



## Réseau à capacité d'autodéfense Cisco



**Mai 2007**

# Self-Defending Network – Réseau à Capacité d'Autodéfense Cisco

“Le réseau peut identifier, s'adapter et répondre aux attaques”

Succursale

Les 3 piliers du SDN:

- Intégration
- Collaboration
- Réaction

MARS & CSM



PC avec client NAC

PC avec client 802.1x

CSA – Cisco Security Agent

“Distribution automatique des signatures”

Wan avec chiffrement

Routeur ISR

FW  
IPS  
VPN

Pare-feu

ASA  
FW  
VPN  
IPS  
Anti-X

Prévention d'Intrusion

NAC Appliance

Fonctions de Sécurité au niveau des commutateurs

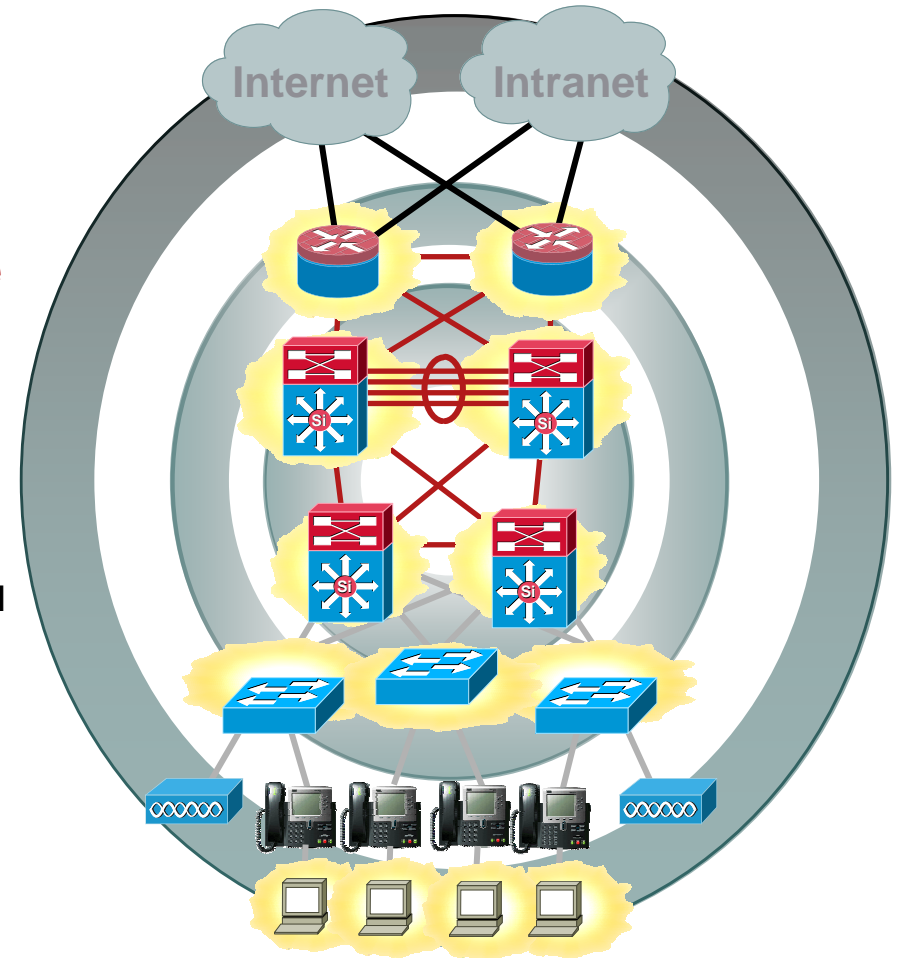
Serveurs

CSA

Serveurs Radius AAA

# Programme

- **Authentification**
  - ▲ Qui peut accéder le réseau
  - ▲ L'impact de la téléphonie
  - ▲ 802.1x, les visiteurs, Web Base Authentication
- La conformité des postes au moment de la connexion
  - ▲ Sur le LAN, en VPN, etc...
- Les bonnes pratiques pour le contrôle des usagers connectés au réseau
  - ▲ Fonctions de sécurité présentent dans les commutateurs Cisco
  - ▲ QoS déployée?
  - ▲ Cisco Sécurité Agent (CSA)
- La surveillance et la configuration du réseau



# IEEE 802.1x – filaire

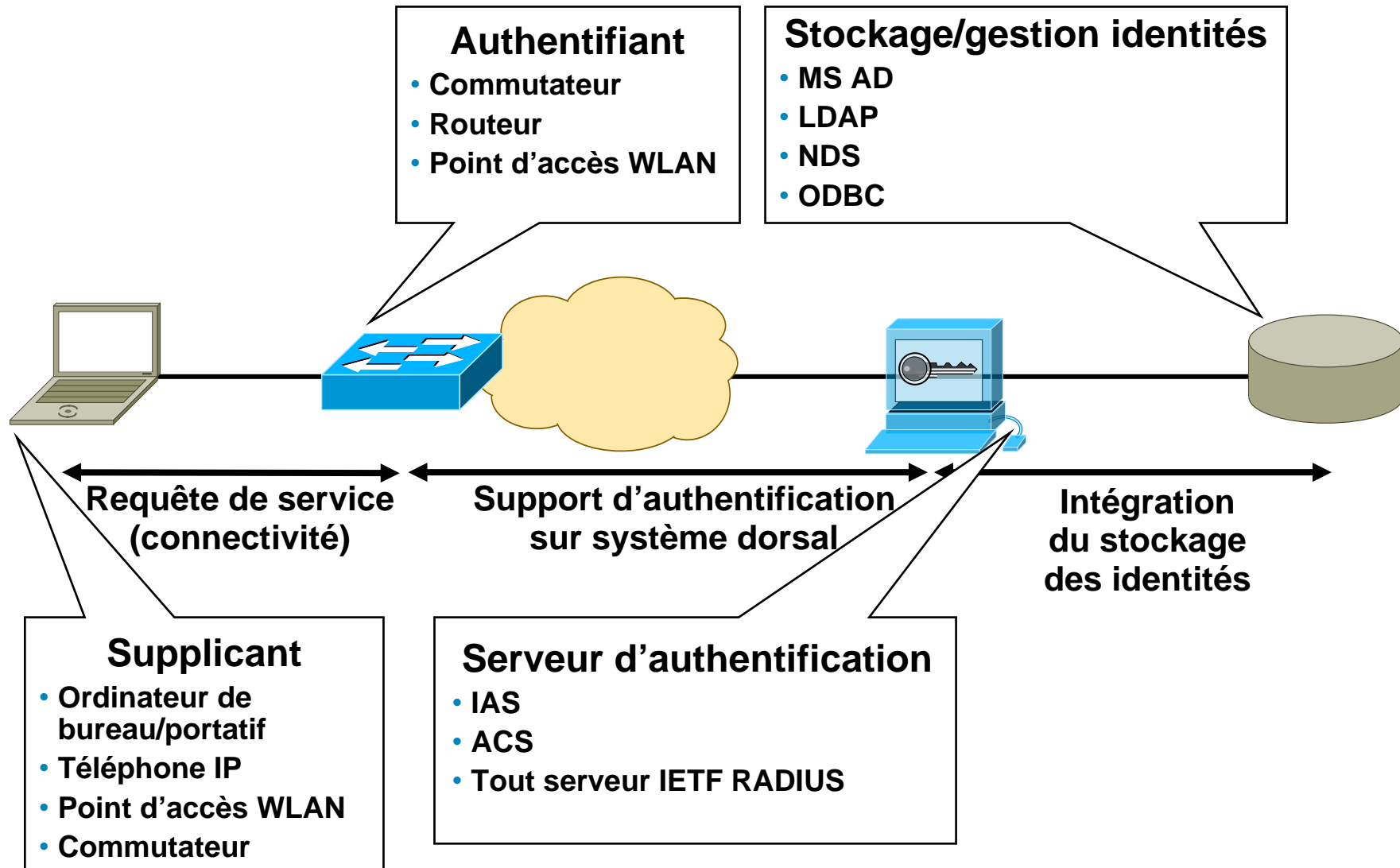
- Norme établie par le groupe de travail **IEEE 802.1**
- Structure conçue pour fournir **un contrôle des accès basé sur les ports** grâce à la fonction d'authentification
- 802.1x est avant tout une définition d'encapsulation pour EAP sur un support IEEE 802, et EAPOL (EAP sur réseau local) est le protocole clé
- **Protocole de couche 2** pour le transport de messages d'authentification (**EAP**) entre le supplicant (utilisateur/PC) et l'authentifiant (commutateur ou point d'accès)
- Assure une connexion sécurisée
- **La mise en application se fait en fait grâce à une surveillance de l'état des ports**



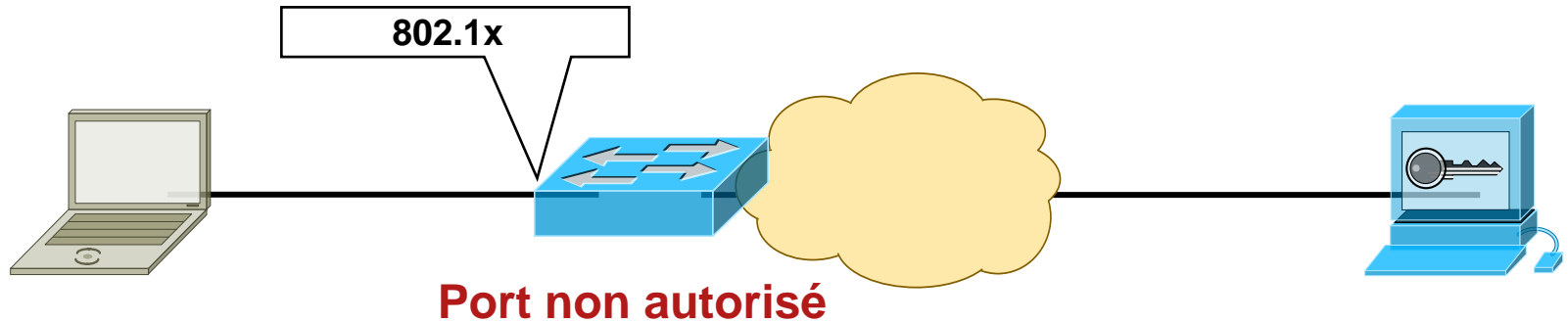
# Un peu de terminologie IEEE

Terme IEEE	Terme de tous les jours
Supplicant	Client
Authentifiant	Dispositif d'accès au réseau
Serveur d'authentification	Serveur AAA/RADIUS

# Modèle de contrôle des accès au port 802.1x



# Examinons de plus près :



## Cisco IOS

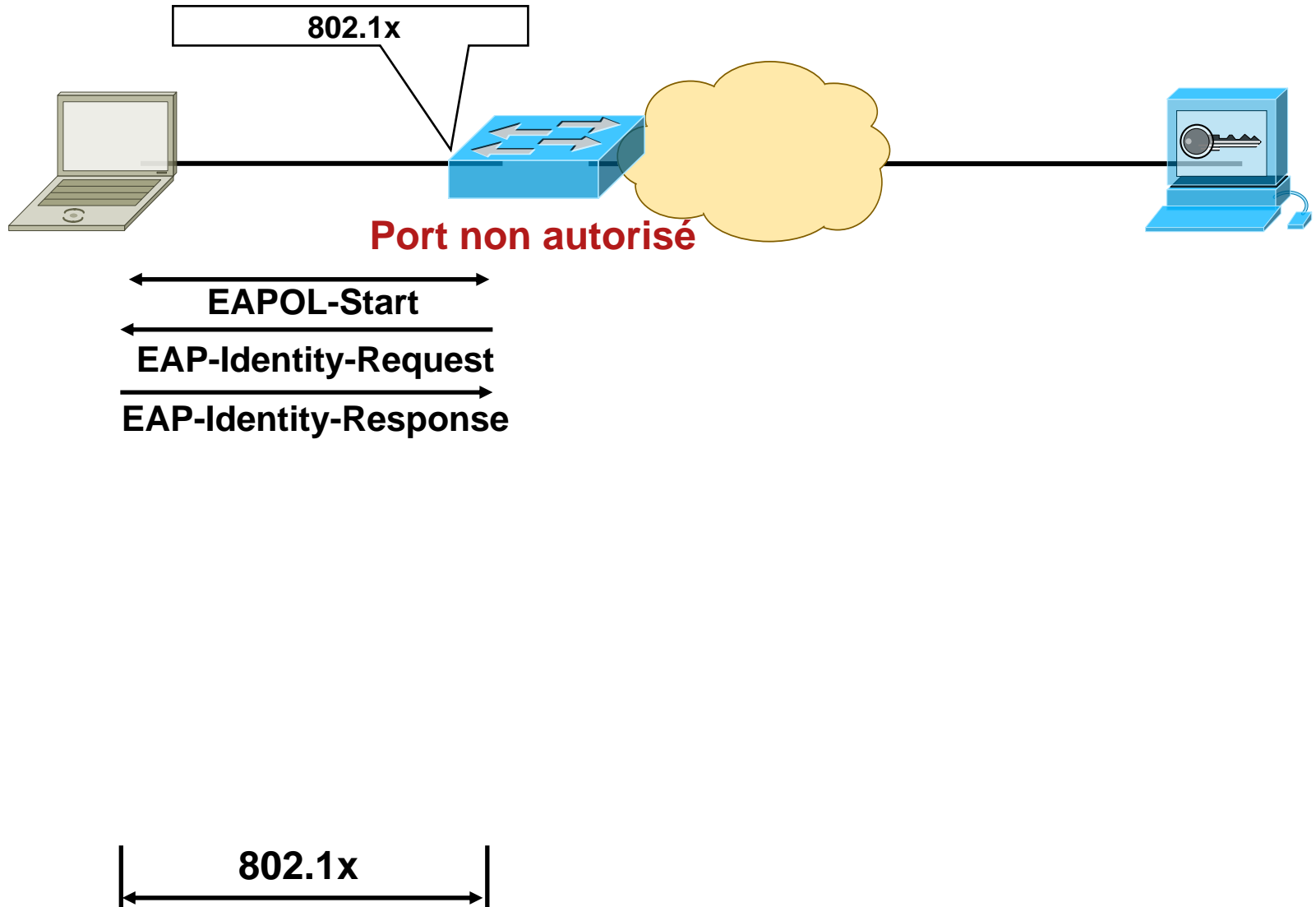
```
aaa authentication dot1x default group radius
aaa authorization network default group radius

radius-server host 10.100.100.100
radius-server key cisco123

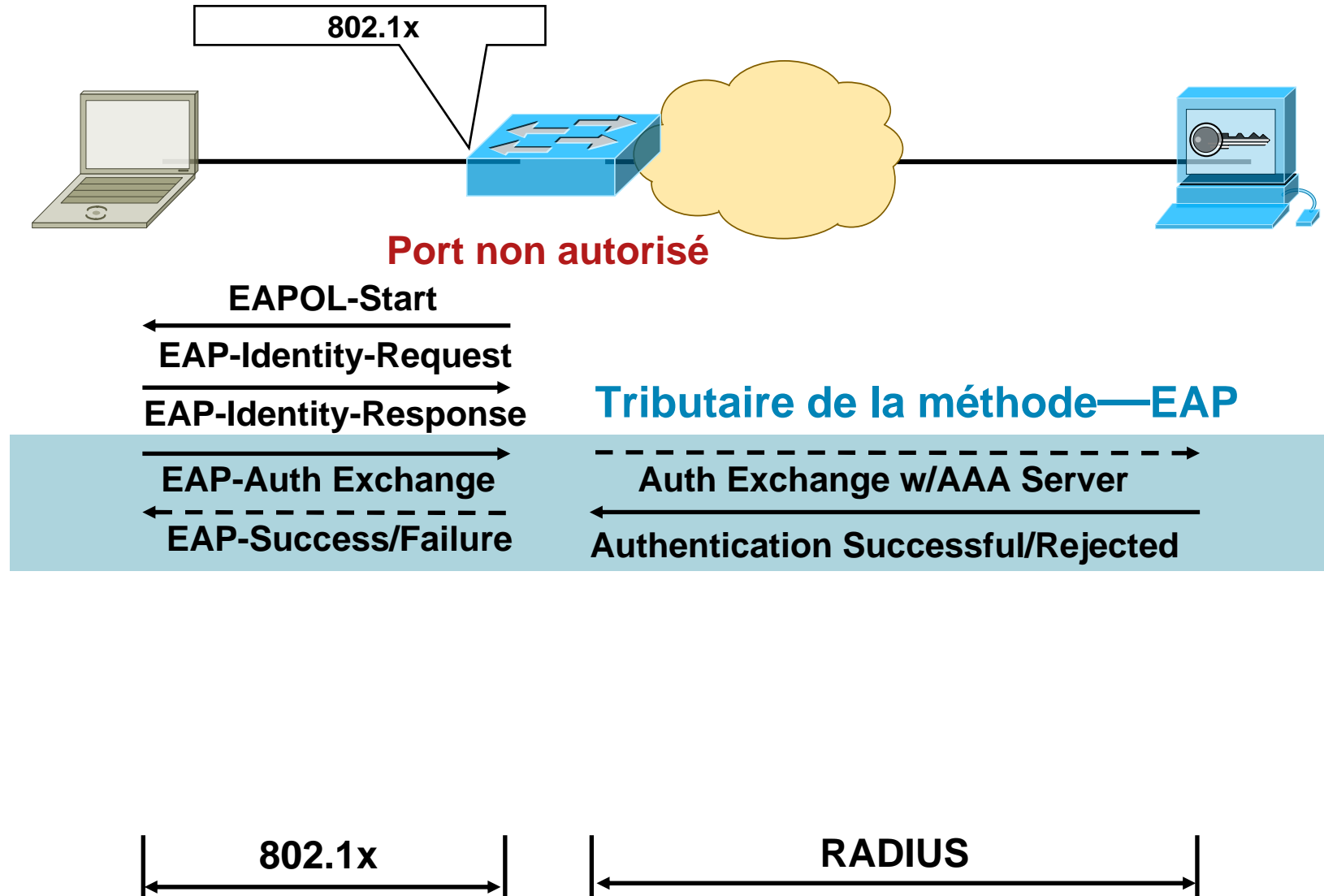
dot1x system-auth-control

interface GigabitEthernet1/0/1
dot1x port-control auto
```

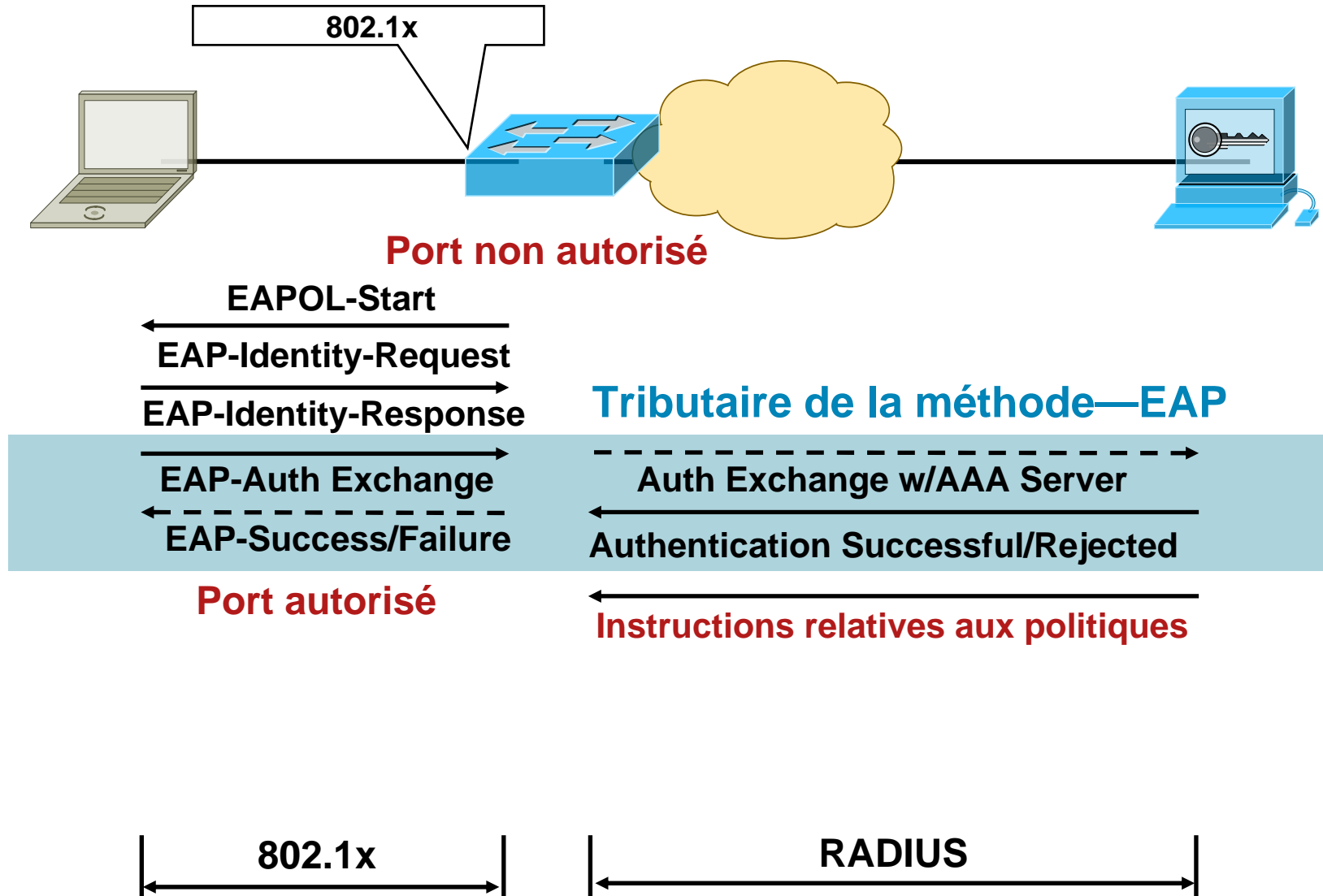
# Examinons de plus près :



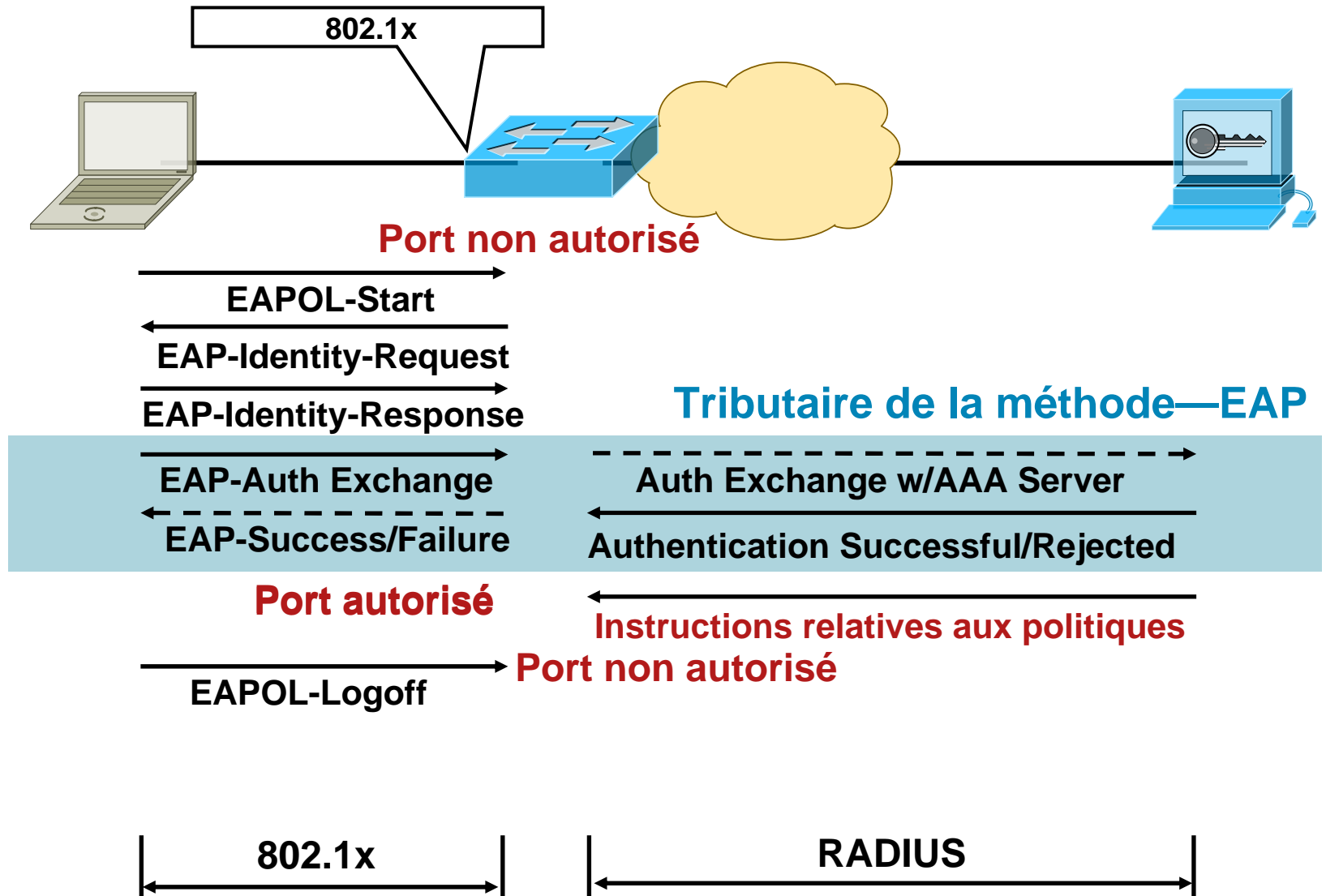
# Examinons de plus près :



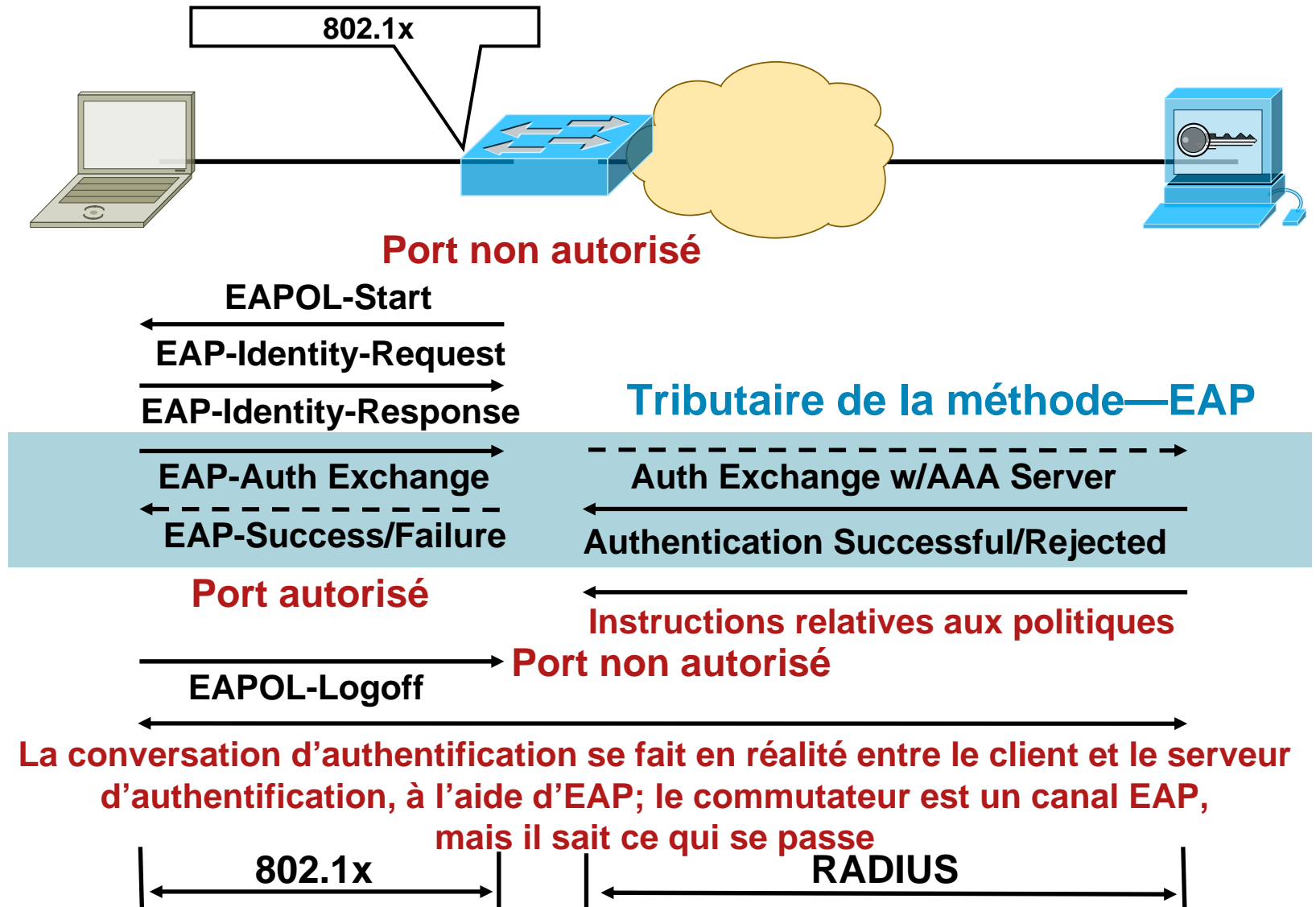
# Examinons de plus près :



# Examinons de plus près :



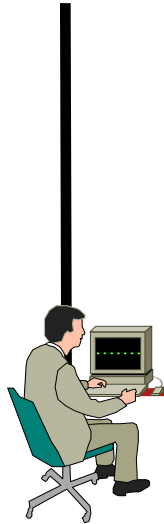
# Examinons de plus près :



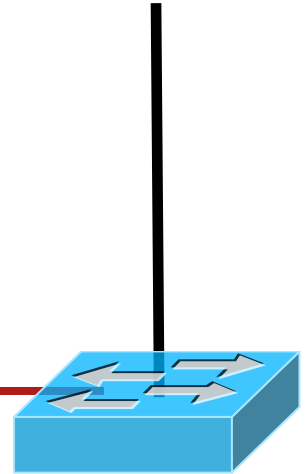


# 802.1x : opération par défaut

Aucun EAPOL



Processus 802.1x



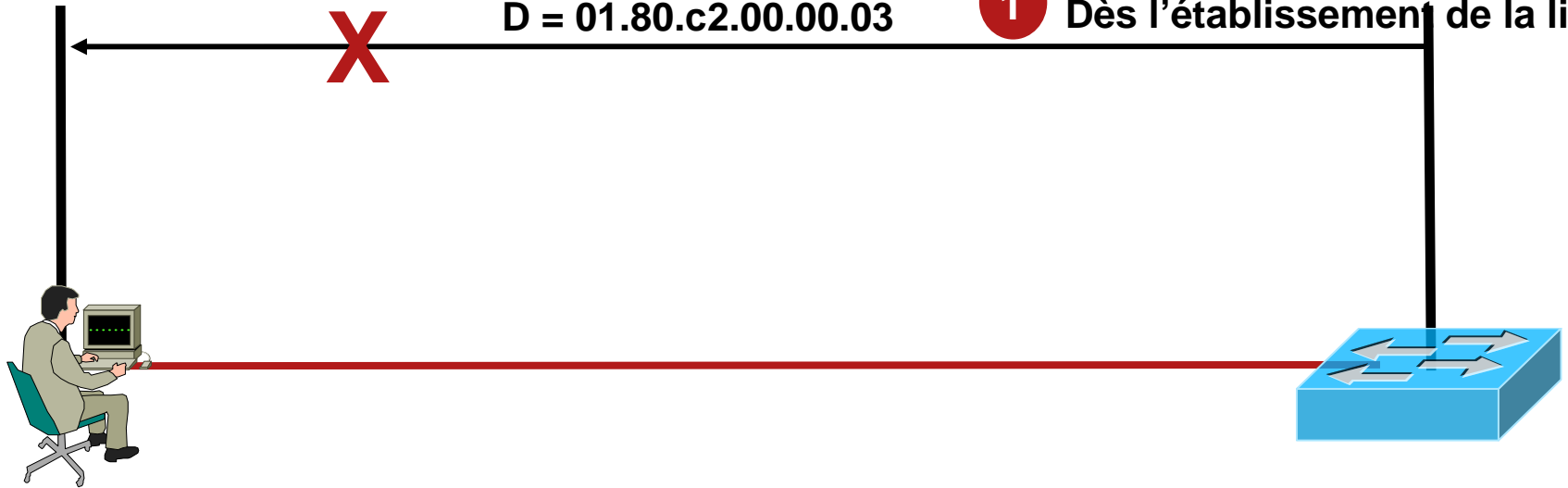
# 802.1x : opération par défaut

Aucun EAPOL

EAPOL-Request (Identity)  
D = 01.80.c2.00.00.03

1

Processus 802.1x  
Dès l'établissement de la liaison



# 802.1x : opération par défaut

Aucun EAPOL

X  
X

EAPOL-Request (Identity)

D = 01.80.c2.00.00.03

1

Processus 802.1x  
Dès l'établissement de la liaison

EAPOL-Request (Identity)

D = 01.80.c2.00.00.03

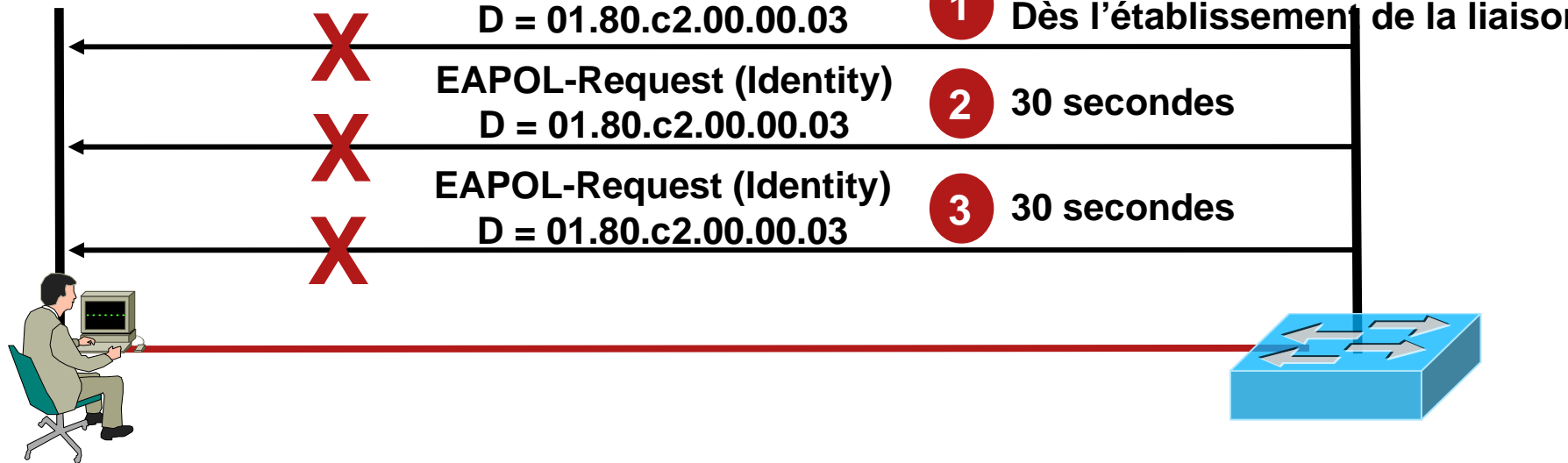
2

30 secondes

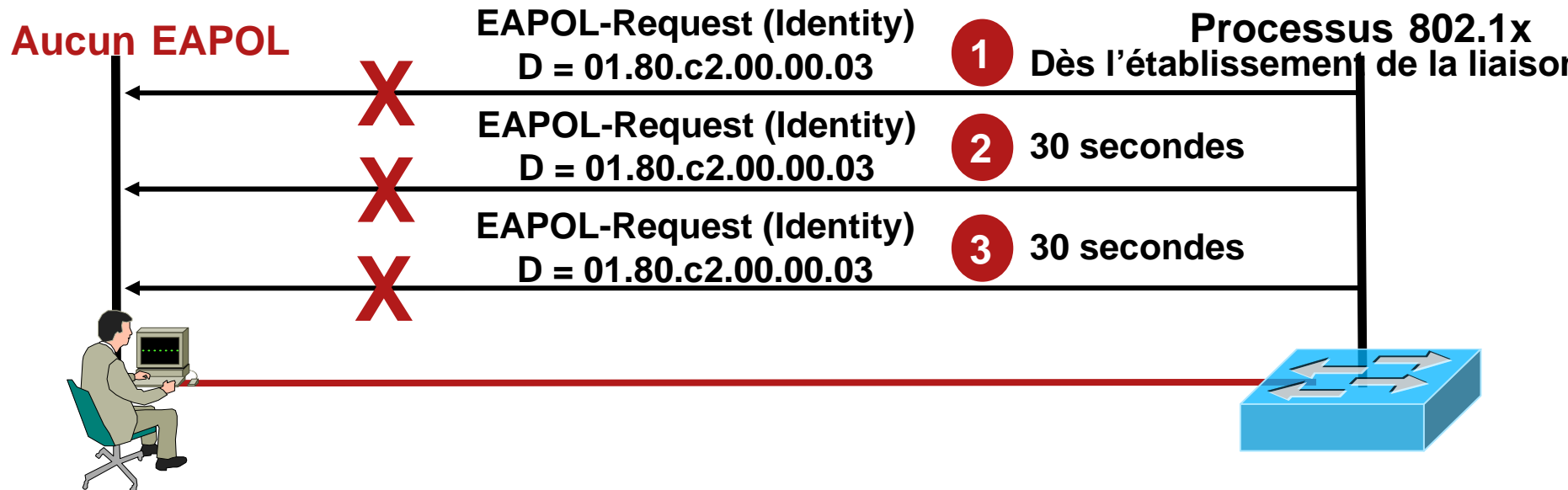


# 802.1x : opération par défaut

Aucun EAPOL



# 802.1x : opération par défaut « aucun supplicatant »



- Tout port de commutateur adapté à 802.1x enverra **des trames de requêtes d'identité EAPOL** sur le fil (qu'un supplicatant soit présent ou non)
- Le commutateur passe à la configuration par défaut « **aucun supplicatant** » sur le fil, s'il ne reçoit aucune réponse EAPOL à ses requêtes
- Aucun accès au réseau n'est accordé
- État transitoire; tout le processus redémarre après un temps de maintien
- Le processus peut redémarrer si un supplicatant apparaît sur le port

# 802.1x, avec Guest VLAN

- La temporisation par défaut est de 30 secondes, avec trois relances; la période de temporisation totale par défaut est de 90 secondes
- En l'absence de réponse aux trames de requêtes d'identité EAPOL du commutateur (que l'on peut considérer comme des dialogues d'accueil 802.1x) un dispositif est déployé sur le réseau Guest VLAN
- Aucune autre sécurité ou authentification à appliquer
- C'est comme si l'administrateur avait déconfiguré 802.1x et établi de force (hard-set) le port à un réseau VLAN déterminé
- Aucune machine qui parle le langage 802.1x (ou qui peut répondre au commutateur via EAPOL) ne devrait être placée sur le réseau Guest VLAN



