



Hervé Schauer Sécurité

SecuArch

Sécurité des architectures

mars 2021



Accueil

Bienvenue en SecuArch !

mars 2021

En résumé...

C'est là où on se présente et où on présente la formation.

- | | | |
|---|------------------------------|----|
| 1 | Présentation de la formation | 5 |
| 2 | Objectifs de la formation | 18 |
| 3 | Signalétique | 23 |

1	Présentation de la formation	5
	Présentation	6
	Déroulement de la formation	11

Bienvenue !

Jordan Hordé <jo.horde.glhf@gmail.com>

- 8 ans d'expérience en informatique et SSI
 - Auditeur
 - Formateur indépendant en sécurité

Certifications

- PCI QSA (Payment Card Industry Qualified Security Assessor) par le PCI SSC
- EBIOS 2010 et ISO 27005 Risk Manager, ISO 27001 Lead Implementer et Lead Auditor par LSTI
- INTRU1, SECWEB, INFO1 et SECWIN par HSC

Formations

- SECUARCH
- EBIOS2018
- ISO27RM
- EBIOS2010
- ISO27LA

Mikaël Smaha <formation-secuarch@mx.ouda.fr>

- 12 ans d'expérience en informatique et SSI
 - Coordinateur technique de réponse aux incidents
 - Formateur indépendant en sécurité

Certifications

- EBIOS 2010 et ISO 27005 Risk Manager, ISO 27001 Lead Implementer et Lead Auditor par LSTI
- GNFA (GIAC Network Forensic Analyst) GIAC
- SECWIN et SECDRIS par HSC

Formations

- SECUARCH
- EBIOS2018
- EBIOS2010
- ISO27RM
- ISO27LA

Matthieu Schipman <matthieu.schipman@gmail.com>

- 40 ans, 16 ans d'expérience en informatique et SSI
 - 10 ans en entreprise, 5 ans en SSII
 - Pentesteur et formateur indépendant en sécurité

Certifications

- CISSP (Certified Information Systems Security Professional) par ISC²
- GPEN (GIAC Penetration Tester), GCFE (GIAC Certified Forensic Examiner), GCWN (GIAC Certified Windows Security Administrator), GMON (GIAC Continuous Monitoring Certification) par GIAC
- ISO 27001 Lead Implementor par LSTI

Formations

- ESSCYBER
- SECUCYBER
- SECUBLUE
- SECUWIN
- SECUARCH
- RSSI
- CISSP

1	Présentation de la formation	5
	Présentation	6
	Déroulement de la formation	11

- De 9h30 à 18h00
 - Ouverture de la salle à partir de 9h00
 - Fermeture à 18h30 (centre)
- Pauses le matin et l'après-midi
 - Boissons froides, chaudes et viennoiseries à disposition
- Repas
 - 12h00 - 13h30
 - Inclus dans le tarif de la formation
 - Restaurant différent tous les jours
 - **Merci de nous dire le matin :**
 - Si vous ne souhaitez pas venir
 - Ou si vous avez une demande spécifique

- Locaux non-fumeurs
 - Mais très belle terrasse au 5ème :)
- Toilettes au bout du couloir
- Téléphone portable
 - Si possible durant les pauses
 - Sinon, à l'extérieur de la salle
- Le centre propose un Wi-Fi gratuit
 - Avec vos équipements personnels
 - Pas avec les PC d'exercice

- Lundi
 - Matin
 - Premier contact
 - Introduction aux architectures sécurisées
 - Rappels théoriques et réseaux
 - Après-midi
 - Composants d'architectures
 - Quelques aspects importants des flux
- Mardi
 - Matin
 - Architecture de base
 - Architecture en bulles
 - Authentification
 - Administration

- Mardi
 - Après-midi
 - Architecture de base (suite)
 - Infrastructure et sécurité
 - Applications
- Mercredi
 - Matin
 - Architecture de base (fin)
 - Continuité
 - Exercice !
 - Après-midi
 - Architectures spécifiques
 - Examen

- Mercredi après-midi
 - Dans cette salle, sur un PC fourni par HS2
- 1h, 50 questions
 - QCM, une et une seule bonne réponse
- Support de cours autorisé
- Seuil de réussite : 70%
- Pour le retour, pensez à réserver votre transport à l'avance

- Prénom, nom, organisme et fonctions actuelles
- Parcours, expérience en sécurité
- Manipulation de l'architecture
 - Conception ?
 - Mise en œuvre ?
 - Audit ?
- Connaissances systèmes et réseaux
- Attentes vis-à-vis de la formation

Objectifs de la formation

- | | | |
|---|------------------------------|----|
| 1 | Présentation de la formation | 5 |
| 2 | Objectifs de la formation | 18 |
| 3 | Signalétique | 23 |

- Savoir identifier les choix structurants
 - *Est-ce que je dois créer une DMZ pour exposer mon Kibana sur Internet ?*
- Savoir faire des choix de conception
 - *Puis-je mettre en œuvre une supervision centralisée ?*
 - *Comment mutualiser la supervision entre plusieurs systèmes d'information clients dédiés ?*
- Savoir évaluer le niveau de sécurité d'une architecture
 - *Tous les serveurs ont une interface d'administration dans le VLAN 800. C'est bien ?*
- Savoir sécuriser les architectures communément mises en œuvre
 - *À quoi dois-je faire attention quand j'installe mon Active Directory ?*

Nous nous concentrerons sur l'architecture !

- Savoir gérer un projet d'évolution d'architecture
 - *Combien de temps me faudra-t-il pour segmenter mon réseau ?*
- Savoir administrer et exploiter un système d'information
 - *Comment j'applique les correctifs sur un serveur Debian 9 ?*
- Connaître le détail de protocoles de communication réseaux
 - *Comment fonctionne IKE ?*
- Connaître le détail de paramètres de configuration
 - *Quelle est la commande pour définir un 'Private VLAN' en mode isolé sur le VLAN 800 ?*
- Répondre à des situations personnelles
 - *J'ai un client, <Entrez ici le nom du client>, qui administre son z/OS avec Telnet parce que [...]*

Généralisez vos questions pour en aider d'autres

- Expérience de l'audit et du conseil
- Réflexion sur les principes de sécurité et leurs déclinaisons
- Référentiels de bonnes pratiques
 - Guides NSA, NIST, Clusif, ANSSI, ENISA
- Documentation
 - RFC, normes
 - Documentations éditeurs
 - Code source de logiciels libres
- Discussions multiples

- La logique d'élaboration est le cœur de la formation
- La sécurité est toujours une question de compromis
 - La sécurité ajoute souvent des coûts et des contraintes
 - Différents aspects de la sécurité peuvent s'opposer
- Nous espérons que vous aurez aussi votre point de vue
 - Et que nous pourrons en discuter sereinement

- 1 Présentation de la formation
- 2 Objectifs de la formation
- 3 Signalétique

5

18

23



Regardez en haut à droite !

Cela représente un type d'équipement (ici, un pare-feu) et sera repris à l'identique dans les schémas d'architecture tout le long de la formation.



Point à retenir



Points principaux du chapitre



Point de détail qu'il n'est pas nécessaire de retenir



Vulnérabilités, menaces, risques liés au sujet traité



Mesures de sécurité ou bonnes pratiques liées au sujet traité et aux risques associés

Introduction

mars 2021



En résumé...

C'est là où on définit les bases et où on fait un point de vocabulaire.

1	Principes de sécurisation	29
2	Principes d'architecture	32
3	Vocabulaire	43
4	Lien avec d'autres domaines	47
5	Dessine-moi un schéma	53

Définition : sensibilité

Aptitude à ressentir la douleur [...] à l'action de certains agents.

- **Objectif #1** : identifier les éléments à protéger : *Biens essentiels / Actifs primordiaux / Valeurs métier*
 - Informations : on cherche les données
 - Processus : on suit les éléments de support
 - Serveurs, composants réseaux, etc.
 - Éléments de sécurité
 - Authentifiants, clefs de chiffrement, sauvegardes, etc.

Définition : attractivité

Aptitude à inciter un être vivant à se rapprocher.

- Être vivant = attaquant / se rapprocher = compromettre
 - En général : ce qui est sensible est attractif

Définition : exposition

Fait d'être soumis à l'action de [menaces].

- Dépend de facteurs liés aux sources de menaces :
 - motivation (\Rightarrow attractivité)
 - nombre et types
 - capacité à les maîtriser

Définition : connectivité

Aptitude d'un ou plusieurs éléments conducteurs à être liés.

- **Objectif #2** : diminuer la surface d'attaque
 - Durcissement système, **durcissement réseau**
 - Minimisation des priviléges, **minimisation des interconnexions**
 - Globalement, on cherche à supprimer des branches dans l'arbre d'attaque

1	Principes de sécurisation	29
2	Principes d'architecture	32
3	Vocabulaire	43
4	Lien avec d'autres domaines	47
5	Dessine-moi un schéma	53

La sécurité est un compromis...

... alors il faut se lever tôt pour obtenir un résultat satisfaisant.

Définition

La défense en profondeur vise à maîtriser l'information et le système qui la supporte par l'équilibre et la coordination de lignes de défense indépendantes, dynamiques ou statiques, dans toute la profondeur du système d'information (c'est à dire dans la dimension organisationnelle, de la mise œuvre et des technologies).

- La perte d'une mesure de sécurité doit permettre de renforcer les suivantes
 - Difficile à appliquer en dehors d'un château fort
- Donc on additionne des mesures de sécurité
 - indépendantes
 - dans un unique objectif (réduisant le même risque)



Tout composant a ou aura sa RCE sans pré-requis

CVE-2021-26855 OWA d'Exchange

CVE-2020-1472 Contrôleurs de domaine (10.0 CVSS,
nommée Zerologon)

CVE-2020-1350 DNS de l'AD (10.0 CVSS)

CVE-2019-11510 Firewall Pulse : lecture de fichiers arbitraires
non authentifiées (10.0 CVSS)

CVE-2019-1579 Firewall Global Protect de Palo-Alto (8.1
CVSS)

- CVE-2019-12255-65 Pile IP et TCP de VxWorks (7.5 CVSS nommée URGENT/11)
- CVE-2019-0708 RDP sur Windows XP à Windows 2008 R2 (10.0 CVSS nommée Bluekeep)
- CVE-2018-0101 SSL du VPN Cisco (10.0 CVSS)
- CVE-2018-6789 SMTP dans Exim (7.5 CVSS)
- CVE-2018-1207 CGI iDrac (7.5 CVSS)
- CVE-2017-12542 HTTP sur iLO (10.0 CVSS)
- CVE-2017-0147 (MS17-010) SMB sur Windows XP à Windows 10 (9.3 CVSS nommée EternalBlue)
- CVE-2016-6277 HTTP sur Netgear (9.3 CVSS)

CVE-2014-0160 SSH d'OpenSSL (5.0 CVSS nommée Heartbleed)

CVE-2008-4250 (MS08-067) RPC sur Windows 2000 à Windows 2008 (10.0 CVSS)



Tout fournisseur a ou aura sa compromission (du réseau bureautique)

Keep it simple, stupid !

Toute complexité superflue doit être évitée.

- Temps, compétences nécessaires au maintien et à l'évolution
- Erreurs de manipulation, de configuration, de compréhension
- Principes associés : **homogénéité**, exploitabilité, etc.

Cohérence

Le niveau de sécurité d'un système d'information est celui de son composant le plus faible.

- La protection des grands réseaux à plat est quasiment impossible
- Le niveau d'un flux non sécurisé est celui du réseau le plus faible qu'il traverse

Vision à long terme

L'architecture nécessite d'avoir une vision à long terme de l'évolution de son réseau.

- Les mauvais choix d'architecture se paient longtemps

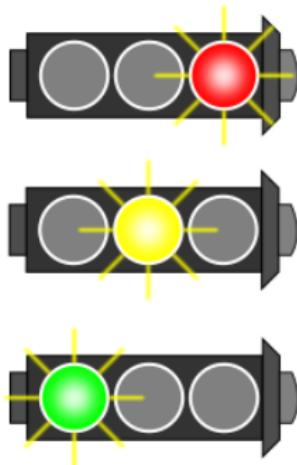


Figure – Les niveaux avant



Figure – Les niveaux maintenant

- Moindre privilège
- Besoin d'en connaître
- Minimisation
- Respect des exigences contractuelles, légales, réglementaires et statutaires
- ...
- Peuvent également être applicables !

1	Principes de sécurisation	29
2	Principes d'architecture	32
3	Vocabulaire	43
4	Lien avec d'autres domaines	47
5	Dessine-moi un schéma	53

Segmentation

Division en segments. *Synon. fractionnement, fragmentation.* (i.e. installer des commutateurs et des routeurs.)

Cloisonnement

Action de diviser, séparer par une ou plusieurs cloisons. (i.e. ajouter du filtrage entre les segments.)

Isolation

Action, fait de mettre à part, mettre à l'écart matériellement ou moralement. (i.e. déconnecter un composant du reste du réseau.)

Ségrégation

Action de séparer quelqu'un ou quelque chose d'un ensemble.
(i.e. diviser un ensemble en sous-ensembles. (cf. **segmentation**?)
i.e. déplacer des éléments en dehors de l'ensemble. (cf. **isolation**?))

Risque (ISO/IEC 27000)

Effet de l'incertitude sur l'atteinte des objectifs.

- Plus précisément : exploitation d'une vulnérabilité sur un actif par une menace
 - Évalué selon sa vraisemblance et ses conséquences

Vulnérabilité (ISO/IEC 27000)

Faillie dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces.

- On cherche donc des moyens de traiter les risques élevés
 - Ce qui mène à des choix de conception

Origine

Du latin *personare* (*per-sonare* : « parler à travers »). Désigne le masque que portaient les acteurs de théâtre romains.

Informatique

Désigne l'identité numérique qui réalise une action.

- Il n'y a pas forcément de relation 1 :1 entre persona et personne
 - Mutualisation d'un persona par plusieurs personnes
 - Utilisation de multiples personas par une même personne
 - Vol ou duplication du persona

1	Principes de sécurisation	29
2	Principes d'architecture	32
3	Vocabulaire	43
4	Lien avec d'autres domaines	47
5	Dessine-moi un schéma	53

- But = traiter les risques et mettre en œuvre des mesures de sécurité associées
 - Une architecture correctement conçue constitue un ensemble de mesures de sécurité
 - Cloisonnement des composants et diminution de la surface d'attaque
 - Une architecture (même correctement conçue) présente des vulnérabilités
 - Qui seront analysées dans une gestion de risques

- Apporte de la sécurité, donc des changements de pratiques
 - "Contraintes"
 - Parce qu'on ne peut plus se connecter en RDP avec son compte d'admin' de domaine pour installer Excel sur un PC de la compt'.
 - Demande de la rigueur aux administrateurs

- Même chose que l'administration pour ce qui est de l'intervention de prestataires
- Impacte également la manière de s'interconnecter avec des tiers
 - Oubliez les réseaux MPLS à plat pour interconnecter toutes les filiales du groupe.

- Vision des systèmes d'information en couches :

Processus

Applications

Technique

(logiciel, système, réseau)

Physique

- On traite principalement les aspects techniques et parfois physiques
 - Les aspects processus et applications sont censés conduire l'*urbanisation* des systèmes d'information
 - Mais beaucoup se limitent aux aspects logiciels, parfois systèmes, et délaissement notamment les aspects réseaux

- Apporte des contraintes (qui doivent être spécifiées dans les cahiers des charges)
 - Méthodes d'authentification
 - Configuration de relais et relais inverses
 - Séparation des fonctions
 - *tiers* logiciels : présentation / traitement / accès aux données
 - et autres paradigmes d'architecture logicielle

1	Principes de sécurisation	29
2	Principes d'architecture	32
3	Vocabulaire	43
4	Lien avec d'autres domaines	47
5	Dessine-moi un schéma	53

Exemples

Réseau d'une baie

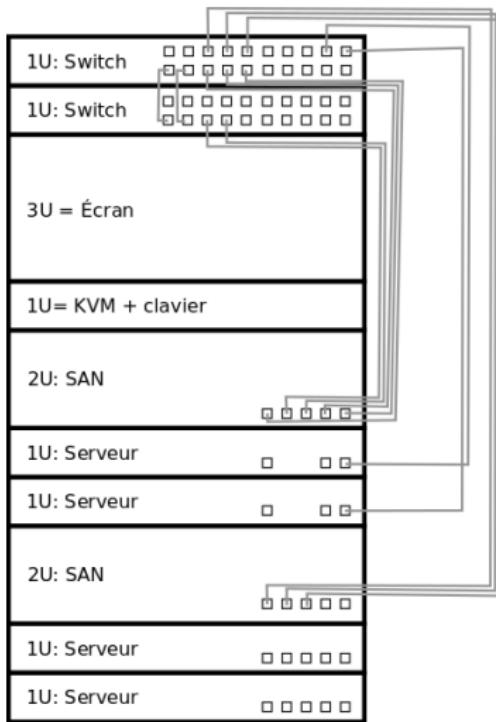


Figure – Réseau niveau 1

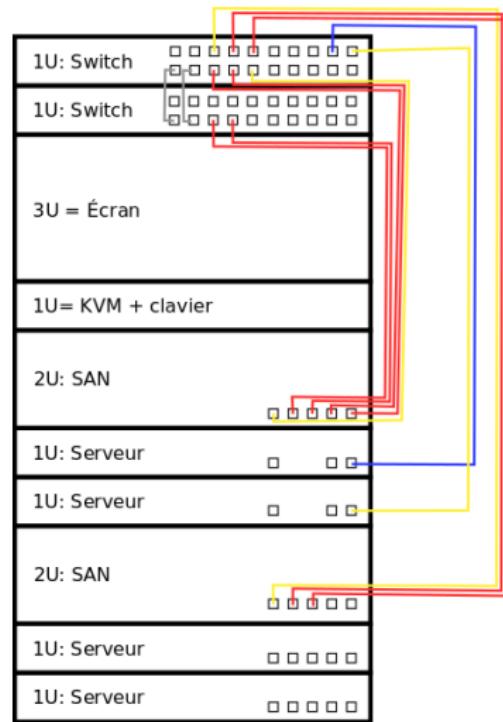


Figure – Réseau niveau 1½

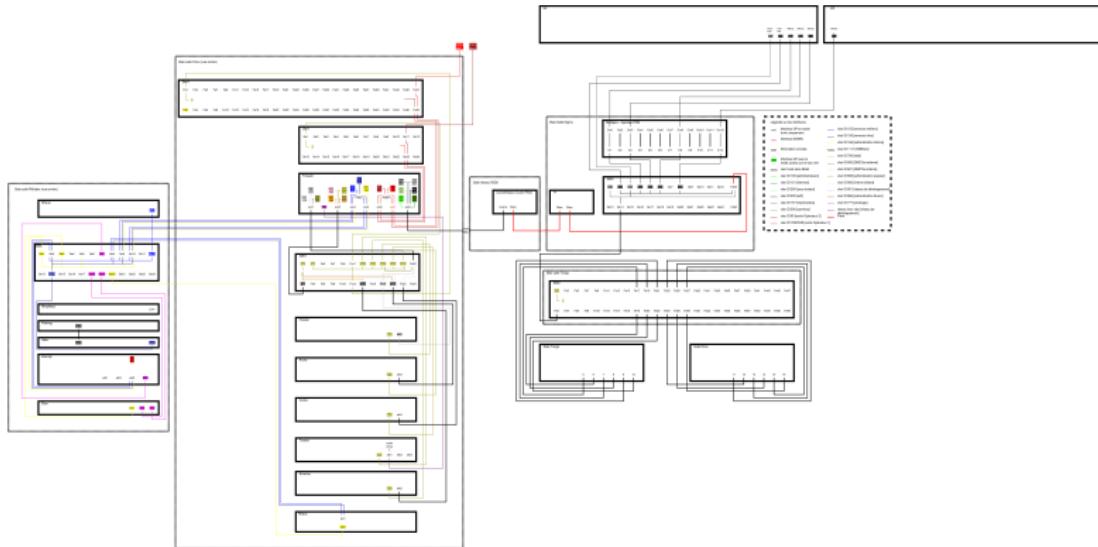


Figure – Réseau niveau 1 et 2

Exemples

Réseau simplifié

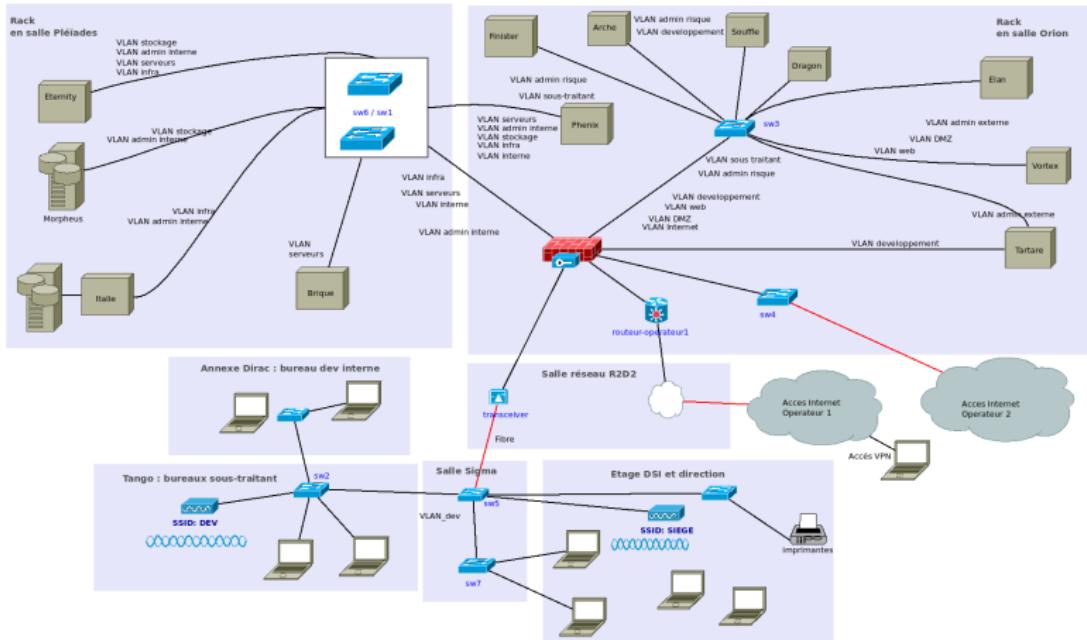


Figure – Réseau niveau 2

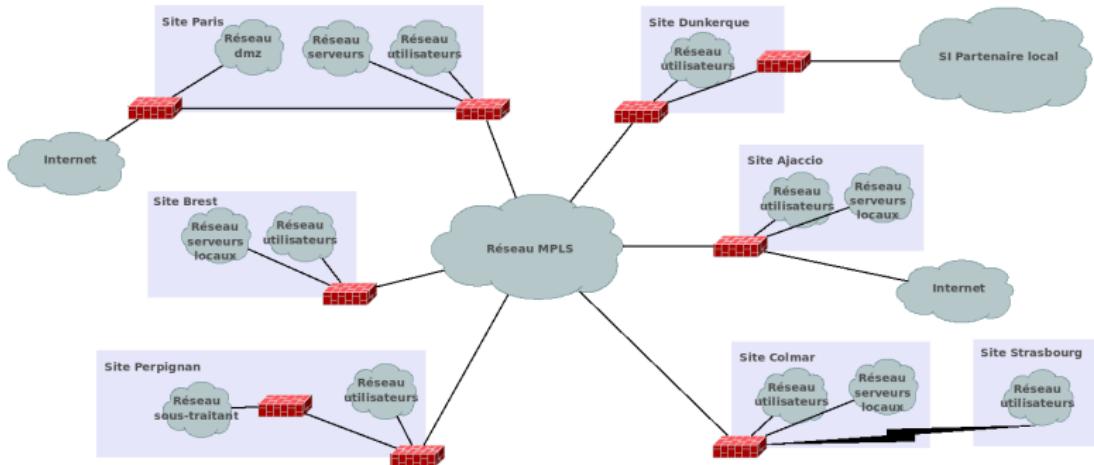


Figure – Réseau MPLS niveau 3

Exemples

Réseaux de machines virtuelles

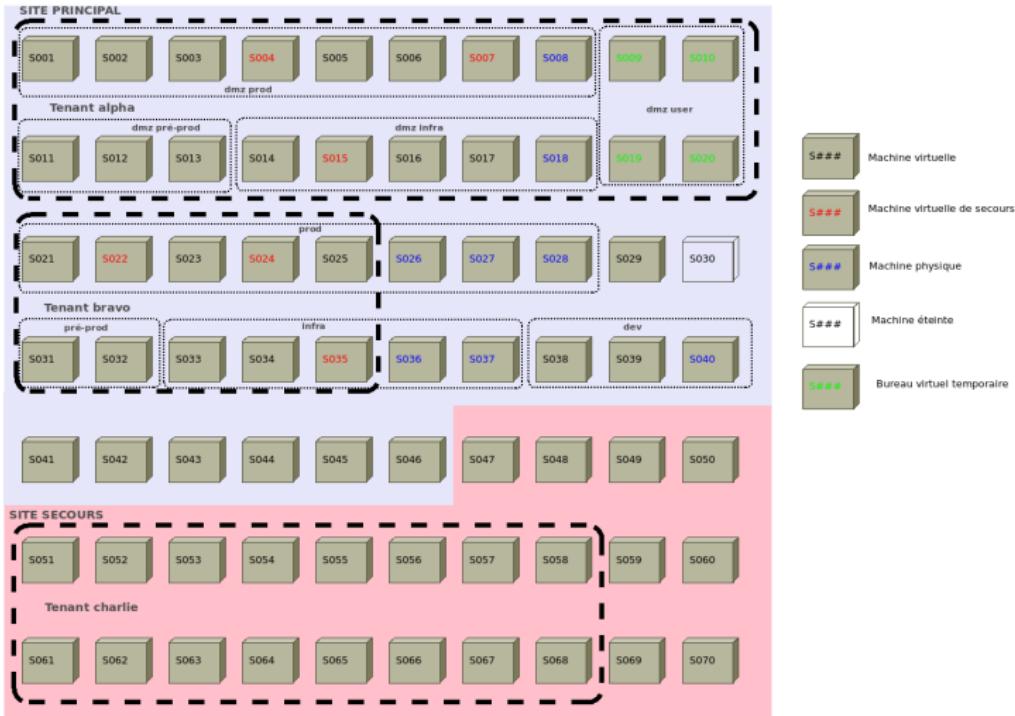


Figure – Réseau virtuel niveau 2

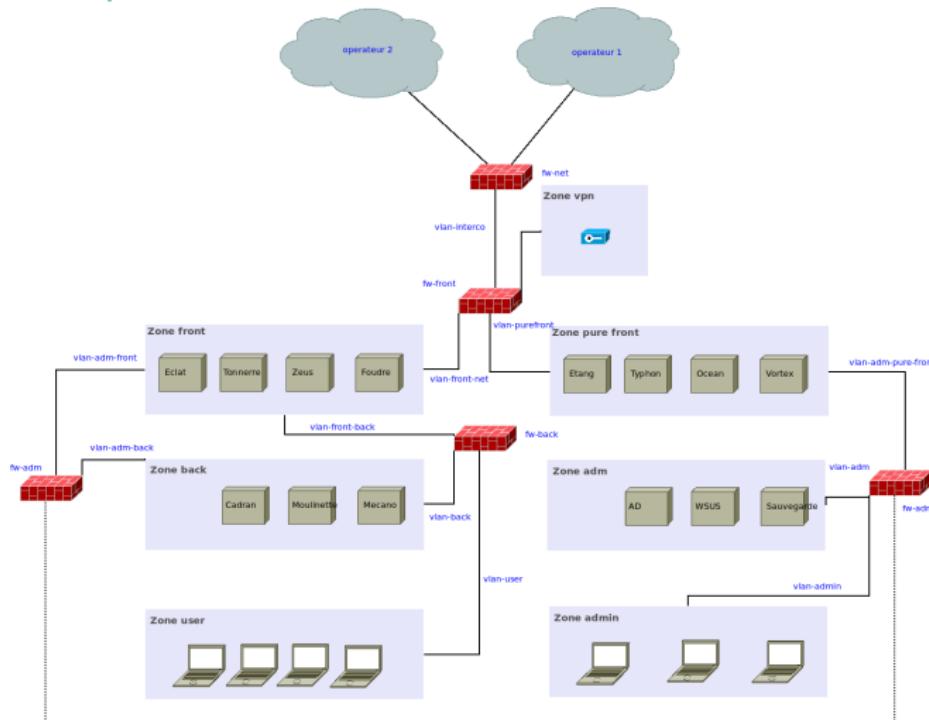


Figure – Réseau niveau 3

Niveau	1	2	3	4-7
Emplacement physique	✓			
Port physique	✓			
Equipement réseau niveau 2	✓	✓		
VLAN des interfaces		✓		
VLAN des connexions		✓	✓	
Machine virtuelle		✓		
Equipement réseau niveau 3	✓	✓	✓	
Zone		✓	✓	✓
Flux applicatif			✓	✓
Domaines et forêt AD			✓	✓
Relation inter-domaines				✓

- Niveau 4
 - Discuter le fonctionnement d'une application et sa sécurité
 - Identifier des besoins de connectivité
- Niveau 3
 - Discuter l'architecture des applications et la sécurité
 - Paramétrier les équipements de filtrage
- Niveau 2
 - Valider et mettre en œuvre l'architecture définie
 - Configurer les équipements réseau de niveau 2
 - Creuser les dysfonctionnements réseaux
- Niveau 1
 - Mettre en œuvre le niveau 2
 - Faciliter la maintenance du câblage



Chaque représentation a son usage



Multiplier les usages, c'est ajouter de la confusion



Un bon schéma doit avoir ses règles et s'y tenir

- Définir l'objectif du schéma
- Définir un vocabulaire graphique commun
 - Légende
 - Symbole constant pour des équipements équivalents
 - Jeu de couleurs, de traits et de polices
- Être patient
 - Un dessin de câblage clair prend du temps
- Être bon dessinateur

- Visio
- Dia
- Draw.io
- Inkscape
- Imprimante A3 voire supérieure
- Tableau ou paperboard
- Graphviz (cas spécifique)

Notions de réseaux

mars 2021



Hervé Schauer Sécurité



©Hervé Schauer Sécurité 2021

Wenqiang WANG

65

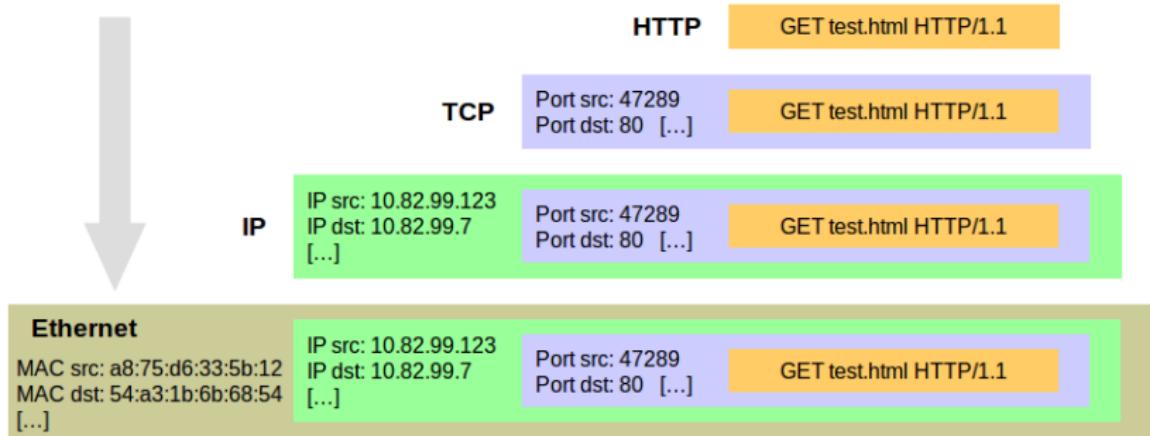
En résumé...

C'est là où on rappelle les bases de la communication entre composants informatiques et où on décrit les matériaux et alliages nécessaires à nos constructions ultérieures.

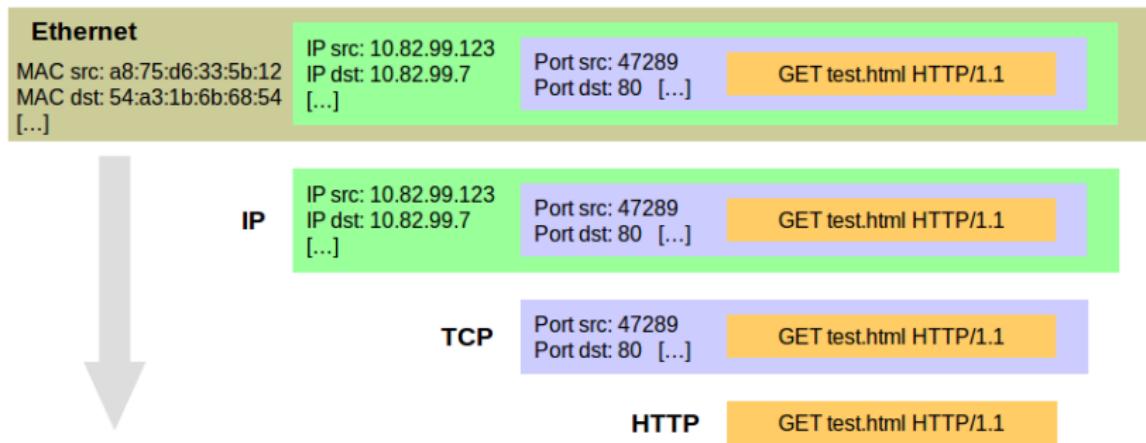
1	Modèles théoriques	67
2	Quiz introductif	71
3	Couche 2 : liaison	75
4	Couche 3 : réseau	104
5	Échanges d'informations	117
6	Composants spécifiques	124

	OSI	TCP/IP	
X.400, X.500...	7 Application		DNS, HTTP, SSH...
X.226, X.236...	6 Présentation	4 Application	MIME, Unicode...
X.225, X.235...	5 Session		NetBios, SOCKS...
X.224, X.234...	4 Transport	3 Transport	TCP, UDP, SCTP...
X.25 PLP...	3 Réseau	2 Réseau	IP, ICMP, OSPF...
X.25 LAPB...	2 Liaison		Ethernet, 802.11n, PPP, Token Ring...
X.21bis...	1 Physique	1 Liaison	10BaseT, 802.11n, RS232, CAN Bus...

Envoi : encapsulation



Réception : dé(sen)capsulation



1	Modèles théoriques	67
2	Quiz introductif	71
3	Couche 2 : liaison	75
4	Couche 3 : réseau	104
5	Échanges d'informations	117
6	Composants spécifiques	124

Que se passe-t-il quand on accède à l'URL `http://www.example.com/index.html` ?

IP source : 10.82.99.123/24

serveur DNS : 10.82.1.5, passerelle par défaut : 10.82.99.1

Note : l'adresse IP de `www.example.com` est 93.184.216.34

Ordonnez les événements suivants :

- A Envoi d'un paquet IP contenant : `GET /index.html HTTP/1.1 [...]`
- B Envoi d'un segment TCP à 93.184.216.34 : [...] `port_dst: 80, flags: SYN`
- C Création d'un datagramme UDP : `port_src: 38741, port_dst: 53 [...]`
- D Consultation de la table de routage pour 10.82.1.5
- E Fermeture de la connexion TCP
- F Réception de la réponse HTTP
- G Envoi d'une requête ARP pour connaître l'adresse MAC de 10.82.99.1
- H Réception de la réponse DNS
- I Consultation de la table de routage pour 93.184.216.34



Que se passe-t-il quand on accède à l'URL `http://www.example.com/index.html?`

IP source : 10.82.99.123/24

serveur DNS : 10.82.1.5, passerelle par défaut : 10.82.99.1

1. (L7) Une requête DNS est envoyée

`www.example.com: type A, class IN`

- a. (L4) ^C La requête est encapsulée dans un datagramme UDP
`port_src: 38741, port_dst: 53`
- b. (L3) Puis dans un paquet IP
`ip_src: 10.82.99.123, ip_dst: 10.82.1.5`
- c. (L3) ^D Consultation de la table de routage
`10.82.1.5 via 10.82.99.1 dev wlan0`
- d. (L2) ^E Une requête ARP est envoyée pour connaître l'adresse MAC de 10.82.99.1
`arp reply 10.82.99.1 is-at 64:b5:1c:43:11:89`
- e. (L2) Le paquet est encapsulé dans une trame Ethernet
`src_mac: a8:75:d6:33:5b:12, dst_mac: 64:b5:1c:43:11:89`
- f. (L1) La trame est "envoyée" sur le câble

2. ^H Une réponse DNS est reçue (en théorie)

`www.example.com: type A, class IN, addr 93.184.216.34`

3. (L7) Une requête HTTP est envoyée à 93.184.216.34

a. (L4) **B** Début de la connexion TCP

`port_src: 38878, port_dst: 80, flags: SYN`

- i. (L3) Segment encapsulé dans un paquet IP
- ii. (L3) **T** Consultation de la table de routage
- iii. (L2) Consultation du cache arp pour obtenir l'adresse MAC de 10.82.99.1
- iv. (L2) Le paquet est encapsulé dans une trame Ethernet
- v. (L1) La trame est "envoyée" sur le câble

b. (L4) Réception d'un segment SYN/ACK

c. (L4) Envoi d'un segment ACK

⇒ Connexion établie

d. (L4) **A** Envoi d'un segment PSH/ACK avec la requête HTTP

`GET /index.html HTTP/1.1 [...]`

e. (L4) Fermeture de la connexion TCP (côté client)

f. (L4) **F** Réception de la réponse HTTP

`HTTP/1.1 200 OK [...]`

g. (L4) **E** Fermeture de la connexion TCP

⇒ Connexion terminée

4. Affichage de la page par le navigateur (enfin...)

Bonus : citez **toutes les attaques possibles** aux différentes étapes de cet échange

1	Modèles théoriques	67
2	Quiz introductif	71
3	Couche 2 : liaison	75
4	Couche 3 : réseau	104
5	Échanges d'informations	117
6	Composants spécifiques	124

3 Couche 2 : liaison

Réseau local

Composants de base

Adressage

Segmentation

Sécuriser le lien local

75

76

79

81

84

92

Domaine de collision

Ensemble d'entités qui partagent un même medium de communication (niveau 1).

Domaine de diffusion

Ensemble d'entités pouvant communiquer sans routage (niveau 2).

Domaine de collision / domaine de diffusion

Illustration

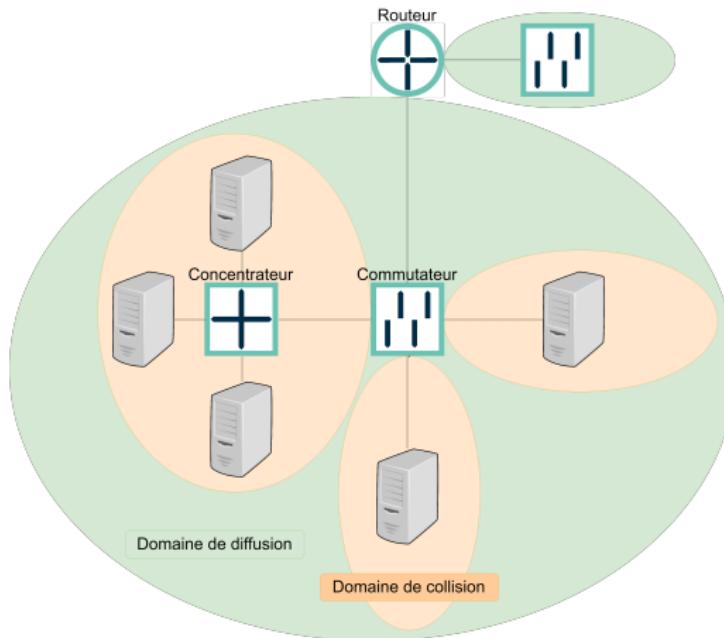


Figure – Domaines de collision et de diffusion

3 Couche 2 : liaison	75
Réseau local	76
Composants de base	79
Adressage	81
Segmentation	84
Sécuriser le lien local	92



- Équipements de niveau 2 : LAN
 - ARP (*Address Resolution Protocol*)
 - Proches des feuilles (postes de travail, serveurs)
- Commutateur (*switch*) : mise en liaison un à un
 - Une trame = une interface en sortie
 - Certes, plusieurs interfaces pour un message de broadcast.
 - Déclaration de VLAN (*Virtual Local Area Network*)
- Concentrateur (*hub*) : broadcast systématique
 - Une trame = toutes les interfaces en sortie



Tables ARP pleines

3 Couche 2 : liaison

Réseau local

Composants de base

Adressage

Segmentation

Sécuriser le lien local

75

76

79

81

84

92

- L'adressage dépend du protocole
- Pour Ethernet : **adresse MAC (Media Access Control)^a**
 - Adresse sur 48 bit (6 octets)
 - Unique pour chaque équipement / interface
 - Mais modifiable très facilement
 - Composée de
 - L'OUI (Organizational Unique Identifier)¹ sur 3 octets
 - L'identifiant de l'équipement sur 3 octets

F4:EA:67:5A:42:10

OUI: Cisco Systems, Inc.

