ÉVOLUTION DE LA SÉCURITÉ DÉFENSIVE DES RÉSEAUX LOCAUX

Josselin MOUETTE
Juin 2022

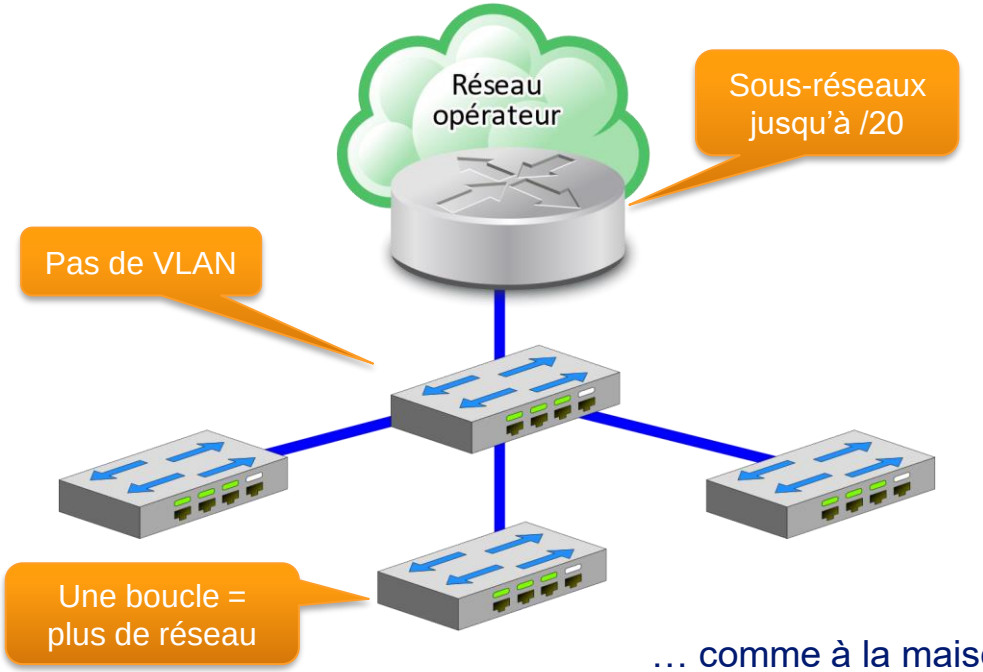
Direction des Services Informatiques & Télécoms

SOMMAIRE

SOMMAIRE

LES DÉBUTS

Réseaux à plat, déployés à partir de la fin des années 1990…



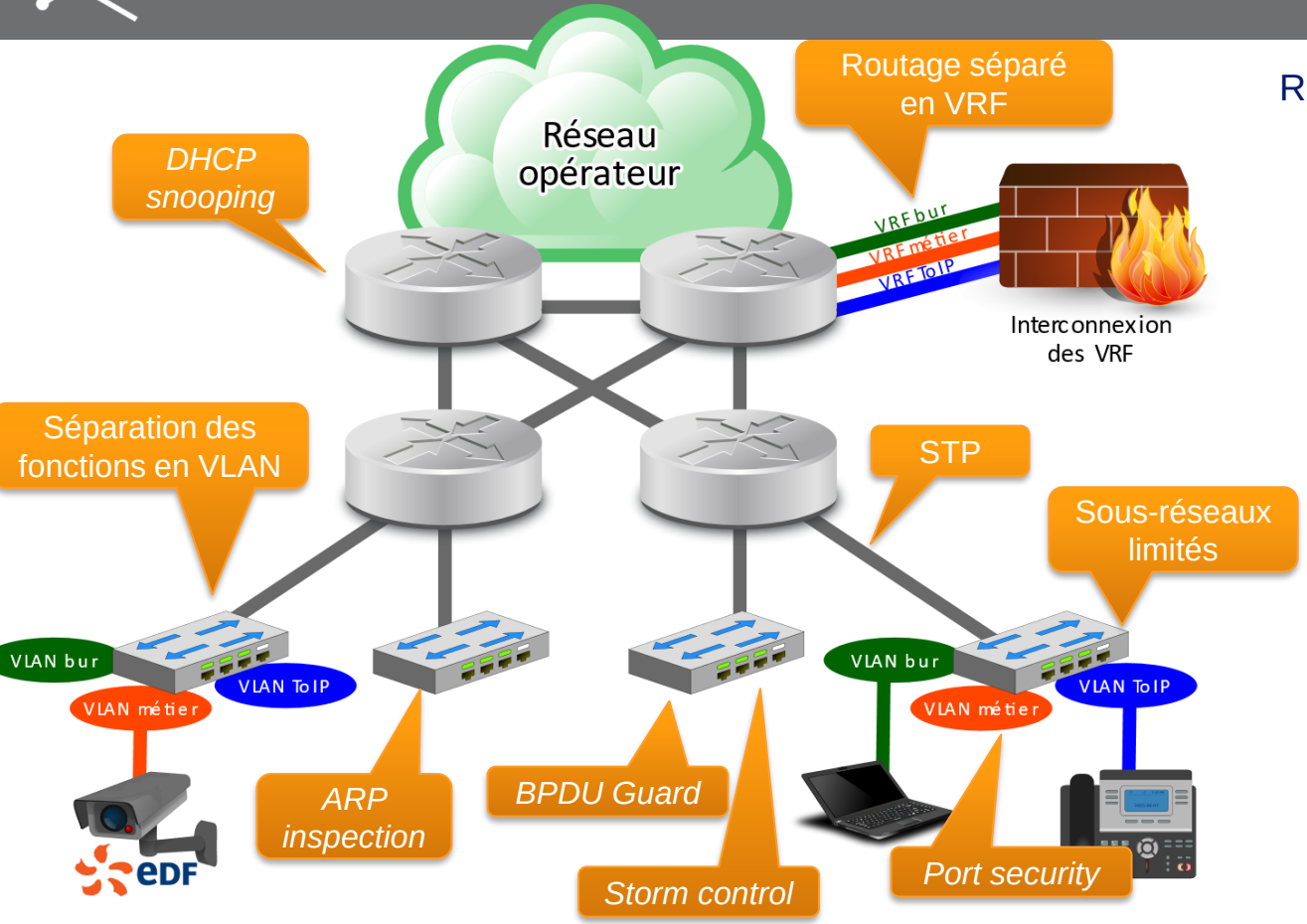
… comme à la maison !

