

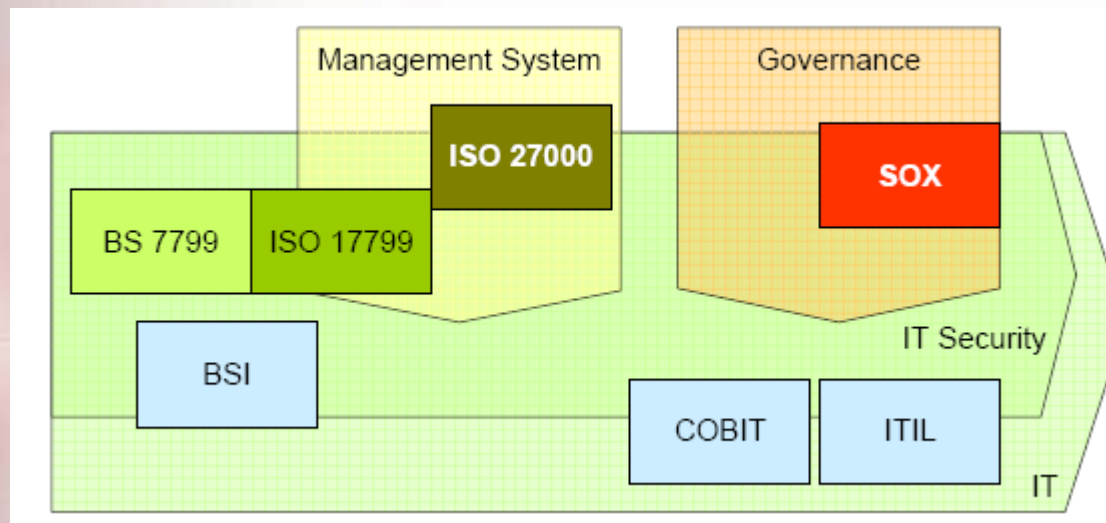
# Sécurité des accès aux réseaux locaux

*Limites de la technologie  
« Network Access Control »*

Serge Richard – Consultant Sécurité IBM GTS – CISSP®

- **Rappel des besoins en sécurité réseau**
- **Rappel de la technologie NAC**
- **Limites de la technologie NAC**
- **Exemples d'implémentation**

# Conformité avec les standards de sécurité



La technologie Network Access Control doit permettre :

- De limiter les accès aux ressources sur le réseau
- De fournir cheminement d'accès aux composants du réseau
- De fournir un inventaire des composants sur le réseau
- De fournir un rapport de conformité entre les différents composants réseau et l'utilisation de ces composants

## Conformité avec le standard X.805

- ✓ ITU-T Recommendation X.805 *Security architecture for systems providing end-to-end communications* had been developed by ITU-T SG 17 (ITU-T Lead Study Group on Telecommunication Security) and was published in October 2003.
- ✓ The group has developed a set of the well-recognized Recommendations on security. Among them are X.800 Series of Recommendations on security and X.509 – *Public-key and Attribute Certificate Frameworks*.

# ITU-T X.800 - Modèle de menace

**1 - Destruction** (an attack on availability):

- Destruction of information and/or network resources

**2 - Corruption** (an attack on integrity):

- Unauthorized tampering with an asset

**3 - Removal** (an attack on availability):

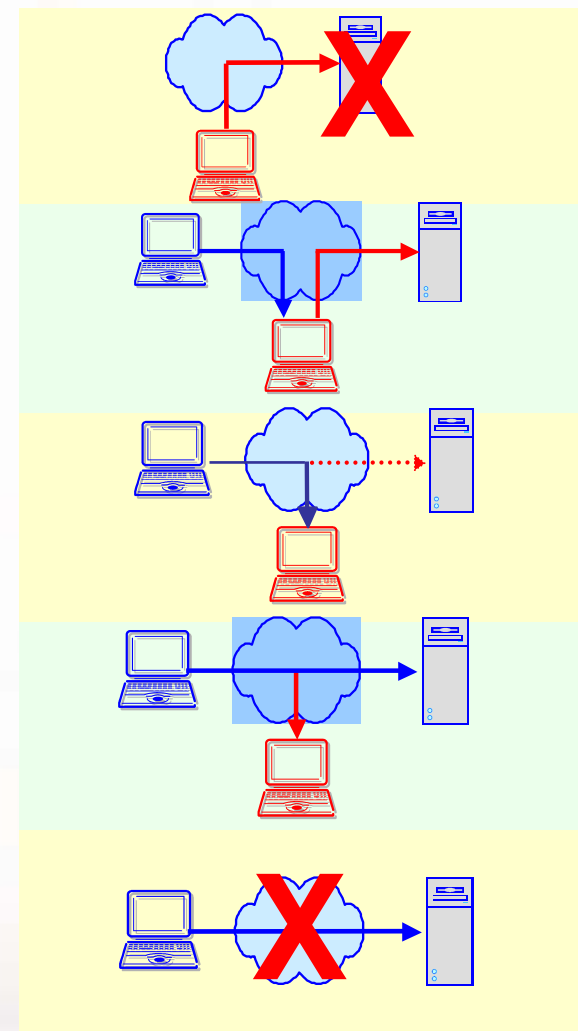
- Theft, removal or loss of information and/or other resources

