

Infrastructure protection
from
"naive" end-nodes,
what is the choice?

Franjo Majstor
Senior Technical Director EMEA, CipherOptics, Inc
10/24/06 - DEF 105

Agenda

- Technology Briefing
- Making The Right Choice
- Conclusion & Challenges



Technology Briefing

 CIPHEROPTICS Franjo Majstor, DEF-105

**RSACONFERENCE
EUROPE 2006**



FEAR Of Technical
Details...

UNTIL YOU HAVE THE COURAGE TO LOSE SIGHT OF THE SHORE,
YOU WILL NOT KNOW THE TERROR OF BEING FOREVER LOST AT SEA.

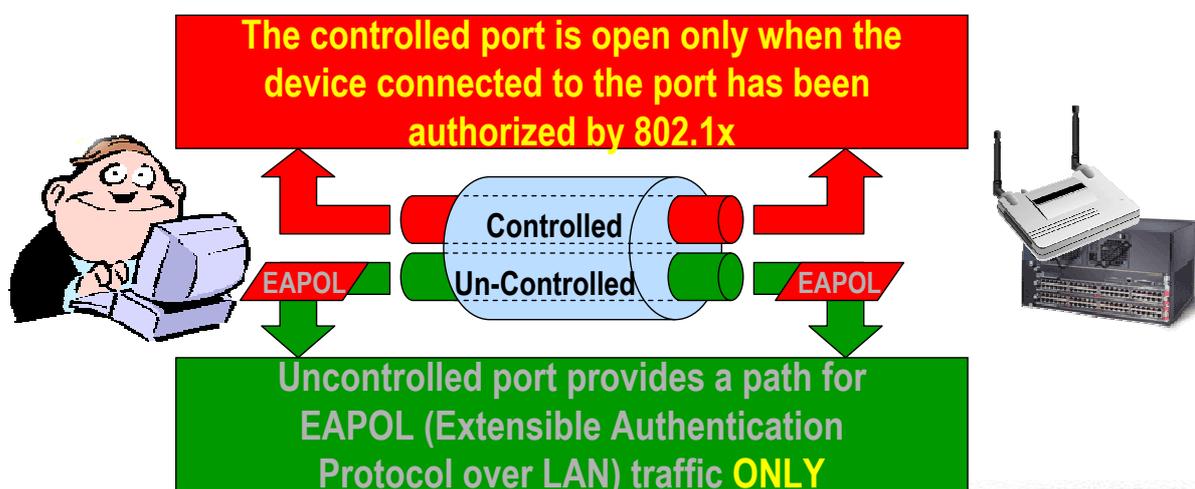
www.despait.com

Technology Briefing

- 802.1x
- EAP
- RADIUS/Diameter
- IPS/IDS
- End Node SW
- IPS/IDS
- PVLAN
- SSL VPN

IEEE 802.1x (Port Authentication)

For each 802.1x switch port, the switch creates
TWO virtual access points at each port



- **E**xtensible **A**uthentication **P**rotocol is an extension of CHAP/PAP within PPP

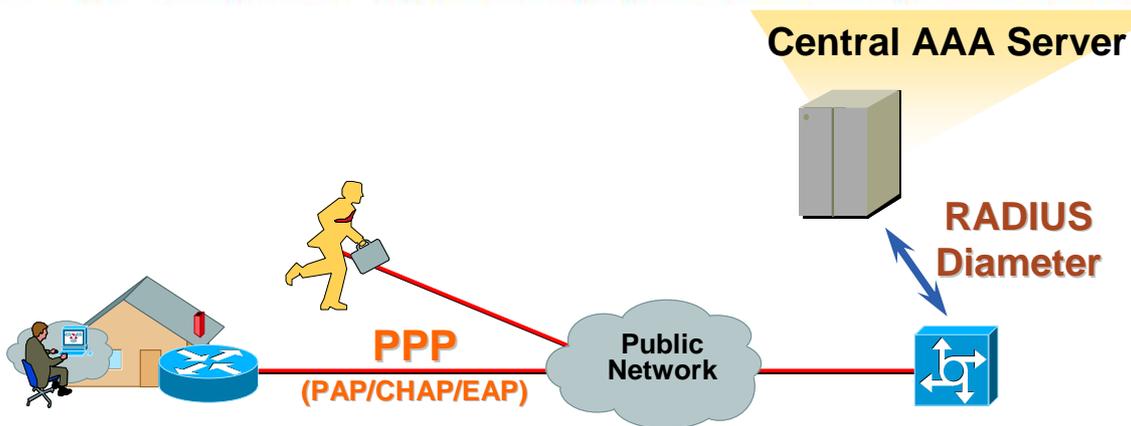
Support multiple “authentication” schemes:

