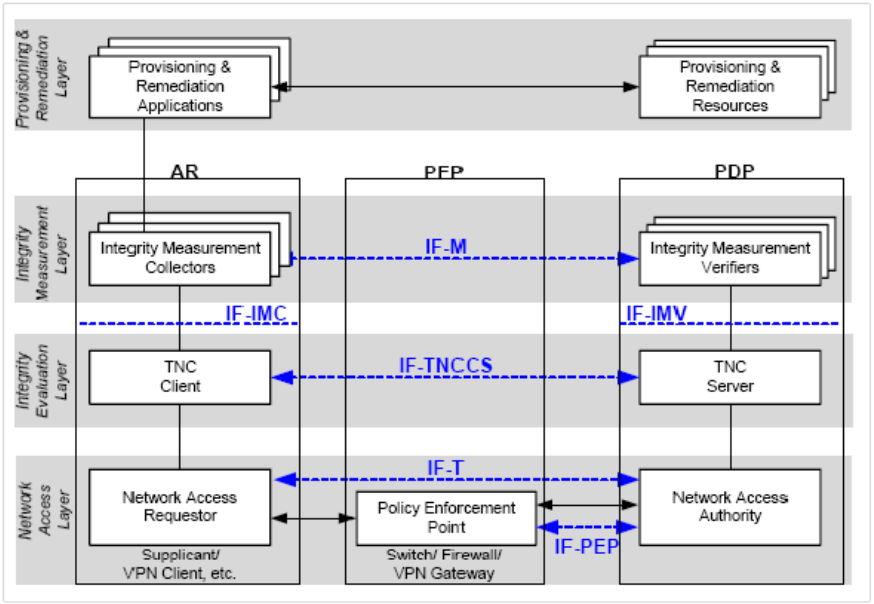


TNC Specification Architecture

AR:
Access Requestor

PEP:
Policy Enforcement Point

PDP:
Policy Decision Point



www.trustedcomputinggroup.org/downloads/TNC

Solution / Feature Support

Features / Solution	Requires Dedicated HW	Isolation	Access Media Supported	Remedy
TNC	No	VLAN/ACL	Open	Out of Scope
NAC	Yes/No*	VLAN/ACL	802.1x, 802.1x/UDP, IPsec VPN	3rd party
NAP	No	Subnet, VLAN, ACL	802.1x, L2TP VPN, IPsec VPN, DHCP	3rd party
SNAC	Yes	VLAN,ACL	802.1x, 802.1x/UDP, L2TP VPN, IPsec VPN, DHCP	Yes
AQE	No**	Port block, MAC filter, VLAN, ACL	IP	3rd party
TQP	No**	Port block, MAC filter, VLAN, ACL	IP	URL redirection to 3rd party
TES	Yes	Port block, MAC filter, VLAN, ACL	802.1x, IP	Yes

* NAC requires Cisco router or switch infrastructure; Cisco also released dedicated NAC appliance

** No dedicated infrastructure HW needed, while both TQP and AQE require dedicated IDS/IPS for malware activity detection

Solution / Feature Support

Features / Solution	Requires End Node Software	End Node OS Supported	Requires SW/HW Upgrade	PVLAN recommended
TNC	Yes	Open Specification	Once implemented - Yes	No
NAC	Yes	Microsoft only	Yes	No
NAP	No*	Microsoft only	Yes	No
SNAC	Yes	Microsoft only	Yes	No
AQE	No	Any	No	Yes***
TQP	No	Any	No	Yes***
TES	Yes/No**	Microsoft / Any**	Yes/No**	No

* Bundled with Microsoft OS

** Enterasys TES has agent-based and network-based options

*** PVLAN usage is not required, however is strongly recommended

References

AEQ - Automated Quarantine Engine:
www.alcatel.com/enterprise/en/products/ ip_networking/crystalsec_security/ pdf/AutoQuarantineEngine.pdf

NAC - Network Admission Control:
www.cisco.com/go/nac

NAP - Network Access Protection:
msdn.microsoft.com/library/default.asp?url=/library/en-us/wcecomm5/html/wce50conNetworkAccessPointNAP.asp

SNAC - Sygate Network Admission Control:
www.sygate.com/news/universal-network-access-control-snac_rls.htm

TNC - Trusted Network Connect:
www.trustedcomputinggroup.org/downloads/TNC

TES - Enetrasys Trusted End-System:
www.enterasys.com/solutions/secure-networks/trusted_end_system

HP news:
www.techworld.com/security/news/index.cfm?NewsID=3128

Nortel news:
www.nortel.com/corporate/news/newsreleases/2004d/12_13_04_microsoft_alliance.html