**4 - Disclosure** (an attack on confidentiality):

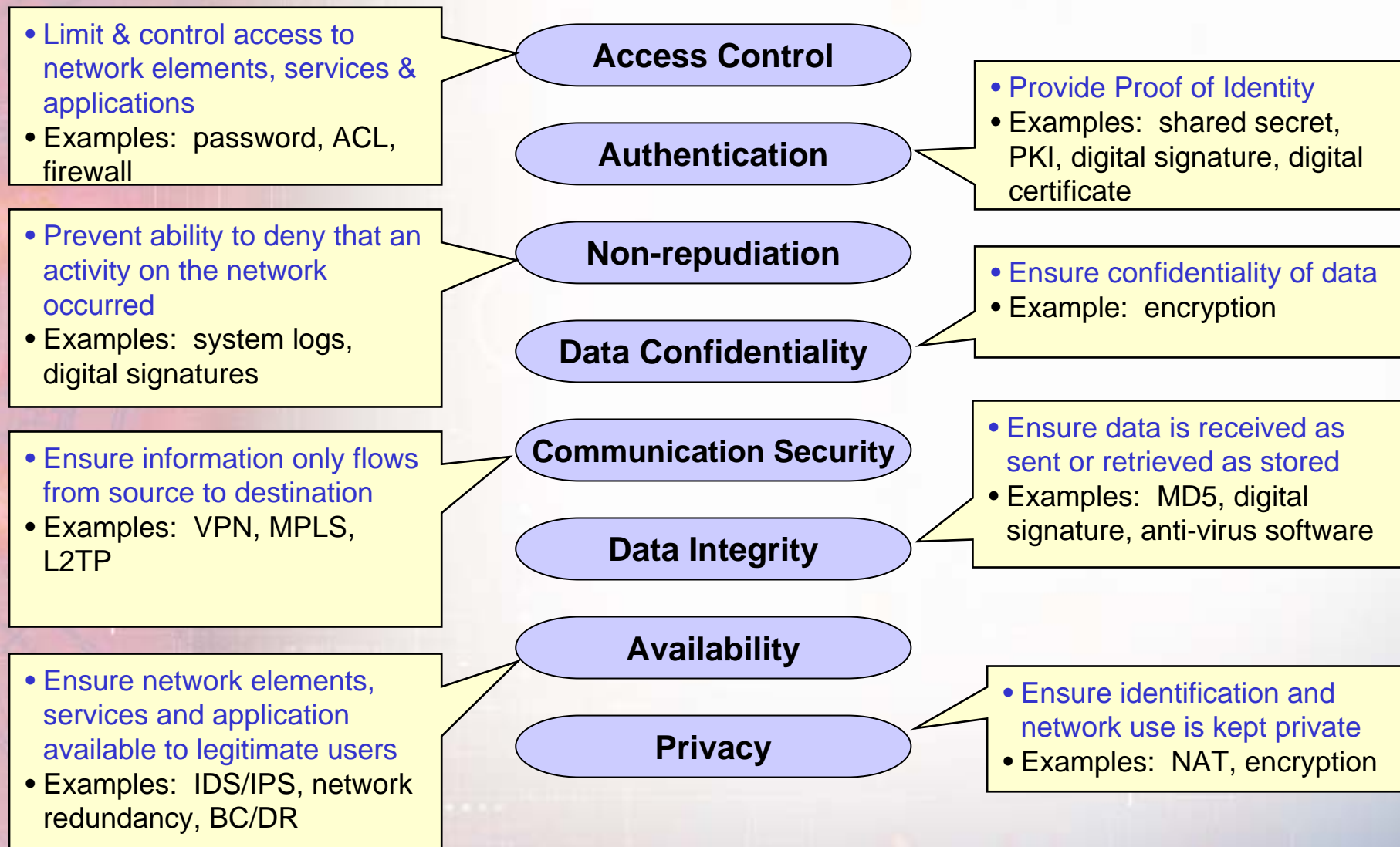
- Unauthorized access to an asset

**5 - Interruption** (an attack on availability):

- Interruption of services. Network becomes unavailable or unusable



## ITU-T X.800 – Les 8 niveaux de sécurité



# ITU-T X.800 – Corrélation niveaux et menaces

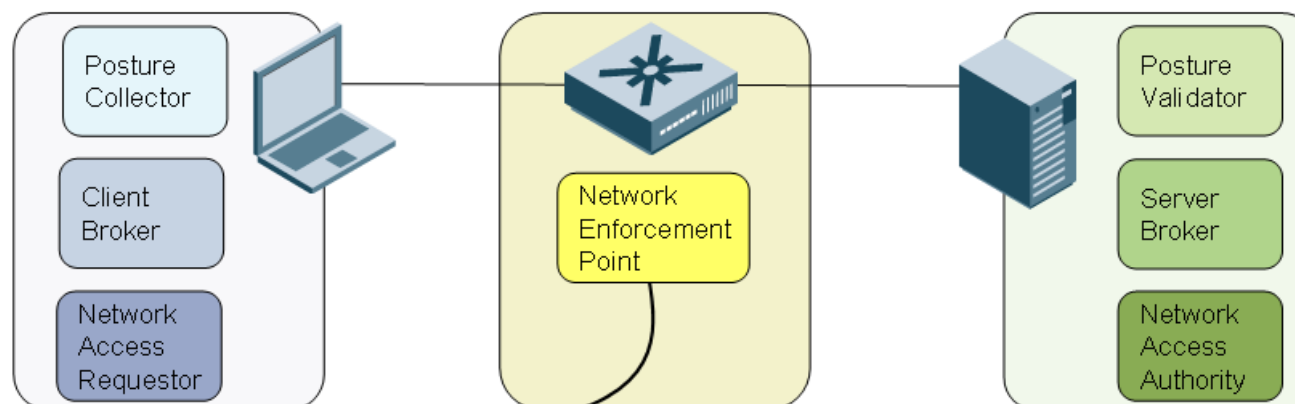


NAC

Security Dimension	X.800 Security Threats				
	Destruction	Corruption	Removal	Disclosure	Interruption
Access Control	✓	✓	✓	✓	
Authentication			✓	✓	
Non-Repudiation	✓	✓	✓	✓	✓
Data Confidentiality			✓	✓	
Communication Security			✓	✓	
Data Integrity	✓	✓			
Availability	✓				✓
Privacy				✓	

## Architecture de référence NAC

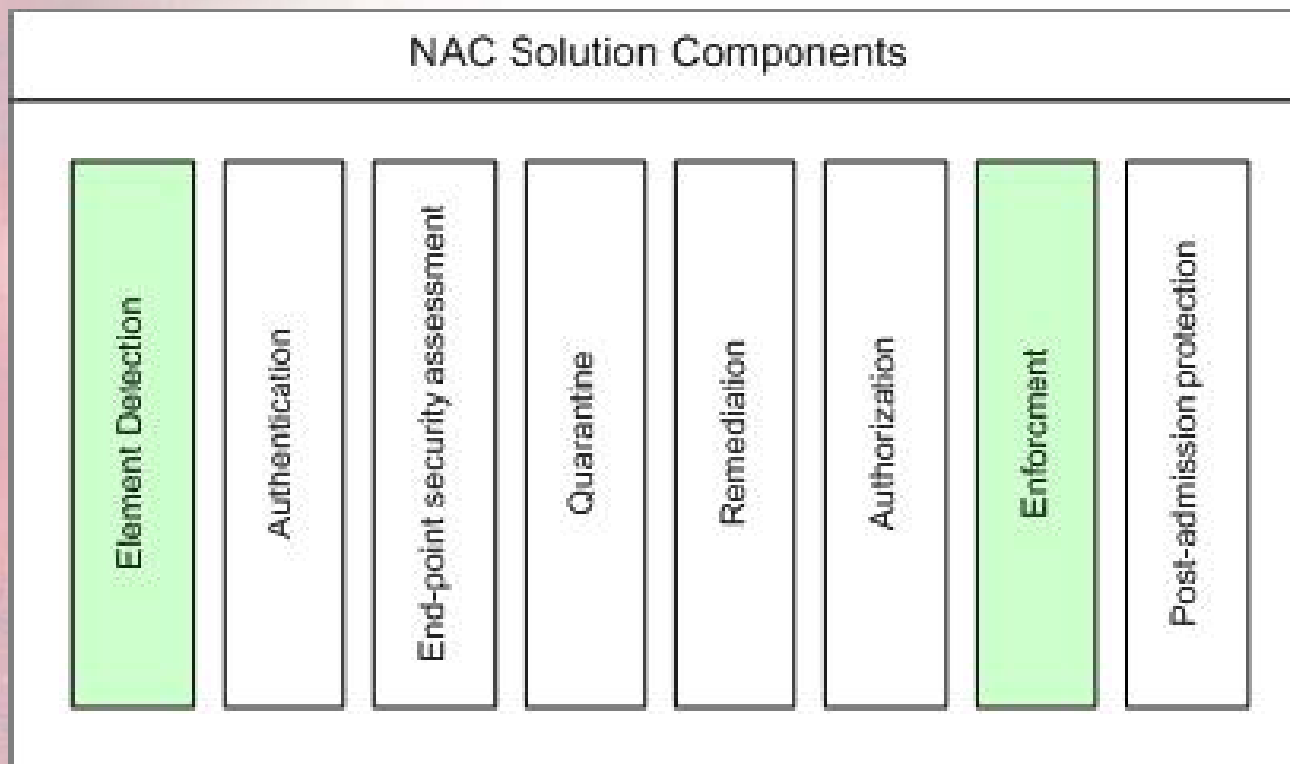
What is it?	TCG TNC	Microsoft NAP	Cisco NAC
<b>Posture Collector</b> Third-party software that runs on the client and collects information on security status and applications, such as 'is A/V enabled and up-to-date?'	Integrity Measurement Collector	System Health Agent	Posture Plug-in Applications
<b>Client Broker</b> "Middleware" that runs on the client and talks to the Posture Collectors, collecting their data, and passing it down to Network Access Requestor	TNC Client	NAP Agent	Cisco Trust Agent
<b>Network Access Requestor</b> Software that connects the client to network. Examples might be 802.1X supplicant or IPSec VPN client. Used to authenticate the user, but also as a conduit for Posture Collector data to make it to the other side	Network Access Requestor	NAP Enforcement Client	Cisco Trust Agent