Identifiant de l'équipement
(i.e. de l'interface réseau)

1. Pour connaître l'OUI d'une adresse MAC : <http://hwaddress.com>

- Comment savoir quelle est l'adresse MAC du prochain noeud ?

⇒ ARP (Address Resolution Protocol) (RFC 826^b)

- À cheval entre couches 2 (selon TCP/IP) et 3 (selon OSI)
- Principe :
 - Hurler : "Qui dans la salle a l'adresse IP 10.82.99.7?"
 - Attendre une adresse MAC en réponse

```
# tcpdump -ennqti any
a8:75:d6:33:5b:12  ff:ff:ff:ff:ff:ff  42: arp who-has 10.82.99.7 tell 10.82.99.123
54:a3:1b:6b:68:54  a8:75:d6:33:5b:12  60: arp reply 10.82.99.7 is-at 54:a3:1b:6b:68:54
```

```
# arp -n
Address      HWtype  HWaddress          ...  Iface
10.82.99.7    ether    54:a3:1b:6b:68:54    eth0
192.168.0.1   ether    28:2c:b2:5c:c0:98    wlan0
[...]
```

Note : ARP est remplacé par NDP (Neighbour Discovery Protocol) en IPv6

3 Couche 2 : liaison	75
Réseau local	76
Composants de base	79
Adressage	81
Segmentation	84
Sécuriser le lien local	92

- Standard IEEE **802.1Q** ^c
 - Une manière de mettre en œuvre des VLAN
- Objectif : créer plusieurs réseaux indépendants partageant les mêmes câbles/équipements
 - Réduit la taille du domaine de diffusion
 - Gestion des flux facilitée
 - Création de différentes zones réseaux
 - Contrôle d'accès par des goulots d'étranglement (pare-feu)

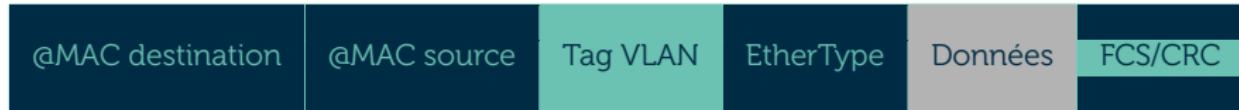


Table – Trame Ethernet avec champs VLAN (fond bleu clair)

VLAN (Virtual Local Area Network)

Principes

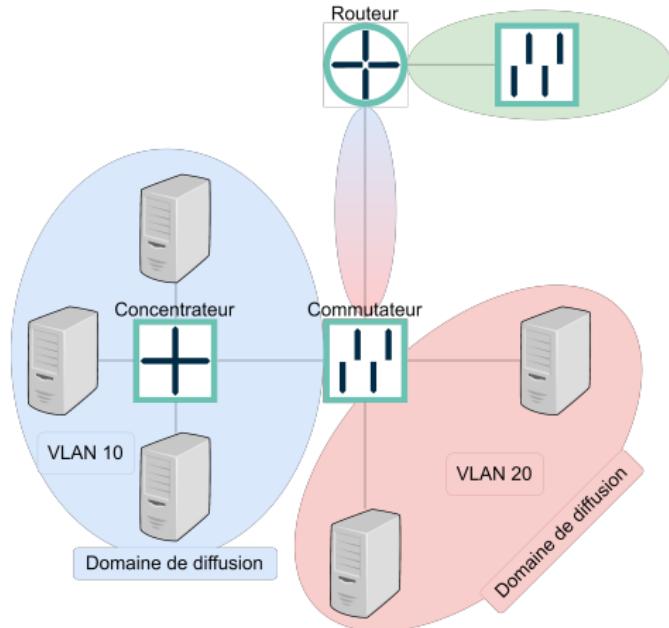


Figure – VLAN : principe

- Configuration statique
 - Basée sur l'interface du commutateur (*tagged/untagged*²)
- Configuration dynamique
 - Par adresse MAC / IP (**très mauvaise pratique**)
 - Après authentification 802.1X (point abordé ultérieurement)
 - Par protocole propriétaire
 - VTP (VLAN Trunking Protocol)
 - Propagation de la configuration entre commutateurs
 - DTP (Dynamic Trunking Protocol)
 - Activation du mode *trunk* d'un port

2. Cisco emploie respectivement les termes *trunk port* et *access port*



- Routage inter-VLAN
- Séparation logique (et non physique) :
 - Saut de VLAN (*VLAN hopping*)
 - Double encapsulation 802.1q
 - Émulation d'un commutateur via DTP (*Dynamic Trunking Protocol*)
 - Reconfiguration via VTP (VLAN Trunking Protocol)
 - Attaquant branché sur un port tagged
 - "Authentification" par adresse MAC / adresse IP



- Désactiver le VLAN *natif* (VLAN "par défaut" - VLAN ID 1)
- Désactiver DTP (*Dynamic Trunking Protocol*)
 - switchport nonegotiate
- Authentifier VTP (VLAN Trunking Protocol)
 - vtp password AXm5vRtt8xZnsSmuUcWCFn2f
- Protéger les interfaces *tagged*
 - Sécurité physique
 - Segmentation
 - Administration *out-of-band*
 - Etc.

- Mesure d'isolation très efficace
 - Un VLAN primaire (porté par une interface tagged) est divisé en VLAN secondaires
 - "Sous-domaines de diffusion"
 - Mode **isolé** ou mode **communauté**
- Les hôtes d'un même VLAN ne peuvent plus communiquer entre eux
 - Envoi des trames vers le port *trunk*
 - Décision de filtrage par un routeur ou pare-feu
- L'attaquant ne peut plus rebondir!



- VACL (VLAN Access Control Lists)
- *switchport protected*
 - Défini au niveau *interface*
 - Un port *protected* ne peut pas transmettre de paquets à un autre port *protected*

- RFC 7348^d
- Objectif : segmentation par VLAN au-delà du domaine de diffusion
 - Encapsulation de trames Ethernet dans UDP (UDP 4789)

		@MAC dst VXLAN	@MAC src VXLAN	Tag VLAN VXLAN	IP VXLAN	UDP	...
VXLAN ID	-	@MAC dst	@MAC src	Tag VLAN	IP	TCP / UDP	...
Données							

Table – Trame Ethernet avec encapsulation VXLAN (texte en blanc)



Fragmentation

3 Couche 2 : liaison

Réseau local

Composants de base

Adressage

Segmentation

Sécuriser le lien local

75

76

79

81

84

92

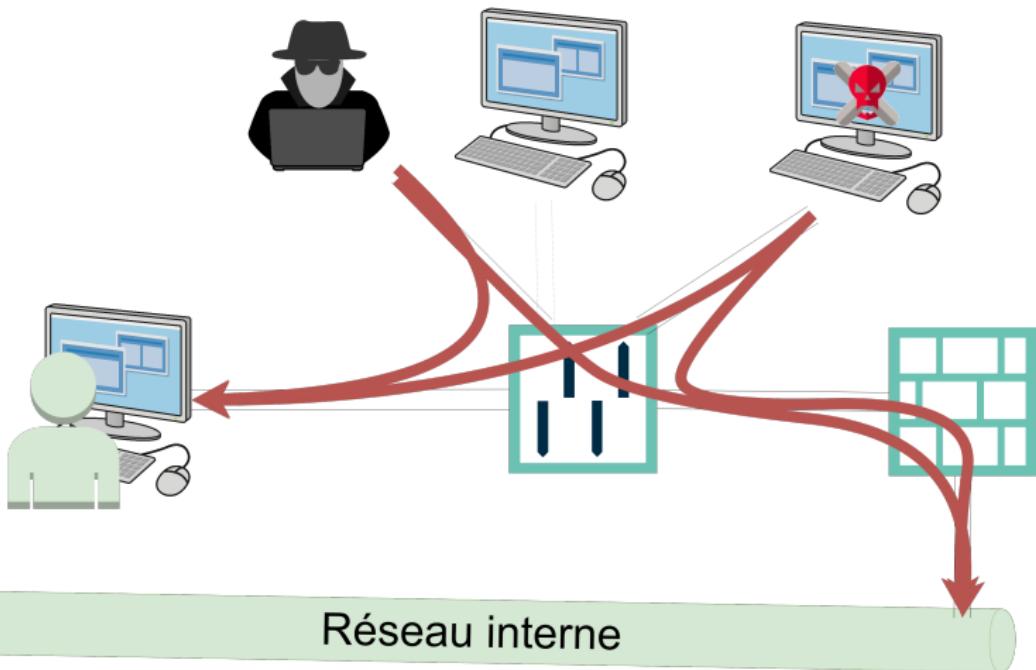
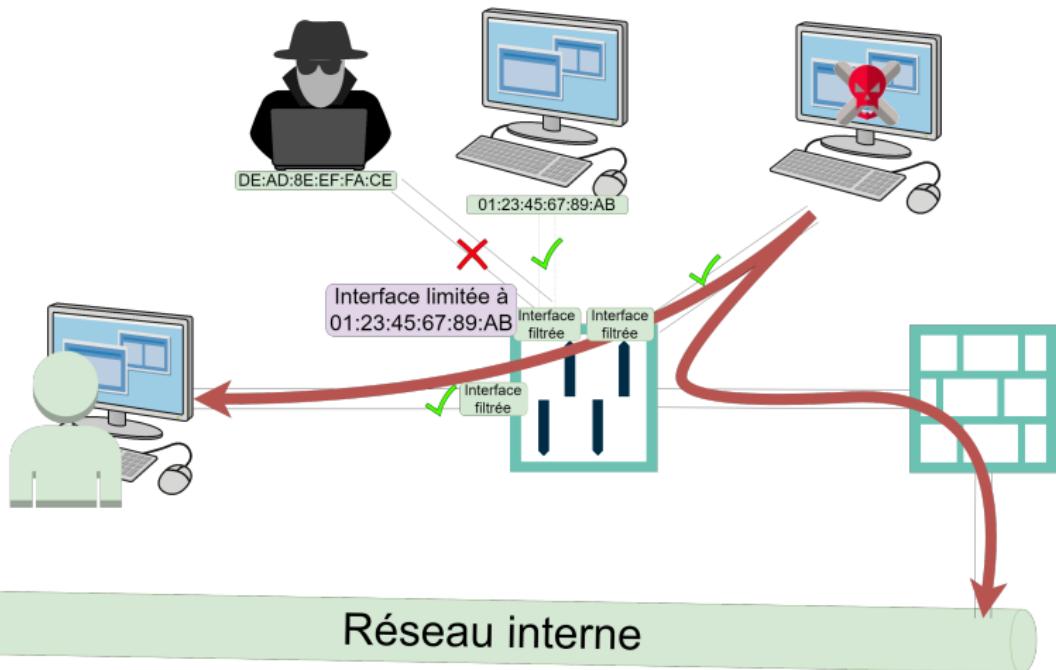


Figure – Les problématiques de sécurité du lien local



Réseau interne

Figure – Port security

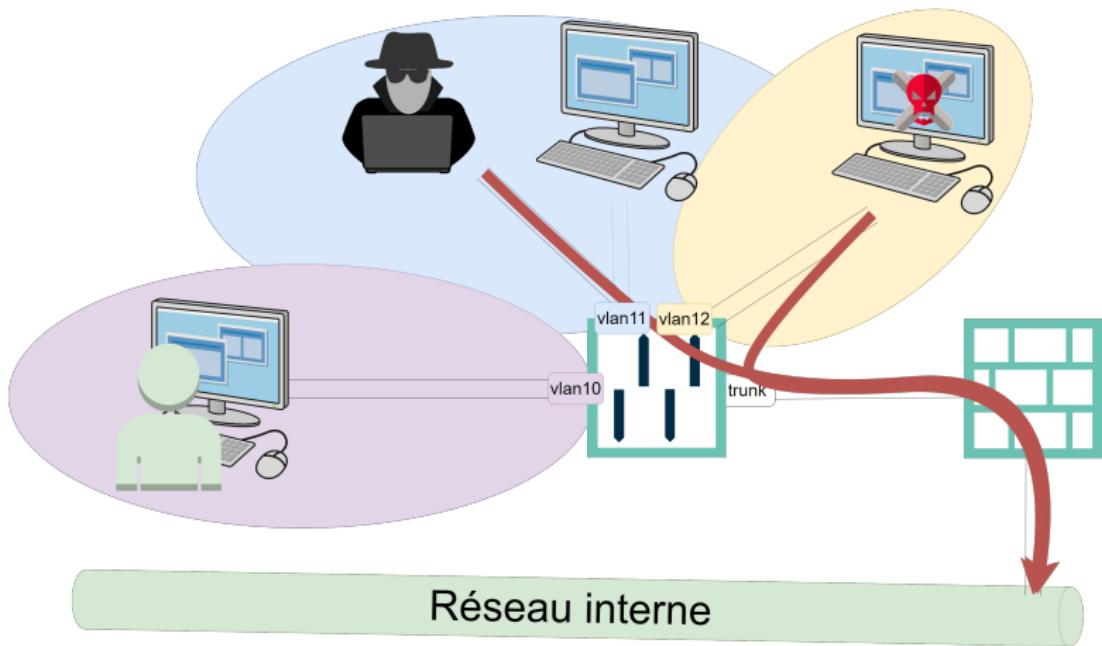


Figure – VLAN par port

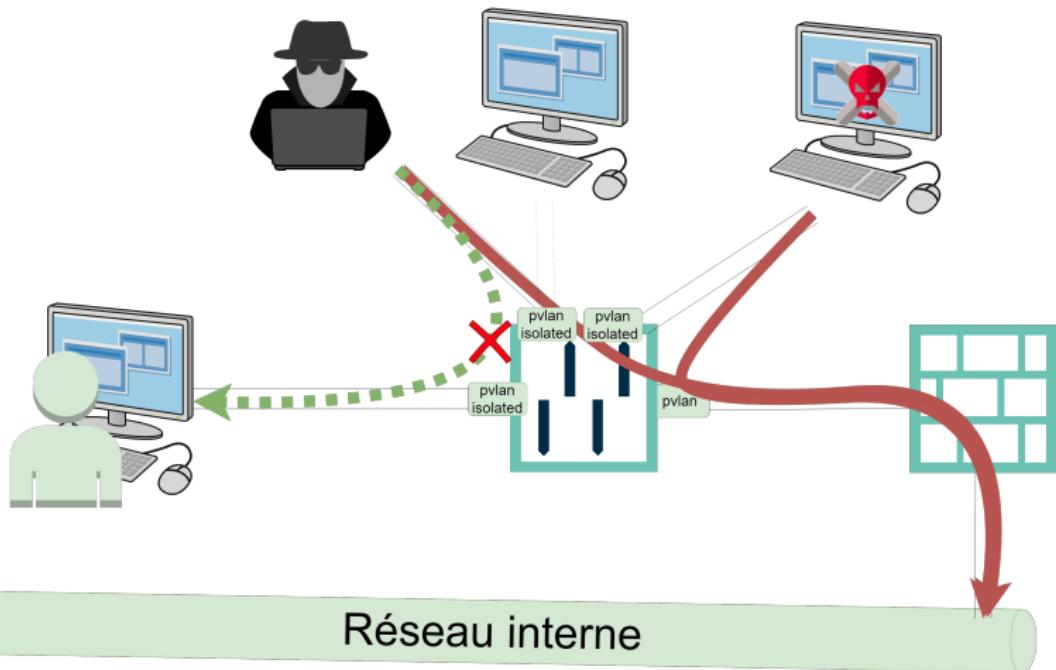
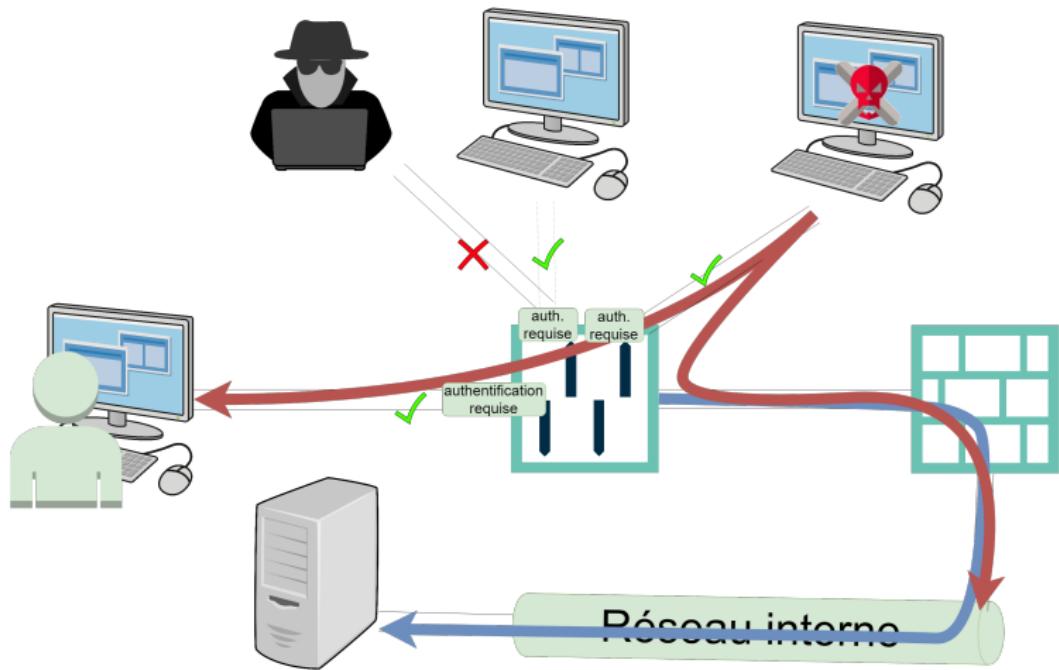


Figure – Private VLAN en mode isolated



Serveur d'authentification

Figure – 802.1X

Sécuriser le lien local

Tables ARP statiques

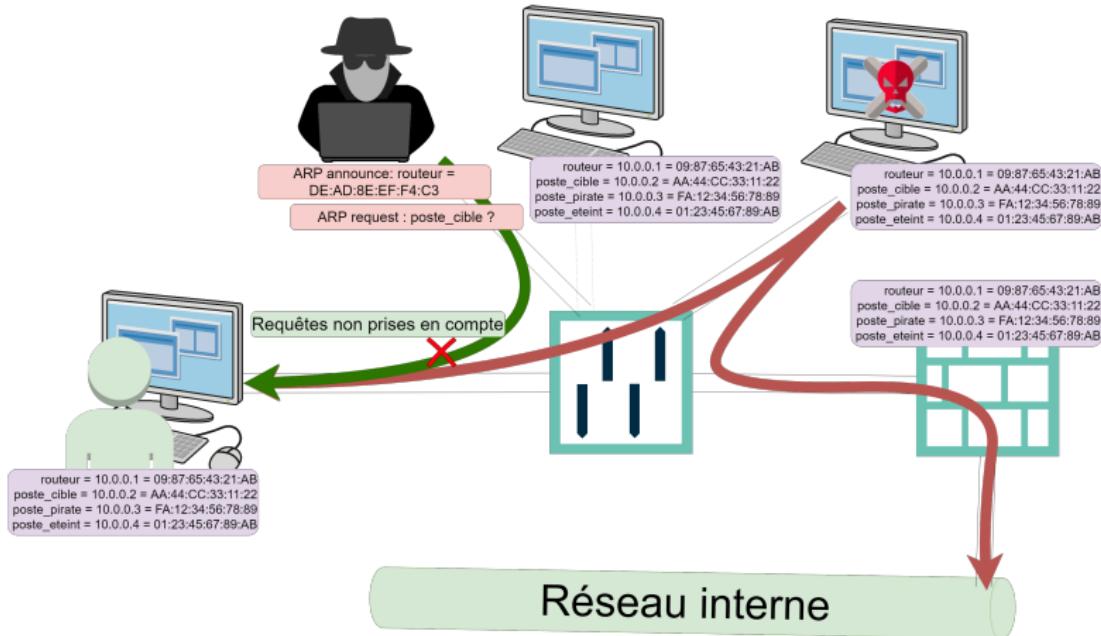


Figure – Tables ARP statiques

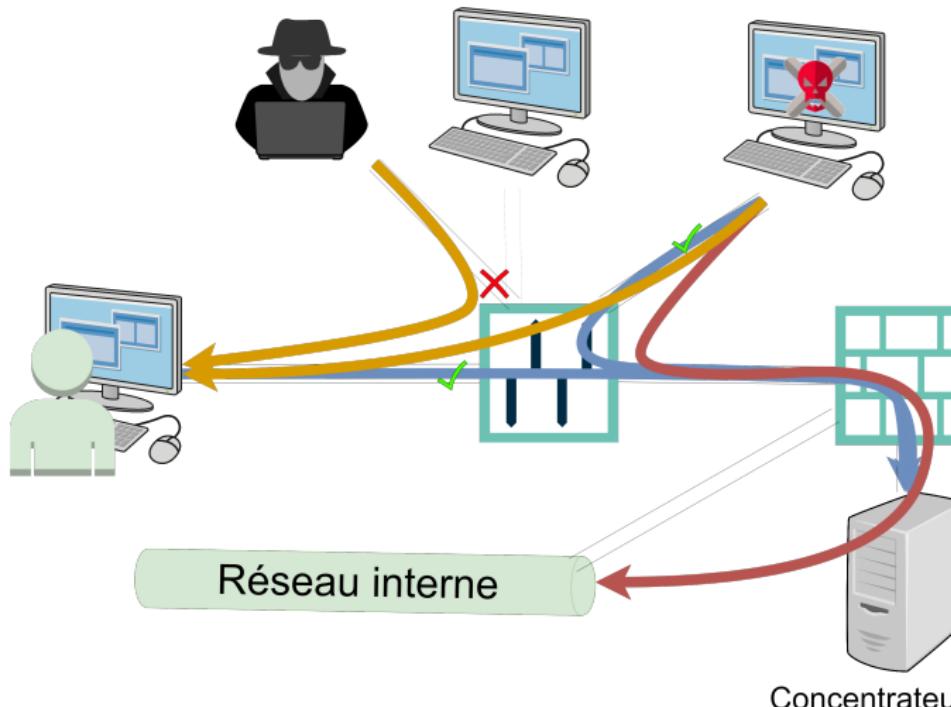


Figure – VPN

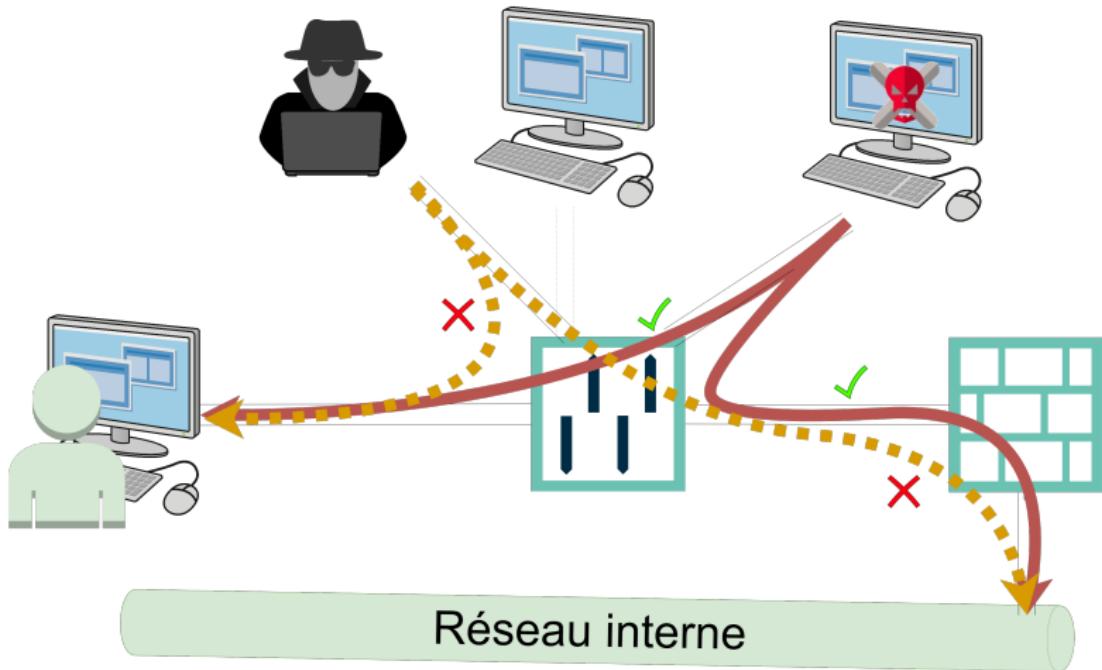


Figure – IPSec systématique

Poste Cible	Externe au SI		Du SI	
	Lien local	Réseau interne	Lien local	Réseau interne
Aucune	Ouvert	Filtré	Ouvert	Filtré
Port security	Ouvert / Bloqué	Filtré	Ouvert	Filtré
VLAN par port	Bloqué	Filtré	Filtré	Filtré
PVLAN isolated	Bloqué	Filtré	Filtré	Filtré
802.1X	Bloqué	Bloqué	Ouvert / réduit	Filtré
Tables ARP répliquées	Écoute requise	Écoute requise	Ouvert	Filtré
Tables ARP statiques réduites	Écoute requise	Écoute requise	Limité	Filtré
VPN	Très limité	Bloqué	Très limité	Filtré
IPSec syst.	Très limité	Filtré	Ouvert	Filtré

Solution	Chiffré	Complexité
Aucune	Non	Aucune
Port security	Non	Gestion des commutateurs
VLAN par port	Non	Paramétrage commutateurs
PVLAN isolated	Non	Paramétrage commutateurs
802.1X	Non	Gestion des certificats et paramétrage commutateurs
802.1X + MACsec	Oui	Gestion des certificats et paramétrage commutateurs
Tables ARP répliquées	Non	Collecte et propagation des adresses MAC
Tables ARP statiques réduites	Non	Collecte, triage et propagation des adresses MAC
VPN	Oui	Gestion des certificats et paramétrage des postes
IPSec syst.	Oui	Gestion des certificats et paramétrage des postes



- Segmentez
 - = diviser les domaines de collision/diffusion
- Remplacez tous les concentrateurs par des commutateurs
- Si VLAN il y a :
 - N'utilisez pas le VLAN ID '1'
 - Désactivez/configurez DTP, VTP et le VLAN natif
- Sécurisez les liens locaux
 - *port security < 802.1X < PVLAN en mode isolé*

1	Modèles théoriques	67
2	Quiz introductif	71
3	Couche 2 : liaison	75
4	Couche 3 : réseau	104
5	Échanges d'informations	117
6	Composants spécifiques	124

4 Couche 3 : réseau	104
Composants de base	105
Adressage	108
Segmentation	115



- Équipements de niveau 3
 - IP (*Internet Protocol*)
 - Cœurs de réseaux
- Un paquet = un chemin, une interface en sortie
- Idée du pare-feu : filtrer les flux
 - Par adresse IP source/destination (niveau 3)
 - Par adresse MAC source/destination (niveau 2)
 - Par protocole et port (niveau 4)
 - [...]
 - Par une association de plusieurs de ces éléments
 - **ACL (Access Control List)**



`any src | any dst | any [0-65535] | allow`



- Objectifs multiples : redondance, performance, etc.
 - Disponibilité
- Essentiel : associé à du NAT (*Network Address Translation*)
 - Présentation d'adresses IP virtuelles (VIP)
- Souvent associé à d'autres fonctionnalités (niveau 3+)
 - Pare-feu
 - Relais applicatif
 - Pare-feu applicatif (WAF)
 - Relais de terminaison TLS
 - [...]



SPOF (*Single Point Of Failure*)

4 Couche 3 : réseau	104
Composants de base	105
Adressage	108
Segmentation	115

- Pour désigner un hôte, il faut une **adresse** (32 bit) et un **préfixe**

Adresse IP	10	.	82	.	99	.	7	I 24
Bit	1 2 3 4 5 6 7 8	9 10 11 12 13 14 15 16	17 18 19 20 21 22 23 24	25 26 27 28 29 30 31 32				(Préfixe)
Masque réseau	255	.	255	.	255	.	0	
	1 1 1 1 1 1 1 1 1	.	1 1 1 1 1 1 1 1 1	.	1 1 1 1 1 1 1 1 1	.	0 0 0 0 0 0 0 0 0	
Adresse du réseau	10	.	82	.	99	.	0	
Adresse de diffusion	10	.	82	.	99	.	255	

- Ex : 198.51.100.99/21

```
$ ipcalc 198.51.100.99/21
Address: 198.51.100.99          11000110.00110011.01100 100.01100011
Netmask: 255.255.248.0 = 21    11111111.11111111.11111 000.00000000
Wildcard: 0.0.7.255            00000000.00000000.00000 111.11111111
=>
Network: 198.51.96.0/21        11000110.00110011.01100 000.00000000
HostMin: 198.51.96.1           11000110.00110011.01100 000.00000001
HostMax: 198.51.103.254         11000110.00110011.01100 111.11111110
Broadcast: 198.51.103.255       11000110.00110011.01100 111.11111111
Hosts/Net: 2046                  Class C
```

- Même principe, mais sur 128 bits³
 - 8 groupes de 2 octets
 - Notation hexadécimale (ex : 10 = 0x0a, 255 = 0xff...)
- Exemple :
fe80:0000:0000:0000:a875:d6ff:fe33:5b12/64
- Notation abrégée
On remplace **un groupe** de "0" consécutifs par " ::"
⇒ fe80::a875:d6ff:fe33:5b12/64

3. Soit 340 milliards de milliards de milliards de milliards d'adresses possibles

Certaines adresses ont un usage spécifique

- **Adresses de bouclage *loopback*** : 127.0.0.0/8
 - Identifient l'interface locale (l'équipement vers lui-même)
- **Adresses *multicast*** : 224.0.0.0/4 (224.0.0.0 - 239.255.255.255)
 - Utilisées pour les communications de groupe
 - Duplication des paquets seulement si nécessaire
- **Adresses auto-configurées** : 169.254.0.0/16
 - Valables uniquement sur le segment réseau
 - Parfois assignées quand aucune adresse n'est configurée
- **Adresses de documentation** (RFC 5737 et 3849)
192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24
 - Pour éviter de pointer vers des systèmes existants

- Adresses à connaître : les **adresses IP privées** (RFC 1918)
 - Classe A : 10.0.0.0/8 (10.0.0.0 - 10.255.255.255)
 - Classe B : 172.16.0.0/12 (172.16.0.0 - 172.31.255.255)
 - Classe C : 192.168.0.0/16 (192.168.0.0 - 192.168.255.255)
- Valables seulement sur le **réseau local**
 - Inutilisables sur Internet : elles ne sont pas routables
 - Comment communiquer avec d'autres réseaux ?

Traduction d'adresse

NAT (Network Address Translation)

- SNAT (Source NAT) pour communiquer vers l'extérieur
- DNAT (Destination NAT) ou PAT (Port Address Translation) pour être joint *depuis* l'extérieur



Attention à ne pas oublier les deux adresses en IPv6

- link-local
- adresse globale



Éviter d'affecter IPv4 et IPv6 aux serveurs. Il faut choisir !

- Utilisation d'une double pile
- Utilisation d'une infrastructure de conversion
- nat64 et dns64

4 Couche 3 : réseau	104
Composants de base	105
Adressage	108
Segmentation	115

- Objectif : instancier des routeurs "virtuels"
 - Co-existence de plusieurs tables de routage sur un même routeur
 - Chaque interface (physique ou logique) appartient à un unique VRF
- Segmentation logique à tous les niveaux



Le VRF est au niveau 3 ce que le VLAN est au niveau 2!



Saut de VRF (*VRF hopping*)^{e f}

1	Modèles théoriques	67
2	Quiz introductif	71
3	Couche 2 : liaison	75
4	Couche 3 : réseau	104
5	Échanges d'informations	117
6	Composants spécifiques	124

	OSI	TCP/IP	
X.400, X.500...	7 Application		DNS, HTTP, SSH...
X.226, X.236...	6 Présentation	4 Application	MIME, Unicode...
X.225, X.235...	5 Session		NetBios, SOCKS...
X.224, X.234...	4 Transport	3 Transport	TCP, UDP, SCTP...
X.25 PLP...	3 Réseau	2 Réseau	IP, ICMP, OSPF...
X.25 LAPB...	2 Liaison		Ethernet, 802.11n, PPP, Token Ring...
X.21bis...	1 Physique	1 Liaison	10BaseT, 802.11n, RS232, CAN Bus...



Complexité à transférer les informations de contexte
d'un niveau au suivant

- Le correspondant IPSec
- L'adresse IP source

Exemple en IP sur Ethernet :

- Le minimum :
 - Une adresse MAC
 - L'adresse IP de la machine
 - Et son masque de sous-réseau (ou préfixe)
- Pour communiquer avec d'autres réseaux :
 - Une passerelle par défaut (*default gateway*)
- Et dans la vraie vie :
 - Serveur de résolution de noms
 - Etc.

statique les informations sont saisies manuellement

piloté un serveur central fournit les informations nécessaires

négocié les composants s'échangent les informations entre eux

Composant	Piloté	Négocié
Adresse MAC	N/A	ARP
Adresse IP	DHCPv4	Bonjour / AVAHI
Routeur de sortie	DHCPv4	<i>ICMP</i>
Serveur de nom (DNS)	DHCPv4	N/A
Noms de domaines	DNS, NetBios	mDNS, LLMNR

Table – Obtention des informations avec la pile IPv4

Composant	Piloté	Négocié
Adresse MAC	N/A	NDP
Adresse IP	DHCPv6	NDP
Routeur de sortie	DHCPv6	NDP
Serveur de nom (DNS)	DHCPv6	N/A
Noms de domaines	DNS, NetBios	mDNS, LLMNR

Table – Obtention des informations avec la pile IPv6

1	Modèles théoriques	67
2	Quiz introductif	71
3	Couche 2 : liaison	75
4	Couche 3 : réseau	104
5	Échanges d'informations	117
6	Composants spécifiques	124



- Architecture : mêmes risques, mêmes mesures
 - Espionnage (C) - Chiffrement
 - Interception (I) - Authentification sur le réseau (WPA2 / 802.1X)
 - Déni de service (D) - Redondance
- Sécurité physique : risques similaires
 - Protection des équipements, des interfaces physiques, etc.



Exclusivité du sans-fil

- Support non localisé : périmètre d'interception plus important

- Cas général : sans-fil uniquement en bordure

- Architecture réseau/système :
≈ mêmes risques, ≈ mêmes mesures
 - ... pour les composants virtuels



Exclusivité de la virtualisation

- Segmentation entre composants virtuels
- Administration des hyperviseurs
- Composants de gestion centralisée
- ...

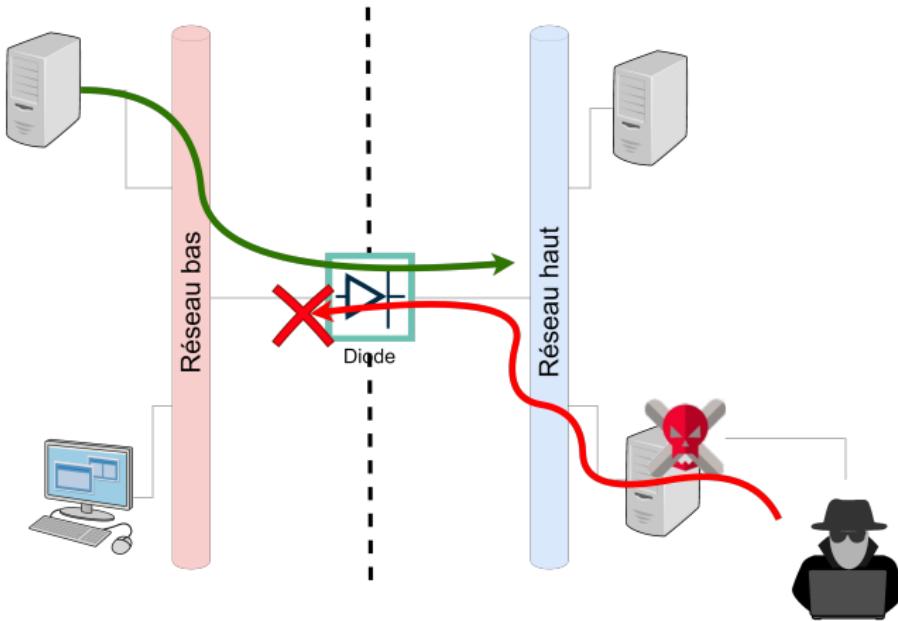


Figure – Diode réseau : principe

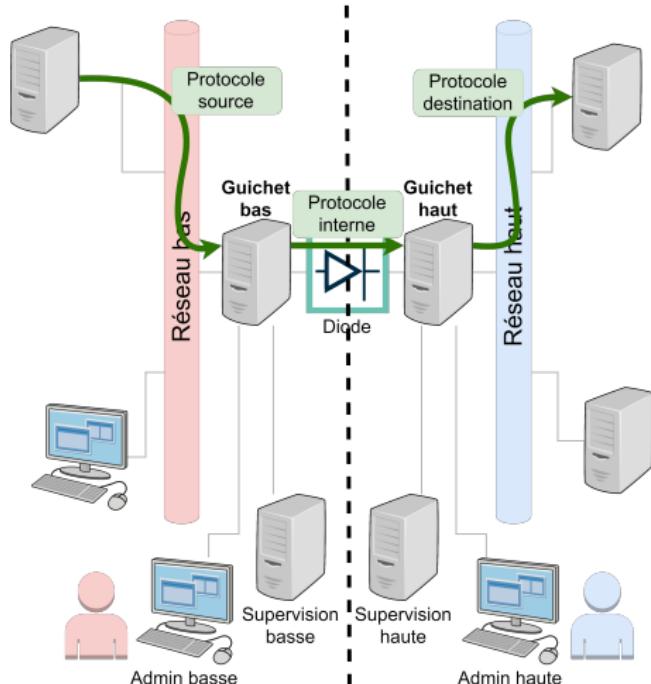


Figure – Diode réseau : mise en œuvre



1. Perte d'information ou perte de la liaison

- Supervision des flux (au niveau du guichet haut)
 - Détection des pertes
 - Statistiques
 - Protocoles
- Supervision de la liaison
 - *Heartbeat* entre les guichets, de bas en haut



2. Perte d'intégrité et infection virale

- Filtrage des flux
 - Antivirus
 - Vérification de formats
 - Vérification de signatures
 - Liste noire/blanche de contenu
 - Liste noire/blanche de source(s)/destination(s)



3. Protocoles sérialisables uniquement

- Dépôt de fichiers (SCP, SFTP, NFS, etc.)
- Protocoles asynchrones (SMTP, MQ, etc.)
- Relais (bas) / Rejeu (haut) TCP

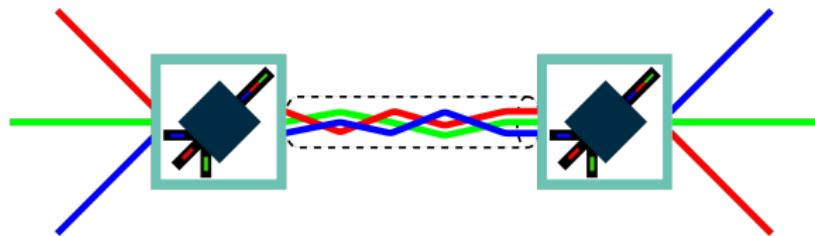
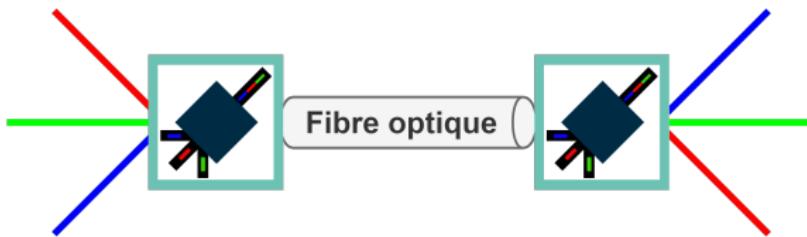


Figure – Multiplexage de longueurs d'onde : principe



Globalement les mêmes problématiques qu'un commutateur



Avec des avantages supplémentaires

- Equipement passif qui ne pilote que de l'optique
 - Reste fonctionnel sans électricité
- Ne devrait pas être piratable depuis la fibre



- Composants logiciels et/ou matériels de capture
 - De flux / de comportements
- Exemples :
 - Tap ou TAP (Test/Terminal Access Point) réseau
 - Sonde Netflow
 - Sonde IDS/IPS
 - Réseau : NIDS/NIPS et WIDS⁴/WIPS
 - Local : HIDS/HIPS/EDR
- Capture partielle ou complète
 - Que veut-on détecter ?
 - Que peut-on détecter ?
 - Volume de capture, capacité de traitement

4. Wireless Intrusion Detection System

- Equipement passif
 - Le trafic passe quoi qu'il arrive
 - Pas d'impact sur la performance
- Avantages
 - Idéal pour les gros volumes
 - Capture tout ce qui passe (y compris les erreurs de bas niveau)
 - *Full Packet Capture*
- Inconvénients
 - Sur un seul lien (contrairement à un SPAN)
 - Cher

- Informations sur les flux IP
 - IP source / destination
 - Protocole de transport utilisé
 - Ports source / destination
 - Volume échangé, etc.
- Source
 - Routeurs, commutateurs, boitiers NPM (Network Performance Monitor)...
 - Equipements Netflow dédiés sur port SPAN⁵ ou Tap
- Exporté vers un collecteur central (UDP ou SCTP⁶)

5. Switched Port Analyzer

6. Stream Control Transmission Protocol

7. IP Flow Information Export

- Détection

- Basé sur les signatures
- Ou l'analyse comportementale (*behavior based*)
 - Apprentissage du fonctionnement normal du système (*baseline*)
 - Puis alerte si comportement considéré malveillant, basé sur
 - L'intégrité des fichiers
 - Les accès des processus
 - Les connexions réseaux
 - [...]