- plain password hash (MD5)
- token cards
- GSS-API (Kerberos)
- TLS (based on x.509 certificates)
- ...

Extensible Authentication Protocols

- **EAP-MD5 (Message Digest 5)**
 - Supported in Win 2K/XP and other Windows versions
 - Does **not** provide **mutual** authentication **nor WEP key derivation**
- **EAP-Cisco Wireless, or LEAP**
 - Supported client in WinXP/2K/NT/ME/98/95/CE, Linux, Mac, DOS.
 - Provides **mutual** authentication and **WEP key derivation**
- **EAP-TLS (mutual EAP-TLS)**
 - Supported in Win 2K/XP and other Windows versions
 - Requires **client certificates** and **server certificates**
- **PEAP**
 - Supported in XP and, soon other Windows versions
 - Uses server-side TLS, which requires **only server certificates**
- **EAP-TTLS**
 - Is supported by Funk Software's Odyssey
 - Uses server-side TLS
- **EAP-FAST** (*draft-cam-winget-eap-fast-03.txt*)
 - Latest effort from Cisco to address LEAP weaknesses and do fast roaming

RADIUS/Diameter



- **AAA** stands for Authentication, Authorization, and Accounting services
- **RADIUS** - Remote Authentication Dial In User Service, RFC 2865, 2866, 2869
 - Initially used for dial-in networks – now greatly expanded to a variety of uses
 - System user account centralized authentication
 - Network device user account AAA services
 - Dial-in/VPN service AAA services
- **Diameter** - not an acronym, next generation AAA protocol, RFC 3588

End Node SW

Client Software Applications

- Pop Up Blocker
- Spyware/Adware
- HIDS
- Anti-Virus
- Personal FW
- URL Filter
- Spam Filter
- VPN Client
- SSL Client
- Citrix Client