IETF terms

What is it?	TCG TNC	Microsoft NAP	Cisco NAC
<b>Network Enforcement Point</b> Component within the network that enforces policy, typically an 802.1X-capable switch or WLAN, VPN gateway, or firewall.	Policy Enforcement Point	NAP Enforcement Server	Network Access Device
<b>Posture Validator</b> Third-party software that receives status information from Posture Collectors on clients and validates the status information against stated network policy, returning a status to the TNC Server	Integrity Measurement Verifier	System Health Validator	Policy Vendor Server
<b>Server Broker</b> "Middleware" acting as an interface between multiple Posture Validators and the Network Access Authority	TNC Server	NAP Administration Server	Access Control Server
<b>Network Access Authority</b> A server responsible for validating authentication and posture information and passing policy information back to the Network Enforcement Point.	Network Access Authority	Network Policy Server	Access Control Server

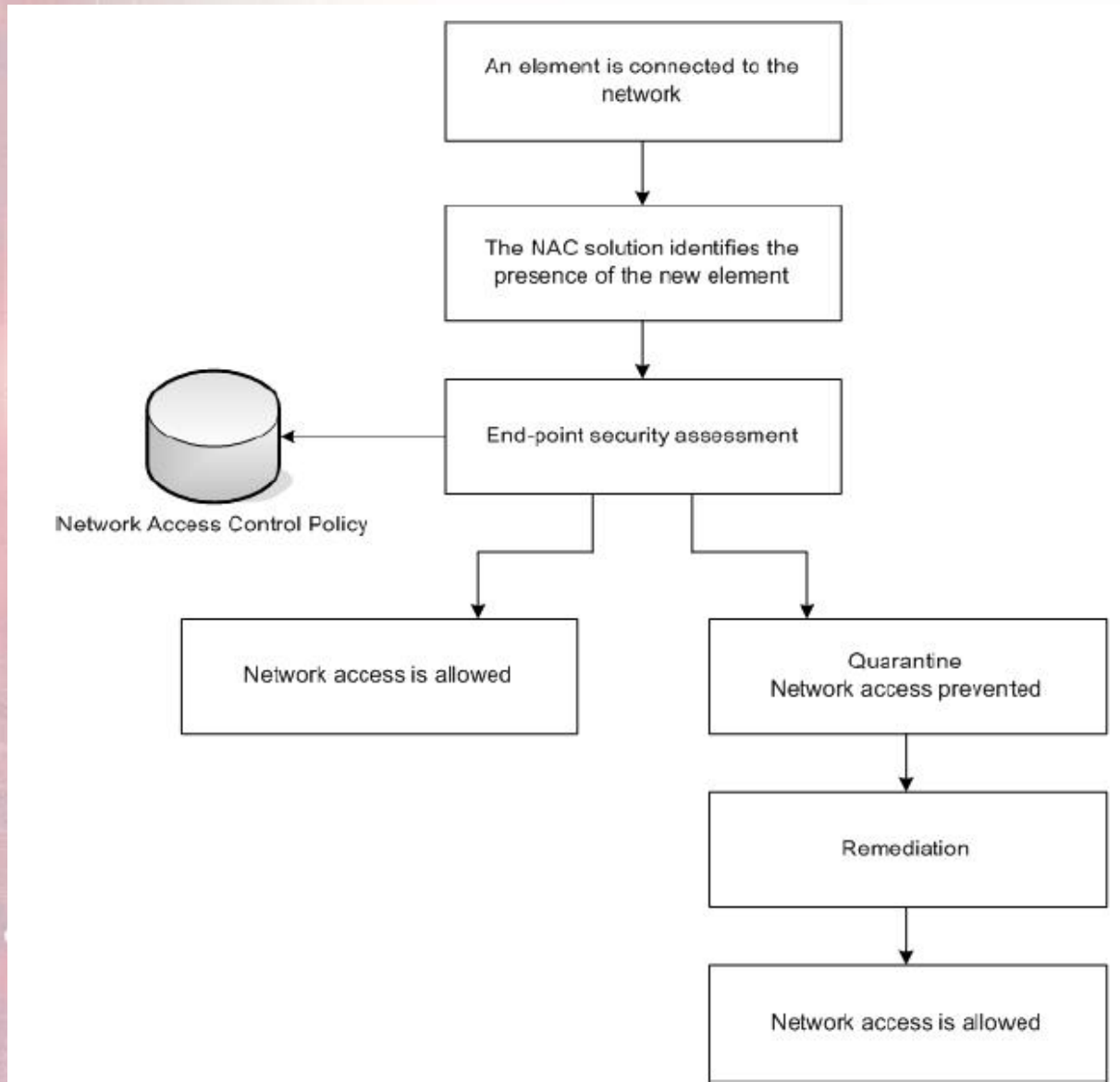
# Composants (éventuels) d'une solution NAC