2009 : crise Conficker

Un unique PC contaminé pouvait mettre à genoux le site (saturation par *broadcast*)

Un unique malware a eu raison des réseaux de niveau 2 à EDF

LA SÉCURITÉ DEVIENT UN BESOIN



Réseaux routés, déployés depuis le courant des années 2000

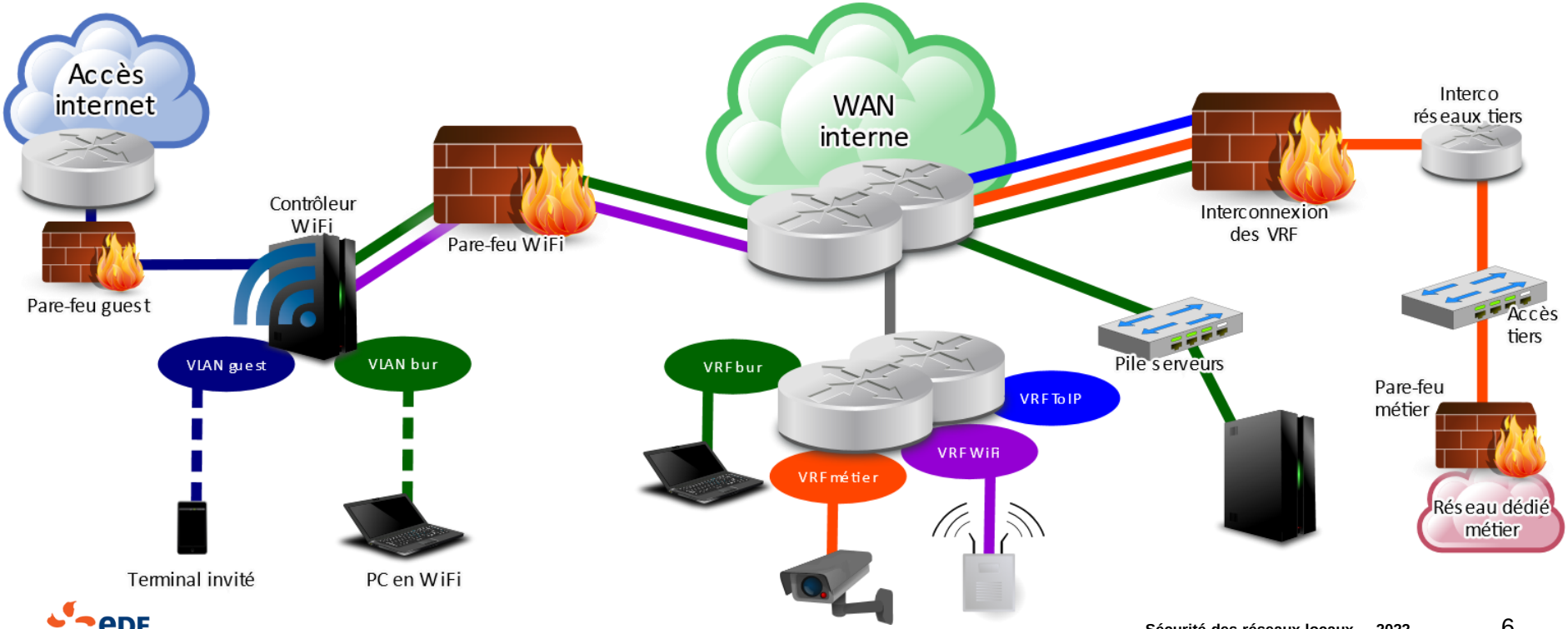
Sécurité active :

- Contre les boucles
- Contre les tempêtes
- Contre les usurpations
- Contre le *DHCP starvation*

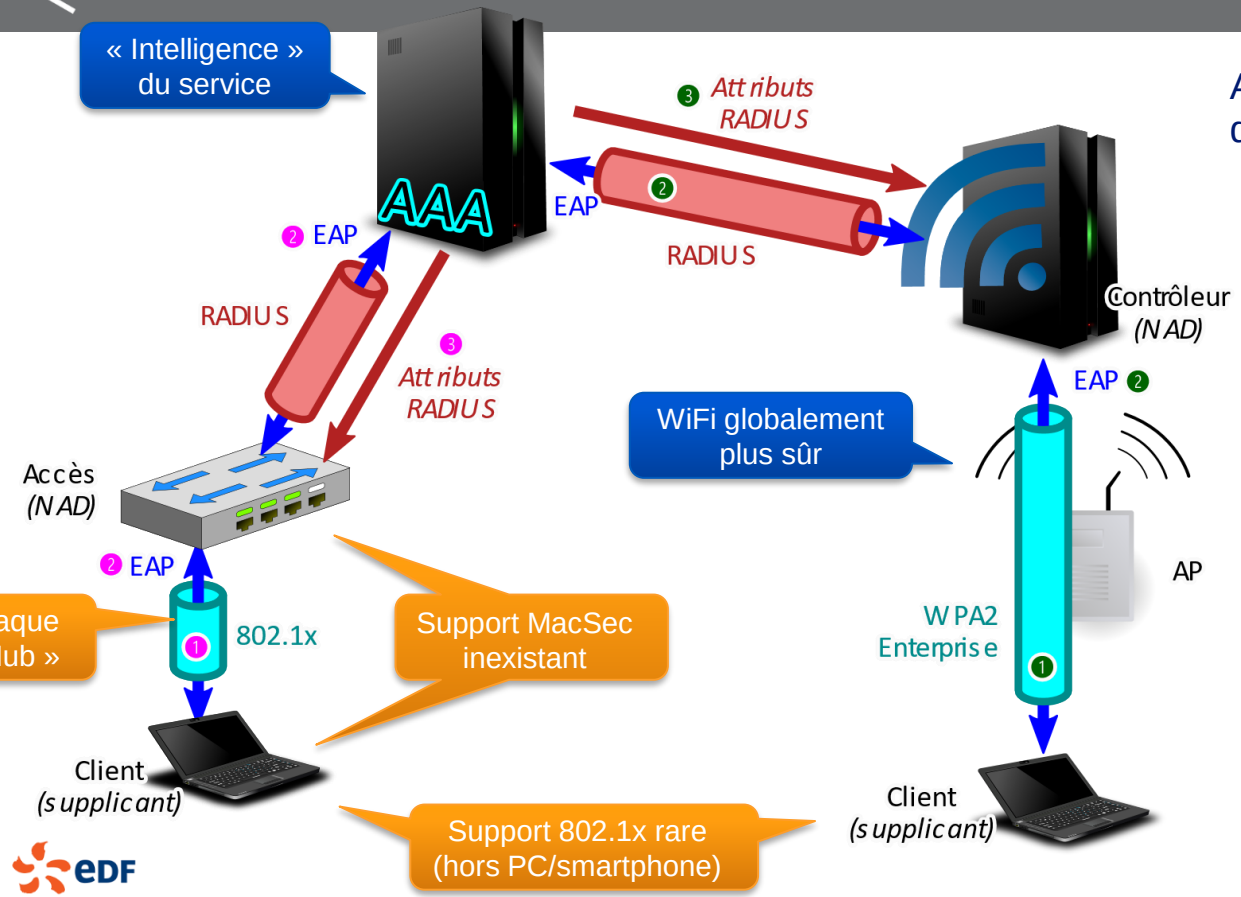
Sécurité orientée disponibilité du réseau

ÇA SE COMPLIQUE…

Au fil du temps, on ajoute des réseaux supplémentaires avec des besoins de sécurité différents.



