Évolution de la sécurité défensive des réseaux locaux : historique, SD-LAN et micro-segmentation, vers le zero-trust

Josselin Mouette
josselin.mouette@edf.fr

EDF

Résumé. Les réseaux locaux chez les opérateurs industriels ont connu des évolutions importantes dans le passé pour améliorer leur résilience aux cyber-attaques. Ils sont à présent vus comme des leviers pour lutter activement contre des menaces sur le système d'information. De nouvelles technologies, basées sur le SD-LAN et la micro-segmentation, ont été déployées à EDF et ont permis des gains considérables dans la posture défensive après un investissement humain et technique important. Elles permettent de préparer des évolutions futures vers un système implémentant la doctrine *Zero Trust* au niveau réseau.

Cet article présente les principes du déploiement de solutions de réseaux locaux de nouvelle génération dans le système d'information d'un gros industriel avec de nombreux enjeux de cybersécurité. Après une présentation du contexte historique et des enjeux liés aux réseaux locaux, nous présenterons le fonctionnement général des technologies de SD-LAN disponibles sur le marché. Nous poursuivrons, sur la base du retour d'expérience de notre déploiement d'une de ces technologies, avec les leviers à utiliser pour améliorer la sécurité du réseau et les limites de ces solutions. Enfin, nous aborderons brièvement les évolutions envisagées vers une architecture *Zero Trust*.

1 Contexte : les réseaux locaux chez un opérateur industriel

1.1 Historique

Les débuts Comme dans beaucoup d'entreprises similaires, des réseaux locaux furent massivement déployés chez EDF à partir de la fin des années 1990. À l'époque, la sécurité n'entrait pas en compte dans les exigences : il fallait connecter les utilisateurs et leur permettre de travailler en réseau. Le réseau, schématisé sur la figure 1, ressemblait donc à ce qu'on trouverait

aujourd'hui chez un particulier, le NAT en moins : un réseau de niveau 2, à plat, étendu sur tout le bâtiment. Entre autres problèmes qui choqueraient aujourd'hui, on peut citer :

— l'absence de dispositif anti-boucles (un simple mauvais brassage en salle de réunion pouvait mettre l'ensemble du site à terre) ;
— l'absence de séparation en VLAN ;
— des tailles de sous-réseaux déraisonnables (jusqu'à des /20).

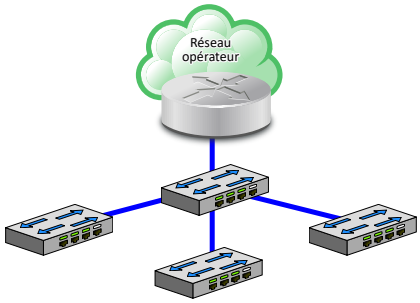

Fig. 1. Réseau à plat sans sécurité

En 2009, le ver Conficker frappa violemment EDF [8] malgré le faible nombre de machines vulnérables. La raison : nombre de réseaux locaux, saturés de requêtes *broadcast*, s'écroulèrent. La traque des PC infectés dura plusieurs mois. Cette crise eut raison des réseaux artisanaux de niveau 2, qui furent résorbés dans le cadre d'un coûteux projet de renouvellement.

La sécurité devient un besoin L'architecture déployée alors, schématisée sur la figure 2, était similaire à celle que l'on retrouve aujourd'hui majoritairement en entreprise :

— des architectures routées qui limitent les tailles de sous-réseaux ;
— une segmentation en VLAN et en VRF pour séparer les fonctions ;
— de nombreuses protections de sécurité active conformément aux bonnes pratiques [4] :
  — contre les boucles (*BPDU Guard*, *Spanning Tree*),
  — contre les tempêtes de *broadcast* (*Storm Control*),
  — contre l'usurpation de services réseau (*DHCP snooping*, *ARP inspection*),
  — contre le *DHCP starvation* (*Port Security*),
  — *etc.*

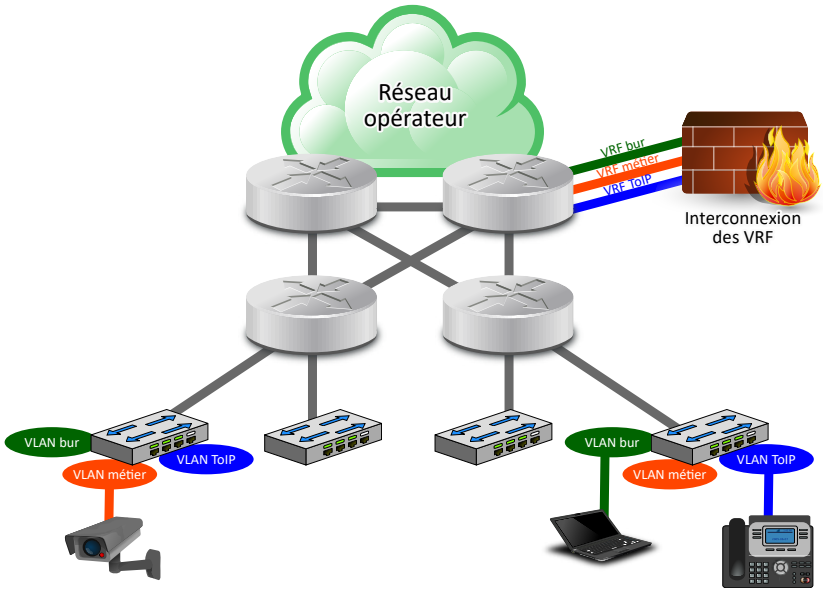

Fig. 2. Réseau routé avec une VRF par besoin

Les besoins de sécurité de ce réseau étaient alors centrés sur la disponibilité : il s'agissait d'assurer une résilience maximale face aux incidents de sécurité, que la connectivité reste présente et que jamais la crise Conficker ne se reproduise. Le réseau n'était pas vu comme un levier de sécurité pour les équipements qui y sont connectés, et la sécurisation des équipements réseau eux-mêmes fut sous-dimensionnée.

En parallèle, les autres réseaux présents sur site, jusqu'ici séparés physiquement pour chaque besoin (gestion technique de bâtiment, contrôle–commande, automates industriels…) et *air-gappés*, commençaient à avoir des besoins d'interconnexion externe. Avec l'arrivée du WiFi et l'interconnexion de ces systèmes métier, l'architecture se complexifia pour accueillir tous ces besoins tout en maintenant une segmentation de sécurité. Cela nécessita une multiplication des équipements de sécurité, qui à son tour augmenta les coûts d'exploitation. La figure 3 représente l'architecture typique qui en découle encore aujourd'hui sur de nombreux sites.

Le contrôle d'accès au réseau (NAC) L'arrivée du WiFi d'une part, et les menaces pesant sur le réseau dans des zones parfois insuffisamment