# Description des composants

- ✓ **Détection d'élément** : Détecter de nouveaux composants qui se présente sur le réseau.
- ✓ **Authentification** : Authentification de chaque utilisateur accédant au réseau.
- ✓ **Évaluation de sécurité** : Evaluation d'un nouveau composant se présentant sur le réseau pour savoir si celui-ci est conforme au politique de sécurité de l'organisation.
- ✓ **Remédiation** : Mise en quarantaine d'un composant qui n'est pas conforme à la politique définie de sécurité jusqu'à ce qu'il devienne conforme.
- ✓ « **Enforcement** » : Restriction de l'accès pour composant au réseau si celui-ci n'est pas conforme au politique définie de sécurité.
- ✓ **Autorisation** : Vérification de l'accès aux ressources de réseau selon les niveaux d'autorisation définis dans un système de gestion d'autorisation (RBAC).
- ✓ **Protection Post-Admission** : Contrôle des composants en continu après une connexion au réseau.

# Cheminement d'un accès



# Comment détecter un nouveau composant

- ✓ **DHCP Proxy** : A NAC solution intercepts DHCP requests for network configuration information coming from elements operating on the network disclosing their presence.
- ✓ **Broadcast Listener** : A NAC solution listens to broadcast network traffic, such as ARP requests, DHCP requests, etc., generated by elements operating on the network disclosing their presence.
- ✓ **Listening to (sniffing) IP traffic** : IP packets passing through a certain monitoring location disclosing a certain element is connected to the network.
- ✓ **Client-Based Software** : Some NAC solutions make use of client-based software as part of the solution architecture, which is used to perform endpoint security assessment in order to prevent an element from obtaining network configuration information until it is evaluated and to notify a centralized management console the element is on the network.
- ✓ **SNMP Traps** : Some switches can be configured to send an SNMP trap when a new MAC address is registered with a certain switch port. The SNMP trap information details the MAC address and the network interface on which it was registered.

# Les vecteurs d'attaque

NAC solutions can be attacked using a variety of different attack vectors. These attack vectors can be divided into several categories based on the way each can compromise the operation of a NAC solution:

- ✓ **Architecture** : The architecture of a NAC solution is usually combined from various elements, each responsible for one or more NAC function. Analyzing the architecture of a NAC solution may reveal a design flaw allowing weakening the NAC solution or even bypassing it.
- ✓ **Technology** : A NAC solution uses various technologies in order to provide NAC functionality. Each of these technologies may contain a weakness, which may allow bypassing the NAC solution.
- ✓ **Components** : A NAC solution is combined from various components, such as servers, client-side software, etc. A vulnerability that may be present with one or more of these components may allow the component to be controlled, which may facilitate the bypassing the NAC solution.

# Attaques sur détection de composant

Usually, a NAC solution listens to network traffic (sniffing) trying to detect a new element operating on the network by analyzing network traffic generated by the element. Element detection can be performed by analyzing traffic at different TCP/IP layers:

- ✓ Layer 2 network traffic (i.e. an ARP request)
- ✓ Layer 3 network traffic (i.e. SYN request)
- ✓ Any network traffic

The following attacks are some examples:

- ✓ Element detection using DHCP proxy can be bypassed by assigning a static IP address.
- ✓ Element detection using a broadcast listener can be bypassed when an element is not generating broadcast network traffic.
- ✓ Element detection using a sniffer attached to a switch/router can be bypassed when elements communicate inside their network segment without sending their network traffic through the monitoring point.

# Limitations sur détection de composant

- ✓ **Masquerading and Virtualization** : The technology limitations that prevent NAC solutions from detecting a rogue element are connected to the network behind a device providing it network address translation (NAT) services and access to the network from an allowed element. Due to the fact the masquerading element is free to operate on the network without being detected by a NAC solution, virtualization solutions that provide NAT services should be a major concern for NAC solutions.
- ✓ **Managed vs. Unmanaged Elements** : After a NAC solution has learned about the existence of a new element, it may need to determine if the element complies with the security policy of the organization. In order to do this, a NAC solution may use a set of checks that may include the ability to gather knowledge regarding an element's operating system, the list of installed patches, the presence of anti-virus software and its virus signature date, etc. In order to perform endpoint security assessment, many NAC solutions require the installation of clientbased software. Such client-based software is usually available only for Microsoft Windows operating systems (Microsoft Windows 2000 and later versions).

# Limitations sur l'évaluation de sécurité

✓ **Checked Information** : Knowledge regarding an element's operating system, the list of installed patches, the presence of antivirus software and its virus signature date are usually gathered as part of an endpoint security assessment process. Organizations may not enroll a security patch as soon as it is released. The security patch is first tested and unless its installation will not cause any apparent damages, then and only then, is it installed. The matter of fact is that until this day many organizations still have not enrolled Microsoft Windows XP service pack 2. As a result and in many cases, the barrier of entry for an element for entering the network might be lower than the desired one.