LE CONTRÔLE D'ACCÈS AU RÉSEAU : **NAC**



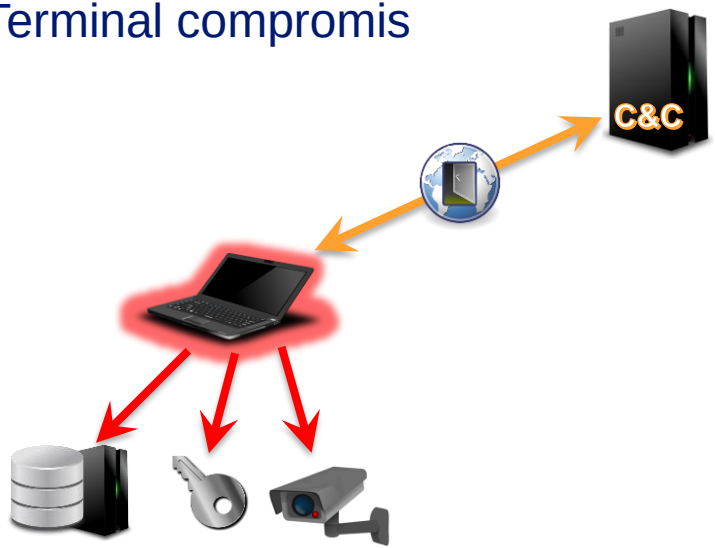
Authentification sur la couche 2 du modèle OSI

Protocole EAP :

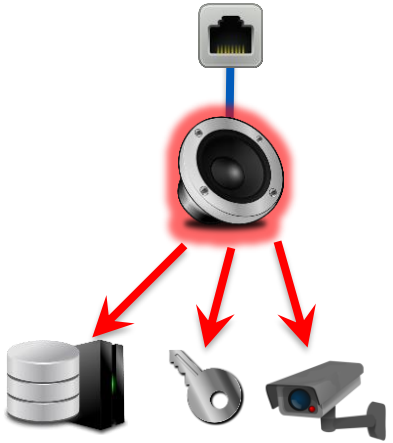
- **EAP-TLS** (certificat)
- EAP-TTLS : login/mdp
- EAP-AKA : carte SIM
- …

EXEMPLES DE MENACES À PRENDRE EN COMPTE

Terminal compromis



Matériel piégé



Menaces hybrides

- Physiques + cyber

PRAETORIAN

Protection of Critical Infrastructures from advanced combined cyber and physical threats

EDF

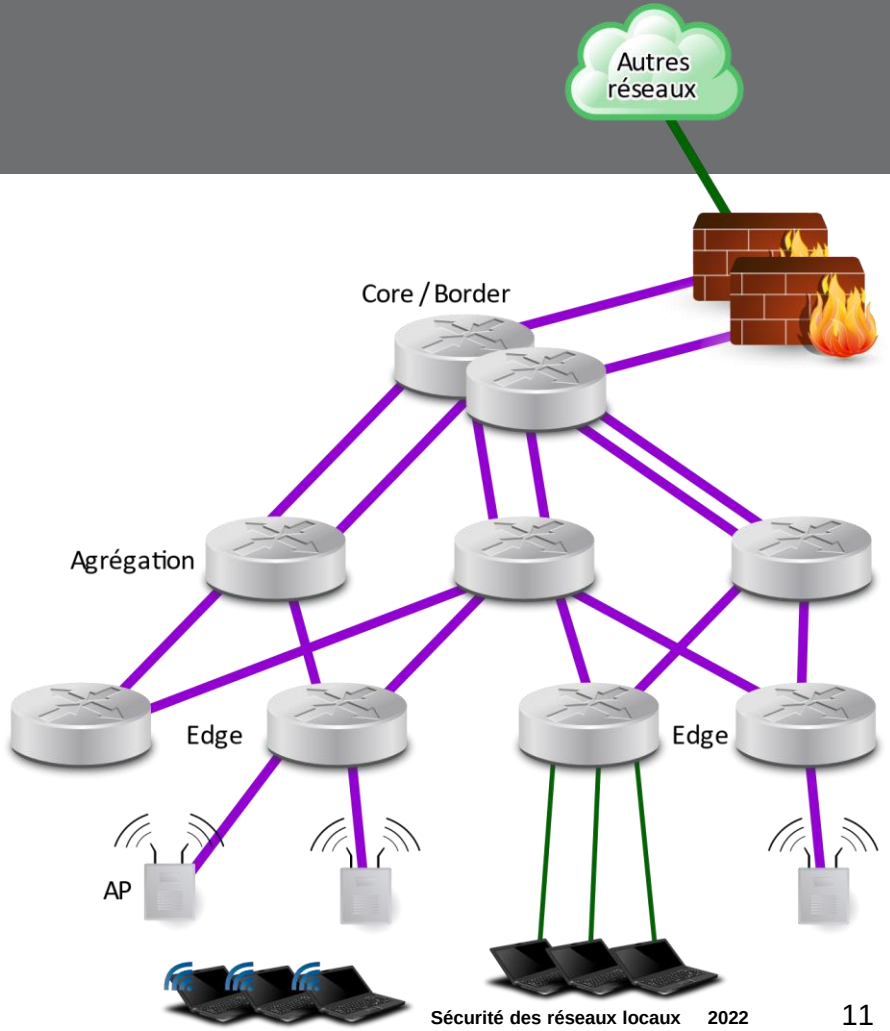
SOMMAIRE

LE SD-LAN (1/2)

*Les architectures SD-LAN sont basées sur des **tunnels** faisant circuler des réseaux logiques (**overlays**) sur un réseau physique (**underlay**)*

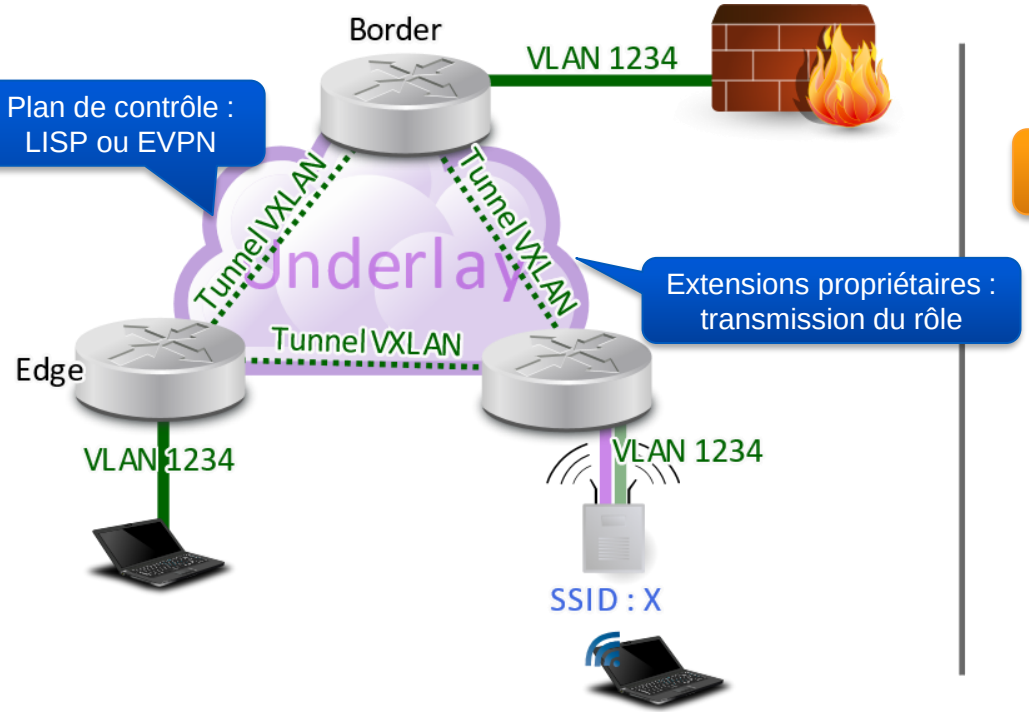
Le réseau underlay

- Réseau niveau 3
- Routage simple (OSPF, ISIS)
- Assure la connectivité entre :
  - *Edge* : commutateur d'accès
  - *AP* WiFi
  - *Border* : liens avec l'extérieur du LAN