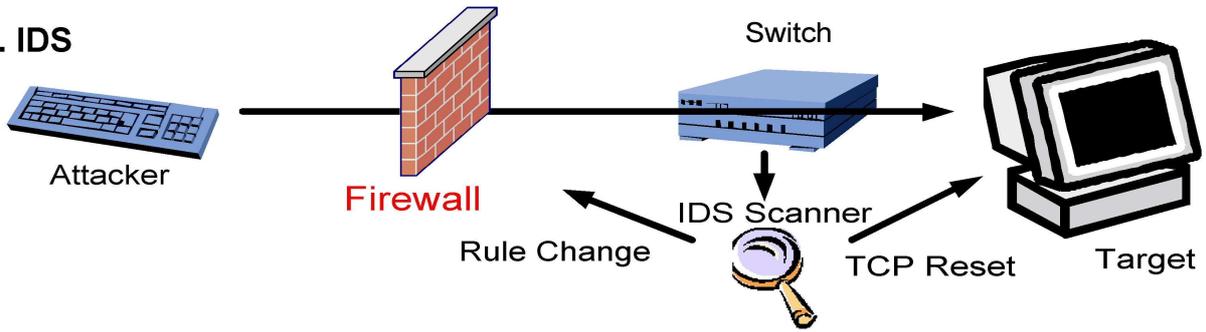


- OS dependent
- Device dependent
- Updating issue
- Disparate solution set

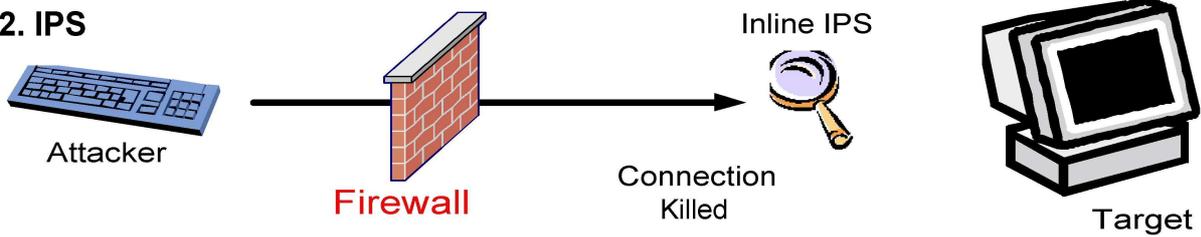


IDS/IPS

1. IDS



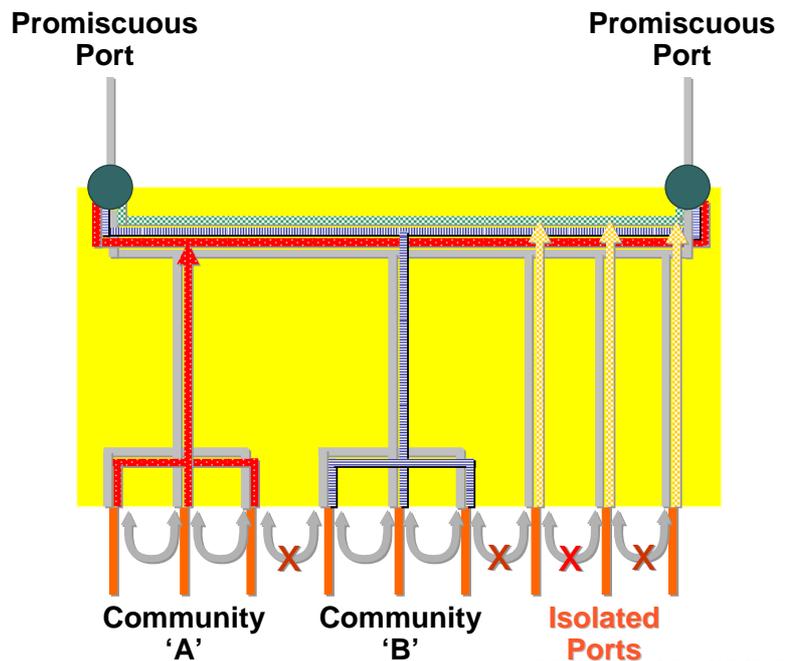
2. IPS



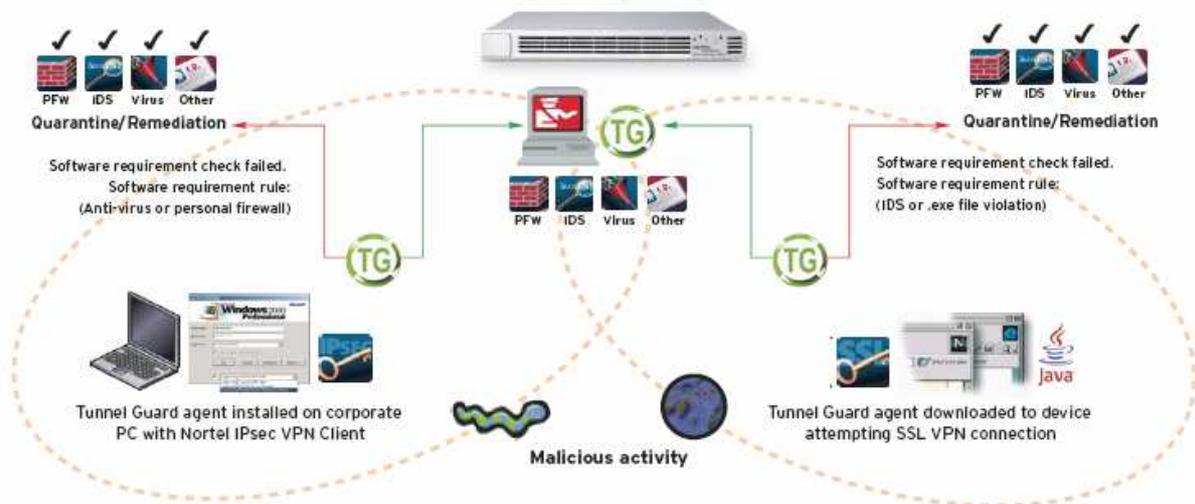
Private VLANs (PVLAN)