✓ **Falsifying Checked Information** : In order to perform an endpoint security assessment, a NAC solution may use a set of checks that may include the ability to gather knowledge regarding an element's operating system, the list of installed patches, the presence of anti-virus software and its virus signature date, etc. The information a NAC solution assess is stored in a Microsoft Windows operating system's registry. Any user with administrative privileges can override these registry settings to represent a different, falsified set of values, allowing an attacker to introduce an element to the network even if it does not actually have any of the required software.

# Limites sur la rémédiation

When an element is isolated from the network, it is usually quarantined into a designated network, unable to access the enterprise network's resources. The following are different strategies that can be used when quarantining an element:

### ✓ Layer 3

- Placing an element into a quarantined network segment by assigning different network configuration information. Usually it is done by using an IP belonging to non-routable network segment or by using an ACL on routers in order to restrict the quarantined network segment's access.

### ✓ Layer 2

- Placing an element into a designated quarantined VLAN.
- Placing an element into a designated private VLAN (P-VLAN).
- ARP mitigation using ARP spoofing to redirect an element to a quarantine corridor, including the element and the NAC solution server, which is able to determine the endpoint security status of the element as well as to provide remediation services.

The following are examples of how a quarantine method can be bypassed.

- ✓ When an element is quarantined into a network segment by assigning the element a different set of network configuration information (through DHCP for example), changing the configuration with parameters belonging to an allowed network then permits the element to detach itself from the quarantined network and regain access to the main enterprise network.
- ✓ When ARP mitigation is used to redirect an element to communicate only with the NAC solution, it can be bypassed by statically defining ARP entries on a newly introduced element.

# Attaques sur la rémédiation

- ✓ When an element is isolated from the network, it is usually quarantined into a designated network without access to the resources of the organization. In most cases, all quarantined elements share the same isolated network.
- ✓ The elements placed in quarantine shares a common characteristic - they do not comply with the security policy of the organizations.
- ✓ As such, they may be vulnerable to a certain number of viruses, worms and/or vulnerabilities.
- ✓ If an infected element is placed into quarantine, it may infect other elements sharing the quarantine network.
- ✓ **Thus, the quarantine network opens a unique opportunity for an attacker.**

# Attaques sur la protection post-admission

✓ **Blinding Post-Admission Protection** : The goal of post-admission protection is to continuously monitor allowed users, elements and their sessions for suspicious activity, such as worms, viruses, malware, abnormality and so. If a suspicious activity is detected, the action taken by a NAC solution may vary from isolating the offending system to dropping the session.

Post-admission protection relies on the ability to observe traffic coming from and going to elements against which the NAC system operates. This is also its main drawback. If network communications from and/or to an element does not pass through the monitoring point of the NAC solution, it is unable not to draw conclusions if a certain violation or an abnormality had occurred.

Communications between elements found on the same network segment is an example of a communication type that is usually not observed. Another example is with elements connected to the same Layer 2 switch that may communicate with each other without the knowledge of the NAC solution.

Another drawback that needs to be considered is the usage of encryption. If used between elements operating on the enterprise network as a means to securely communicate, it will “blind” the NAC solution.

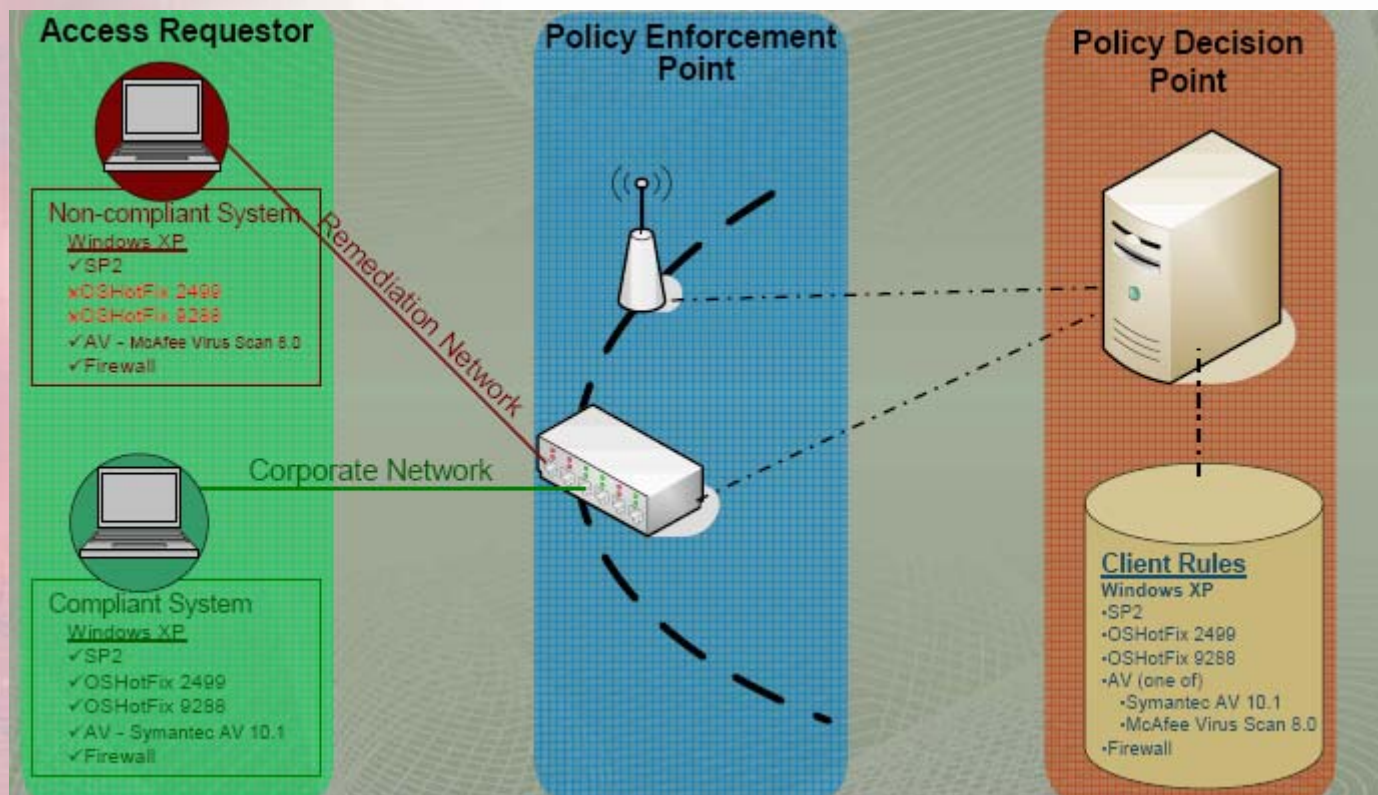
# Quand utiliser la technologie NAC ?