# 802.1x, avec Guest VLAN

Aucun EAPOL



Processus 802.1x



# 802.1x, avec Guest VLAN

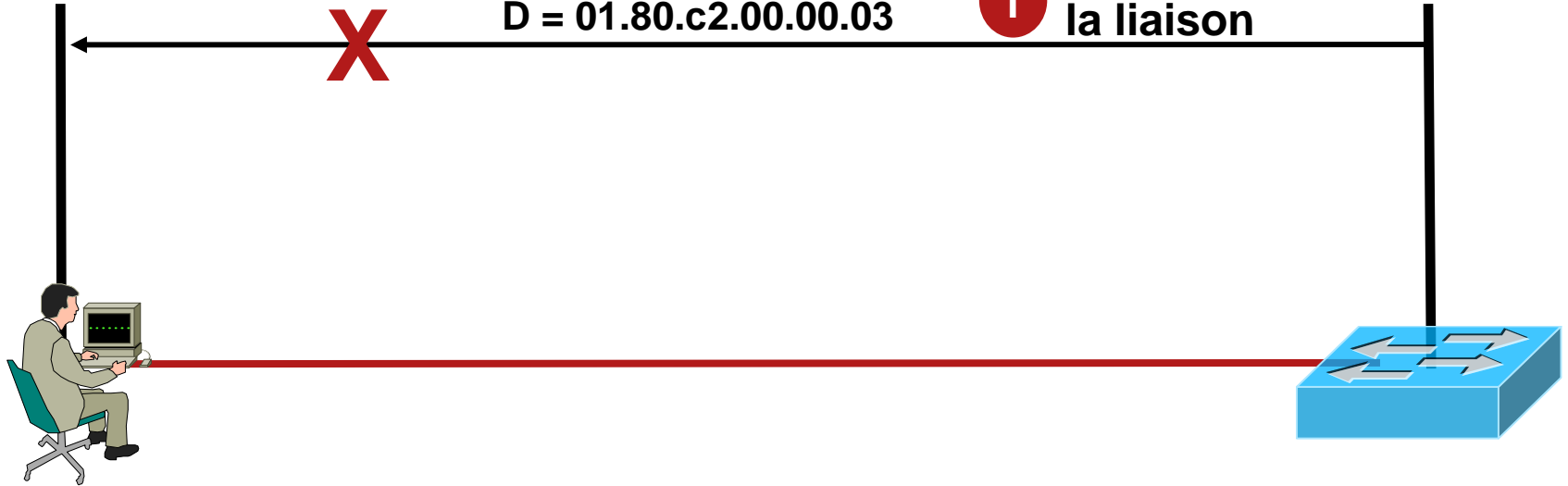
Aucun EAPOL

EAPOL-Request (Identity)  
D = 01.80.c2.00.00.03

1

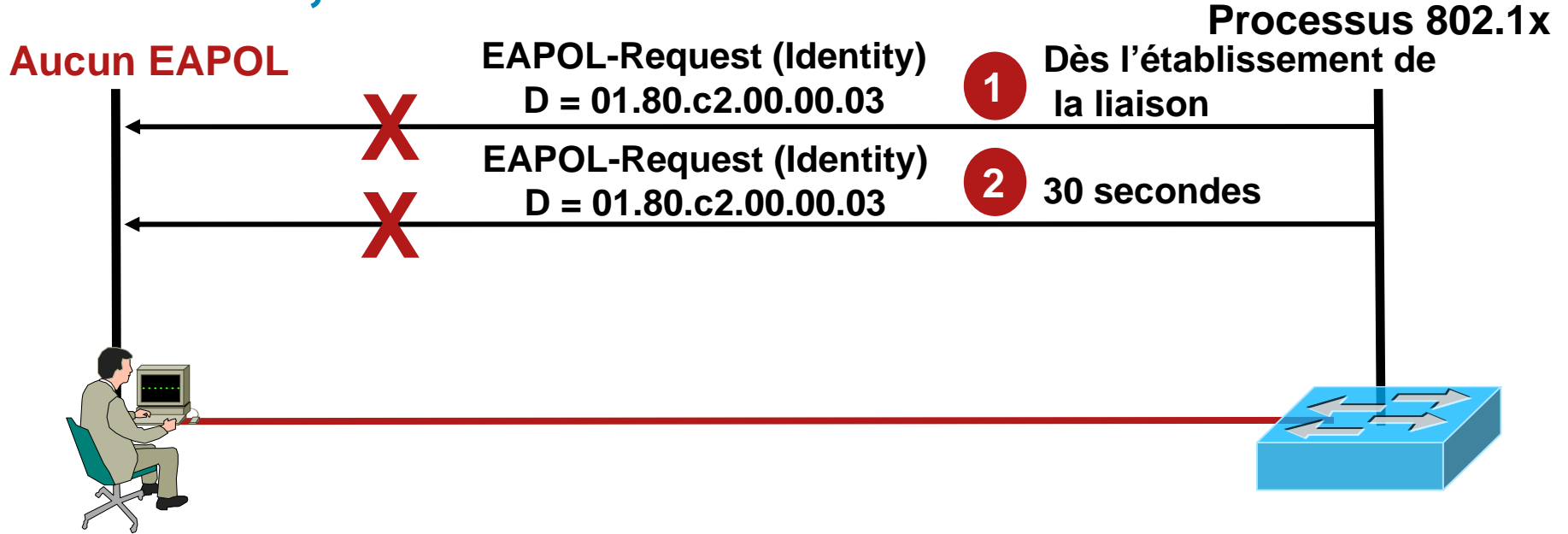
Dès l'établissement de  
la liaison

Processus 802.1x

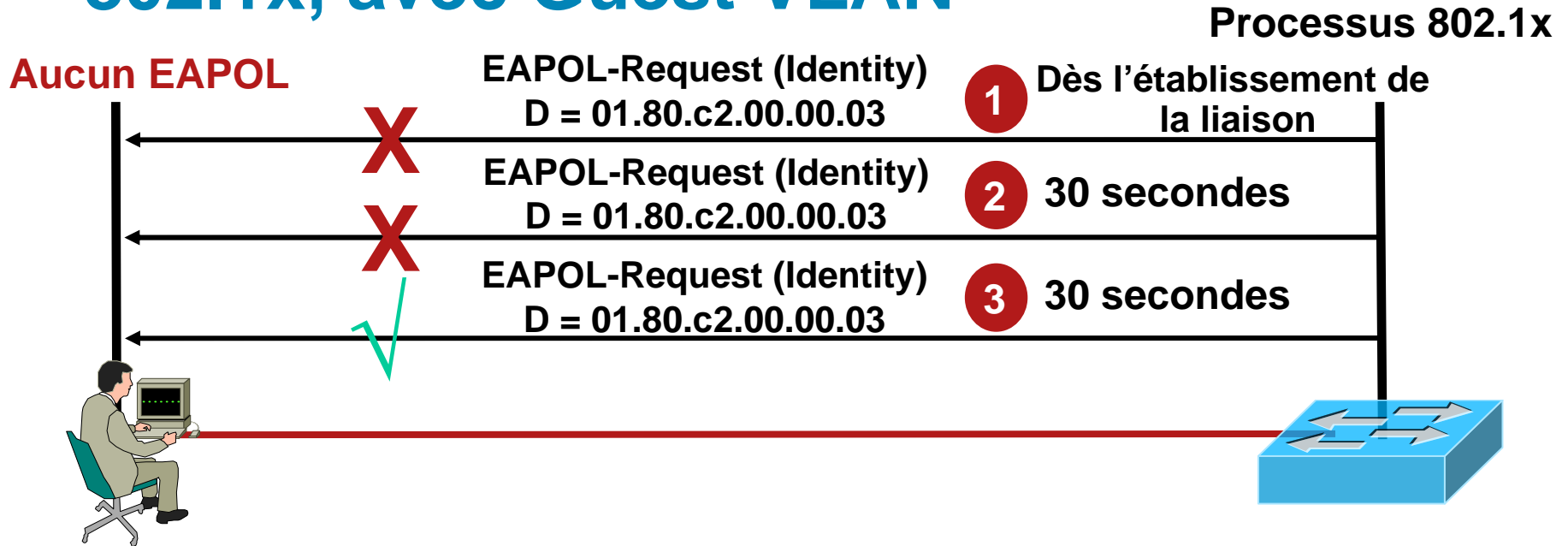




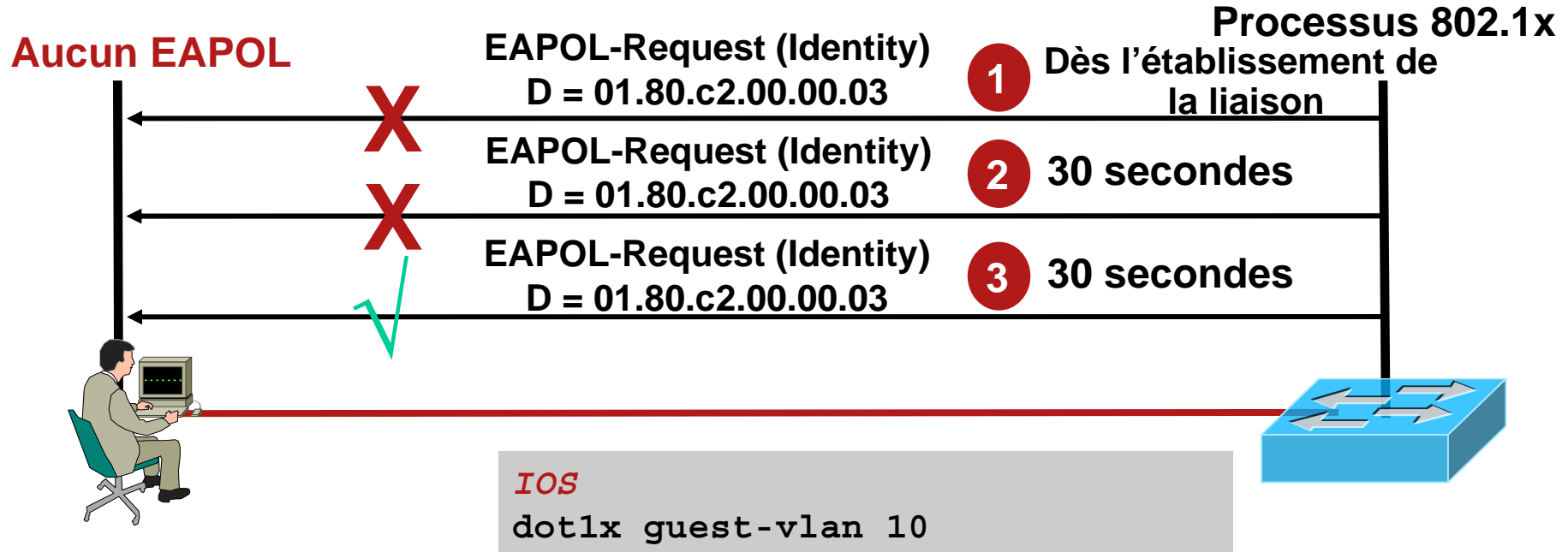
# 802.1x, avec Guest VLAN



# 802.1x, avec Guest VLAN

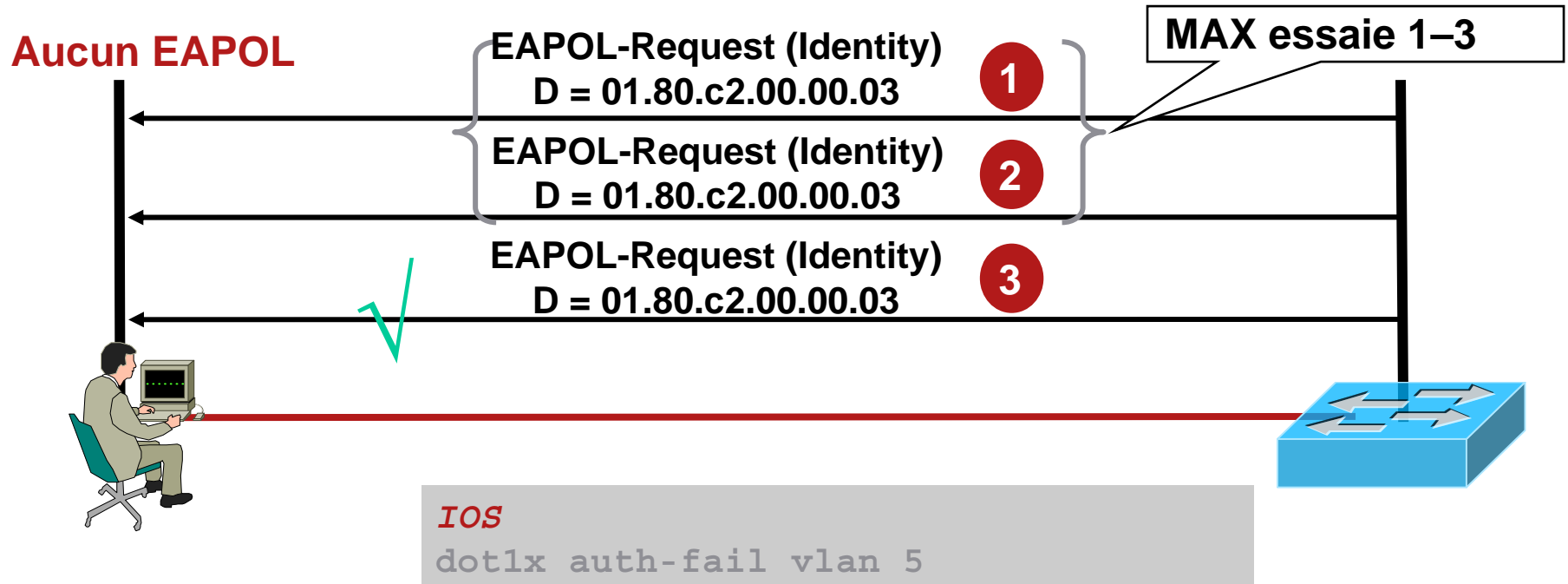


# 802.1x, avec Guest VLAN



- Tout port de commutateur adapté à 802.1x enverra **des trames de requêtes d'identité** sur le support (qu'un supplicatant soit présent ou non)
- Le port est déplacé au réseau **Guest VLAN** après l'étape 3 ci-dessus; au lieu de passer à **déconnecté**, le port passe immédiatement à l'état **autorisé**, et l'état auth-SM (state machine) est **authentifié**

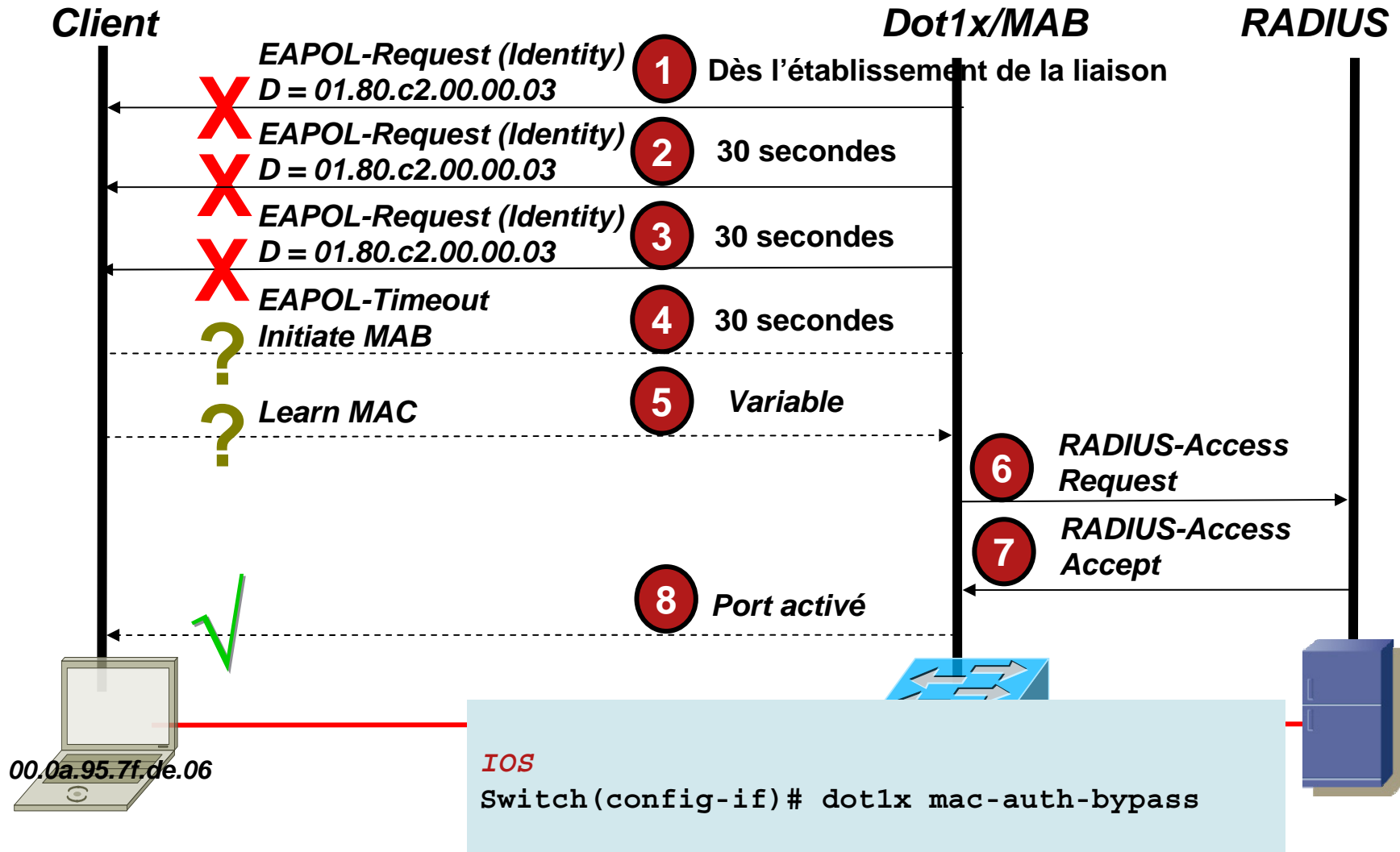
# 802.1x, avec Auth Fail VLAN - Le client échoue l'authentification.



- Tout port de commutateur adapté à **802.1x** enverra des trames de requêtes d'identité sur le support (qu'un supplican soit présent ou non)
- Le port est déplacé au réseau auth fail VLAN après l'étape 3 ci-dessus; au lieu de passer à **déconnecté**, le port passe immédiatement à l'état **autorisé**, et l'état auth-SM est **authentifié**
- Exige un comportement de supplican approprié

- DEMO OF 802.1x

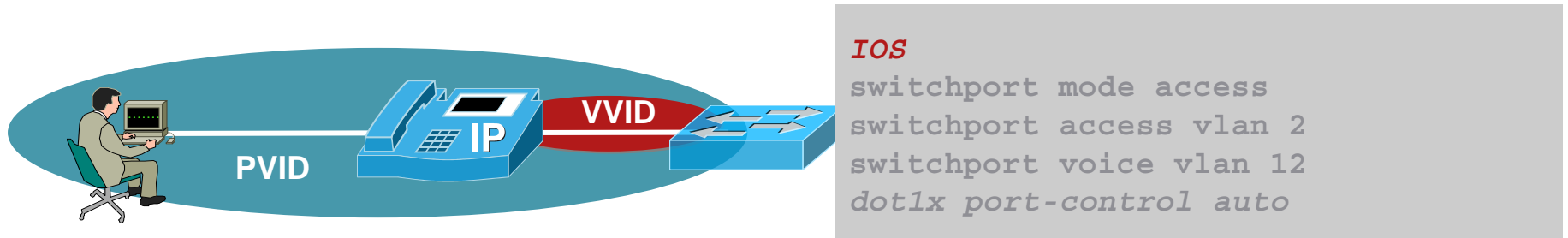
# MAC Authentication Bypass (MAB)



# ■ DEMO OF MAB ?

# 802.1x, avec VVID - VoIP

- Accès **non-authentifié** au réseau VLAN de voix (VVID)
- Accès **authentifié** au réseau VLAN de données (PVID)
- Cela permet à 802.1x et à VoIP de coexister simultanément



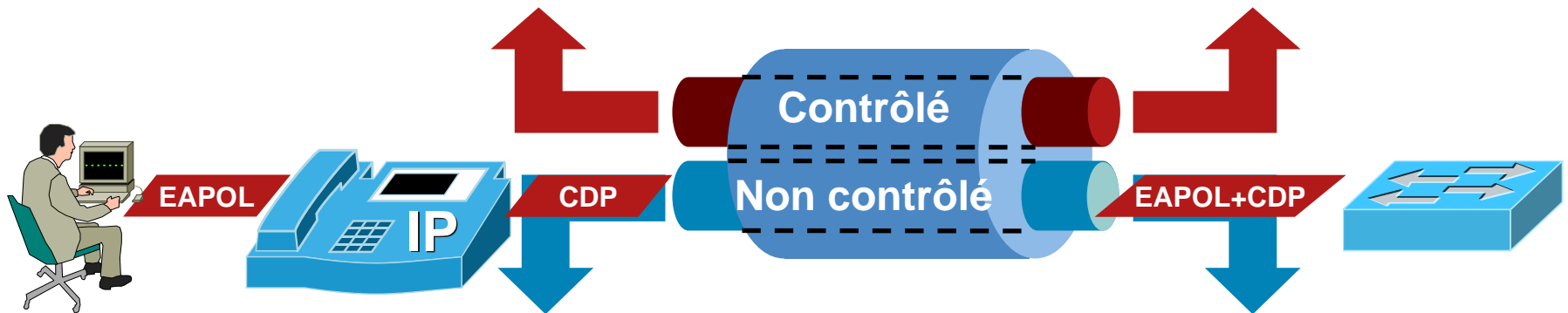
- Le PC doit être authentifié avant d'obtenir l'accès au réseau VLAN de données
- Le téléphone IP (sans mise en œuvre de supplicant dot1x) peut obtenir l'accès au réseau VLAN vocal après avoir envoyé les paquets CDP appropriés, peu importe l'état du port dot1x



# 802.1x, avec VVID - VoIP

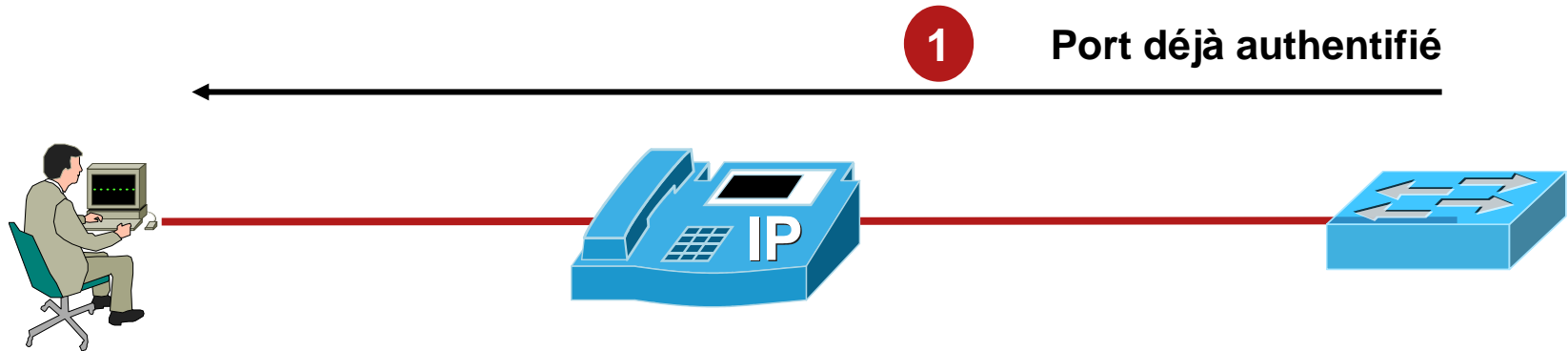
Pour chaque port de commutateur 802.1x, le commutateur crée **deux** points d'accès virtuels

Le port contrôlé est uniquement ouvert lorsque le dispositif qui lui est connecté a été autorisé par 802.1x



Un port non contrôlé fournit un chemin au protocole EAPOL (Extensible Authentication Protocol over LAN) **et** au trafic CDP **seulement**

# 802.1x, avec VVID : limitations antérieures



# 802.1x , avec VoIP : limitations antérieures

Si un utilisateur final se déconnecte, le port demeure autorisé par 802.1x

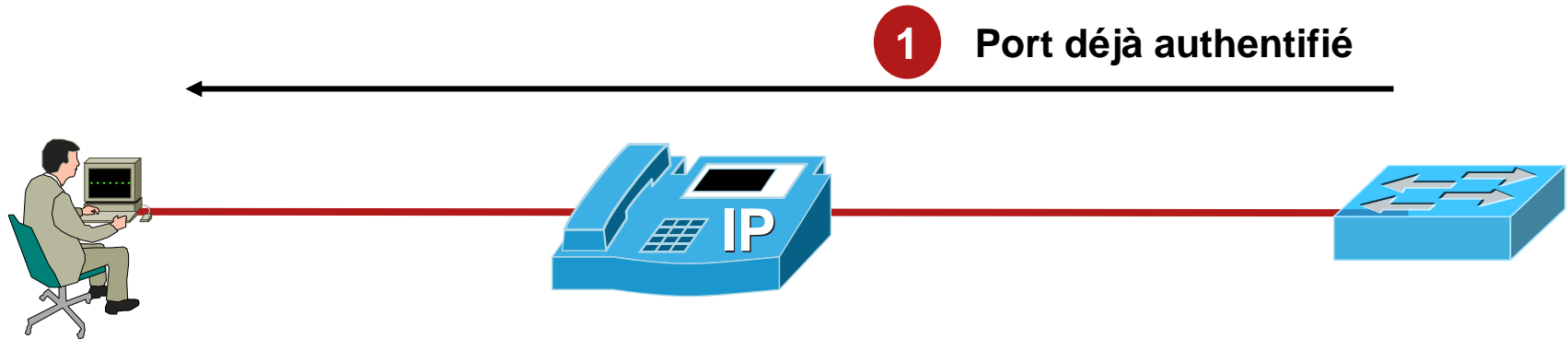


# 802.1x, avec VoIP : limitations antérieures



- Un **utilisateur illégitime** peut maintenant obtenir l'accès au port en usurpant l'adresse MAC authentifiée et contourner complètement 802.1x—**cela constitue une faille dans la sécurité**
- En tentant de contourner cette situation, certains clients ont activé une réauthentification périodique des dispositifs limités (end-devices)
- Cela ne constitue pas une bonne raison pour activer une réauthentification
- Nous devons admettre que n'importe quelle machine peut disparaître du réseau sans que le commutateur (et 802.1x) s'en aperçoive de façon explicite (c'est-à-dire que la liaison ne tombe pas en panne)

# 802.1x, avec VVID : limitations antérieures



# 802.1x, avec VVID : limitations antérieures

Si un utilisateur final se déconnecte, le port demeure autorisé par 802.1x

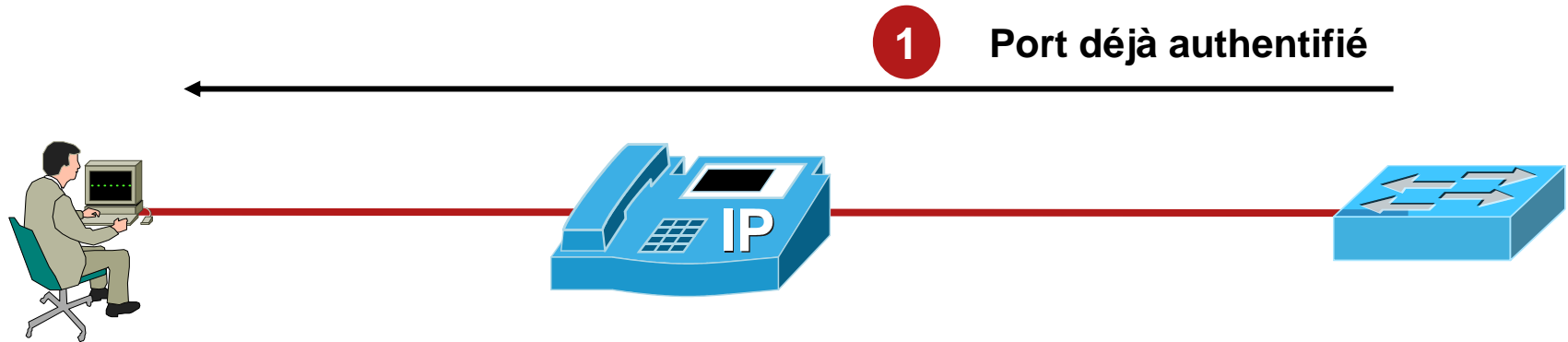


# 802.1x, avec VVID : limitations antérieures



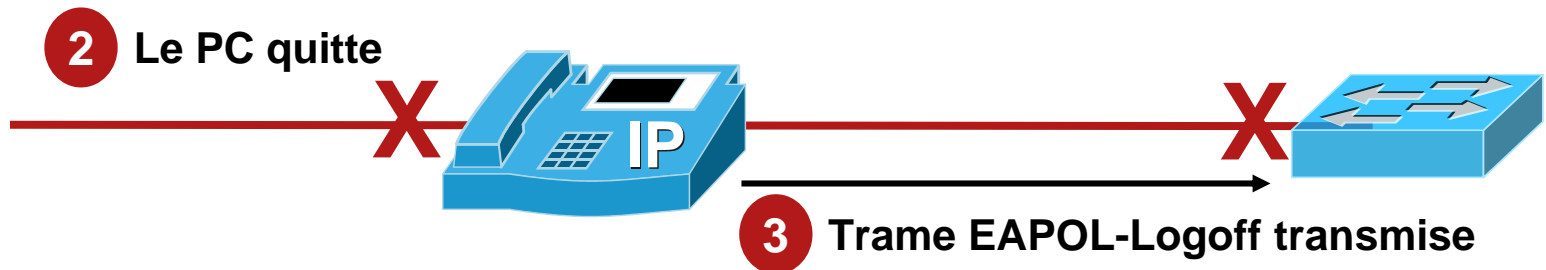
- Un utilisateur légitime peut maintenant tenter d'obtenir l'accès au port, par l'intermédiaire de 802.1x
- Cependant, si l'on présume que les adresses MAC sont différentes, le commutateur pourrait considérer cela comme une violation de la sécurité
- En tentant de contourner cette situation, certains clients ont activé une réauthentification périodique des dispositifs limités (end-devices)
- Cela ne constitue pas une bonne raison pour activer une réauthentification
- De façon générale, le problème est le même que celui vu sur les diapositives précédentes

# 802.1x, avec VVID : EAPOL-Logoff





# 802.1x, avec VoIP : EAPOL-Logoff



- Si un utilisateur se déconnecte, un téléphone IP transmet une trame EAPOL-logoff au commutateur

SA = PC MAC address

DA = 01-80-C2-00-00-03 (PAE group address)

- Le téléphone doit effectuer deux fonctions de base:

–Surveiller l’adresse de groupe **PAE** (Port Access Entity) (state machine dans le commutateur) pour déterminer l’état du supplicat

–Transmettre la trame EAPOL-logoff

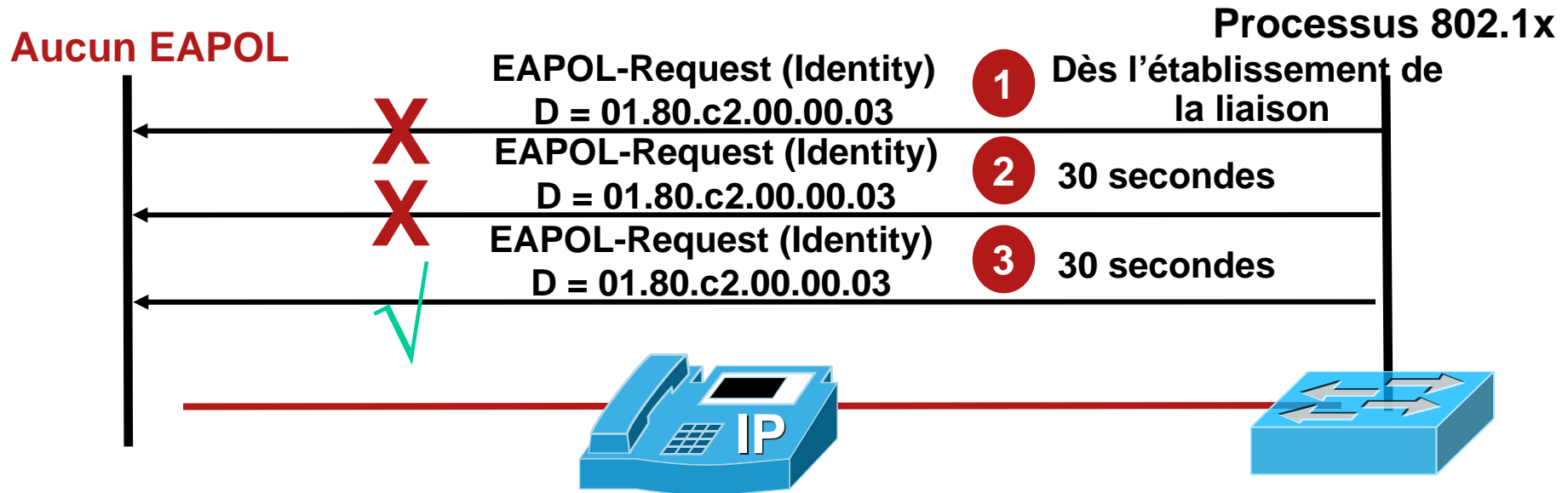
# 802.1x, avec VVID : EAPOL-Logoff



## 4 Nouvelle session authentifiée

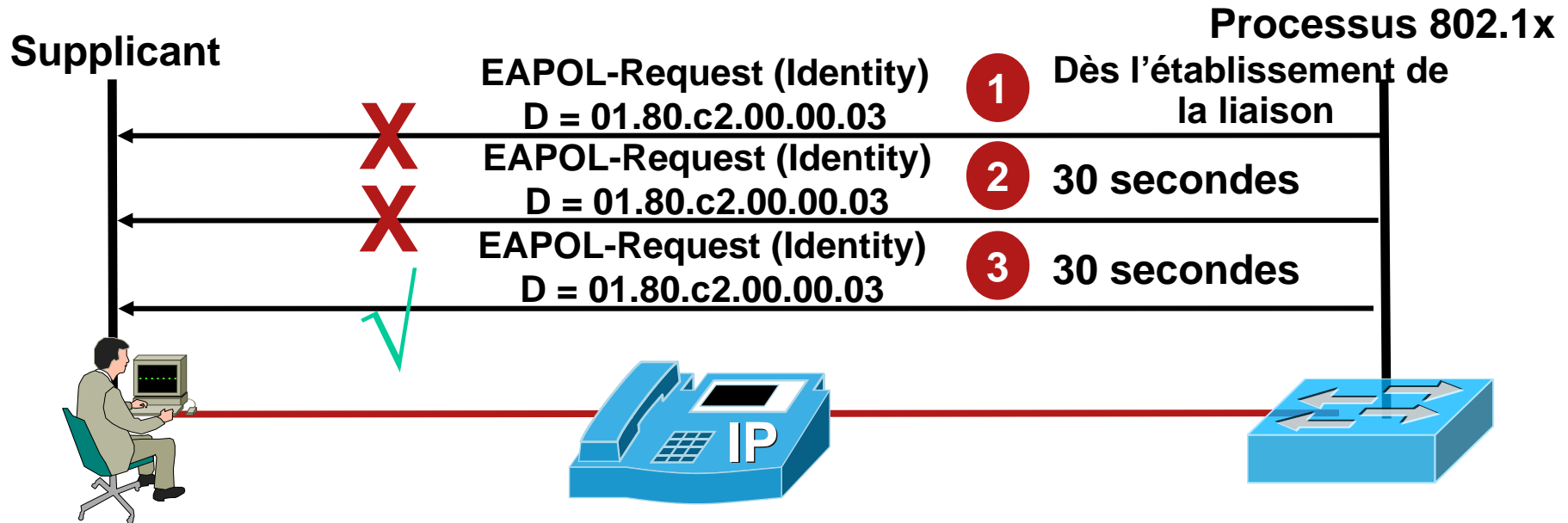
- Le commutateur pense que c'est une trame EAPOL-logoff standard transmise par un supplicant, qui indique une fin de service
- Cela met fin à la faiblesse de sécurité actuelle et permet ensuite la mobilité des postes

# 802.1x, avec VVID : problématiques de déploiement



- Présument qu'il n'y a aucun supplicatant sur le câble, un port sera déployé sur le réseau Guest VLAN après avoir passé l'étape 3 ci-dessus, si Guest VLAN est configuré

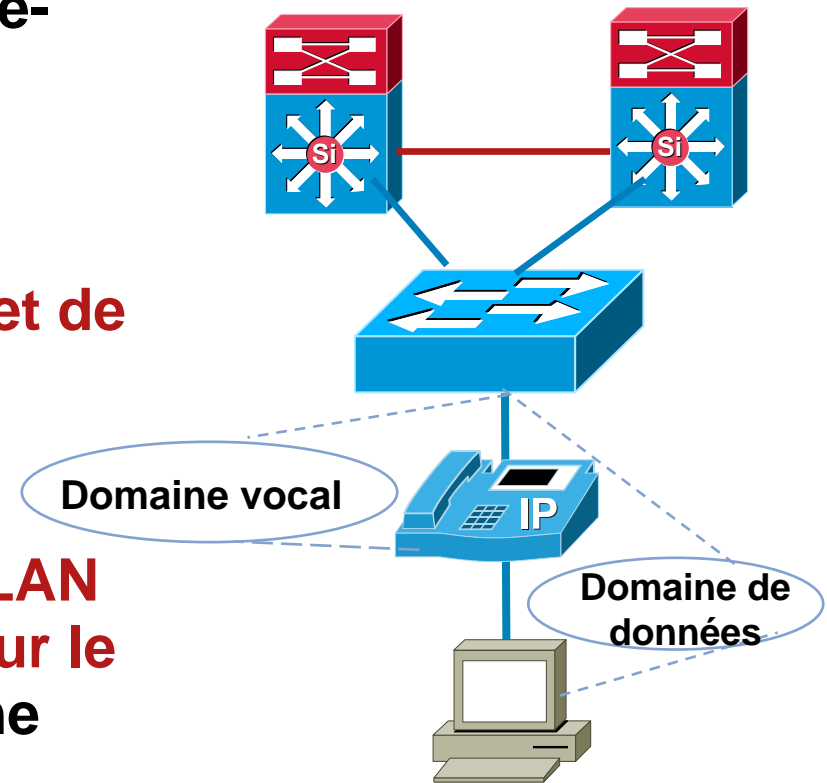
# 802.1x, avec VVID : problématiques de déploiement



- Si un utilisateur, quel qu'il soit, se branche au téléphone, 802.1x est maintenant totalement dépendant de la façon dont son supplicant est configuré
- Par défaut, **les supplicants Microsoft Windows n'envoient pas de EAPOL-start**; vous voudrez savoir pourquoi 802.1x fonctionne lorsque vous vous branchez à un commutateur et pourquoi ça ne fonctionne pas lorsque vous vous branchez à un téléphone

# Multi Domain Authentication (MDA)

- Déploiement : téléphone IP (Cisco ou tiers) + un seul hôte en arrière-plan du téléphone
- Sécurité améliorée via une **authentification et autorisation, 802.1x ou MAB** du téléphone IP et de l'hôte
- L'hôte est placé sur le réseau VLAN de données, et le téléphone IP sur le réseau VLAN vocal – sur le même port de commutateur



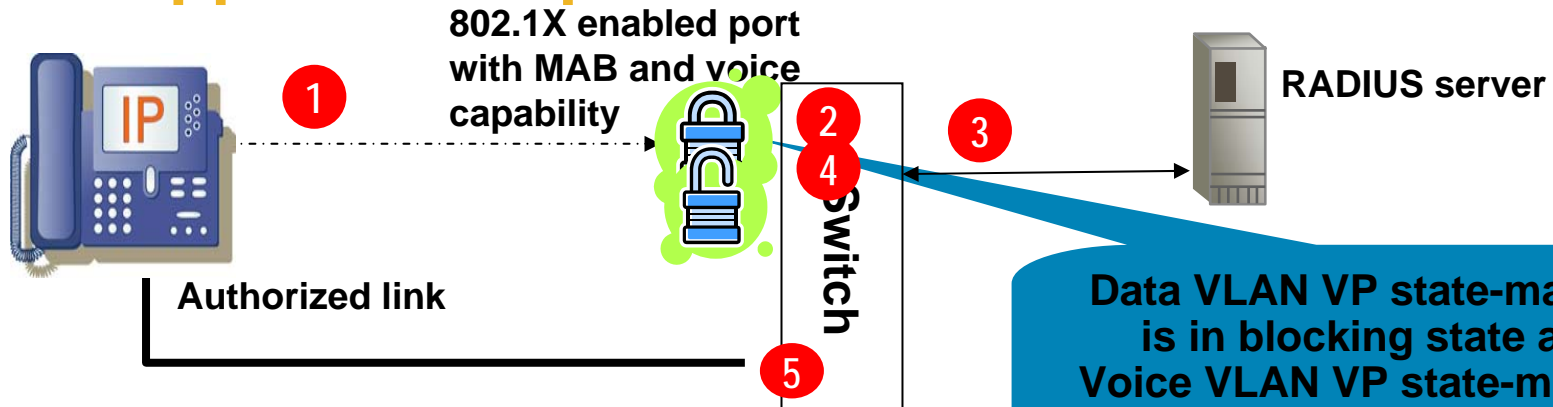
# 802.1X sur téléphone IP Cisco IP

- Supplicant 802.1X sur téléphone IP Cisco  
EAP-MD5 supported on Models  
7906/7911/7931/7941/7961/7970/7971  
Phone load 8.2(1) **December 2006**



# Solution for non-Cisco IP Phones

## No supplicant on phone



- 1 - Phone sends untagged DHCP blocked by switch
- 2 - 802.1X times out (phone not allowed to communicate to the network yet)
- 3 - Switch initiates MAB Access-Request on behalf of the phone
- 4 - Switch receives Access-Accept & information that the device is an IP phone. Port-forwarding is allowed on either VLAN.
- 5 - Non-Cisco phone continues to send traffic which is now allowed on the PVID as a result of authenticating the MAC-Address. Phone then reboots onto VVID normally.