- Prévention

- Idem
- + Blocage du comportement (e.g. arrêt du processus)

- Détection

- Capture et centralisation de flux
- Alerte si flux détecté comme malveillant, basé sur
 - Les sources / destinations (MAC / IP / noms de domaines)
 - Le contenu des paquets (basé sur des signatures - *regexp*)
 - Des caractéristiques trop éloignées de la *baseline*
 - Volume, protocoles...
 - [...]

- Prévention

- Idem
- + Filtrage du flux
- Configuration beaucoup moins "agressive" (faux positif = DoS)

- Méthode de capture
 - NIPS : En coupure
 - NIDS :
 - Port miroir (SPAN) : facile mais perte de paquets probable
 - Sur un TAP
- Placement des sondes
 - Externe : inutile (sauf pour la recherche)
 - Parapluie : beaucoup de trafic
 - Bureautique : détection facilitée des rebonds
 - Près des systèmes critiques : peu d'alertes, mais de qualité

- *Host-based*

 Avantages

- efficacité large (flux, processus, etc.)
- transparent pour le réseau

 Inconvénients

- apprentissage long, coûteux, risqué (apprentissage sur système infecté...)
- coûteux en termes de ressources (*overhead*)
- difficile à déployer sur l'ensemble d'un SI
- mise à jour difficile
- systèmes spécifiques = logiciels spécifiques

- *Network-based*

 Avantages

- invisible par l'attaquant

 Inconvénients

- nombreux faux-positifs
- SPOF (*Single Point Of Failure*) (si placé en interception)
- pas d'analyse des flux chiffrés

- Prévention

 Avantages

- empêche les comportements malveillants

 Inconvénients

- impacte potentiellement les performances
- peut provoquer un déni de service

Flux

mars 2021



Hervé Schauer Sécurité



En résumé...

C'est là où on l'on regarde ce qui circule dans les tuyaux.

1 Filtrage

143

2 Modes de connexion

154

3 Chiffrement

177

- Niveau 2
 - Interface d'entrée et/ou de sortie
- Niveau 3
 - Plage d'adresses IP source et/ou destination
- Niveau 4
 - Protocole applicatif
 - Port source et/ou destination en TCP, UDP et SCTP
- Niveau 7
 - URL ou domaine de destination en HTTP
 - UUID du backend sollicité en RPC



- Ouverture d'une connexion dans l'autre direction
- Ouverture de connexions avec des ports dynamiques
 - FTP
 - RPC
 - 1024-65535 pour Windows 2000-2003
 - 49152-65535 pour Windows 2008+
 - SIP
 - RTSP



- Utiliser des pare-feu gérant ces cas avec de l'inspection de trafic
- Réduire les ports utilisés par ces protocoles

- Définir la clef :

[HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet]

- Ajouter les valeurs suivantes :

Valeur	Type	Contenu
Ports	MULTI_SZ	5000-5100
PortsInternetAvailable	REG_SZ	Y
UseInternetPorts	REG_SZ	Y

Service	Clef	Valeur	Type	Contenu
AD replication	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters]	TCP/IP Port	DWORD	6000
File Replication Service	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTFRS\Parameters]	RPC TCP/IP Port Assignment	DWORD	6001
Distributed File Services Replication Service	<code>dfsrdiag StaticRPC /port: 6002 /Member: target.example.tld</code>			

Nom standard	Nom	Requis	UUID
AD Replication	MS NT Directory DRS Interface	✓	E3514235-4B06-11D1-AB04-00C04FC2DCD2
Outlook address book	MS NT Directory NSP Interface		F5CC5A18-4264-101A-8C59-08002B2F8426
Local Security Authority	LSA RPC	✓	12345778-1234-ABCD-EF00-0123456789AB
Remote logon	Netlogon	✓	12345678-1234-ABCD-EF00-01234567CFFB
Security Accounts Managers	SAM RPC	✓	12345778-1234-ABCD-EF00-0123456789AC

Nom standard	Nom	Requis	UUID
AD Backup	NTDS Backup Interface		ECEC0D70-A603-11D0-96B1-00A0C91ECE30
AD Restore	NTDS Restore Interface		16E0CF3A-A604-11D0-96B1-00A0C91ECE30
FRS Replication	File Replication Service	✓	F5CC59B4-4264-101A-8C59-08002B2F8426
FRS Administration	File Replication API	✓	D049B186-814F-11D1-9A3C-00C04FC9B232
DFS-R Interface	DFS Replication Service	✓	897E2E5F-93F3-4376-9C9C-FD2277495C27

Définir la politique de filtrage sachant que

- La R&D est un réseau contenant les données les plus sensibles de l'organisation
- Tout flux avec Internet devrait passer par une DMZ
- Il y a toujours des exceptions avec des anciennes applications ou des contrats de télémaintenance avec une partie des outils utilisés par les commerciaux

Exemple de politique :

- Flux interdits
- Flux précis autorisés
- Flux précis autorisés après validation du RSSI
- Flux autorisés si encapsulés dans un tunnel



De \ Vers	Interne	R&D	DMZ In	DMZ Out	Internet
Interne					
R&D					
DMZ In					
DMZ Out					
Internet					





- Définir une logique et s'y tenir
- Éviter les alternances de règles allow et deny sans logique

1. Listes noires globales
2. Autorisation pour les règles d'infrastructure communes à plusieurs réseaux
 - LDAP, DNS, NTP, supervision, journalisation, sauvegarde...
3. Du réseau le plus sensible au moins sensible
 - 3.1 Vers le réseau le plus sensible au moins sensible
 - Autorisation pour les flux de réseau à réseau
 - 3.2 Blocage des flux en provenance de ce réseau



- Utilisation de all ou any dans les règles



- Utiliser reseau_rfc1918 ou not reseau_interne au lieu de all ou any pour éviter les inférences
- Filtrage en mode « ceinture et bretelles » :
 - Filtrer sur les interfaces
 - ET
 - Filtrer sur les réseaux

1	Filtrage	143
2	Modes de connexion	154
3	Chiffrement	177

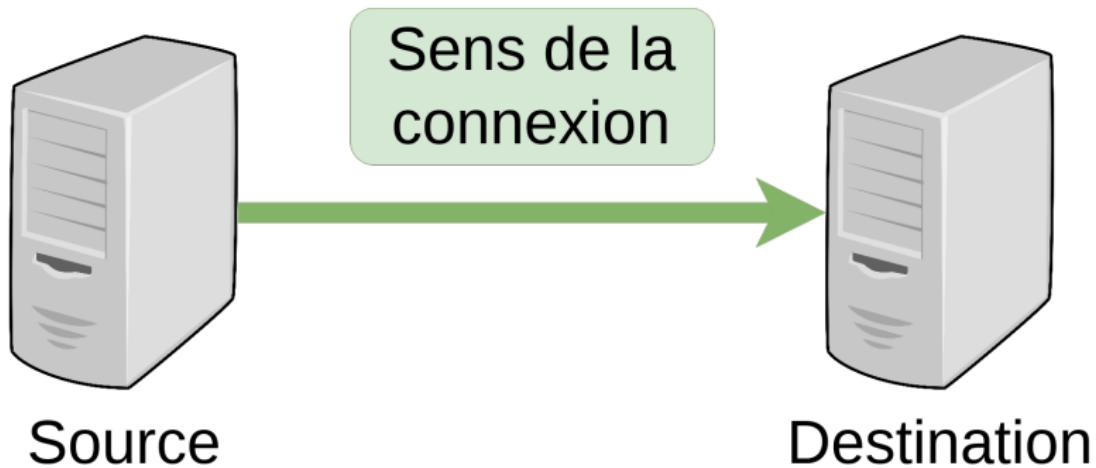


Figure – Définition de connexion, source et destination

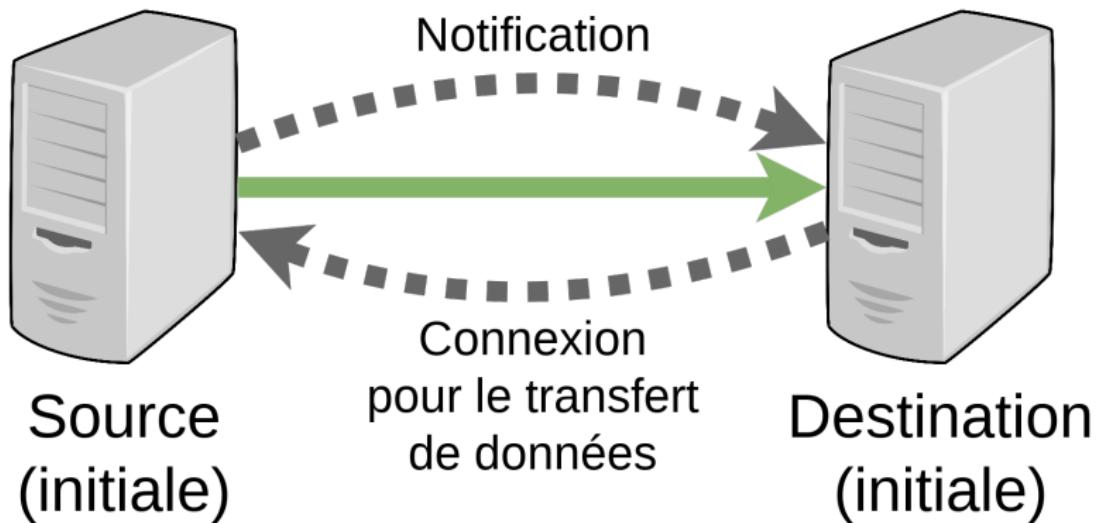


Figure – Définition de connexion et notification

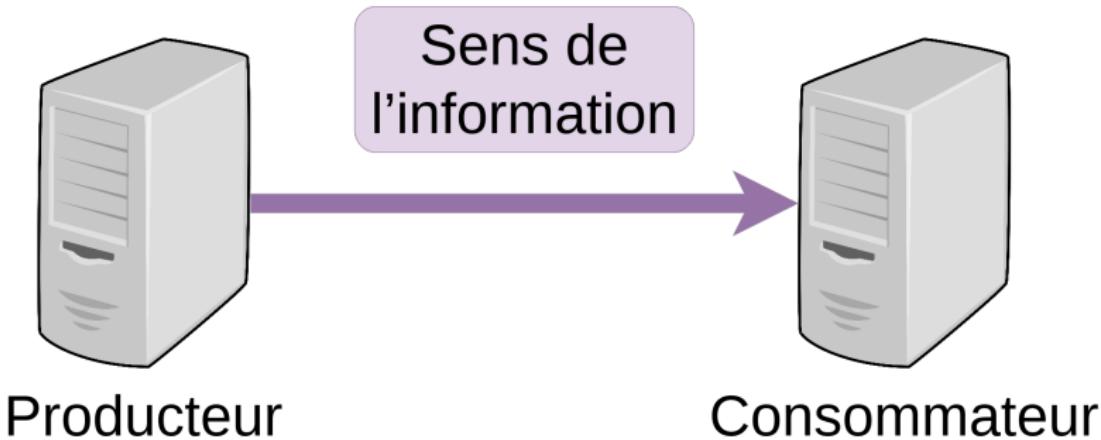


Figure – Définition de producteur et consommateur

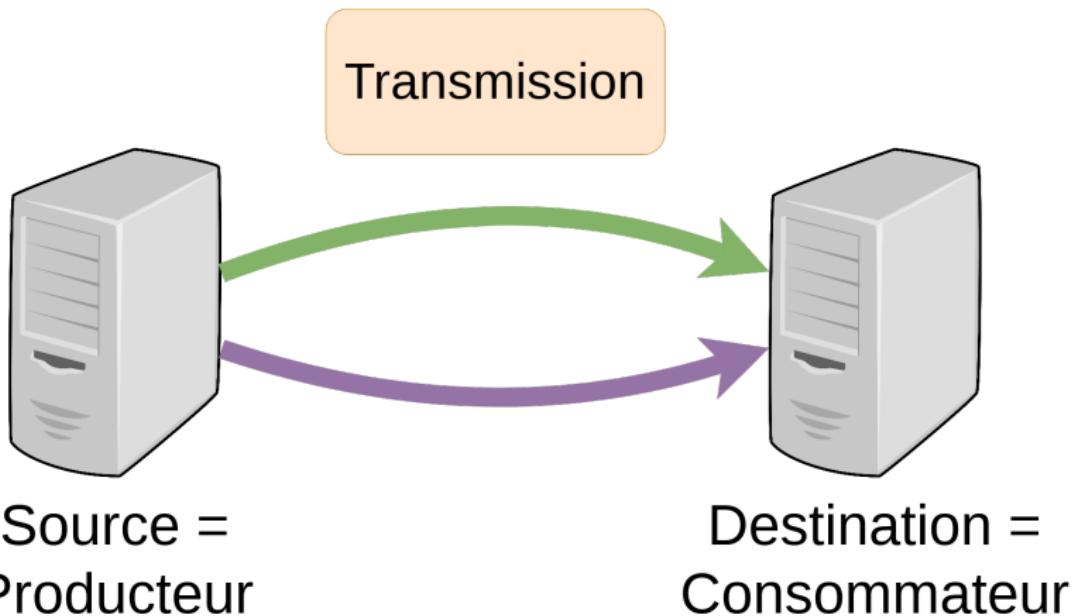
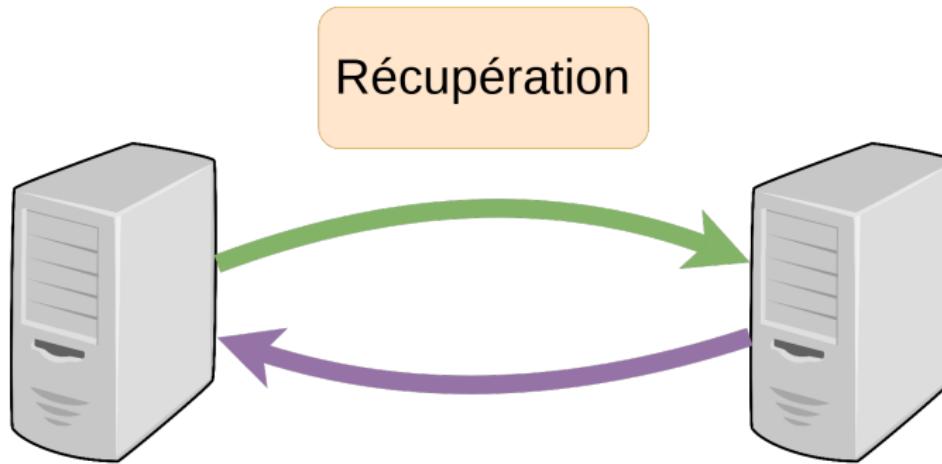


Figure – Définition de la transmission



Source =
Consommateur

Destination =
Producteur

Figure – Définition de la récupération

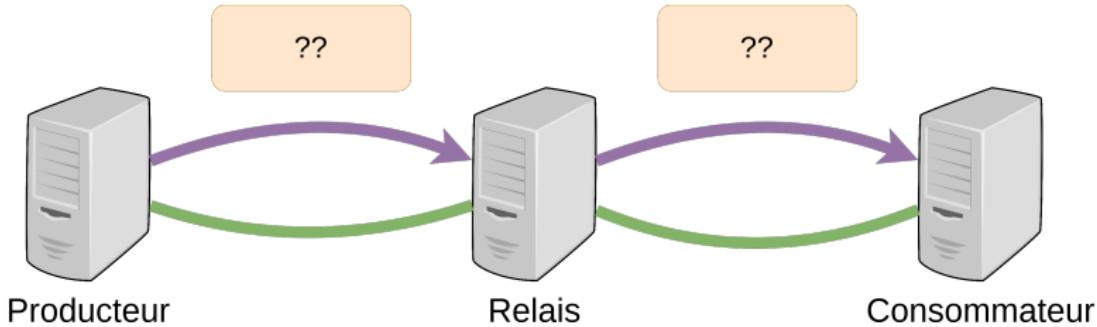


Figure – La question du relais



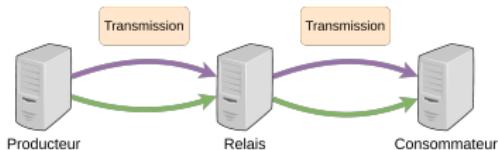


Figure – Relais mandataire

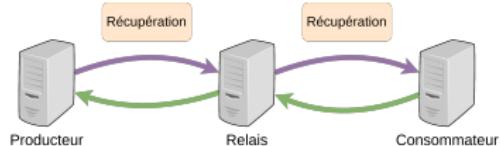


Figure – Relais mandataire

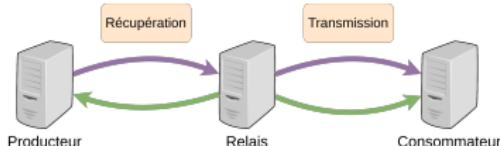


Figure – Relais pilote

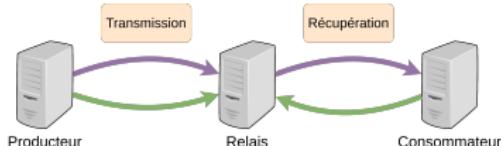


Figure – Relais tampon

Modes de connexion

Connexion synchrone?

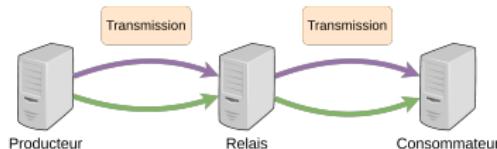


Figure – Relais mandataire

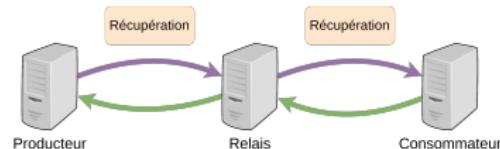


Figure – Relais mandataire

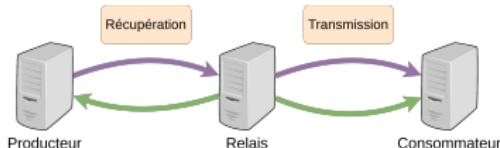


Figure – Relais pilote

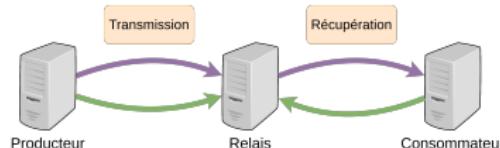


Figure – Relais tampon



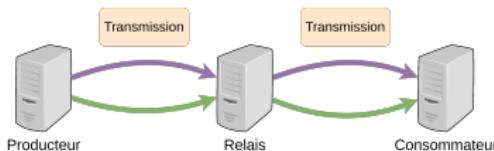


Figure – Relais mandataire : OK

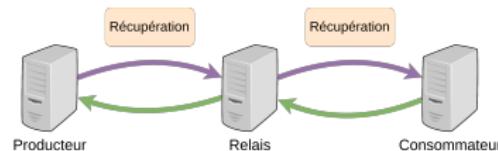


Figure – Relais mandataire : OK

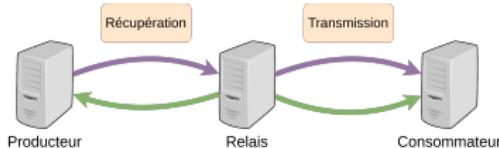


Figure – Relais pilote : KO

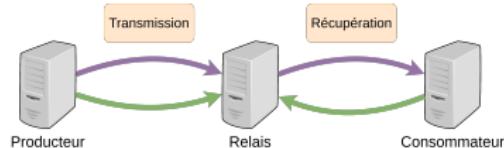


Figure – Relais tampon : KO

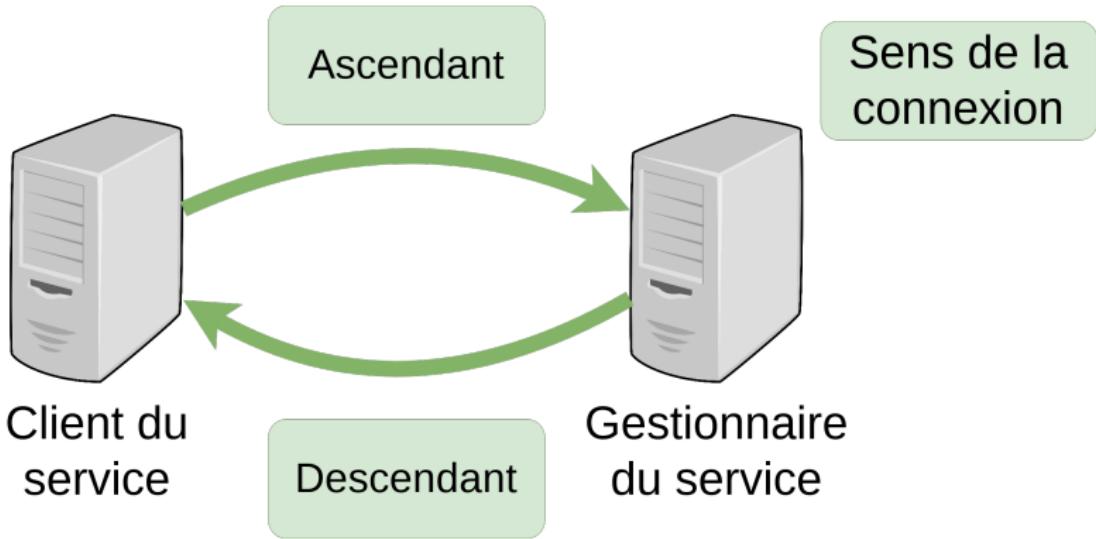


Figure – Définition d'ascendant et descendant

- Sauvegarde
- DNS
- Mise à jour
- Supervision
- Configuration
- NTP



- Sauvegarde : les deux
- DNS : ascendant
- Mise à jour : les deux
- Supervision : les deux
- Configuration : les deux
- NTP : ascendant

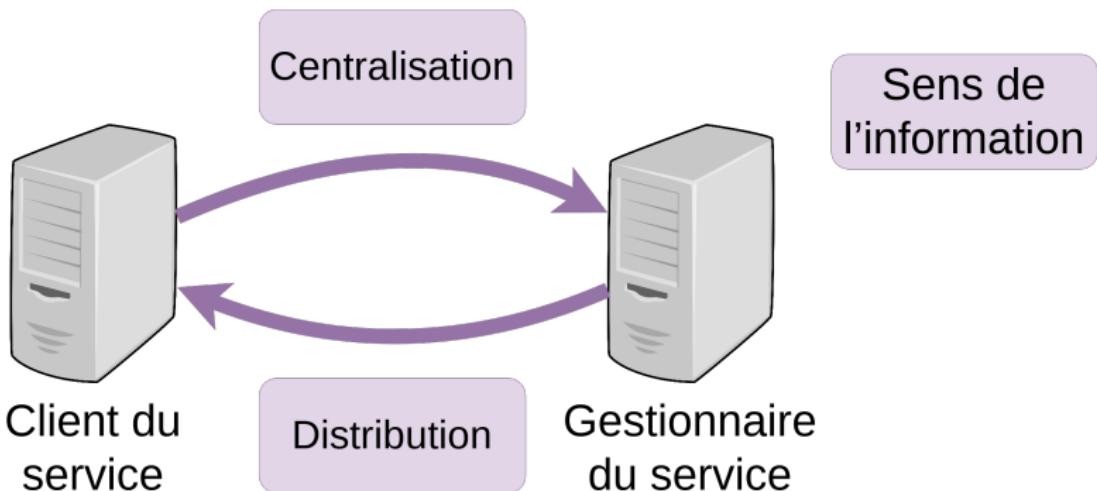


Figure – Définition de distribution et centralisation

- Sauvegarde
- DNS
- Mise à jour
- Supervision
- Configuration
- NTP



- Sauvegarde : centralisation
- DNS : distribution
- Mise à jour : distribution
- Supervision : centralisation
- Configuration : distribution
- NTP : distribution

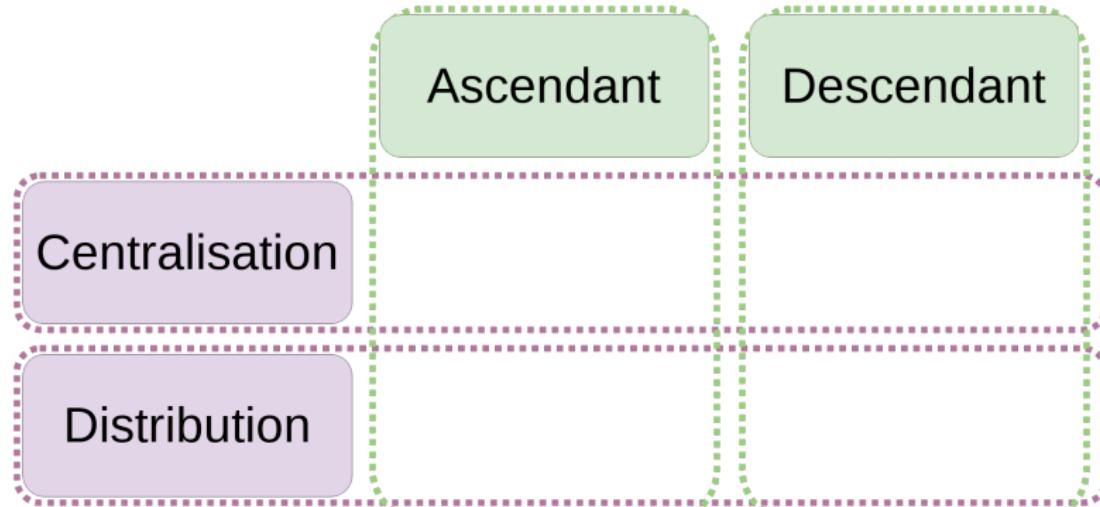


Figure – Transmission ou récupération ?



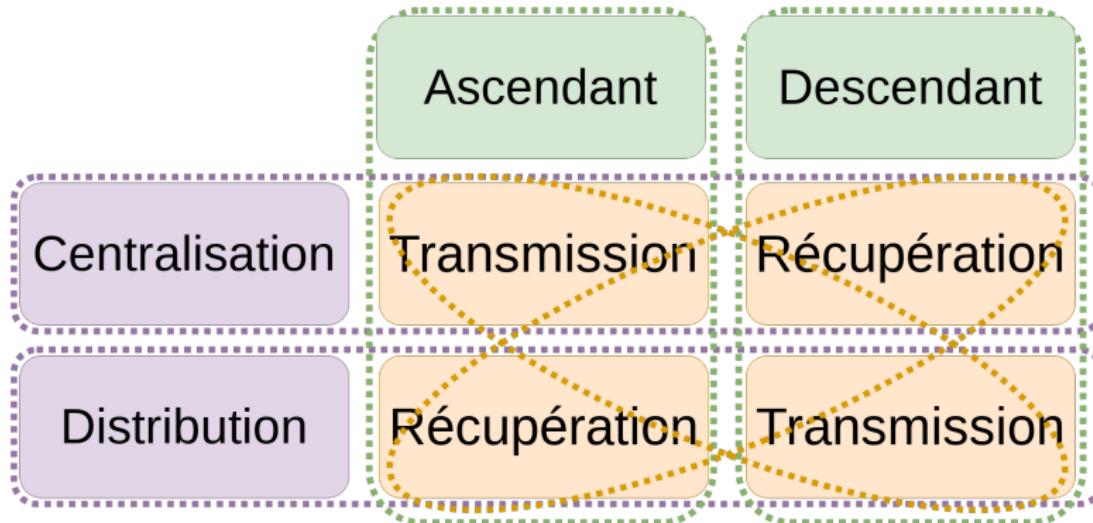


Figure – Transmission et récupération

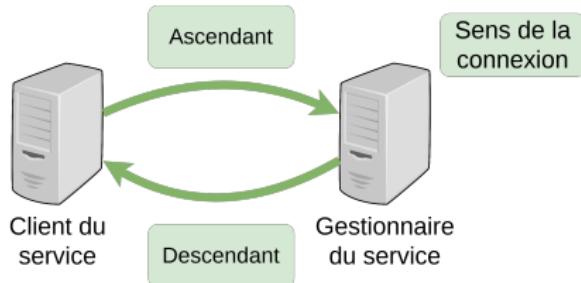
	Ascendant	Descendant
Centralisation	Sauvegarde Supervision	
Distribution	DNS NTP	Mise à jour Configuration

	Ascendant	Descendant
Centralisation	Transmission Sauvegarde Supervision	Récupération
Distribution	Récupération DNS NTP Mise à jour Configuration	Transmission

	Ascendant	Descendant
Centralisation	Transmission Sauvegarde rsync Borg Supervision Nagios NSCA	Récupération Veeam NRPE
Distribution	Récupération Mise à jour WSUS Package mirror	Transmission SCCM Configuration Puppet Windows GPO

Modes de connexion

Flux ascendants / descendants



Ascendant	Descendant
Prise en charge de clients à connectivité variable	Clients à connectivité variable complexes à gérer
Gestionnaire très exposé	Gestionnaire peu exposé
Clients peu exposés	Gestionnaire a des privilèges (potentiellement élevés) sur tous ses clients

- *push* ≈ Transmission
- *pull* ≈ Récupération



Les éditeurs peuvent employer des termes contradictoires, ne pas toujours s'y fier !

1	Filtrage	143
2	Modes de connexion	154
3	Chiffrement	177



Chiffrer protège contre l'interception



Chiffrer restreint également les mesures de filtrage

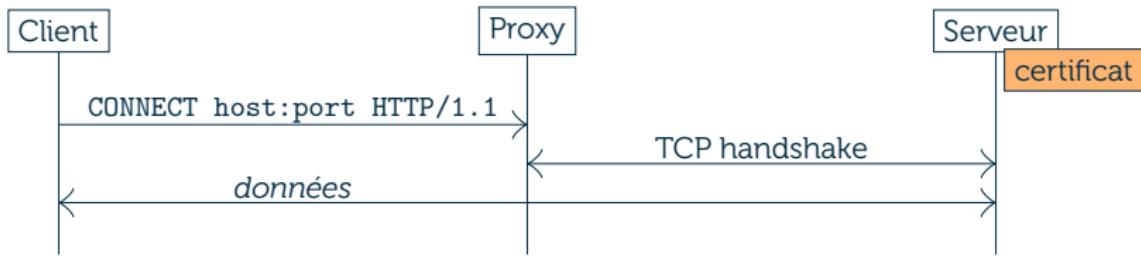


Figure – Transfert de données chiffrées

- Accès limité aux domaines sollicités (SNI)

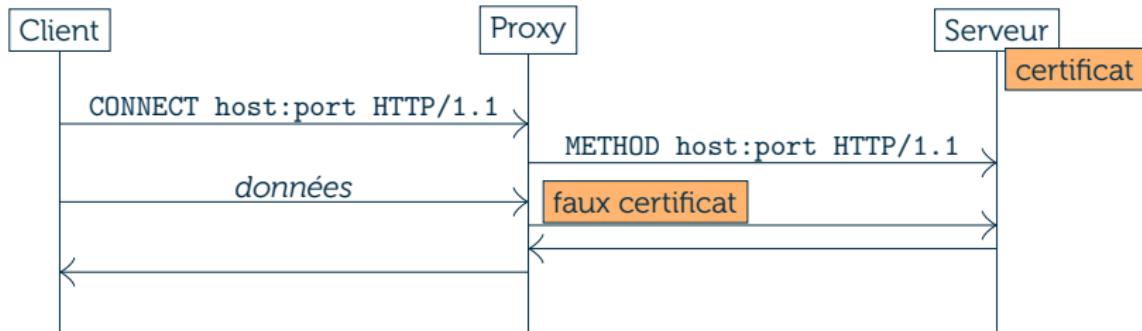


Figure – Interception TLS

- Accès à l'ensemble du contenu web

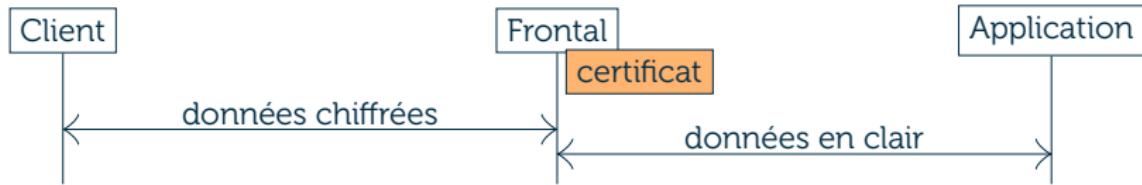


Figure – Réception des requêtes TLS

- Possibilité d'utiliser un autre moyen de chiffrement entre le frontal et l'application

- ESP (chiffrement / authentification)
 - Entête TCP/UDP inaccessible



Impossibilité de filtrer sur le port et donc le service sollicité

- AH (authentification)
 - Entête TCP/UDP accessible derrière l'entête AH
 - Est-ce que les pare-feu le trouveront ?
 - Avantage à l'IPv6 ici qui mixe options et paquets imbriqués



- Filtrez au niveau de toutes les couches
 - adresses IP, port destination, noms de domaines, UUID RPC
 - et évitez les *any* ou autres *all*
- Raisonnez le filtrage en règles générales
 - et documentez/justifiez toutes les exceptions
- Déterminez le mode de connexion le plus pertinent pour un service avant sa mise en œuvre
 - selon les avantages et risques de chaque mode
 - éviter de mixer les différents mode de connexion pour un même service
- Dans l'idéal, limiter les flux entre deux zones à une seule direction

Authentification et autorisation

mars 2021



Hervé Schauer Sécurité



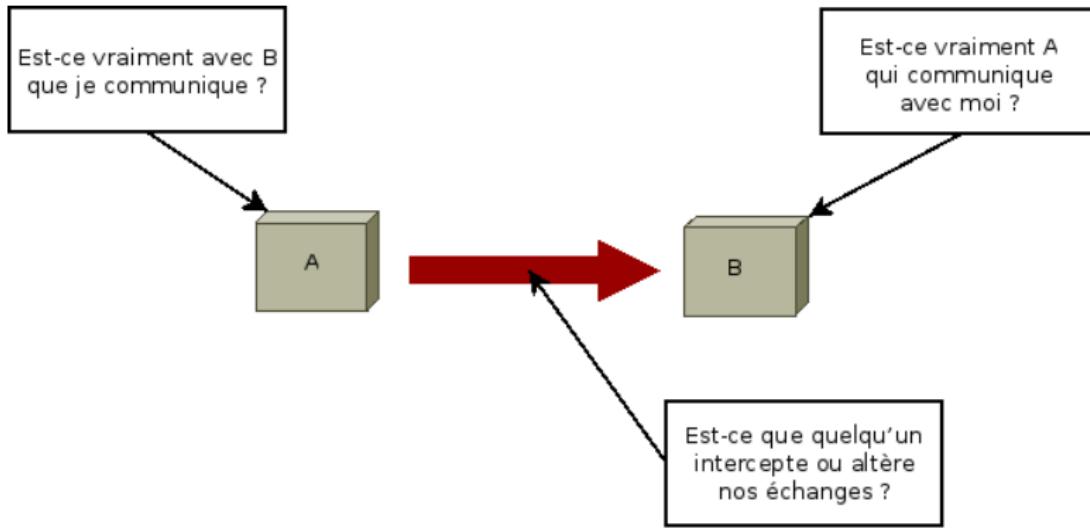
En résumé...

C'est là où on l'on regarde comment deux entités s'assurent de l'identité de l'autre.

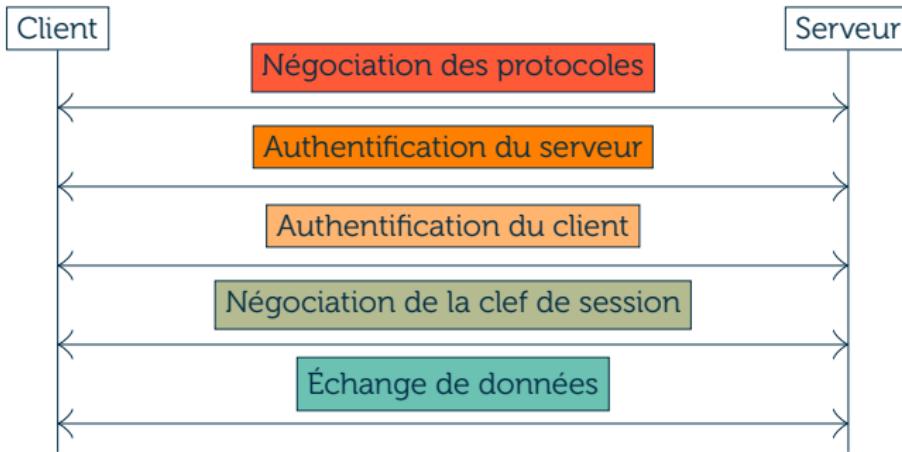
1	Flux d'authentification	186
2	Architecture d'authentification	244
3	Architecture d'autorisation	255
4	Enchaînement d'accès	261
5	Comptes de service	276

1 Flux d'authentification

Communication sécurisée et authentification	186
Négociation des protocoles d'échange	187
Authentification serveur	192
Authentification client	199
Authentification forte	209
Gestion de session	230
	239



Établissement d'une connexion sécurisée



Ces phases sont généralement entrelacées entre elles et facultatives



Les confusions de vocabulaire sont courantes

Protocole de transport

Méthode de communication sécurisée négociée ou imposée
Authentification par certificat client

TLS

Utilisation de AES128-CBC-HMAC-256

Spécification du protocole

SMB

Logiciel qui les implémente

Samba



Les confusions de vocabulaire sont courantes

Spécification des transactions réseaux

Spécification des API des bibliothèques associées à ces transactions réseaux

Kerberos

GSSAPI

OAuth

SASL

Protocole réseau

Format de stockage de secrets

NTLMv1, NTLMv2

NTLM (hash)

1 Flux d'authentification

Communication sécurisée et authentification	187
Négociation des protocoles d'échange	192
Authentification serveur	199
Authentification client	209
Authentification forte	230
Gestion de session	239

- Faciliter la transition vers de nouveaux protocoles plus sécurisés
- Proposer des modes d'authentification adaptés à l'architecture existante
- S'adapter à la vitesse de migration des clients
 - (ce qui pose question pour les services mis à disposition d'Internet)



Une attaque *man-in-middle* permet de dégrader le niveau de sécurité

- Version du protocole utilisable
- Méthode d'authentification du serveur
- Méthode d'authentification du client
- Méthode de génération de la clef de session
- Méthode de chiffrement des données incluant :
 - l'algorithme de chiffrement utilisé
 - la méthode d'enchaînement utilisée (bloc ou flot)
- Méthode d'authentification des données

- Version du protocole utilisable
 - Protocol
- Méthode d'authentification du serveur
 - HostKeyAlgorithms
- Méthode d'authentification du client
 - AuthenticationMethods
 - PubkeyAuthentication avec PubkeyAcceptedKeyTypes
 - ChallengeResponseAuthentication
 - GSSAPIAuthentication
 - HostbasedAuthentication avec HostbasedAcceptedKeyTypes
 - KerberosAutentication
 - PasswordAuthentication

- Méthode de génération de la clef de session
 - KexAlgorithms
 - GSSAPIKeyExchange avec GSSAPIKexAlgorithms
- Méthode de chiffrement des données incluant
 - Ciphers
- Méthode d'authentification des données
 - MACs
 - Déjà intégré par certains Cipher

- Choix des suites cryptographiques en fonction de la compatibilité attendue avec les clients
 - Exemple de catégories selon Mozilla⁸

Configuration	Firefox	Android	Chrome	Edge	Internet Explorer	Java	OpenSSL	Opera	Safari
Modern	63	10.0	70	75	--	11	1.1.1	57	12.1
Intermediate	27	4.4.2	31	12	11 (Win7)	8u31	1.0.1	20	9
Old	1	2.3	1	12	8 (WinXP)	6	0.9.8	5	1

- Configuration associée (pour la catégorie "moderne")
 - TLS_AES_128_GCM_SHA256 (TLSv1.3)
 - TLS_AES_256_GCM_SHA384 (TLSv1.3)
 - TLS_CHACHA20_POLY1305_SHA256 (TLSv1.3)
- Propose aussi un générateur de configuration⁹

8. https://wiki.mozilla.org/Security/Server_Side_TLS

9. <https://ssl-config.mozilla.org/>

- PPP pour les liaisons point à point, généralement auprès des fournisseurs de connectivité (ISP)
- EAP pour les liaisons point à point, les réseaux filaires et Wi-Fi
- SSL/TLS pour les protocoles TCP (notamment ceux en mode texte)
- SSH
- IKE
- SPNEGO¹⁰



Chaque protocole de transport impose un certain nombre de limites sur les protocoles négociables.