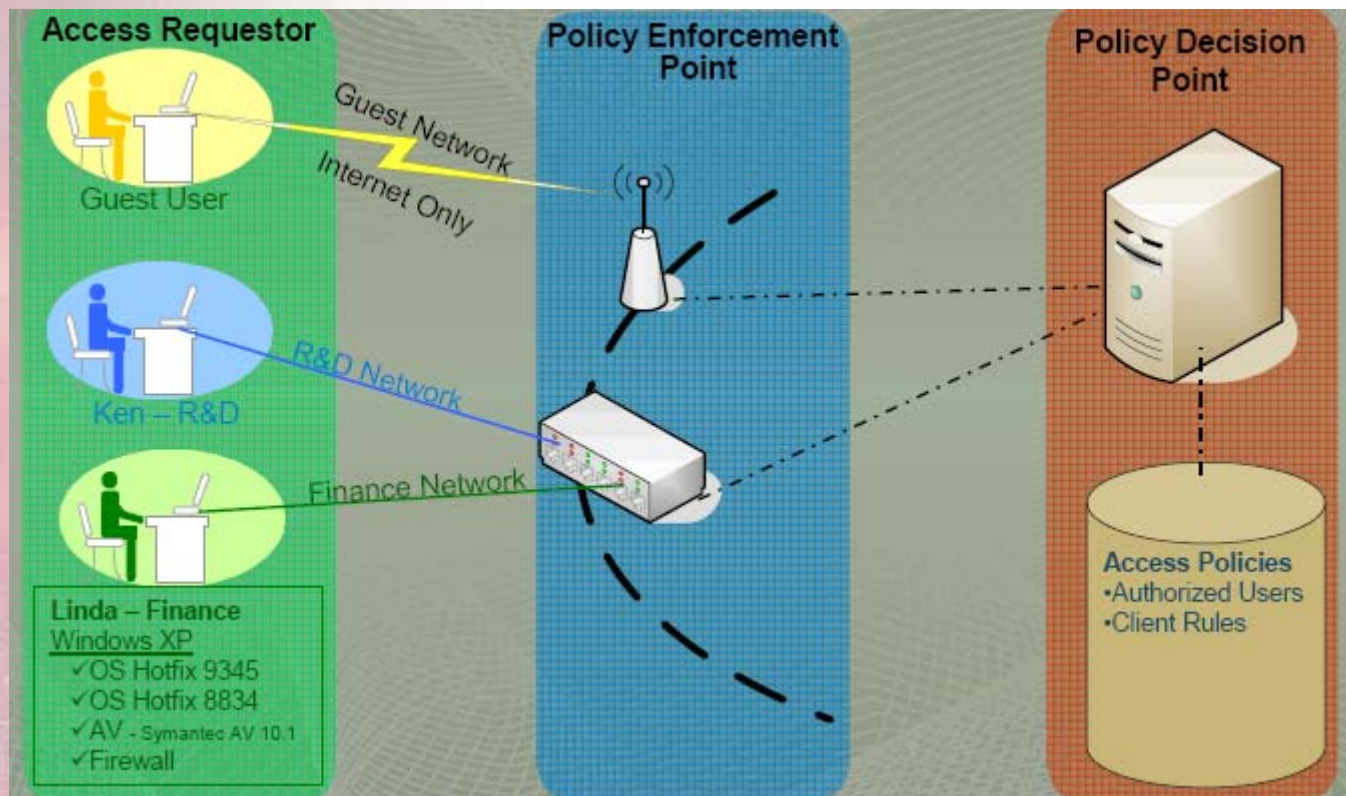
NAC peut être utilisé :