# Infos sur le commutateur...

```
Switch#sh dot1x int g1/0/1 details

Dot1x Info for GigabitEthernet8/0/1
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = MULTI_DOMAIN
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0
Mac-Auth-Bypass = Enabled (EAP)
  Inactivity = None
Guest-Vlan = 401
```

## Dot1x Authenticator Client List

```
-----
Domain = DATA
Supplicant = 1222.c0a8.0102
  Auth SM State = AUTHENTICATED
  Auth BEND SM State = IDLE
Port Status = AUTHORIZED
Authentication Method = Dot1x
Authorized By = Authentication Server
Vlan Policy = 100
```

```
Domain = VOICE
Supplicant = 000f.8fb7.16a0
  Auth SM State = AUTHENTICATED
  Auth BEND SM State = IDLE
Port Status = AUTHORIZED
Authentication Method = MAB
Authorized By = Authentication Server
Vlan Policy = N/A
```

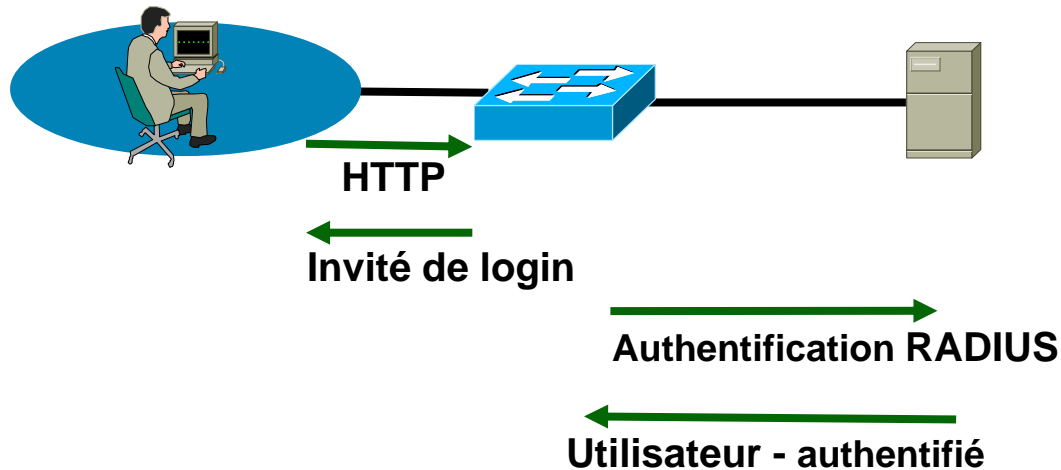
PC authentifié  
par 802.1X

Phone authentifié  
par MAB



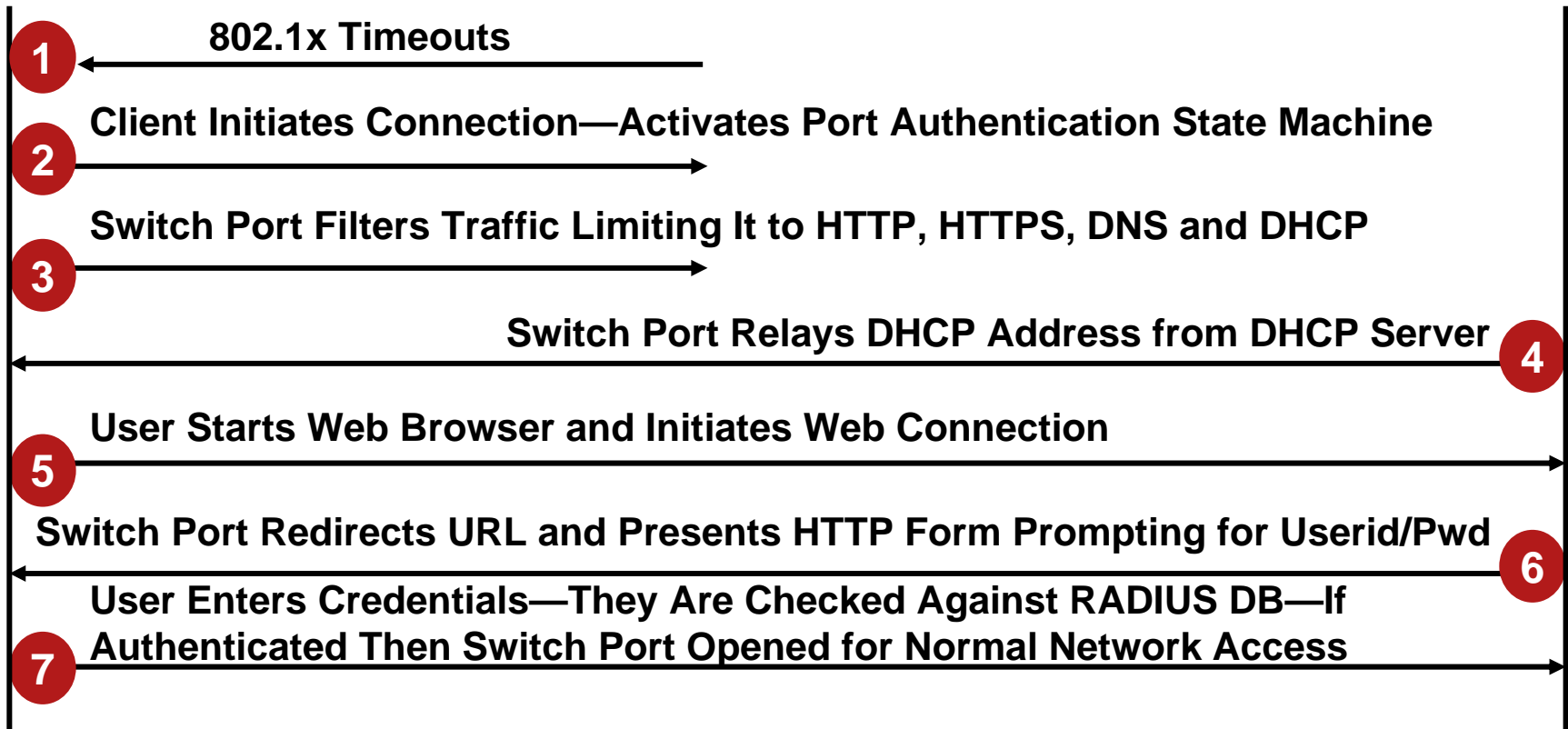
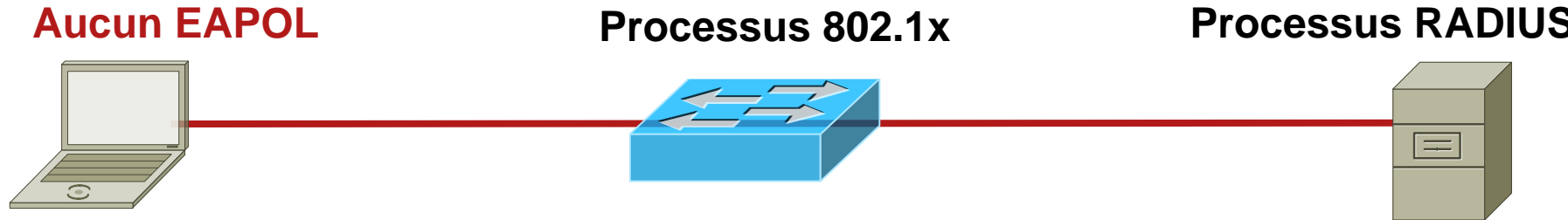
# ■ DEMO OF MDA

# Authentification 802.1x des mandataires basée sur le Web



- L'Utilisateur démarre une connection HTTP ou HTTPs
- Le commutateur intercepte la requête et affiche login/password
- Le commutateur relait les qualifications de l'utilisateur (credentials) au serveur RADIUS
- L'utilisateur est authentifié

# Authentication de mandataires basée sur le Web

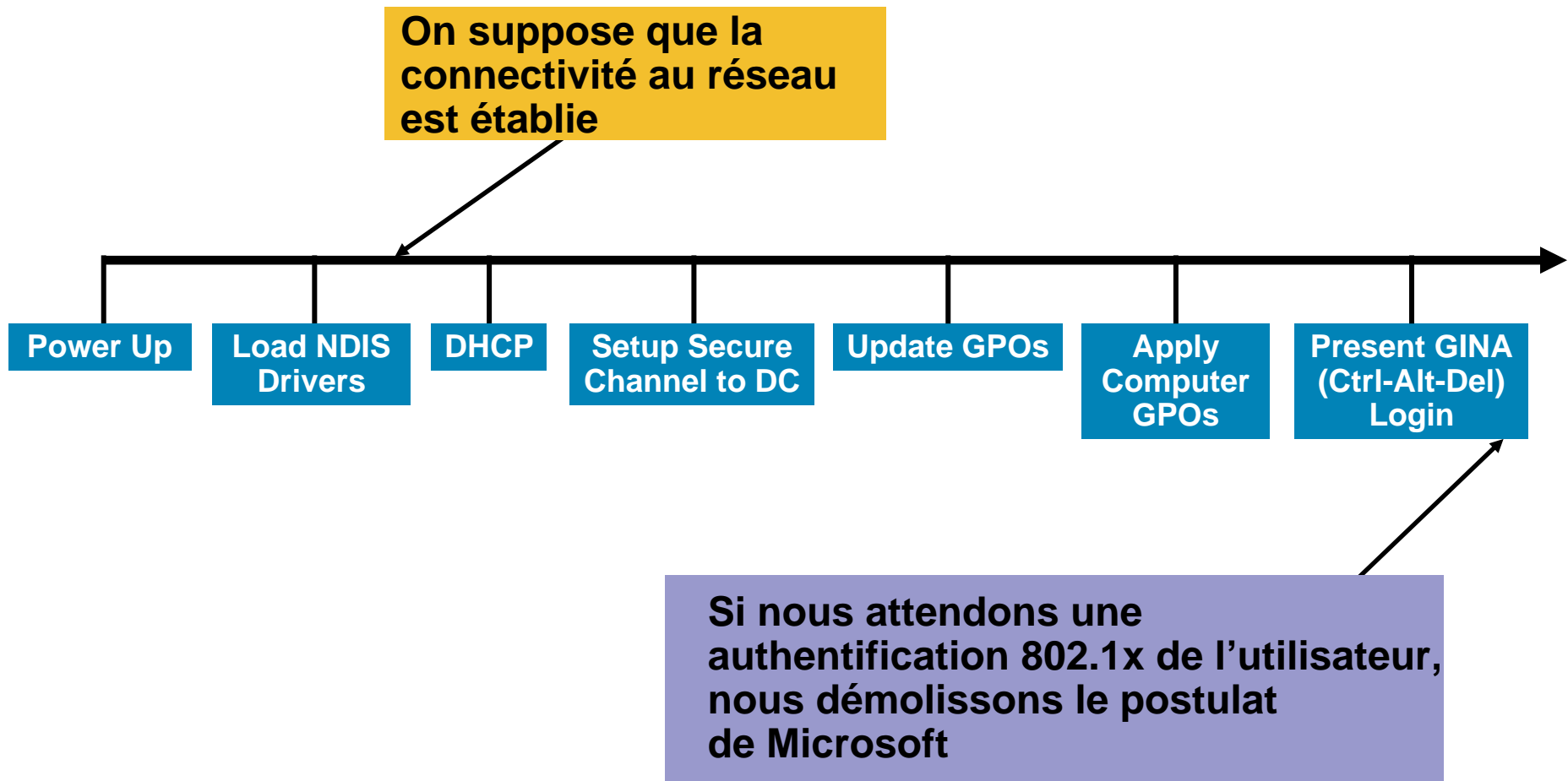


# Démo de l'Authentification de mandataires basée sur le Web

# Mises en oeuvre de de systèmes d'exploitation



# Aperçu du cycle d'amorçage de Windows



# Microsoft et l'authentification des machines

- Qu'est-ce qu'une authentification de machine?

La **capacité d'un poste de travail Windows d'effectuer une authentification sous sa propre identité**, indépendamment de l'exigence d'une session utilisateur interactive

- À quoi sert-elle?

L'authentification de machine est utilisée à l'amorçage, par les systèmes d'exploitation Windows, pour **s'authentifier auprès des contrôleurs de domaines Windows** et communiquer avec eux pour télécharger les politiques de groupe.

- Pourquoi cela a-t-il de l'importance?

Avant la norme 802.1x, le postulat était que la connectivité réseau était un acquis; depuis l'utilisation de cette norme, **le blocage d'un accès réseau avant une authentification faite par 802.1x casse le modèle des politiques de groupe basé sur les machines**—À MOINS QUE la machine puisse s'authentifier à l'aide de sa propre identité sous 802.1x

# Procédure d'ouverture de session Windows

## Authentification de l'utilisateur



• Aucune connectivité au contrôleur de domaine jusqu'à ce que l'utilisateur ouvre une session (62 sec timeout DHCP)

## Authentification de la machine

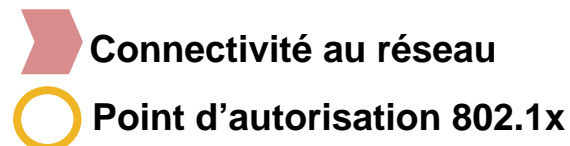


\* 802.1x tôt dans le processus d'amorçage

## Authentification de la machine et de l'utilisateur



\* Les utilisateurs peuvent être authentifiés individuellement



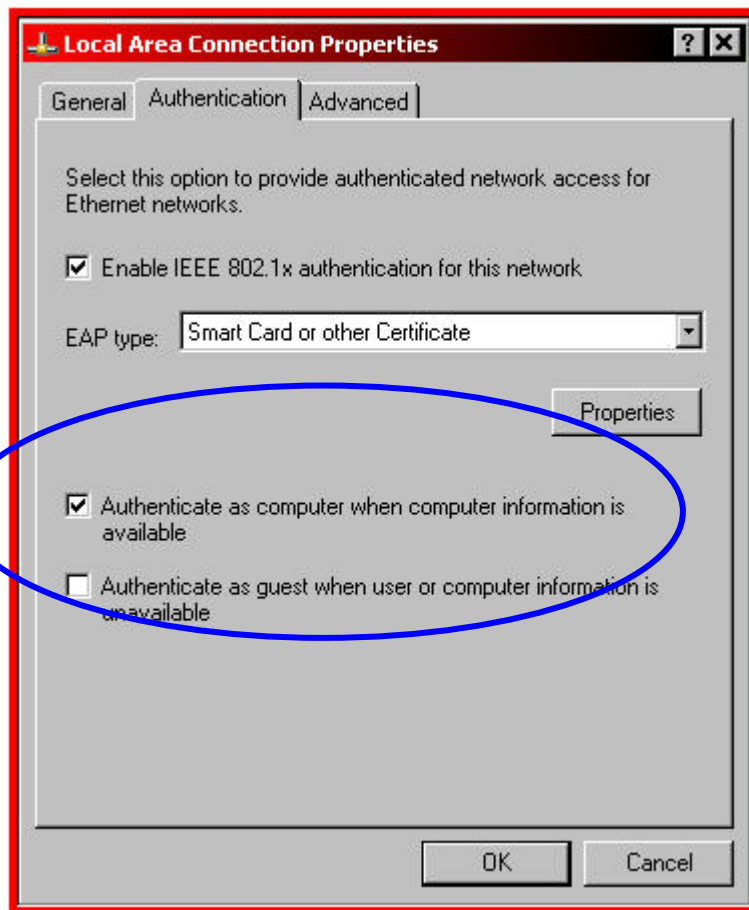


# Différents modes d'authentification dans les environnements Microsoft

- Contrôlé par des clés de registre
- Authentification par machine seulement
  - Aucun besoin d'authentifier l'utilisateur si l'authentification de la machine a été réussie
- Authentification par utilisateur seulement
  - Aucune authentification de machine— attention, cela empêche l'application des politiques système et de groupes
- Authentification par utilisateur et par machine
  - Authentification de la machine et de l'utilisateur, change de contexte lorsqu'elle passe de l'un à l'autre

# Comment activer une authentification de machine?

- S'assurer que l'ordinateur est un membre du domaine
- Si TLS est utilisé, s'assurer que l'ordinateur obtienne un certificat, soit via un enregistrement automatique soit manuellement
- Si EAP-FAST, PEAP ou EAP-TLS est utilisé, s'assurer que le certificat CA est stocké sur la machine locale; habituellement ajouté si l'autorité CA est activée et fonctionnelle lorsque la machine est ajoutée au domaine; sinon, il est possible de forcer l'ajout du certificat via un enregistrement automatique
- Cliquer sur la case à cocher « **authenticate as computer when computer information is available** » sous l'onglet d'authentification de la fenêtre de propriétés de la connexion locale



# Authentification d'une machine à l'aide de PEAP ou de TLS

- Authentification d'une machine à l'aide de PEAP

Utilise les informations relatives au compte pour l'ordinateur créé au moment où la machine est ajoutée au domaine

L'ordinateur **doit** être un membre du domaine

Dans le cas d'une authentification mutuelle, l'ordinateur **doit** faire confiance à l'autorité de certification (CA) qui signe le certificat du serveur RADIUS

- Authentification d'une machine à l'aide de EAP-TLS

Authentifie l'ordinateur à l'aide de certificats

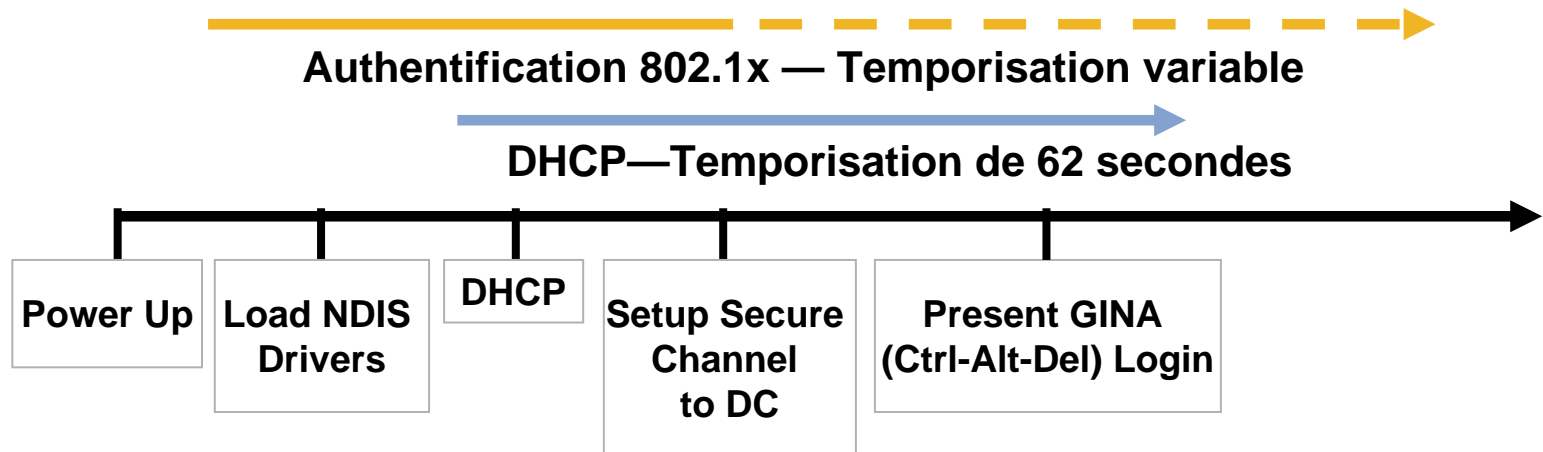
L'ordinateur **doit** avoir un certificat valide

Dans le cas d'une authentification mutuelle, l'ordinateur **doit** faire confiance à l'autorité de certification (CA) qui signe le certificat du serveur RADIUS

# Problématiques de Microsoft concernant DHCP

## DHCP est un événement parallèle, indépendant de l'authentification 802.1x

- Dans le cas d'une connexion filaire, une authentification 802.1x réussie **ne** force **pas** un renouvellement de l'adresse DHCP (pas de changement au niveau du média)
- Cela entraîne un problème en cas de planification inadéquate
- DHCP démarre aussitôt que l'interface est activée
- Si l'authentification 802.1x prend trop de temps, DHCP peut arriver au bout de son délai



# Comment régler le délai d'attente DHCP à l'aide de 802.1x?

- Utiliser l'authentification des machines — cela permet à l'authentification initiale de la machine d'obtenir une adresse IP
- Le comportement du supplicant est pris en charge par Microsoft
  - Windows XP : installer l'ensemble de modifications provisoires 1a + KB 826942
  - Windows 2000 : installer l'ensemble de modifications provisoires 4
- Les supplicants mis à jour déclenchent un renouvellement des adresses IP DHCP

Dans le cas d'une authentification réussie, le client envoie un ping à la passerelle par défaut (trois fois) caractérisé par un délai d'attente inférieur à la seconde

L'absence d'une réponse par écho déclenche un renouvellement des adresses IP DHCP

S'il y a une réponse par écho, les adresses IP resteront telles quelles

Un ping de pré-renouvellement empêche de perdre des connexions lorsque le sous-réseau reste tel quel, mais que le client est peut-être en itinérance sur le réseau WLAN

# 802.1x et la restriction d'accès de la machine

- Si l'authentification de la machine échoue ou qu'elle n'est pas activée, un utilisateur peut quand même accéder au réseau
- Ainsi, l'authentification de la machine n'empêche pas les utilisateurs d'accéder au réseau par l'intermédiaire d'une machine non enregistrée



Authentification de  
l'utilisateur

- Si l'utilisateur ouvre une session sur la machine, celle-ci envoie un message EAPOL-log-off pour avertir le point d'accès ou le commutateur que l'authentification précédente n'est plus valide
- L'authentification EAP-TLS, PEAP-MS-Chapv2, EAP-FAST suivante sera faite moyennant les justificatifs d'identité de l'utilisateur

**!** Les nouvelles fonctionnalités du serveur RADIUS Cisco ACS complètent désormais une authentification d'utilisateur seulement si antérieurement une authentification de la machine a été réussie

# ■ DEMO Machine auth



# Support du supplicanant 802.1x

- 802.1x exige le code du côté client (code du supplicanant)
- Support croissant des supplicanants dans l'industrie
  - Microsoft—natif dans Win2K, XP et 2003
  - Meetinghouse : maintenant Cisco CSSC — support de WinNT, Win2K, WinXP, Win98, WinME, Solaris, Red Hat Linux
  - Opensource—Open1x xsupplicant pour les plates-formes UNIX/Linux
  - Apple—support natif de OS X
  - Cisco :
    - ACU : client sans fil
    - CTA : client câblé

# Supplicant – Points à examiner

- **Microsoft Windows**

- Authentification de l'utilisateur et de la machine
  - Temporisation de la requête DHCP
  - Restrictions liées à l'authentification de la machine
  - Méthodes par défaut : MD5, PEAP, EAP-TLS

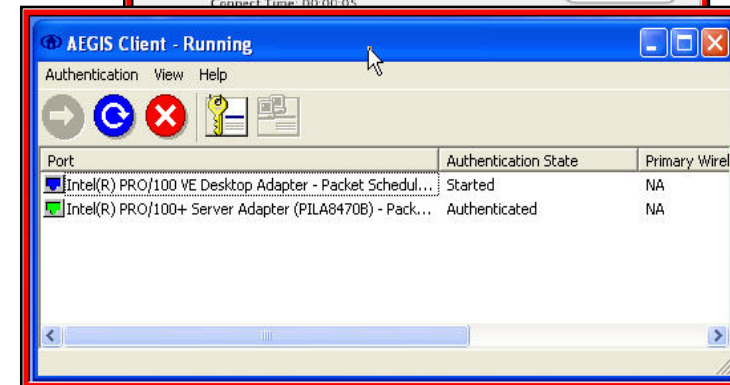
- **Points Unix/Linux à examiner**

- Code source libre : xsupplicant Project (University of Utah)
  - Disponible à l'adresse <http://www.open1x.org>
  - Supporte EAP-MD5, EAP-TLS, PEAP/MSCHAPv2, PEAP/EAP-GTC

- **Support d'un supplicant 802.1x à même OS X 10.3**

- 802.1x est désactivée par défaut!
  - Paramètres par défaut TTLS, LEAP, PEAP, MD5 supportés
  - Support des interfaces d'aéroport et câblées
  - La signature unique peut être effectuée à l'aide de Applescripts

- **Produits commerciaux Cisco CSSC**



# Autorisation

- L'autorisation représente la **capacité d'appliquer les politiques aux identités**
- Les politiques sont habituellement appliquées moyennant une méthodologie de groupe, ce qui facilite la gérabilité
- L'objectif consiste à appliquer les notions de gestion et de politiques de groupe au réseau
- **L'autorisation la plus élémentaire** dans 802.1x est la **capacité de permettre ou de refuser l'accès** au réseau
- Autres formes d'autorisation : attribution d'un **VLAN**, d'une **liste de contrôle d'accès (ACL)** et de politiques de **QoS**.

# 802.1x, avec attribution d'un réseau VLAN

- Attribution dynamique d'un réseau VLAN fondée sur l'identité d'un groupe ou d'un individu, au moment de l'authentification
- Les VLAN sont attribués par nom — cela permet une gestion plus souple des VLAN
- Permet d'appliquer des politiques VLAN dynamiques à des groupes d'utilisateurs (par ex., QoS VLAN, listes ACL VLAN, etc.)
- Les attributs relatifs aux tunnels sont utilisés pour retourner des informations sur la configuration VLAN à l'authentifiant (commutateur – AP etc)
- Les attributs relatifs aux tunnels sont définis par RFC 2868
- L'utilisation, dans le cas des VLANs, est indiquée dans la norme 802.1x

# 802.1x, avec attribution d'un réseau VLAN

Utilisation d'attributs AV-pairs, (attribute values) toutes conformes à la norme IETF

- [64] Tunnel-type—"VLAN" (13)
- [65] Tunnel-medium-type—"802" (6)
- [81] Tunnel-private-group-ID—<VLAN name>



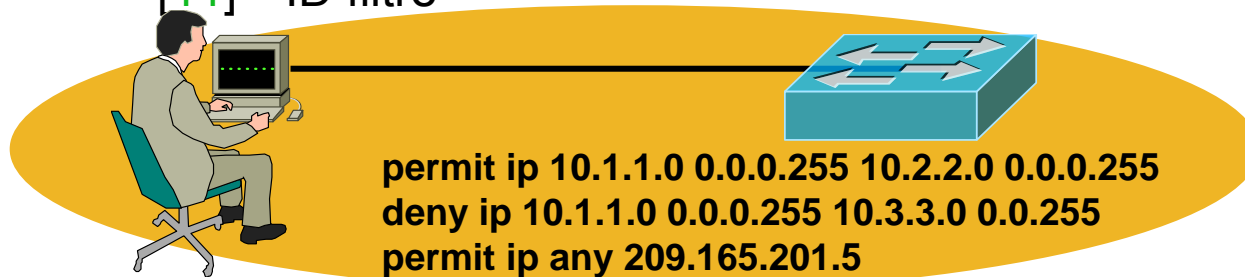
*IOS*

```
aaa authorization network default group radius
```

- **VLAN Name** doit correspondre dans la configuration du commutateur
- Une non correspondance entraîne l'échec de l'autorisation

# 802.1x, avec attribution d'une liste de contrôle des accès (ACL)

- Attributs spécifiques aux fournisseurs, utilisés pour RADIUS
  - [026]—spécifique à un fournisseur
  - [009]—ID de fournisseur pour Cisco
  - [001]—réfère au numéro VSA (vendor specific attribute)
- Attribut utilisé pour des listes ACL prédéfinies
  - [11]—ID filtre



*IOS*

```
aaa authorization network default group radius
```

# 802.1x, avec listes de contrôle des accès (ACL)

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

Cisco IOS/PIX RADIUS

[009\001] cisco-av-pair

```
ip:inacl#1=deny ip any host
10.1.8.3
ip:inacl#2=permit ip any any
```

[010] Framed-Routing

[011] Filter-Id

acl=eng

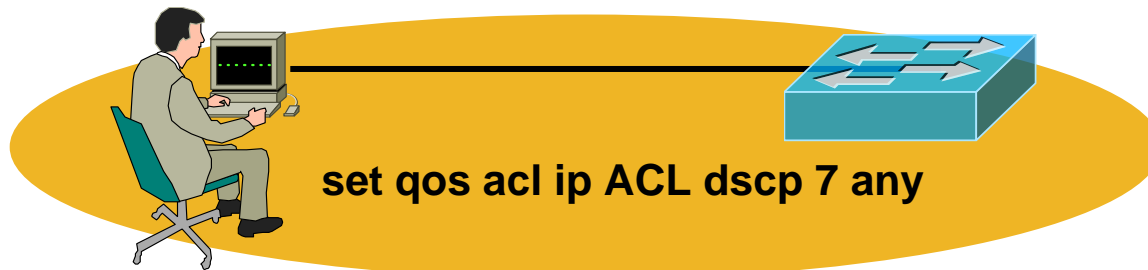
[012] Framed-MTU (64..65535)

```
id-3550-5#sho dot1x interface f0/7
Supplicant MAC 00e0.8105.8d93
AuthSM State = AUTHENTICATED
BendSM State = IDLE
PortStatus = AUTHORIZED
MaxReq = 2
HostMode = Single
Port Control = Auto
QuietPeriod = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod = 3600 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 30 Seconds
Guest-Vlan = 0

id-3550-5#sho access-lists
Extended IP access list FastEthernet0/7#0 (per-user)
deny ip any host 10.1.8.3
permit ip any any
```

# 802.1x, avec une politique de QoS

- **Attributs spécifiques aux fournisseurs, utilisés pour RADIUS**
  - [026]—spécifique à un fournisseur
  - [009]—ID de fournisseur pour Cisco
  - [001]—réfère au numéro VSA



*IOS*

```
aaa authorization network default group radius
```

- **Utilisée pour permettre l’approvisionnement automatique de QoS des utilisateurs**
- **Dans cet exemple, RADIUS envoie un nom QoSACL en même temps qu’un paquet d’acceptation**
- **La politique est convertie en ACE (access control entries) et installée sur ce commutateur**



# 802.1x, avec une politique de QoS

### Cisco IOS/PIX RADIUS Attributes

[009\001] cisco-av-pair

qos:inpacl=Team1QoSACL

```
id-switch> (enable)
id-switch> (enable) sho qos acl map runtime Team1QoSACL
QoS ACL mappings on input side:
ACL name                               Type Vlans
-----
Team1QoSACL                             IP
ACL name                               Type Ports
-----
Team1QoSACL                             IP 3/11
QoS ACL mappings on output side:
ACL name                               Type Vlans
-----
Team1QoSACL                             IP
id-switch> (enable)
```

# 802.1x et échec d'autorisation

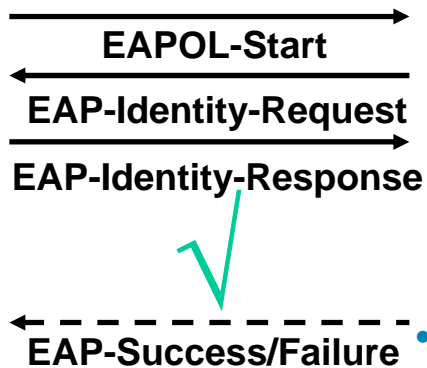
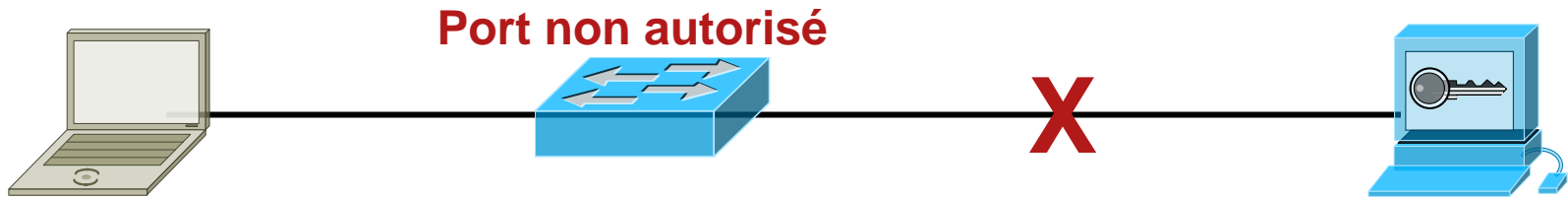
- Le commutateur fera échouer l'authentification vers un client si l'autorisation émanant du serveur d'authentification ne peut pas lui être appliquée
- Par exemple, vlan = employé, mais le commutateur ne comporte aucun vlan portant le nom employé
- Le problème est exacerbé dans le cas de NAC2 car la liste contextuelle de CTA indique que tout va bien, ACS indique que tout va bien, le commutateur fait échouer l'authentification et le client atteste une authentification échouée

# Contournement d'authentification inaccessible

## Le serveur Radius ne répond plus !

*IOS*

```
Dot1x critical
radius-server x.x.x.x username test password test
Interface gigabitethernet 1/0/1
dot1x critical
dot1x critical vlan 10
```



- Port autorisé
- Déplacement pour accéder au VLAN (première authentification)
- Ou garder le VLAN existant (ré-authentification)

# 802.1x, avec RADIUS Accounting

- Semblable à d'autres mécanismes de comptabilisation et de suivi qui existent déjà et utilisent RADIUS
  - Peut maintenant se faire en passant par 802.1x
- Augmente la sensibilisation aux sessions de réseau
- Fournit des informations sur l'infrastructure de gestion : qui ouvre une session, durée de la session, support de rapports d'utilisation pour une facturation de base, etc.
- Fournit une façon d'établir une correspondance entre les informations des éléments suivants qui ont été authentifiés :

**Identité, Port, MAC, Commutateur**



**IP, Port, MAC, Commutateur**

=

**Identité → IP**

**Commutateur + Port = Emplacement**

*IOS*

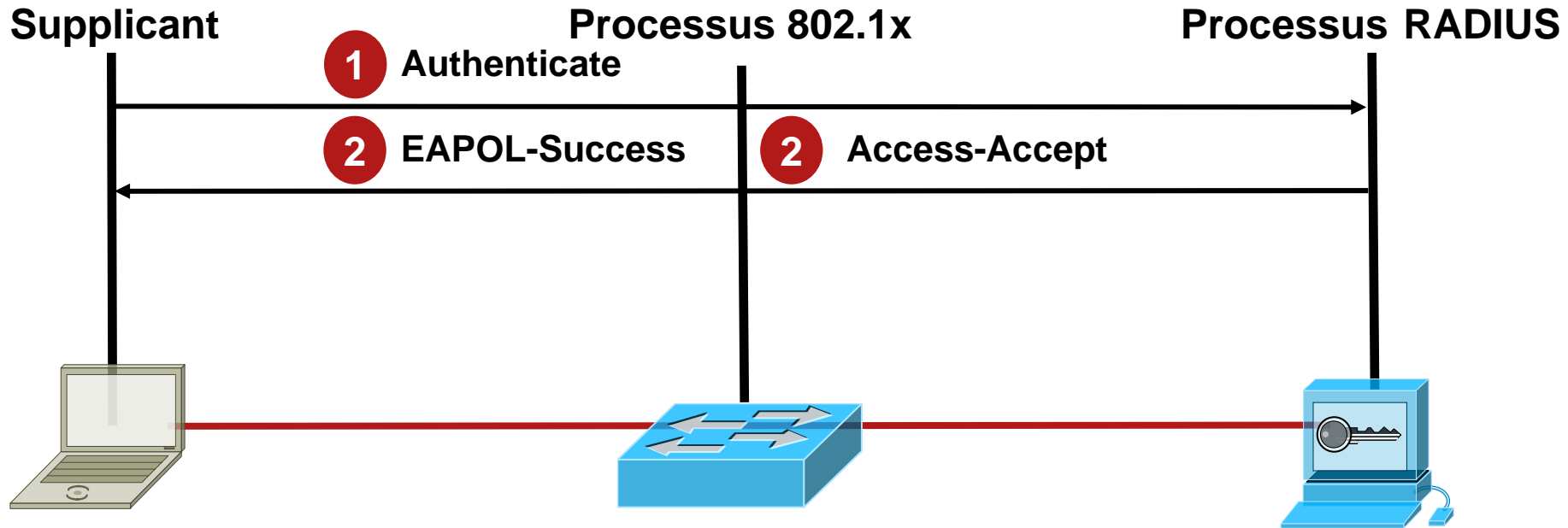
```
aaa accounting dot1x default start-stop group radius
```