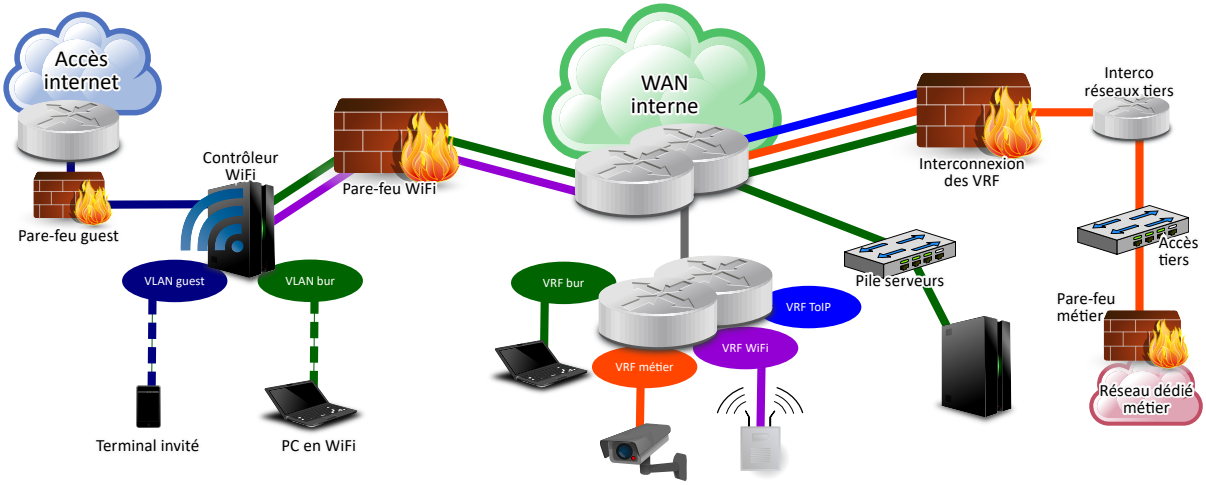

Fig. 3. Architecture simplifiée d'un site industriel typique

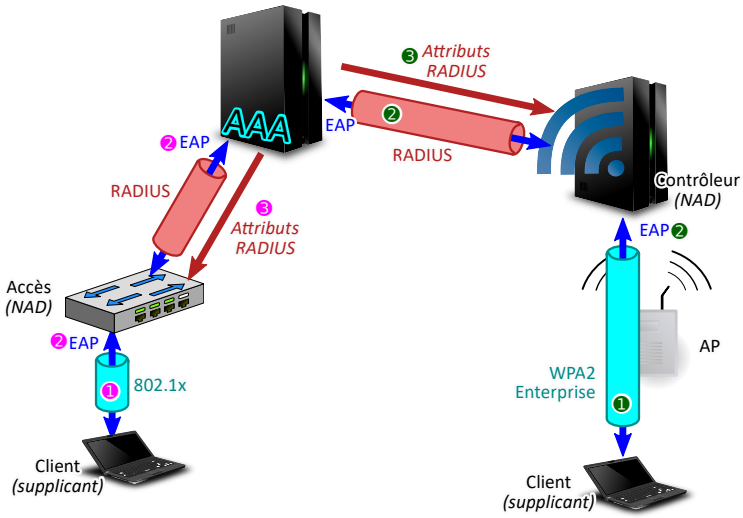

Fig. 4. Schéma de principe du contrôle d'accès au réseau

sécurisées physiquement d'autre part, imposèrent la mise en place d'une infrastructure de contrôle d'accès, schématisée sur la figure 4. Ce contrôle d'accès sur la couche 2 est défini, pour les accès filaires, par le protocole 802.1x [5,11], et pour les accès WiFi, par le protocole WPA2-Enterprise [2] puis WPA3-Enterprise [1]. Il s'appuie sur une authentification EAP [7] entre le terminal et le point d'accès (commutateur ou contrôleur WiFi), relayée par protocole RADIUS jusqu'à un serveur centralisé dit AAA (*Authentication, Authorization & Accounting*).

L'usage du protocole EAP permet une grande flexibilité dans les modes d'authentification :

— EAP-TLS : authentification par certificat (le mode le plus sécurisé) ;
— EAP-TTLS : authentification par mot de passe ou OTP dans un tunnel TLS ;
— d'autres extensions sont disponibles, comme PEAP, EAP-FAST, EAP-GTC, LEAP.

1.2 Enjeux actuels sur les réseaux locaux

Équipements à connecter Avec la généralisation du télétravail, le terminal bureautique n'est plus au cœur des besoins de sécurité du réseau. Si ce terminal reste un utilisateur important et guide les besoins en performance (bande passante, latence, qualité de service), sa sécurité peut de plus en plus être rendue indépendante du réseau par l'usage de protocoles considérés comme quasi inviolables quand ils sont correctement configurés (IPsec, TLS).

Dans des bureaux, les autres équipements avec des besoins de connectivité sont typiquement des imprimantes, des équipements multimédia (écrans, barres de son), des téléphones IP, des systèmes de visioconférence et parfois des équipements plus exotiques : automates de salle de réunion, éclairage connecté, volets roulants... Ces matériels ont une durée de vie qui dépasse largement celle du support sécurité de leurs systèmes embarqués, quand ce support existe. Ils sont donc vulnérables à des attaques latérales et peuvent servir de rebond à un attaquant pour joindre des systèmes sensibles, quand ils ne manipulent pas eux-mêmes des informations sensibles.

Avec des risques plus élevés encore, on trouvera les systèmes de gestion technique du bâtiment et de la sécurité physique : contrôle d'accès, vidéosurveillance, contrôle environnemental. Les systèmes de sûreté des personnes (incendie, évacuation, ascenseurs) doivent rester physiquement isolés.

À tous ces équipements viennent s'ajouter une myriade de capteurs issus de l'internet des objets (IoT) : capteurs de présence, de température, de bon fonctionnement des systèmes industriels ou tertiaires... De plus en plus, ces capteurs n'ont pas de connectivité IP : ils peuvent utiliser des réseaux BLE (Bluetooth Low Energy), Zigbee, Enocean ou se baser sur un opérateur LPWAN.

Enfin, en fonction de l'usage des locaux, on trouvera des systèmes industriels dont il est nécessaire de faciliter l'interconnexion depuis n'importe quel point du bâtiment, tout en préservant une isolation physique pour les plus sensibles.

Limites du NAC Il est aujourd'hui possible de déployer simplement des certificats sur les terminaux Windows, Linux, Android et iOS, permettant leur authentification en EAP-TLS sur les infrastructures réseau. Il devient également possible de protéger ces certificats physiquement, avec un module TPM2 sur PC ou son équivalent chez certains constructeurs de smartphones. Ce n'est pas le cas de l'immense majorité des autres équipements à connecter.

En WiFi, la quasi-totalité des terminaux supportera, au mieux, une authentification de type WPA2-PSK, sécurisée par une clé partagée. Cela a conduit les fournisseurs de matériel WiFi à proposer des technologies de clés partagées multiples sur un unique SSID, appelées *Multiple PSK* ou *Dynamic PSK*, permettant d'avoir une clé par type d'équipement. La compromission d'une clé ne permet donc d'attaquer que les sous-réseaux qui abritent ces équipements.

En Ethernet, il est très rare de trouver des éditeurs avec du support 802.1x. Tout accès authentifié au réseau se base donc sur une fonctionnalité des commutateurs nommée « authentification MAC ». L'authentification EAP est remplacée par un unique identifiant qui n'est autre que l'adresse MAC. Cela revient donc en pratique à supprimer l'authentification pour la remplacer par un mécanisme extrêmement simple à usurper.

Pour ces raisons, l'accès WiFi, jadis considéré comme une vulnérabilité, présente aujourd'hui des risques nettement moins élevés que l'accès Ethernet au même réseau local. Cette conclusion a été corroborée par plusieurs audits.

Menaces La menace la plus fréquente actuellement est la compromission d'un terminal connecté au réseau local. En effet, les terminaux disposant d'un accès e-mail ou Internet, qu'il soit direct ou indirect, invité ou interne, peuvent être compromis par de nombreuses techniques, la plus

répandue étant le phishing. De plus, notre modèle de menace considère qu'un terminal peut conduire des opérations offensives sans être totalement compromis ; par exemple, une attaque de type XSS peut conduire à exécuter du code Javascript malveillant qui va pouvoir tenter des connexions à d'autres machines sur le réseau interne.

Bien que moins courante, la menace d'introduction d'un équipement compromis est augmentée par le nombre et la variété des équipements interconnectés au réseau. Ceci est en particulier vrai pour les équipements multimédia, dont il existe des dizaines de fournisseurs et dont il est impossible d'auditer toutes les références.

Pour les systèmes les plus critiques, nous utilisons de plus en plus un modèle de menace prenant en compte les attaques hybrides, mélangeant les menaces cyber et physiques. À ce titre, la gestion du risque doit prendre en compte simultanément les menaces cyber sur les systèmes de sécurité physique et les menaces physiques sur le réseau. À noter qu'EDF est maître d'œuvre du projet européen Praetorian [12], qui vise à mettre en place des outils d'anticipation et de réaction face à de telles menaces.

