SSL VPN-based NAC

Dr. Pipat Sookavatana
อาจารย์ภาควิศวกรรมศาสตร์
มหาวิทยาลัยเทคโนโลยีมหานคร

Agenda

- Background- Why NAC/NAP?
- SSL VPN-based NAC
  - Agent Based + ActiveX Plugin
  - Agentless
  - In-line deployment
  - Out-of-Band (Deployment with firewall)

Need More Security and Control

How do we ensure that all of them are using clean computers ?

How do we control their right to access to our network ?

- Internet café
  - Email, FTP, Telnet, Login to E-Banking
- Connect your PDA or Notebook to public network, i.e. Public WiFi
- Click “Yes” or “No” at any popup dialogbox
- Run email attach files

Kaspersky Top 20

A set of data different from the McAfee data comes from Kaspersky which shows the top 20 threats the company has detected in March 2007. This list and other data may be found at Kaspersky's VirusList site.

1	New	Trojan-Spy.HTML.Bankfraud.ra	31.93%
2	+2	Email-Worm.Win32.NetSky.q	13.96%
3	-1	Email-Worm.Win32.Bagle.gt	10.69%
4	-4	Email-Worm.Win32.NetSky.t	8.50%
5	New	Email-Worm.Win32.Warezov.jx	8.23%
6	+4	Email-Worm.Win32.NetSky.aa	3.89%
7	-	Net-Worm.Win32.Mytob.c	2.32%
8	+6	Email-Worm.Win32.Scano.gen	1.60%
9	+7	Email-Worm.Win32.NetSky.b	1.38%
10	Return	Email-Worm.Win32.Mydoom.l	1.32%
11	+9	Exploit.Win32.IMG-WMF.y	1.25%
12	Return	Worm.Win32.Feebs.gen	1.22%
13	Return	Email-Worm.Win32.Warezov.do	1.20%
14	Return	Email-Worm.Win32.NetSky.x	1.03%
15	Return	Email-Worm.Win32.Mydoom.m	0.88%
16	-13	Email-Worm.Win32.Zhelatin.dam	0.82%
17	+2	Email-Worm.Win32.Bagle.gen	0.78%
18	Return	Net-Worm.Win32.Mytob.bt	0.63%
19	Return	Net-Worm.Win32.Mytob.dam	0.53%
20	-3	Packed.Win32.PePatch.gr	0.51%
		Other malicious programs	7.33%

The big story here, obviously, is the huge number of Trojan-Spy.HTML.Bankfraud.ra detections. This threat was first detected on February 27, and reached No. 1 with a bullet.

Latest Malware Descriptions

04 17	Trojan-Dropper.Ichitaro.Tarodrop.d
04 17	Trojan-Dropper.Ichitaro.Tarodrop.c
04 16	Trojan.JS.Seeker.l
04 16	Trojan.JS.Seeker.k
04 16	Email-Worm.JS.Mountoni
04 16	Backdoor.Win32.Poison.h
04 16	Trojan-Downloader.Win32.Nurech.bf

Data from viruslist.com 14.22pm 17/04/07
http://www.viruslist.com/en/index.html

Why is the enforcement of device-level security policies important?

- Harmful malicious code can spread rapidly across networked computers
- There are many reasons why personal computers are out-of-compliance with prevailing policies. IT administration may not roll-out patches and service packs immediately and end users may not update virus signatures nor run anti-spyware software frequently enough.

NAC/NAP

- NAC
  - Network Access Control
  - Network Admission Control
- NAP
  - Network Access Protection

Simple NAC Definition

Network Access Control (NAC) aims to do exactly what the name implies:

control access to a network.

Wikipedia's NAC

(Network Access Control)

: April 16, 2007

Network Access Control

From Wikipedia, the free encyclopedia

This article or section does not adequately cite its references or sources.

Please help improve this article by adding citations to reliable sources. (help, get involved!)

Any material not supported by sources may be challenged and removed at any time. This article has been tagged since July 2006.

The introduction to this article provides **insufficient context** for those unfamiliar with the subject matter.

Please help improve the introduction to meet Wikipedia's layout standards. You can discuss the issue on the talk page.

Network access control (also called "network admission control" and "network access protection") is a method by which access to enterprise network resources is granted based upon authentication of the user and device as well as verification of the device's compliance to policy.

Network Access Control (NAC) aims to do exactly what the name implies: control access to a network. The term NAC is also sometimes used for Network Admission Control, which is focused on authenticating users and performing a posture check on the connecting device. The broader definition of NAC, as access control, includes pre-admission endpoint security policy checks and post-admission controls over where users can go on a network and what they can do.

NAC's roots trace back to the trusted computing movement, and the work of the Trusted Computing Platform Alliance. The TCPA morphed and reappeared as the Trusted Computing Group (TCG). The TCG has created the Trusted Network Connect (TNC) sub group to create an open-architecture alternative to proprietary NAC initiatives. The Trusted Network Connect Sub Group (TNC-SG) aims at enabling network operators to provide endpoint integrity at every network connection, thus enabling interoperability among multi-vendor network endpoints.