All ports in the same Subnet:

- Primary VLAN
- - - Community VLAN
- - - Community VLAN
- - - Isolated VLAN



SSL - VPN



Source of info: www.nortel.com/products/01/contivity/collateral/nn106181.pdf

Making The Right Choice

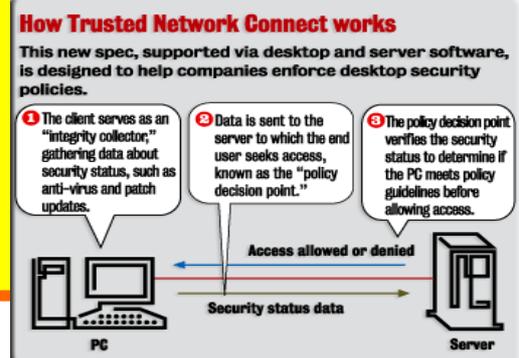
Choices

- Trusted Network Connect (**TNC**)
- Network Admission Control (**NAC**)
- Network Access Protection (**NAP**)
- Secure Network Access (**SNA**)
- Automated Quarantine Engine (**AQE**)
- TippingPoint Quarantine Protection (**TPQ**)
- Unified Access Control (**UAC**)
- Total Access Protection (**TAP**)
- Open Source NetAuth
- ...

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:

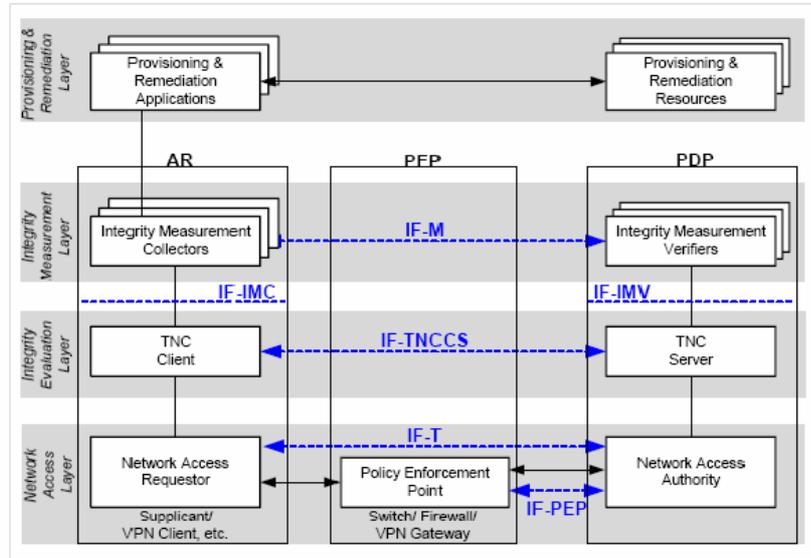
Access Requestor

PEP:

Policy Enforcement Point

PDP:

Policy Decision Point



www.trustedcomputinggroup.org/downloads/TNC

Open Source/Commercial Solutions

Dashboard > Salsa-NetAuthWG > Home > Commercial NetAuth Type Products

Commercial NetAuth Type Products

Added by Steve Oshansky, last edited by Kevin Amorin on Apr 26, 2006 (view changes) Labels: (None)

Company	Product	Home Page
3com	TipplingPoint	http://www.tippling.com
Aruba Networks	Mobility Management	http://www.arubanetworks.com
Bradford Networks	Campus Manager	http://www.bradfordnetworks.com
Cisco	Cisco Clean Access (formerly Perigo)	http://www.cisco.com
Checkpoint	Integrity (formerly ZoneLabs)	http://www.checkpoint.com
ConSentry Networks	LANShield	http://www.consentry.com
CyberGuard	TSP	http://www.cyberguard.com
DeepNines	Edge Infection Quarantine	http://www.deepnines.com
Endforce	ENDFORCE Enterprise	http://www.endforce.com
Extreme	Sentriant	http://www.extremepoint.com
Enterasys Networks	Enterasys Sentinel	http://www.enterasys.com
ForeScout	CounterACT	http://www.foressc.com
Full Armor	PolicyPortal	http://www.fullarmor.com
HP	HP ProCurve	http://www.hp.com
Impulse Point	Safe Connect	http://www.impulsec.com
InfoBlox	ID Aware	http://www.infoblox.com
InfoExpress	CyberGatekeeper	http://www.infoexpress.com
Ipasec	Universal Policy Enforcement	http://www.ipasec.com
Juniper	Endpoint Assurance (formerly Funk)	http://www.funk.com
Labis Networks	StillSecure Safe Access	http://www.stillsecure.com
Lancope	StealthWatch	http://www.lancope.com
LANDesk	Trusted Access	http://www.landesk.com