2 De nouvelles solutions défensives basées sur la micro-segmentation

2.1 Le SD-LAN

Les concepts de *Fabric* et de SDN (*Software Defined Network*) se déclinent sur les réseaux locaux en SD-LAN. Selon les constructeurs, on pourra aussi parler de *SD Access*, *SD Edge* ou *SD-Branch*. Ces architectures sont basées sur des tunnels permettant de mettre en place des réseaux logiques, dits *overlays*, par dessus un réseau physique dit *underlay*, dont l'architecture typique est représentée figure 5.

Réseau underlay L'*underlay* est un réseau de niveau 3 dont la principale fonction est de fournir une interconnexion fiable entre les équipements qui constituent le réseau local. Il est routé par un protocole simple (IS-IS ou OSPF) et ne fournit aucun service aux utilisateurs. L'interconnexion des équipements avec les réseaux logiques se fait au niveau de certains routeurs, dits *Edge* (qui sont des commutateurs d'accès avec des fonctionnalités SDN) et *Border* (qui peuvent être mutualisés avec le cœur de réseau). Les points d'accès WiFi sont considérés comme faisant partie de l'*underlay*.

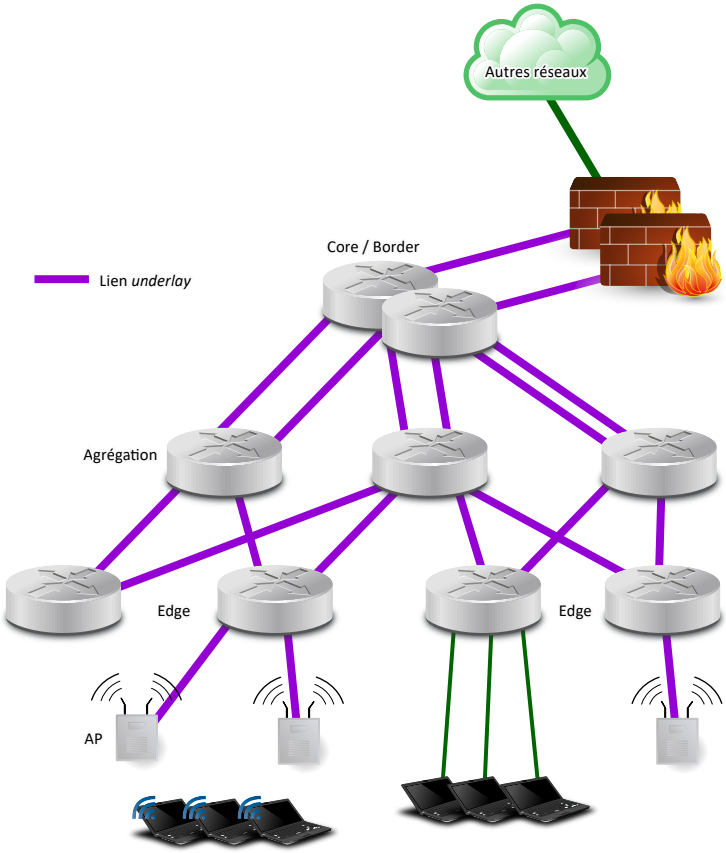

Fig. 5. Exemple d'architecture réseau Underlay pour un SD-LAN

Types d'overlay L'*overlay* consiste en une encapsulation des protocoles de niveau 3, voire de niveau 2, pour pouvoir reconstituer des réseaux virtuels à travers un nombre arbitraire de nœuds du réseau physique.

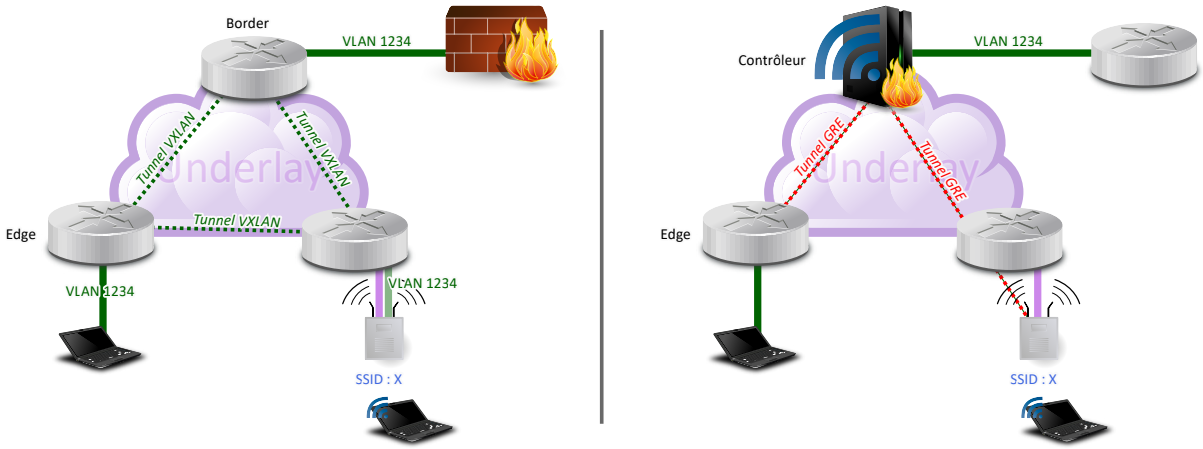

Fig. 6. Overlays pour les deux principales architectures SD-LAN du marché : maillé (à gauche) et *hub-and-spoke* (à droite)

Les principaux modèles de SD-LAN sont schématisés figure 6. Le modèle proposé par Cisco, imité en cela par Huawei et Extreme Networks, est basé sur un *overlay* de type maillé. Celui-ci interconnecte l'ensemble des nœuds du réseau avec un tunnel multipoint.

— Les routeurs *Edge* et *Border* échangent entre eux des informations sur les équipements présents avec un protocole de contrôle, qui peut être EVPN (*Ethernet VPN*) ou LISP (spécifique Cisco).
— Les paquets de données eux-mêmes sont encapsulés dans le protocole VXLAN, qui ajoute au paquet un identifiant de réseau virtuel (VNI – *Virtual Network Identifier*) et éventuellement des extensions propriétaires comme un rôle. Chez Cisco, l'extension se nomme SGT (*Security Group Tag*).
— Grâce aux informations échangées sur le plan de contrôle, les paquets du plan de données sont envoyées, par le chemin le plus court en routage *underlay*, au routeur qui héberge l'équipement qui en est destinataire.

Le deuxième leader du marché est HPE/Aruba, qui propose à la fois un *overlay* VXLAN-EVPN sans extensions propriétaires, mais aussi un *overlay* de type *hub-and-spoke* nommé « segmentation dynamique ». Ce

dernier concentre l'ensemble de la connectivité dans un équipement, le contrôleur de mobilité, qui reprend les fonctionnalités du contrôleur WiFi.

Dans la segmentation dynamique, chaque équipement d'accès (borne WiFi ou routeur *Edge*) ouvre, pour chaque équipement connecté, un tunnel point-à-point avec le contrôleur de mobilité, sur la base du protocole GRE. Le plan de contrôle est totalement interne au contrôleur de mobilité, qui gère l'assignation des différents terminaux aux différents VLAN, et peut leur appliquer des politiques de sécurité avancées avec un pare-feu transparent intégré.

EDF utilise les deux types d'*overlay* sur le même *underlay*, ce qui permet de maximiser les fonctionnalités disponibles dans un environnement où de multiples besoins métier se côtoient. De manière générale, l'*overlay* maillé VXLAN présente une architecture plus élégante et garantissant d'optimiser l'usage des liens sur le réseau local tout en exploitant l'ensemble des fonctionnalités du routeur *Edge*. En revanche, la solution « segmentation dynamique » permet de concentrer des fonctions de sécurité dans un unique équipement beaucoup plus performant et d'appliquer des politiques dynamiques qu'il est plus facile de faire évoluer.