It is still an emerging technology space, and many vendors are taking advantage of this lack of definition to jump on the NAC bandwagon. But if we boil down NAC to its essence, we are referring to the ability to:

- Enforce security policy and restrict prohibited traffic types

navigation
- Main page
- Contents
- Featured content
- Current events
- Random article

interaction
- About Wikipedia
- Community portal
- Recent changes
- Contact us
- Make a donation
- Help

search
Go Search

toolbox
- What links here
- Related changes
- Upload file
- Special pages

Network Admission Control

From Wikipedia, the free encyclopedia

Network Admission Control (NAC) refers to restricting access to the network based on identity or security posture. When a network device (switch, router, access point, DHCP server, etc.) is configured for NAC, it can force user or machine authentication prior to granting access to the network. In addition, guest access can be granted to a quarantine area for remediation of any problems that may have caused authentication failure. This is enforced through an inline custom network device, changes to an existing switch or router, or a restricted DHCP class. A typical (non-free) WiFi connection is a form of NAC. The user must present some sort of credentials (or a credit card) before being granted access to the network.

Posture assessment

[edit]

Besides user authentication, authorization in NAC can be based upon compliance checking. This posture assessment is the evaluation of system security based on the applications and settings that a particular system is using. These might include Windows registry settings or the presence of security agents such as anti-virus or personal firewall. NAC products differ in their checking mechanisms.[1]:

- 802.1x Extensibile Authentication Protocol
- Microsoft Windows Administrator access - login credentials
- Cisco NAC Appliance L2 switch or L3 authentication
- Pre-installed security agent
- Web-based security agent

navigation
- Main page
- Contents
- Featured content
- Current events
- Random article

interaction
- About Wikipedia
- Community portal
- Recent changes
- Contact us
- Make a donation
- Help

search
Go Search

toolbox
- What links here
- Related changes
- Upload file
- Special pages

เป้าหมายหลักของ NAC/NAP

- Security posture of an endpoint
- ต้องการให้เฉพาะ client ที่ได้รับการ ตรวจสอบแล้วเท่านั้น เข้าใช้งาน ทรัพยากร เช่น เซิฟเวอร์ได้
  - การตรวจสอบก็เช่น
    - เครื่องนั้น ได้รับการ Authorized แล้ว
    - ผู้ใช้คนนั้น ได้รับการ Authorized แล้ว
    - เครื่องนั้น มีการติดตั้ง Personal Firewall เหมาะสม
    - เครื่องนั้น มีการติดตั้ง Antivirus เหมาะสม และมีการ update signature เรียบร้อยแล้ว

NAC/NAP Maturity

- Maturity ของ field ยังอยู่ในระยะเริ่มแรก
- มี Definition ที่หลากหลาย อุปกรณ์ในหลายยี่ห้อ ทำเรื่องนี้กันในหลาย Layer และหลายรูปแบบ
- ยังไม่มีการนำไปใช้งานจริง ๆ ภายในองค์กร ส่วนใหญ่อยู่ในช่วงการ evaluate solution ซึ่งมักจะใช้เวลานาน เพราะ technology อยู่ในช่วงเริ่มต้น และ product ต่าง ๆ ก็มีความสามารถหลากหลายแตกต่างกันไป

NAC Business Benefits

- Dramatically improves security
- Ensures endpoints (laptops, PCs, PDAs, servers, etc.) conform to security policy
- Proactively protects against malware (worms, viruses, spyware)
- Focuses operations on prevention, not reaction