# Démonstrations 802.1x

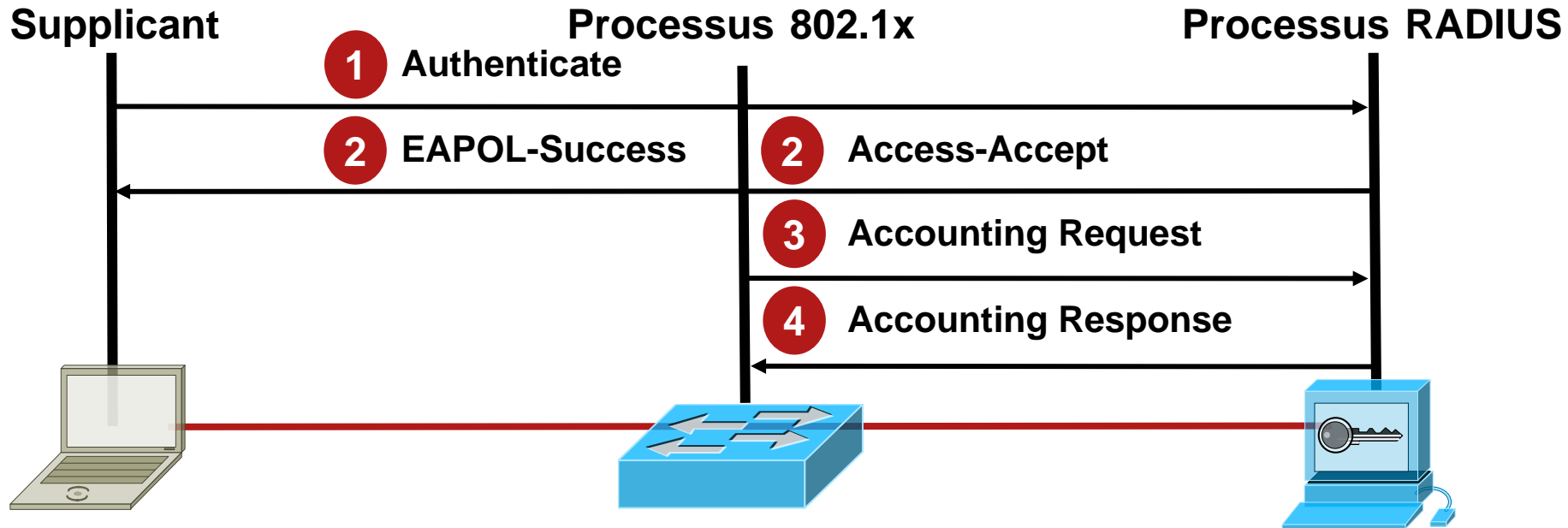
# IBNS – Rapports et surveillance

- Principales composantes pour une surveillance IBNS
  - RADIUS Accounting
  - Journaux NAD
  - Journaux RADIUS
  - CLI NAD
- Principales composantes pour les rapports IBNS
  - Rapports d'activités corrélés (MARS)

# 802.1x, avec RADIUS Accounting



# 802.1x, avec RADIUS Accounting



- Paquets Accounting-request
- Renferme une AV-pair ou plus pour signaler, au serveur RADIUS, divers événements et les informations qui leur sont associées
- Des événements de suivi des utilisateurs sont utilisés dans le même mécanisme

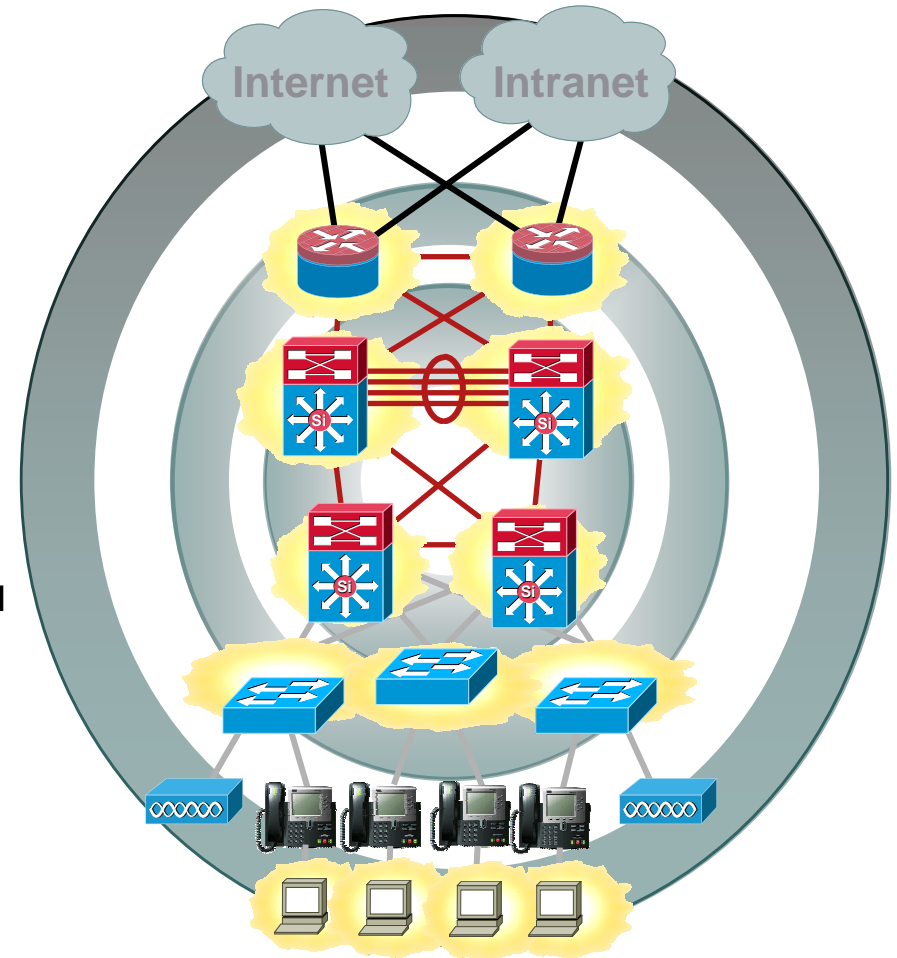


# Demo Accounting 802.1x

# Fin section Sylvain D

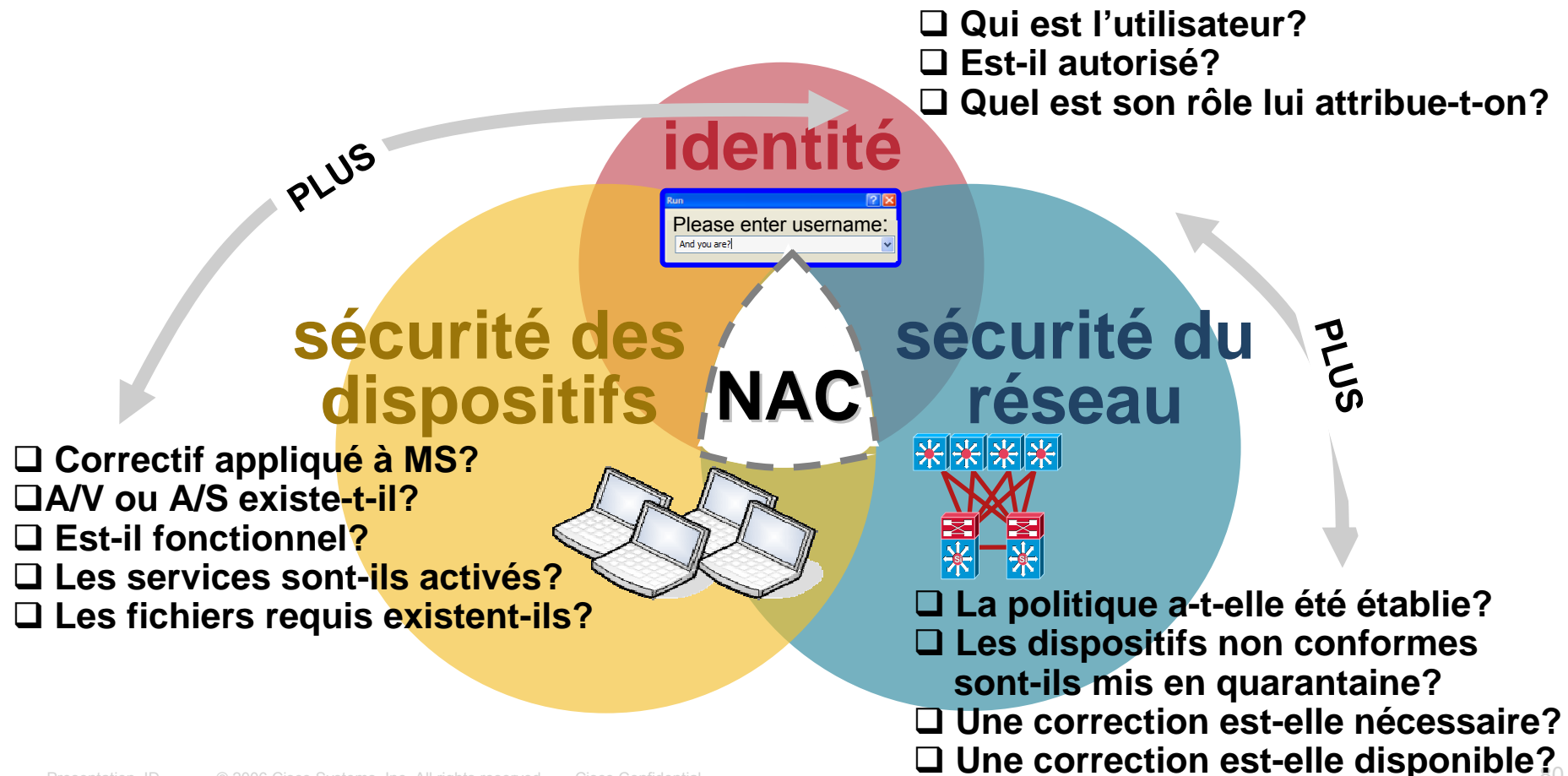
# Programme

- **Authentification**
  - ▲ Qui peut accéder le réseau
  - ▲ L'impact de la téléphonie
  - ▲ 802.1x, les visiteurs, Web Base . Authentification
- **La conformité des postes au moment de la connexion**
  - ▲ Sur le LAN, en VPN, etc...
- **Les bonnes pratiques pour le contrôle des usagers connectés au réseau**
  - ▲ Fonctions de sécurité présentent dans les commutateurs Cisco
  - ▲ QoS déployée?
  - ▲ Cisco Sécurité Agent (CSA)
- **La surveillance et la configuration du réseau**

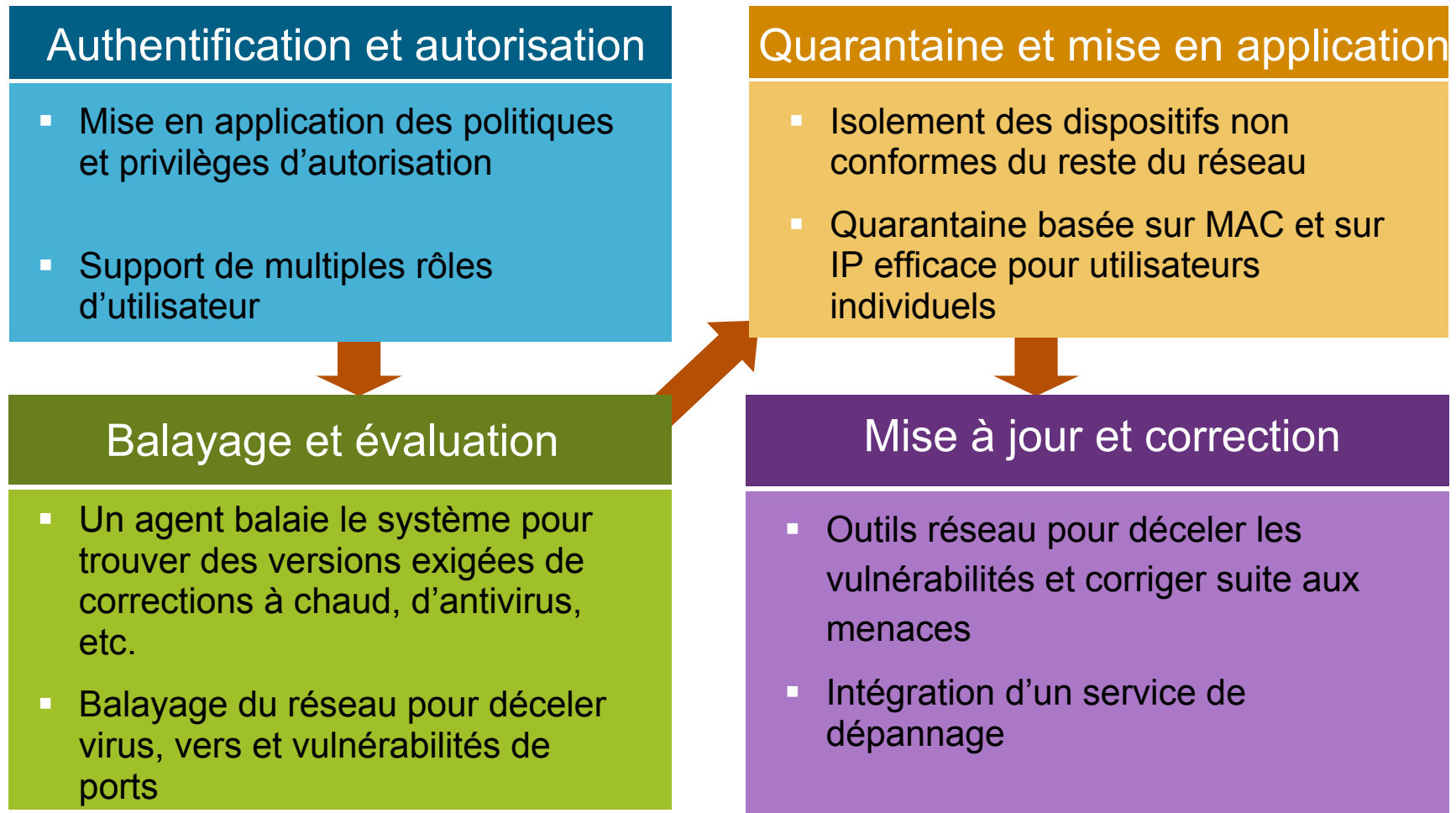


# Qu'est-ce que le protocole Network Admission Control?

L'utilisation du réseau pour assurer l'application des politiques garantit la conformité des dispositifs entrants



# Subordonner l'accès à la conformité



**PAS DE CONFORMITÉ = PAS D'ACCÈS AU RÉSEAU**

# NAC = meilleurs critères de sécurité



**De quel système s'agit-il?**

Windows, Mac ou Linux  
Ordin. de bureau, portatif ou ass. PDA  
Imprimante ou autre bien d'entreprise

**Qui en est le propriétaire?**

Compagnie  
Employé  
Entrepreneur  
Invité  
Inconnu

**D'où vient-il?**

VPN  
LAN  
WLAN  
WAN

**Que renferme-t-il?  
Est-il actif?**

Antivirus, anti-logiciel espion  
Pare-feu personnel  
Outils de correction

**Quelle est la façon privilégiée  
de le vérifier ou de le corriger?**

Vérifications pré-configurées  
Vérifications personnalisées  
Auto-correction ou correction  
automatique  
Logiciel tiers

# Quatre grandes capacités de Cisco NAC

	<b>Identification</b> sûre des dispositifs et des utilisateurs	<b>Mise en application</b> uniforme des politiques	<b>Quarantaine</b> et <b>correction</b>	<b>Configuration</b> et <b>gestion</b>
Qu'est-ce que cela signifie?	Association des utilisateurs aux dispositifs	Évaluation des dispositifs; mise en application des politiques	Isolation et correction des dispositifs non conformes	Création et gestion faciles des politiques
Pourquoi est-ce important?	L'association des utilisateurs aux dispositifs permet une mise en application granulaire des politiques, par rôle ou par groupe	La mise en application au niveau du réseau réduit la dépendance à l'intégrité du point limite	La mise en quarantaine est essentielle pour empêcher la propagation des vulnérabilités; la correction s'occupe du problème à la racine	Des politiques faciles à créer et à maintenir entraînent une meilleure exploitation des systèmes et un plus grand respect des politiques

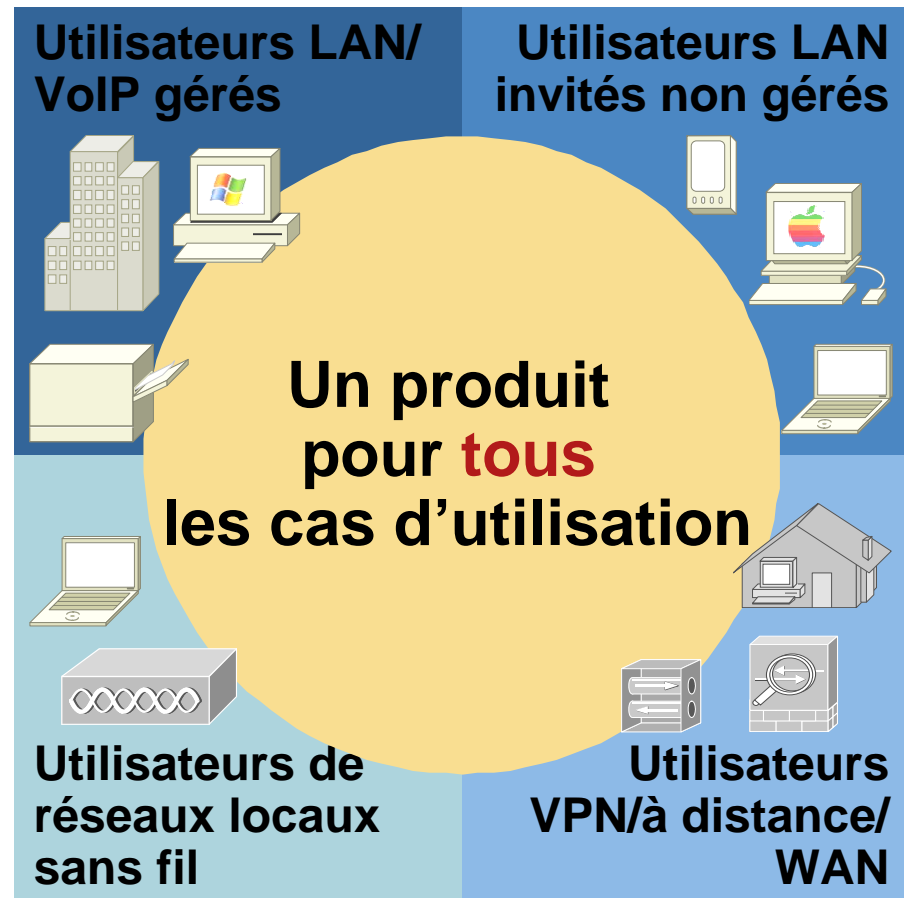
Une solution NAC exhaustive doit comporter **les quatre capacités** : l'absence d'une seule d'entre elles affaiblit la solution

# L'utilisation de Cisco NAC est aujourd'hui répandue

- NAC Appliance : 2000+ clients mondialement
- Marché intermédiaire et grandes entreprises
  - Services financiers
  - Soins de santé / fabrication
  - Secteur public
- Tous les cas d'utilisation
  - Accès à distance
  - Sans-fil / Invité
  - Réseau local en campus

« Cisco.. reste sans concurrent en tant que leader du marché dans le créneau d'appareils NAC, en détenant plus de **45 %** du marché. »

-- Frost & Sullivan, 11/06

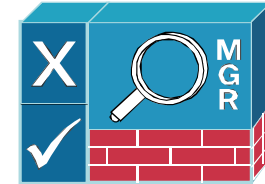




# Composantes de NAC Appliance

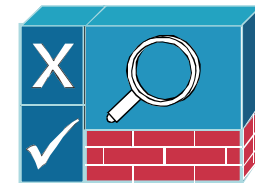
- Cisco Clean Access Manager

Centralise la gestion pour les administrateurs, le personnel de soutien et les opérateurs



- Cisco Clean Access Server

Sert de point de mise en application pour le contrôle des accès au réseau



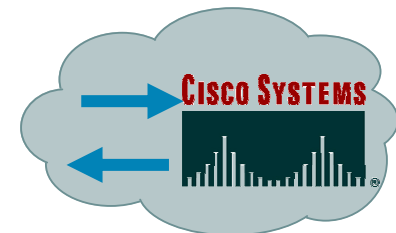
- Cisco Clean Access Agent

Client léger optionnel pour les balayages de registres basés sur dispositifs dans des environnements non gérés

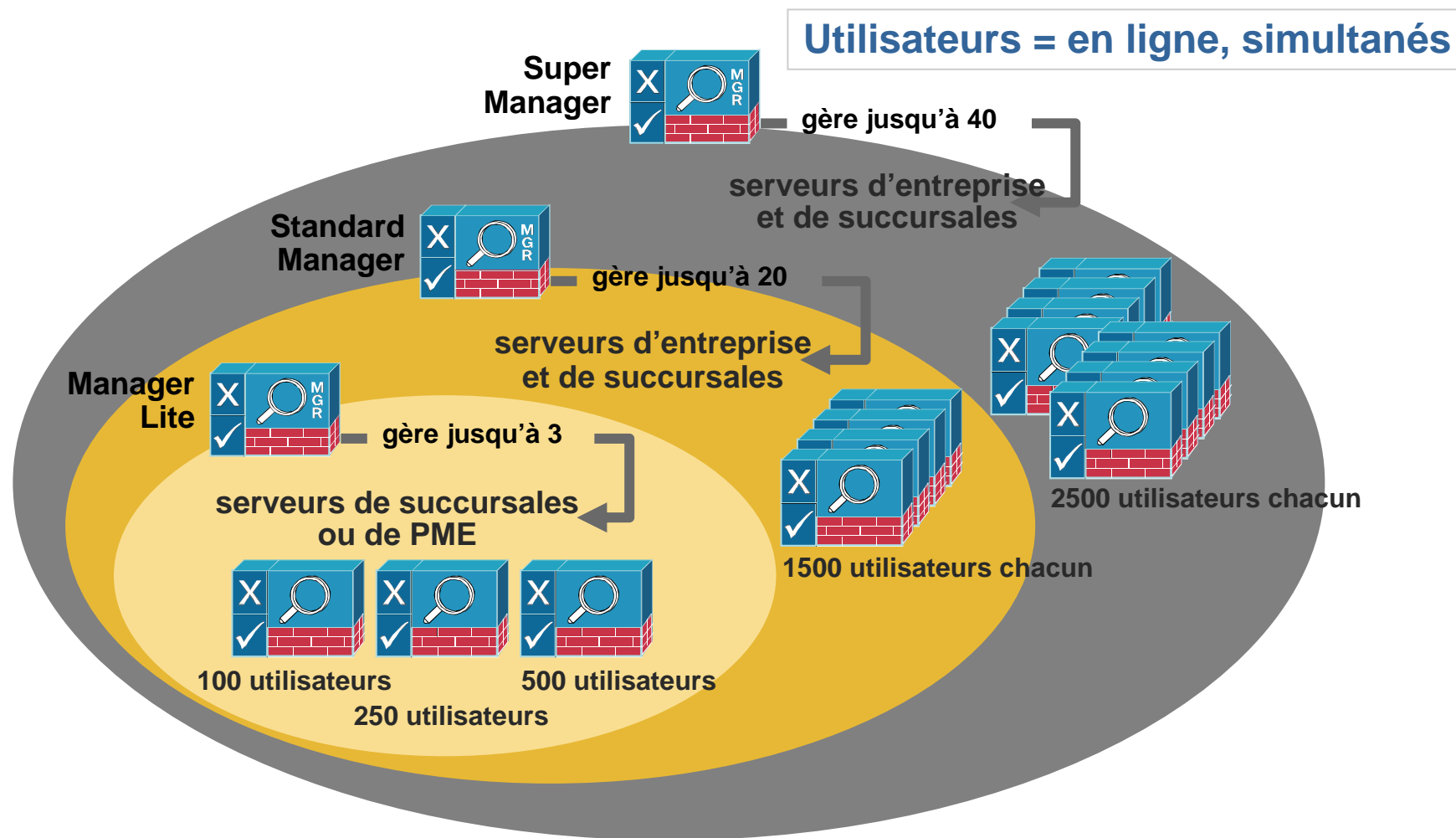


- Rule-set Updates

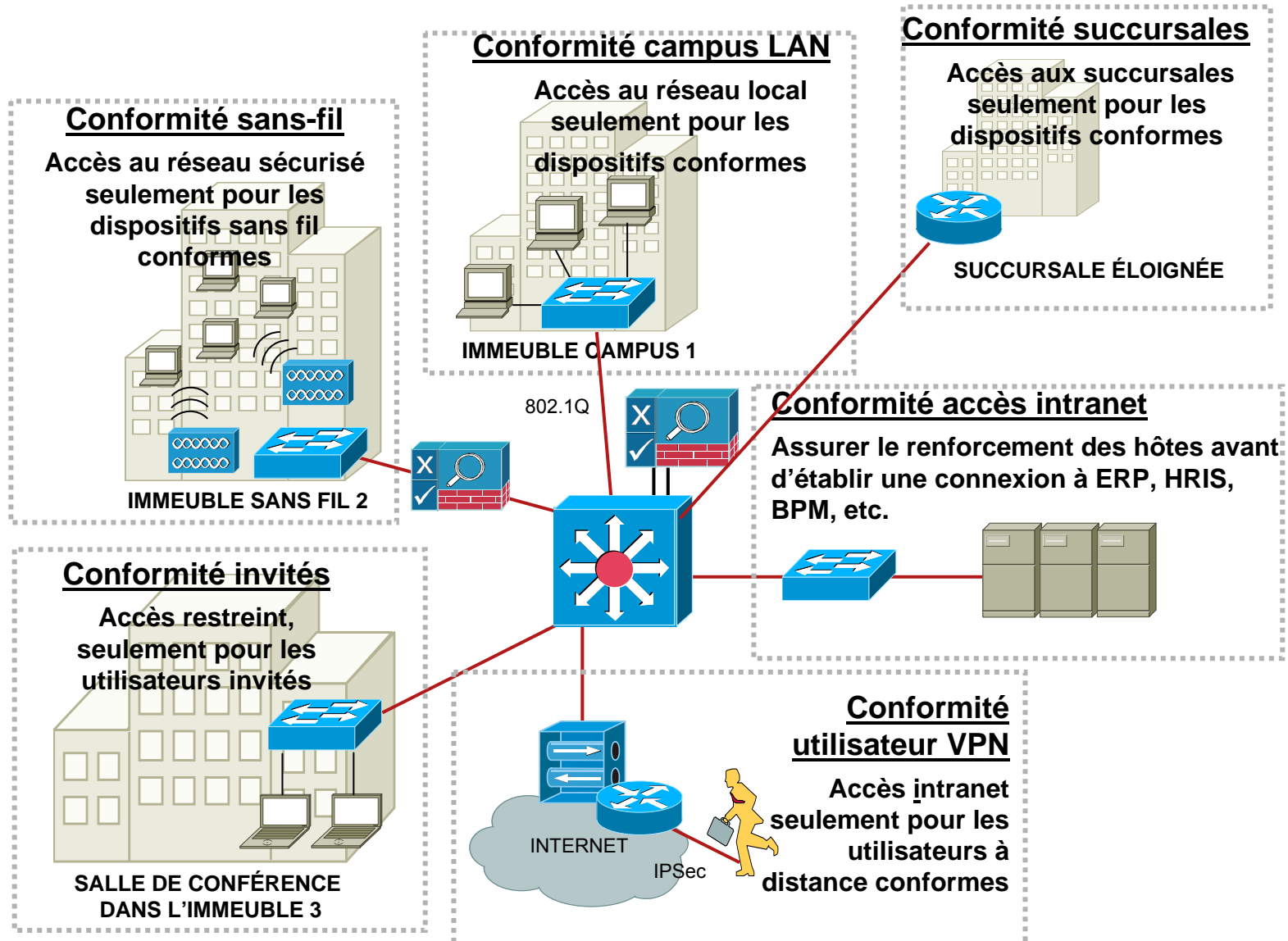
Mises à jour automatiques programmées, pour les antivirus, les corrections à chaud critiques et autres applications



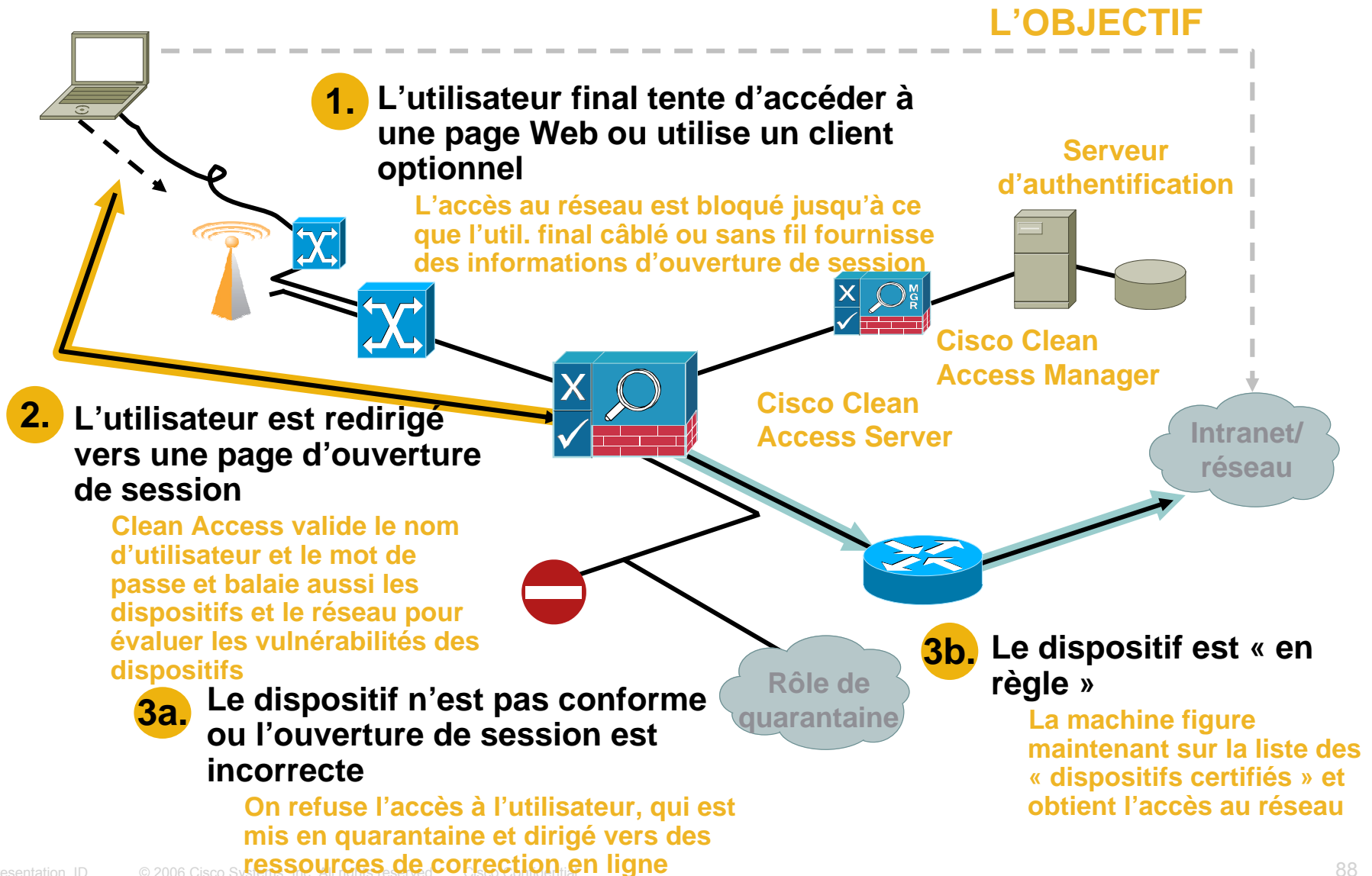
# Dimensionnement de NAC Appliance



# NAC Appliance – Cas d'utilisation



# Aperçu de Cisco NAC Appliance



# Expérience de l'utilisateur final : basée sur le Web

Un balayage est effectué  
(les types de vérifications dépendent du rôle  
de l'utilisateur / du système exploitation)

## Cisco Clean Access Authentication

**CISCO SYSTEMS**

Username

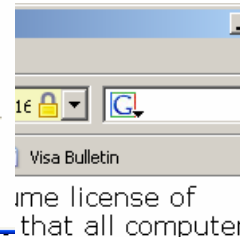
Password

Provider Local DB

Please provide your credentials to access this network.

Powered by [Cisco Clean Access](#)

## Fenêtre d'ouverture de session



accessing the network have the Anti-Virus software installed and updated. If you have not yet installed the Anti-Virus software, please do so now. The volume license includes regular updates to protect your computer against new viruses.

Note that all existing anti-virus software should be removed from your computer before installing the Anti-Virus software. For complete installation instructions, see the How-To document.

The ITS Support Center will be delighted to answer any questions you have about the procedure. Contact

**Vulnerability Scan Report of iyao's Machine**

Type	Service	Description	Instruction	Link
INFO	microsoft-ds (445/tcp)	A CIFS server is running on this port		
INFO	netbios-ssn (139/tcp)	An SMB server is running on this port		
INFO	netbios-ns (137/udp)	The following 3 NetBIOS names have been gathered : IYAOSFO03 IYAOSFO03 = This is the computer name PERFIGO = Workgroup / Domain name The remote host has the following MAC address on its adapter : 00:02:2d:09:f3:5d If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621		

Done 192.168.151.10

Correction en suivant les boutons à cliquer

# Expérience de l'utilisateur final : basée sur le Web



# Expérience de l'utilisateur final : avec Agent

Fenêtre  
d'ouverture  
de session

Cisco Clean Access Agent

## Clean Access Agent

Please enter your user name and password:

User Name :  
ricco

Password :  
[masked]

Remember Me

Please select your authentication provider:  
Local DB

**Un balayage est effectué**

(les types de vérifications dépendent du rôle de l'utilisateur)

**Le balayage échoue**

**Correction**

Cisco Clean Access Agent

## Clean Access Agent

**! You have temporary access !**

Your system does not meet the requirements enforced by the network administrator. You may only have limited access to the network until your system meets all the requirements.

There is approximately 0:03:59 left before your temporary access expires.

Please click on "Continue" and follow the instructions to satisfy network access requirements.

Continue

Cisco Clean Access Agent

## Clean Access Agent

**! Please download and install the required software before accessing the network.**

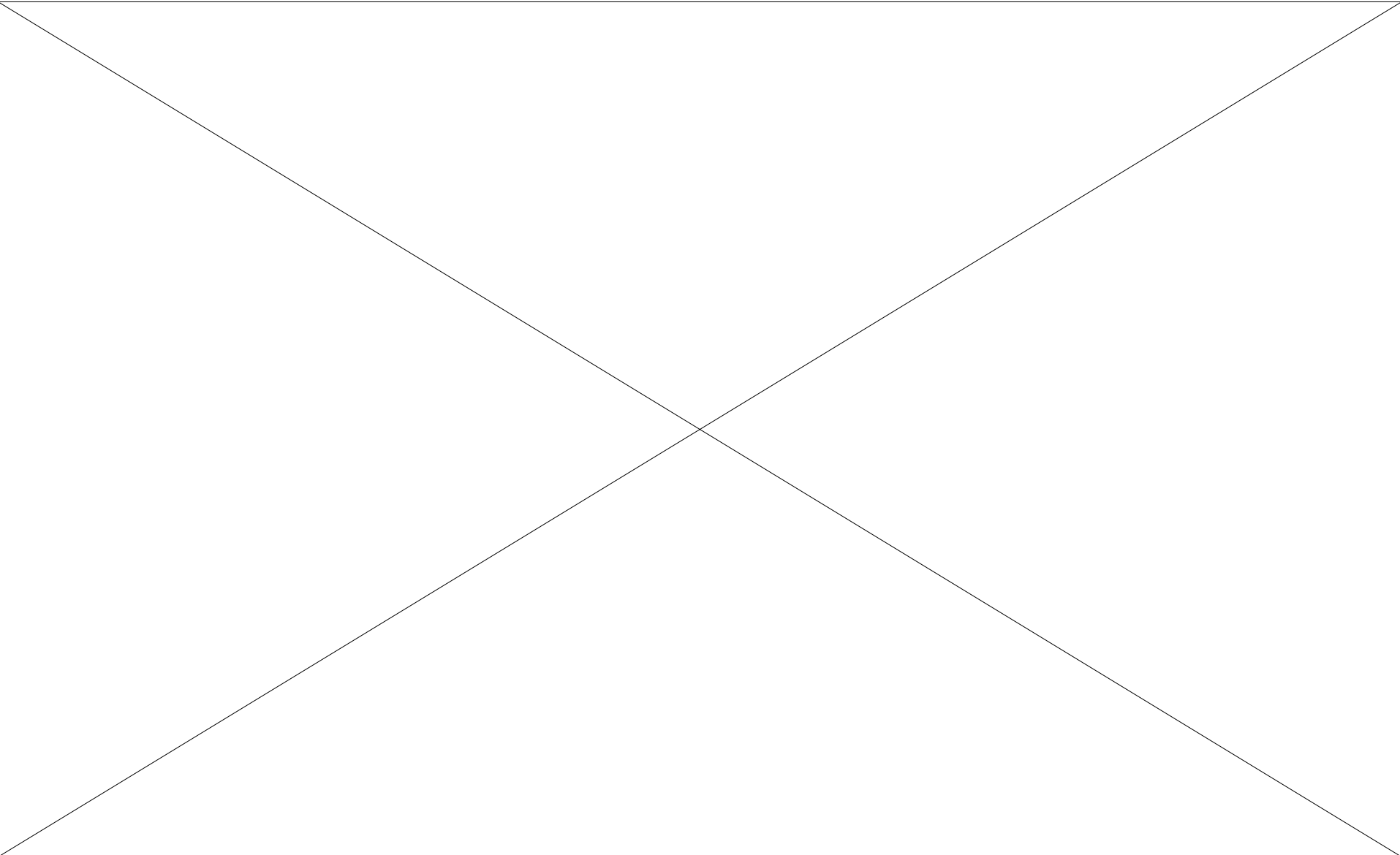
**Required Software** (0:03:10 left)

Name : Anti-Spyware (Optional) Software  
Version :  
Location : <http://www.lavasoft.com/support/download/>

Description : Our security policy recommends that you download an anti-spyware program. Click Go To Link to download a free Anti-Spyware program or click Next to skip.

Go To Link Next Cancel

# Expérience de l'utilisateur final : avec Agent





# Partenariats Cisco NAC Appliance

Cisco NAC entend protéger les investissements du client dans les applications de partenaires

NAC Appliance supporte les politiques de 300+ applications, dont celles des fournisseurs suivants :

Ahn AhnLab



authenticum

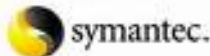


Microsoft

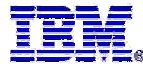


Computer Associates®

LAVASOFT



webroot Spy Sweeper®



GRISOFT



Spybot Search & Destroy



Sunbelt Software

SOPHOS  
SOPHOS ANTI-VIRUS

BulletProofSoft

Windows OneCare Live

SOFTWIN  
Software and Services  
bitdefender  
secure your every bit



YAHOO!