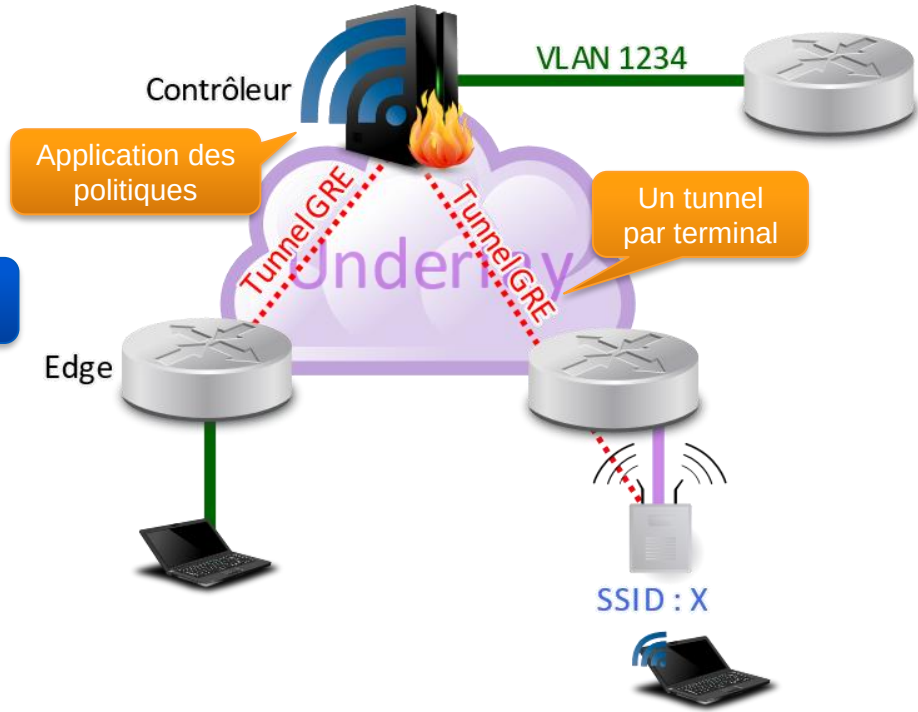
LE SD-LAN (2/2) : TYPES D'OVERLAY

Overlay maillé : VXLAN



- Plus élégant
- Optimise la performance des liens

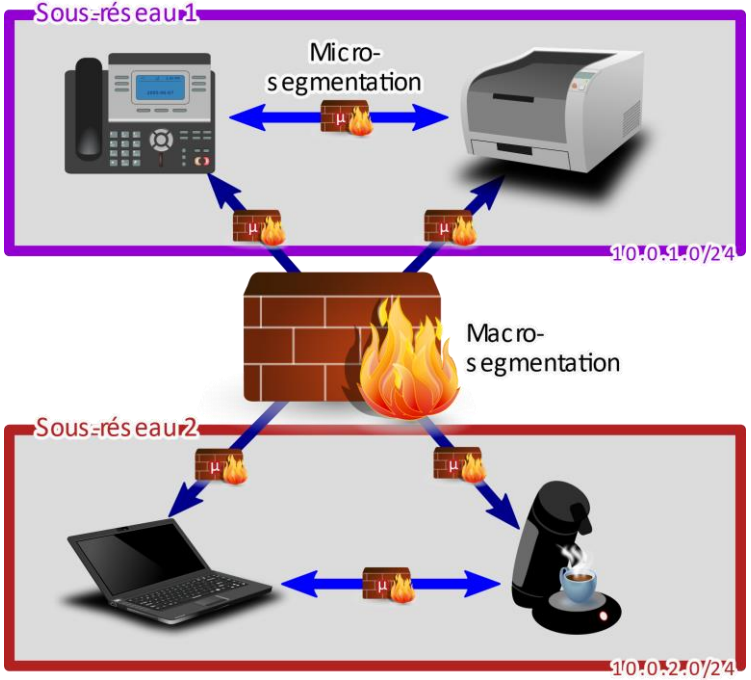
Overlay hub & spoke : « segmentation dynamique »



- Fonctions de sécurité plus avancées
- Déploiement simplifié des politiques

LA MICRO-SEGMENTATION

*Micro-segmentation : technologie de filtrage interne à un sous-réseau associée à des **rôles***



Pour les architectures maillées

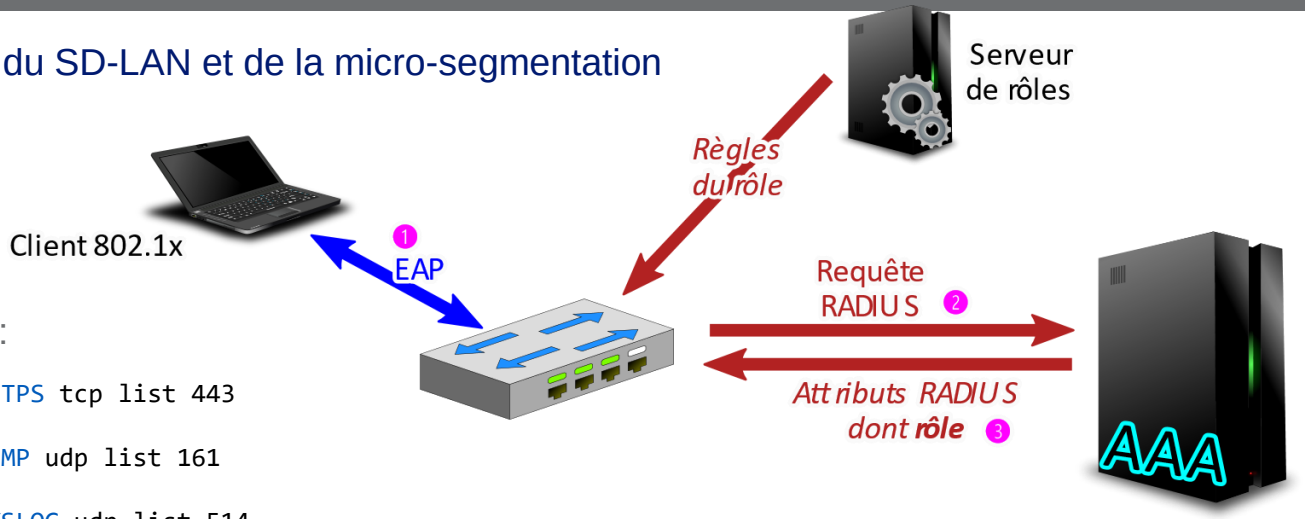
- Porté par chaque commutateur d'accès
- ACL dynamiques
- Technologie **stateless**