2.2 La micro-segmentation

Filtrage Le concept de micro-segmentation, schématisé figure 7, consiste à introduire des capacités de filtrage internes à un sous-réseau. L'efficacité du filtrage et la granularité de la matrice de flux sont très dépendants de la solution retenue. Concernant le SD-LAN, cette micro-segmentation est associée à une notion de rôle utilisateur (en réalité un rôle associé au terminal).

— Pour les architectures maillées, le filtrage est nécessairement *stateless*. Il est effectué au niveau de chaque commutateur sous forme d'ACL dynamiques associées à chaque rôle. Le rôle est propagé avec chaque paquet IP sous forme d'extensions propriétaires au protocole VXLAN.
— Pour l'architecture *hub-and-spoke*, le filtrage est effectué par le contrôleur qui peut avoir le gros avantage de disposer d'un pare-feu de couches 4 à 7 intégré, avec inspection des flux, filtrage *stateful* et journalisation.

Dans les deux cas, chaque flux, même interne à un sous-réseau, doit être autorisé par le dispositif de filtrage. De plus, il est possible de concentrer les terminaux dans un unique sous-réseau de grande taille, privé de ses fonctionnalités de *broadcast*.

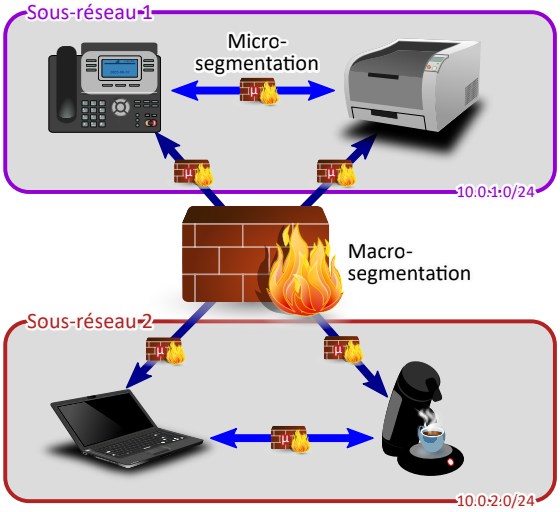

Fig. 7. Schéma de principe de la micro-segmentation

Gestion des rôles Chaque terminal devant être associé à une matrice de flux, la gestion de ces flux est dévolue à une infrastructure centralisée. Le terminal, au moment où il se connecte, est authentifié (par protocole EAP) ou identifié (avec son adresse MAC ou une PSK) par l'infrastructure à travers le point d'accès au réseau, appelé NAD (*Network Access Device*). Le serveur AAA fournit donc à ce NAD (point d'accès WiFi, routeur *Edge* ou contrôleur) toutes les informations nécessaires. En plus d'attributs standard RADIUS comme le numéro de VLAN, il va retourner, avec des extensions propriétaires, les informations sur le rôle utilisateur.

Selon les constructeurs, le détail du rôle, et en particulier la matrice de flux associée, est descendu par l'outillage d'automatisation sur chaque équipement ou directement téléchargé sur le serveur AAA. Le listing 1 montre un exemple de rôle téléchargeable avec micro-segmentation.

```
1  netservice SVC-HTTPS tcp list 443
2  !
3  netservice SVC-SNMP udp list 161
4  !
5  netservice SVC-SYSLOG udp list 514
6  !
7  netdestination NETDEST-SRV-IMP-WINDOWS
8      host 10.10.42.42
9      host 10.10.42.43
10 !
11 netdestination NETDEST-SRV-IMP-SYSLOG
12     host 10.14.1.12
13 !
```

```
14 netdestination NETDEST-SRV-IMP-OUTILLAGE
15     host 10.14.1.42
16 !
17 ip access-list session ACL-SESSION-PRINTERS
18     alias NETDEST-SRV-IMP-OUTILLAGE user SVC-HTTPS permit
19     alias NETDEST-SRV-IMP-OUTILLAGE user SVC-SNMP permit
20     user alias NETDEST-SRV-IMP-SYSLOG SVC-SYSLOG permit
21     alias NETDEST-SRV-IMP-WINDOWS user tcp 9100 permit
22 !
23 user-role cppmrole
24     vlan 1234
25     reauthentication-interval 480
26     access-list session ACL-SESSION-PRINTERS
27 !
```

Listing 1. Exemple de rôle téléchargeable pour une infrastructure Aruba

2.3 Le profilage d'équipements

Pour les (nombreux) équipements nécessitant une connectivité Ethernet mais incapables de s'authentifier en 802.1x, les éditeurs de solutions réseau proposent un mécanisme nommé *profiling*. Il consiste à détecter, par son comportement, les caractéristiques d'un terminal afin de pouvoir lui attribuer un rôle. Le fonctionnement général du profilage est représenté figure 8.

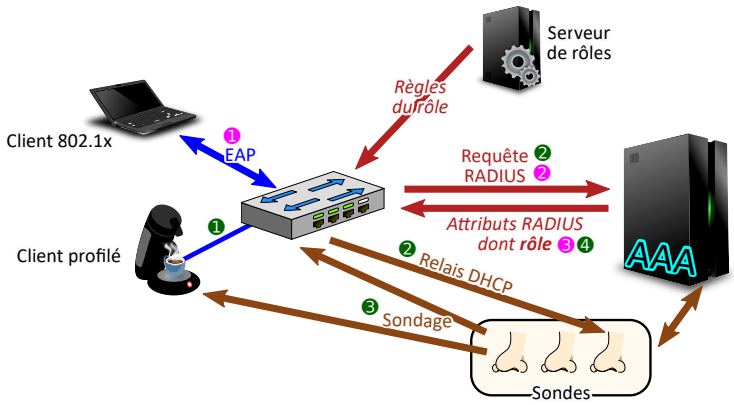

Fig. 8. Schéma de principe de l'attribution des rôles et du profilage

Le profilage se base sur des sondes étudiant le comportement du terminal placé dans un sous-réseau dédié, par exemple :

— contenu de la requête DHCP ;

— interrogation par SNMP ;
— analyse du trafic par NetFlow ;
— agent propriétaire situé sur le terminal ;
— *User-Agent* des requêtes HTTP ;
— connexion par SSH ou WMI.

Une fois l'équipement profilé, son adresse MAC est enregistrée dans une base de données interne et les caractéristiques associées peuvent être associées à un rôle. Ainsi, et c'est un élément crucial pour la cybersécurité, le profilage se substitue en réalité à l'identification par adresse MAC et n'apporte pas de sécurité supplémentaire face à un attaquant qui usurperait des adresses MAC.

3 Sécurité des approches SD-LAN micro-segmentées

3.1 Construire son architecture SD-LAN

À moins d'avoir des besoins assez simples, auquel cas on s'orientera vers la version managée de ces solutions, les architectures SD-LAN ne sont pas fournies clés en mains par les éditeurs et vont devoir s'intégrer à un contexte souvent complexe dans une grande structure.

Protéger l'administration et l'underlay Les protocoles de tunnelisation sur l'*underlay* sont assez complexes, aussi on ne s'étonnera pas d'y trouver, encore récemment, des vulnérabilités très sérieuses [9]. L'isolation complète de l'*underlay* de l'ensemble des réseaux accessibles aux utilisateurs est donc une nécessité absolue. Un pare-feu assurera que seuls les réseaux dédiés aux administrateurs sont autorisés à se connecter. On prendra en particulier garde à ne pas rendre accessibles les interfaces de management des points d'accès et des contrôleurs WiFi, ce qui veut dire empêcher qu'ils aient des interfaces de niveau 3 dans les VLAN utilisateurs.