McAfee  
SECURITY

ZONE  
LABS

PREVX



AVIRA AntiVir®

# Évaluation de la posture de l'entreprise / employé

## Marque d'inventaire de l'entreprise :

- Registres uniques insérés dans des dispositifs d'entreprise
- Certificats PKI d'entreprise installés dans des dispositifs d'entreprise

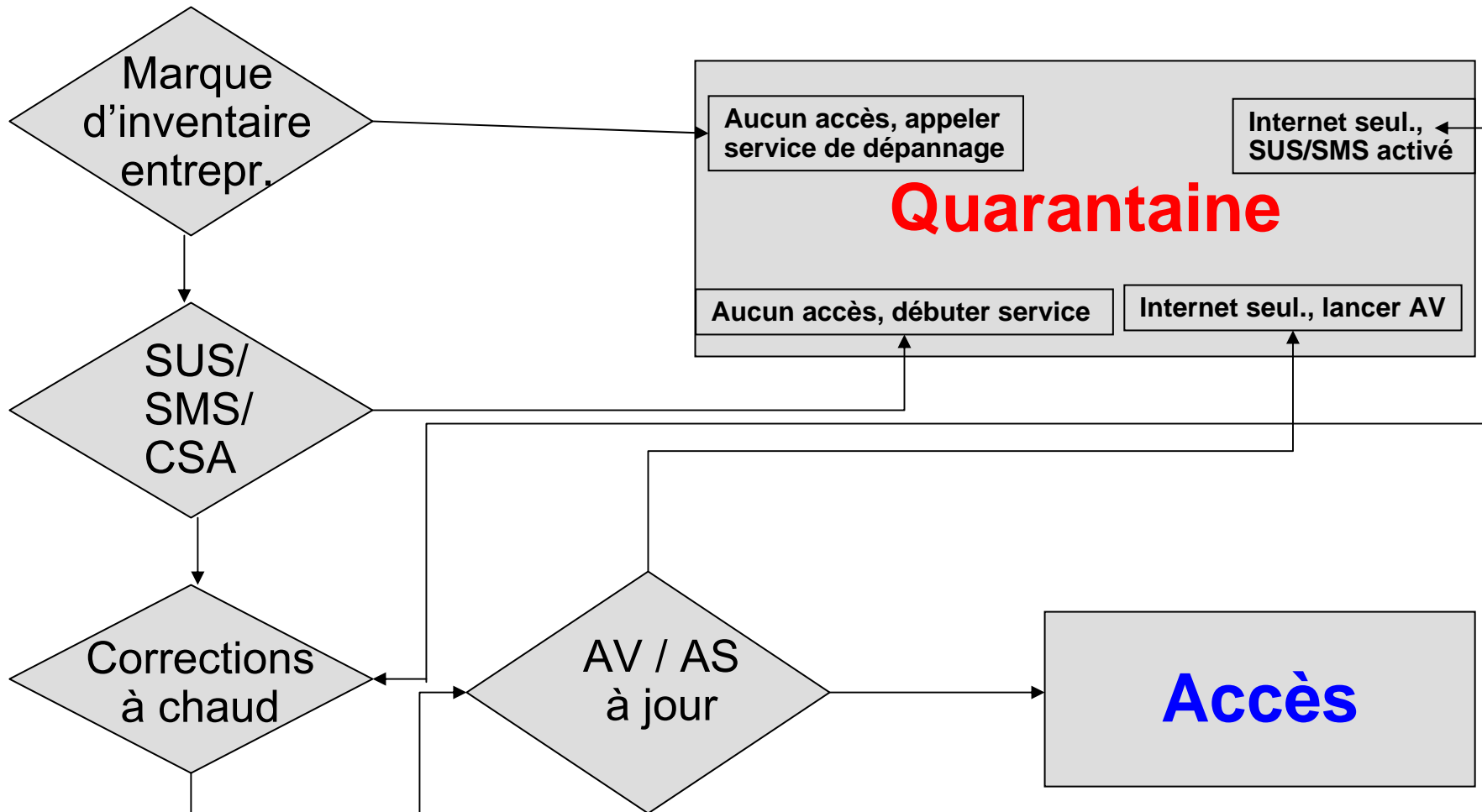
## Corrections à chaud de Microsoft :

- Vérifications de corrections à chaud vitales (fournies via des mises à jour Cisco automatisées)
- SUS/WUS activé ou AU Options (peut forcer le paramétrage)
- Logiciel de gestion de correctifs activé (peut lancer qualified .exe)

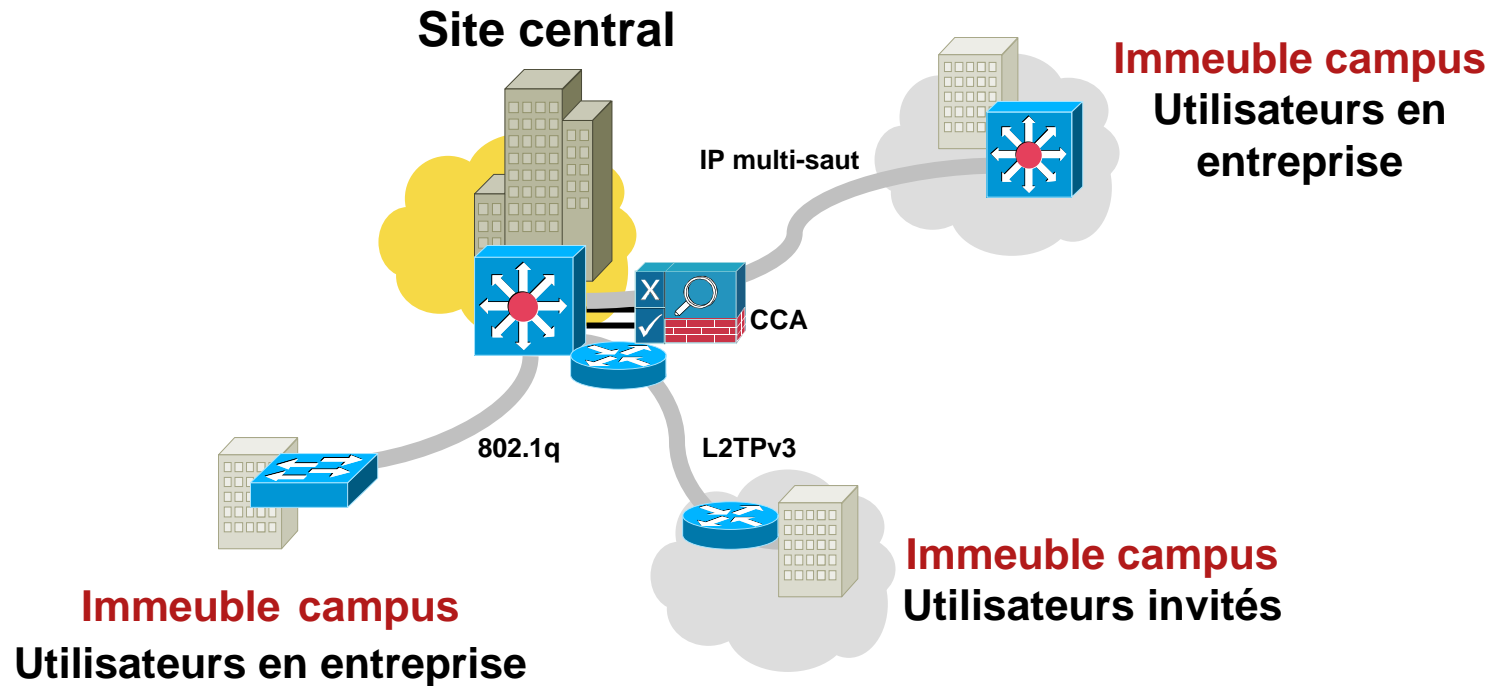
## Applications de sécurité :

- HIDS (CSA) ou pare-feu personnel installé et activé
- Antivirus installé et activé, et le DAT le plus récent (peut lancer un AV)
- Anti-logiciel espion installé et activé
- Logiciel de chiffrement installé et actif

# NAC Decision Tree relatif aux employées



# Cisco Clean Access pour un réseau local d'entreprise



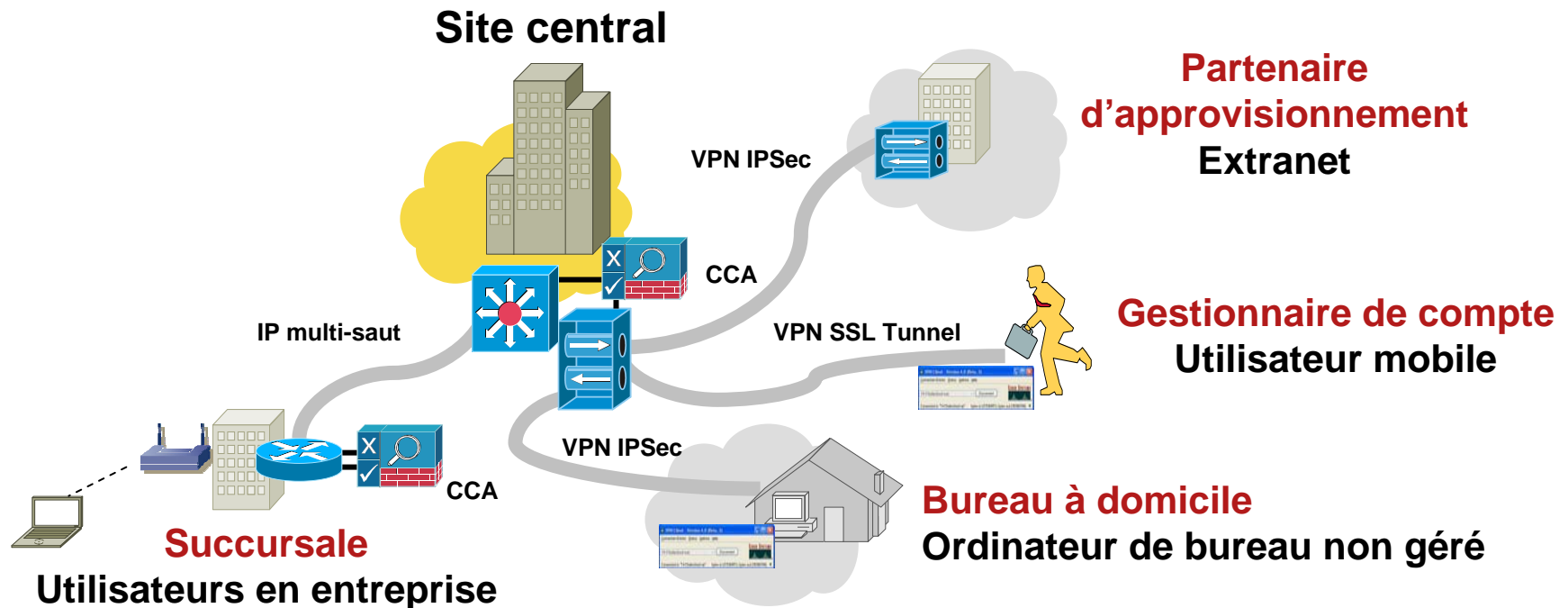
## CARACTÉRISTIQUES

- Supporte l'agrégation 802.1q
- Supporte L3 multi-saut et L2
- Supporte la tunnelisation L2TPv3
- Supporte intrabande et hors-bande

## AVANTAGES

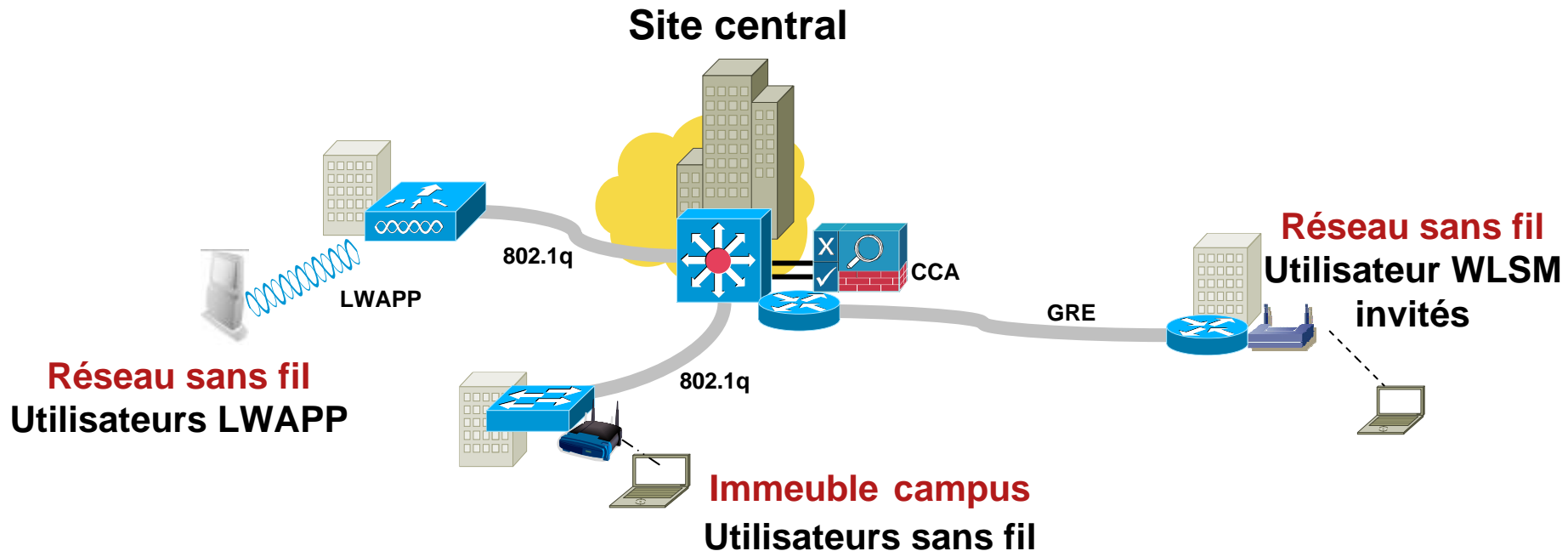
- Permet un mode de déploiement central
- Les dispositifs des utilisateurs finals peuvent être situés à une distance de plusieurs sauts
- Étend la mise en application aux immeubles du campus
- Tire parti de AD SSO

# Cisco Clean Access pour utilisateurs à distance



CARACTÉRISTIQUES	AVANTAGES
<ul style="list-style-type: none"> <li>Supporte les réseaux VPN IPsec et SSL Tunnel</li> <li>Supporte les réseaux VPN site-à-site</li> <li>Supporte l'ouverture de session d'un utilisateur VPN</li> </ul>	<ul style="list-style-type: none"> <li>Étend l'application des politiques et la conformité à celles-ci aux utilisateurs VPN et à distance</li> <li>Étend l'application des politiques aux partenaires VPN site-à-site</li> <li>Tire parti de l'ouverture de session VPN pour signature unique</li> </ul>

# Cisco Clean Access pour utilisateurs sans fil



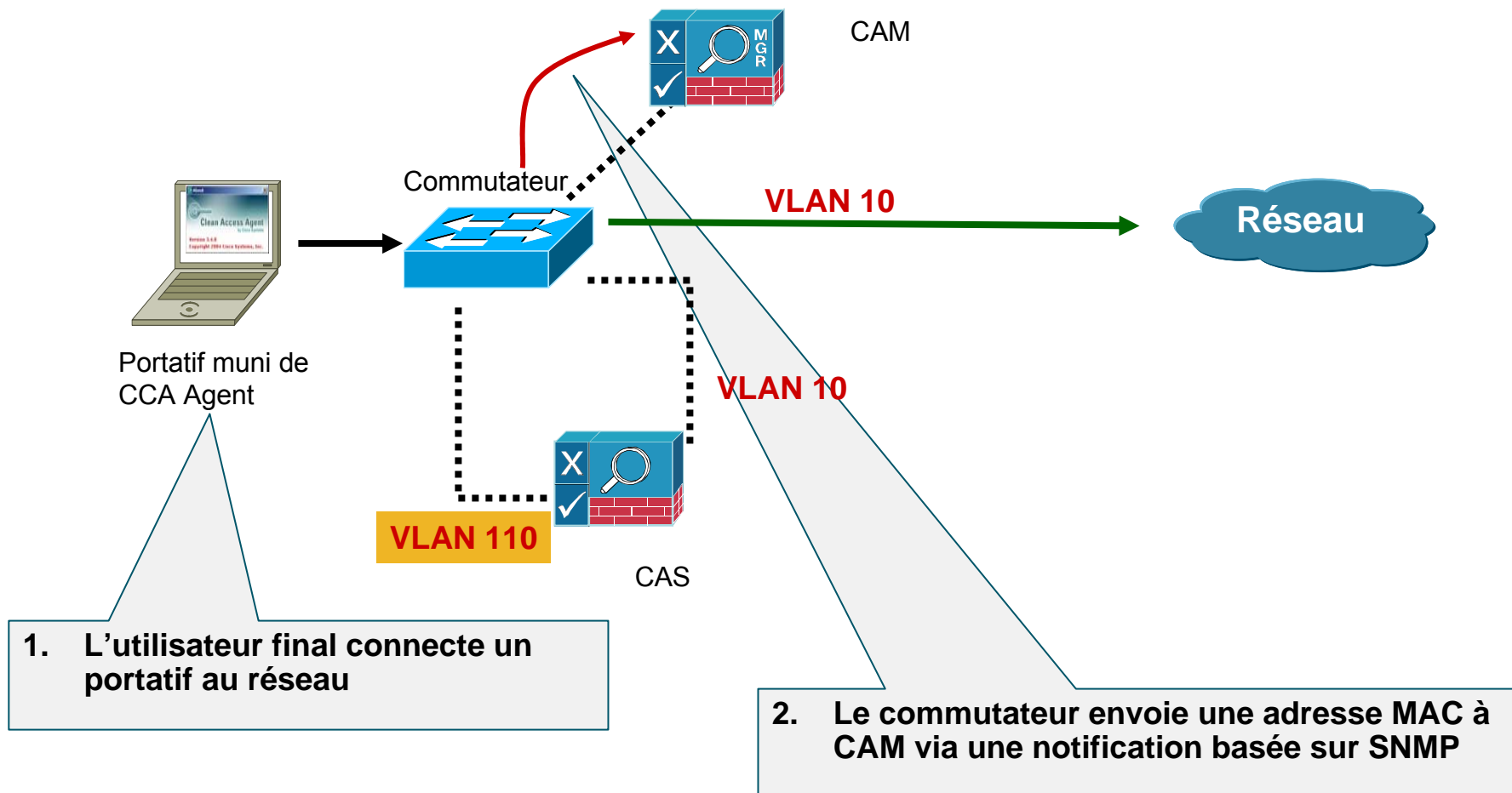
## CARACTÉRISTIQUES

- Supporte l'agrégation 802.1q
- Supporte la tunnelisation L2TPv3 ou GRE
- Supporte les points d'accès 802.11 sans fil complets ou allégés
- Supporte l'ouverture des sessions d'utilisateurs sans fil

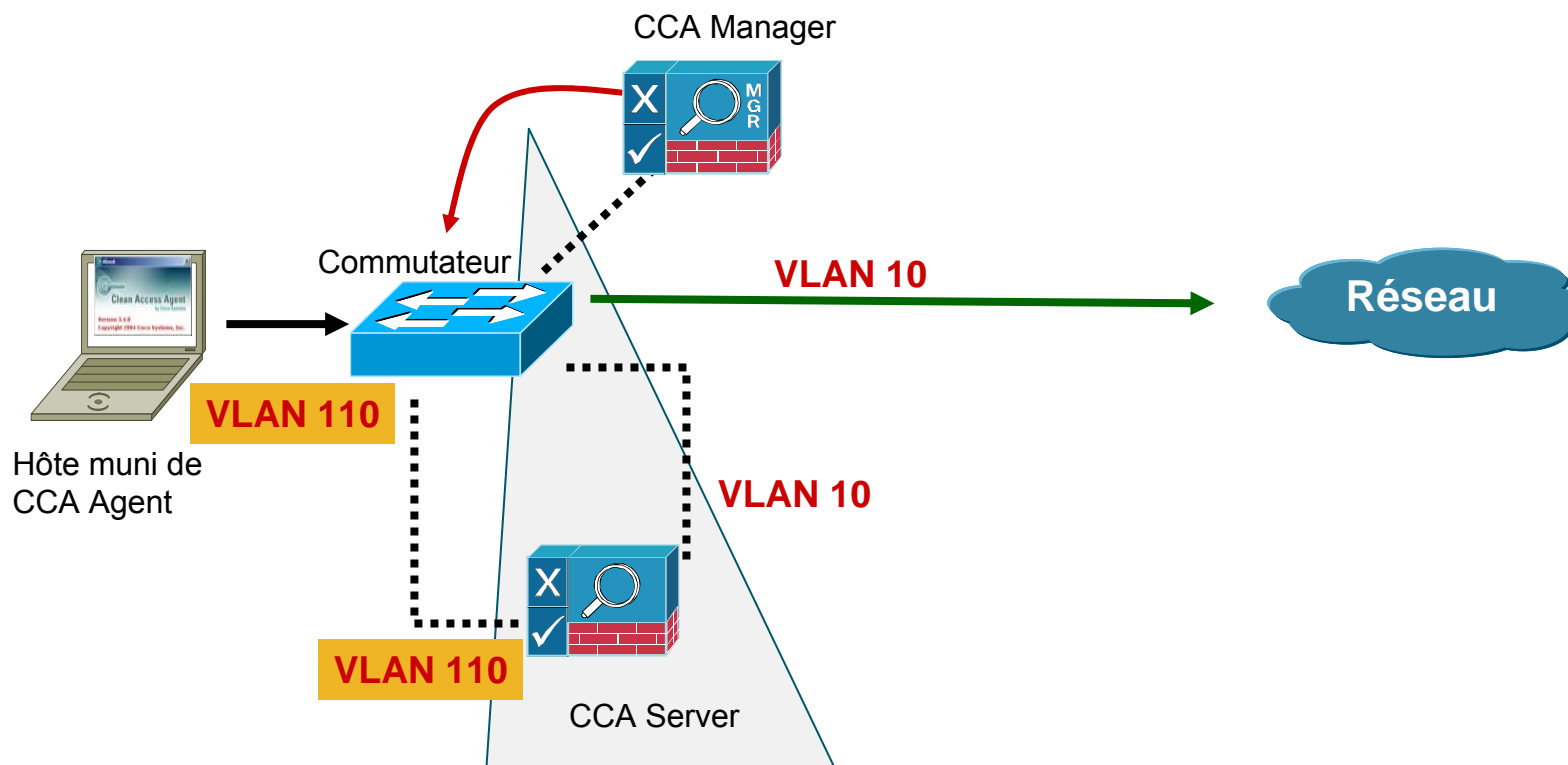
## AVANTAGES

- Permet un mode de déploiement central
- Les dispositifs des utilisateurs finals peuvent être situés à une distance de plusieurs sauts
- Étend l'application des politiques à n'importe quel réseau sans fil
- Tire parti de l'ouverture de session EAP pour signature unique

# NAC Appliance – Flux du processus Accès hors bande



# NAC Appliance – Flux du processus Accès hors bande

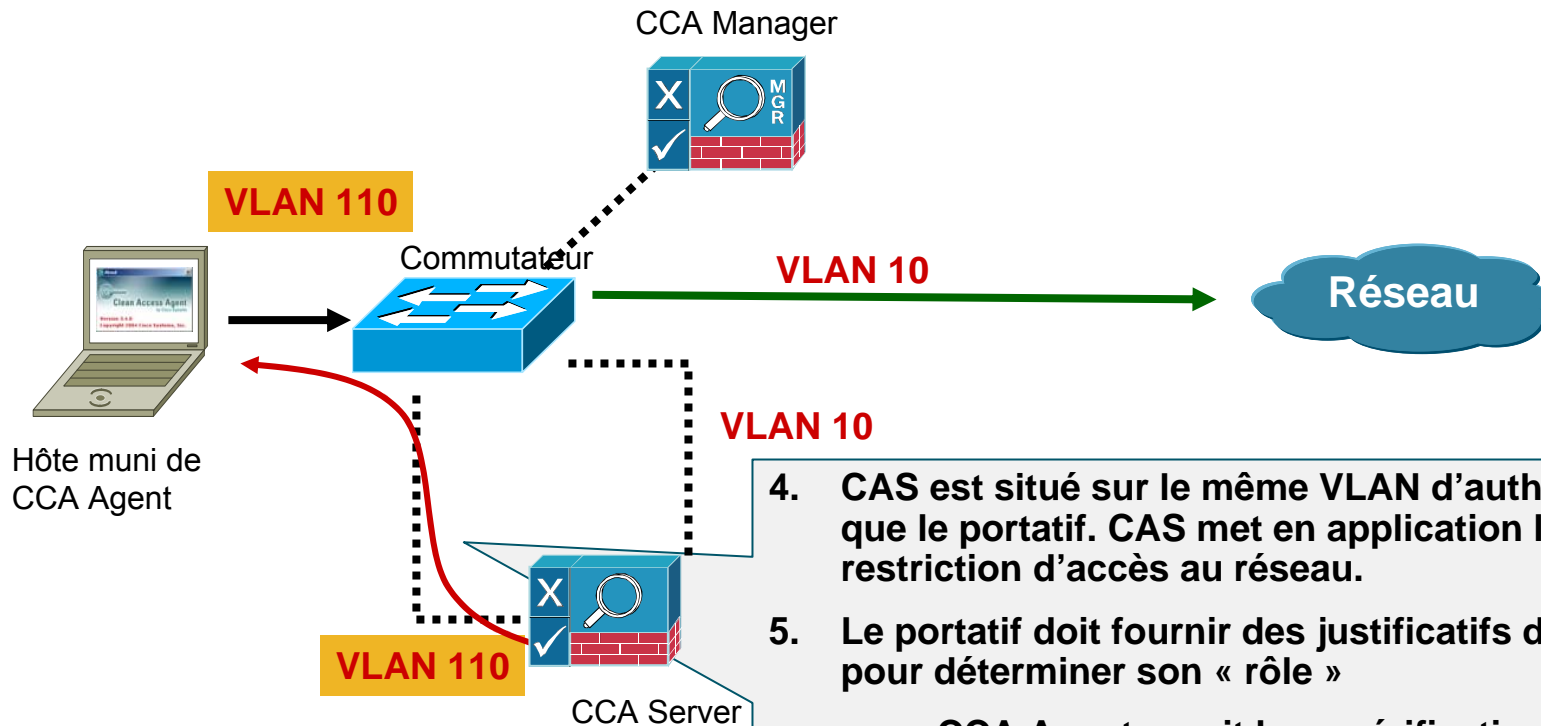


3. **CAM vérifie si le portatif est sur la liste « OOB online » ou « Certified devices ».**
  - Si le portatif n'est pas sur une de ces listes, CAM demande au commutateur d'attribuer un port au VLAN d'authentification.
  - Une adresse DHCP est attribuée au passage du trafic DHCP/DNS dans CAS, à l'aide d'une mise en correspondance VLAN.



# NAC Appliance – Flux du processus

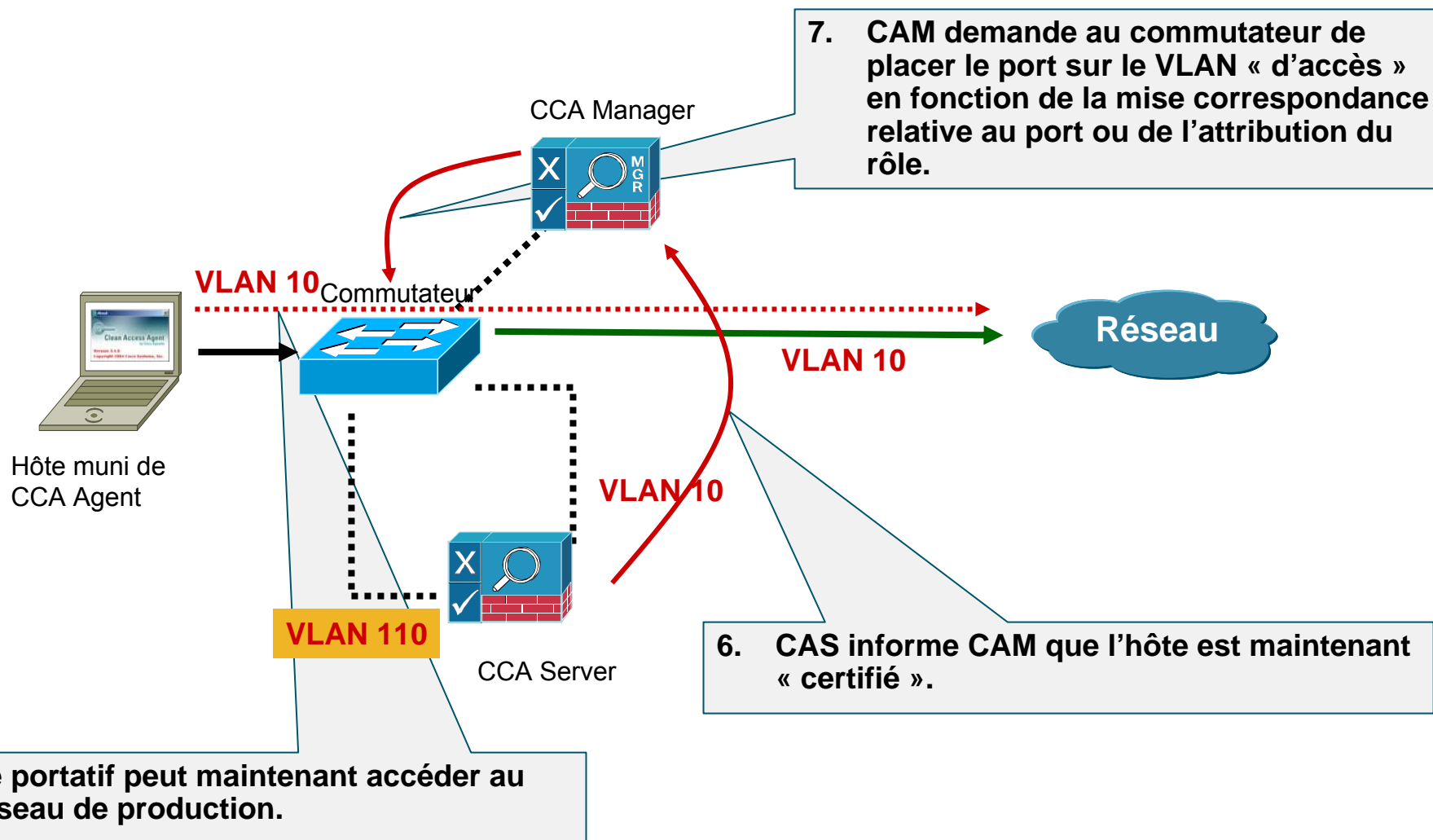
## Accès hors bande



4. CAS est situé sur le même VLAN d'authentification que le portatif. CAS met en application la restriction d'accès au réseau.
5. Le portatif doit fournir des justificatifs d'identité pour déterminer son « rôle »
  - CCA Agent reçoit les « vérifications » de conformité de CAS basées sur le « rôle ».
  - CCA Agent guide l'hôte étape par étape dans le processus de correction.
  - L'utilisateur a la permission d'accéder aux sites de correction mis en application par CAS.

# NAC Appliance – Flux du processus

## Accès hors bande



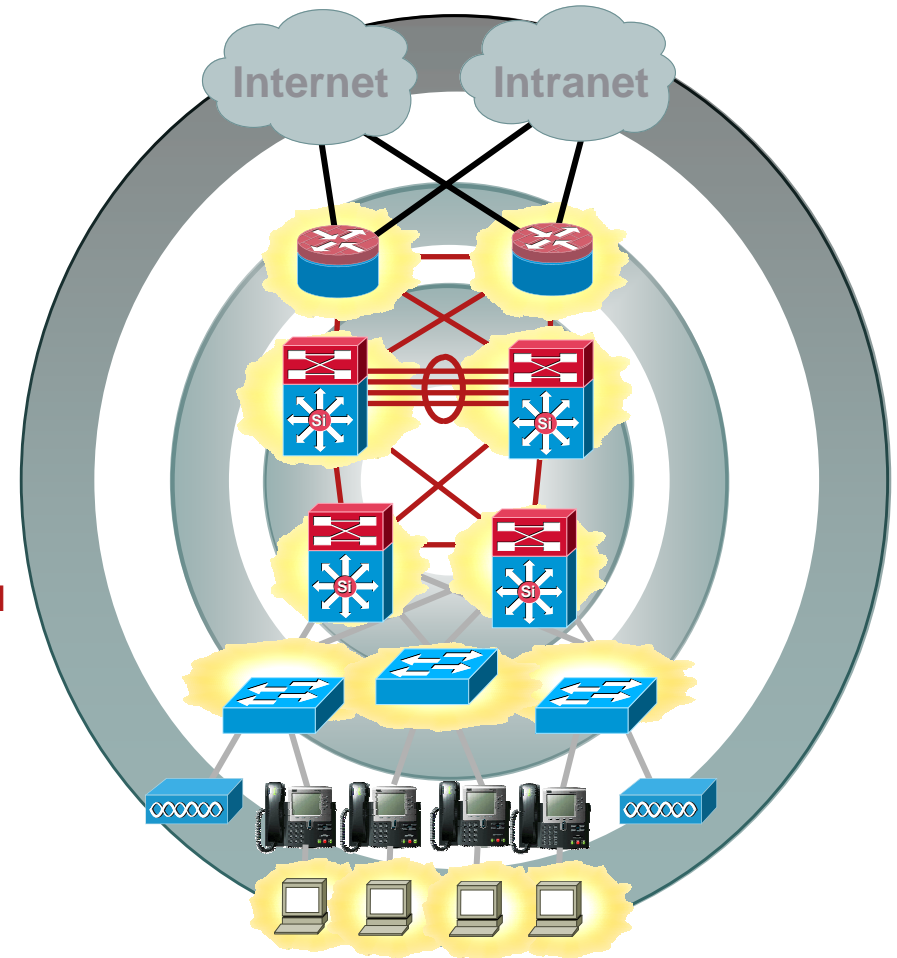
# NAC Appliance – Flux du processus

## Accès hors bande



# Programme

- Authentication
  - ▲ Qui peut accéder le réseau
  - ▲ L'impact de la téléphonie
  - ▲ 802.1x, les visiteurs, Web Base . Authentication
- La conformité des postes au moment de la connexion
  - ▲ Sur le LAN, en VPN, etc...
- Les bonnes pratiques pour le contrôle des usagers connectés au réseau
  - ▲ Fonctions de sécurité présentent dans les commutateurs Cisco
  - ▲ QoS déployée?
  - ▲ Cisco Sécurité Agent (CSA)
- La surveillance et la configuration du réseau



# Listes de contrôle des accès de Catalyst

## Fonction :

Permet ou refuse l'accès en fonction de l'adresse source ou de destination.

Limite les utilisateurs à des zones désignées du réseau, bloquant les accès non autorisés à toutes les autres applications et informations.

## Avantages :

Empêche les accès non autorisés aux serveurs et aux applications.

Permet à des utilisateurs choisis d'accéder à des serveurs spécifiques.

**PACL** – Fournit un contrôle granulaire, aux fins d'accès limité via le port d'accès du dispositif

**RACL** – Contrôle le trafic sur les interfaces des couches 2 et 3.

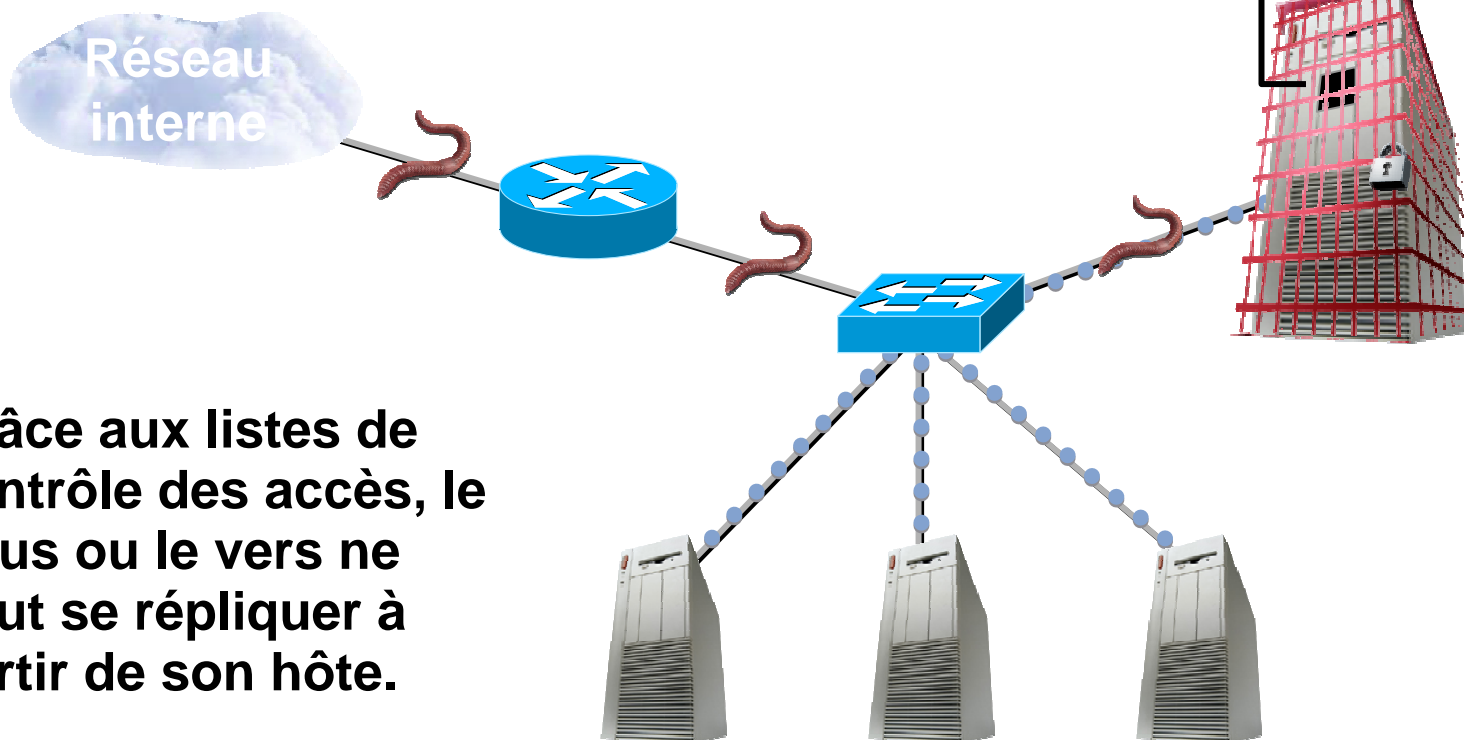
**VACL** – Fournit un contrôle granulaire, aux fins d'accès limité à même un réseau VLAN ou un sous-réseau.

**Time-Based ACL** – ACL s'active à un moment précis de la journée

# Protection contre les vers – 1

## Fonctionnement :

La liste ACL fournit un mécanisme qui permet de protéger les serveurs, les utilisateurs et les applications contre les vers, en déterminant quels flux de trafic ou utilisateurs peuvent accéder à quels ports.



Grâce aux listes de contrôle des accès, le virus ou le vers ne peut se répliquer à partir de son hôte.

# Listes de contrôle des accès basées sur l'heure

Fonctionnement :

Contrôle la commutation des données en fonction de l'heure du jour.