Pour les architectures *hub & spoke*

- Porté par le contrôleur en central
- **Stateful**, journalisation, filtrage couches 4/7

GESTION DES RÔLES

Configuration centralisée du SD-LAN et de la micro-segmentation



Exemple de rôle (Aruba) :

```
netservice SVC-HTTPS tcp list 443
!
netservice SVC-SNMP udp list 161
!
netservice SVC-SYSLOG udp list 514
!
netdestination NETDEST-SRV-IMP-WINDOWS
    host 10.10.42.42
    host 10.10.42.43
!
netdestination NETDEST-SRV-IMP-SYSLOG
    host 10.14.1.12
!
netdestination NETDEST-SRV-IMP-OUTILLAGE
    host 10.14.1.42
!
```

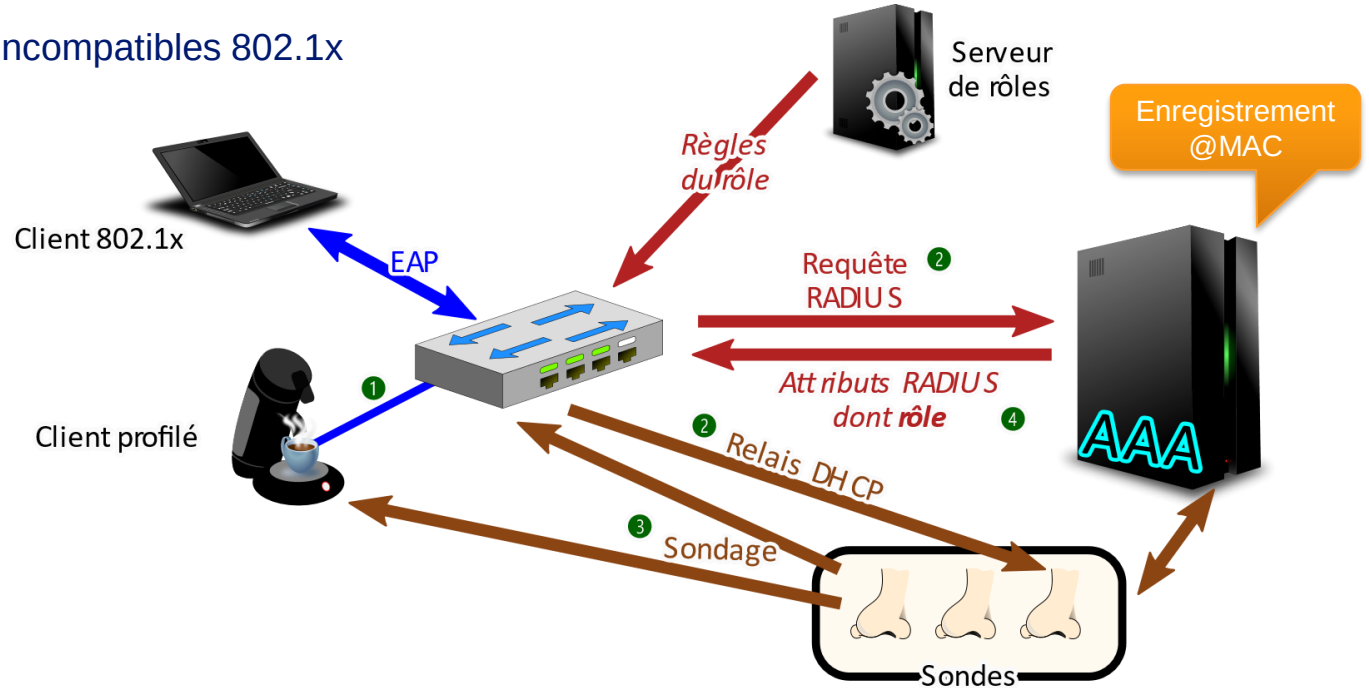
```
ip access-list session ACL-SESSION-PRINTERS
    alias NETDEST-SRV-IMP-OUTILLAGE user SVC-HTTPS permit
    alias NETDEST-SRV-IMP-OUTILLAGE user SVC-SNMP permit
    user alias NETDEST-SRV-IMP-SYSLOG SVC-SYSLOG permit
    alias NETDEST-SRV-IMP-WINDOWS user tcp 9100 permit
!
user-role cppmrole
    vlan 1234
    reauthentication-interval 480
    access-list session ACL-SESSION-PRINTERS
!
```

LE PROFILAGE D'ÉQUIPEMENTS

Gestion des équipements incompatibles 802.1x

Sondes possibles

- Requête DHCP
- SNMP sur le switch
- NetFlow
- Agent sur le terminal
- *User-Agent* HTTP
- Connexion SSH/WMI



Le profilage ne se substitue pas à une authentification !

SOMMAIRE

1. CONTEXTE & HISTORIQUE
2. NOUVEAUX RÉSEAUX LOCAUX : SD-LAN & MICRO-SEGMENTATION
3. SD-LAN ET SÉCURITÉ
4. VERS LE ZTNA

PROTÉGER ADMINISTRATION & UNDERLAY

Authentication Bypass Leading to Remote Code Execution in ClearPass Policy Manager Web-Based Management Interface (CVE-2022-23657, CVE-2022-23658, CVE-2022-23660)

Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise..

Management

Underlay

Buffer Overflow Vulnerabilities in the PAPI protocol (CVE-2021-37716)

There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of devices running ArubaOS. This may potentially allow for denial-of-service attacks and/or remote code execution in the underlying operating system.

La quasi-totalité des vulnérabilités critiques nécessite un accès management ou underlay

- Le filtrage stateful des réseaux qui portent ces interfaces est indispensable
- Protection contre l'exploitation et la post-exploitation

Cette sécurité n'est pas intégrée par défaut par les constructeurs.

Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021

Critical

Advisory ID:	cisco-sa-apache-log4j-qRuKNEbd
First Published:	2021 December 10 18:45 GMT
Last Updated:	2022 January 31 21:16 GMT

CVE-2021-44228
CVE-2021-44832
CVE-2021-45046

???