Dashboard > Salsa-NetAuthWG > Home > Open Source NetAuth Type Solutions

Open Source NetAuth Type Solutions

Added by Steve Oshansky, last edited by Kevin Amorin on Mar 21, 2006 (view changes) Labels: (None)

List of open source solutions for Network Authentication, Detection, and Remediation. In order of last release date.

Type	Home Page	Last Updated
Agents		
	ResTek http://resstek.wvu.edu/projects/vst/	25-Oct-2005
	ESP Wizard http://www.utoronto.ca/security/UTORprotected/ESP/	23-Mar-2005
	Daisy http://vt.edu/~w2k/vt.edu/daisy.htm	16-Aug-2005
Registration Systems		
	HUPnet http://hupnet.sourceforge.net/	4-March-2005
	NetReg 2.0 http://sourceforge.net/projects/netreg/	30-Jun-2003
	NoCatAuth http://nocat.net/	17-May-2003
Registration, Active Detection		
	Southwestern NetReg http://www.netreg.org/	25-Jun-2005
Remediation, Passive Detection		
	Ungoliant http://ungoliant.sourceforge.net/	16-Dec-2005
	NetSQUID http://netsquid.tamu.edu/	8-Oct-2004

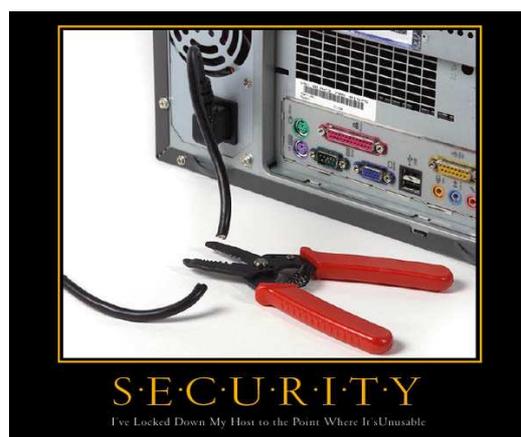
Registration, Remediation, Active/Passive Detection

Source of info: <http://wiki.internet2.edu/confluence/display/NetAuthWG/Home>

Conclusion & Challenges

Conclusion & Challenges

- Client or client-less?
- Per port or inline appliance?
- 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!**



References

AEQ - Automated Quarantine Engine:

www.alcatel.com/enterprise/en/resource_library/pdf/wp/wp_enterprise_security.pdf

NAC - Network Admission Control:

www.cisco.com/go/nac

NAP - Network Access Protection:

www.microsoft.com/technet/itsolutions/network/nap/default.aspx

Open Source:

wiki.internet2.edu/confluence/display/NetAuthWG/Home

TNC - Trusted Network Connect:

www.trustedcomputinggroup.org/downloads/TNC

TES - Entrasys Trusted End-System:

www.enterasys.com/solutions/secure-networks/trusted_end_system

HP news:

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

SNA - Nortel Secure Network Access:

www2.nortel.com/go/solution_content.jsp?prod_id=55121

Whitepaper on End Node Security:

www.employees.org/~franjo/papers/EndNodeSecurity_wp2.pdf



CIPHEROPTICS Franjo Majstor, DEF-105

RSACONFERENCE
EUROPE 2006

DEF-105

Infrastructure protection
from "naive" end-nodes,
what is the choice?

Franjo Majstor



CIPHEROPTICS Franjo Majstor, DEF-105

RSACONFERENCE
EUROPE 2006