10. Simple and Protected GSSAPI Negotiation Mechanism

1 Flux d'authentification

Communication sécurisée et authentification

Négociation des protocoles d'échange

Authentification serveur

Authentification par cryptographie asymétrique

Authentification par secret partagé

Authentification client

Authentification forte

Gestion de session

186

187

192

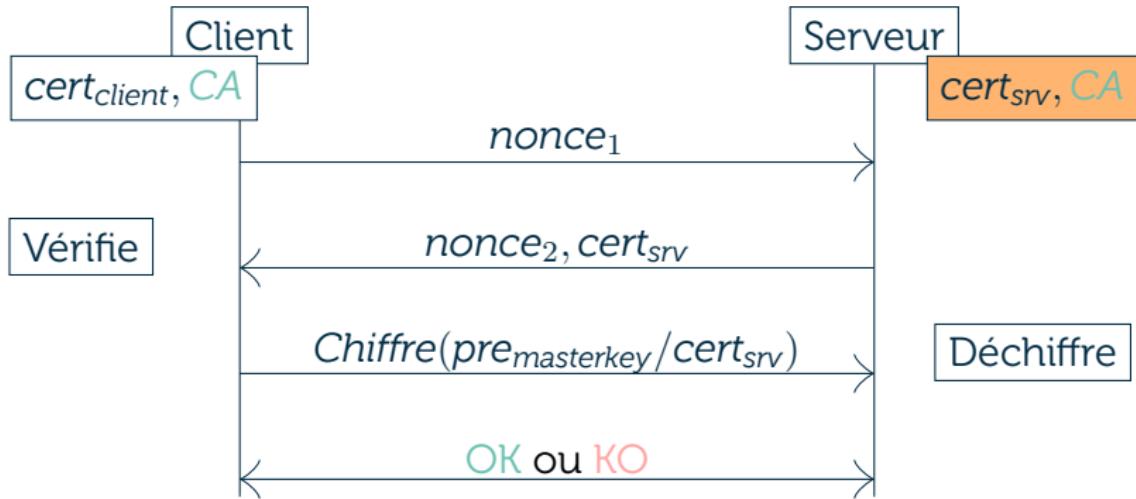
199

209

230

239

- Authentification par cryptographie asymétrique
 - Authentification par mémorisation de l'empreinte
 - Authentification via autorité tierce
- Authentification par secret partagé





Seule l'étape de vérification diffère

- Vérification standard du certificat
 - Validité du nom
 - Validité des dates
- Authentification par mémorisation de l'empreinte
 - Validation de l'association empreinte-nom dans une base du client
- Authentification via autorité tierce
 - Validation de l'authenticité du certificat par validation de la signature du certification par une autorité reconnue

- Exemples de protocoles :
 - SSL/TLS
 - SSH

Non sécurisé

À éviter

Fiable

Authentification par cryptographie asymétrique

Authentification par mémorisation de l'empreinte



Facilité d'implémentation



- Connexion non sécurisée lors de la première connexion
 - Risque d'interception des communications
- Transmission d'une mauvaise habitude aux utilisateurs
 - Risque d'interception des communications

Authentification par cryptographie asymétrique

Authentification par mémorisation de l'empreinte

```
$ ssh user@example.net
The authenticity of host 'example.net (10.0.0.1)' can't be established.
ECDSA key fingerprint is 20:99:0b:b8:65:28:98:db:66:ed:11:1f:14:dd:d1:94.
Are you sure you want to continue connecting (yes/no)?
```

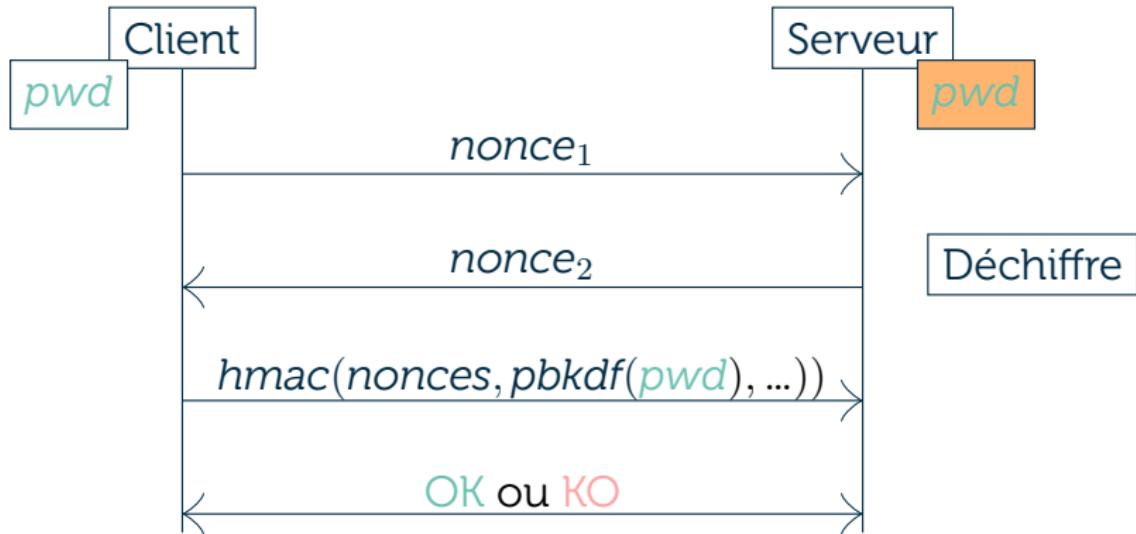
Figure – Certificat autosigné

Authentification par cryptographie asymétrique

Authentification via autorité tierce - Faiblesses et avantages



- Complexité de gestion (gestion du renouvellement)
 - Risque d'indisponibilité
- Gestion de la confiance dans les tiers
 - Risque d'interception des communications



- SCRAM-*
- Kerberos



Réutilisation d'un élément déjà défini

1 Flux d'authentification

Communication sécurisée et authentification

186

Négociation des protocoles d'échange

187

Authentification serveur

192

Authentification client

199

Authentification par transmission du secret

209

Authentification par Challenge-Response

Authentification par cryptographie asymétrique

Authentification par jeton

Authentification forte

230

Gestion de session

239



Considérer la sécurité d'usage et la sécurité du protocole

Une authentification triple facteurs peut se traduire par un simple échange NTLMv1.

Catégories de protocoles d'authentification client

- Authentification par transmission du secret
- Authentification par *Challenge-Response*
 - Authentification par secret partagé
 - Authentification par cryptographie asymétrique
- Authentification par jeton d'authentification
 - Jeton reposant sur une graine partagée
 - Jeton délivré par une autorité



Il est possible de combiner ces méthodes d'authentification

- Emplacement et format de stockage des secrets
- Réutilisabilité des éléments transmis sur le réseau
- Dépendance à des composants externes
- Interopérabilité avec un autre système d'authentification
- Capacité à fonctionner avec un annuaire
- Capacité à délivrer une authentification forte
- Etc.

Authentification par transmission du secret

Le fonctionnement



- Exemples de protocoles :
 - Authentification par **formulaire web** avec mot de passe en base de données
 - **PAP**¹¹ - RFC 1334¹²

Non sécurisé

À éviter

Fiable

11. Password Authentication Protocol

12. <https://tools.ietf.org/html/rfc1334>

Authentification par transmission du secret

Faiblesses et avantages



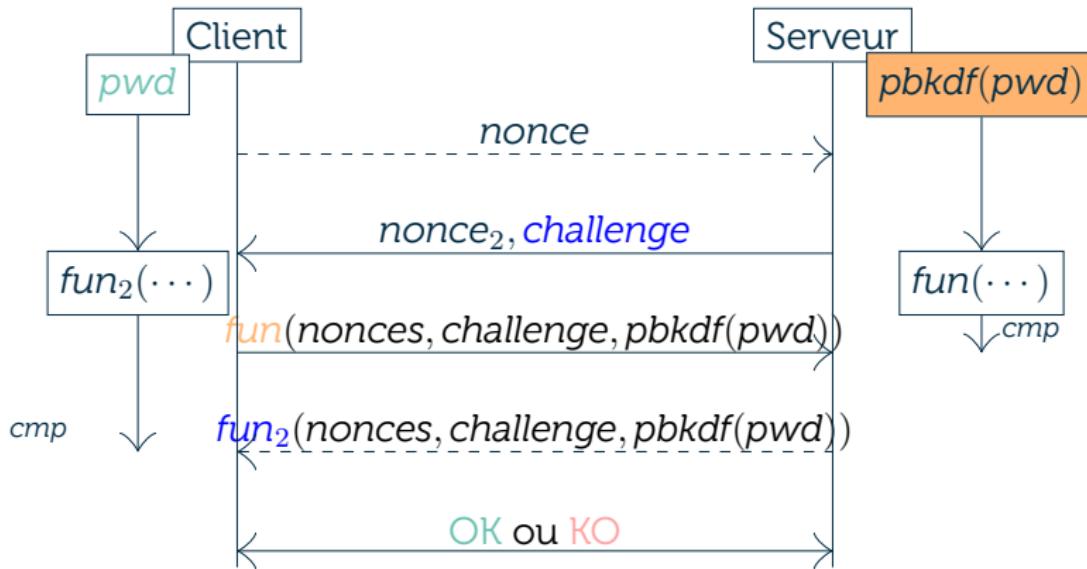
- Découpage entre transmission et stockage
- Facilité d'implémentation



- Transmission du secret en clair
 - Risque d'interception du secret
- Transmission potentiel du secret en clair entre le serveur et l'annuaire (LDAP, SQL)

Authentification par Challenge-Response

Le fonctionnement



Les flux en pointillés et fun_2 sont facultatifs

Authentification par Challenge-Response

Exemples de protocoles

- DIGEST-MD5 avec $pbkdf = Id$ et $fun = md5$
- CRAM-MD5 avec $pbkdf = Id$ ou $md5$ et $fun = hmac$
- SCRAM-* avec $pbkdf$ qui dépend de la déclinaison et usage de fun_2
- LM avec $pbkdf$ et fun basés sur DES
- NTLMv1 avec $pbkdf$ basé sur MD4 et DES et fun basée sur DES
- NTLMv2 avec $pbkdf$ basé sur MD4 et HMAC-MD5 et fun basée sur HMAC-MD5
- EAP-MD5
- [MS-]CHAP

Non sécurisé

À éviter

Fiable

Authentification par Challenge-Response

Faiblesses et avantages



- Mot de passe non transmis
- Stockage du *hash* du mot de passe



- Stockage du mot de passe dépendant du protocole
 - Restriction sur la méthode de stockage utilisée
 - Complexité à faire évoluer le stockage et le protocole
- Connaissance de $pbkdf(pwd)$ suffisante pour s'authentifier
 - Vulnérable aux attaques *pass-the-hash*

Authentification par Challenge-Response

Cas particulier de SCRAM-*



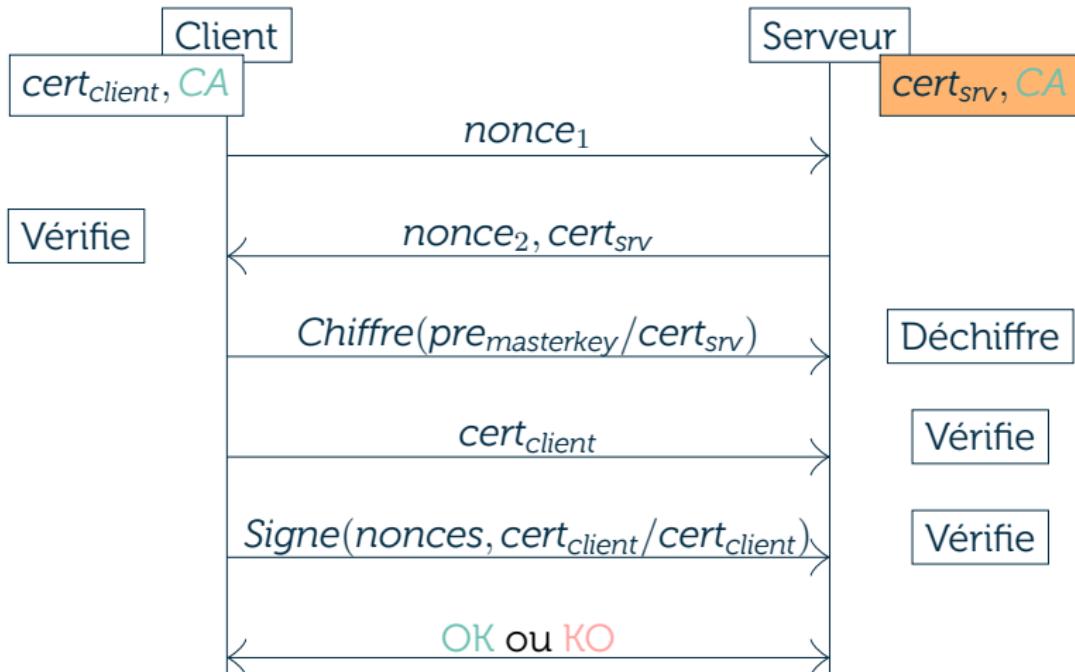
- Utilisation d'un format de *pbkdf* fiable et ajustable
 - ex : PBKDF2
- Stockage de deux dérivés de *pbkdf(pwd)* du mot de passe
 - L'accès à la base de données insuffisant pour réaliser des attaques *pass-the-hash*
- Utilisation de *fun₂*
 - Authentifie le serveur auprès de l'utilisateur



- Utilisation d'un format de stockage inhabituel
 - 2 dérivés de *pbkdf(pwd)* et
 - les paramètres liés au calcul du hash
 - Difficulté pour trouver des solutions compatibles
 - Difficulté pour étendre la solution au reste du SI

Authentification par cryptographie asymétrique

Le fonctionnement



- **SSL/TLS** avec des certificats x509
 - Schannel sous Windows
 - LibreSSL et OpenSSL sous Un*x
- **SSH** avec des clefs SSH certifiées ou non, ou des clefs GPG
- **U2F** avec des certificats générés à la demande
- **EAP-TLS** avec des certificats x509

Non sécurisé

À éviter

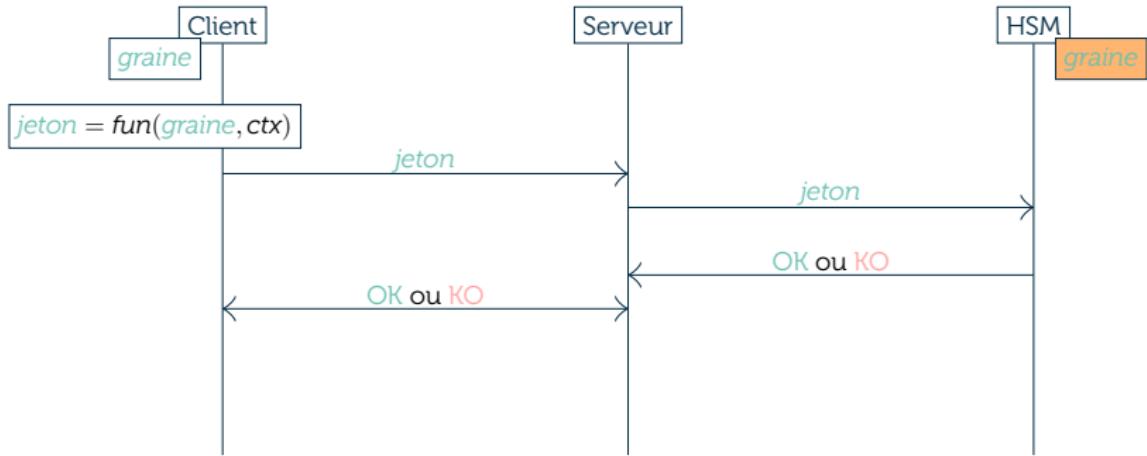
Fiable



Clef privée non transmise et présente uniquement au niveau client



- Opérations coûteuses en ressource et en latence
 - Contrainte forte pour l'IoT
- Gestion d'une PKI interne ou
- Sécurité reposant sur celle du distributeur de certificat
 - Attaque des fournisseurs
- Repose sur des problèmes mathématiques et $NP > P$



Authentification par jeton reposant sur une graine

Exemples de protocoles

- [Yubi] **OTP** avec des certificats x509
- **TOTP** basé sur le *timestamp*
- **HOTP** basé sur un compteur
- **Google Authenticator**, un TOTP
- **SecurID**, un TOTP associé à un PIN

Non sécurisé

À éviter

Fiable



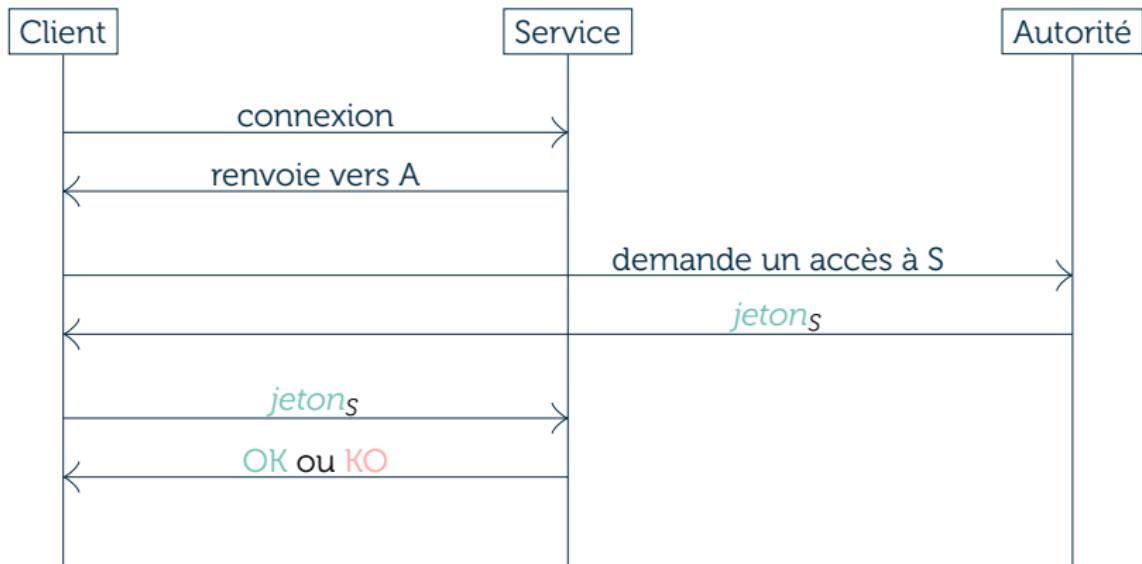
Durée de vie limitée du jeton



- Jeton indépendant de l'origine
 - Attaque par rejeu immédiat possible
- Stockage de la graine
 - Usurpation d'identité par génération des OTP
- Dépendance à un serveur stockant les graines (SecurID, YunoHost OTP)
 - Indisponibilité
- Requiert une synchronisation temporelle (pour les TOTP)
 - Indisponibilité

Authentification par jeton délivré par une autorité

Le fonctionnement



Authentification par jeton délivré par une autorité

Exemples de protocoles

- SAML
- OpenID
- Kerberos

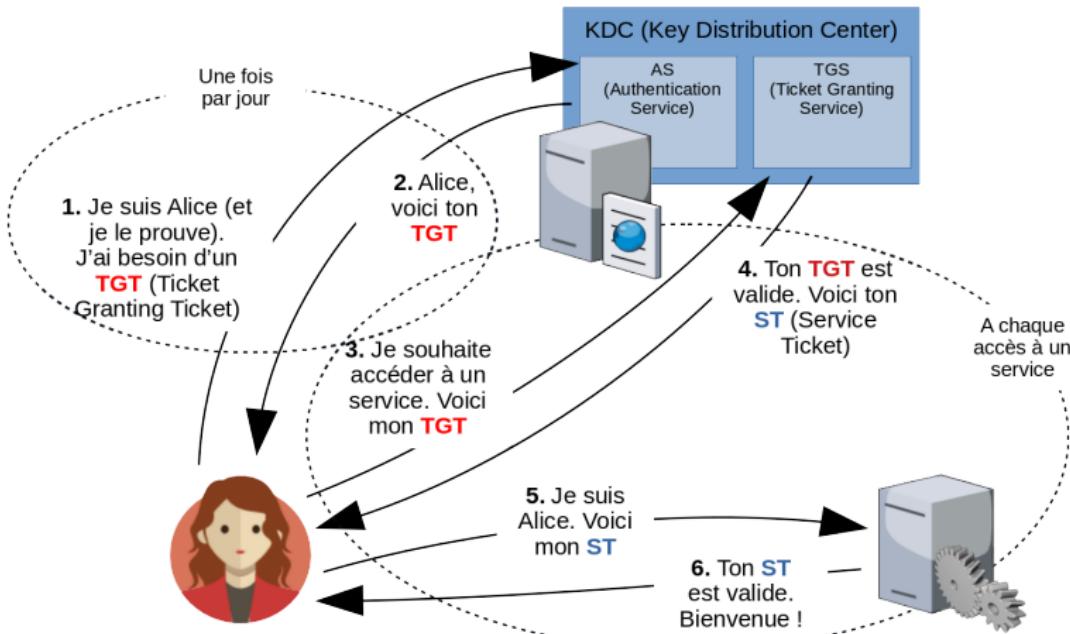
Non sécurisé

À éviter

Fiable

Authentification par jeton délivré par une autorité

Kerberos



Authentification par jeton délivré par une autorité

Faiblesses et avantages



- Durée de vie limitée du jeton
- Jeton dépendant de la source



- Repose sur un autre moyen d'authentification auprès du serveur faisant autorité
- Stockage d'une clef maître
 - Usurpation d'identité par génération d'identité
- Dépendance au service faisant autorité (ex : KDC)
 - Indisponibilité
- Requiert une synchronisation temporelle
 - Indisponibilité

Assimilable à la génération d'un certificat temporaire

1 Flux d'authentification

Communication sécurisée et authentification	186
Négociation des protocoles d'échange	187
Authentification serveur	192
Authentification client	199
Authentification forte	230
Gestion de session	239

- Ce que l'on sait
 - Mot de passe
- Ce que l'on a
 - Élément matériel
- Ce que l'on est (biométrie)
 - Empreinte digitale
 - Iris
 - Frappes clavier
 - Etc.



Quid du certificat présent sur ma machine et protégé par un mot de passe !^g



Authentification forte
≠
Authentification multi-facteurs



Authentification forte =
Il n'y a jamais de données suffisantes pour rejouer
l'authentification :

- au delà d'une courte durée
- sur n'importe quel composant client hors HSM/carte à puce

USB + Carte à puce
sinon X

Indiquer s'il s'agit réellement d'une authentification forte ou non et justifier en indiquant une manière de récupérer les éléments d'identification le cas échéant

Authentification basée sur...

- Un certificat protégé par mot de passe présent sur le poste X
- Un certificat associé à la machine et un mot de passe X
- Un certificat présent sur un périphérique USB connecté au moment de l'authentification et un mot de passe X
- Un certificat présent sur une carte à puce et protégé par un code PIN ✓
- Google Authenticator avec un développeur réintégrant la graine dans un script de connexion automatique X

can be reversed
locally



Indiquer s'il s'agit réellement d'une authentification forte ou non et justifier en indiquant une manière de récupérer les éléments d'identification le cas échéant

Authentification basée sur...

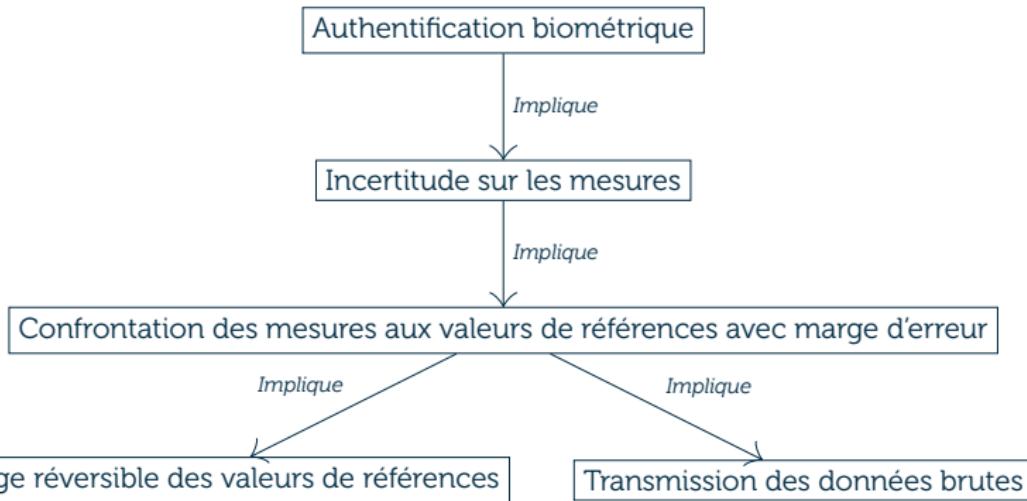
- Un mot de passe et un OTP présent sur un token externe 
- Le compte machine piloté par l'AD et un compte utilisateur 
- Une vérification biométrique transmise à un serveur central avec le mot de passe 
- Une vérification biométrique effectuée vis-à-vis de données stockées sur une carte magnétique et qui renvoie un secret avec le mot de passe 



Authentification basée sur...

- Un certificat protégé par mot de passe présent sur le poste
 - Certificat déchiffré en RAM
 - Rejouable => KO
- Un certificat associé à la machine et un mot de passe
 - Éléments accessibles par un administrateur machine
 - Rejouable => KO
- Un certificat présent sur un périphérique USB connecté au moment de l'authentification et un mot de passe
 - Simple clef USB ou HSM ?
 - Dépend du périphérique !
- Un certificat présent sur une carte à puce et protégé par un code PIN
 - Non rejouable => OK

- Google Authenticator avec un développeur réintégrant la graine dans un script de connexion automatique
 - Graine accessible
 - Rejouable => KO
- Un mot de passe et un OTP présent sur un token externe
 - Non rejouable => OK
- Le compte machine piloté par l'AD et un compte utilisateur
 - Mot de passe du compte machine renouvelé tous les mois
 - Question ouverte !



- Une vérification biométrique transmise à un serveur central avec le mot de passe
 - Toutes les informations sont accessibles depuis le serveur
 - Rejouable => KO
- Une vérification biométrique effectuée vis-à-vis de données stockées sur une carte magnétique et qui renvoie un secret avec le mot de passe
 - Le secret est accessible et rejouable depuis le serveur
 - Rejouable => KO

1 Flux d'authentification

Communication sécurisée et authentification	186
Négociation des protocoles d'échange	187
Authentification serveur	192
Authentification client	199
Authentification forte	209
Gestion de session	230
	239

- Génération de la clef maître
- Gestion des clefs de session
- Reprise de session
- Mécanismes de Heartbeat...

- Usage de PFS¹³ ou confidentialité persistante
 - Empêche d'accéder au contenu des messages à partir de la clef privée du serveur
- Exemple : Diffie-Hellman
 - Génération d'un secret commun
 - La clef de session n'est pas échangée
- Contre-exemple : échange de clefs RSA
 - Enregistrement des communications X années
 - Compromission ultérieure de la clef privée
 - Déchiffrement des échanges antérieurs



S'assurer de ne pas utiliser des options dégradant le niveau de sécurité



- Sélectionnez les mécanismes, architectures, solutions d'authentification selon
 - les composants sur lesquels reposent le risque d'usurpation d'identité
 - les mécanismes cryptographiques disponibles
- Supprimez les mécanismes d'authentification par *challenge-response* et par transmission du secret
 - formulaires web, LM, NTLMv1-2
- Configurez les paramètres des protocoles négociés
 - notamment les paramètres cryptographiques
- Assurez-vous que votre authentification multi-facteurs est forte

1	Flux d'authentification	186
2	Architecture d'authentification	244
3	Architecture d'autorisation	255
4	Enchaînement d'accès	261
5	Comptes de service	276

- Composants impliqués :
 - Client
 - Destination (service)
 - Référentiel d'authentification

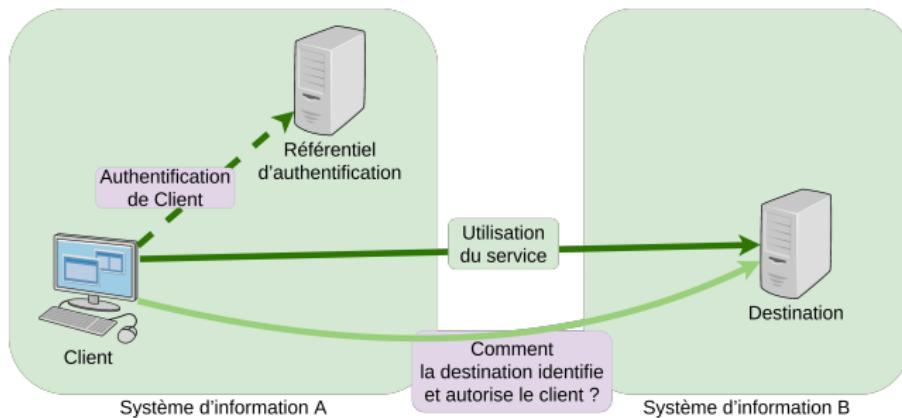


Figure – Architecture : problématiques

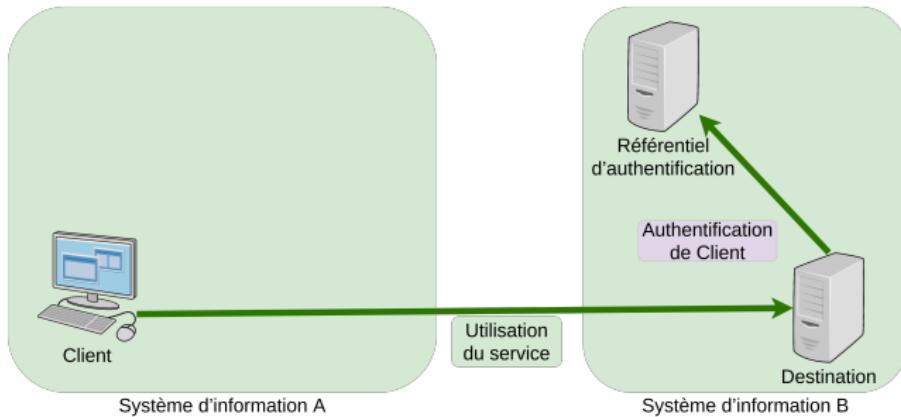


Figure – Architecture : Authentification locale



- Pas de problématique d'intégration
- Requiert juste l'ouverture de flux à destination du service



- Multiplication des mots de passe
 - Risque de réutilisation des mots de passe (récupérable et réutilisable par un attaquant)
 - Risque d'utilisation erronée d'un mot de passe valide sur une autre plateforme (récupérable et réutilisable par un attaquant)

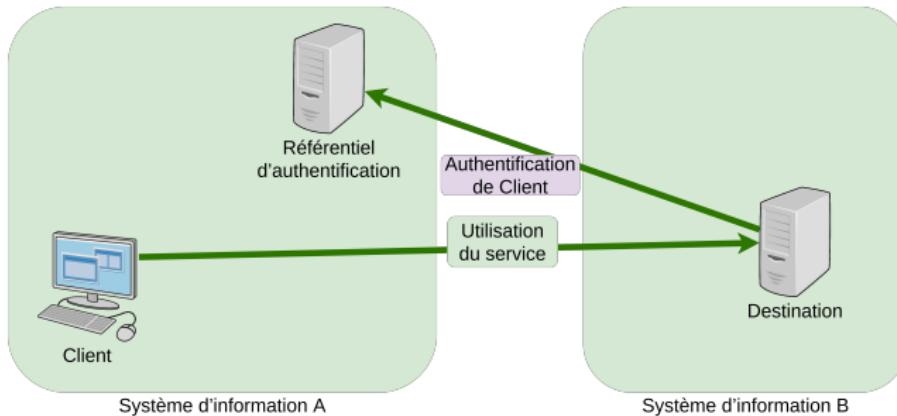


Figure – Architecture : Réauthentification



- Même mot de passe partout



- Saisie des mêmes identifiants sur de multiples plateformes
 - Récupérable et réutilisable par un attaquant
 - Permet l'accès à l'ensemble des services utilisant ce mécanisme
- Requiert d'ouvrir des flux vers le référentiel d'authentification depuis le service
 - Bref : inacceptable pour des services externes
 - Risque de bruteforce depuis l'extérieur

Architecture : locale et réauthentification

Attention aux protocoles utilisés entre le service et le référentiel

- TACACS assurant une transmission en clair
- TACACS+ ajoute le chiffrement
- RADIUS avec ses nombreuses extensions (PAP, [MS-]CHAP, EAP)
- Diameter
- MySQL, utilisable avec SSL/TLS, authentification NTLM et authentification Challenge / Response
- MS-SQL, utilisable avec SSL/TLS, authentification Basic, Digest, NTLM, Kerberos
- LDAP, sécurisable avec SSL/TLS, authentification via SASL

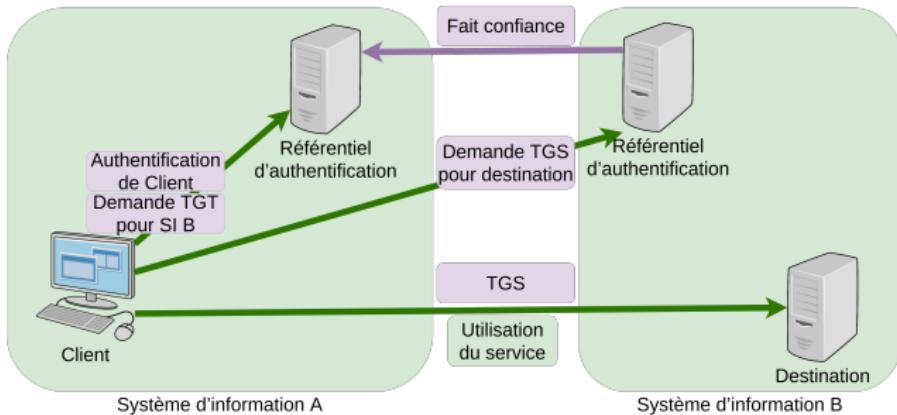


Figure – Architecture : Relation d'approbation



- Même mot de passe partout
- Pas besoin de le ressaisir



- Faire attention à la configuration pour ne pas créer de trou de sécurité béant via cette relation
- Requiert d'ouvrir des flux vers le référentiel d'authentification pour l'ensemble des composants sollicitant des services internes
 - Bref : unacceptable pour des services externes
Risque de bruteforce depuis l'extérieur

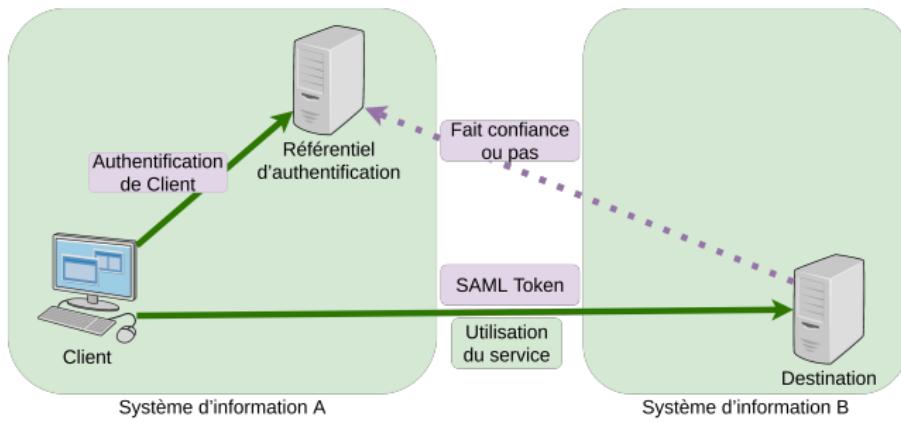


Figure – Architecture : Fédération d'identité / SAML



- Même mot de passe partout
- Pas besoin de le ressaisir
- Pas besoin d'un lien entre le service et le référentiel d'authentification
 - Provisionnement initial du lien via un certificat

1	Flux d'authentification	186
2	Architecture d'authentification	244
3	Architecture d'autorisation	255
4	Enchaînement d'accès	261
5	Comptes de service	276

- Composants impliqués :
 - Client
 - Serveur
 - Base de données d'accès
- Trois types d'autorisations
 - Autorisation locale
 - Autorisation sur annuaire centralisé
 - Autorisation par encapsulation

- Exemples d'annuaires centralisés :
 - LDAP
 - *SQL

- Exemples d'encapsulation :
 - *Claims* dans Kerberos
 - *Capabilities* dans les certificats x509
 - Clef dans OAuth

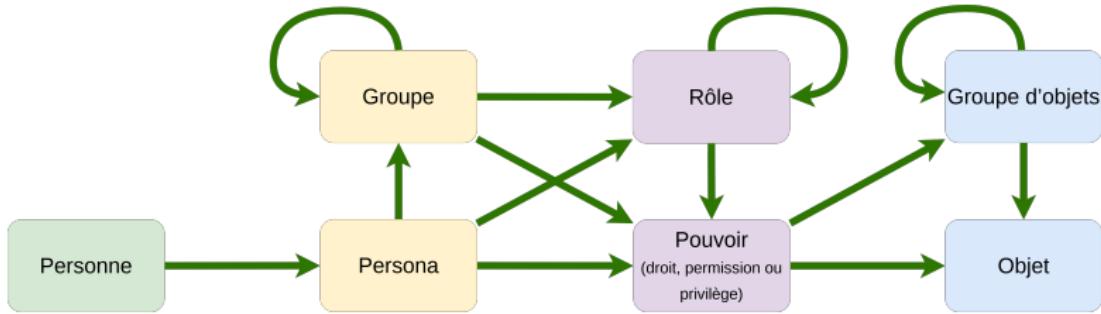


Figure – Architecture d'attribution de pouvoirs



- Éviter d'utiliser plusieurs circuits entre persona et pouvoirs
- L'utilisation de groupes et de rôles doit rester une aide
- Éviter les groupes imbriqués



Une bonne solution doit permettre de :

- Lister les pouvoirs d'un persona
- Les personas ayant un ensemble de pouvoirs
 - Notamment ceux ayant des priviléges d'administration

1	Flux d'authentification	186
2	Architecture d'authentification	244
3	Architecture d'autorisation	255
4	Enchaînement d'accès	261
5	Comptes de service	276

En résumé...

C'est ici que l'on regarde comment *Client* s'authentifie auprès de *Destination* en passant par *Intermédiaire*.