Cisco Identity Services Engine (ISE)	CSCwa47133	2.4 hotfix (15 Dec 2021) 2.6 hotfix (15 Dec 2021) 2.7 hotfix (15 Dec 2021) 3.0 hotfix (15 Dec 2021) 3.1 hotfix (17 Dec 2021)
Cisco DNA Center	CSCwa47322	2.2.2.8 patch (Available) 1.2.8 patch (Available) 2.3.4 patch (Available)

Outillage

Critical

Advisory ID:	cisco-sa-wlc-auth-bypass-JRNhV4fF
First Published:	2022 April 13 16:00 GMT
Version 1.0:	Final
Workarounds:	Yes
Cisco Bug IDs:	CSCwa43249
CVSS Score:	Base 10.0

CVE-2022-20695
CWE-303

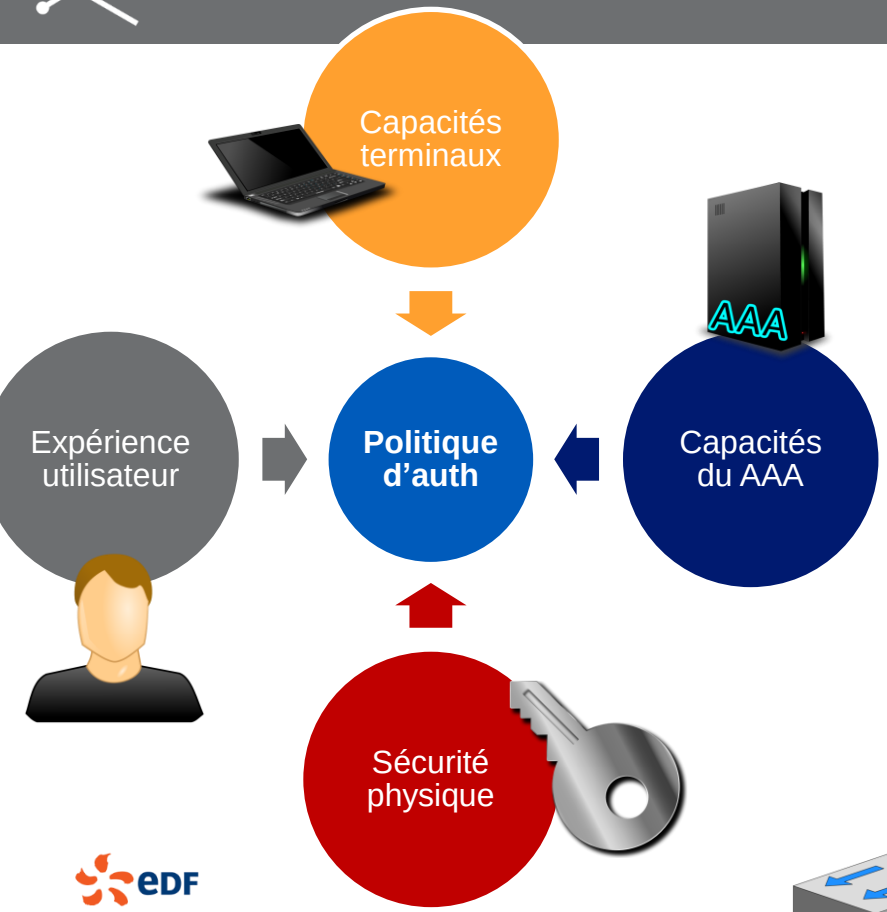
Download CVRF
Email

Management

Summary

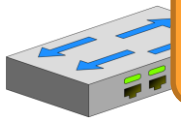
A vulnerability in the authentication functionality of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to bypass authentication controls and log in to the device through the management interface

DÉFINIR UNE POLITIQUE D'AUTHENTIFICATION



S'adapter au contexte de l'organisation

Exemple simplifié :	*Se connecter depuis…* Le WiFi ou une zone ouverte	Une zone contrôlée	Un local technique sécurisé
Accéder au rôle… Invité	Login / mot de passe invité		N/A
Interne	Certificat protégé par TPM		
Imprimante	N/A	Certificat constructeur	
Multimédia	N/A	Profilage équipement	N/A
Contrôle d'accès	N/A	N/A	Profilage équipement



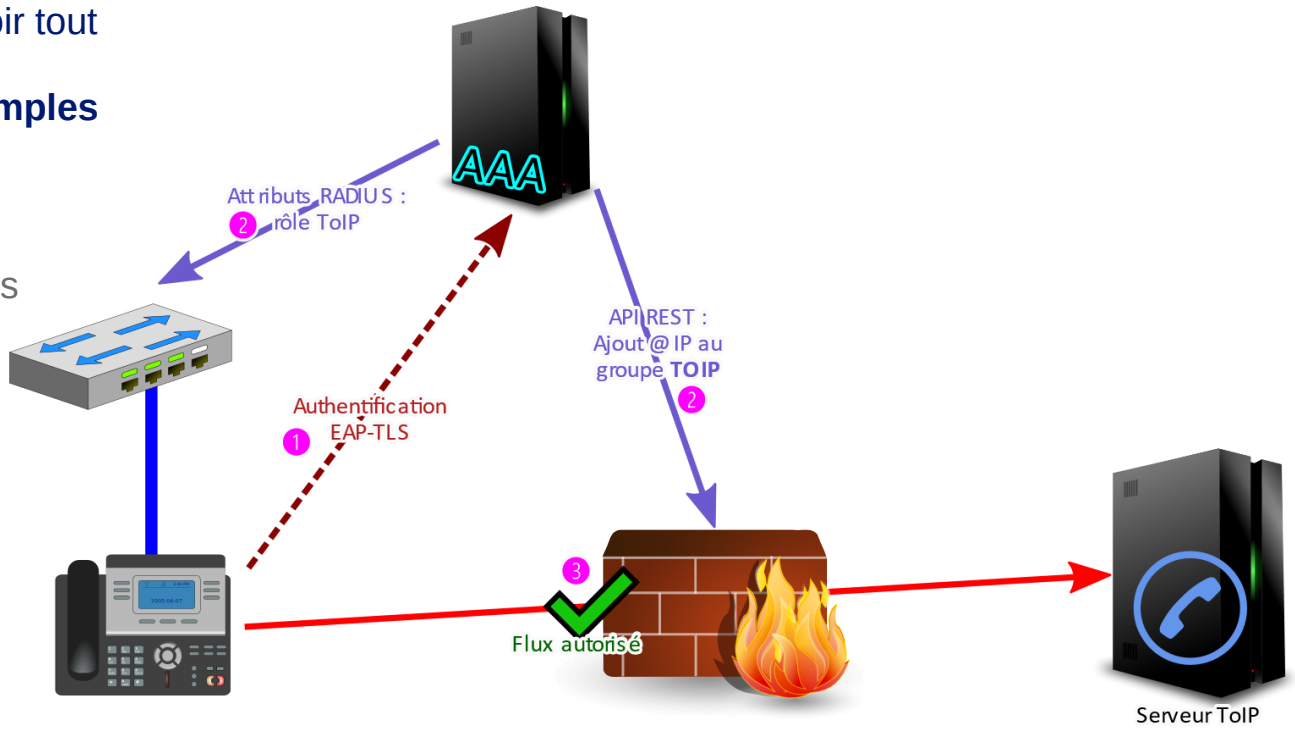
La politique est appliquée dynamiquement sur des ports à la configuration banalisée, en fonction de leur localisation physique et de l'authentification.