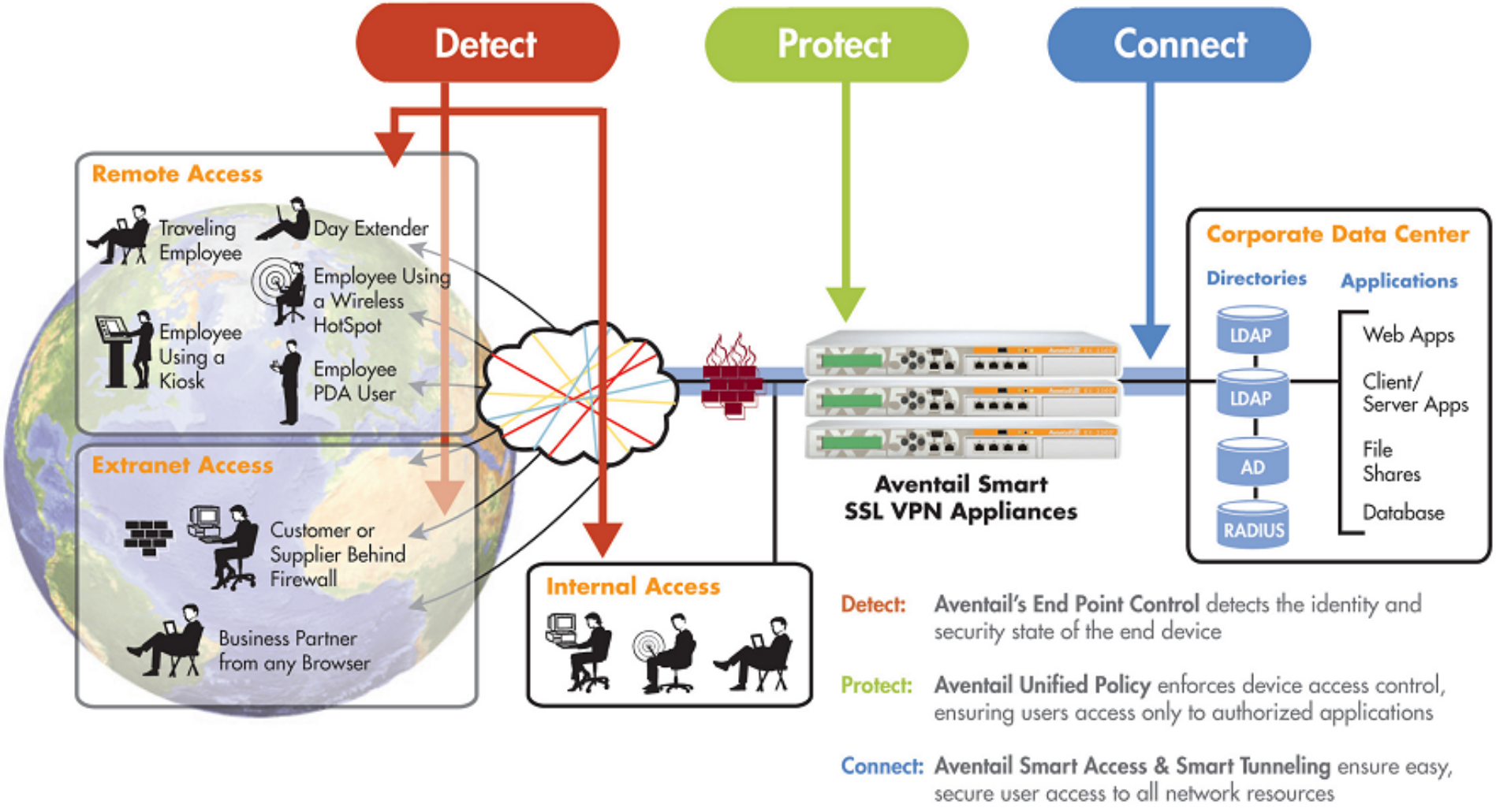
NAC+SSL VPN Implementation

- Agent-based & Agentless (Network-Based) Posture Check
  - The present of antivirus + latest signature update
  - The present of personal firewall
  - The present of latest OS patches
- **Policy Decision** and **Policy Enforcement**

Policy Decision vs Policy Enforcement

- Policy decision may be separate from policy enforcement - this architecture is often called an **out-of-band deployment**.
- When policy decision and policy enforcement occur in the same device, this is called an **inline deployment**.

Wikipedia's NAC (Network Access Control)
: April 16, 2007


Detect
Protect
Connect
Remote Access
Traveling Employee
Day Extender
Employee Using a Wireless HotSpot
Employee Using a Kiosk
Employee PDA User
Extranet Access
Customer or Supplier Behind Firewall
Business Partner from any Browser
Internal Access
Aventail Smart SSL VPN Appliances
Corporate Data Center
Directories
Applications
LDAP
LDAP
AD
RADIUS
Web Apps
Client/ Server Apps
File Shares
Database
Detect: Aventail's End Point Control detects the identity and security state of the end device
Protect: Aventail Unified Policy enforces device access control, ensuring users access only to authorized applications
Connect: Aventail Smart Access & Smart Tunneling ensure easy, secure user access to all network resources

กรณีการ deploy แบบ inline

- สามารถทำได้เลย แต่อาจจะต้องออกแบบ Network ใหม่ ให้แยกส่วนที่เก็บทรัพยากร ออกจากส่วนที่ client อยู่ การเข้าไปใช้ ทรัพยาการต้องมีการ authenticate ผ่าน NAC Appliance ซึ่งกรณีของ SSL VPN, SSL VPN appliance ก็ทำหน้าที่เป็น NAC Appliance
- NAC Appliance มักจะใช้การ deploy แบบ inline นี้

กรณีการ deploy แบบ Out-of-band

- ใช้ Firewall ในการแยก ทรัพยากรกลุ่มเซิฟเวอร์ กับ Client ทั้งหลายออกจากกัน
- ใน Firewall policy จะจำกัดให้ Client access เข้าไปยัง VPN Gateway ได้เท่านั้น (Firewall โดยปกติจะไม่ทำ user authentication และ Posture check)
- Client จะเข้าใช้งาน Server อื่น ๆ ได้ หลักจากต่อเชื่อไปยัง VPN Gateway สำเร็จแล้วเท่านั้น

คำถาม?