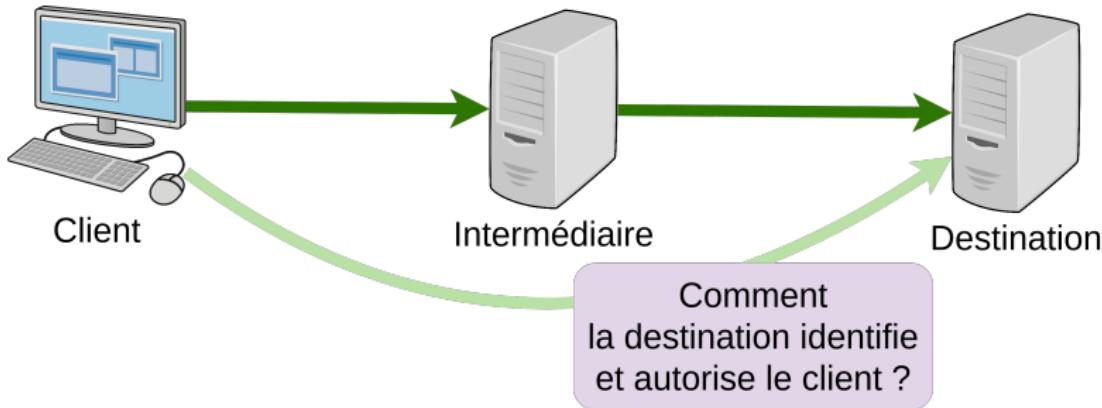


Figure – Enchaînement de l'authentification

- Rebond par confiance au relais
- Rebond par proxy réseau
- Rebond par réauthentification
- Rebond par utilisation d'un compte de service
- Rebond par délégation d'accès
- Rebond par délégation d'accès restreint

L'*Intermédiaire* se contente de transmettre l'identité du *Client* à *Destination* sans s'authentifier

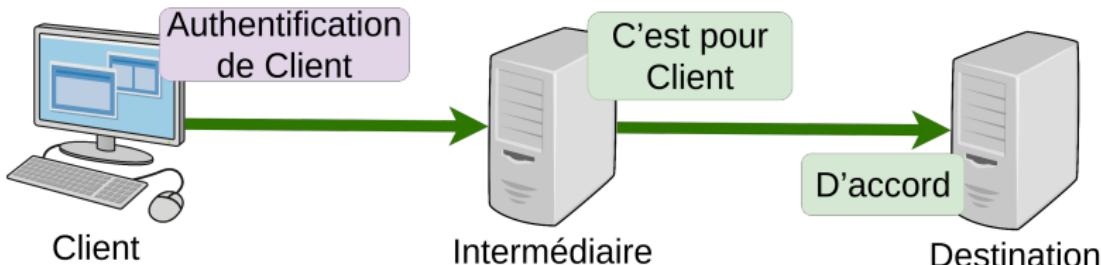


Figure – Rebond : confiance au relais

- Exemple
 - Entête `RemoteUser` entre le frontal web et la couche applicative



- Tout service ayant accès à *Destination* peut se faire passer pour n'importe qui

L'*Intermédiaire* se contente de relayer le trafic

- Authentification de *Client* auprès de *Intermédiaire*
 - Activation du proxy réseau sur *Intermédiaire*
- Authentification de *Intermédiaire* auprès de *Destination*

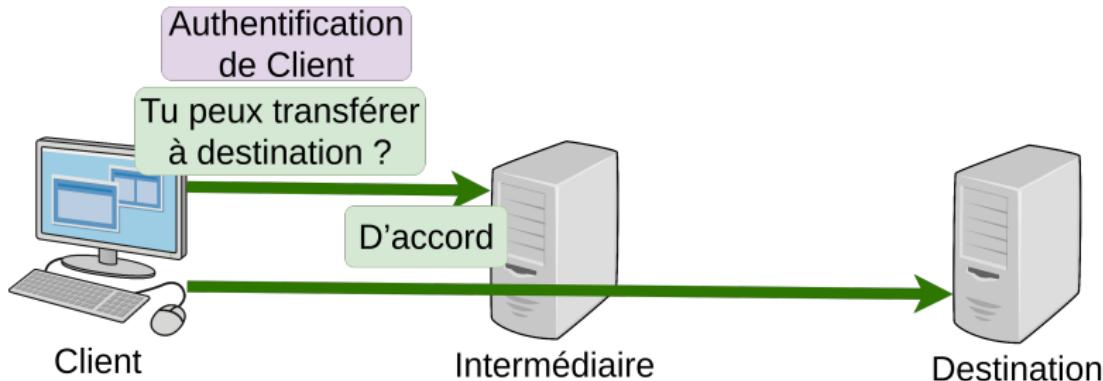


Figure – Rebond : proxy réseau



Empêche tout accès de *Intermédiaire* à *Destination* si le mécanisme de connexion est sécurisé



- Ne permet pas à *Intermédiaire* d'accéder à nos données sur *Destination*
⇒ Pose problème pour certaines utilisations
Ex : Client → Web app. → BDD
Ex : Journalisation des échanges

- Exemples d'*Intermédiaire*

- relais HTTP autorisant CONNECT
- serveur SSH autorisant AllowTcpForwarding

- Authentification de *Client* auprès de *Intermédiaire*
- Authentification de *Intermédiaire* auprès de *Destination*

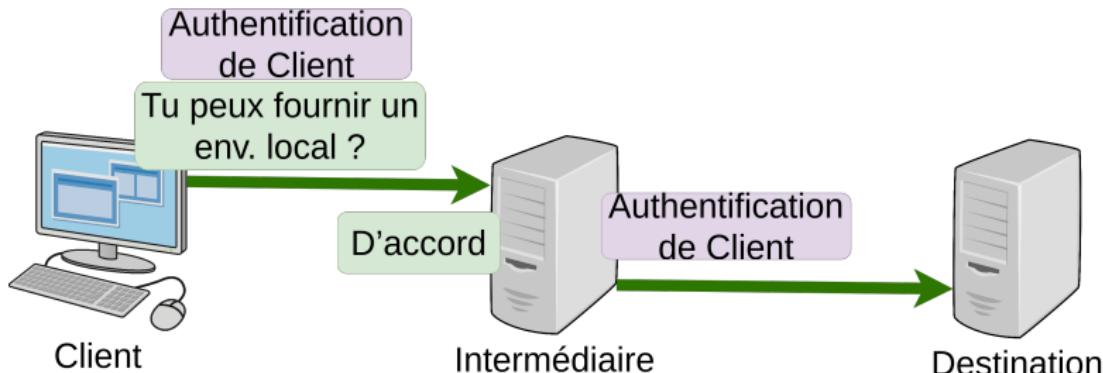


Figure – Rebond : réauthentification



Permet d'utiliser deux comptes différents pour les accès



- Lourd pour les utilisateurs
- Risque d'usurpation par l'administrateur de *Intermédiaire*

- Exemples d'*Intermédiaire*
 - serveur VNC
 - serveur XenDesktop
 - serveur "de rebond"

Rebond par utilisation d'un compte de service 1/2

- Authentification de *Client* auprès de *Intermédiaire*
- Authentification de *Intermédiaire* auprès de *Destination* avec le compte de service

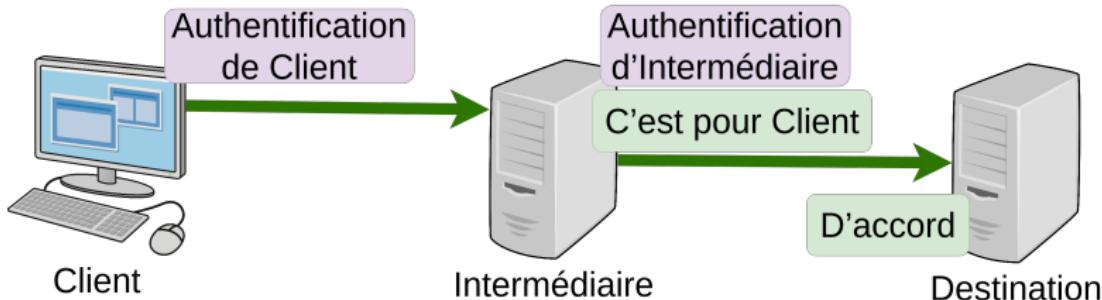


Figure – Rebond : compte de service

Rebond par utilisation d'un compte de service 2/2



Permet de mutualiser les accès et d'améliorer les performances



- Déporte le contrôle d'accès à *Destination* sur le code applicatif
 - Risque lié à l'exploitation de failles logicielles

- Exemple

- Architectures 3 tiers des sites web
- Approche de TheBastion¹⁴ avec un compte de service par groupe d'utilisateurs

14. TheBastion : <https://github.com/ovh/the-bastion>

- Authentification de *Client* auprès de *Intermédiaire* avec son ticket TGS
- Transmission de son ticket TGT à *Intermédiaire*
- Obtention d'un TGS pour *Destination* par l'*Intermédiaire* avec le TGT reçu
- Authentification de l'*Intermédiaire* auprès de *Destination* avec un ticket TGS au nom de *Client*

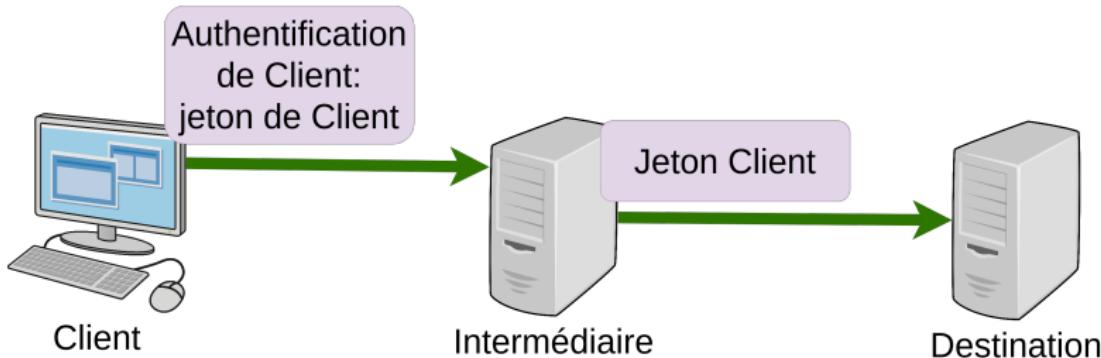


Figure – Rebond : délégation des autorisations d'accès



Transparence et conservation du SSO



- Persistance du ticket T sur *Intermédiaire*
- Risque d'usurpation par l'administrateur de *Intermédiaire*

• Exemples d'*Intermédiaire*

- serveur RDP (non restreint)
- serveur SSH avec activation du *ForwardAgent*
- Délégation Kerberos non contrainte

Identique à la délégation d'accès mais :

- ServicesAllowedToSendForwardedTicketsTo de *Intermédiaire* contient *Destination*



Offre le meilleur compromis



Mise en œuvre complexe à anticiper au niveau applicatif

- Exemples d'*Intermédiaire*
 - Proxy Kerberos (Windows)
 - *Constrained Delegation* (Windows > 2012)
 - *Impersonation* du service (Windows, S4U)



- Limitez la propagation des identifiants ou équivalents au sein du système d'information
- Privilégiez des mécanismes systèmes plutôt qu'applicatif pour gérer les accès sensibles

1	Flux d'authentification	186
2	Architecture d'authentification	244
3	Architecture d'autorisation	255
4	Enchaînement d'accès	261
5	Comptes de service	276

Pourquoi faire ?

Tout service qui communique avec un autre requiert un compte de service

Un compte de service :

- Est un compte comme un autre
- Possède les mêmes mécanismes d'authentification
- Est récupérable et rejouable

- Chaque machine a un compte machine
- Chaque machine a un compte administrateur local
- Chaque relation d'approbation a un compte
- De nombreux services ont un compte
- Le tout est sous contrôle d'un compte maître (`krbtgt`)



- Attention aux comptes
 - par défaut
 - non utilisés, mais qui existent
- Quid du renouvellement des mots de passe !
 - Comment se protéger contre les exfiltrations sur le long terme
- Quid des réutilisations du même mot de passe
 - Problématique de la gestion des comptes administrateur locaux



- Chaque machine a un compte machine
 - ⇒ Renouvellement gérable par GPO
- Chaque machine a un compte administrateur local
 - ⇒ Utilisation de LAPS
- Chaque relation d'approbation a un compte
- De nombreux services ont un compte
 - ⇒ Renouvellement des comptes MSA et gMSA
 - Mais pas compatible partout
- Le tout est sous contrôle d'un compte maître (`krbtgt`)
 - ⇒ Script de renouvellement de LAPS

Architecture de base

mars 2021



Hervé Schauer Sécurité



©Hervé Schauer Sécurité 2021

Wenyong WANG

281

En résumé...

C'est là où on commence avec un réseau à plat et où on démarre une construction propre pour obtenir une architecture conçue.

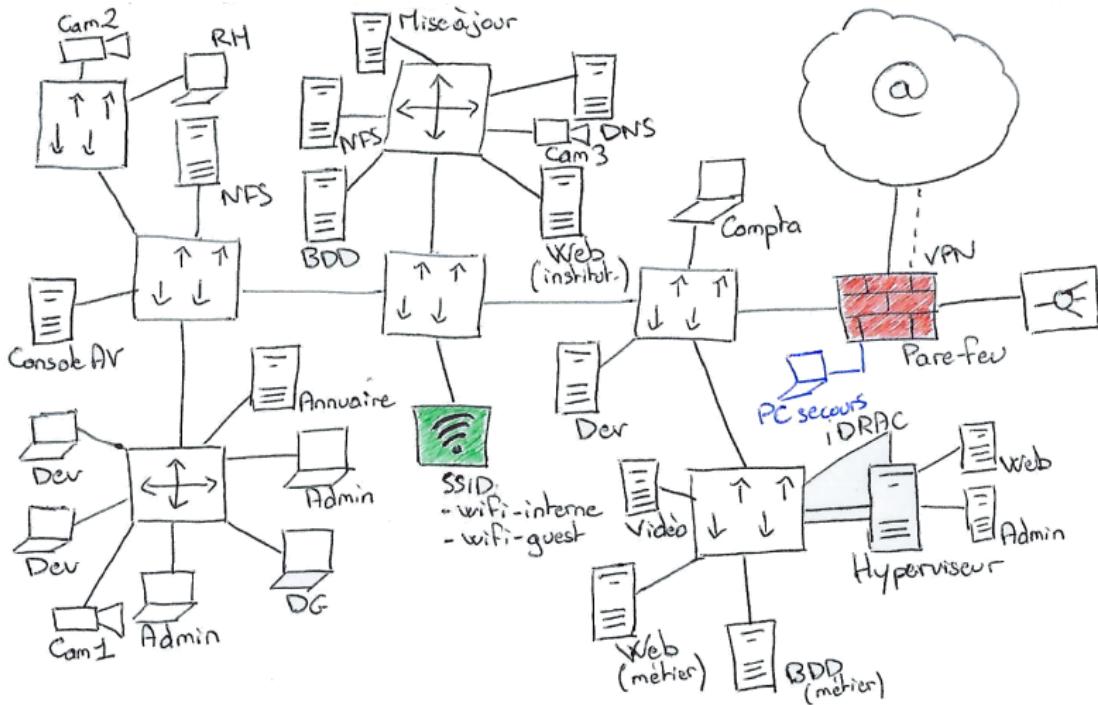


Figure – Réseau à plat

1	Bulles et tiers-{0-2}	284
2	Séparation des environnements	301
3	Administration, privilèges et relations de contrôle	308
4	Services d'infrastructure et de sécurité	370
5	Applications	444
6	Continuité	452

- À l'origine : segmentation applicative, particulièrement dans le monde Windows (au sein d'un domaine)
- Segmentation des différents SI selon la notion de sensibilité

Niveau d'exigence en sécurité ↑

- **Tiers-0 : gestion de la confiance**
 - Authentification
 - Référentiel centralisé
 - Infrastructure de gestion de clefs
- **Tiers-1 : SI sensibles**
 - Serveurs métiers et infrastructure
 - Il peut y avoir plusieurs SI de tiers-1
- **Tiers-2 : autres SI**
 - SI utilisateurs
 - SI largement exposés (IoT, SI non maîtrisés...)



Le niveau de sécurité d'une bulle est celui du composant le plus faible !

- À chaque bulle son administration
 - Administration tiers-0
 - Administration(s) tiers-1
 - Administration(s) tiers-2



On parle ici de composants logiques plus que de personnes.



Si l'administration du tiers-0 est en tiers-1, le niveau de sécurité du tiers-0 descend à celui du tiers-1.



On détaillera l'architecture et les mécanismes de séparation des différentes bulles dans ce chapitre.

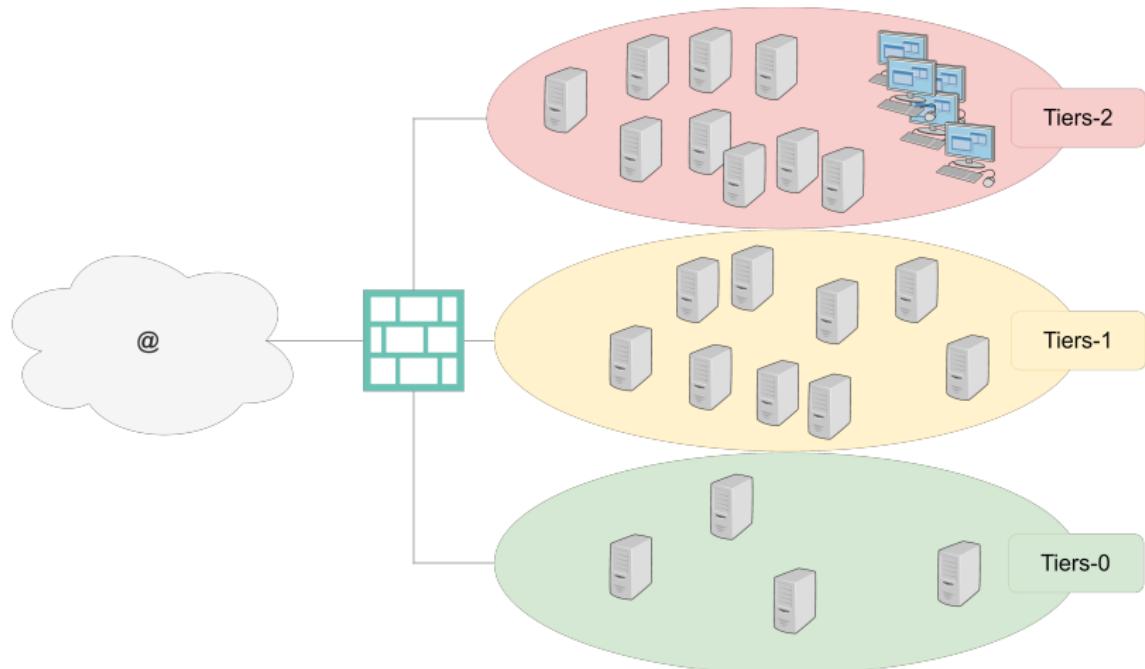


Figure – Architecture en bulles : principe des bulles

- Segmentation applicative (notamment au niveau de l'authentification)
- Mais défense en profondeur
 - donc on l'applique au niveau réseau

Tout à plat ?

- Segmentation du tiers-1 en plusieurs bulles de même niveau
 - métier 1, métier 2, infrastructure
- Segmentation des bulles en zones en incluant la notion de connectivité
 - "Zone(s) démilitarisée(s)" (DMZ (DeMilitarized Zone))
 - Zone tampon d'interconnexion entre deux zones de confiance hétérogène
 - Soit l'extérieur de la bulle et les composants les plus sensibles
 - Zones internes



- Segmentation purement réseau...
 - ...qui impactera l'architecture applicative
 - Séparation des fonctions selon la notion d'exposition

DMZ

Zone tampon d'interconnexion entre deux zones de confiance hétérogène.

- Considérée comme **potentiellement compromise**
- Porte des fonctions de sécurité
 - Filtrage en entrée et en sortie
 - Deux pare-feu distincts
 - Rupture protocolaire
 - Analyse et détection
 - Sondes réseau - IDS/IPS



La DMZ ne doit pas pouvoir être contournée.



Une DMZ est considérée comme une zone potentiellement compromise.

Souhaite-t-on exposer notre annuaire d'authentification aux équipements de cette zone ?

- Plusieurs solutions possibles
 - Annuaire dédié
 - *RODC (Read-Only Domain Controller)*
 - Relais d'authentification en DMZ
 - Relais authentifiant en interne
 - Infrastructure d'authentification dédiée

Une seule DMZ ? ⇒ Une zone par cinématique de flux

1. Services exposés (flux entrants)

- Web
- e-mail
- Résolution de noms
- ...

2. Services relais (flux sortants)

- Web
- e-mail
- Résolution de noms
- Synchronisation de temps
- Mise à jour
- ...

3. Accès distant

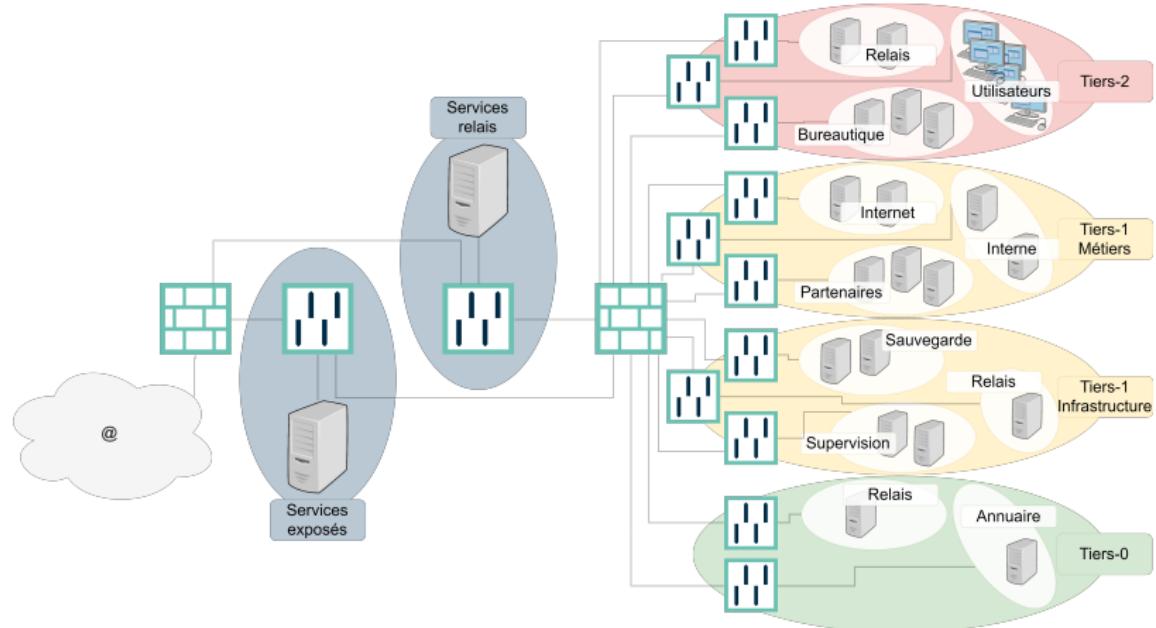


Figure – Architecture en bulles : principe des zones

Système d'information

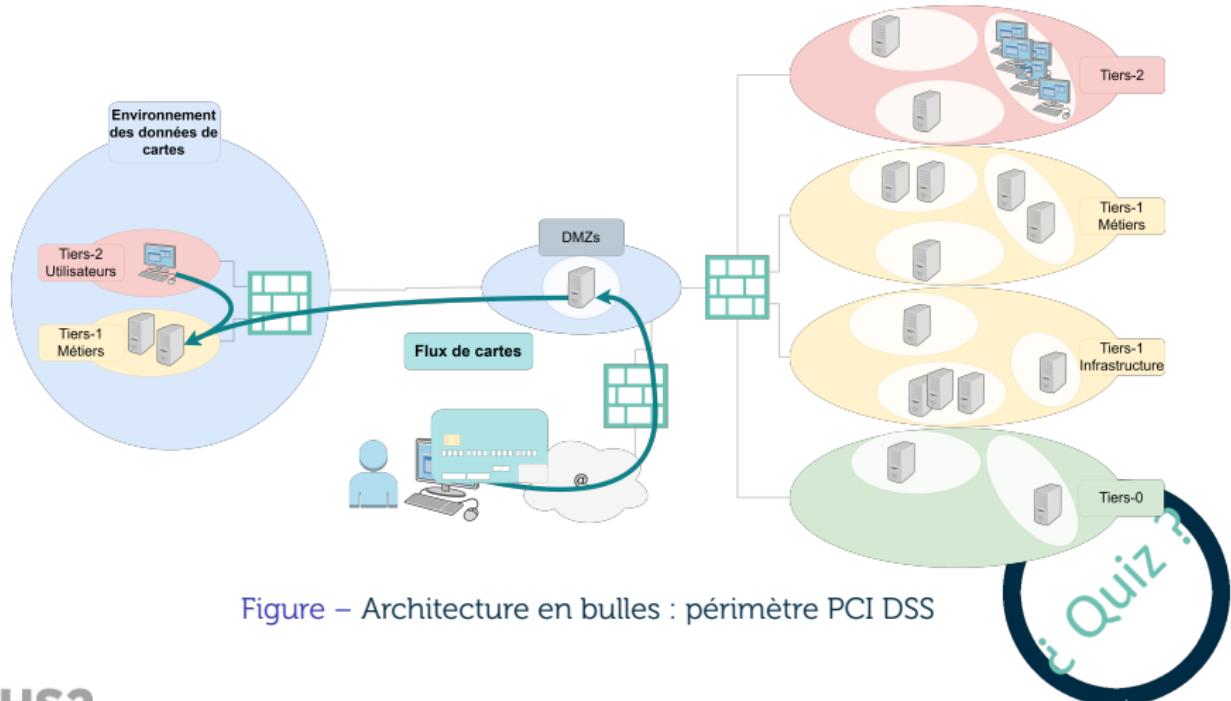
Ensemble indépendant de bulles (tiers-0 à tiers-2).

- Création de DMZ entre SI
 - Tout comme entre le SI interne et Internet
 - Même chose entre le SI interne et un SI externe



Le cas de l'accès Internet illustre ce sujet plus loin dans ce chapitre.

Mutualisation du tiers-0 entre SI ?



- (Contre?)-exemple : définition du périmètre selon PCI DSS
 - Tout composant qui stocke, traite ou transmet des données de cartes
 - Tout composant connecté ou pouvant impacter la sécurité d'un composant du périmètre
 - Tiers-0 (qui porte l'authentification)
 - Administration
 - Tiers-1 d'infrastructure
 - Tiers-1 dédié PCI DSS

Architecture en bulles

Illustration : SI cartes de paiement

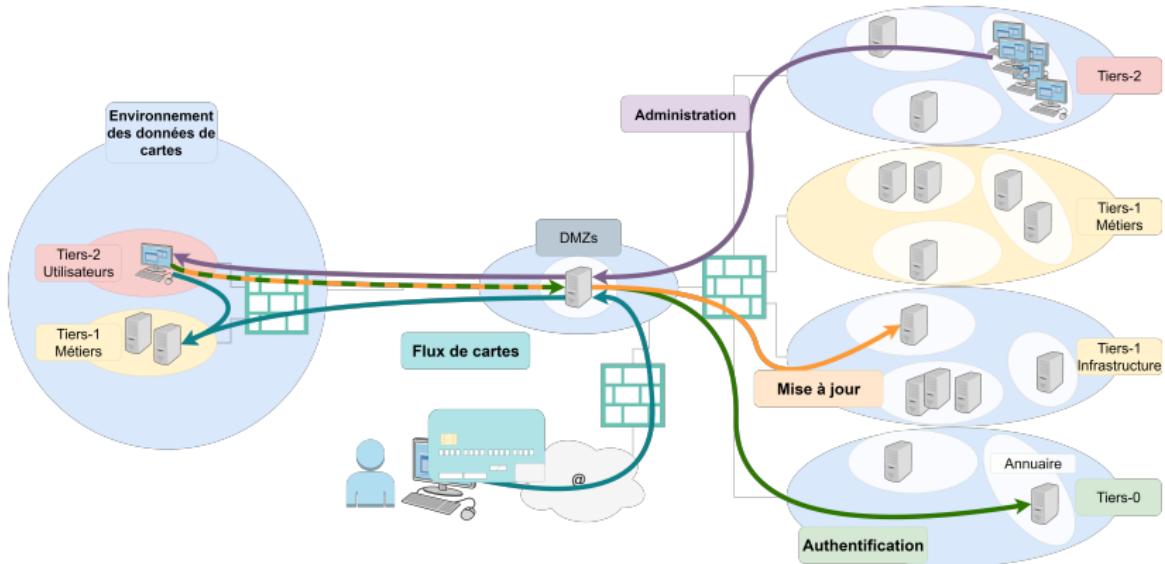


Figure – Architecture en bulles : périmètre PCI DSS (réalité)

⇒ Propagation d'exigences de sécurité

- Les exigences PCI DSS sont alors imposées à toute l'administration et au socle
 - Politique de mots de passe
 - Durcissement
 - Etc.
- La réalité :
 - L'architecture initiale est mal conçue, donc on ne peut pas simplement mettre en conformité les composants du tiers-0 et ainsi pouvoir les mutualiser
 - Isolation de l'environnement PCI DSS == duplication de tous les composants d'infrastructure (tiers-0, tiers-1 d'infrastructure, administration, etc.)
 - Toute version hybride est vouée à l'échec

Architecture en bulles

Illustration : SI cartes de paiement

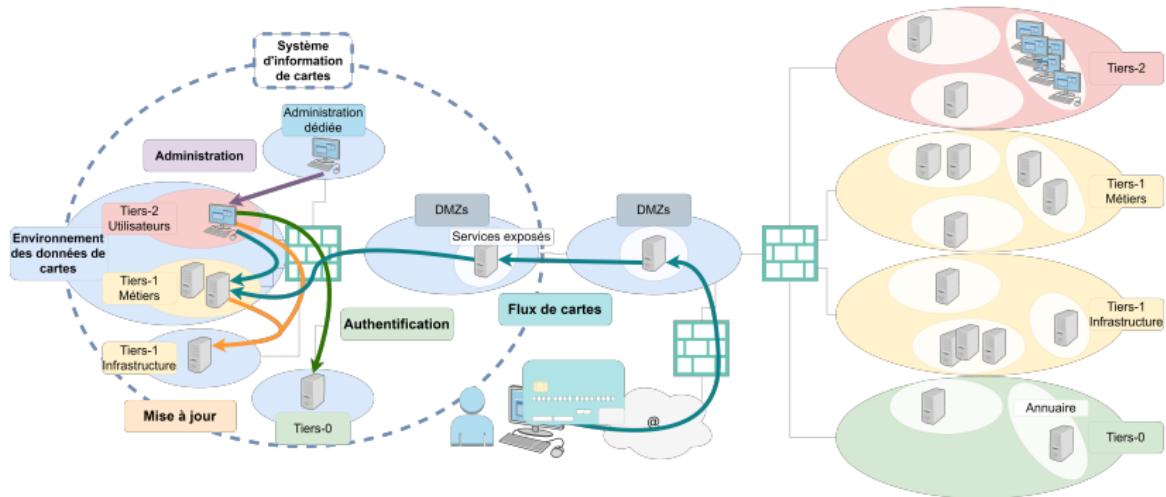


Figure – Architecture en bulles : système d'information PCI DSS

1	Bulles et tiers-{0-2}	284
2	Séparation des environnements	301
3	Administration, privilèges et relations de contrôle	308
4	Services d'infrastructure et de sécurité	370
5	Applications	444
6	Continuité	452



En opposition à l'environnement de production, on appellera les autres environnements hors production.

- Pré-production (*staging*)
- Intégration (*acceptance*)
- Homologation / test
- Développement
- [...]

- Quel tiers pour ces composants ?

- Serveur métier de production **1**
- Serveur de bases de données de développement **1**
- Bandes de sauvegarde **0**
- Site de continuité d'activité (*disaster recovery*) **0**

1/2



- Quel tiers pour ces composants ?
 - Serveur métier de production
 - Tiers-1
 - Serveur de bases de données de développement
 - Tiers-1 ou tiers-2 selon les cas
 - Bandes de sauvegarde
 - Tiers-0 ou tiers-1 selon les cas
 - Site de continuité d'activité (*disaster recovery*)
 - Tiers-*
 - Selon les bulles faisant partie du plan de continuité d'activité



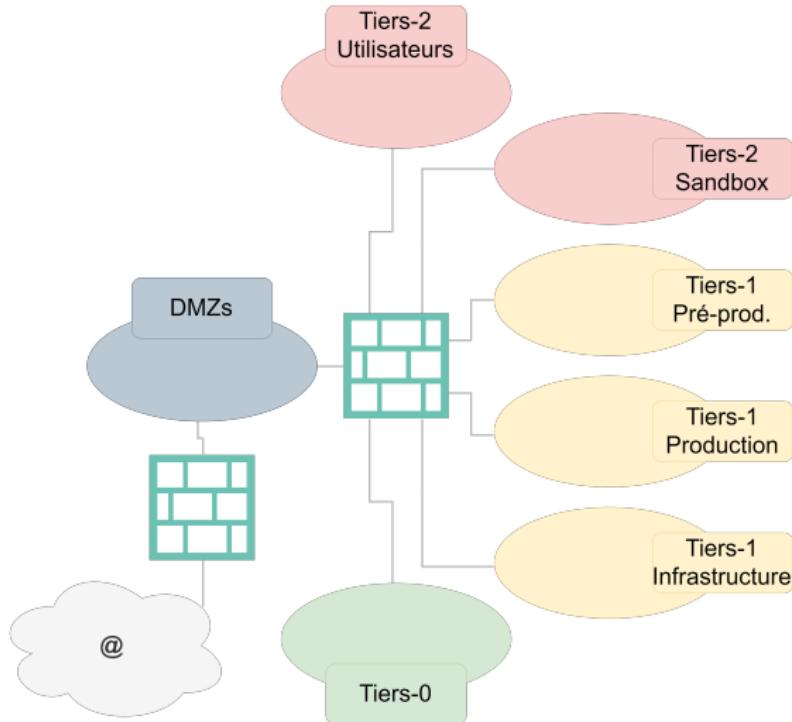


Figure – Architecture en bulles : séparation des environnements





- Cloisonnez votre SI en bulles
 - sur le principe de sensibilité
 - en cloisonnant/isolant les environnements hors production
 - en commençant par le plus sensible : le tiers-0
- Concevez une (ou plusieurs) DMZ
 - et assurez-vous qu'aucune ne peut être contournée

Administration, privilèges et relations de contrôle

1	Bulles et tiers-{0-2}	284
2	Séparation des environnements	301
3	Administration, privilèges et relations de contrôle	308
4	Services d'infrastructure et de sécurité	370
5	Applications	444
6	Continuité	452

3	Administration, privilèges et relations de contrôle	308
	Zones d'administration	309
	Qu'est-ce qu'un administrateur ?	321
	Illustration : Windows et Active Directory	325
	Postes d'administration	350

Que pensez-vous de cette situation ?

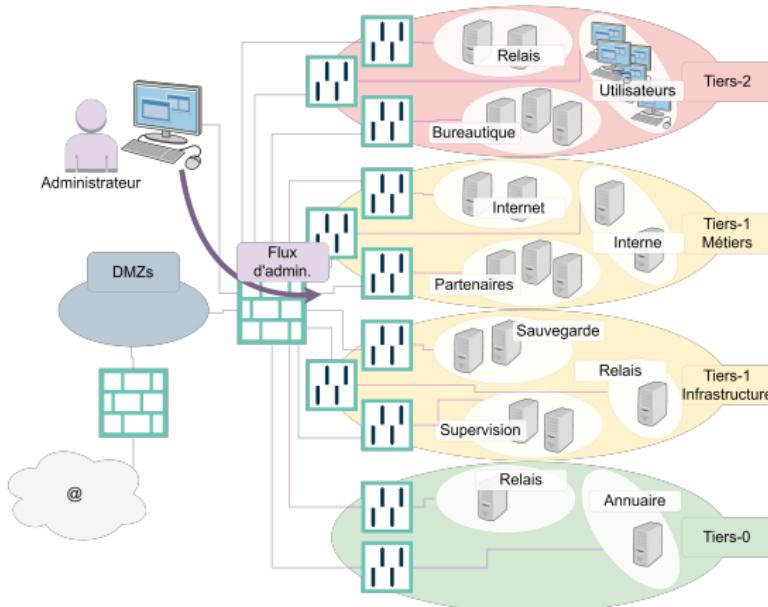


Figure – Administration : configuration par défaut





Exposition des interfaces d'administration

- Défense en profondeur : cloisonnement réseau des interfaces d'administration des composants
- Permet de réduire un risque en disponibilité
 - Si infrastructure de production indisponible, toujours la maîtrise de l'administration
 - Si infrastructure d'administration indisponible, production toujours disponible
- Principes
 - Interfaces réseau dédiées pour l'administration
 - Séparation des flux d'administration et de production

Que pensez-vous de cette (nouvelle) situation ?

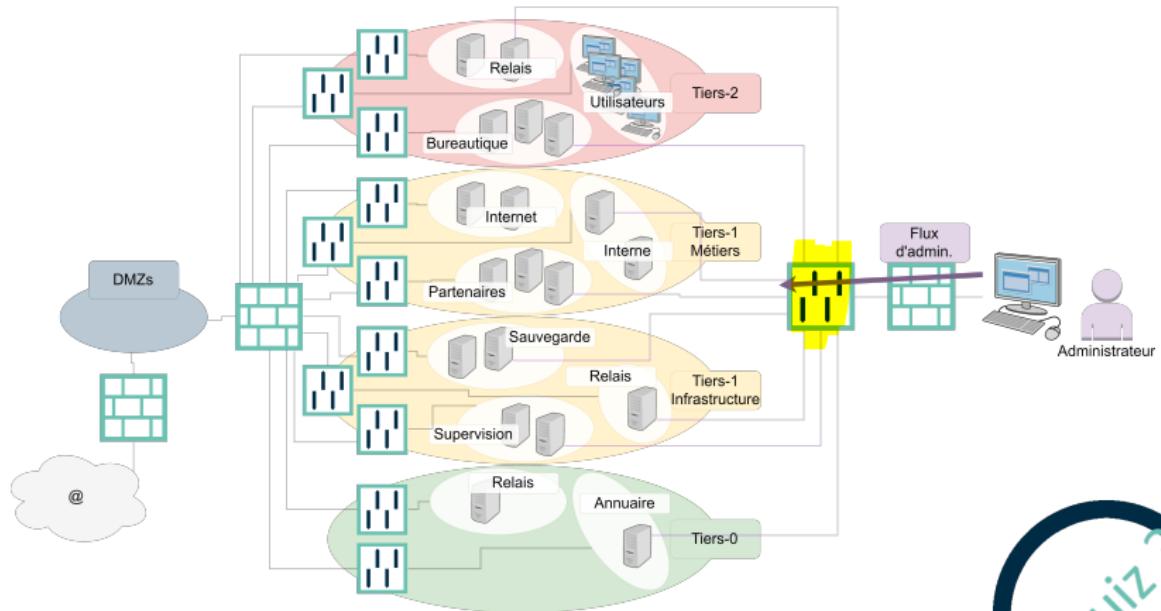


Figure – Administration : interfaces réseaux dédiées





1. Annihiler la segmentation



Une zone ⇒ sa zone d'administration



Sécurité du lien local (entre les ressources administrées)



2. Erreur de configuration des services : écoute sur toutes les interfaces
3. Erreur de configuration réseau : service utilisant la mauvaise interface



- **Auditer !**
- Et configurer un pare-feu local sur les serveurs

- Problème : comment réaliser cette coupure ?
 - DNS sur interface de production ou interface d'administration ?
 - Les deux nécessitent potentiellement ce service

⇒ Choix à faire

- Les composants physiques ont des interfaces d'administration dédiées
 - iLO, iDRAC, IMM, IPMI, etc.
- Idem avec des commutateurs KVM



Zones dédiées

Bastion

Point central pour accéder aux interfaces d'administration
⇒ Accès CLI, déport d'affichage, interfaces web



- Segmentation / contrôle d'accès
- Journalisation
- Single Sign-On (SSO)



Points d'attention ?



- SPOF
 - Disponibilité
 - Secrets d'authentification
- Contournable ?