AVANCER PAS À PAS (1/2)

La tentation est grande de vouloir tout faire rapidement, mais il faut **commencer avec des rôles simples**

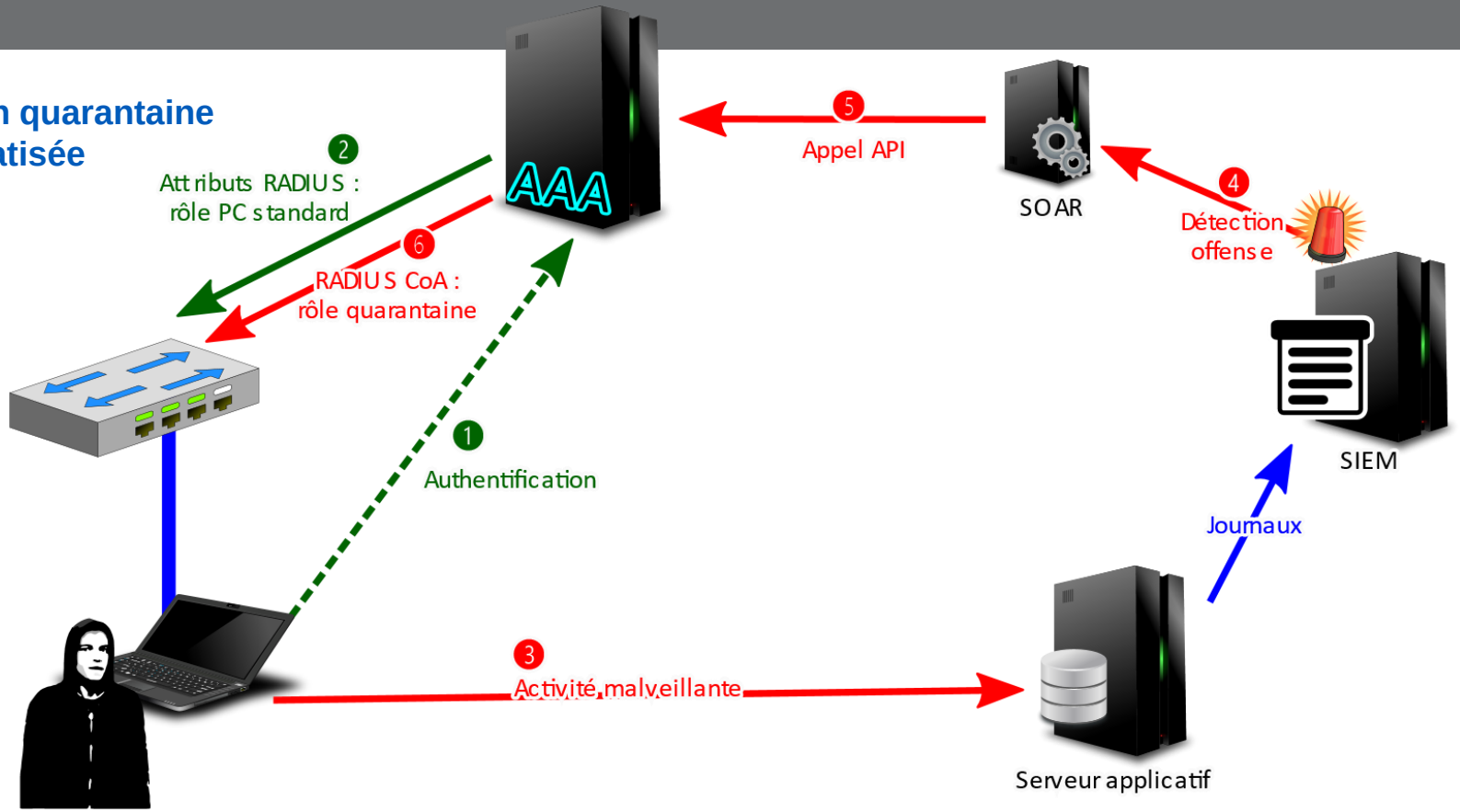
Évolutions ultérieures possibles

- Authentification en deux temps
- Rôles secondaires
  - Lien utilisateur / annuaire d'entreprise
- **Intégration du rôle avec d'autres composants**
  - Pare-feux, proxy…
- Mise en quarantaine automatisée
- *etc.*

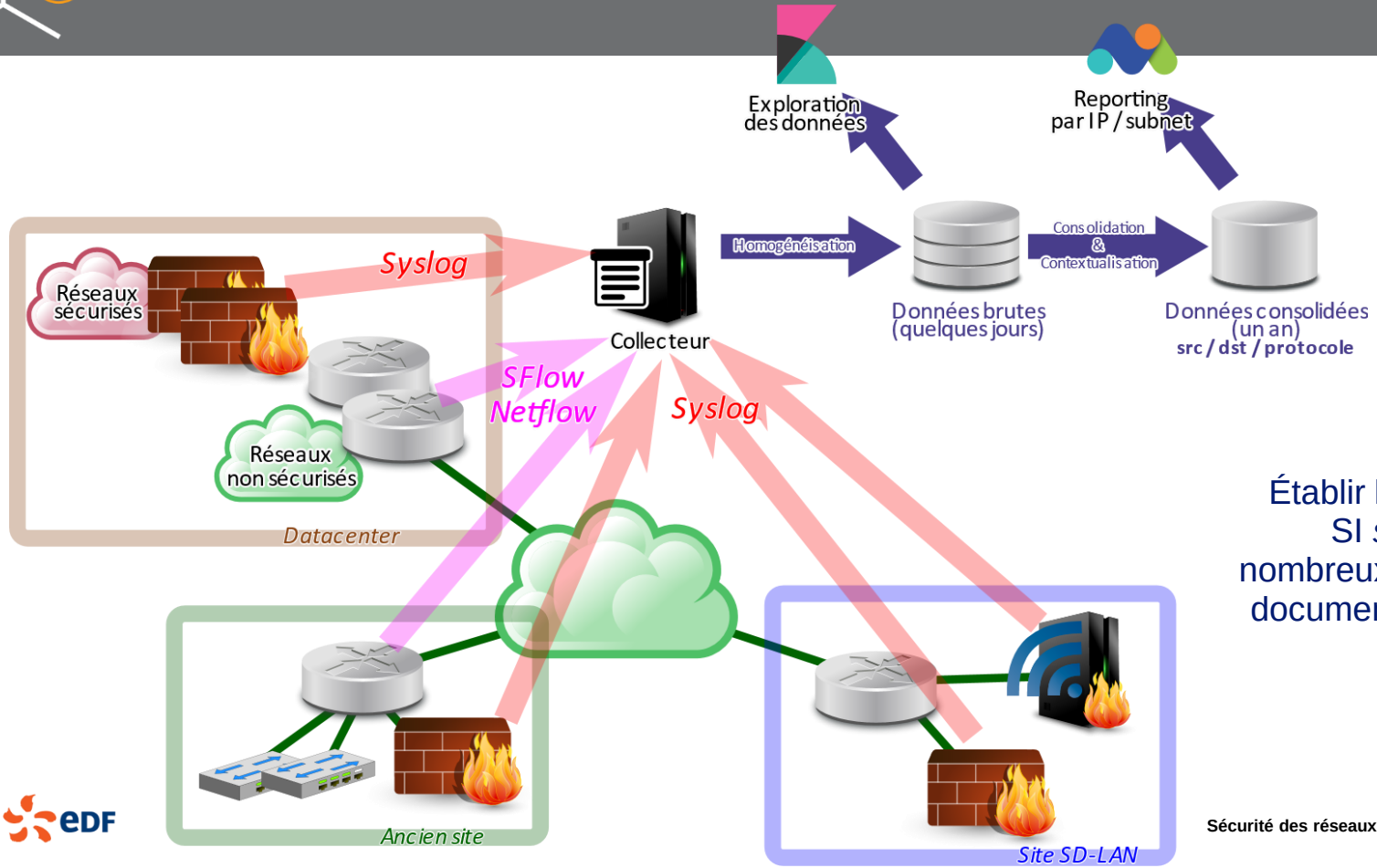


AVANCER PAS À PAS (2/2)

- **Mise en quarantaine automatisée**



CONNAÎTRE SON SYSTÈME D'INFORMATION



Établir les rôles depuis un SI *sédimenté* avec de nombreux équipements à la documentation « variable »

LIMITES ET VULNÉRABILITÉS

Interopérabilité des solutions

- **Constructeur unique** pour tout l'écosystème
- Limites sur l'**underlay**
  - MTU vs. xDSL, liens radio…
- **Propagation des rôles**
  - µ-segmentation datacenter
  - SD-WAN

- Une exception notable : des **API REST** extensives au niveau des solutions AAA.