De même, le service AAA dispose de spécifications et de fonctionnalités très complexes, et une vulnérabilité exploitable peut avoir des effets catastrophiques. Aussi il importe de réduire au strict minimum la surface d'attaque sur ces infrastructures, et de limiter leur accès direct aux seuls équipements réseau par leur interface de service. En particulier, on fuira les fonctionnalités de portail captif proposées par tous les éditeurs ; outre les mauvaises habitudes données aux utilisateurs, elles sont un nid à vulnérabilités. Il ne devrait rester qu'un canal, indirect, accessible aux attaquants : le protocole EAP utilisé pour authentifier le terminal. Et même ce canal est potentiellement exploitable : une implémentation vulnérable

à Log4j pouvait vraisemblablement être attaquée en passant une chaîne malveillante dans un argument d'authentification [3].

Définir sa politique d'authentification Les possibilités d'authentification sont souvent très vastes du côté du serveur AAA, et plus limitées du côté du terminal. Il est donc nécessaire, d'une part, de réaliser un travail prenant en compte, conjointement, l'expérience utilisateur et la sécurité pour définir la solution d'authentification principale. Les limitations fonctionnelles des *supplicants* (clients EAP) peuvent conduire à des compromis ou des travaux d'adaptation non triviaux. Les détails comptent : par exemple, si le client ne vérifie pas correctement la signature du certificat du serveur AAA, il peut être vulnérable à une attaque *man in the middle* et le modèle d'authentification doit en tenir compte.

D'autre part, la politique de sécurité doit être déclinée sous forme d'une politique d'accès au réseau, qui décrit quel type d'authentification est nécessaire pour accéder à quel profil, depuis chaque média d'accès et en fonction de la sécurité physique. Cette politique peut définir des zones de sécurité physiques, et le niveau de protection à atteindre pour y héberger un équipement faiblement authentifié ou non authentifié, et que cet équipement accède à des rôles potentiellement sensibles. Une attention particulière doit évidemment être portée aux équipements de contrôle d'accès physiques eux-mêmes, qui font pleinement partie de la stratégie défensive. Un exemple simplifié de politique d'accès est montré tableau 1.

		Se connecter depuis...		
		Le WiFi ou une zone non contrôlée	**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 de l'équipement	N/A
	Contrôle d'accès	N/A	N/A	Profilage de l'équipement

Tableau 1. Exemple de politique d'authentification

Rendre tout dynamique Le déploiement du SD-LAN est l'opportunité de se débarrasser de toutes les spécificités, en particulier les configurations spécifiques sur tel ou tel port. Sources d'erreur elles-mêmes présentant

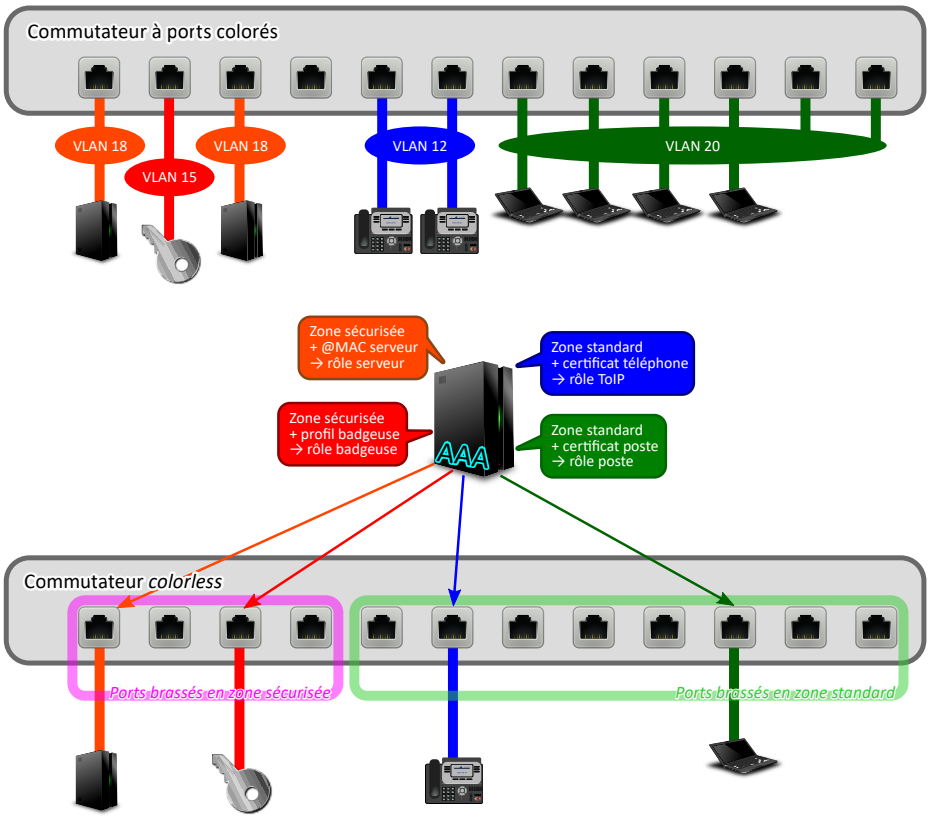

Fig. 9. Schéma de principe d'une configuration dynamique des ports de commutateur

des risques de cybersécurité, ces configurations spécifiques peuvent être réduites à zéro. On parle de commutateurs d'accès *colorless*, en référence aux réseaux de différentes couleurs qui pouvaient cohabiter sur les mêmes équipements et devaient être attribués port par port. La seule « couleur » qui doit rester, et on ne peut pas faire sans elle, est la zone de sécurité correspondant à l'emplacement où le port est brassé. C'est le croisement entre le zonage physique et le niveau d'authentification qui permet de définir le niveau de confiance dans un équipement et donc s'il peut avoir accès à un rôle donné. La figure 9 montre l'évolution dans le mode de paramétrage des ports d'un commutateur.

Avancer pas à pas La palette de fonctionnalités offerte par les services AAA modernes peut donner de grandes ambitions à un architecte ayant pour mission de renforcer la sécurité des réseaux. La complexité de l'approche rend cependant nécessaire de se « faire la main » sur des rôles suffisamment simples. Il reste toujours possible, au fil de l'eau, de faire évoluer la configuration afin :

— d'effectuer une authentification en deux temps si le service le supporte (par exemple, vérifier qu'une imprimante s'est authentifiée sur le serveur d'impression) ;
— de définir des rôles secondaires en fonction de qui est connecté sur le terminal et de ses droits dans l'annuaire d'entreprise ;
— de transmettre les rôles à d'autres composants d'infrastructure (en particulier les pare-feux) ;
— de mettre en place un mécanisme de mise en quarantaine automatisée quand la surveillance sécurité détecte un incident ;
— *etc.*

La figure 10 décrit l'exemple du fonctionnement d'un système de quarantaine, couplé au SIEM de l'entreprise, qui vient s'ajouter à l'existant. L'outillage d'automatisation du SOC (SOAR pour *Security Orchestration, Automation & Response*) vient utiliser les API exposées par le service AAA pour modifier à la volée le rôle d'un terminal au fonctionnement suspect. Celui-ci est alors déconnecté ou placé dans un VLAN dans lequel il n'a accès qu'à des éléments très limités permettant investigation et remédiation.