- Dans les laboratoires de recherche et développement (sites sensibles)
- Dans un réseau de station de travail
- Dans les salles de réunions
- Dans les salles d'accès libre
- Dans le cas d'une réorganisation ou de rachat

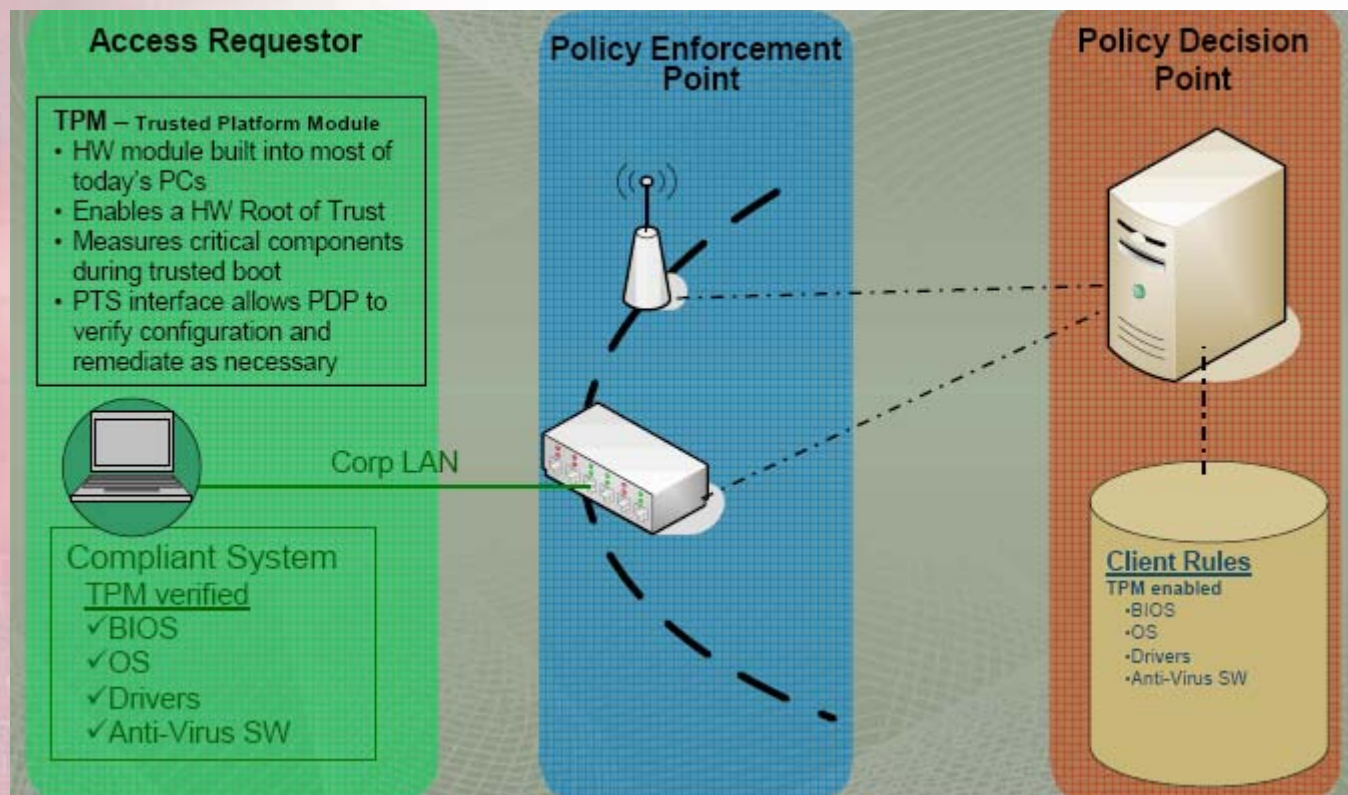
## Politique de sécurité profil entreprise



# Politique de sécurité profil utilisateur



## Politique de sécurité profil TPM



# Conclusion

- ✓ La technologie NAC, qui doit être une partie essentielle de la sécurité des réseaux, est toujours dans sa phase immature.
- ✓ Les solutions de NAC, qui visent à autoriser l'accès d'un composant à un réseau d'entreprise, n'ont pas la connaissance complète et précise concernant les mécanismes qu'elles doivent opérer.
- ✓ De plus , certaines des solutions de NAC peuvent être contournées, permettant ainsi à un attaquant d'accéder librement au réseau et à ses ressources.
- ✓ Une solution de NAC doit avoir la connaissance complète et précise concernant l'environnement ou elle opère (topologie, inventaire), détecter les changements, et réagir à ceux-ci en temps réel.

# Références

- ✓ Bypassing Network Access Control Systems by Insightix Ltd.
- ✓ Controlling Network Access and Endpoints by Trusted Computing Group
- ✓ Efficient and easy-to-use network access control and dynamic vlan management by Swisscom
- ✓ The Importance of Standards to Network Access Control by Juniper Networks, Inc.
- ✓ ITU-T Recommendation X.805 Security Architecture for Systems Providing End-to-End Communications by IETF

# **Merci de votre attention**

## **Questions / Réponses**