- Idéal : système d'information d'administration
 - Référentiel d'authentification dédié
 - Services d'infrastructure et de sécurité dédiés
 - Supervision, sauvegarde, journalisation, etc.



...qui a sa bulle d'administration dédiée.

- Dans tous les cas :
 - Outils dédiés
 - Y compris partages de fichiers ou messagerie (déconnectée)

Zones d'administration

Schéma (final)

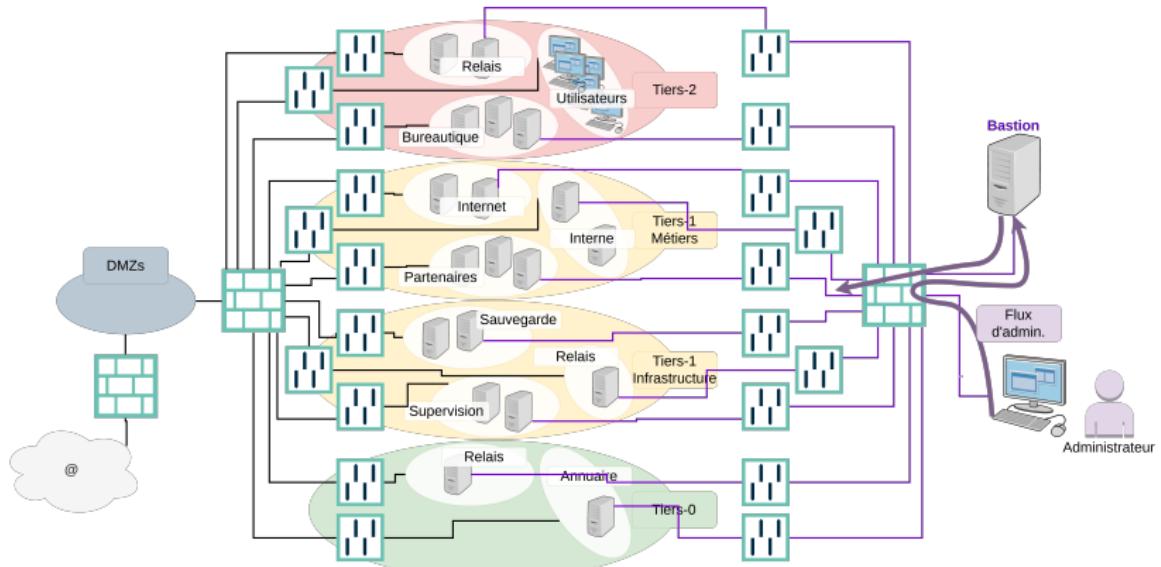


Figure – Administration : cloisonnement des interfaces d'administration et bastion

3	Administration, privilèges et relations de contrôle	308
	Zones d'administration	309
	Qu'est-ce qu'un administrateur ?	321
	Illustration : Windows et Active Directory	325
	Postes d'administration	350

Administrateur

Personne qui assure, en tant que responsable, le fonctionnement d'un service.

Utilisateur qui possède tous les pouvoirs sur le système.

- Compte d'administration
 - *root / Administrator*
- Groupe d'administration
 - Idem

C'est tout ?

```
jhe-user ALL = (ALL) /usr/bin/vim  
-rwsr-xr-x 1 root root 217K 2017-02-18 16:37 /usr/bin/find  
my.sh = cap_setuid+ep
```

Privilège, droit, permission?...

- **Permission** : contrôle d'accès lié à un objet (ACL)
 - Sur tout type d'objets : fichiers, attributs AD, GPO...
 - Basiques : lire, écrire, exécuter
 - Ou selon l'objet : lire tel attribut, déléguer, etc.
- **Privilège** : action autorisée sur le système
 - Lié à un principal
 - Débuguer, charger des pilotes, usurper une identité...
- **Droit** : façon de se connecter à un système
 - Localement, Remote Desktop, restrictions horaires...

Un administrateur est simplement un utilisateur qui a :
Des droits, des priviléges, accès à des objets

3	Administration, privilèges et relations de contrôle	308
	Zones d'administration	309
	Qu'est-ce qu'un administrateur ?	321
	Illustration : Windows et Active Directory	325
	Postes d'administration	350

- Les objets sous Active Directory sont classés dans plusieurs arborescences distinctes
 - Site, forêt, domaine, UO, groupes...
- Le périmètre de sécurité d'un Active Directory est la **forêt**, pas le domaine
 - Détermine le champ d'action des administrateurs



- Tous les domaines d'une même forêt se font confiance
⇒ Un domaine compromis menace toute la forêt

= Chemins d'authentification

- Implicite entre les domaines d'une forêt
- **Forest** : entre des forêt distinctes
- **External** : domaine situé dans une forêt distincte
- **Realm** : pour lier 2 royaumes Kerberos AD et non-AD
- **Shortcut** : pour accélérer l'authentification entre 2 domaines "feuilles" d'une forêt
- Bi- ou Uni-directionnel ($A \Rightarrow B$: B accède aux ressources de A)
 - Transitivité : Si $A \Rightarrow B$ et $B \Rightarrow C$, alors $A \Rightarrow C$
- Périmètre d'authentification
 - Forêt : accès à toutes les ressources de la forêt cible
 - Domaine : limité au domaine cible
 - Authentification selective (si rel. inter-forêts ou externes)
 - L'accès à chaque ressource doit être explicitement autorisé

- Rappel : un utilisateur ayant certains privilèges peut usurper n'importe quel utilisateur de la machine
- En fonction :
 - Des systèmes administrés
 - Des relations de confiance
 - De la configuration des machines (délégation, etc.)
 - Et de bien d'autres facteurs...

⇒ Un compte peut prendre le contrôle d'un autre
Potentiellement = **élévation de privilèges**

- Nécessité d'un cloisonnement **logique** entre les niveaux d'administration (en plus du cloisonnement réseau)
 - Un compte dédié par niveau
 - Restriction des interactions entre les niveaux

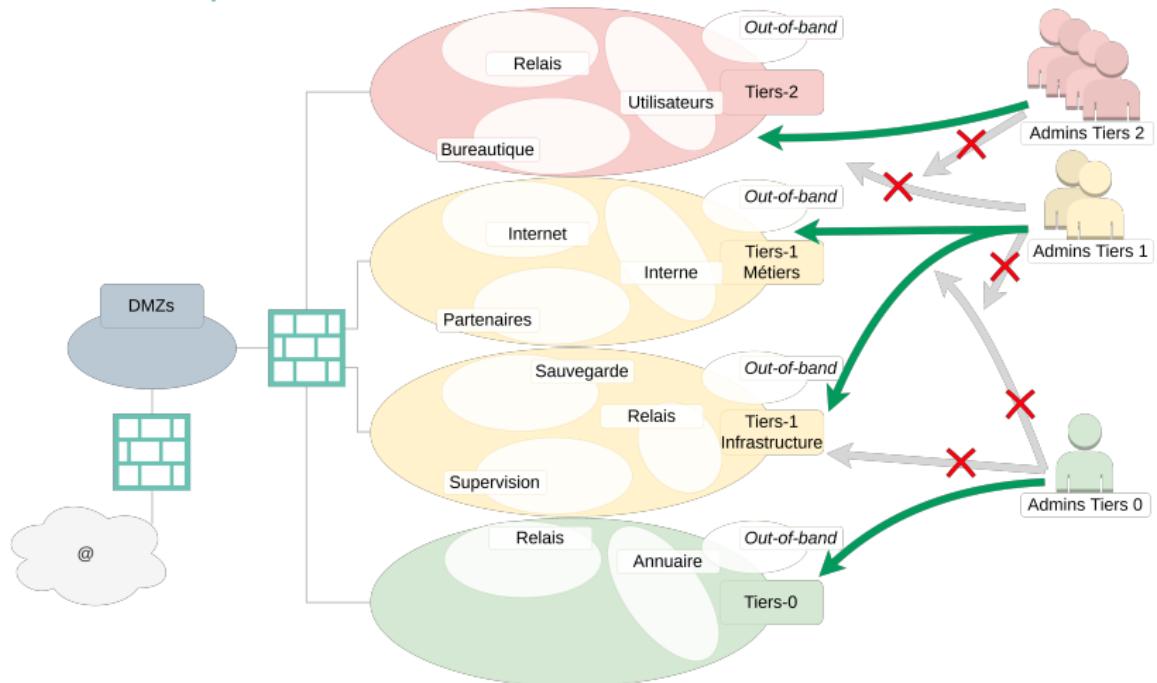


Figure – Niveaux d'administration

- **Tiers 0**

- Gère (contrôle) les équipements des tiers 0, 1, 2
- *Logon* sur des équipements tiers 0 uniquement

- **Tiers 1**

- Gère (contrôle) les équipements des tiers 1 et 2
- *Logon* interactif sur des équipements tiers 1 uniquement
- Accès non interactif aux services des tiers 0 et 1

- **Tiers 2**

- Gère (contrôle) les équipements du tiers 2
- *Logon* interactif sur des équipements tiers 2 uniquement
- Accès non interactif aux services des tiers 0, 1, 2

- Attention à la délégation non contrainte !

- Solution : *Account is sensitive and cannot be delegated*

Plusieurs mécanismes pour isoler les niveaux entre eux

- Gestion de l'authentification
 - Gestion des droits
 - Stratégies et silos d'authentification
 - Forêt d'administration

- Regroupement des machines / utilisateurs à l'aide de groupes et d'UO¹⁵
- Appliquer les restrictions selon les groupes "Tiers N"
 - Deny logon locally (type 2)
 - Deny logon through Remote Desktop (type 10)
 - Deny access to this computer from the network (type 3)
 - Deny log on as a batch job (type 4)
 - Deny log on as a service (type 5)
- Solution la plus simple

15. Unité d'Organisation

Limitations

- Les droits ne se surchargent pas
 - Une GPO en aval peut écraser les "Deny Logon.."
 - "Forcer" la GPO en question peut régler ce point
- Plus gênant :
 - Si NTLM est utilisé, l'authentification a lieu AVANT la vérification des droits
⇒ Celui qui contrôle la machine cible récupère
 - Le mot de passe (si interactif)
 - Ou le défi réponse (si réseau)

- Kerberos Armoring (blindage Kerberos)
 - Implémentation de FAST¹⁶
 - Protection des échanges d'authentification des utilisateurs par une clef dérivée du mot de passe de la machine
 - Avantage : le KDC reçoit le TGT de la machine quand l'utilisateur s'authentifie
 - Il peut donc aussi filtrer en fonction de la machine source
`AllowedToAuthenticateFrom` (TGT)
`AllowedToAuthenticateTo` (ST)
- = Stratégies d'authentification

16. Flexible Authentication via Secure Tunneling

- **Silo d'authentification** = container pour des machines / utilisateurs / services
- Exemple d'utilisation :
 - Mettre les machines / utilisateurs / services du tiers 0 dans un silo
 - Lui rattacher la stratégie d'authentification suivante
Authentification des utilisateurs du silo possible seulement sur les machines du silo

Cloisonnement logique des niveaux d'administration

Stratégies et silos d'authentification

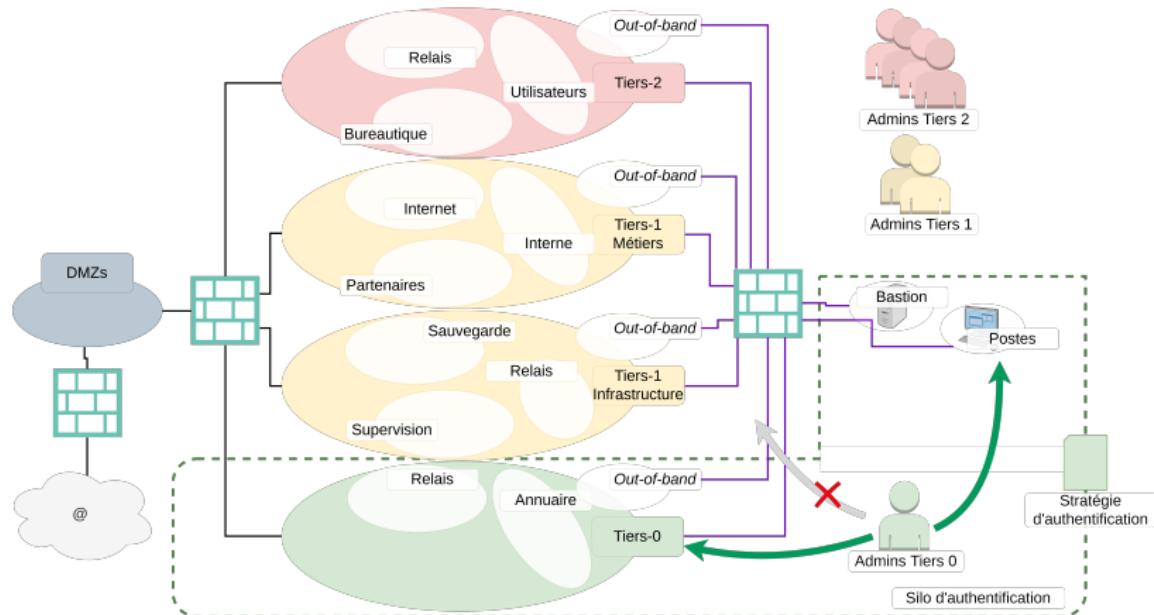


Figure – Stratégies et silos d'authentification

- Avantage :
 - Facilite la gestion de l'authentification
- Inconvénient :
 - Au niveau **compte** (impossible d'ajouter des groupes)
 - Vient **en complément** des mesures d'hygiène classiques

Cloisonnement logique des niveaux d'administration

Forêt bastion ou *Red Forest*

ESAE (Enhanced Security Administrative Environment)

- Forêt dédiée à l'administration (ADM)
- Peut être beaucoup mieux durcie que la forêt PROD
- Les admins n'ont pas de privilège sur la forêt d'administration
 - Shadow Principals (win2016+) : copie "miroir" de comptes et groupes d'une autre forêt
 - Privilèges temporaires pour administrer PROD
 - La forêt PROD a une relation "*PIM*¹⁷ trust" vers ADM
- Potentiellement couplé
 - Au JiTA (Just in Time Admin) et JEA (Just Enough Admin)
 - À MIM¹⁸ pour des workflows d'attribution des privilèges

17. Privileged Identity Management

18. Microsoft Identity Management

Cloisonnement logique des niveaux d'administration

Forêt bastion ou *Red Forest*

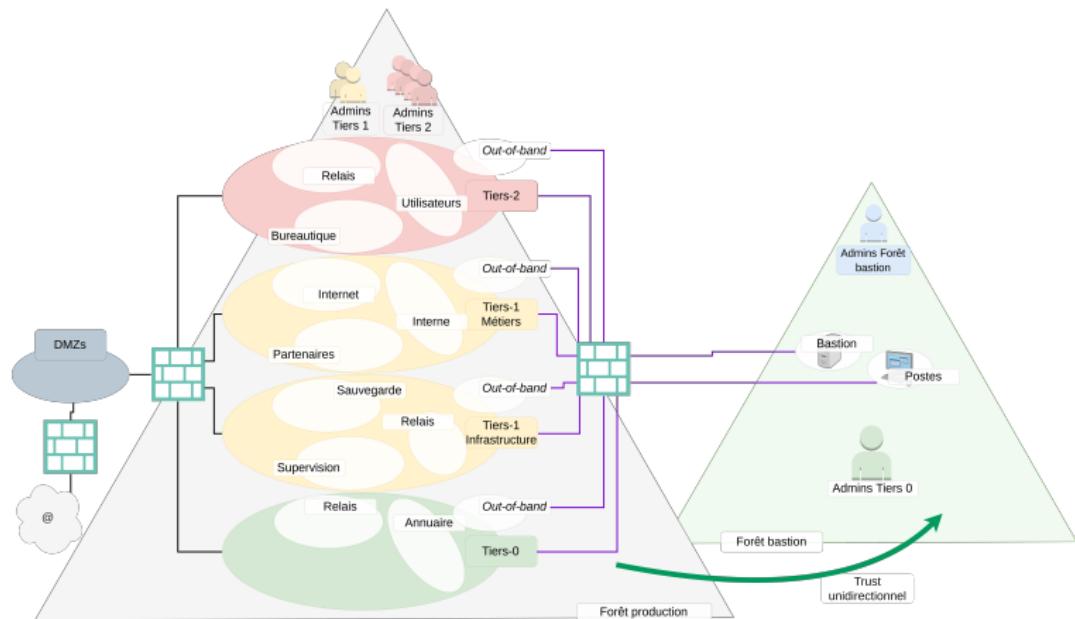


Figure – Forêt d'administration

Cloisonnement logique des niveaux d'administration

Forêt bastion ou *Red Forest* - Remarques

- Incompatible avec certaines applications / usages
- Si utilisé sur des utilisateurs (au lieu des groupes), s'apparente un peu à de la sécurité par l'obscurité :
 - Les administrateurs ne font plus partie du groupe *Domain Admins*, mais d'une UO/groupe "tier 0", "priv", "Red"...
⇒ L'attaquant les trouvera
- N'apporte presque rien si pas de *Tiering* en PROD
 - Sans doute un petit plus si utilisé complètement (MIM, JiTA)
- Finalement présenté¹⁹ comme
 - Un moyen de "nettoyer" un AD compromis
 - Ou d'administrer un environnement multi-forêts

19. Voir les commentaires de Marcin Krzanowicz sur
<https://blogs.technet.microsoft.com/389thoughts/2017/06/19/ad-2016-pam-trust-how-it-works-and-safety-advisory/>

Les restrictions sur l'authentification sont appliquées.
Victoire ?

- **Non**, ce n'est pas suffisant. Principe *clean source* :
 - Maitriser les **relations de contrôle** entre les objets
 - Utilisateur A \Rightarrow a des privilèges sur la machine B
 - Permissions sur objet O \Leftarrow donnent le contrôle à C
 - Clef USB \Rightarrow sert à installer une machine
 - Etc.

- Seul moyen d'auditer **une partie** de ces liens : utiliser un outil spécialisé basé sur les graphes
 - Bloodhound²⁰
 - AD-Control-Paths²¹
- Exemple avec Bloodhound : 2 phases
 - Récupération d'informations (utilisateur privilégié ou non)
 - Script SharpHound.ps1²² (ou bloodhound.py²³)
 - Analyse des données (hors ligne)
 - Base de données Neo4j + GUI Javascript



20. <https://github.com/adaptivethreat/Bloodhound>

21. <https://github.com/ANSSI-FR/AD-control-paths>

22. <https://github.com/BloodHoundAD/BloodHound>

23. <https://github.com/fox-it/BloodHound.py>

Types d'*ingestors* et données recueillies :

- **Connexion au DC seulement**

- Group - Appartenance aux groupes globaux
- GPOLocalGroup - Groupe local "Administrators" par les GPO
- ObjectProps - Propriétés de tous les utilisateurs/machines
- Container - Structure des UO et GPO associées
- Trusts - Relations de confiance
- ACL - Permissions sur tous les objets
- DCOnly - Group + Trusts + ACL + ObjectProps + Container + GPOLocalGroup

- Connexion à de nombreuses machines
 - LocalAdmin - Groupe local "Administrators"
 - DCOM - Groupe local "Distributed COM Users"
 - RDP - Groupe local "Remote Desktop Users"
 - Session - Enumération des sessions
 - SessionLoop - Enumération continue des sessions
 - LoggedOn - Enumération des sessions (nécessite des priviléges)
 - ComputerOnly - Session + LocalAdmin
 - LocalGroup - LocalAdmin + DCOM + RDP
- Default - Trusts + Session + Group + LocalAdmin
- All - Tout sauf GPOLocalGroup et LoggedOn

Cloisonnement logique des niveaux d'administration

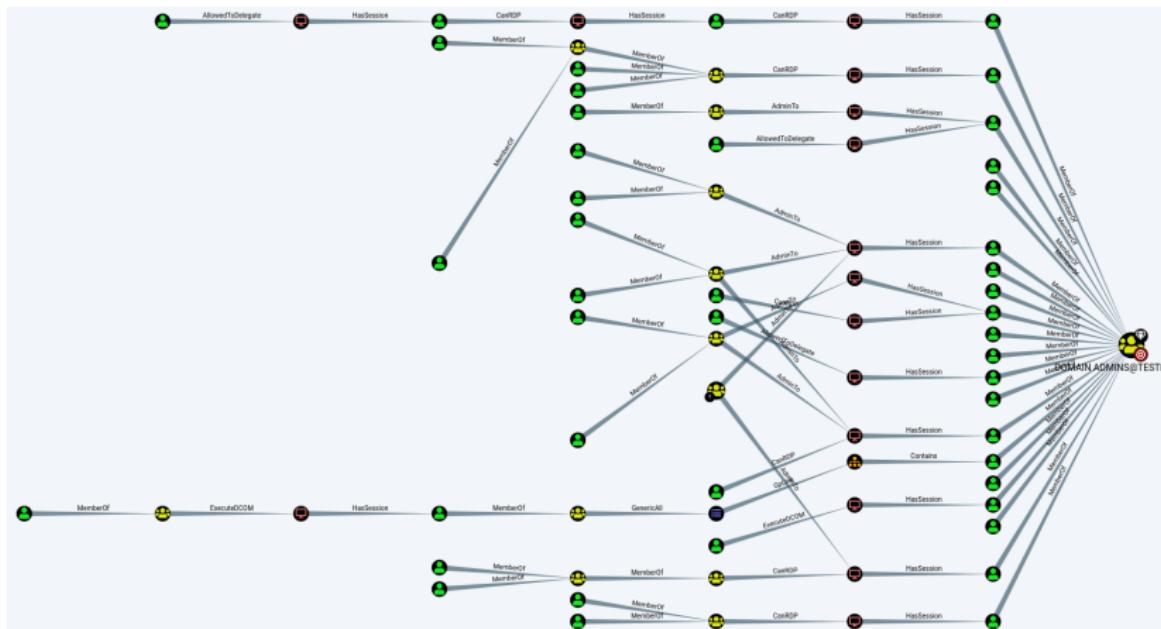


Figure – Exemples de chemins d'attaque

Cloisonnement logique des niveaux d'administration

Chemins de contrôle

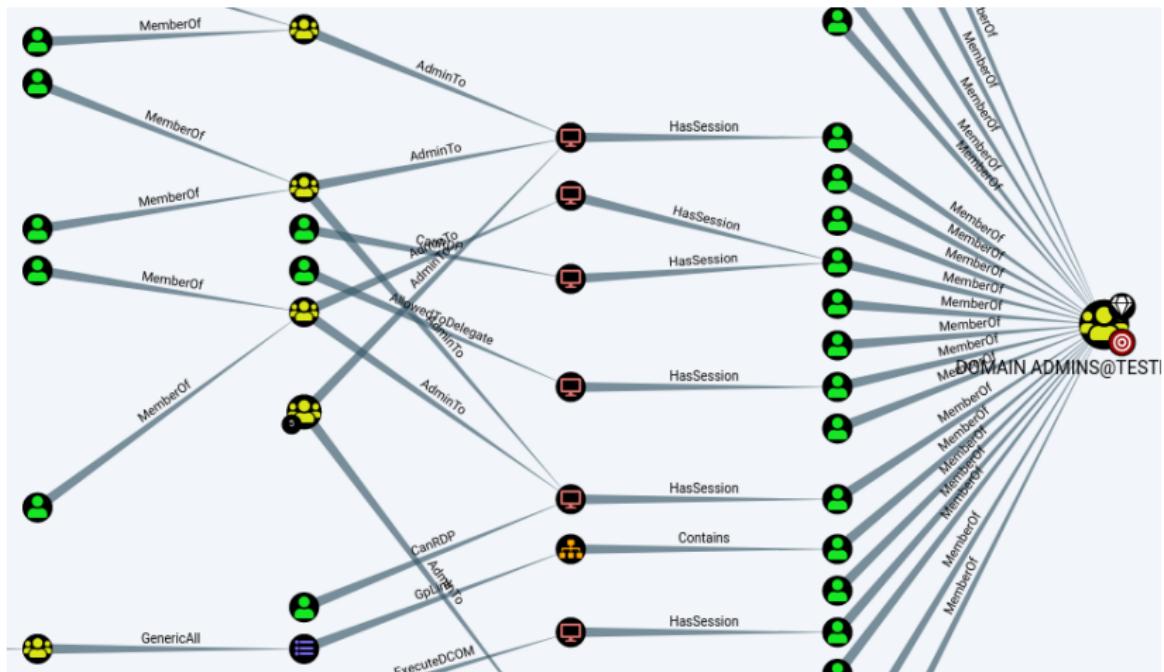


Figure – Exemples de chemins d'attaque

Types de relations :

- Défaut
 - MemberOf
 - HasSession
 - AdminTo
 - TrustedBy
- Containers
 - Contains
 - GpLink
- Autres
 - CanRDP
 - ExecuteDCOM
 - AllowedToDelegate
- ACL
 - AllExtendedRights
 - AddMember
 - ForceChangePassword
 - GenericAll
 - GenericWrite
 - Owns
 - WriteDACL
 - WriteOwner
 - ReadLAPSPassword

Que reste-t-il à faire ?

- En tant qu'attaquant :
 - En fonction du graphe et des comptes déjà compromis, suivre le chemin le plus facile
 - Pas forcément discret, mais presque imparable : (
- En tant que défenseur :
 - Tenter de scier un maximum de branches
 - Relancer l'outil régulièrement
 - Surveiller l'apparition de nouvelles pousses

Ce n'est pas tout...

- D'autres chemins de contrôle existent :
 - Mise à jour
 - Sauvegarde
 - Gestion de configuration
 - Outils d'inventaire
 - Console antivirus / suites de sécurité
 - Scanners de vulnérabilité
 - Etc.

3	Administration, privilèges et relations de contrôle	308
	Zones d'administration	309
	Qu'est-ce qu'un administrateur ?	321
	Illustration : Windows et Active Directory	325
	Postes d'administration	350



- Privilèges importants sur les biens supports (métiers)
- Exposition des biens essentiels
 - Potentiel de nuisance important



- Vol d'authentifiants d'administration =
 - Compromission de l'ensemble des SI
 - PKI, AD, etc. irrécupérables



D'où la nécessité de séparer l'administration de chaque tiers.

- Administration de l'administration ?
 - Toujours au sein de la même bulle !
 - Ou d'une bulle de même niveau

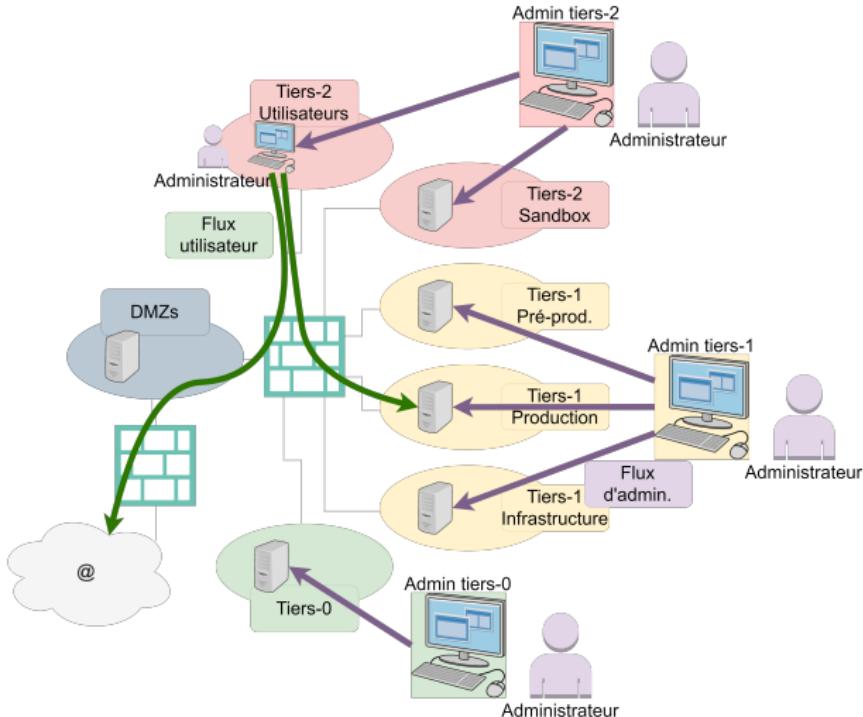


Figure – Architecture d'administration : segmentation des postes

- Idéal :
 - Poste d'administration dédié à chaque bulle
 - Poste utilisateur bureautique (accès Internet, etc.)
- Moins idéal mais correct :
 - Poste d'administration dédié pour le tiers-0
 - Cela représente moins d'une dizaine de personnes
 - Poste d'administration mutualisé tiers-1 et tiers-2
 - Poste utilisateur "bureautique"

- Solution *discount* :
 - Poste d'administration dédié en "tiers-0,5"
 - Poste utilisateur "bureautique"
 - Impossible de mutualiser les comptes d'administration des différentes bulles
 - administration tiers-0 (référentiel centralisé / administration du domaine)
 - administration tiers-1 (un ou plusieurs)
 - administration tiers-2 (postes de travail)
 - utilisation *standard* (faibles priviléges)

- Particulièrement dans le cas de cette solution *discount*, mesures complémentaires nécessaires :
 - Au minimum : contrôler quel compte peut se connecter à quelle machine
 - Exemple sous Windows :
 - Silos d'authentification
 - Restriction des droits (*Allow/Deny logon from network*, *Allow/Deny logon interactively*, etc.)

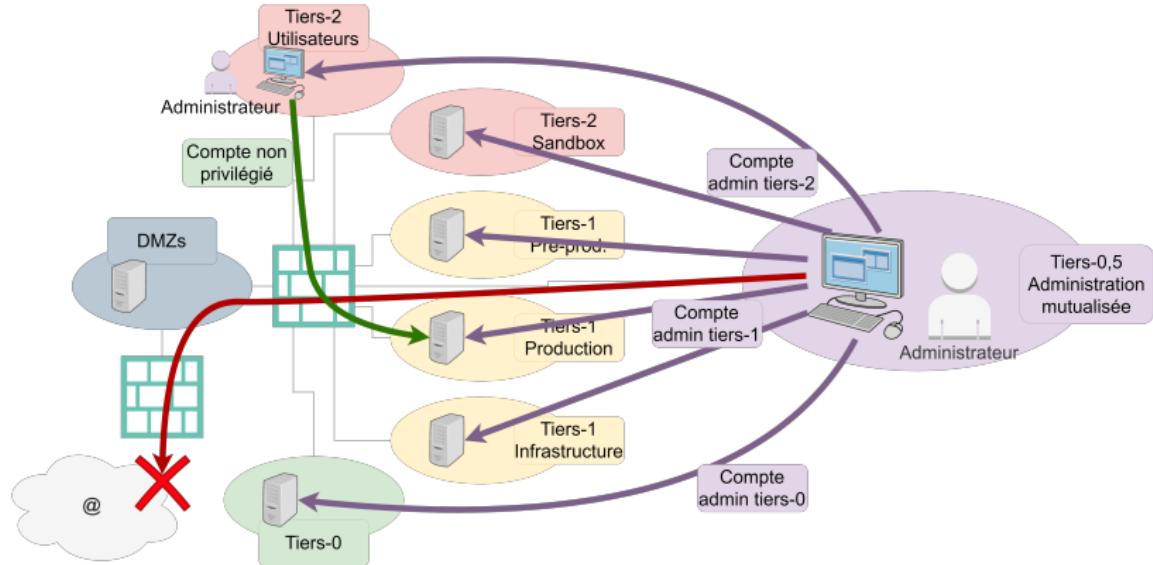


Figure – Architecture d'administration : proposition de poste mutualisé

- Unique poste bureautique et d'administration en tiers-0
- Unique poste bureautique et d'administration en tiers-2



- Unique poste bureautique et d'administration en tiers-0
 - Accès libre à Internet depuis le tiers-0



Augmentation drastique du niveau d'exposition donc de risque

- Unique poste bureautique et d'administration en tiers-2
 - Propagation d'authentifiants du tiers-0 en tiers-2



Perdu

- Hôte bureautique avec machine virtuelle d'administration
- Hôte d'administration avec machine virtuelle bureautique



- Hôte bureautique avec machine virtuelle d'administration



Compromission de la machine bureautique ⇒ compromission de l'administration

- Hôte d'administration avec machine virtuelle bureautique



Faiblesse du cloisonnement du mécanisme de virtualisation^{h i j}

- Poste d'administration multi-niveaux
 - Virtualisation/conteneurisation
 - Au niveau système/noyau

- Hôte bureautique et connexion vers un bureau virtuel d'administration
- Hôte d'administration et connexion vers un bureau virtuel bureautique



- Hôte bureautique et connexion vers un bureau virtuel d'administration



Compromission du poste bureautique ⇒ compromission de l'administration

- Hôte d'administration et connexion vers un bureau virtuel bureautique



RCE à travers le protocole de connexion^{k l m}

- Hôte d'administration et connexion vers un bureau virtuel bureautique



- Désactivation des fonctions d'échange (copier/coller, partage d'écran, prise en charge des périphériques, partages réseaux, etc.)
- Filtrage des flux
- Différenciation des annuaires bureautique et d'administration



Dans tous les cas, d'autres mesures s'appliquent

- Authentification sur le réseau d'administration
- Minimisation, durcissement des systèmes d'exploitation
- Restriction des priviléges sur le poste d'administration
- Etc.
- Et surtout : **aucune connectivité avec Internet !**





- Isolez les environnements bureautique et d'administration
- Cloisonnez les comptes d'administration selon les tiers/bulles
 - Pas de compromis pour le tiers-0 !
- Segmentez les réseaux *out-of-band*
- Séparez les réseaux d'administration de ceux de production

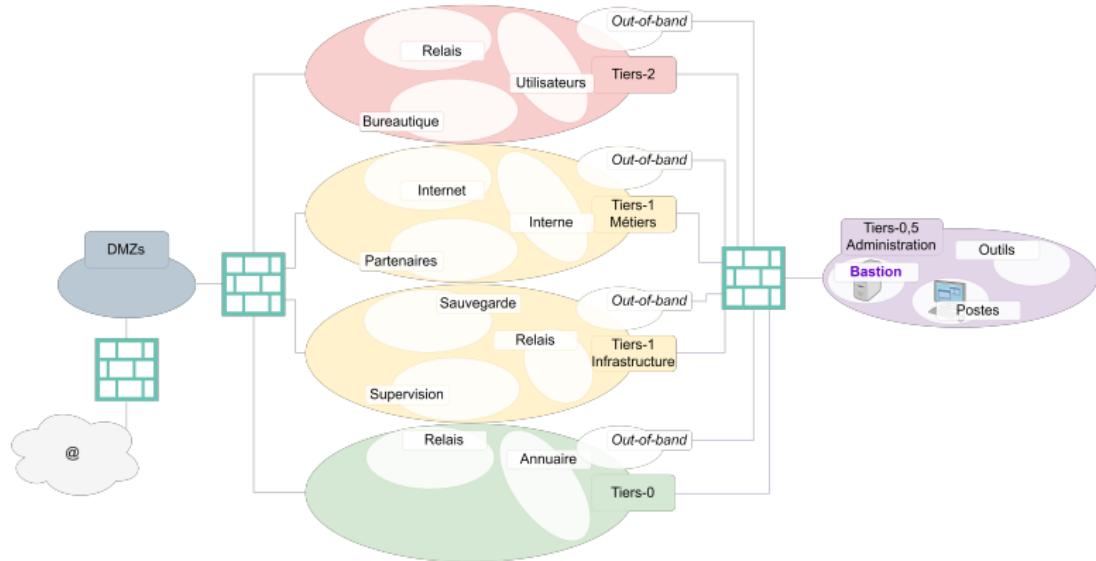


Figure – Architecture d'administration : cloisonnement réseau

1	Bulles et tiers-{0-2}	284
2	Séparation des environnements	301
3	Administration, privilèges et relations de contrôle	308
4	Services d'infrastructure et de sécurité	370
5	Applications	444
6	Continuité	452

4 Services d'infrastructure et de sécurité	370
Services de récupération ascendante (distribution)	371
Services de transmission ascendants et descendants	386
Cas de la résolution de nom	392
Cas de la supervision	403
Cas de la sauvegarde	411
Cas de l'accès Internet	419
Cas du VPN utilisateur	430
Interconnexion avec les sous-traitants	436

Services d'infrastructure de récupération ascendante

Principes

- Utilisant une source de confiance externe
 - Généralement sur Internet
- Services de noms, de temps, de mise à jour (systèmes, bibliothèques, bases de signature, etc.)
- Utilisent un relais interne basé sur une ou plusieurs sources externes



1. Menaces sur la source de confiance / *man-in-the-middle* sur Internet



- Disponibilité
 - Redondance, multiplication des sources de confiance
- Intégrité et confidentialité
 - Repose largement sur le protocole utilisé
 - Authentification, signature, chiffrement
- Parfois d'autres mesures sont possibles en internalisant le référentiel
 - NTP avec horloge GPS



2. Compromission du relais interne ayant des impacts sur le service



- Mécanismes supportés par le protocole
- Segmentation du relais interne selon les bulles

Segmentation des relais internes de récupération ascendante

Mode isolé



Segmentation du relais interne selon les bulles : mode isolé

- Une bulle = un relais
- Chaque relais consomme le service sur une source externe (éventuellement tous la même)



Peu de mutualisation : coûte cher

Risques résiduels

- Désynchronisation NTP entre les différentes bulles
 - Kerberos KO
- Complexité d'exploitation
 - Exemple DNS
 - Le référentiel d'authentification a un nom de domaine
 - Donc duplication des entrées DNS sur les relais des tiers supérieurs ?
 - ⇒ Même complexité que gérer des fichiers hosts

Segmentation des relais internes de récupération ascendante

Exemple de la mise à jour

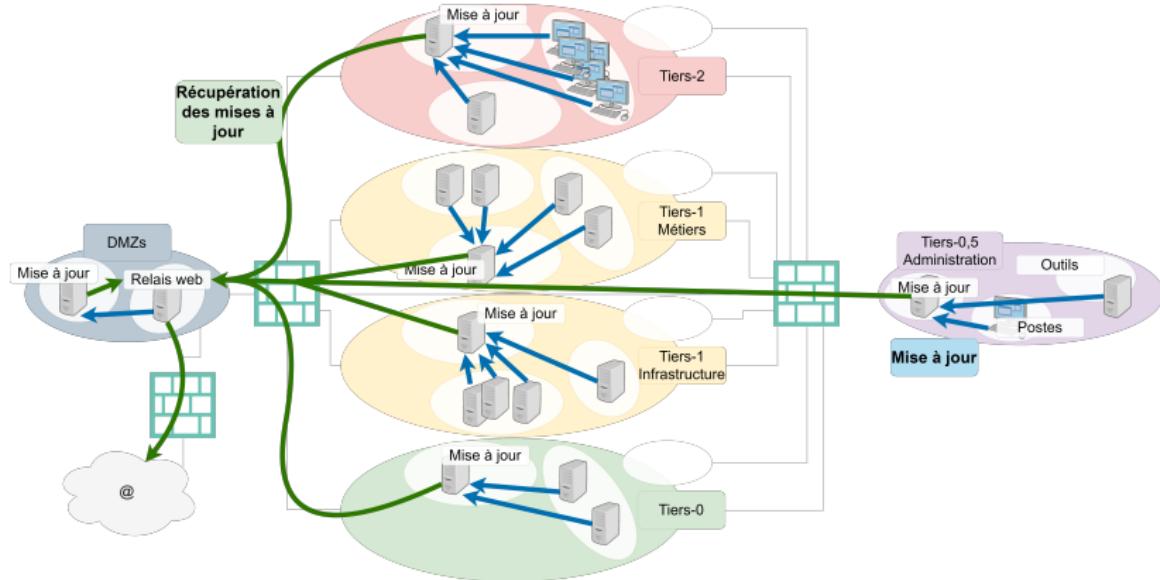


Figure – Mise à jour : proposition 1

Segmentation des relais internes de récupération ascendante

Mode hiérarchique



Segmentation du relais interne selon les bulles : mode hiérarchique

- Une bulle = un relais
- Hiérarchie des relais : cas 1 ($T2 \rightarrow T0$)
 - Relais de tiers-0 sert le tiers-0 et le relais de tiers-1
 - Relais de tiers-1 sert le tiers-1 et le relais de tiers-2
 - Relais de tiers-2 sert le tiers 2
 - Pourquoi pas l'inverse (cas 2)?
 - Tiers-0 → tiers-1 → tiers-2