Connaître son système d'information L'établissement de règles de filtrage pertinentes et fonctionnelles pour l'ensemble des équipements connectés au réseau local requiert une connaissance détaillée des activités réseau de ces équipements. Même dans un contexte de processus existants

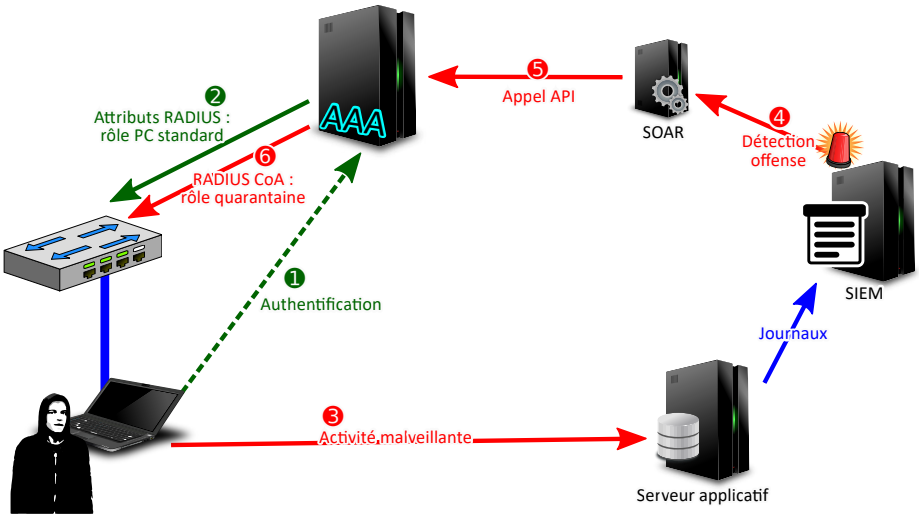

Fig. 10. Schéma de principe de la mise en quarantaine d'un terminal suspect

de validation complète et avec une documentation extensive, la qualité de l'information disponible est très inégale. Elle dépend de la rigueur passée des responsables de projets achevés voilà plusieurs années, et de l'exhaustivité de la documentation des éditeurs. Force est de constater que certains d'entre eux, y compris des leaders du marché, sont avares d'informations techniques pertinentes.

En conséquence, nous avons dû développer des processus et des outils spécifiques pour identifier les flux nécessaires à des équipements pour lesquels la documentation était insuffisante, avec deux approches successives.

L'approche manuelle consiste à positionner les équipements dont on cherche à déterminer les flux dans un réseau routé par un pare-feu avec un filtrage laxiste, et à récupérer les journaux du pare-feu. Un ensemble de scripts Python permet de reconstituer les flux manuellement et de vérifier que tous les paquets observés entrent dans la matrice de flux ainsi reconstituée.

Nous déployons actuellement une approche entièrement automatisée, basée sur notre cluster ELK mutualisé, schématisée figure 11.

— Les données sur tous les flux qui circulent dans le SI sont collectées par les équipements qui en sont capables (pare-feux, contrôleurs) à travers des journaux syslog.
— Pour les anciens réseaux ne disposant pas de dispositifs de filtrage, la tâche s'est révélée plus ardue. Les routeurs en question, même an-

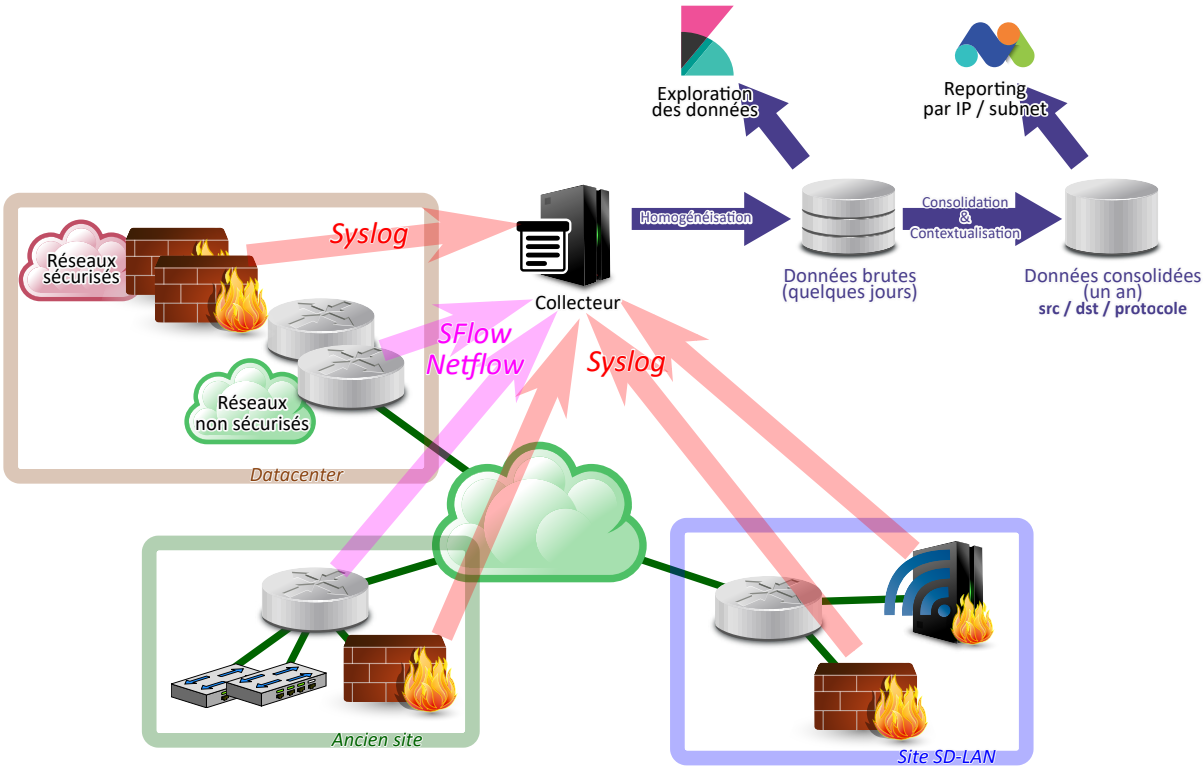

Fig. 11. Schéma de la collecte et de l'analyse des informations de flux réseau

ciens, disposant tous de capacités de journalisation des données par protocole NetFlow ou SFlow, nous avons opté pour ces mécanismes.
— L'ensemble des données (syslog, SFlow, NetFlow) sont centralisées sur un collecteur qui les traite en un format commun, et identique quel que soit la source.
— Ces données brutes, très volumineuses, peuvent être conservées quelques jours pour exploration à l'aide du moteur Kibana.
— Les données sont retraitées pour être consolidées dans une base qui regroupe les flux par source, destination et protocole. Ces données, plus légères, peuvent être conservées plus longtemps.
— Les données sont enrichies par des informations de contexte issues des bases de données d'exploitation : nom des serveurs, applicatifs concernés, instances, exploitants...
— Le moteur Matomo est utilisé pour construire des rapports automatisés permettant, en entrant une adresse IP ou un sous-réseau, d'obtenir la matrice des flux échangés avec ce réseau, regroupés par protocoles et sources/destinations et enrichis des informations de contexte.

3.2 Limites et vulnérabilités de l'approche

Interopérabilité Les solutions de SD-LAN sont, sans exception, propriétaires et non interopérables entre elles. Elles obligent à utiliser le même constructeur pour l'ensemble de l'écosystème : commutateurs, WiFi, serveur AAA, outillage d'automatisation. Cela induit un verrouillage éditeur qui rend difficile la migration vers une autre solution.

De plus, l'interconnexion de l'*underlay*, qui en théorie peut se faire à travers n'importe quel réseau de niveau 3 quelle que soit la technologie sous-jacente, est en pratique limitée.

— Il peut exister des contraintes de support si l'*underlay* transite à travers une technologie différente.
— Les encapsulations ajoutent des octets à chaque paquet, diminuant d'autant la MTU. Celle-ci est recommandée à 9000 par les éditeurs, et selon les configurations c'est une exigence absolue, par exemple quand les routeurs *Edge* ne supportent pas la fragmentation. L'usage de liaisons xDSL ou radio, pour joindre des zones reculées d'un site industriel, est donc complexifié.

Plus gênant, ces solutions ne sont que peu interopérables avec le reste du système d'information. En particulier, un rôle n'est pas propagé d'un site à un autre, ceci même si on utilise une solution de SD-WAN du

même éditeur pour les interconnecter. De même, l'interopérabilité avec les solutions de micro-segmentation existant en datacenter est inexistante.