Limitations de la µ-segmentation

- Maxi **4 domaines** de macro-segmentation (Cisco)
- **Objets de filtrage**
  - Pas de **récursivité**
  - Limite du nombre total (Aruba)
  - Pas de **synchronisation** avec d'autres solutions
- **Fonctions de filtrage**
  - Granularité du filtrage ICMP
  - Limite de **taille des politiques**
- **Filtrage *stateless*** (hors Aruba)
  - Contournable
  - Pas de détection protocolaire

NAC & profilage

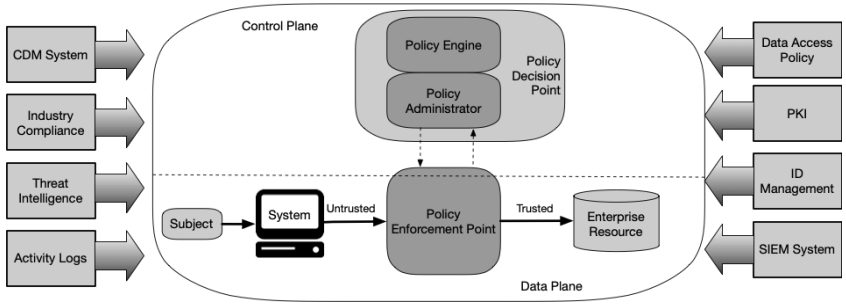
- **Sondes de profilage actives**
  - SSH, WMI avec mot de passe !
- **Usurpation** @MAC
- Attaques sur **802.1x**
- La sécurité physique n'est pas morte

- Solution pour certains objets : le WiFi en **MPSK / DPSK**
  - Une PSK par catégorie d'équipements

SOMMAIRE

POURQUOI LE ZTNA
ZERO TRUST NETWORK ACCESS

- Le modèle **Zero Trust** (NIST) : une implémentation rigoureuse du principe de moindre privilège
- Adaptée aux **enjeux actuels**
  - Entreprise étendue
  - Déplacement des activités sur le cloud

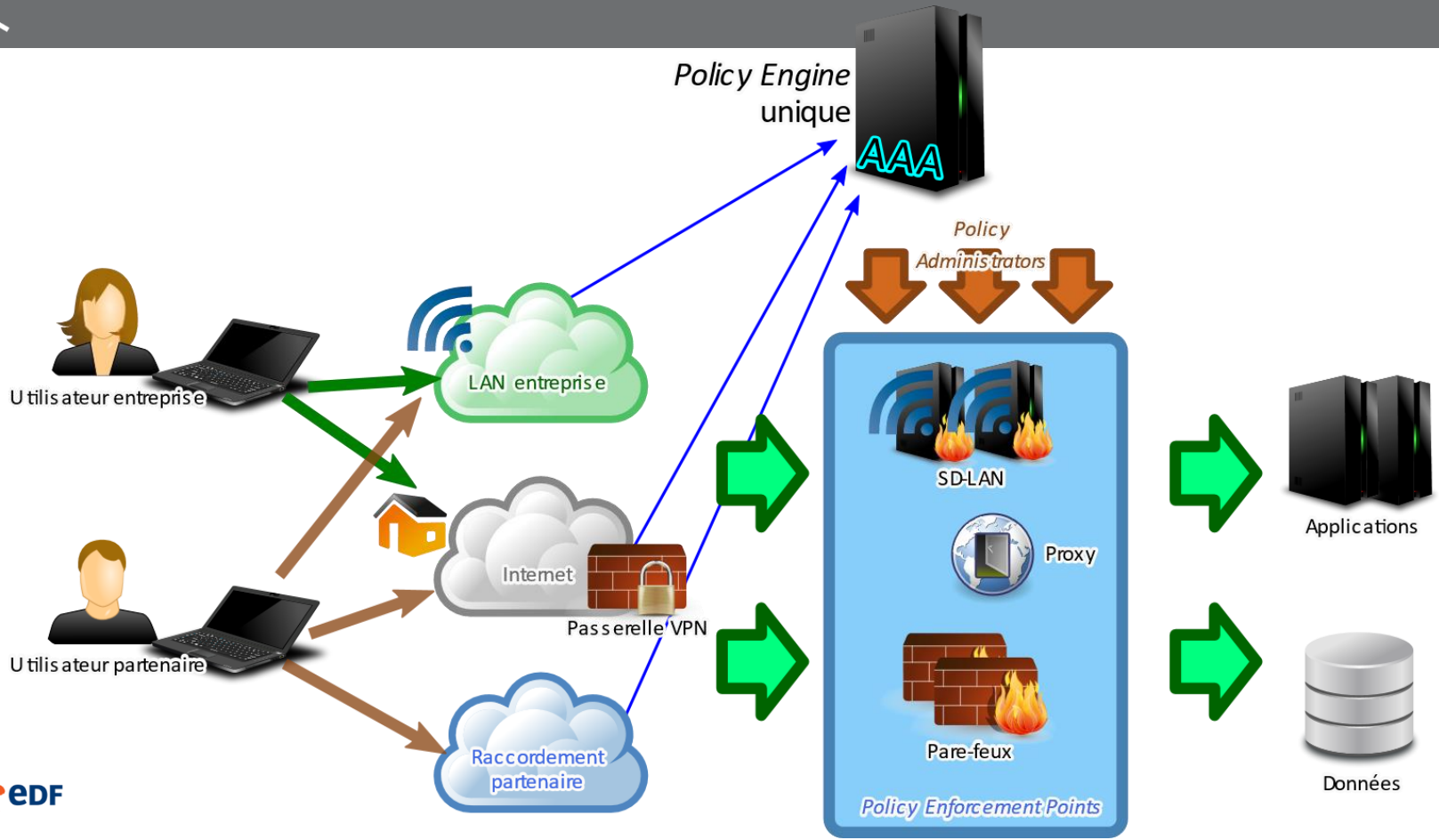


- Comment adapter au ZT des applications avec les **cycles de développement très longs** d'un industriel ?
  - Un projet nucléaire / hydraulique = 100 ans

EDF

ZTNA : un modèle transitoire où la ressource dont on contrôle l'accès est **le réseau**

LE SD-LAN, UN SOCLE ÉVOLUTIF VERS LE ZTNA



MERCI

Si on vous a fait envie :
https://www.edf.fr/edf-recrute