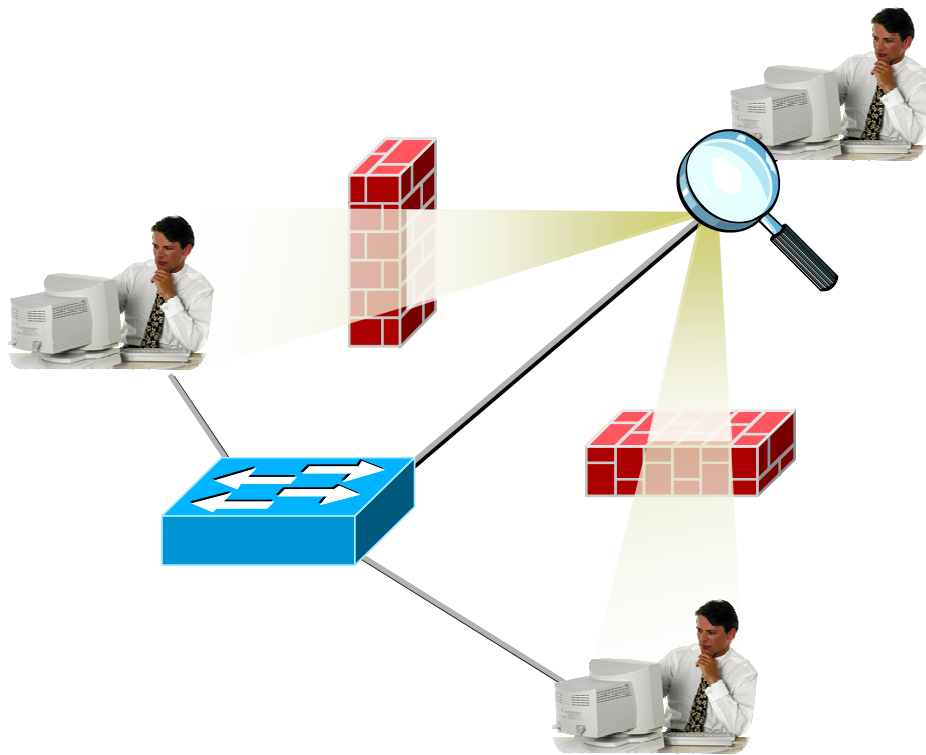
OK to Use server 1  
Not OK to Use server 2  
OK to Use Server 3  
Not OK to Use Server 4



ACL démarre  
à 8 h

ACL s'arrête  
à 17 h

# Assurer la séparation des voisins



## Problème :

Des voisins sur le même commutateur peuvent voir leur trafic mutuel, y compris les ID et mots de passe d'ouverture de session. Mise en application de la politique régissant la façon dont le trafic passe entre les groupes de travail.

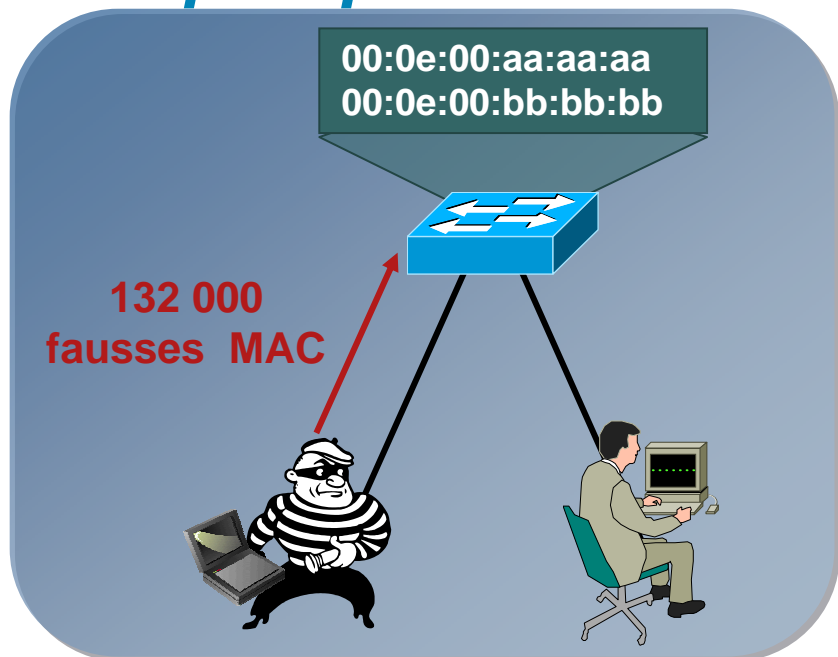
## Solution :

Une périphérie VLAN privée pour bloquer le trafic de couche 2 entre des utilisateurs sur un même réseau VLAN

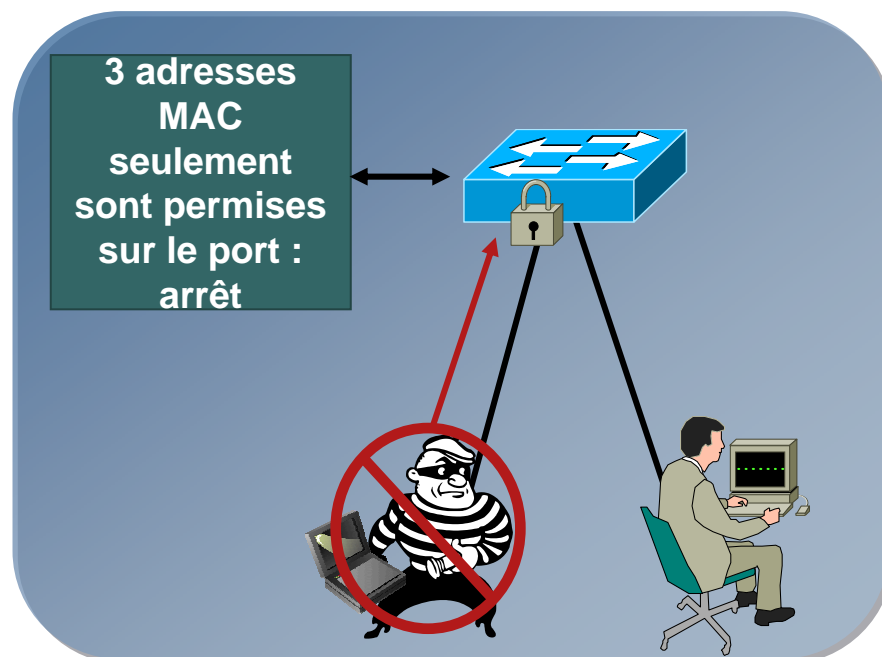


# Monter la barre en matière de surveillance des attaques

## Attaques par inondation d'adresses MAC



- Des outils de « pirate adolescent » permettent d'inonder les tables CAM du commutateur avec de fausses adresses MAC; transformer le réseau VLAN en « concentrateur » et éliminer le piratage
- La table CAM du commutateur supporte un nombre limité d'adresses MAC



- La sécurité du port limite les attaques par inondation d'adresses MAC, verrouille le port et envoie un déroutement SNMP

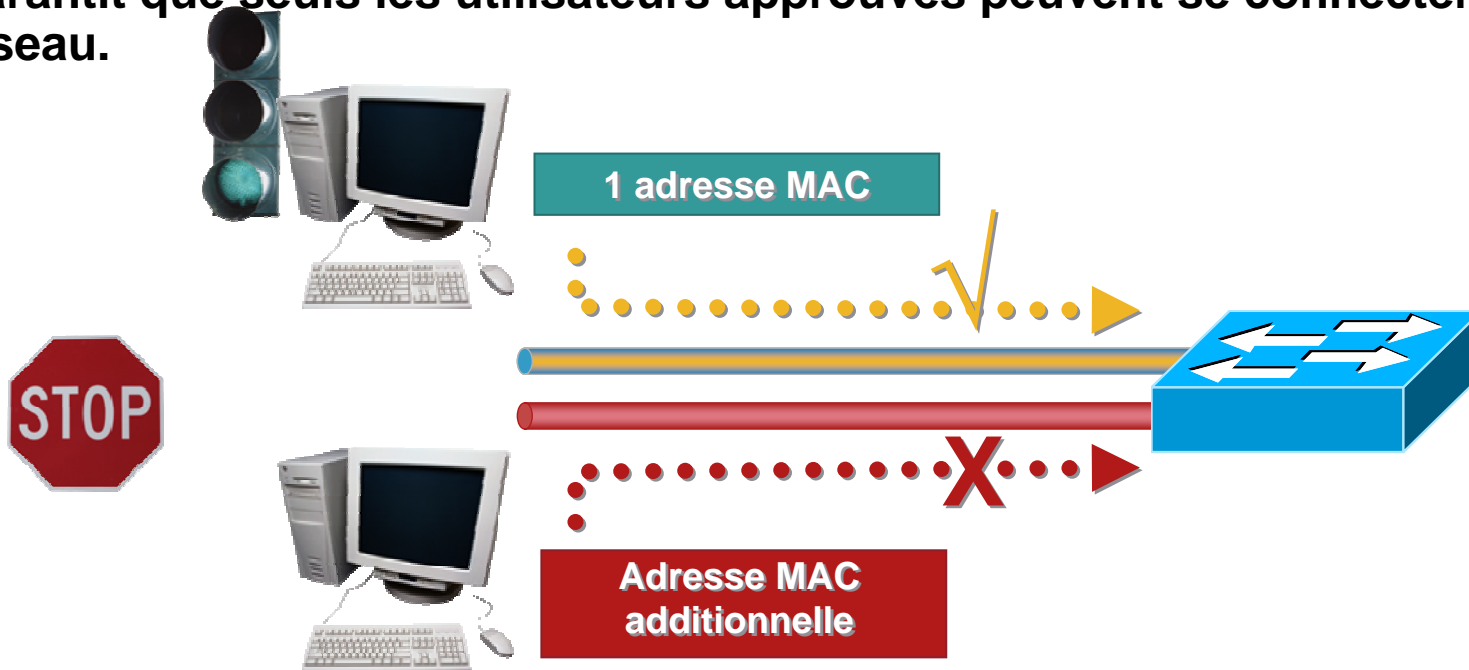
# Sécurité du port

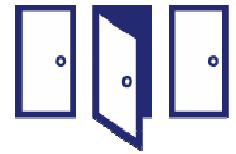
## Fonction :

Limite le nombre d'adresses MAC qui peuvent se connecter à un commutateur et garantit que seules les adresses MAC approuvées peuvent accéder au commutateur.

## Avantages :

Garantit que seuls les utilisateurs approuvés peuvent se connecter au réseau.

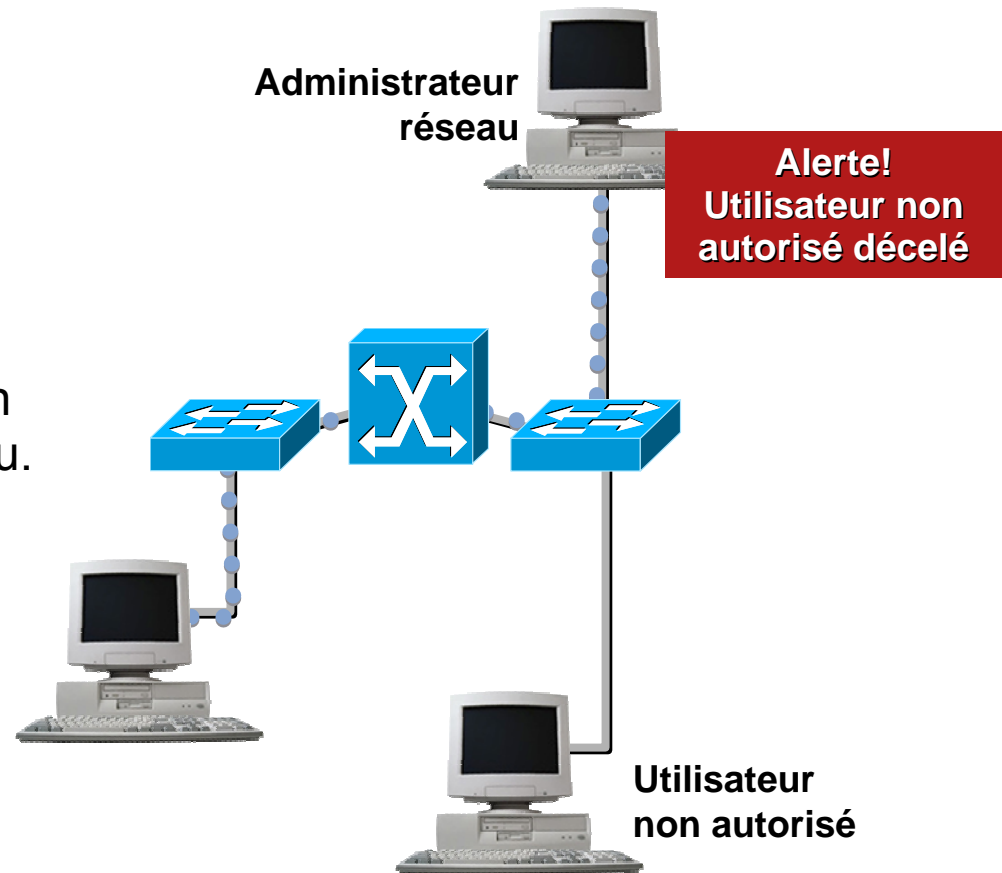




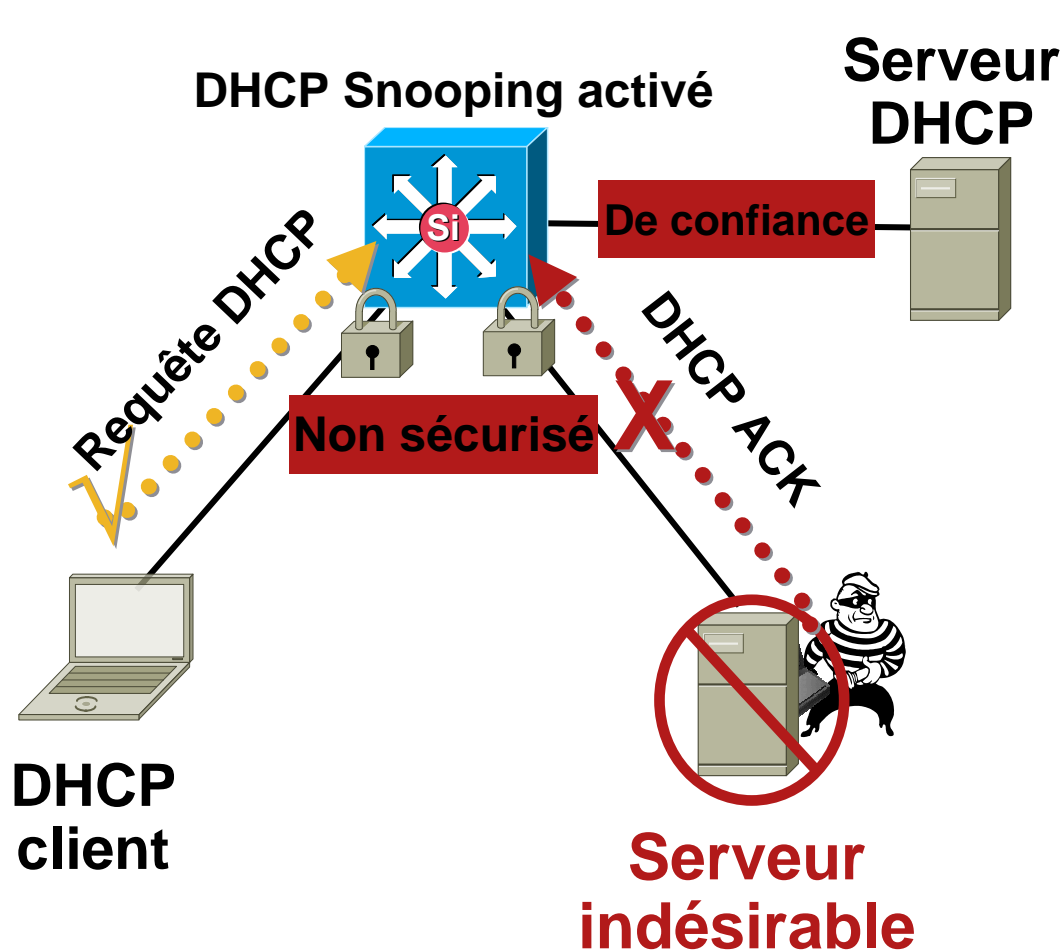
# Notification d'intrusion

- **MAC Address Notification**

Alerte les administrateurs réseau si des utilisateurs non autorisés accèdent au réseau.



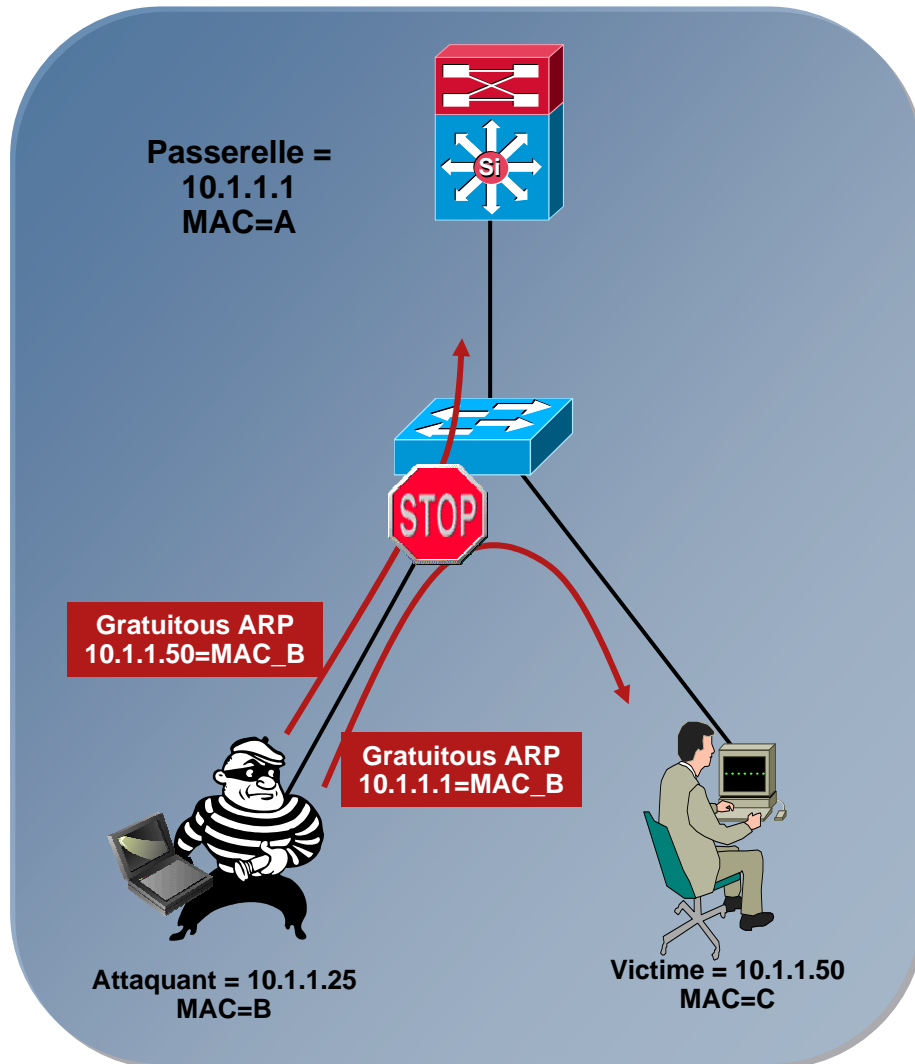
# Surveillance du trafic DHCP



**Fonctionnement :**  
Le commutateur envoie seulement des requêtes DHCP à partir de ports d'accès non sécurisés, élimine tous les autres types de trafic DHCP. N'accepte que les ports DHCP ou de liaison montante désignés et de confiance pour transmettre des messages DHCP.  
Crée une table d'associations DHCP qui renferme l'adresse IP client, l'adresse MAC client, le numéro de port et de réseau VLAN

**Avantage :**  
Empêche des dispositifs indésirables de se comporter comme un serveur DHCP

# Dynamic ARP Inspection

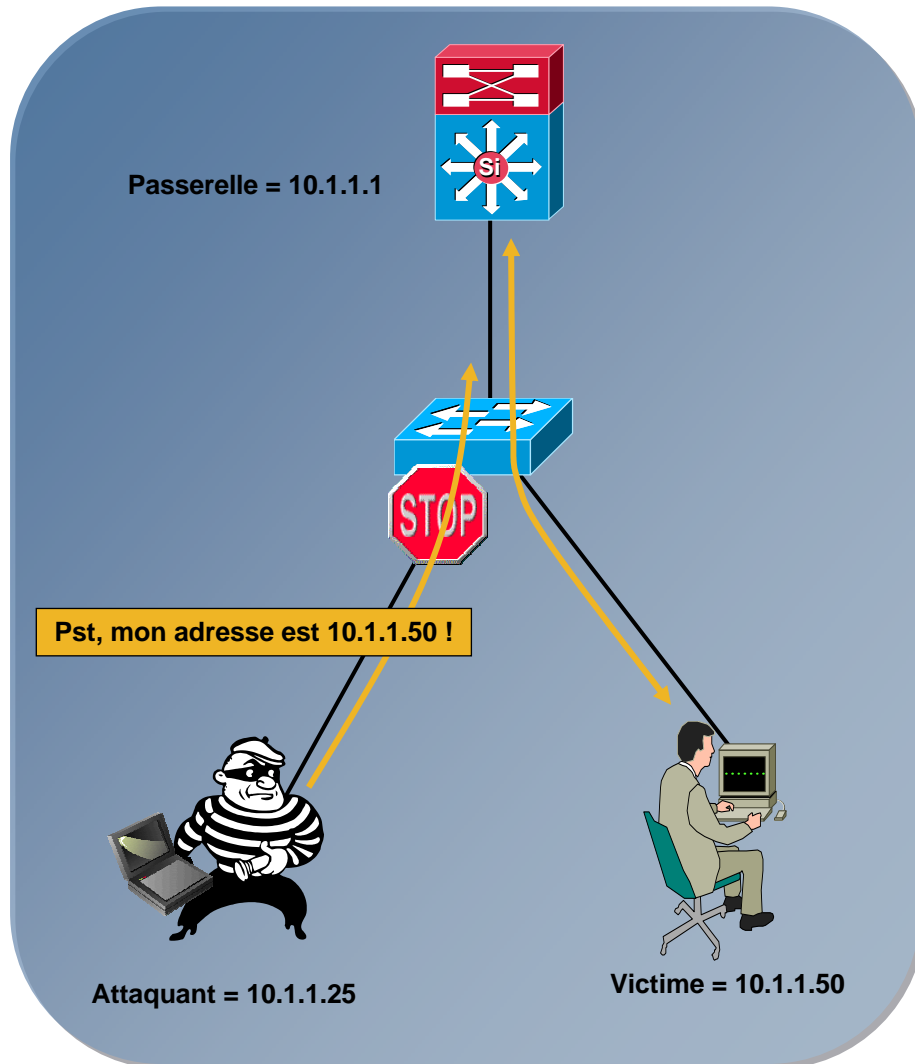


## Dynamic ARP Inspection *protège contre l'empoisonnement de ARP*

- Utilise la table des associations liée à la surveillance du trafic de DHCP
- Piste les adresses MAC à IP, à partir de transactions DHCP
- Limite le volume de requêtes ARP lancées à partir de ports client; arrête le balayage des ports
- Élimine les faux ARP; empêche l'empoisonnement de ARP, les attaques par intermédiaire (MIM)

# IP Source Guard

## Protection contre les fausses adresses IP



## IP Source Guard protège contre les fausses adresses IP

- Utilise la table des associations liée à la surveillance du trafic de DHCP
- Retracer l'adresse IP aux associations relatives aux ports
- Programme dynamiquement la liste de contrôle des accès du port pour que soit éliminé le trafic qui ne provient pas d'une adresse IP attribuée via DHCP

# Réseau VLAN privé

Fonctionnement :

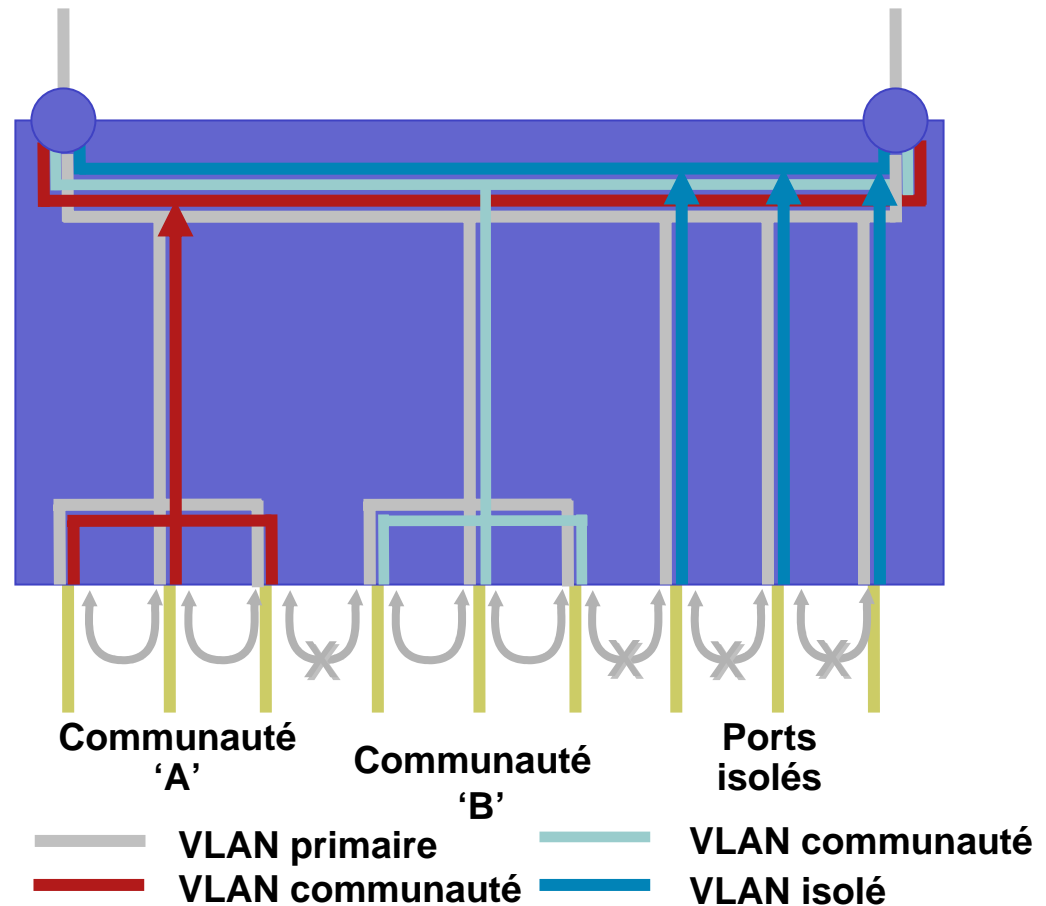
Un sous-réseau commun est subdivisé en de multiples VLAN privés. Les hôtes d'un VLAN privé donné peuvent uniquement communiquer avec la passerelle par défaut et NON avec d'autres hôtes sur le réseau.

Avantage :

Mécanisme simplifié de gestion du trafic tout en conservant l'espace adresse IP

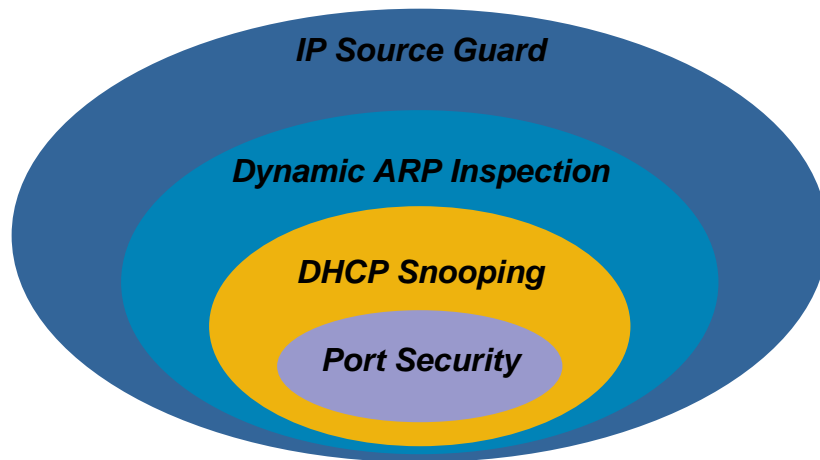
Passerelle par défaut

Passerelle par défaut



# Fonctions de sécurité intégrées du Catalyst

## Sommaire IOS



- Port Security empêche les attaques par inondation d'adresses MAC
- DHCP Snooping empêche l'attaque de clients sur le commutateur et le serveur
- Dynamic ARP Inspection ajoute une sécurité à ARP, en utilisant la table de surveillance du trafic de DHCP
- IP Source Guard ajoute une sécurité à l'adresse IP source, en utilisant la table de surveillance de DHCP
- Toutes ces fonctions sont utilisées sur les ports de commutateurs

```
ip dhcp snooping  
ip dhcp snooping vlan 2-10  
ip arp inspection vlan 2-10  
!  
interface fa3/1  
switchport port-security  
switchport port-security max 3  
switchport port-security violation restrict  
switchport port-security aging time 2  
switchport port-security aging type inactivity  
ip arp inspection limit rate 100  
ip dhcp snooping limit rate 100  
!  
Interface gigabit1/1  
ip dhcp snooping trust  
ip arp inspection trust
```





## Cisco Security Agent : prévention des intrusions basée sur l'hôte



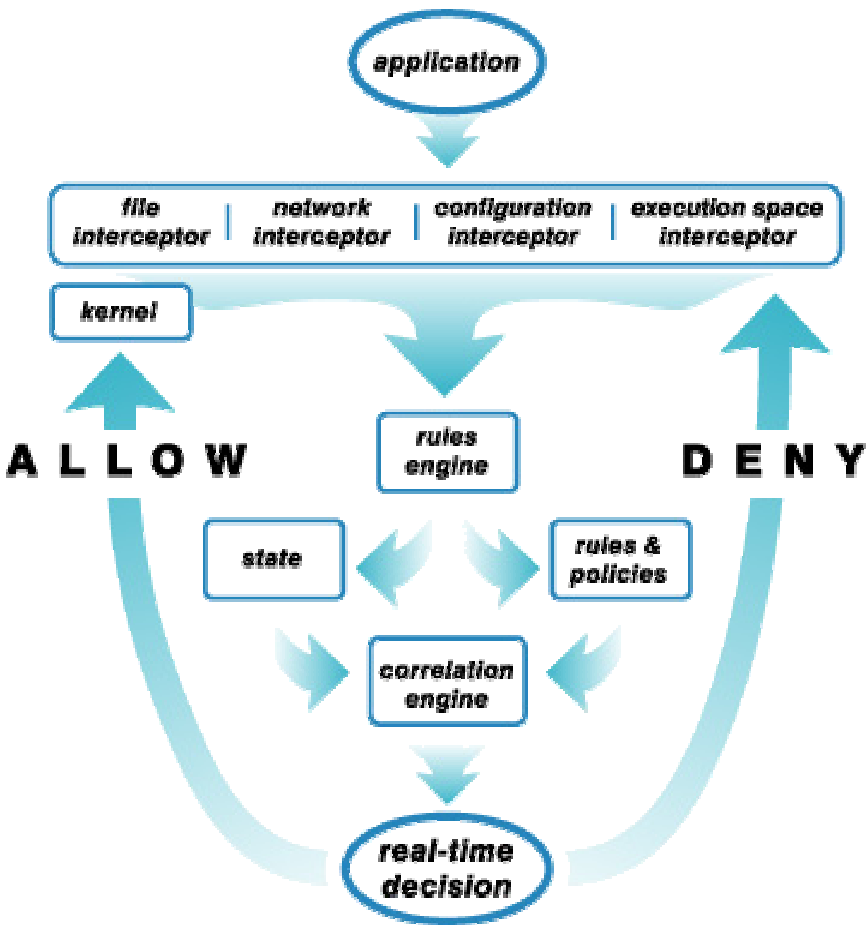
Point limite + réseau = Sécurité collaborative **efficace**

# Protection à partir du jour J

- Cisco définit la prévention des intrusions basée sur l'hôte comme **la capacité de bloquer les programmes malveillants de type jour J, sans reconfiguration ou mise à jour.**
- CSA a arrêté de façon efficace les exploits jour J, vers et virus au cours des six dernières années :
  - 2001 – Code Red, Nimda (les 5 exploits), Pentagone (Gonner)
  - 2002 – Sircam, Debplot, SQL Snake, Bugbear,
  - 2003 – SQL Slammer, So Big, Blaster/Welchia, Fizzer
  - 2004 – MyDoom, Bagle, Sasser, exploit JPEG browser (MS04-028), exploit RPC-DCOM (MS03-039), Buffer Overflow in Workstation service (MS03-049)
  - 2005 – Internet Explorer Command Execution Vulnerability, Zotob
  - 2006 – Internet Explorer textrange vulnerability

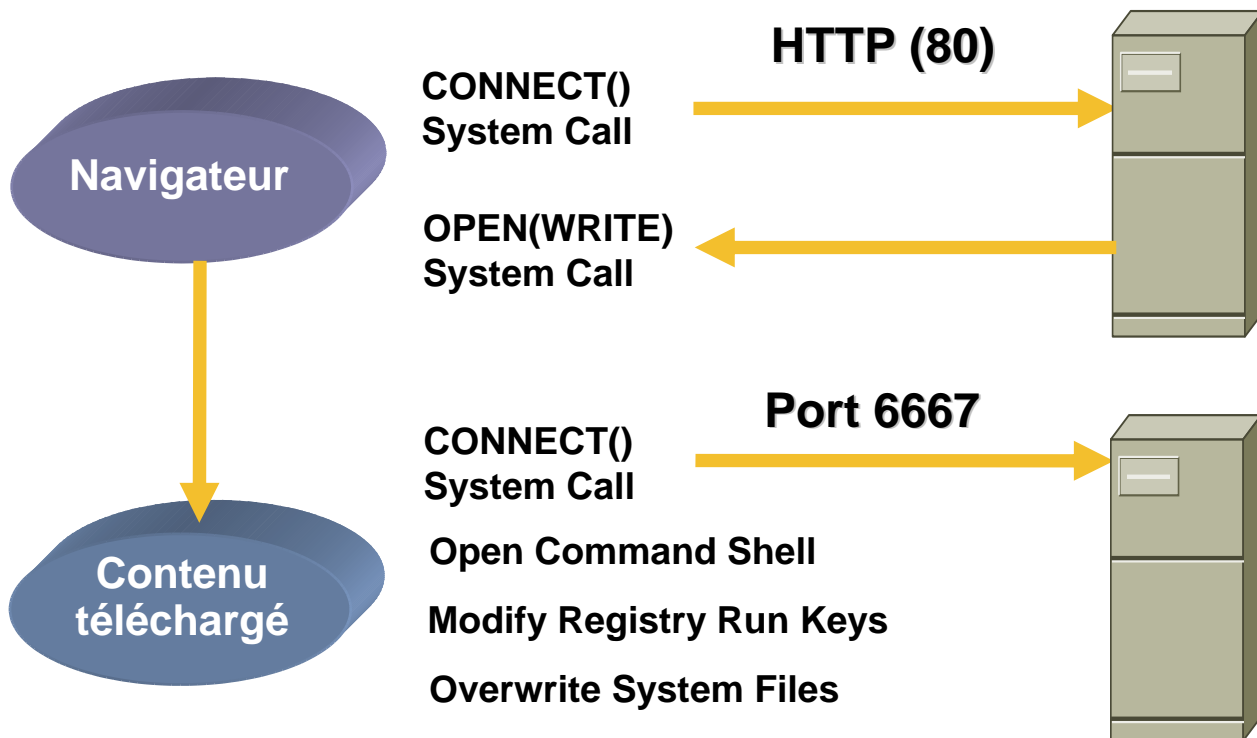
Aucune signature, reconfiguration ou mise à jour binaire requise

# Interception des appels système



- Cisco Security Agent intercepte les appels système d'applications et invoque une réponse permission/refus
- Des intercepteurs surveillent les appels de ressources d'accès :
  - Système de fichiers
  - Réseau (entrant/sortant)
  - Registre
  - Exécution (création de processus, accès aux bibliothèques, appel exécutable)
- Architecture « Zero Update » – un contrôle basé sur le comportement signifie que vous n'avez pas besoin d'une nouvelle signature pour arrêter la prochaine attaque

# Corrélation

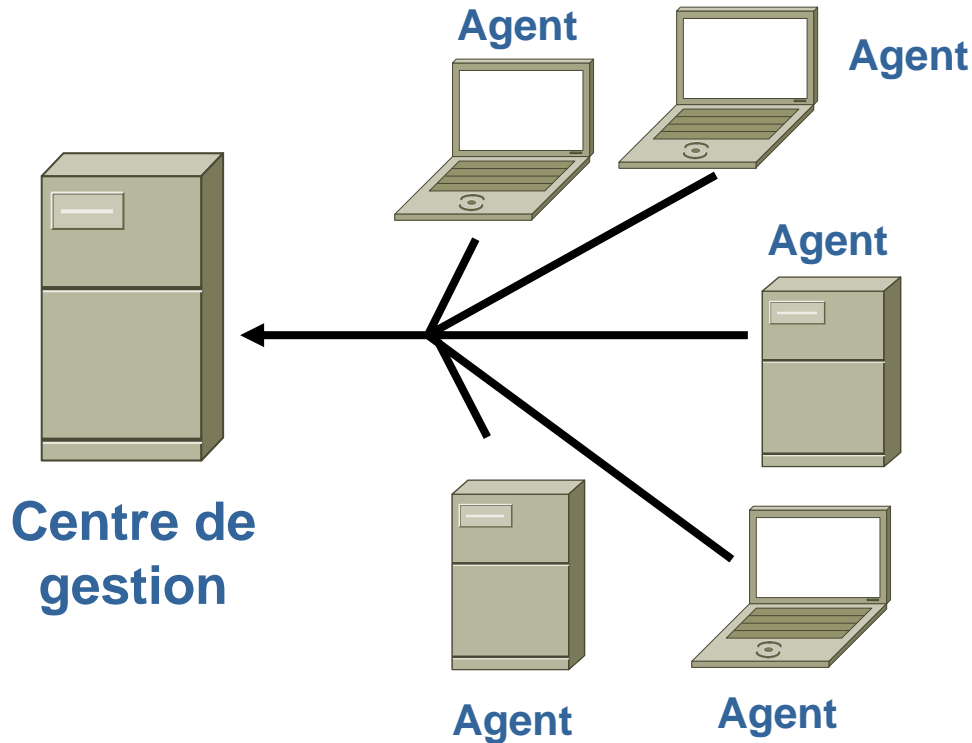


Un comportement malveillant est identifié de façon précise en contexte. La corrélation de Cisco Security Agent fait cela automatiquement – aucune configuration requise.