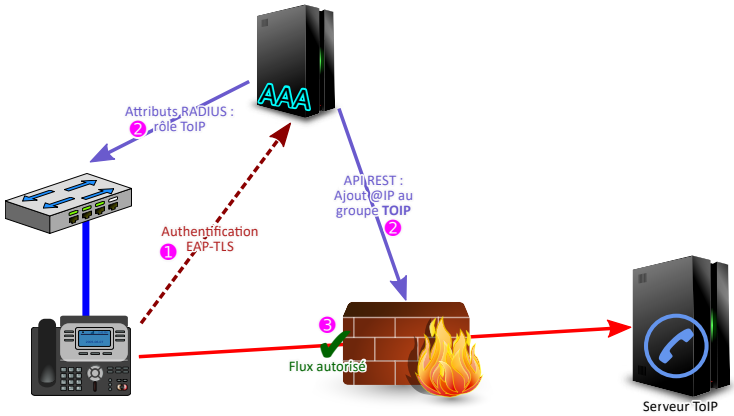

Fig. 12. Intégration d'un système AAA avec des pare-feux pour du filtrage dynamique

Une exception notable à ce manque d'interopérabilité, qui permet de pallier de nombreux défauts, est l'interconnexion des serveurs AAA avec des pare-feux de plusieurs constructeurs, pour peu qu'ils soient capables de gérer des groupes de filtrage dynamiques. Il est donc possible d'ouvrir un flux depuis ou vers un rôle, comme schématisé figure 12.

De manière générale, les serveurs AAA disposent à la fois d'API REST extensives et de la capacité de faire appel à des API REST tierces en fonction d'événements. Cela permet d'interconnecter de nombreuses infrastructures, au prix de développements parfois significatifs. Par exemple, pour l'interconnexion SIEM/SOAR décrite plus tôt, l'implémentation de l'éditeur SOAR était basée sur une ancienne version de l'API du AAA, et nous avons donc dû en recoder une partie.

Ces API pouvant elles-mêmes présenter des vulnérabilités, on veillera dans tous les cas à les ouvrir avec parcimonie pour éviter les attaques latérales.

Limitations fonctionnelles de la micro-segmentation L'administrateur habitué à mettre en place des politiques complexes entre les réseaux au niveau de ses pare-feux peut être déçu par les capacités des systèmes de micro-segmentation. Ceux-ci présentent de nombreuses limites techniques

et fonctionnelles, qui peuvent introduire des contraintes arbitraires et limiter les gains de sécurité.

On pourra citer par exemple :

— limitation à 4 réseaux virtuels (VN) sur la solution Cisco, qui limite en pratique un site à seulement 4 domaines de macro-segmentation entre lesquels il est possible de mettre en place du filtrage avancé (comme décrit figure 7) ;
— limitation de la taille des politiques ;
— absence de récursivité dans les définitions d'objets de filtrage (impossible d'inclure un objet dans un autre objet) ;
— limitation du nombre total d'objets téléchargés par un contrôleur Aruba donné ;
— limitation dans la longueur du nom des objets ;
— manque de granularité dans le filtrage ICMP et ICMPv6 ;
— absence totale de détection protocolaire dans les solutions *stateless* ;
— non implémentation de certaines limites techniques du contrôleur dans le service AAA Aruba Clearpass, entraînant des erreurs difficiles à diagnostiquer.

Autre limitation liée au défaut d'interopérabilité, il n'est pas possible de coordonner les politiques ou les objets de filtrage avec ceux d'autres systèmes, y compris avec les solutions d'automatisation des pare-feux.

De plus, les systèmes basés sur des ACL au niveau des commutateurs sont *stateless*, et donc facilement contournés par un attaquant qui jouerait avec les ports source de ses connexions. Éviter cette vulnérabilité impose de se limiter à des matrices de flux de type « tout ou rien » entre deux rôles du même sous-réseau.

Ces limites peuvent obliger à jongler entre plusieurs dispositifs de sécurité, ouvrir les flux plus largement que nécessaire et donner des opportunités à un attaquant qui aurait obtenu accès au rôle concerné, ou encore complexifier le travail des exploitants pour prendre en compte les limites.

Risques liés au NAC et au profilage Le profilage se base sur des sondes diverses. Un certain nombre de sondes, purement passives et inspectant le trafic (Netflow, DHCP, *User-Agent*), présentent relativement peu de risques. En revanche, les sondes allant activement interroger l'équipement peuvent donner, de la part d'un exploitant imprudent, des informations à un attaquant. Les sondes allant interroger un équipement en WMI ou SSH, en utilisant un compte d'administration authentifié par mot de passe, représentent la quintessence de la fonctionnalité à ne jamais activer si on ne souhaite pas subir une correction par le premier pirate en herbe venu.

De plus, comme nous l'avons vu, le profilage est trivialement exploitable par un attaquant qui usurperait l'adresse MAC d'un équipement déjà reconnu, sans même avoir besoin de simuler son comportement auprès des sondes. Le profilage ne peut donc en aucun cas être utilisé comme équivalant à une authentification : si un équipement peut déroger à la politique d'authentification avec une « authentification » par profilage et atteindre les mêmes composants du système d'information qu'un terminal utilisateur authentifié par certificat protégé par TPM, toute la politique de micro-segmentation vole en éclats.

Enfin, même pour les terminaux authentifiés en 802.1x, il existe des attaques nécessitant des moyens assez modestes : un hub et un vol d'adresse MAC. La suppression de cette vulnérabilité nécessite d'étendre la norme 802.1x avec le chiffrement 802.1ae MACSEC [10], dont le support est relativement récent. La plupart des commutateurs sont incapables de le gérer sur les ports d'accès, et seuls les OS clients récents peuvent se connecter. Les OS rudimentaires embarqués sur tous les équipements nécessitant le profilage sont, de fait, loin de pouvoir y migrer.

La gestion de multiples clés WPA2 PSK apporte donc un gain significatif de sécurité, du moins pour les équipements supportant le WiFi et ne pouvant pas être protégés physiquement. Cependant, elle nécessite, pour être pertinente, le renouvellement des clés ; si possible régulièrement, et systématiquement en cas de vol ou perte d'une clé. Cela peut nécessiter une intervention manuelle sur des systèmes ne disposant d'aucun outil d'automatisation, ce qui est rapidement rédhibitoire.

4 Conclusion : vers un modèle ZTNA

Comme dans de nombreuses autres entreprises, la DSIT (Direction des Systèmes Informatiques & Télécom) d'EDF est confrontée à des enjeux métier qui nécessitent de revoir en profondeur la façon dont on accède au système d'information : l'augmentation du trafic vers des hébergeurs de *cloud* public, la nécessité d'ouvrir les applications à des partenaires, de manière granulaire selon les projets (on parle souvent d'« entreprise étendue »), et en parallèle des exigences réglementaires de plus en plus fortes sur la sécurisation de processus métier critiques vis-à-vis des menaces étatiques.

Le choix de long terme de l'entreprise pour répondre à ces enjeux se porte vers un modèle de sécurité de type *Zero Trust* formalisé par le NIST [6, 13]. Les applications basées sur des protocoles exclusivement web et pouvant déléguer leur contrôle d'accès à une infrastructure de

sécurité s'y prêtent nativement et pourront, à l'avenir, faire de plus en plus abstraction du réseau situé entre le terminal utilisateur et le serveur applicatif.

Cependant, EDF exploite des installations hydrauliques ayant déjà plus de 120 ans, et conçoit de futures usines qui devront fonctionner pendant au moins 60 ans. Cette spécificité, partagée avec d'autres industries lourdes, implique que l'écosystème applicatif fonctionne avec des cycles de vie très longs. Nous devons remplir nos objectifs de sécurité avec des logiciels parfois conçus à une époque où la sécurité était un mot inconnu, et nous devrons également mieux protéger des équipements divers et plus ou moins vulnérables qui utilisent nos infrastructures réseau et manient des données sensibles.