Segmentation des relais internes de récupération ascendante

Mode hiérarchique



- Cas 1 ($T_2 \rightarrow T_0$) : exploitation d'une vulnérabilité du service provoquant la compromission du relais de plus bas niveau (jusqu'au tiers-0)
 - CVE-2018-8626 Windows DNS Server Heap Overflow (10.0 CVSS)
- Cas 2 ($T_0 \rightarrow T_2$) : consommation de services fournis par des tiers de plus haut niveau (donc d'un niveau de sécurité moindre)
 - Compromission du WSUS de tiers-2 et altération des mises à jour déployées en tiers-0 (WSUSPectⁿ, WSUSpendu^{o p})

Segmentation des relais internes de récupération ascendante

Mode hiérarchique



Principe de cohérence : consommer un service de tiers supérieur revient à diminuer le niveau de sécurité de la bulle qui utilise le service



- Cas 1 ($T_2 \rightarrow T_0 \geq$ cas 2 ($T_0 \rightarrow T_2$))
 - Idéal : diode
 - Irréaliste
 - Réalité : minimisation, filtrage et analyse des flux
 - Sondes, WAF, etc.
- Cas 2 : N/A

Segmentation des relais internes de récupération ascendante

Mode hybride



Exploitation d'une vulnérabilité du service provoquant la compromission du relais de plus bas niveau

- Principe de prudence (défense en profondeur)



- Isolation des bulles/zones de sensibilité plus importante
 - Ces bulles consomment le service sur Internet
 - Hybride hiérarchique / isolé

Segmentation des relais internes de récupération ascendante

Exemple de la mise à jour

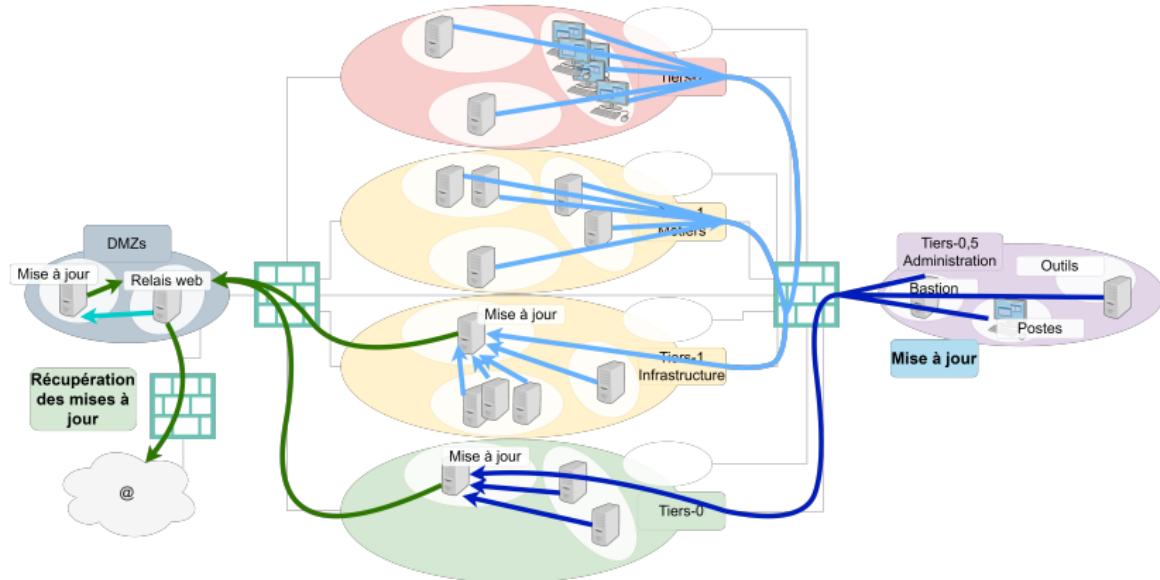


Figure – Mise à jour : proposition hybride (1)

Segmentation des relais internes de récupération ascendante

Exemple de la mise à jour

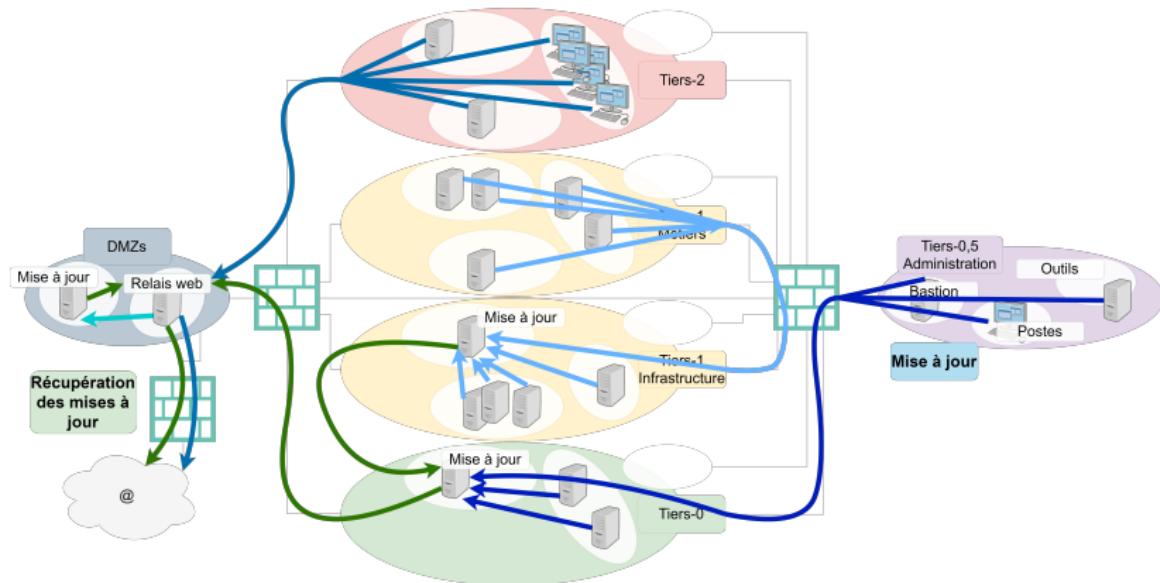


Figure – Mise à jour : proposition hybride (2)

Segmentation des relais internes de récupération ascendante

Exemple de la mise à jour

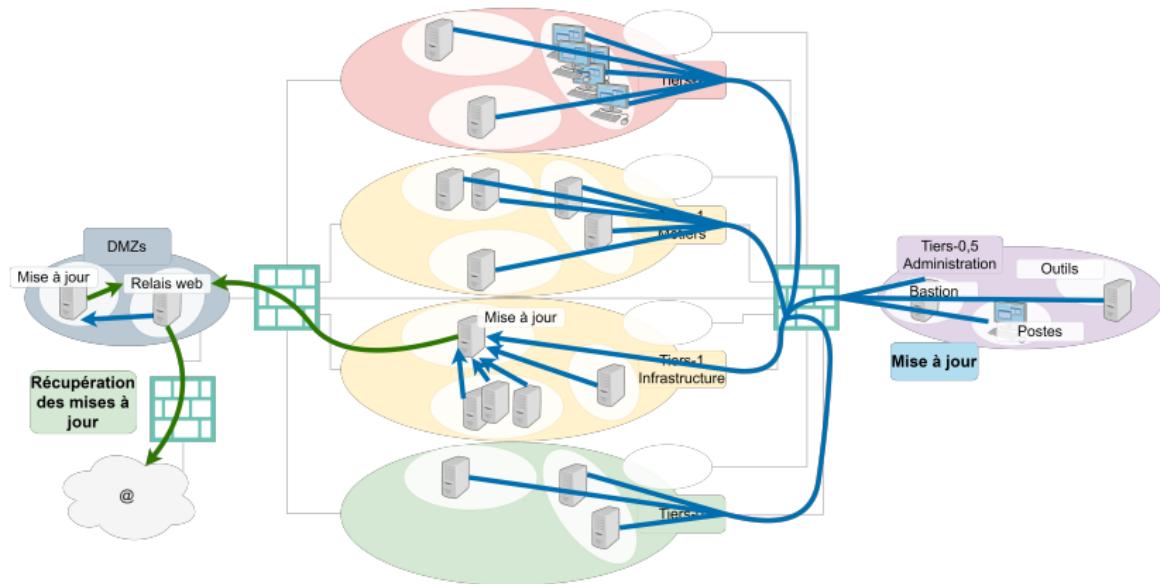


Figure – Mise à jour : (mauvaise) proposition hybride (3)

Segmentation des relais internes de récupération ascendante

Conclusion

- Architecture dépend des services
 - NTP, DNS nécessitent une homogénéité du service et vraisemblance d'une RCE moindre
 - Plutôt mode hiérarchique vers les tiers inférieurs
 - Pour Windows : pas le choix, il faut un DNS proche du contrôleur de domaine (en tiers-0)
 - Mise à jour
 - Plutôt mode hybride

Qu'en est-il des services de récupération en mode descendant (centralisation) ?



4 Services d'infrastructure et de sécurité	370
Services de récupération ascendante (distribution)	371
Services de transmission ascendants et descendants	386
Cas de la résolution de nom	392
Cas de la supervision	403
Cas de la sauvegarde	411
Cas de l'accès Internet	419
Cas du VPN utilisateur	430
Interconnexion avec les sous-traitants	436

Mode ascendant : centralisation

- Architecture dépend de la sensibilité de l'information transmise
 - Possible de se reposer sur un gestionnaire de service mutualisé en tiers inférieur
 - Exemple : tous les tiers centralisent leurs journaux en tiers-1

Mode descendant : distribution

- Exécution de commandes à distance inversée plus difficile
 - Donc globalement moins de risque (mais pas impossible)
 - Plutôt architecture hiérarchique vers les tiers supérieurs
 - Exemple : déploiement en SSH depuis le tiers-0



Accès vers l'ensemble du SI



Il n'y a pas qu'une architecture viable par mode de connexion

- Des pistes ont été présentées dans ce chapitre
 - Mais ces architectures ne peuvent doivent pas être systématisées
 - Dépend des protocoles, du fonctionnement des applications, des informations en transit, etc.

Mode ascendant : centralisation

- Architecture dépend de la sensibilité de l'information transmise
 - Possible de se reposer sur un gestionnaire de service mutualisé en tiers inférieur
 - Exemple : tous les tiers centralisent leurs journaux en tiers-1

Mode descendant : distribution

- Exécution de commandes à distance inversée plus difficile
 - Donc globalement moins de risque (mais pas impossible)
 - Plutôt architecture hiérarchique vers les tiers supérieurs
 - Exemple : déploiement en SSH depuis le tiers-0



Accès vers l'ensemble du SI



	Ascendant	Descendant
Centralisation	Transmission NSCA Service unique T1 Hiérarch. T2→T0	Récupération NRPE Hiérarch. T0→T2
Distribution	Récupération WSUS Hybride Hiérarch. T2→T0	Transmission Ansible Hiérarch. T0→T2

- Isolez les services d'infrastructure de la DMZ



Il n'y a pas qu'une architecture viable par mode de connexion

- Des pistes ont été présentées dans ce chapitre
 - Mais ces architectures ne peuvent doivent pas être systématisées
 - Dépend des protocoles, du fonctionnement des applications, des informations en transit, etc.

4 Services d'infrastructure et de sécurité	370
Services de récupération ascendante (distribution)	371
Services de transmission ascendants et descendants	386
Cas de la résolution de nom	392
Cas de la supervision	403
Cas de la sauvegarde	411
Cas de l'accès Internet	419
Cas du VPN utilisateur	430
Interconnexion avec les sous-traitants	436

La fonction

Obtenir les identifiants techniques des ressources à partir d'un nom intelligible.

Nom	Adresse multicast	Port	Commentaire
mDNS	0.0.251 / ::fb	5353/udp	résolution exclusive de .local
LLMNR	0.0.252 / ::fc	5355/udp-tcp	



Non sécurisé par défaut

Nom	Port	Version sécurisée	Port
DNS	53/tcp-udp	DNSSec DoT, DoH, DNSCurve, DNSCrypt	(récent)
MS-RPC DNS	135/tcp		
NIS (RPC)	135/tcp	NIS+	
NBT-NS / WINS	137/tcp		
LDAP	389/tcp	LDAPS	689/tcp
SMB	445/tcp	version \geq 2.3 en fonction d'options	

```
# /etc/nsswitch.conf
hosts:      dns nis files mdns
```



Est-ce normal ?

- Qu'un serveur en DMZ puisse résoudre les noms de domaines internes
- Qu'un poste de travail puisse résoudre les noms de domaines externes
- Qu'un serveur exclusivement interne puisse résoudre les noms de domaines externes



- Utiliser deux alternative DNS en interne :
 - Un interne
 - Un relais permettant de résoudre les noms internes et externes
- Utiliser un DNS interne pour la DMZ entrante
- Utiliser un DNS externe pour la DMZ sortante
- Limiter au maximum les serveurs pouvant résoudre à l'extérieur
- Faire transiter le trafic via un proxy

Résolution de nom

Déport de la résolution au proxy

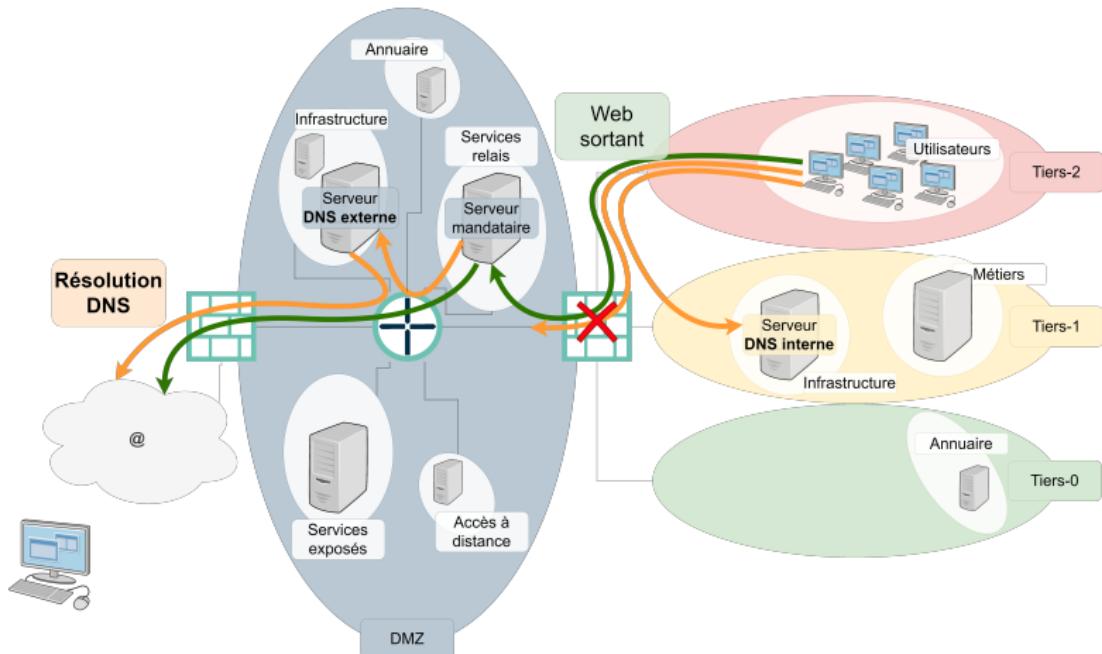


Figure – Résolution DNS par le proxy

Résolution de nom

Résolution DNS interne

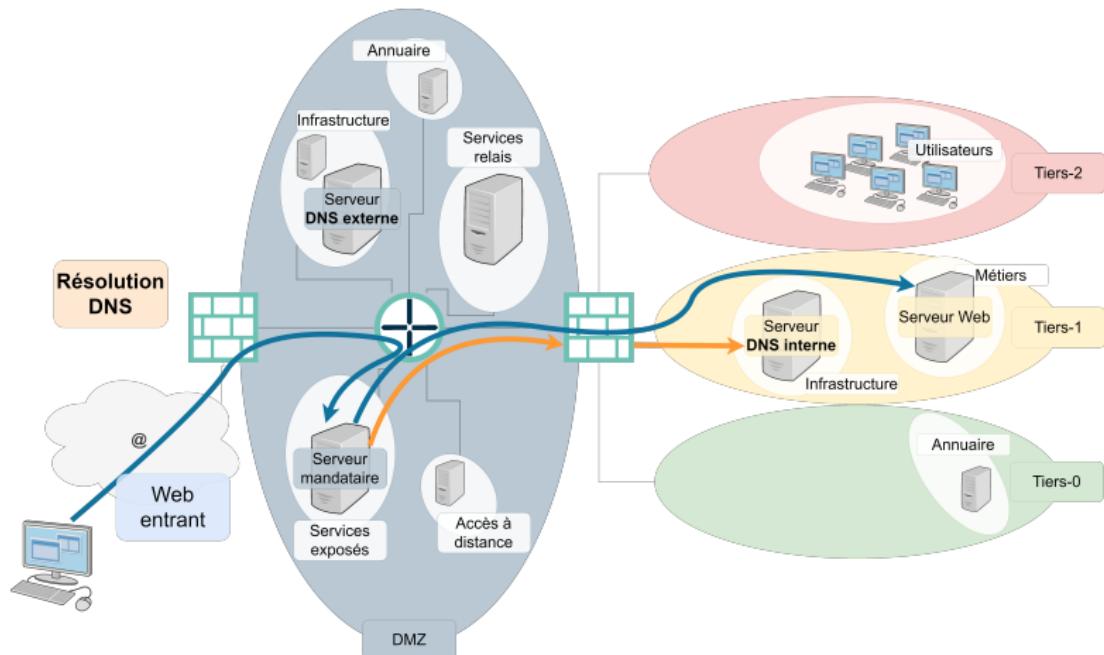


Figure – Résolution DNS interne



Attribuer les mêmes adresses IP pour un nom de domaine, quelle que soit la vue

C'est la source de nombreux maux de tête sinon.



Aucun logiciel DNS ne journalise les réponses DNS



Journaliser les requêtes et les réponses DNS via des outils dédiés

- Sur les serveurs DNS (difficile/impossible)
- Idéal : sonde *Passive DNS* interne
- A défaut : interroger des serveurs DNS passifs externes en cas d'incident

Ex : CIRCL (<https://www.circl.lu/services/passive-dns/>)

4 Services d'infrastructure et de sécurité	370
Services de récupération ascendante (distribution)	371
Services de transmission ascendants et descendants	386
Cas de la résolution de nom	392
Cas de la supervision	403
Cas de la sauvegarde	411
Cas de l'accès Internet	419
Cas du VPN utilisateur	430
Interconnexion avec les sous-traitants	436

La fonction

Déetecter le dysfonctionnement de services.



Accès très privilégiés sur l'ensemble du SI



Limiter les pouvoirs de chaque sonde



- Comptes de services dédiés
- Minimisation des privilèges

Exemple avec une configuration sudoers :

```
# Aucun argument
nrpe-user  ALL=(root)  NOPASSWD: /path/to/script ""
# Arguments spécifiques
nrpe-user  ALL=(root)  NOPASSWD: /path/to/script
                           --arg1 "value" --arg2 "value"
```



Fuite d'informations

- Le service collectant les informations a essentiellement des informations d'architecture
 - Il convient de s'en assurer

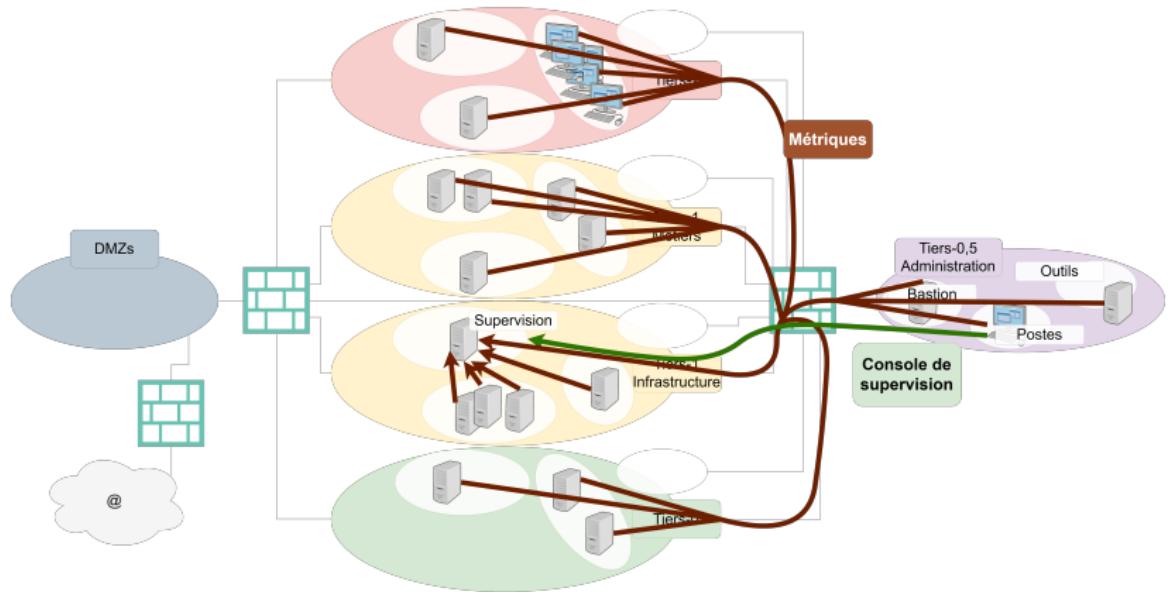


Figure – Architecture de supervision

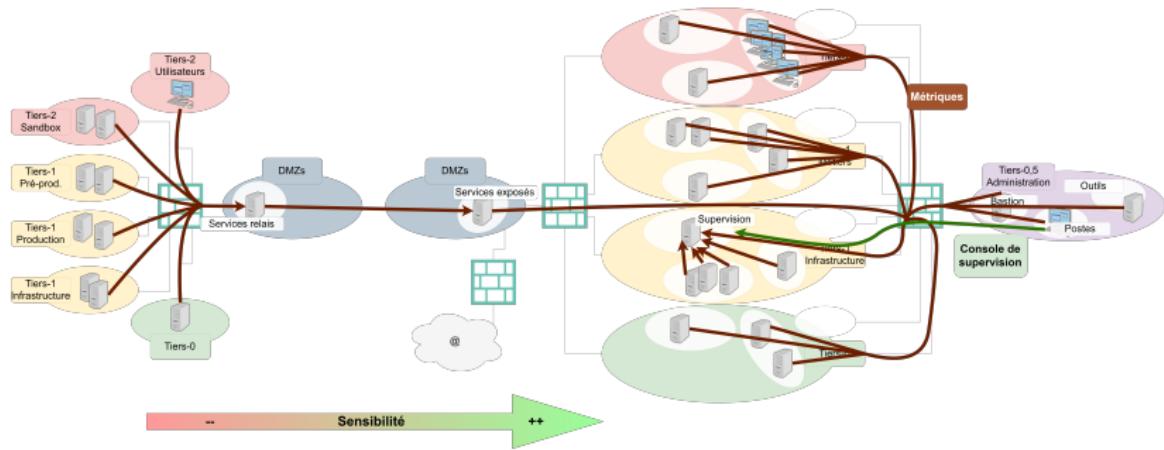


Figure – Architecture de supervision centrale (1)



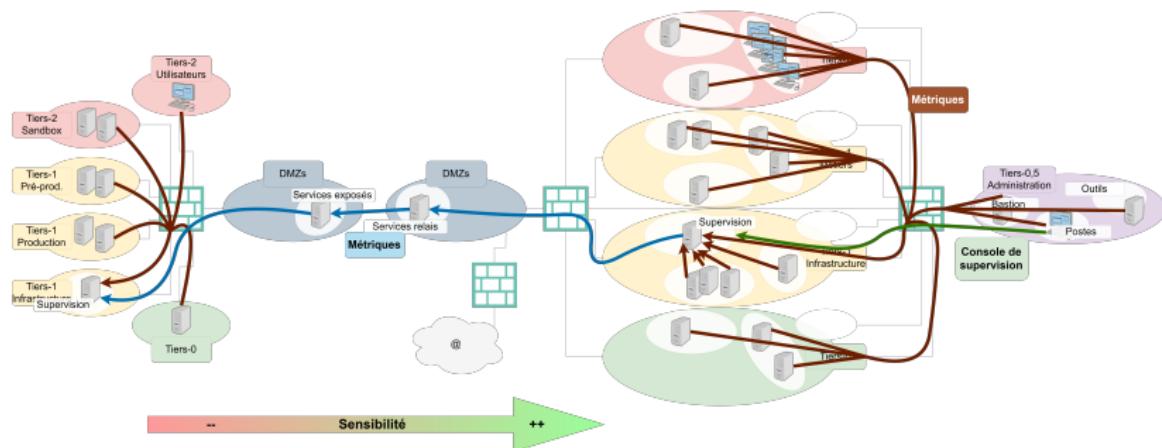


Figure – Architecture de supervision centrale (2)

4 Services d'infrastructure et de sécurité	370
Services de récupération ascendante (distribution)	371
Services de transmission ascendants et descendants	386
Cas de la résolution de nom	392
Cas de la supervision	403
Cas de la sauvegarde	411
Cas de l'accès Internet	419
Cas du VPN utilisateur	430
Interconnexion avec les sous-traitants	436

- Sauvegarde locale (via un gestionnaire de version)
- Sauvegarde par snapshot de VM
- Sauvegarde centralisée
 - Avec l'extraction hors-ligne de certaines



Attention à l'intégrité des bases de données



Attention à la démagnétisation des bandes



Attention à la gestion des clefs de chiffrement des sauvegardes

- Permet d'ordonnancer au mieux les sauvegardes
- Optimise les ressources disques (I/O) et la bande passante
- Facilite la supervision



Accès à l'ensemble du SI



Tous le monde a accès au serveur de sauvegarde, donc potentiellement aux données



Possibilité d'avoir un chiffrement à la source



- Capacités de déduplication limitées sur le serveur de sauvegarde
- Capacités de suppression des sauvegardes par le serveur lui-même (ransomware)



Le dernier point est évitable, mais requiert la mise en place d'un serveur de purge avec l'ensemble des clefs de chiffrement

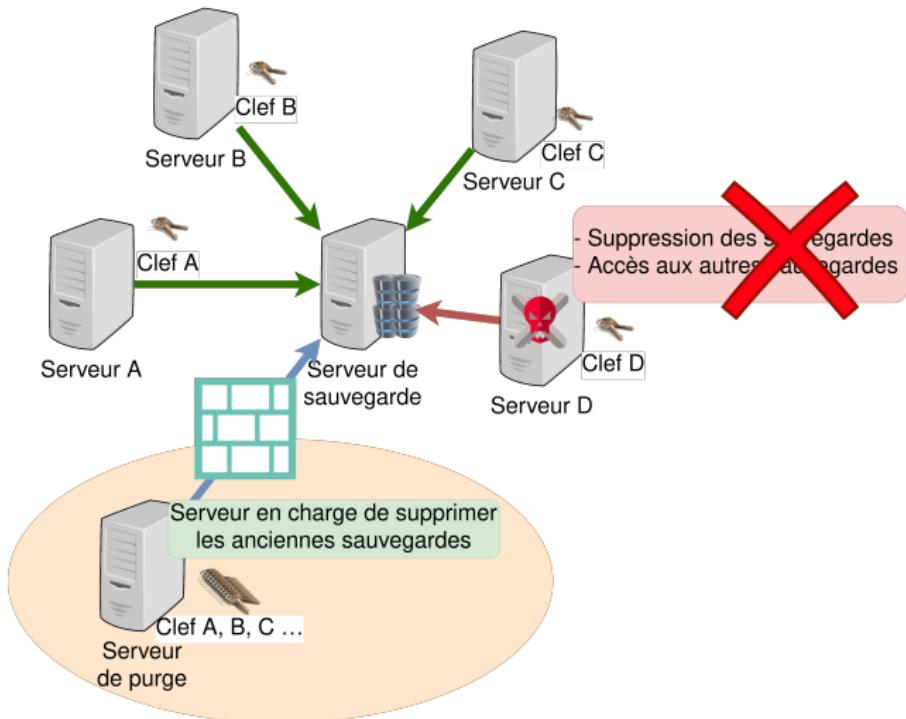


Figure – Architecture de sauvegarde



La sensibilité des sauvegardes est celle des données sauvegardées !

4 Services d'infrastructure et de sécurité	370
Services de récupération ascendante (distribution)	371
Services de transmission ascendants et descendants	386
Cas de la résolution de nom	392
Cas de la supervision	403
Cas de la sauvegarde	411
Cas de l'accès Internet	419
Internet : vecteur d'infiltration	
Internet : vecteur d'exfiltration	
Cas du VPN utilisateur	430
Interconnexion avec les sous-traitants	436

- Premier vecteur d'infiltration
- Premier vecteur d'exfiltration

- Vulnérabilité applicative
- Hameçonnage
- Point d'eau web (*watering hole*)
- Passage par une relation privilégiée avec un tiers



Vulnérabilité applicative



- Architecture applicative 3-tiers
- DMZ entrante
- Une fonction primaire par serveur
 - Coûteux sur une infrastructure non virtualisée

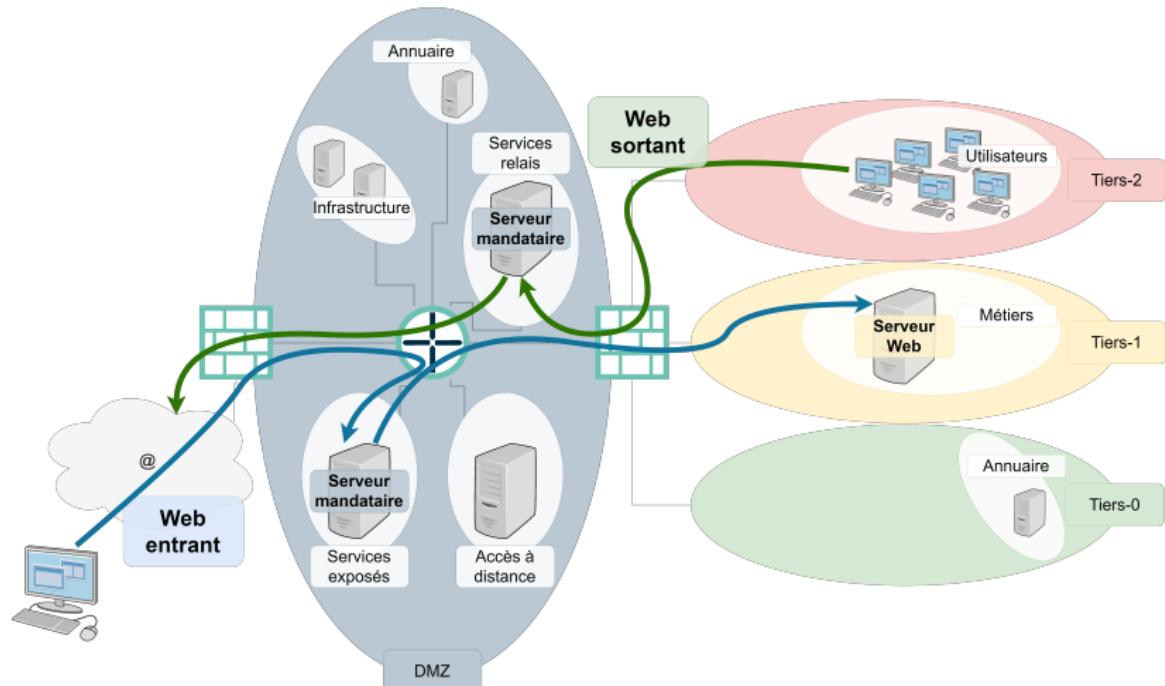


Figure – Architecture de l'accès Internet : DMZ entrante et sortante

DMZ entrante

- Rien ne sort vers Internet



Difficile de maintenir et varier les canaux d'exfiltration

DMZ sortante

- Rien n'entre depuis Internet



Hameçonnage



- Filtre anti-spam
- Anti-virus
- *Graylisting*
- Mécanisme de validation de l'envoi de courriel par l'expéditeur
- Mécanisme de validation d'une nouvelle adresse par le destinataire
- Notification de l'utilisateur d'un courriel provenant d'un nouveau domaine



Point d'eau web



- Relais
- Anti-virus
- NIDS/NIPS



Passage par une relation privilégiée avec un tiers



Cet aspect sera évoqué ultérieurement.

Méthode	Complexité	Protection
En direct	Nulle	À bloquer
Via un proxy	Faible	À restreindre
Via un proxy authentifiant	Moyenne	À restreindre
Via ICMP	Faible	À restreindre drastiquement
Via DNS	Faible	À restreindre
Via e-mail	Elevée	



Fonctions de sécurité de la DMZ

- Filtrage en entrée et en sortie
- Interception TLS
- Analyse, corrélation, détection
 - Journalisation et centralisation des journaux
 - Événements techniques
 - Accès aux contenus web (code des postes et télécommunications)
 - Sondes
- Authentification



La DMZ ne doit pas pouvoir être contournée.

4 Services d'infrastructure et de sécurité	370
Services de récupération ascendante (distribution)	371
Services de transmission ascendants et descendants	386
Cas de la résolution de nom	392
Cas de la supervision	403
Cas de la sauvegarde	411
Cas de l'accès Internet	419
Cas du VPN utilisateur	430
Interconnexion avec les sous-traitants	436

VPN utilisateur

Où positionner le serveur

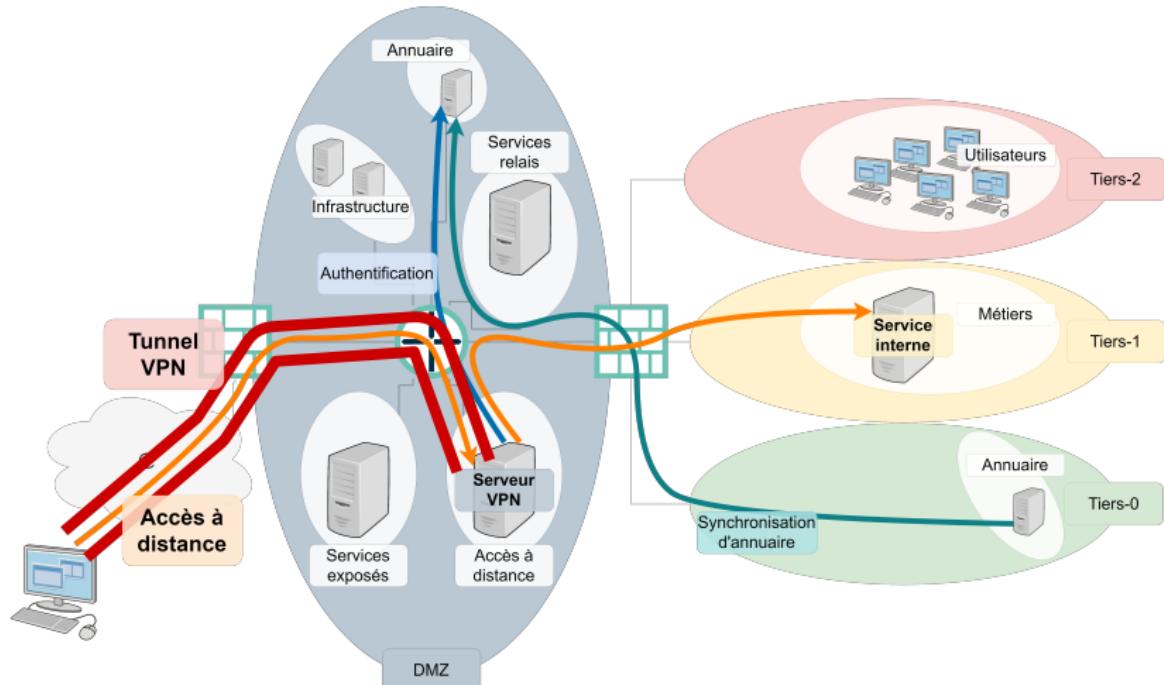


Figure – Architecture VPN : cinématique de flux

Source

- Compte
 - Utilisateur
 - Administrateur
- Poste (compte machine)
 - Utilisateur
 - Administrateur
- Localisation IP
- Réputation de l'adresse
 - Prestataire VPN
 - Nœud Tor
 - Ouvertement malveillante
- OTP / token

Accès

- Admin bulle niveau 0
- Admin bulle niveau 1
- Admin bulle niveau 2
- Application sensible
- Application standard



- Affectation d'un accès situé dans un réseau spécifique en fonction de la confiance dans la source
- Filtrage de chacun des réseaux spécifiques en fonction des accès autorisés



Est-ce normal d'avoir l'enchaînement suivant ?

- L'utilisateur A se connecte en VPN et se voit attribuer l'IP x.x.x.x
- L'IP x.x.x.x établit une connection vers B en tant qu'administrateur C



Segmentation des accès réseau / applicatifs ?

- Accès VPN
 - Certificat machine
 - Mot de passe utilisateur
- Accès applicatif
 - Mot de passe utilisateur (présent en cache)...