# Comportement malveillant



# Corrélation globale



**Cisco Security Agent offre une corrélation unique au plan des agents et de la gestion**

## Corrélation sur l'agent

- Plus grande précision
- Moins de « faux positifs »

## Corrélation sur le gestionnaire

- Plus grande précision
- Moins de « faux négatifs »
- Arrête les attaques avant qu'elles n'atteignent leur cible

Exemple : « balayages par ping » répartis, propagation de vers sur le réseau

# CSA Policy Control

- Certains types de comportements ne sont pas malveillants, mais sont indésirables, car ils violent la politique d'étiquette de réseau
  - Partage de musique via des applications poste à poste (p2p)
  - Messagerie instantanée utilisant des serveurs IM qui n'appartiennent pas à l'entreprise
  - Protection des données organisationnelles confidentielles
  - Verrouillage de la configuration pendant la période de création des rapports de fin d'exercice
  - Quels dispositifs ne peuvent pas être utilisés (mémoire USB, dispositifs multimédia)
  - Utilisation d'applications non autorisées ou de versions d'applications non autorisées
- Les modules CSA Policy Control incluent :
  - Une politique de prévention de vol de données
  - Une politique de contrôle de la messagerie instantanée
  - Une politique de prévention de téléchargement de musique
  - Une politique de verrouillage de réseau

**Fournit des commentaires aux utilisateurs via des interrogations et vérifications en incrustation pour démontrer la conformité.**

# La qualité de service (QoS) comme solution

## Avantages de la QoS

### AU COURS DU DÉSASTRE

Les données à mission vitale passent quand même

Les applications sensibles au délai ne sont pas touchées

### EN GÉNÉRAL

Réductions des coûts – surtout sur les liaisons WAN

## Défis liés à la QoS

La limite de confiance s'arrête habituellement au commutateur d'accès

Processus de configuration lent basé sur les adresses et les ports

De nombreuses applications n'ont pas de fonctions de QoS

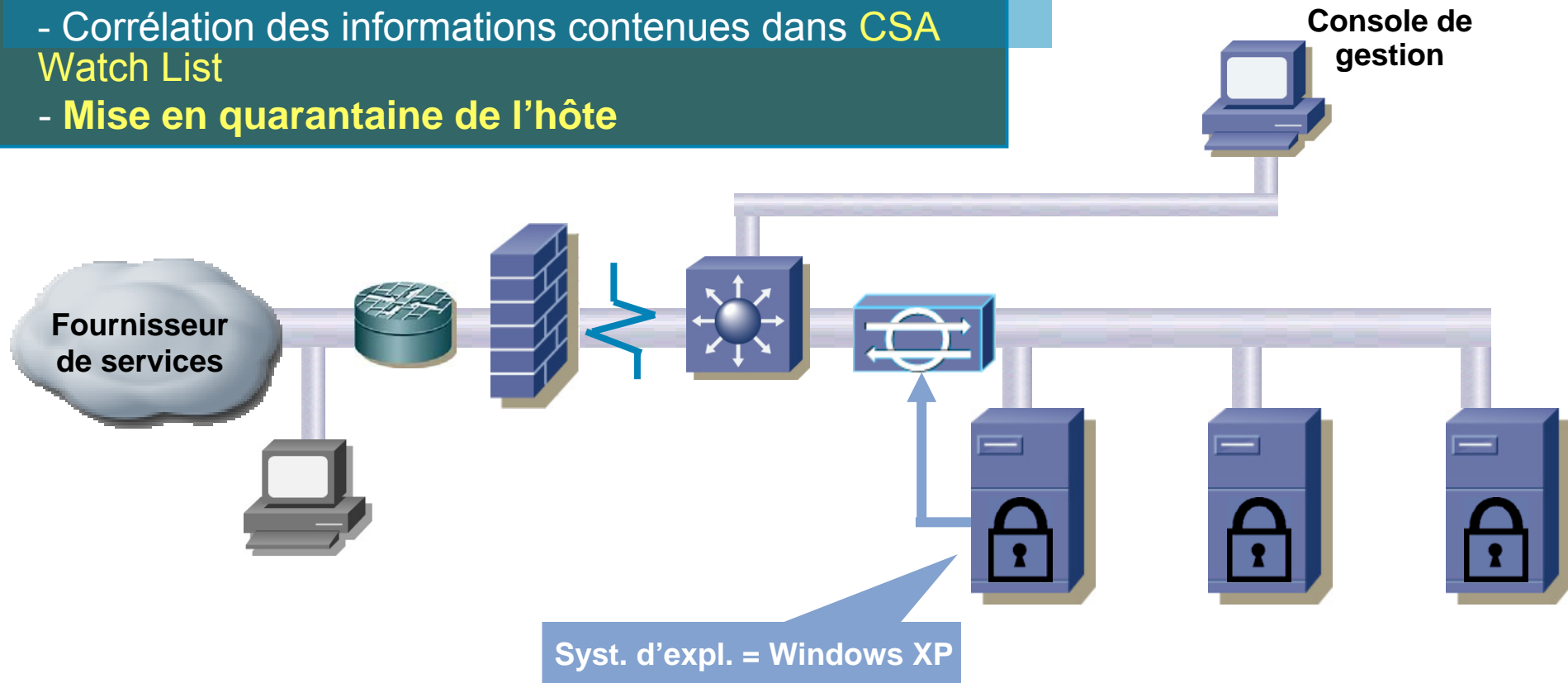
Les tricheurs peuvent biaiser la prestation d'un service

Toute la responsabilité de la QoS repose sur les activités du réseau



# CSA + IPS Collaboration avec Cisco Network IPS version 6.0

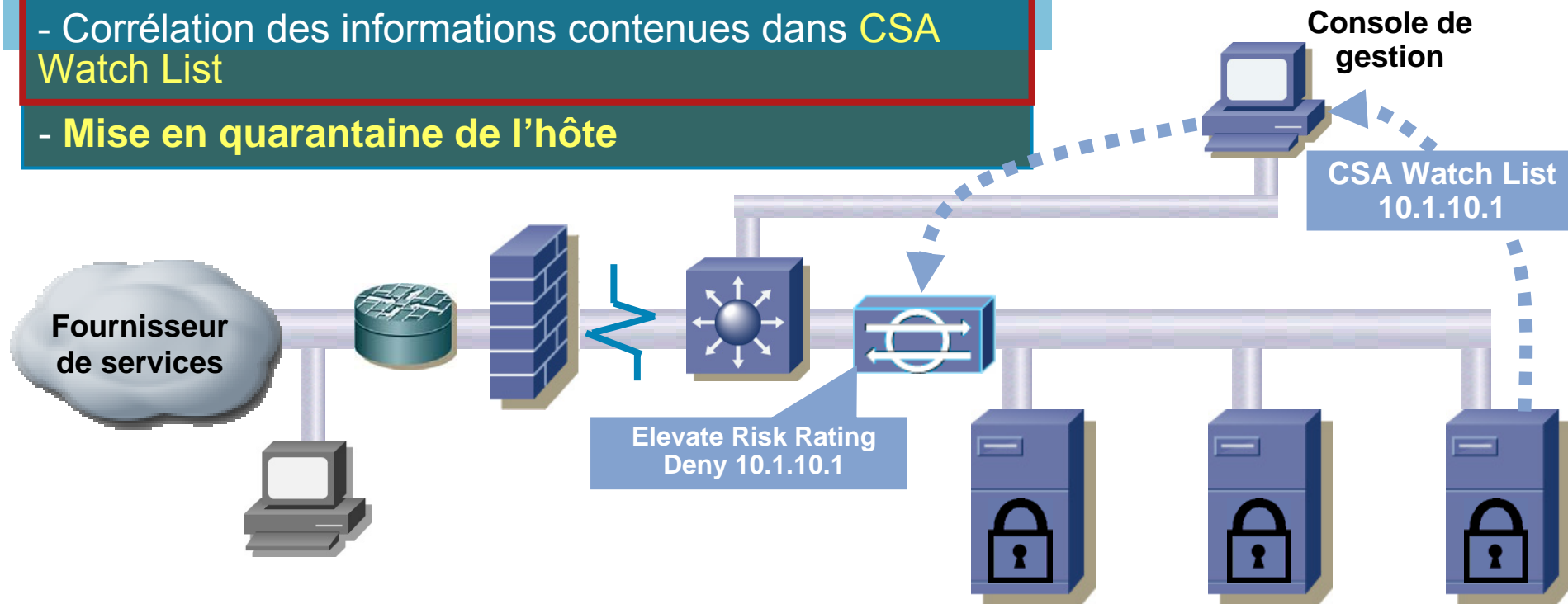
- Analyse contextuelle du point limite améliorée
- Capacité d'utiliser des données CSA pour influencer les actions IPS
- Corrélation des informations contenues dans CSA Watch List
- Mise en quarantaine de l'hôte



# CSA + IPS Collaboration

## avec Cisco Network IPS version 6.0

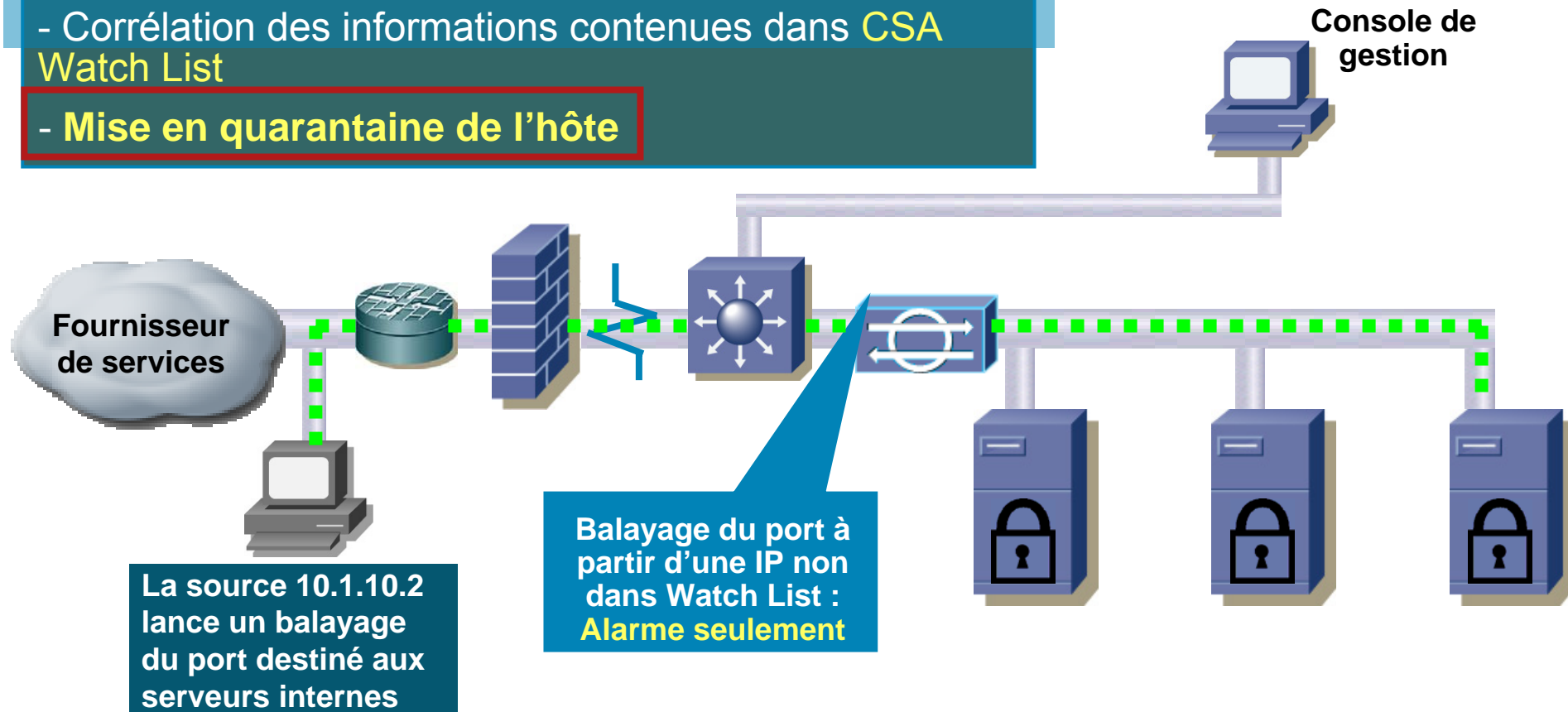
- Analyse contextuelle du point limite améliorée
- Capacité d'utiliser des données CSA pour influencer les actions IPS
- Corrélation des informations contenues dans CSA Watch List
- Mise en quarantaine de l'hôte



# CSA + IPS Collaboration

## avec Cisco Network IPS version 6.0

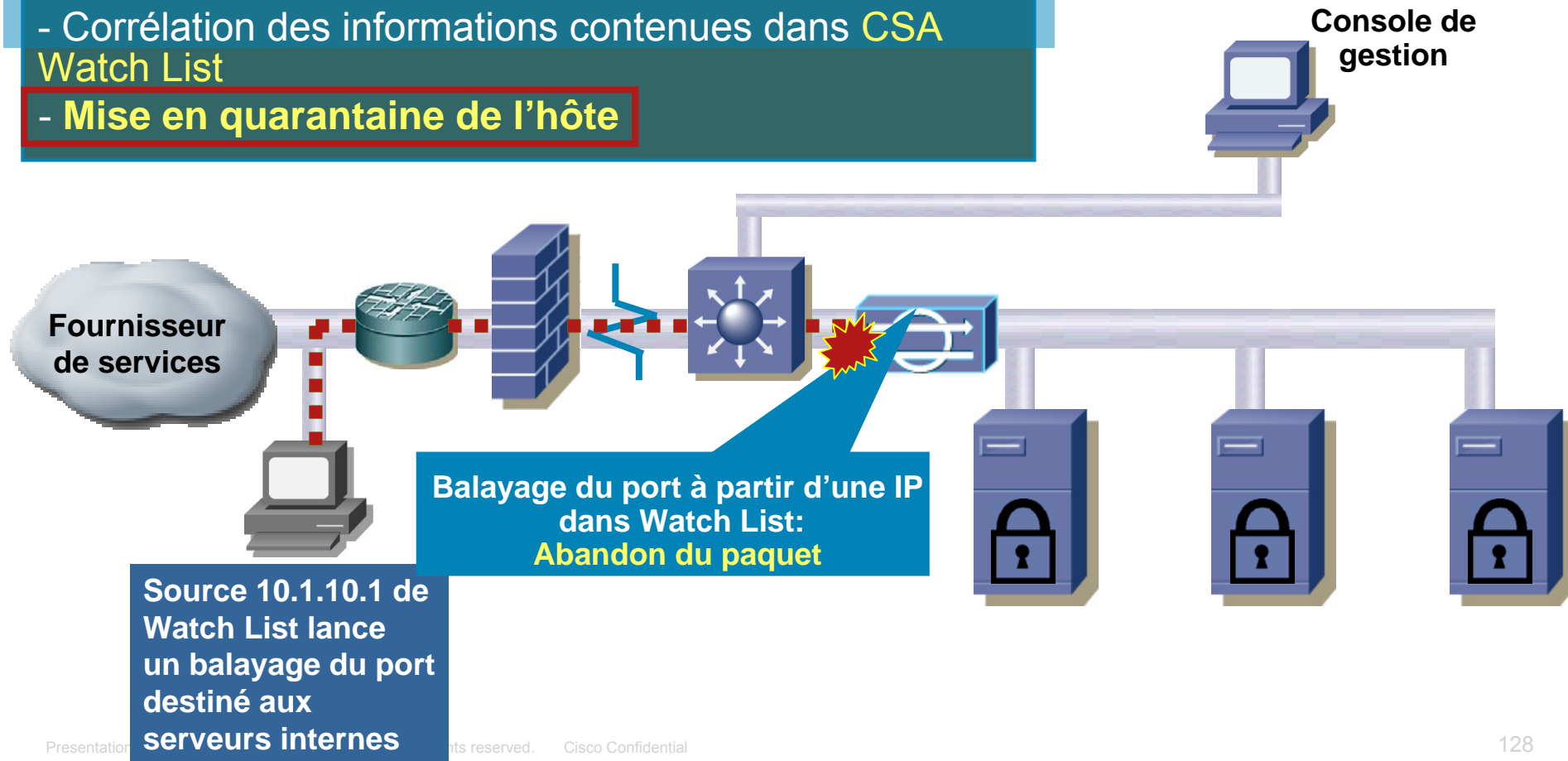
- Analyse contextuelle du point limite améliorée
- Capacité d'utiliser des données CSA pour influencer les actions IPS
- Corrélation des informations contenues dans CSA Watch List
- **Mise en quarantaine de l'hôte**



# CSA + IPS Collaboration

## avec Cisco Network IPS version 6.0

- Analyse contextuelle du point limite améliorée
- Capacité d'utiliser des données CSA pour influencer les actions IPS
- Corrélation des informations contenues dans CSA Watch List
- **Mise en quarantaine de l'hôte**



# Comment l'investigation sous Cisco Security Agent fonctionne-t-elle?

**Qu'est-ce que j'ai?**



**Qu'est-ce que j'utilise?**



**Y a-t-il risque ou malveillance?**



**Comment puis-je la contrôler?**

# Qu'est-ce que j'ai?

Analysis > Application Deployment Investigation > Unknown Applications		
Process Name	Filter: <none>	
<input type="checkbox"/> AUTORUN.EXE	Windows Media Player Hotfix [See KB837272 for more information]	5
<input type="checkbox"/> PLAYER.EXE	Windows Media Player Hotfix [See Q828026 for more information]	9
<input type="checkbox"/> START.EXE	Windows Media Player Hotfix [See wms828026 for more information]	4
<input type="checkbox"/> SMAgent.exe	Windows Media Player system update (9 Series)	27
<input type="checkbox"/> SMax4.exe	Windows Support Tools (5.2.3790)	1
<input type="checkbox"/> SMax4PNP.exe	Windows XP	5
<input type="checkbox"/> compile.exe	Windows XP Hotfix - KB815752 (20030610.131035)	1
<input type="checkbox"/> okclient.exe	Windows XP Hotfix - KB823182 (20030724.164017)	3
<input type="checkbox"/> projselector.exe	Windows XP Hotfix - KB824105 (20030724.164839)	1
<input type="checkbox"/> EngUtil.exe	Windows XP Hotfix - KB824141 (20030925.103600)	3
<input type="checkbox"/> MediaDB.exe	Windows XP Hotfix - KB825119 (20030828.113916)	3
<input type="checkbox"/> Playlist.exe	Windows XP Hotfix - KB826939 (20030902.222348)	3
<input type="checkbox"/> RxMon.exe	Windows XP Hotfix - KB826942 (20031007.111255)	1
<input type="checkbox"/> RxPlayer.exe	Windows XP Hotfix - KB828035 (20031021.165228)	1
<input type="checkbox"/> DrgToDsc.exe	Windows XP Hotfix - KB828741 (20030925.103600)	1
<input type="checkbox"/> WinVNC.exe	Windows XP Hotfix - KB833407 (20030925.103600)	1
	Windows XP Hotfix - KB833987 (20030925.103600)	1
	Windows XP Hotfix - KB833998 (20030925.103600)	1
	Windows XP Hotfix - KB834565 (20030925.103600)	1
	Windows XP Hotfix - KB834707 (20030925.103600)	1
<b>Product</b>		
Fun Web Products Easy Installer		
Kazaa Media Desktop 2.5		1
My Web Search (Outlook, Outlook Express, and IncrediMail)		1
My Web Search (Smiley Central)		1
Search Assistant - My Web Search		1
Spin4Dough		1


Rapports indiquant où des logiciels espion pourraient avoir été installés

Quelles applications connues et non connues sont installées?

Quelles corrections à chaud sont installées?

# Qu'est-ce que j'utilise?

**Title:** *Non-browser apps connecting to external servers*  
**Description:** *These applications are connecting to servers outside the organization's IP address range. Web browsers are not included in this report.*

2/16/2005 4:15:32PM 

LocalAddress	LocalProcess	Operation	Peer Host	Peer Address	Count
0.0.0.0	trillian.exe	CONNECT TO	<Unknown>	216.155.193.176/	1
0.0.0.0	<b>Process Name</b>		<b>Process Path</b>		<b>Port</b>
0.0.0.0	aim.exe		C:\Program Files\Netscape\Communicator\Program\AIM		TCP/8808
0.0.0.0	msmsgs.exe		C:\Program Files\Messenger		TCP/8833
0.0.0.0	pythonw.exe		C:\dev\tool\Python24		TCP/8833
0.0.0.0	aim.exe		C:\Program Files\Netscape\Communicator\Program\AIM		TCP/8851
Host : mcherepo-w2k...	aim.exe		C:\Program Files\Netscape\Communicator\Program\AIM		TCP/8861
0.0.0.0	msmsgs.exe		C:\Program Files\Messenger		TCP/8885
Host : pgiang-w2k.amer...	msmsgs.exe		C:\Program Files\Messenger		TCP/8910
0.0.0.0	aim.exe		C:\Program Files\Netscape\Communicator\Program\AIM		TCP/8959
0.0.0.0	msmsgs.exe		C:\Program Files\Messenger		TCP/8991
0.0.0.0	SshClient.exe		C:\Program Files\SSH Communications Security\SSH Secure Shell		TCP/9001
0.0.0.0	tomcat.exe		E:\Program Files\CSCOPx\IMDC\tomcat\bin		TCP/9007
0.0.0.0	tomcat.exe		C:\Program Files\CSCOPx\IMDC\Tomcat\bin		TCP/9007
0.0.0.0	tomcat.exe		E:\Program Files\CSCOPx\IMDC\tomcat\bin		TCP/9009
0.0.0.0	tomcat.exe		C:\Program Files\CSCOPx\IMDC\Tomcat\bin		TCP/9009
0.0.0.0	SshClient.exe		C:\Program Files\SSH Communications Security\SSH Secure Shell		TCP/9010

Les applications installées ne sont pas toutes utilisées

CSA peut retracer lesquelles et comment elles communiquent

Signale toute application non requise (serveurs qui écoutent sur un port, mais n'acceptent pas de connexions)

# Y a-t-il un risque?

The screenshot shows the Profiler interface for host bfc3. A table lists event counts for various categories:

Category	# of Events
COM (All Events)	76
FILE (All Events)	53
FILE - Read Operations	44
FILE - Write Operations	9
FILE - Writes of Executables	0
NETWORK (All Events)	0
NETWORK - Acting as Client	0
NETWORK - Acting as Server	0
REGISTRY (All Events)	0

An orange arrow points from the text below to the 'COM (All Events)' row in the table.

**Aucun accès réseau – ceci ne représente probablement pas grand un risque**

CSA surveille tous les comportements de fichiers, registres, port COM, et réseau

Il est facile d'investiguer des applications inconnues, même quand l'agent est éloigné

Il est possible de vérifier si une application est malveillante ou sûre, à partir d'un point central



# Comment puis-je la contrôler?

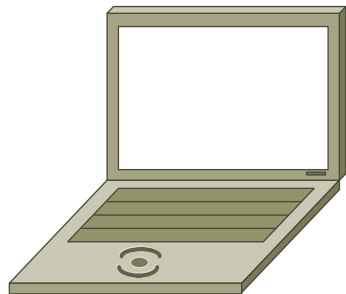
- Contrôle sophistiqué des politiques de Cisco Security Agent :
  - Révoquer l'exécution d'une application
  - Permettre l'exécution, mais bloquer le mauvais comportement
  - Utiliser des messages Query pour laisser savoir à l'utilisateur que ses agissements sont surveillés
- Cisco Security Agent offre une boucle de feedback basé sur le comportement vous permettant de comprendre et de contrôler activement ce qui se passe aux points limites

Une boucle de feedback aide à contrôler un comportement qui a été repéré et à améliorer les politiques par défaut, sans visiter les points limites

# Amorçage de confiance

Mise à jour  
du BIOS

Amorçage  
sur un  
disque non  
primaire



Amorçage  
sur le disque  
primaire

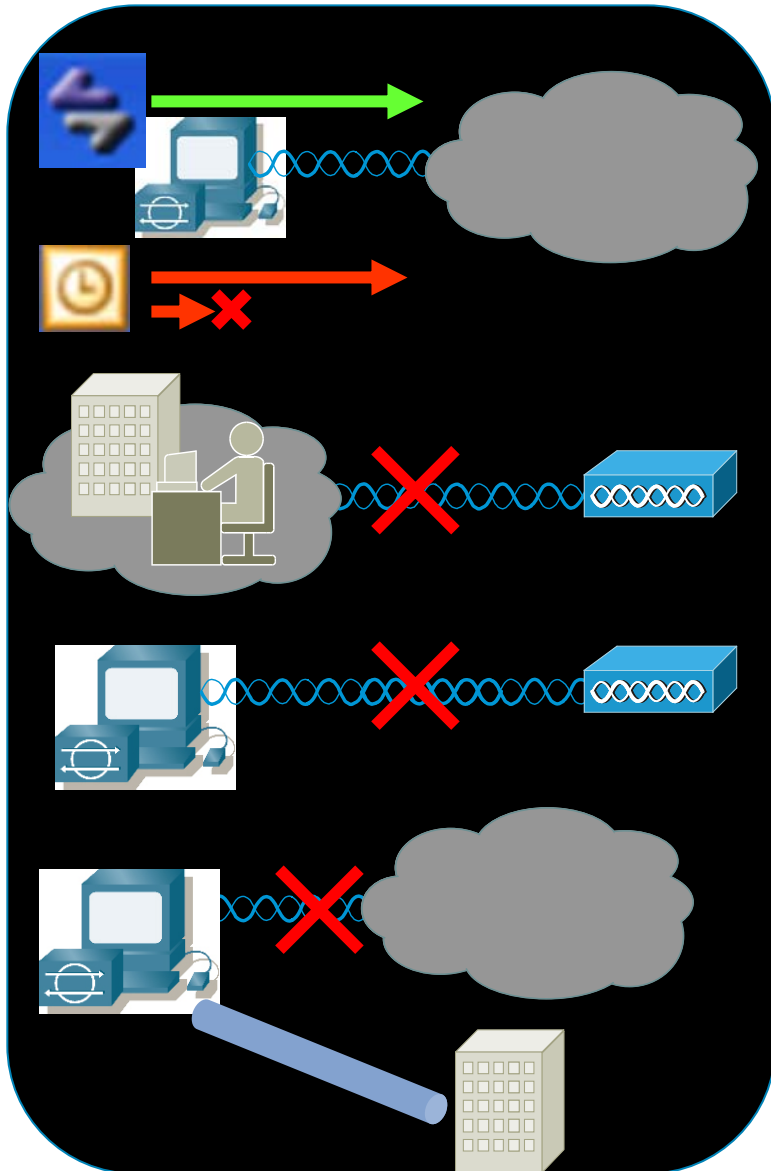
Changement  
dynamique  
des politiques

The screenshot shows a window titled "Boot History" with a close button in the top right corner. Below the title bar, it says "Latest boot events (max 10):". There is a table with four columns: "#", "Time", "Boot Type", and "Event Source".

#	Time	Boot Type	Event Source
2	11/8/2005 5:06:03 PM	Safe mode <input type="checkbox"/>	Cisco Security Agent
Safe mode boots since previous Cisco Security Agent run: 1			
1	11/8/2005 4:58:00 PM	Removable drive <input type="checkbox"/>	Cisco Security Agent
2 other insecure boots recorded since previous Cisco Security Agent run. Type: Removable drive.			

At the bottom of the window, there is a blue hyperlink: [View all boot events generated by IBM-F177AE44A35](#)

# CSA 5.2 – Contrôle du sans-fil



- Prioriser la QoS sur chaque application
- Restreindre la communication sans fil lorsque la carte d'interface réseau câblée est active
- Restrictions en matière de connexion-certaines SSID, chiffrement, ad-hoc
- Exiger une connexion VPN lorsque à l'extérieur du bureau

# Contrôle du sans-fil

- Variable basée sur les propriétés de l'interface et autres chaînes
- Implanté en tant qu'option NACL et en tant qu'état système

**Configuration** > Variables > Network Interface Sets > Wireless Interface 1

[View change history](#)

**Name**  
Wireless Interface 1

**Description**  
Restrict to specific SSID with encryption

Display only in **Show All** mode

**Configuration**

Interface characteristics matching:  ?

[Insert Interface Characteristics](#)

Network address ranges:  ?

[Insert Network Address Set](#)

[double-click variable to view](#)

Using these local interfaces:

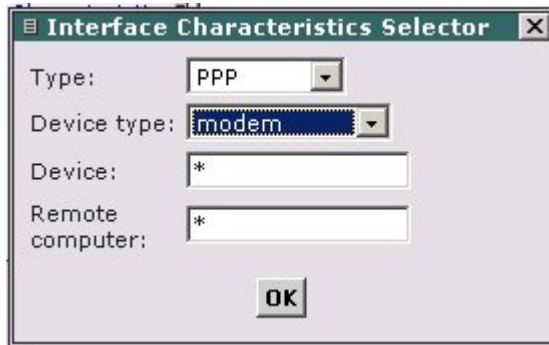
**System Location**

Network interfaces:  ?

[Insert Network Interface Set](#)

[double-click variable to view](#)

# Autres avantages du sans-fil



- Les cartes d'interface réseau (NIC) peuvent apparaître en tant que multiples cartes NIC virtuelles

Séparation des réseaux VLAN voix et données, au point limite

- Il est possible d'imposer une restriction aux cartes large bande en utilisant PPP

**Information** The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to accept a connection as a server on TCP port 445 from [192.168.45.131](#) using interface Wired\AMD PCNET Family PCI Ethernet Adapter. The specified action was taken to set Host Address as Untrusted host (locally and globally).  
[Details](#) [Rule 51](#) [Wizard](#) [Find Similar](#)

# Portrait de la sécurité au point limite

**Client Security Suites**

**Cisco Security Agent**

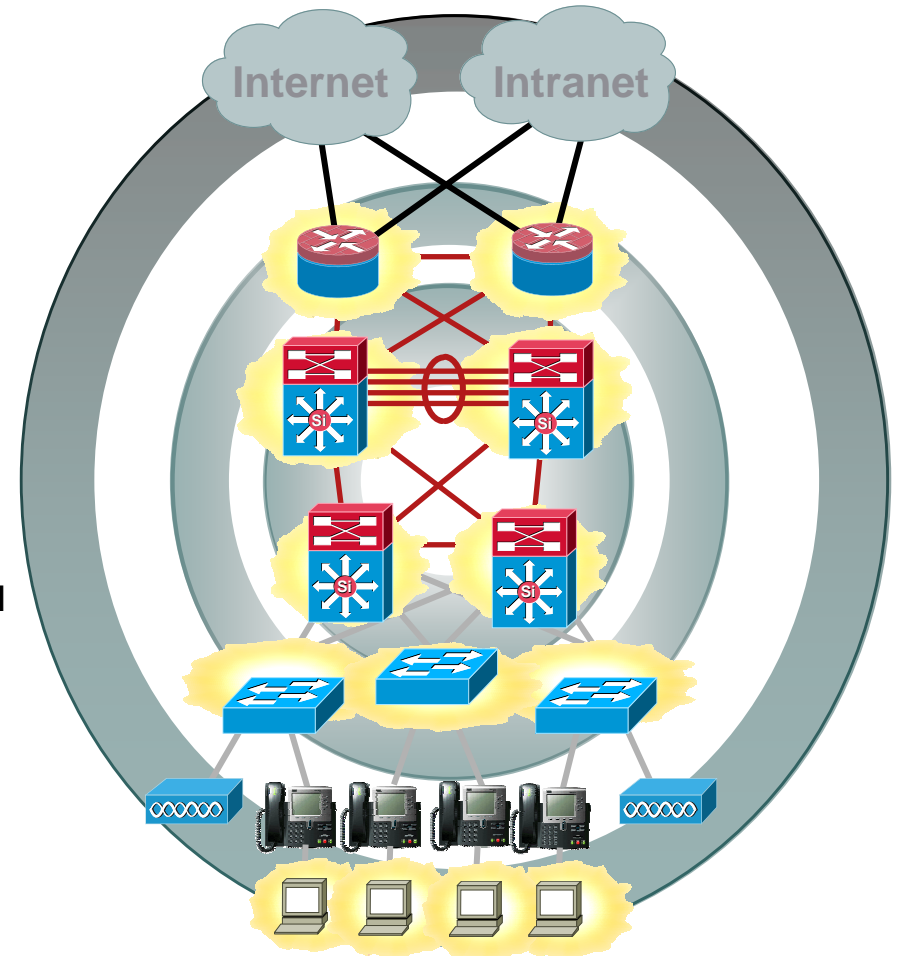
<b>Antivirus</b>	<b>Anti-logiciel espion</b>	<b>Pare-feu personnel</b>	<b>IPS hôte</b>	<b>Politique netiquette</b>	<b>Analyse applications</b>
------------------	-----------------------------	---------------------------	-----------------	-----------------------------	-----------------------------

**QoS de confiance**  
**Plus grande précision d'IPS**  
-  
**Confinement rapide**

L'intégration d'une sécurité du réseau et des points limites Cisco améliore la sécurité et rehausse les services réseau

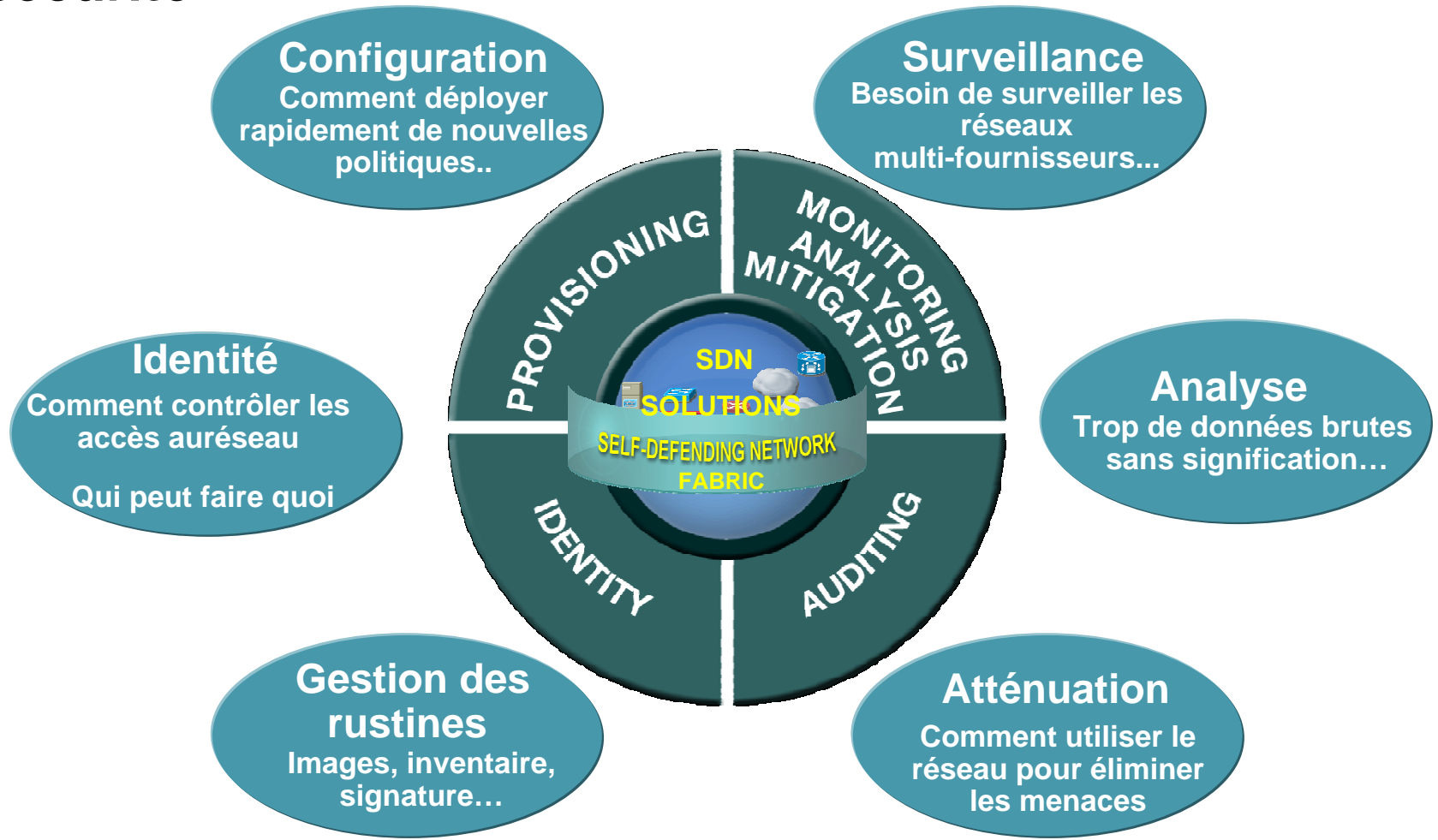
# Programme

- **Authentification**
  - ▲ Qui peut accéder le réseau
  - ▲ L'impact de la téléphonie
  - ▲ 802.1x, les visiteurs, Web Base . Authentification
- **La conformité des postes au moment de la connexion**
  - ▲ Sur le LAN, en VPN, etc...
- **Les bonnes pratiques pour le contrôle des usagers connectés au réseau**
  - ▲ Fonctions de sécurité présentent dans les commutateurs Cisco
  - ▲ QoS déployée?
  - ▲ Cisco Sécurité Agent (CSA)
- **La surveillance et la configuration du réseau**



# Gestion unifiée de sécurité Cisco

## Administration et mise en force des politiques de sécurité





# Cisco Security Manager

## Vue d'ensemble



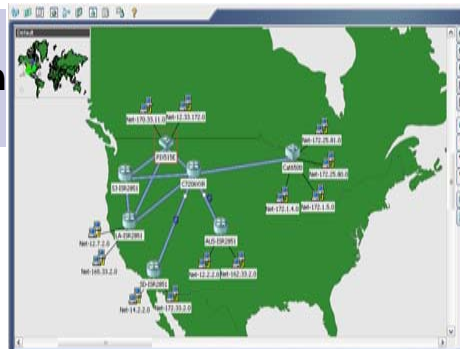
Grande facilité d'utilisation

Gestion des politiques visuellement sur les tables ou la **topologie**

Aide **Jumpstart** : un outil d'apprentissage animé approfondi

**Vues de gestion** souples

- basées sur les politiques
- basées sur les dispositifs
- basées sur la carte
- basées sur VPN



Gestion des pare-feu

Configuration des politiques pour ASA, Cisco® PIX® Firewall, FWSM et le logiciel Cisco IOS®

**Une seule table de règles** pour toutes les plates-formes

**Analyse intelligente** des politiques

Modification sophistiquée de la table des règles

Compression du nombre de règles d'accès requis

Gestion VPN

Configuration de l'**assistant VPN** site à site, hub et spoke, et VPN entièrement maillé avec quelques clics de la souris

Configuration d'accès à distance VPN, DMVPN et dispositifs Easy VPN

Gestion IPS

**Mises à jour automatiques** des détecteurs IPS

Prise en charge de **Outbreak Prevention Services**



# Cisco Security Manager

## « Une solution conviviale et souple »

- Système frontal à fonctions enrichies
- Différentes vues pour différentes préférences de gestion
  - Dispositif
  - Topologie
  - Politique
- Formule centralisée pour la création et la personnalisation VPN
- Gestion unifiée de services

The image displays three overlapping screenshots of the Cisco Security Manager web interface, each with a blue callout box identifying the view:

- Topology View:** Shows a network map with green nodes and connections. A callout box labeled "Topology View" is positioned over the top right of this window.
- Policy View:** Shows a table of firewall rules for "FW-Policy - Default (29 Rules)". A callout box labeled "Policy View" is positioned over the top right of this window.
- Device View:** Shows a table of firewall rules for "AS45520-L3" on device "AS45520-L3". A callout box labeled "Device View" is positioned over the top right of this window.