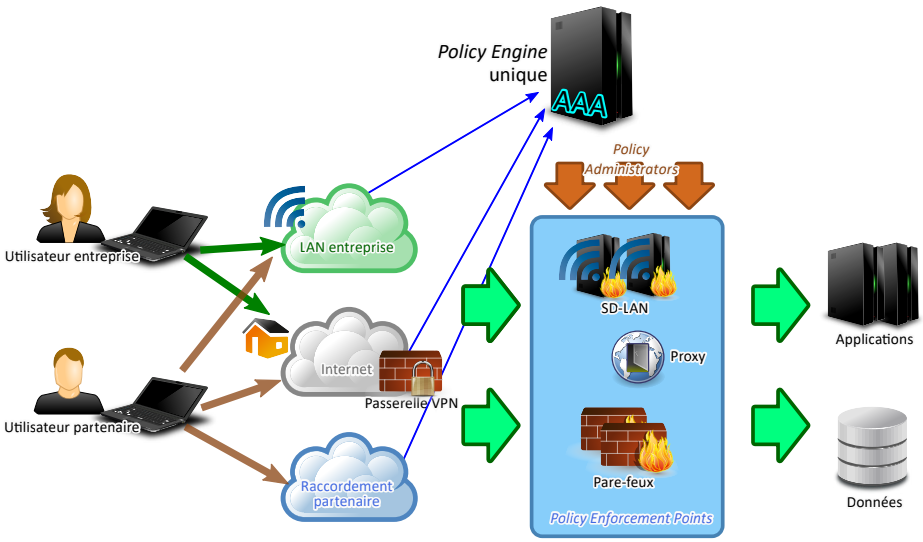

Fig. 13. Schéma de principe d'une architecture ZTNA reprenant les composants du SD-LAN

Pour ces raisons, nous visons à faire évoluer notre architecture réseau vers un modèle dit ZTNA pour *Zero-Trust Network Access*, schématisé figure 13. Dans ce modèle, les contrôles d'accès au réseau, quel que soit le mode de connexion (local ou distant), seront effectués par la même infrastructure, en appliquant les mêmes règles, fonction du niveau de confiance dans le terminal et des droits de l'utilisateur. Ces règles seront appliquées à la fois au niveau des passerelles d'accès au réseau (micro-segmentation, passerelles VPN) et sur les pare-feux au plus près des

applicatifs. Le réseau continuera ainsi à devenir un levier majeur pour bloquer à la source les cyberattaques sur des applicatifs et objets connectés par ailleurs potentiellement sujets à de nombreuses vulnérabilités.

Références

1. Wi-Fi alliance. Wpa3 specification, version 3.0. https://www.wi-fi.org/file/wpa3-specification, 2020.
2. Clint Chaplin, Emily Qi, Henry Ptasinski, Jesse Walker, and Sheung Li. 802.11i overview. https://www.ieee802.org/16/liaison/docs/80211-05_0123r1.pdf. Réf : IEEE 802.11-04/0123r1.
3. Cisco. Vulnerabilities in apache log4j library affecting cisco products : December 2021. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd, 2021.
4. Agence Nationale de la Sécurité des Systèmes d'Information. Recommandations pour la sécurisation d'un commutateur de desserte. https://www.ssi.gouv.fr/uploads/2016/07/nt_commutateurs.pdf, 2016. Réf : DAT-NT-25/ANSSI/SDE.
5. Agence Nationale de la Sécurité des Systèmes d'Information. Recommandations de déploiement du protocole 802.1x pour le contrôle d'accès à des réseaux locaux. https://www.ssi.gouv.fr/uploads/2018/08/guide_802.1x_anssi_pa_043_v1.pdf, 2018. Réf : ANSSI-PA-043.
6. Agence Nationale de la Sécurité des Systèmes d'Information. Avis scientifique et technique : le modèle zero trust. https://www.ssi.gouv.fr/uploads/2021/04/anssi-avis_scientifiques_et_techniques-modele_zero_trust.pdf, 2021.
7. Internet Engineering Task Force. Rfc 3748 – extensible authentication protocol. https://datatracker.ietf.org/doc/html/rfc3748, 2004.
8. Jean-Marc Leclerc. La Marine attaquée par un virus informatique. https://www.lefigaro.fr/actualite-france/2009/02/10/01016-20090210ARTFIG00013-la-marine-attaquee-par-un-virus-informatique-.php, 2009.
9. Aruba Networks. Buffer overflow vulnerabilities in the papi protocol (cve-2021-37716). https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt.
10. Institute of Electrical and Electronics Engineers. 802.1ae-2018 – ieee standard for local and metropolitan area networks-media access control (mac) security.
11. Institute of Electrical and Electronics Engineers. 802.1x - port based network access control.
12. H2020 Praetorian. Praetorian – protection of critical infrastructures from advanced combined cyber and physical threats. https://praetorian-h2020.eu/, 2022.
13. Scott Rosee, Oliver Borchert, Stu Mitchell, and Sean Connelly. Zero trust architecture. https://doi.org/10.6028/NIST.SP.800-207, 2020.

Glossaire

AAA	*Authentication, Authorization & Accounting*	Service de contrôle d'accès au réseau implémentant les 3 composants : authentification, autorisation et comptabilité des accès.
ACL	*Access Control List*	Commandes de filtrage *stateless* mises en place au niveau d'un équipement réseau (commutateur ou routeur).
EAP	*Extensible Authentication Protocol*	Protocole d'authentification modulaire, utilisable pour des authentification filaires (802.1x), WiFi (802.11i) ou IPsec.
EVPN	*Ethernet VPN*	Protocole standard de contrôle de la localisation des adresses MAC sur un sous-réseau étendu.
LISP	*Locator/ID Separation Protocol*	Protocole standard (mais implémenté uniquement par Cisco) de contrôle de la localisation d'équipements sur un sous-réseau étendu.
NAC	*Network Access Control*	Contrôle de l'accès au réseau filaire, sur la base du protocole 802.1x.
NAD	*Network Access Device*	Équipement fournissant l'accès au réseau et client du service RADIUS.
SDN	*Software Defined Network*	Architecture réseau permettant d'abstraire la topologie logique du réseau de sa topologie physique, et de déployer rapidement de nouveaux services.
SD-LAN	*Software Defined LAN*	Implémentation de SDN à usage de réseau local.
SD-WAN	*Software Defined WAN*	Implémentation de SDN à usage de réseau d'interconnexion.
SGT	*Security Group Tag*	Ensemble d'extensions propriétaires Cisco permettant de propager des informations de rôle dans les paquets IP encapsulés.
SIEM	*Security Information Management System*	Outil de collecte et de corrélation des journaux de sécurité.
SOAR	*Security Orchestration, Automation & Response*	Outillage d'automatisation de la réponse sécurité du SOC.
TPM	*Trusted Platform Module*	Module matériel de gestion de la cryptographie n'intégrant pas de stockage dédié.
VLAN	*Virtual LAN*	Réseau virtuel de niveau 2.
VN	*Virtual Network*	Réseau virtuel (équivalent de VLAN) pour la solution de SD-LAN Cisco (SD-Access).
VRF	*Virtual Routing & Forwarding*	Mécansisme permettant d'avoir plusieurs piles IP indépendantes sur un même routeur, permettant de faire cohabiter plusieurs réseaux IP indépendants sur le même équipement.
VXLAN	*Virtual eXtensible LAN*	Protocole d'encapsulation pour monter un tunnel multi-points de niveau 2 sur un réseau de niveau 3, permettant d'étendre un sous-réseau.
ZTNA	*Zero-Trust Network Access*	Implémentation du paradigme *Zero-Trust* sur la couche réseau, autorisant ou empêchant l'accès aux équipements concernés en fonction du terminal et des droits de l'utilisateur.