The Policy View and Device View tables contain the following data:

No.	Permit	Category	Source	Destination	Service	Direction	Action
1	None	any	EngNet	tcp/588	dmz	in	None
2	None	EngNet	any	tcp/322	outside	in	None
3	None	any	FinancialNet	tcp/Web_Servic...	outside	in	None
4	✓	Cat-B	any	any	PPTP-Data-GRE	outside	in
5	✓	Cat-B	any	any	IPSec-AH	outside	in
6	✓	Cat-B	any	any	IPSec-ESP	outside	in
7	✓	Cat-C	any	any	SSH	outside	in
8	✓	Cat-C	any	any	Telnet	outside	in
9	✓	None	any	any	HTTP5	outside	in
10	✓	Cat-B	any	any	All-ICMP	outside	in
11	✓	None	any	any	ICMP-Echo-Reply	outside	in
12	✓	None	any	any	PPTP-Control	outside	in
13	None	None	133.2.6.0/28	10.2.2.2	H323-H225	outside	in
14	✓	None	10.4.3.0/26	10.1.1.100	HTTP	outside	in

# VPN – Configuration basée sur assistant

- Configuration basée sur assistant

- Trois étapes pour créer un VPN

1 → Choisir la topologie VPN et la technologie.

2 → Choisir les participants.

3 → Personnaliser le trafic protégé s'il y a lieu.

The image shows three overlapping screenshots of the Cisco VPN configuration wizard, illustrating the three steps of the process:

- Step 1: Create Hub and Spoke VPN - Name and Technology (Step 1 of 4)**: The user enters the name "TestVPN", a description "VPN created For Test", and selects "Regular IPSec" as the IPsec Technology.
- Step 2: Create Hub and Spoke VPN - Device Selection (Step 2 of 4)**: The user selects a "Hub & Spoke" topology. The "Available Devices" list includes "Catalyst6500" under the "Hubs" category.
- Step 3: Create Hub and Spoke VPN - Endpoints (Step 3 of 4)**: The user configures the endpoints for the VPN. The table below shows the selected endpoints:

Role	Device	VPN Interface	Protected Traffic
Hub (Primary)	Catalyst6500	FastEthernet2/11:FastEthernet2/17, Blade: 5	Internal (No Match)
Spoke	LA-ISR2851	External (ethernet0)	Internal (ethernet1)
Spoke	SD-ISR2851	External (ethernet1)	Internal (ethernet0)
Spoke	NY-ISR2851	External (ethernet0)	Internal (ethernet1)

# Outils puissants : archive de configuration

**Configuration Archive**

Devices Groups: CSM Config Archive

Created On | Created By | Archival Source | Creation Comment | Transcript

Groups: Search

Device: **asa-single-router-4.cisco.com**

Version ID: 29-Sep-2005 14:10:17 | Compare with version: 28-Sep-2005 19:31:07

Config Type:  Full Configuration  Delta Configuration

29-Sep-2005 14:10:17 | 28-Sep-2005 19:31:07

- 158 dhcprelay server 1.3.3.1 inside
- 159 dhcprelay server 1.4.4.1 inside
- 160 **dhcprelay enable inside**
- 161 dhcprelay setroute inside
- 162 dhcprelay timeout 300
- 163 ntp authentication-key 1122
- 164 ntp authenticate
- 165 ntp trusted-key 1122
- 166 ntp server 10.1.2.3 key 1122
- 167 dns retries 5
- 168 dns timeout 10
- 169 dns domain-lookup inside
- 170 dns name-server 1.2.2.4
- 171 dns name-server 0.0.0.0
- 172 request-method rfc connect action reset 100
- 173 aaa accounting match CSM\_AAA\_ACCT\_1 inside TACACS+
- 174 aaa authentication match CSM\_AAA\_AUTHE\_1 outside TACACS+
- 175

139 difference(s) ■ 63 inserted ■ 6 deleted ■ 5 changed ■ 65 moved

Close Help

Close Help

- Récupérer et comparer les configurations delta pour fin de déploiement
- Peut retourner jusqu'à la configuration « golden » ou dernière « bonne configuration »
- Comparer parmi les configurations déployées antérieurement

# Modèle de partage de politique et d'héritage

## « Définition de politique extensible, configuration une fois et déploiement à plusieurs dispositifs »

### Qu'est-ce que c'est?

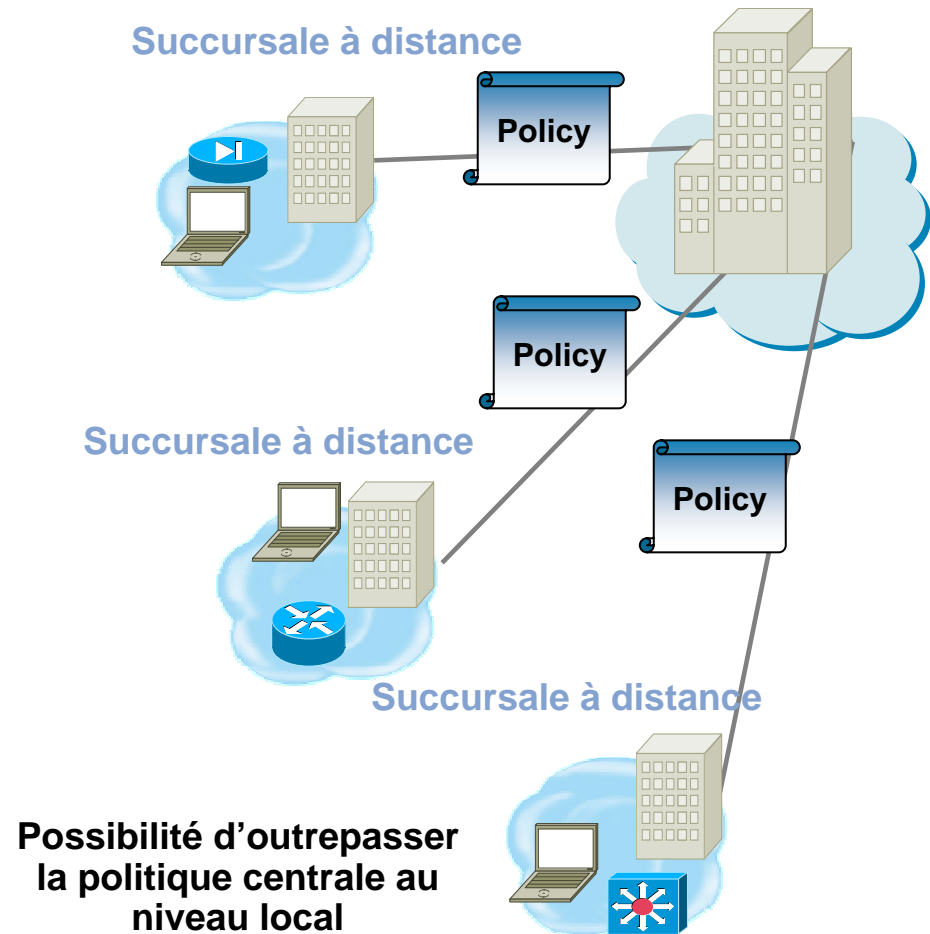
- Dispositif découplé forme les politiques

### Exemple

- Partage de politiques communes sur les groupes de dispositifs pour
  - le pare-feu de la succursale
  - VPN site à site
  - Gestion de dispositifs
- Politiques d'entreprise obligatoires
  - Aucun trafic Napster, point
  - Permet SSH et SSL

### Avantage

- Réduction de la complexité pour les administrateurs
- Effectuer plus de tâches avec moins de ressources



# Flux des travaux

« Permettre à différentes équipes de gestion de travailler ensemble »

## Qu'est-ce que c'est?

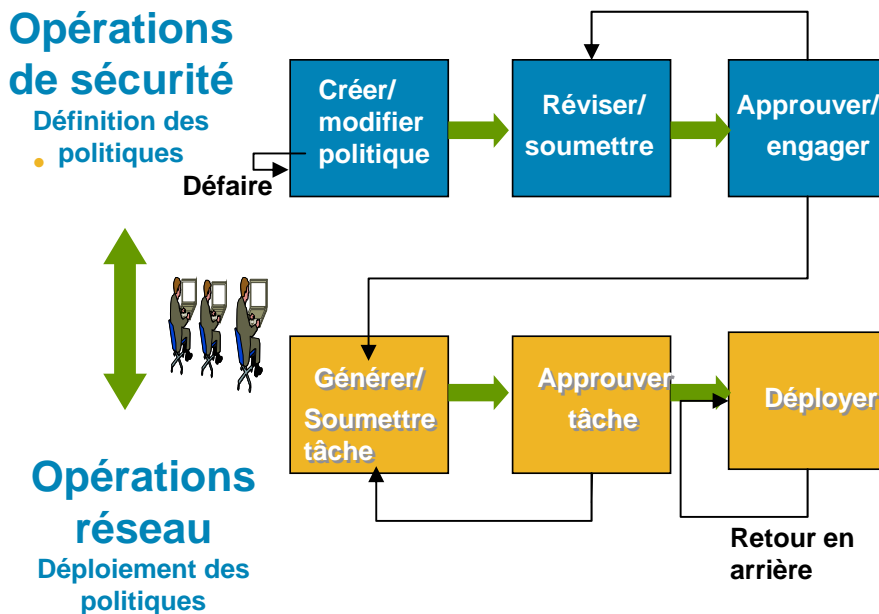
- Processus structuré pour la gestion du changement qui complète votre environnement d'exploitation

## Exemple

- Qui établit les politiques
- Qui les approuve
- Qui peut approuver le déploiement et à quel moment
- Qui peut les déployer

## Avantages

- Permet le travail d'équipe et la collaboration entre les opérations réseau et les opérations de sécurité
- Procure la portée du contrôle



**Pare-feu, VPN et services IPS**



# Contrôle des accès basé sur les rôles

## Qu'est-ce que c'est?

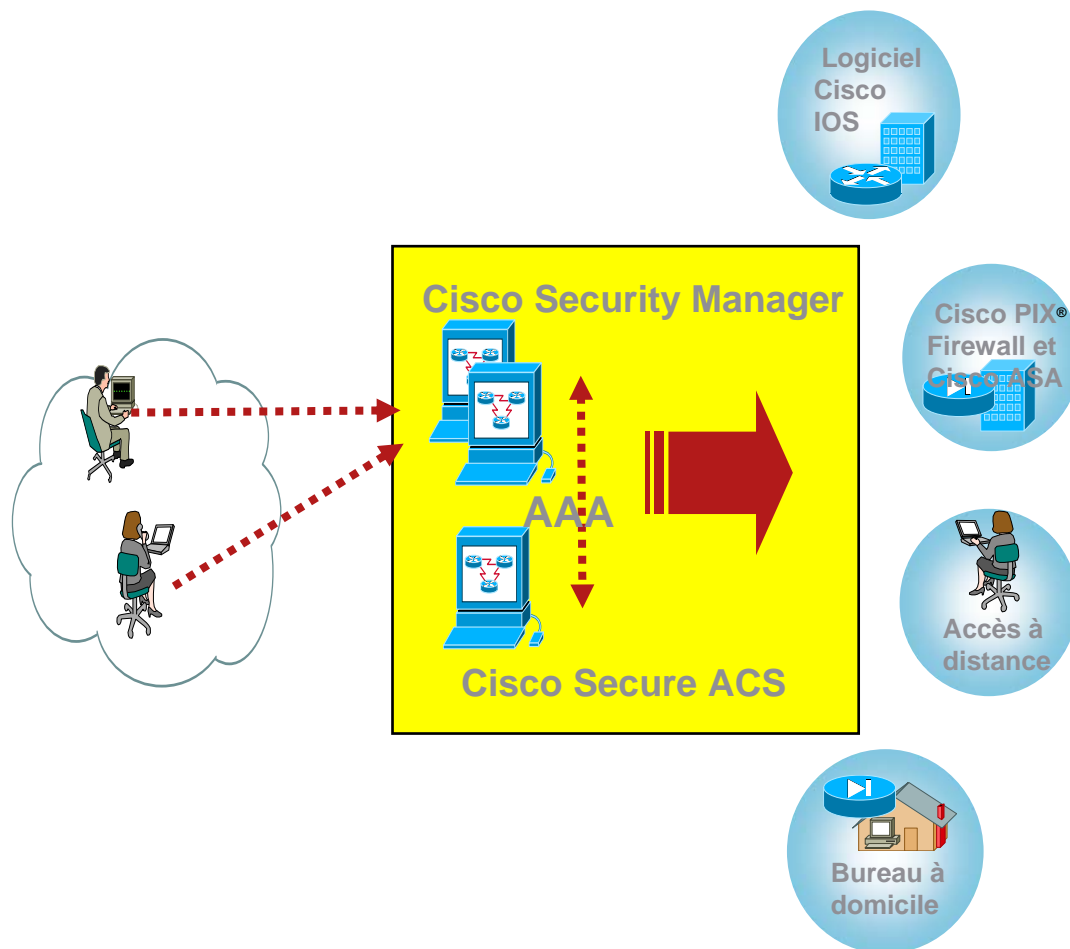
- Authentifie l'accès de l'administrateur au système de gestion
- Détermine les utilisateurs qui ont accès à des dispositifs spécifiques et les fonctions de politiques

## Exemple

- Vérifie l'administrateur et associe les administrateurs à des rôles spécifiques et détermine qui fait quoi

## Avantages

- Permet de déléguer les tâches administratives à plusieurs opérateurs
- Procure la distinction appropriée de l'appartenance et des contrôles



# Cisco Security Manager 3.1 – Lancement multi-plateforme xDM Cisco ASDM, SDM, IDM, and IEV

The screenshot displays the Cisco Security Manager 3.1 interface. The main window is titled "Cisco ASDM 5.2 for ASA - 10.76.251.218 (Preview Release)". The interface is divided into several panes:

- Log Buffer:** A table showing log entries with columns for Severity, Date, and Time. A red circle highlights the "Log Buffer" icon in the left sidebar.
- Devices:** A list of devices including "New Group Type2", "All", "10.76.251.134", "10.76.251.153", "ASA5520-218", "ASA5520-devtest", "ASA5520-test", and "pixdevice".
- Policy:** A table showing rules for "Local (4 Rules)".
- Cisco ASDM: Packet Tracer:** A window for tracing packets, showing interface "DMZ", packet type "ICMP", source IP "171.69.134.90", and destination IP "171.69.230.17". It includes a packet flow diagram and a table of phases and actions.

No.	Permit	Source	Destination
1	Deny	any	any
2	Permit	any	any
3	Permit	any	any
4	Permit	any	any

Phase	Action
ACCESS-LIST	ALLOW
FLOW-LOOKUP	✓
ROUTE-LOOKUP	✓
ACCESS-LIST	✗
RESULT - The packet is dropped.	✗

Utilisation des registres de gestion des dispositifs pour lancement multi-plateformes de la politique

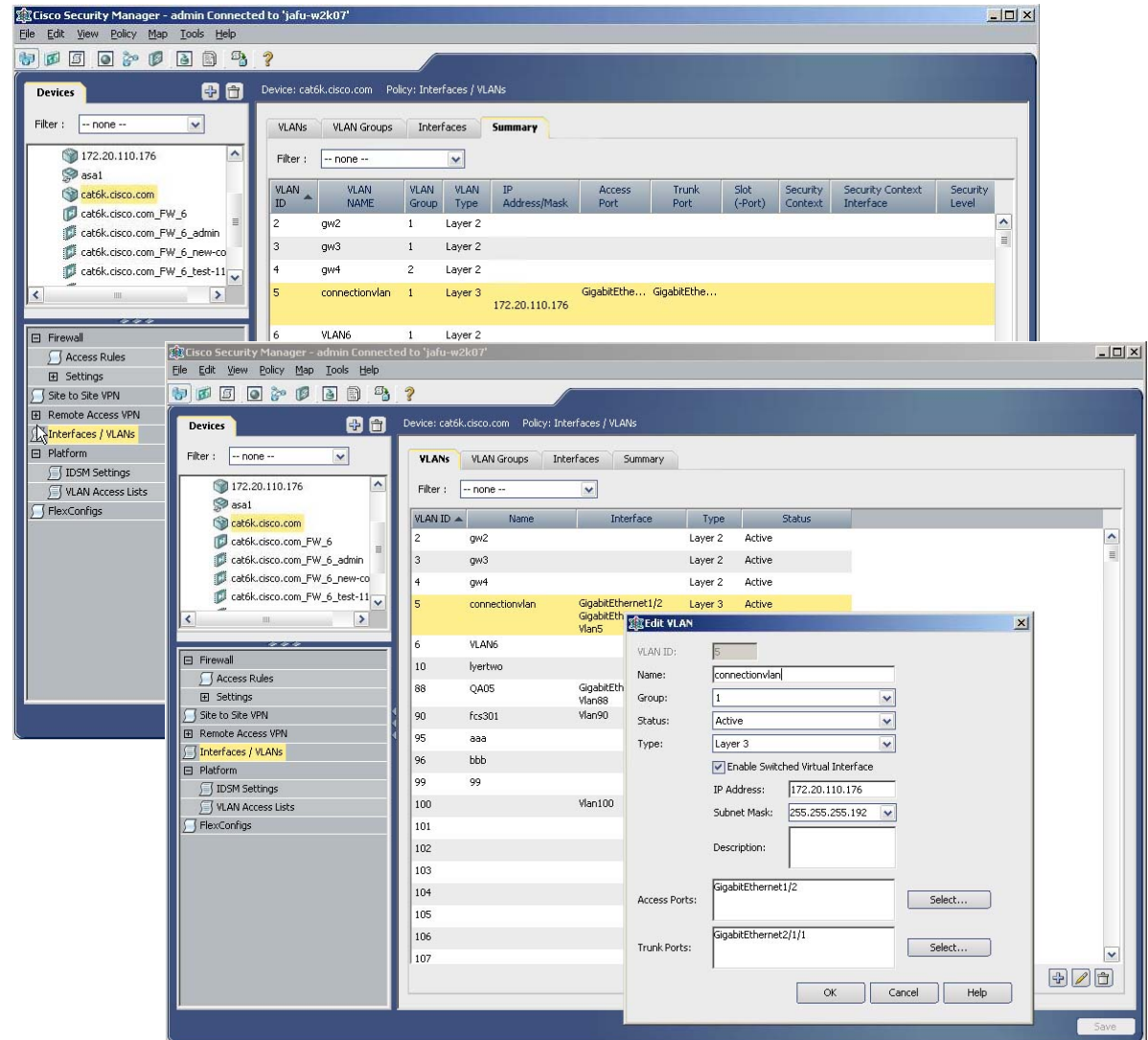
Utilisation de packet tracer dans Cisco Adaptive Security Device Manager (ASDM)



# Cisco Security Manager 3.1 – Gestion en mode natif de Cisco Catalyst 6000

## Interfaces, VLANs et groupes VLAN

- Gestion en mode natif de Cisco Catalyst® 6500 et Cisco® 7600; plus besoin de lancer CiscoView Device Manager (CVDM).
- Gestion de tous les VLANs, interfaces, groupes VLAN et cartes.
- Page de sommaire détaillée indiquant tous les mappages.



# Cisco Security Manager 3.1 –Rapport d'activité

## Champs modifiés; objets modifiés

### Activity Change Report



User: admin  
 Session started on: 13-Nov-2006 13:46:01  
 Current state: Edit Open  
 Report created on: 13-Nov-2006 17:45:30

#### Devices

*mypix.cisco.com*

##### Access Rule

Access Rule

Operation	No.	Mandatory	Permit	Source	Destination	Service	Interface	Dir.	Category	Enabled
Add	1	true	permit	any,	any,	HTTP, HTTPS, FTP	All-Interfaces	in	None	true
Add	2	true	deny	any,	any,	IP	All-Interfaces	in	None	true

#### 10.89.33.138

Device was discovered

#### Shared Policies

##### IPS-IpsEASetting

IpsEASetting: **10.89.33.138\_IpsEASetting\_1**  
**163454688687 (Added)**

Inherits From	--None--
Affected Devices	Total:2. Devices: 10.89.33.138_johnq-vs1 , 10.89.33.138
New Assignments	Total:2. Devices: 10.89.33.138_johnq-vs1 , 10.89.33.138

##### IpsEASetting

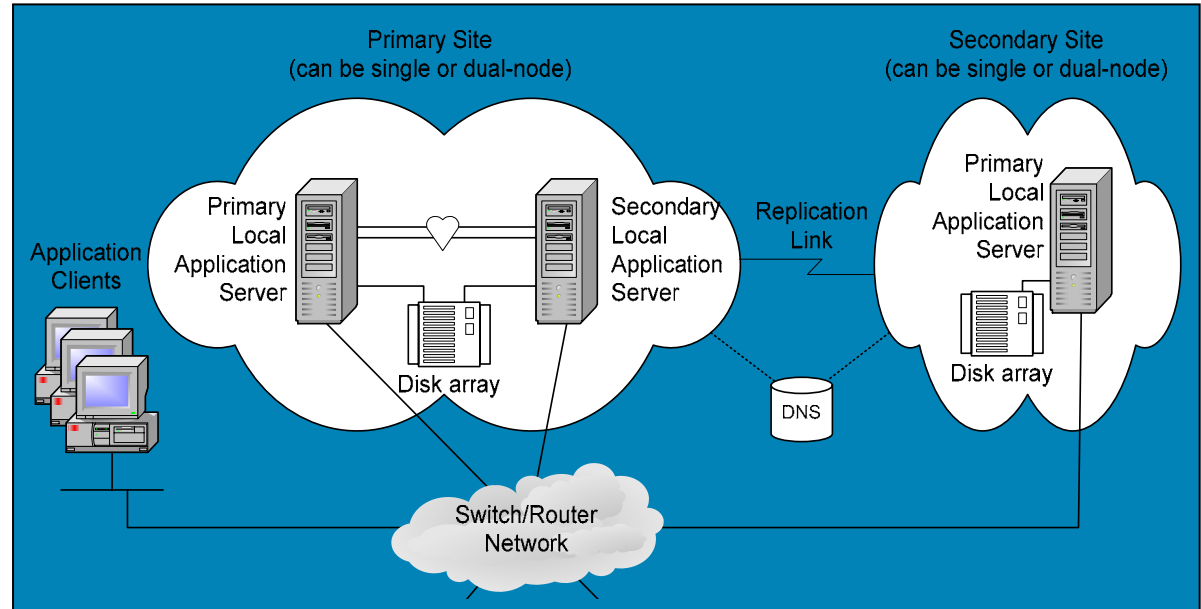
Operation	Global -deny -timeout
Add	3609

##### IPS-IpsAnomalyDetection

# Cisco Security Manager 3.1

## Grande disponibilité et reprise après sinistre

- Configuration optionnelle de haute disponibilité et de reprise après sinistre
- Matériel clé en main (serveurs, matrices de stockage) et (Symantec/Veritas) plus des personnalisations spécifiques pour Cisco® Security Manager



- Prend en charge une grande variété d'options de déploiement basées sur les exigences du client
  - Grappe double nœud unique pour grande disponibilité
  - Plusieurs grappes réparties géographiquement pour reprise après sinistre
  - Détection de panne et reprise entièrement automatisée
  - Stockage local partagé pour assurer qu'il n'y aura aucune perte de données
  - Duplication synchrone ou asynchrone entre les sites pour assurer aucune perte ou presque de données

# Surveiller, analyser et réagir avec CS-MARS

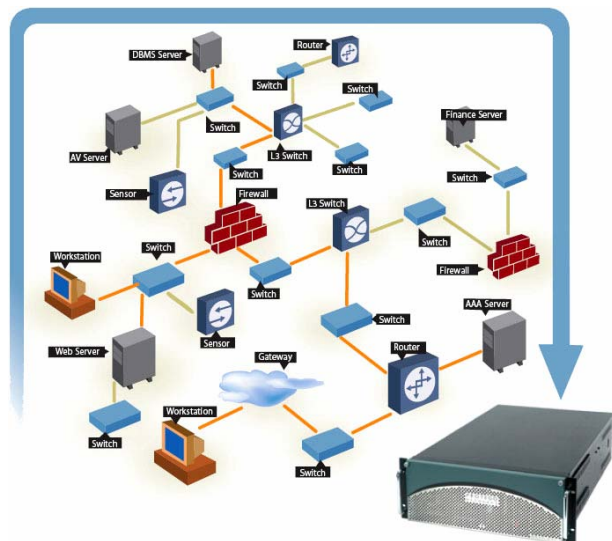
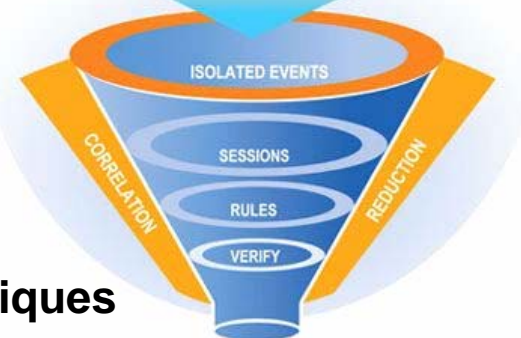


# Cisco Security – MARS

## Monitoring, Analysis and Response System

- **Commande et contrôle de votre investissement existant pou construire une sécurité « omniprésente »**
- **Corrélation des données de l'ensemble de l'entreprise NIDS, pare-feu, routeurs, commutateurs, CSA Syslog, SNMP, RDEP, SDEE, NetFlow, registres d'évènements de dispositifs d'extrémités, multi-fournisseurs**
- **Localisation et atténuation rapides des attaques**

Firewall Log	IDS Event	Server Log
Switch Log	Firewall Cfg.	AV Alert
Switch Cfg.	NAT Cfg.	App Log
Router Cfg.	Netflow	VA Scanner



- **Principales caractéristiques**

Détermine les *incidents* de sécurité en fonction des *messages*, *événements* et *sessions* des dispositifs

Les *incidents* sont sensibles de façon topologique à la visualisation et reprise

Atténuation sur les ports de couche 2 et de point d'engorgement de couche 3

# Commande et contrôle : atténuation de l'attaque

- Utiliser les fonctionnalités de contrôle de votre infrastructure

Chemin de l'attaque couches 2/3 est très visible

Dispositifs de renforcement de l'atténuation sont identifiés

La commande exacte d'atténuation est fournie

Enforcement Device: switch\_server [a], Suggested

Enforcement Device Information

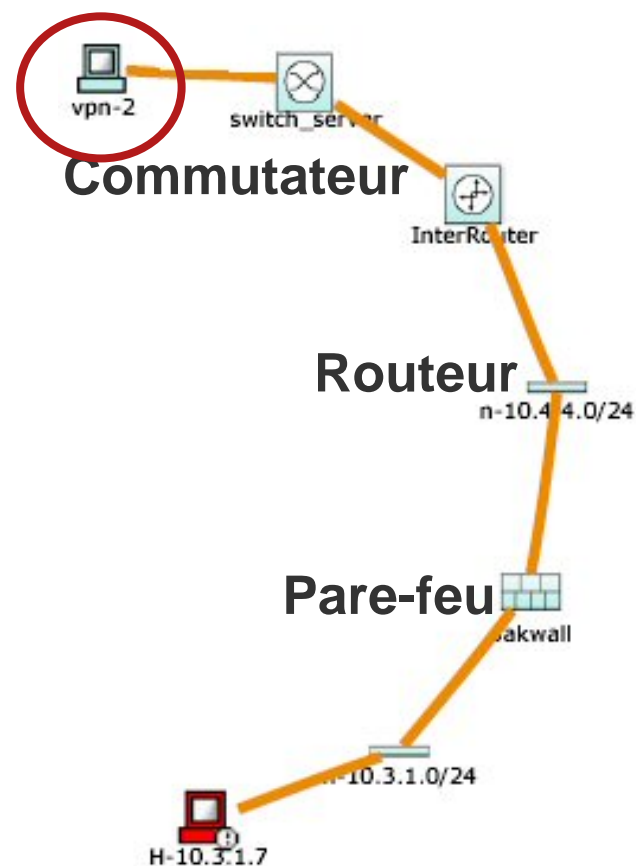
Device	Type	Manager	Children	Log To	Collects From	Info
switch_server [a]	Cisco Switch- IOS 12.2	Protego Networks MARS 1.0 on pntvalis		N/A		

Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time
-----------	------------	----------------	----------	-------------	-----------------

Recommended Policy/Command

```
configure t
interface FastEthernet0/4
no ip address
shutdown
```





# CS-MARS – Équipements supportés

- **Networking**
  - Cisco IOS® 11.x and 12.x Software, Cisco Catalyst® OS 6.x
  - NetFlow v1/v5/v7
  - NAC ACS 3.x, 4.x
  - Extreme Extremeware 6.x
- **Firewall/VPN**
  - Cisco® PIX® 6.x, 7.x Firewall, ASA, Cisco IOS Firewall/IPS, FWSM 1.x, 2.x, 3.1, VPN Concentrator 4.x
  - CheckPoint Firewall-1 NG FPx, NG AI, NGX AI, VPN-1
  - NetScreen Firewall 4.x, 5.x
  - Nokia Firewall
- **IDS**
  - Cisco NIDS 4.x, 5.x, IDSM 4.x, 5.x
  - Cisco ICS
  - Enterasys Dragon NIDS 6.x
  - ISS RealSecure Network Sensor 6.5, 7.0
  - Snort NIDS 2.x
  - McAfee Intrushield NIDS 1.x
  - NetScreen IDP 2.x
  - Symantec ManHunt 3.x
- **Vulnerability Assessment**
  - eEye REM 1.x
  - Foundstone FoundScan 3.x
  - QualysGuard 3.3
- **Host Security**
  - Cisco Security Agent (CSA) 4.5
  - McAfee Enterecept 2.5, 4.x
  - McAfee ePO
  - ISS RealSecure Host Sensor 6.5, 7.0
  - Symantec AnitVirus 9.x
- **Host Log**
  - Windows NT, 2000, 2003 (agent/agent-less)
  - Solaris
  - Linux
- **Syslog/SNMP**
  - Universal device support
- **Applications**
  - Web servers (IIS, iPlanet, Apache)
  - Oracle 9i, 10i database audit logs
  - Network Appliance NetCache

# Rapports de conformité

Rapports populaires avec options de personnalisation et de distribution  
 Les interrogations sont sauvegardées comme des règles ou des

rapports — cadre de travail intuitif

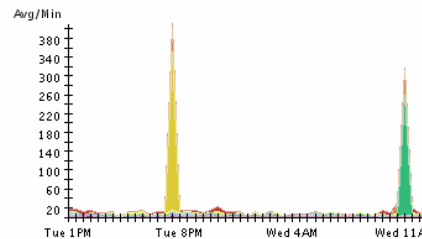
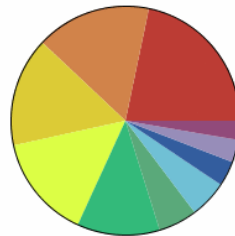
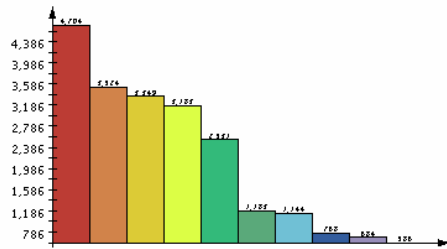
Report: Activity: Denies - Top Destination Ports, 1:07:45 PM

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: Denies - Top Destination Ports	Every hour	Normal	None	Event type: AttacksProtected, FirewallPolicyViolation/ACL, Query Type: Destination Ports ranked by Sessions Time: 1dd:0hh:0mm:0ss	This report ranks the destination ports to which attacks have been targeted but denied.	Finished: Sep 8, 2004 1:07:43 PM PDT	Sep 8, 2004 1:07:39 PM PDT	Sep 7, 2004 1:07:39 PM PDT - Sep 8, 2004 1:07:39 PM PDT

Report type: Destination Ports ranked by Sessions, 1dd:0hh:0mm:0ss

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
ANY	ANY	ANY	AttacksProtected, FirewallPolicyViolation/ACL	ANY	ANY	CA	None	ANY	ANY	ANY

Keywords: [None]



Rank	Count (# of sessions)	Raw Destination Port
1	4704	445
2	3524	80
3	3349	26686
4	3183	135
5	2531	47683
6	1183	1026
7	1144	0
8	768	139
9	684	9898

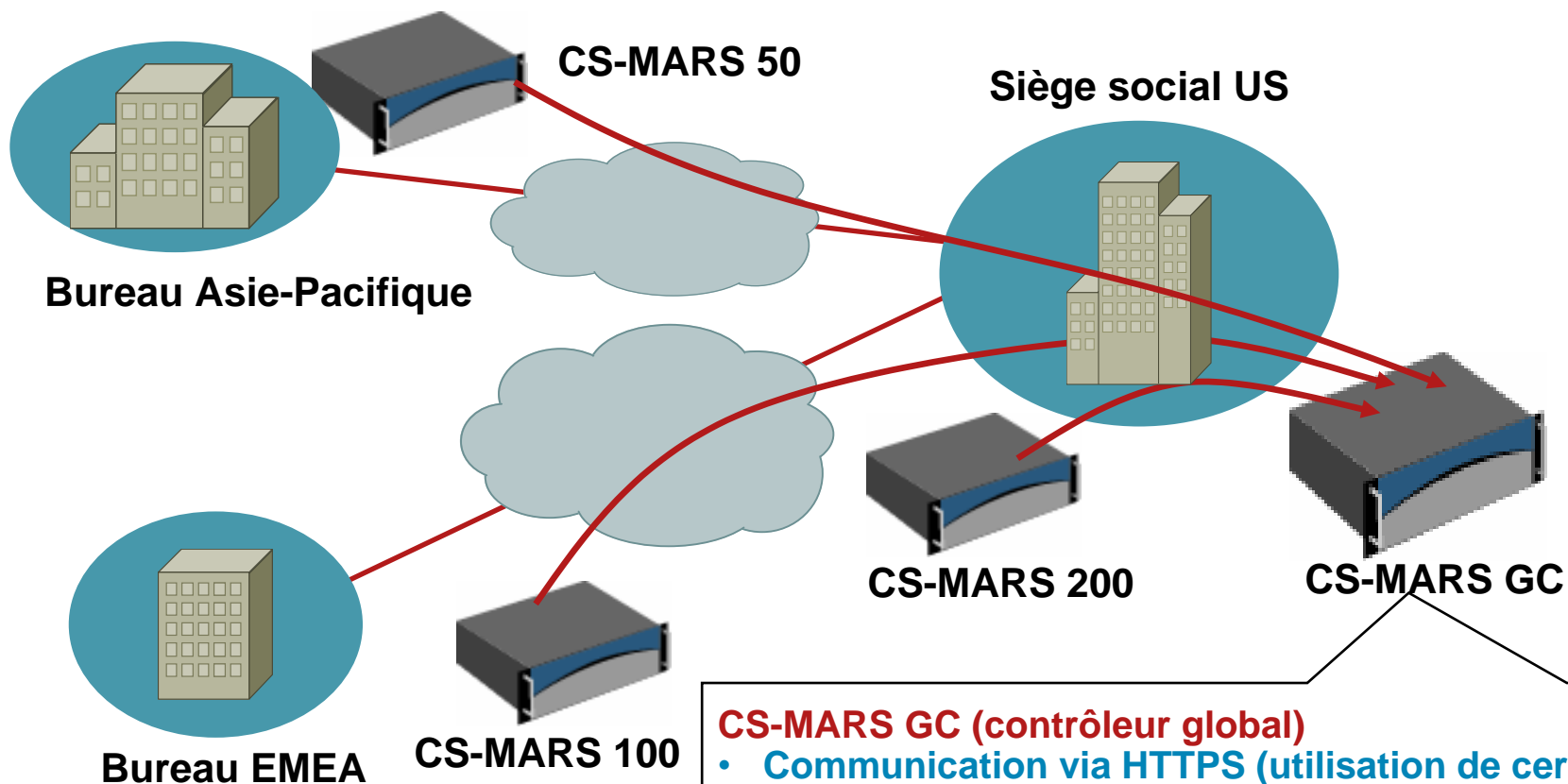


# CS-MARS – Modèles

Modèles Controlleur Local	Evènements/ Sec <sup>[1]</sup>	NetFlows /Sec	Stockage	Dimensions	Type de Controlleur Global	Alimentation
<b>Cisco Security MARS 20R (CS-MARS-20R-K9)</b>	50	1500	120 GB (non-RAID)	1 RU x 16 in.	GC, GCm	300W, 120/240V autoswitch
<b>Cisco Security MARS 20 (CS-MARS-20-K9)</b>	500	15,000	120 GB (non-RAID)	1 RU x 16 in.	GC, GCm	300W, 120/240V autoswitch
<b>Cisco Security MARS 50 (CS-MARS-50-K9)</b>	1,000	30,000	240 GB RAID 0	1 RU x 25.6 in.	GC, GCm	300W, 120/240V autoswitch
<b>Cisco Security MARS 100e (CS-MARS-100e-K9)</b>	3000	75,000	750 GB RAID 10 hot-swappable	3 RU x 25.6 in.	GC, GCm	500W dual-redundant, 120/240V autoswitch
<b>Cisco Security MARS 100 (CS-MARS-100-K9)</b>	5000	150,000	750 GB RAID 10 hot-swappable	3 RU x 25.6 in.	GC, GCm	500W dual-redundant, 120/240V autoswitch
<b>Cisco Security MARS 200 (CS-MARS-200-K9)</b>	10,000	300,000	1,000 GB RAID 10 hot-swappable	4 RU x 25.6 in.	GC, GCm	500W dual-redundant, 120/240V autoswitch
<b>Cisco Security MARS 110R (CS-MARS-110R-K9)</b>	4,500	75,000	1,500 GB RAID 10 hot-swappable	2 RU x 27 3/4" (D); 3.44" (H); 19" (W) in.	GC2	2x 750 W dual-redundant, 120/240V autoswitch
<b>Cisco Security MARS 110 (CS-MARS-110-K9)</b>	7,500	150,000	1,500 GB RAID 10 hot-swappable	2 RU x 27 3/4" (D); 3.44" (H); 19" (W) in.	GC2	2x 750 W dual-redundant, 120/240V autoswitch
<b>Cisco Security MARS 210 (CS-MARS-210-K9)</b>	15,000	300,000	2,000 GB RAID 10 hot-swappable	2 RU x 27 3/4" (D); 3.44" (H); 19" (W) in.	GC2	2x 750 W dual-redundant, 120/240V autoswitch

[1] Évènements par seconde: Quantité maximale avec la corrélation dynamique et toutes les fonctionnalités activées

# Déploiement CS-MARS



## CS-MARS GC (contrôleur global)

- Communication via HTTPS (utilisation de certificats)
- Seuls les incidents des règles globales sont déployés
- Le contrôleur global distribue les mises à jour, règles, gabarits de rapports, règles d'accès et interrogations sur le LC

# Sommaire CS-MARS

## Meilleur

- Intelligence réseau intégré
- Isoler l'attaquant par MAC, port de commutation
- Stopper les attaques en cours
- Visualiser le chemin de l'attaque
- Renforcement de la sécurité du système d'exploitation et du système

## Plus rapide

- Analyse des événements en mémoire
- Algorithmes en attente de brevets
- 10 000 EPS avec corrélation complète (3-10x compétition)
- Architecture d'analyse des événements extensibles et répartis avec CS-MARS Global Controller



## Moins dispendieux

- Offre groupée de l'appareil
- Aucun coût caché pour logiciel/personnalisation
- Licence simple – aucun agent de logiciel

# Démonstration