4 Services d'infrastructure et de sécurité	370
Services de récupération ascendante (distribution)	371
Services de transmission ascendants et descendants	386
Cas de la résolution de nom	392
Cas de la supervision	403
Cas de la sauvegarde	411
Cas de l'accès Internet	419
Cas du VPN utilisateur	430
Interconnexion avec les sous-traitants	436

- Objectif de l'attaquant : dépenser le moins de ressources pour atteindre son objectif
 - Donc trouver la porte la moins bien fermée
 - Et celle-ci pourrait être l'accès réservé aux pompiers

Interconnexion avec les sous-traitants

Le problème

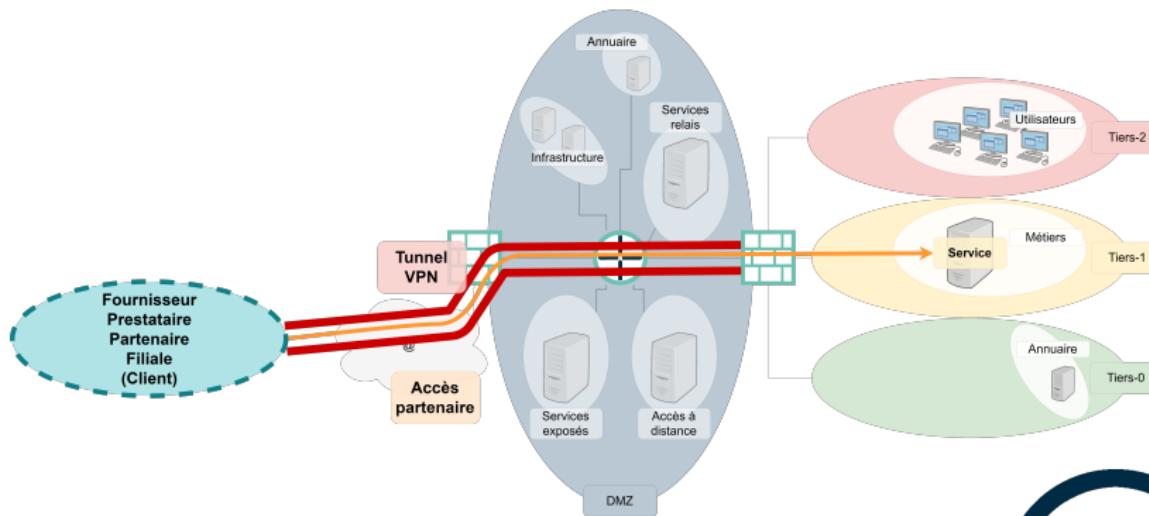


Figure – Interconnexion par VPN site-à-site : accès direct



Interconnexion avec les sous-traitants

Le problème (variante)

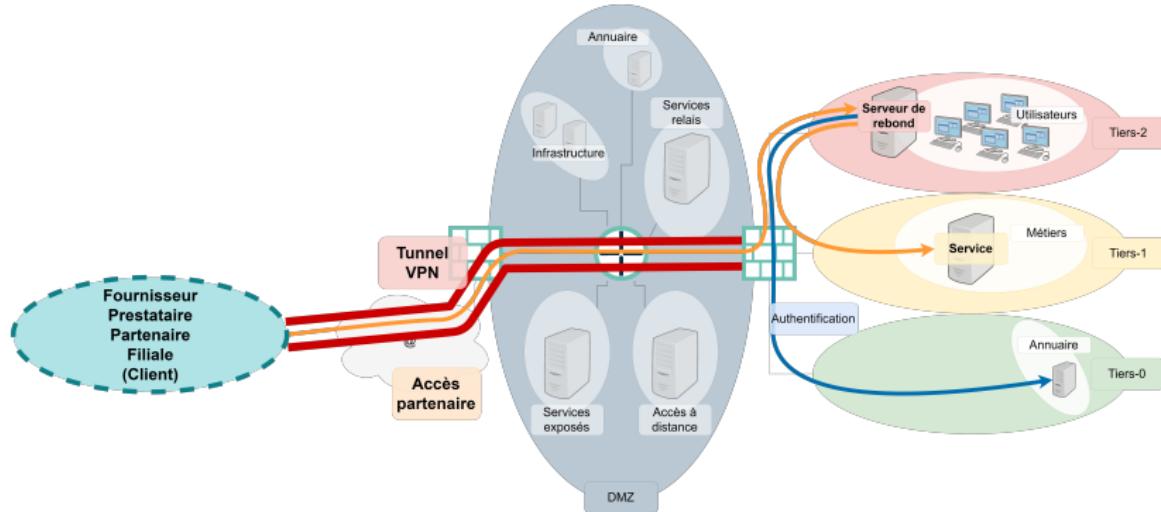


Figure – Interconnexion par VPN site-à-site : rebond

- Cas de la télémaintenance : mêmes recommandations que pour l'accès nomade
 - Si temporaire, activer les comptes et les flux sur demande

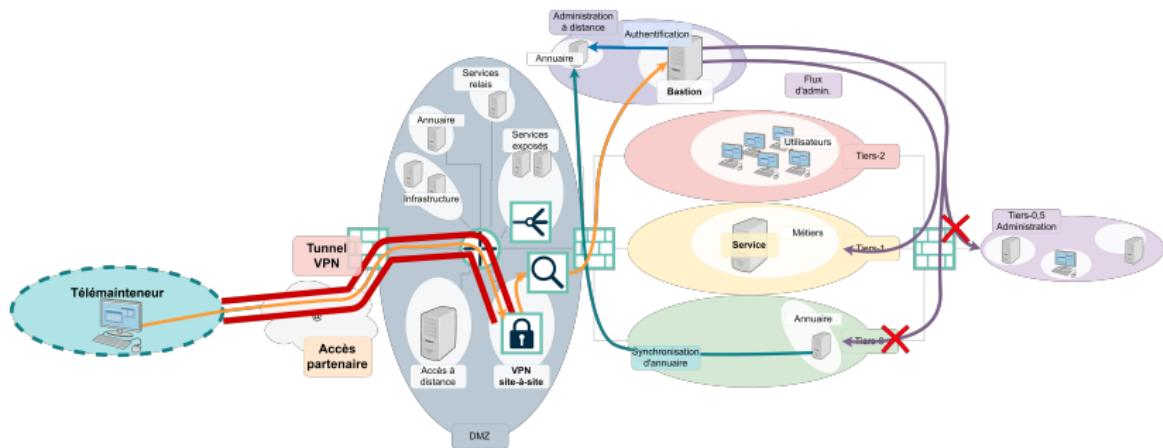


Figure – Interconnexion par VPN personnel pour la télémaintenance

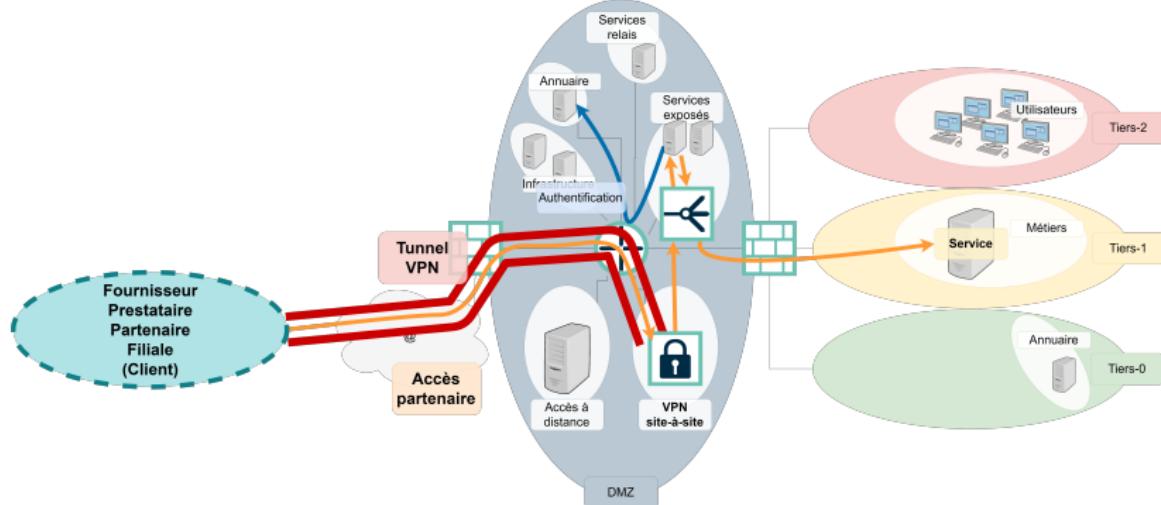


Figure – Interconnexion par VPN site-à-site : DMZ





- N'utilisez pas de services de sécurité de tiers supérieurs
- Identifiez, segmentez et sécurisez les services d'infrastructure centralisés/mutualisés
 - ⇒ ceux qui permettent un effet pivot important
 - attention aux flux sortants et aux DMZ
- Cloisonnez les accès distants selon les populations et leurs priviléges
 - et minimisez ces accès !
- Segmentez les accès Internet selon les usages
- Sauvegardez (et faites des tests de restauration)
 - Rappel : sauvegardes du tiers-0 = tiers-0 (hors chiffrement à la source)

1	Bulles et tiers-{0-2}	284
2	Séparation des environnements	301
3	Administration, privilèges et relations de contrôle	308
4	Services d'infrastructure et de sécurité	370
5	Applications	444
6	Continuité	452

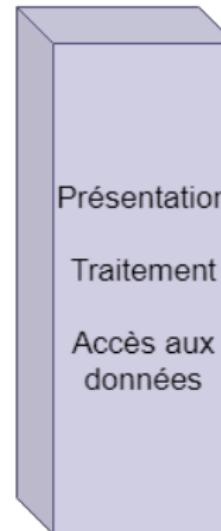
Applications 2-tiers / 3-tiers

Principe

3 tiers

2 tiers

Monolith



Apache
Nginx

Tomcat
Node.js

Oracle
MongoDB

Figure – Applications 2-tiers / 3-tiers : principe

En utilisant tout ce que nous avons vus, comment positionner ces trois tiers ?



Segmentation des tiers en zones selon le concept d'exposition

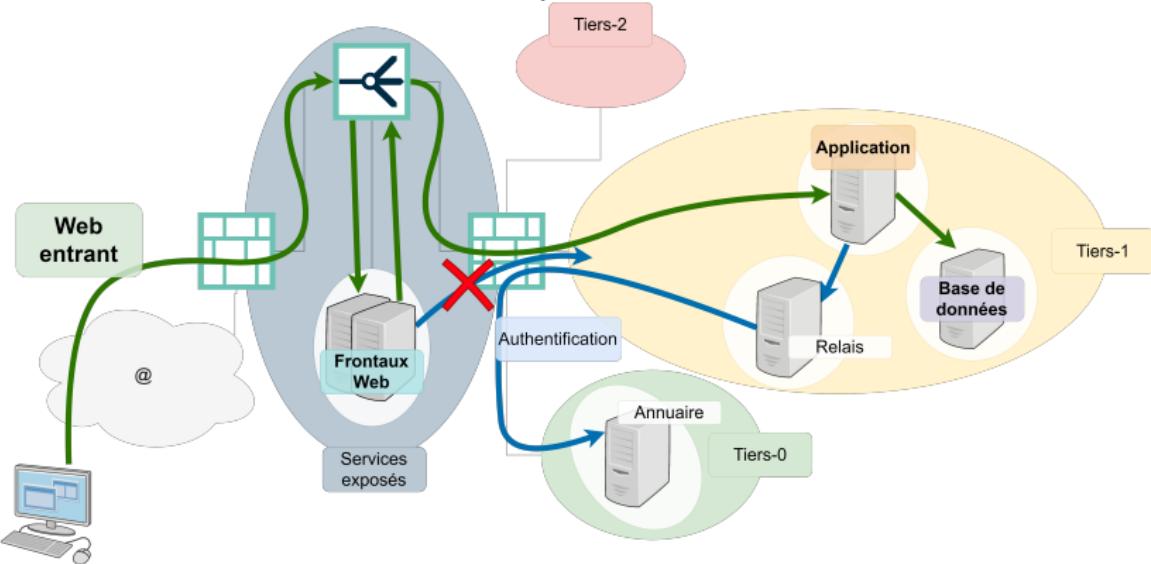


Figure – Applications 2-tiers / 3-tiers : architecture réseau

Partage de contenu

Cloisonner les sources d'informations

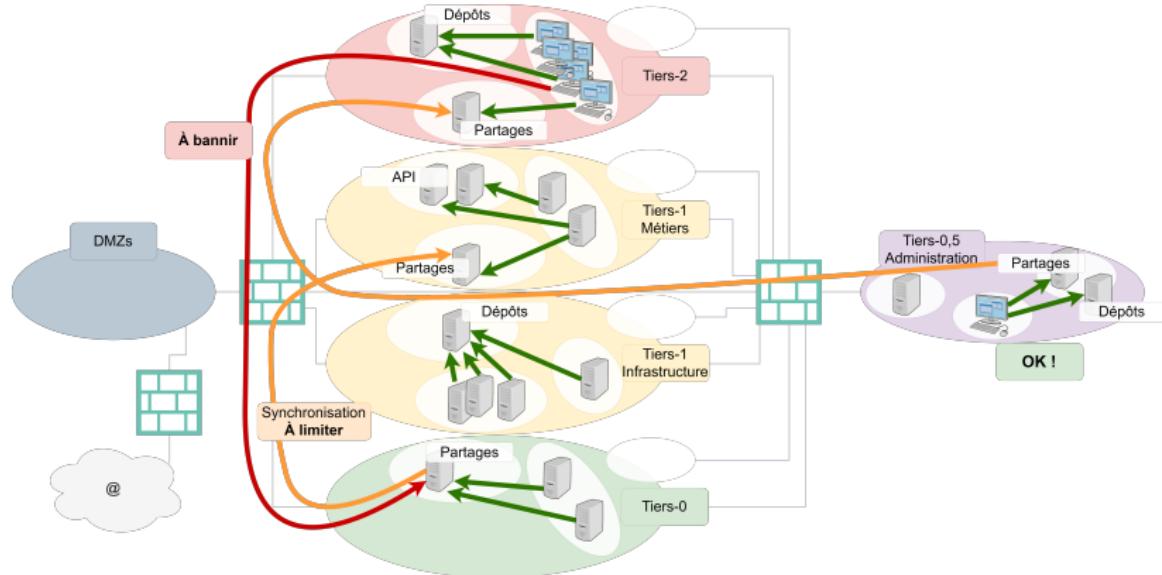


Figure – Partage de contenu : cloisonnement

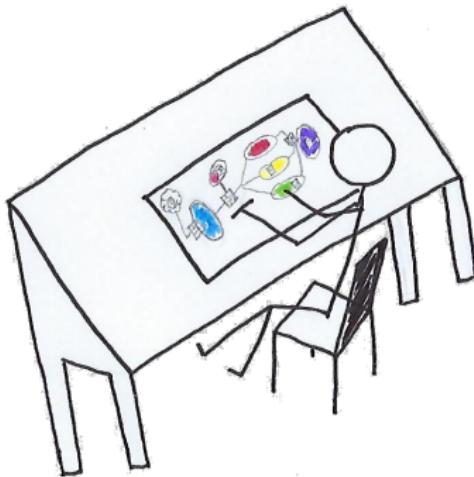


Application offrant de nombreux mécanismes ; et la gestion des privilèges qui va avec...

Exemple : ERP comme SAP, AWS



In-fine les problématiques sont similaires à celle de la gestion des privilèges d'un parc Windows





- Concevez/intégrez vos applications avec une logique de segmentation en tiers
- Cloisonnez les composants applicatifs en zones
- Limitez l'exposition des composants applicatifs
- Considérez les applications complexes comme un SI à part entière
 - donc gérez-les en conséquences
 - segmentation en bulles, cloisonnement des utilisateurs, etc.

1	Bulles et tiers-{0-2}	284
2	Séparation des environnements	301
3	Administration, privilèges et relations de contrôle	308
4	Services d'infrastructure et de sécurité	370
5	Applications	444
6	Continuité	452

6 Continuité	452
Redondance	453
Problématique de continuité	478

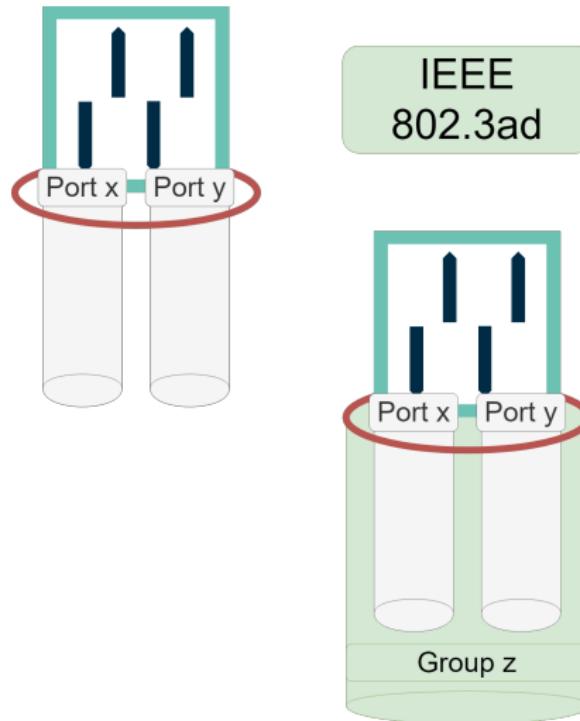


Figure – Agrégation de liens : principe

- CARP (Common Address Redundancy Protocol), libre, *open source*
- VRRP (Virtual Router Redundancy Protocol) - RFC 5798^q, libre
- HSRP (Hot Standby Router Protocol) - RFC 2281^r, propriété de Cisco
- GLBP (Gateway Load Balancing Protocol), propriété de Cisco
 - Permet également la répartition de charge

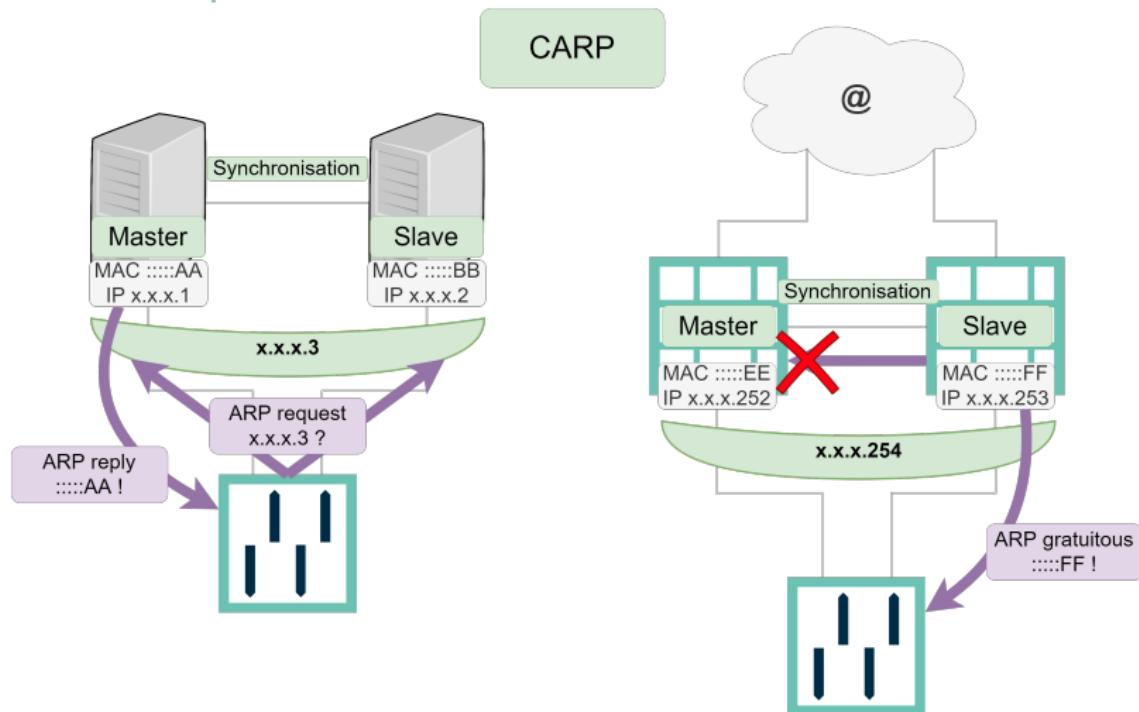
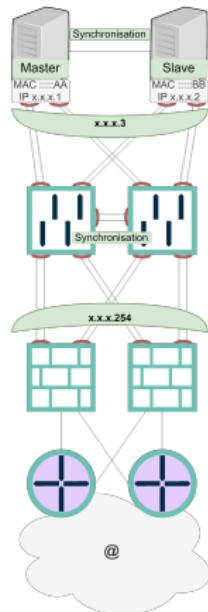


Figure – Agrégation de liens avec CARP



Tout composant non redondé est un SPOF.

Figure – Architecture redondée : principe



Attention aux boucles réseaux !

Boucle réseau

- Niveau 2 : plusieurs chemins sont disponibles pour atteindre la même destination
- Niveau 3 : le *next hop* est le noeud précédent



Boucles niveau 2

- Tempête de diffusion (*Broadcast storm*)
- Duplication de trames
- Instabilité de table MAC (ou table CAM)

Boucles niveau 3

- Connexion avec la destination impossible

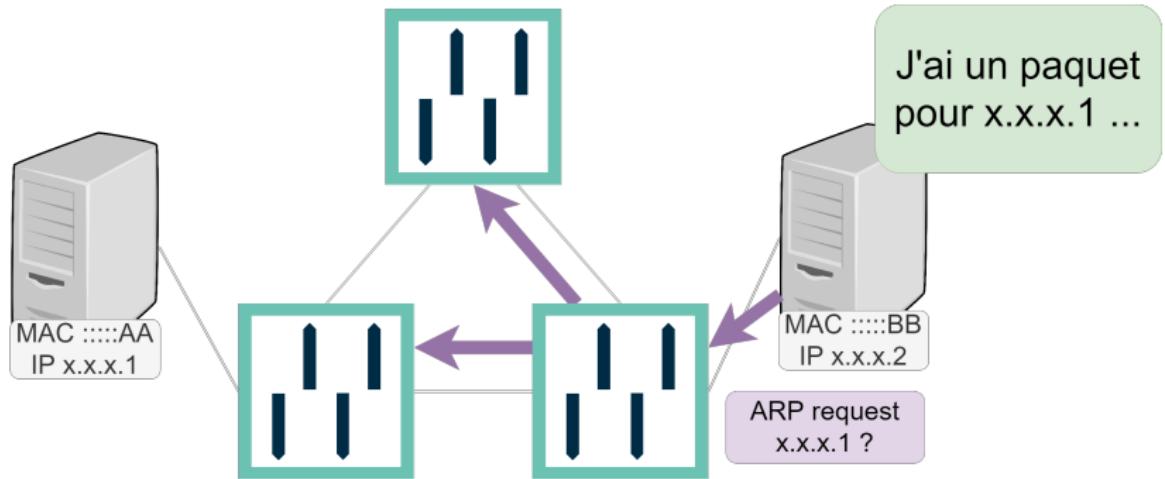


Figure – Architecture redondée : boucles réseaux (1)

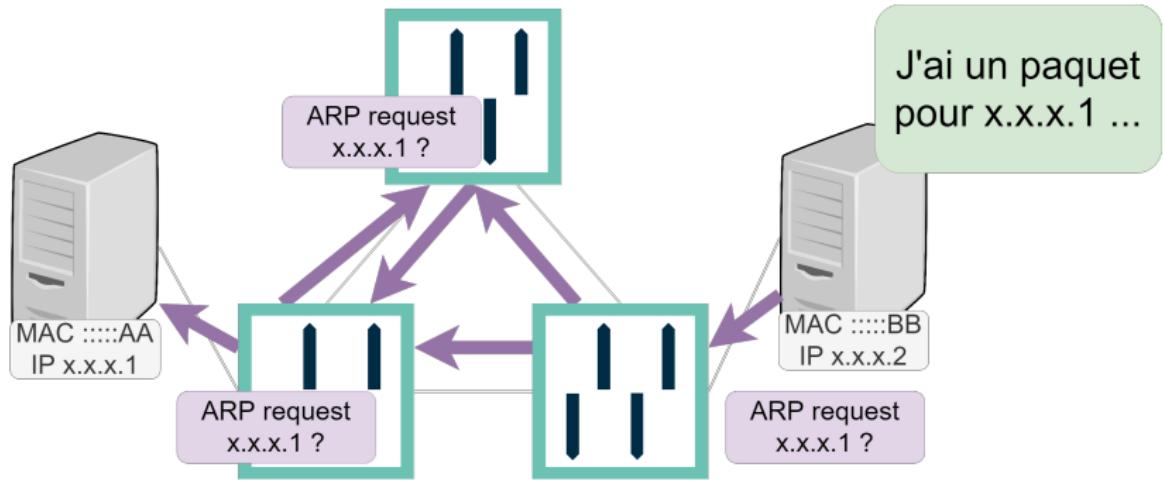


Figure – Architecture redondée : boucles réseaux (2)

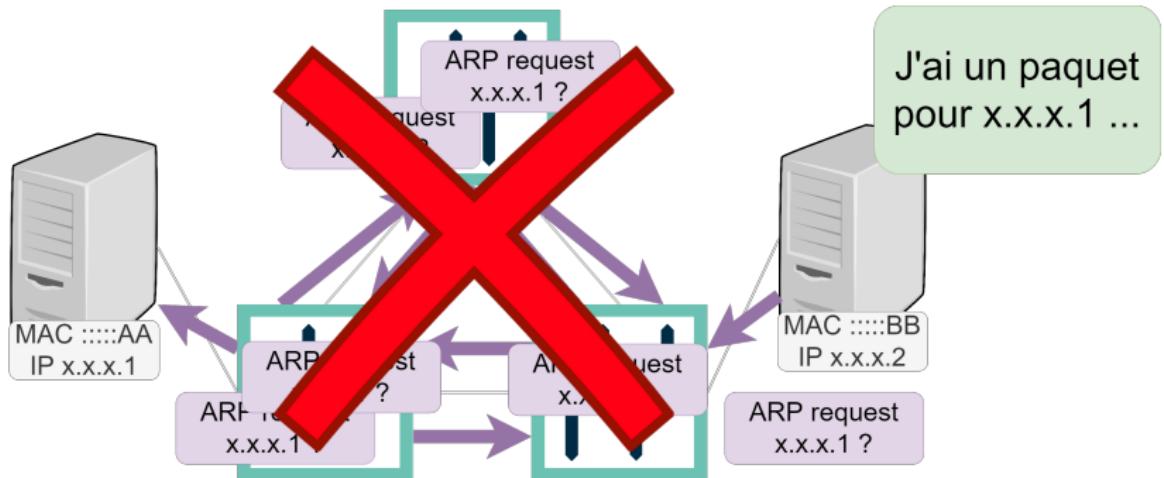


Figure – Architecture redondée : boucles réseaux (3)



- STP (Spanning-Tree Protocol) - IEEE 802.1D
 - RSTP (Rapid STP) - IEEE 802.1w
 - MSTP (Multiple STP) - IEEE 802.1s (inclus dans IEEE 802.1Q)
- SPB (Shortest Path Bridging) - IEEE 802.1aq
 - Cumule la détermination d'une topologie sans boucle et l'agrégation de liens
 - Compétition avec IETF TRILL

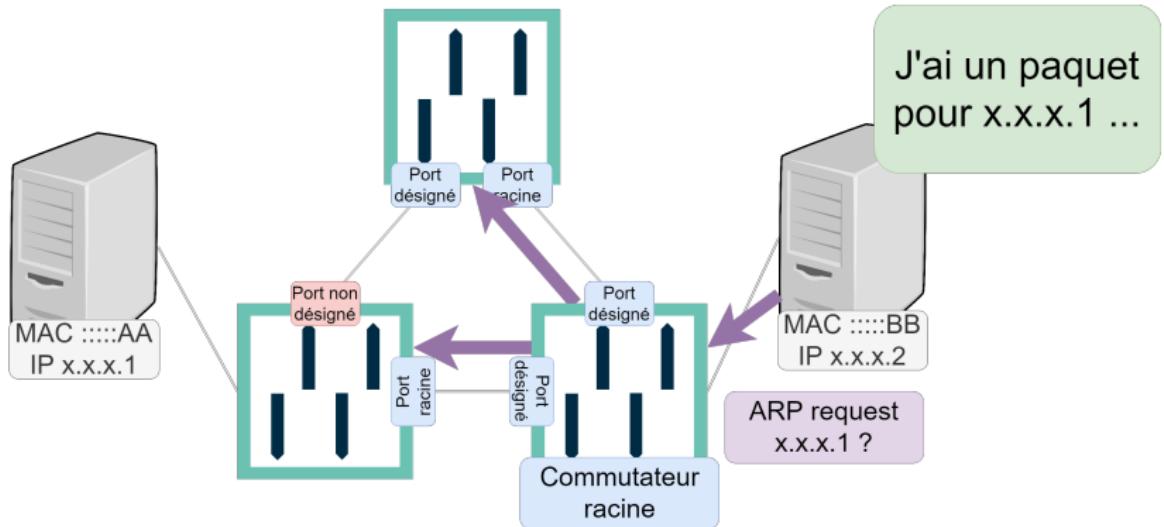


Figure – Architecture redondée : boucles réseaux avec Spanning tree (1)

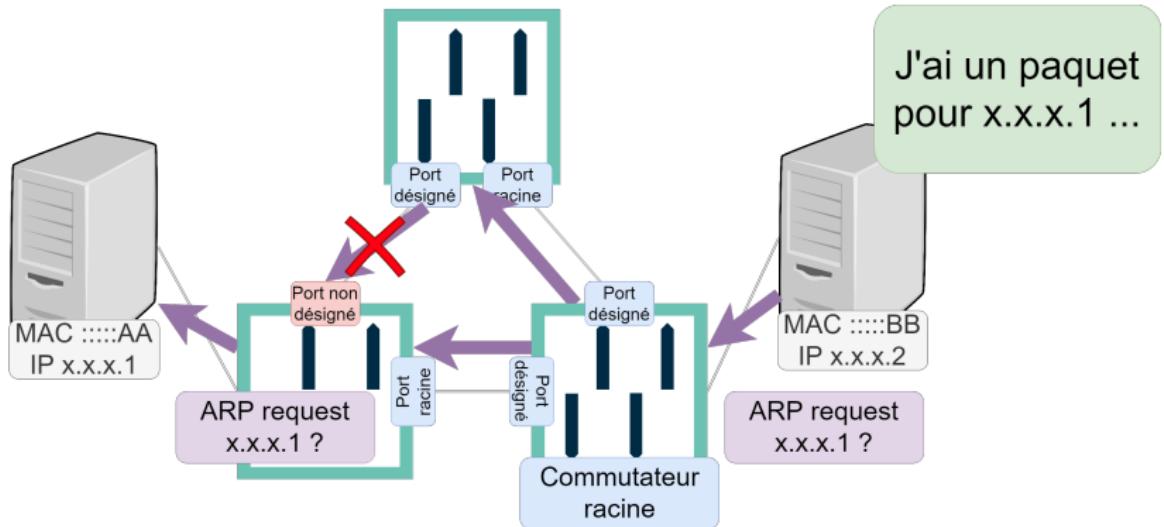


Figure – Architecture redondée : boucles réseaux avec Spanning tree (2)

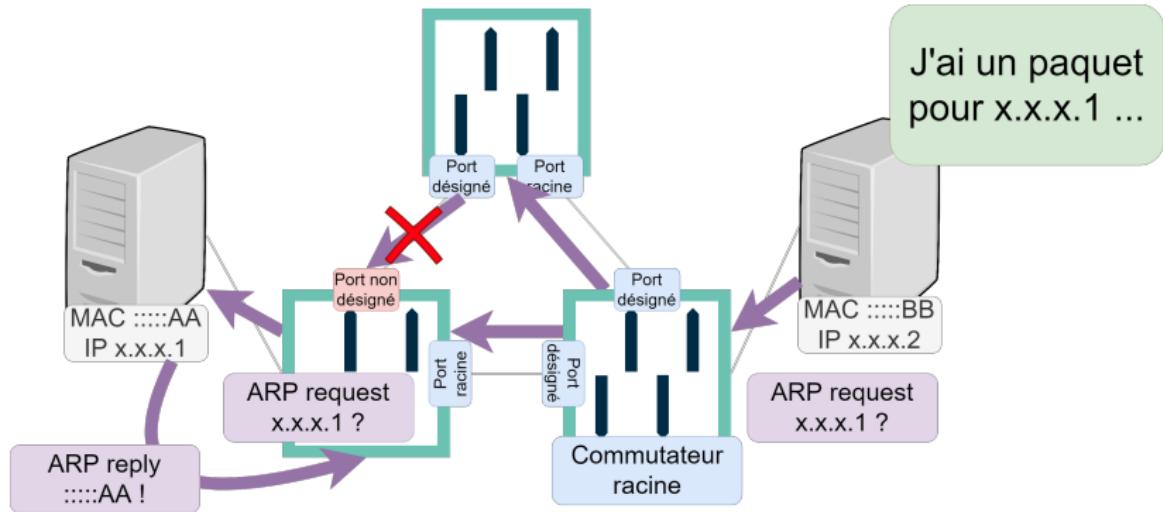


Figure – Architecture redondée : boucles réseaux avec Spanning tree (3)

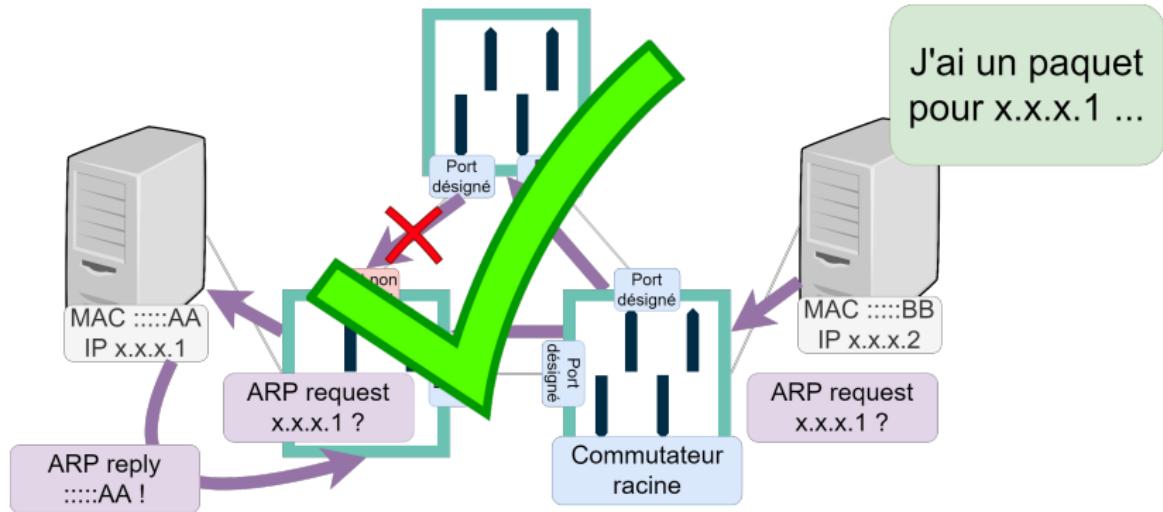


Figure – Architecture redondée : boucles réseaux avec Spanning tree (4)



- Statique
 - Erreurs
 - Mise à jour manuelle à chaque changement
- Dynamique
 - *Spoofing*
 - Fuite d'informations (routes, adresses IP)
 - Chemin non connu à l'avance
 - Difficultés possibles en debug
 - Complexé à mettre en œuvre
 - *Overhead*
 - Réseau et système
 - Boucles



Protocoles de routage

... à état de liens (*link-state routing protocols*)

- *Full/Down* et états intermédiaires

vs.

... à vecteur de distances

(*distance-vector routing protocols*)

- Communication de métriques (nombre de sauts)

vs.

... à vecteur de chemins

(*path vector routing protocols*)

- Basé sur les chemins parcourus

Interior gateway protocols

LS OSPF (Open Shortest Path First) - RFC 2328^s, 5340^t (IPv6)

- Permet l'authentification des paquets (*cleartext/md5*)
- Faible surcharge d'un réseau stable (*hello* de 48 octets toutes les n secondes)

LS IS-IS (Intermediate System to Intermediate System) - ISO/IEC 10589

- Permet l'authentification des paquets (*cleartext/md5*)
- Directement encapsulé en niveau 2, 20 octets de moins (support TCP/IP : RFC 1195^u)

DV RIP (Routing Information Protocol) - RFC 1058^v, 2453^w

- Limité à 15 sauts

DV IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced IGRP) - propriétaires Cisco

PV iBGP (Interior Border Gateway Protocol) - RFC 4271^x

Exterior gateway protocols (EGP)

PV eBGP (Exterior Border Gateway Protocol) - RFC 4271



- Lenteur de la propagation des nouvelles routes
- Oscillation de routes (*route flapping*)
 - Réduction du nombre de messages par *flap damping*
- Authentification et protection d'intégrité faible
 - Détournement de trafic / trou noir
 - Boucles
 - Etc.
- EGP (Exterior Gateway Protocol) - obsolète



- Authentification MD5 (ou mieux si existant)
 - OSPF, IS-IS, CARP
 - "TCP MD5" pour BGP - RFC 2385^y
- Filtrage sur les préfixes et les AS pour BGP
- uRPF (Unicast Reverse Path Forwarding) - RFC 3704^z
- Limiter la configuration aux ports nécessaires (STP, notamment)



RPKI (Resource Public Key Infrastructure) pour BGP

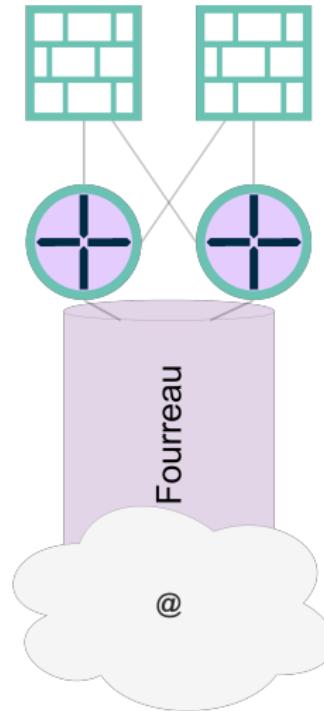
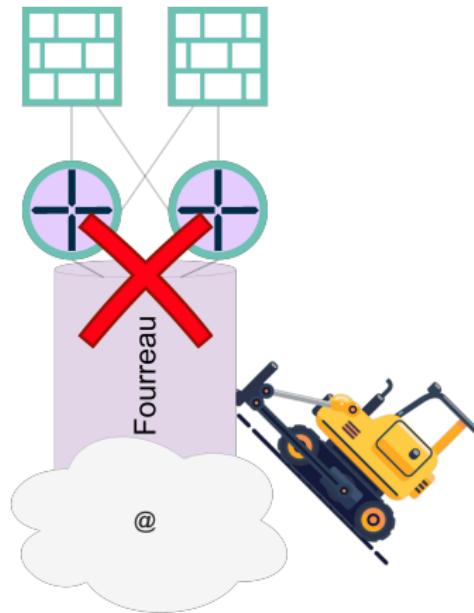


Figure – Architecture redondée : liaisons opérateurs (1)



Attention au passage des raccordements !
(fourreaux, POP)

Figure – Architecture redondée : liaisons opérateurs (2)



- eBGP
- Hébergeur supplémentaire
- Solution "anti-DDoS"
 - Arbor, f5, etc.
- CDN
- *Dynamic DNS*

- Serveurs
 - Redondance machines virtuelles avec contraintes d'exclusion
 - Éviter de les positionner sur le même hyperviseur
 - Éviter de les positionner sur le même site physique
- Stockage
 - Redondance SAN
 - Redondance disques
 - RAID 1, 5, 6

- Relation actif-actif ou actif-passif ?



- Problématique sur les données
 - Bases de données vs. fichiers vs. disques
 - Synchrone vs. asynchrone
- Problématique des sessions
- Problématique du temps de bascule
 - Opérations manuelles éventuellement nécessaires



Stateless

- Redondance électrique
 - Blocs d'alimentation
 - Sources d'alimentation
- Redondance des groupes froid
- [...]

6 Continuité

Redondance

Problématique de continuité

452

453

478



Dépendance circulaire / problématique de l'amorçage



Attention particulière lorsqu'il y a du chiffrement

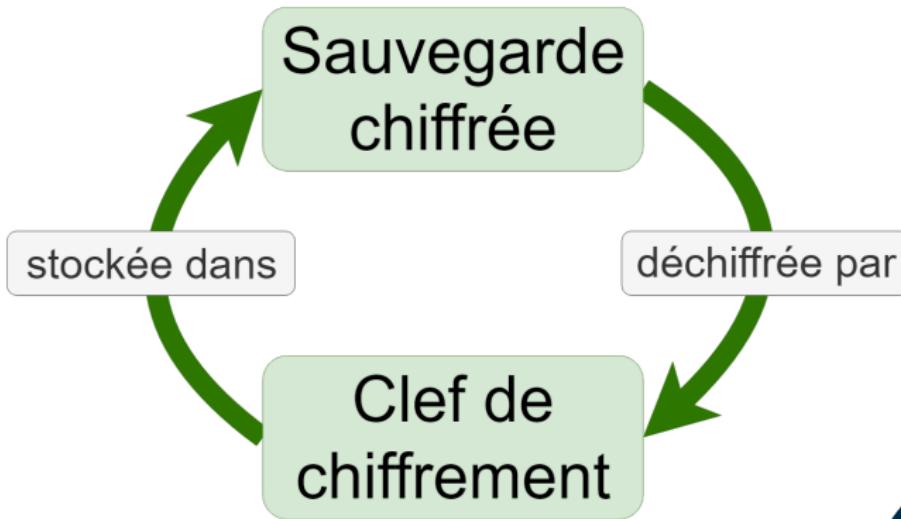


Figure – Dépendance circulaire : sauvegarde chiffrée





Figure – Dépendance circulaire : serveur de gestion de clefs chiffré



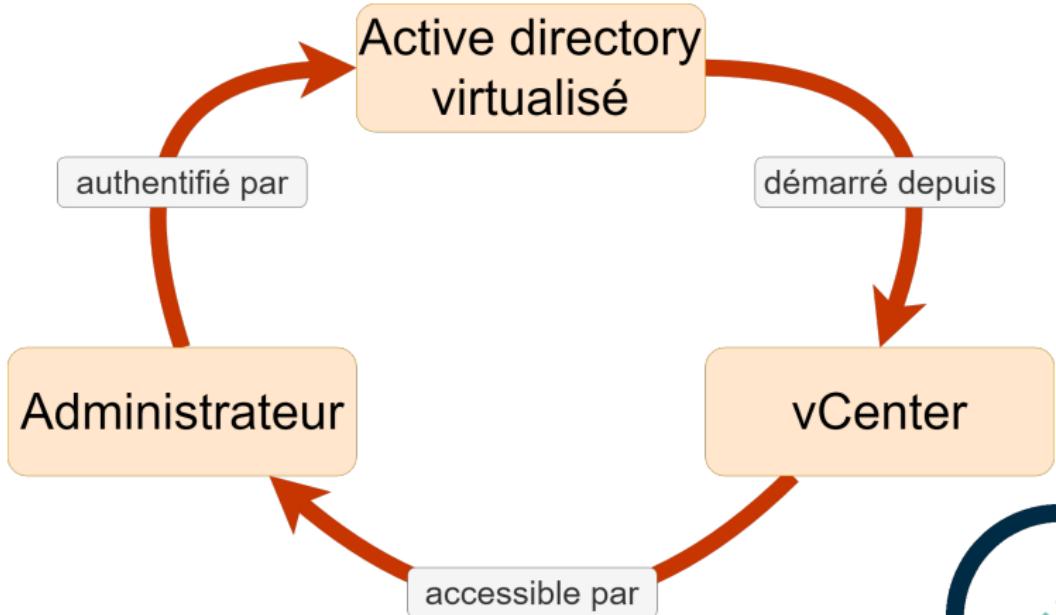


Figure – Dépendance circulaire : authentification centrale virtualisée



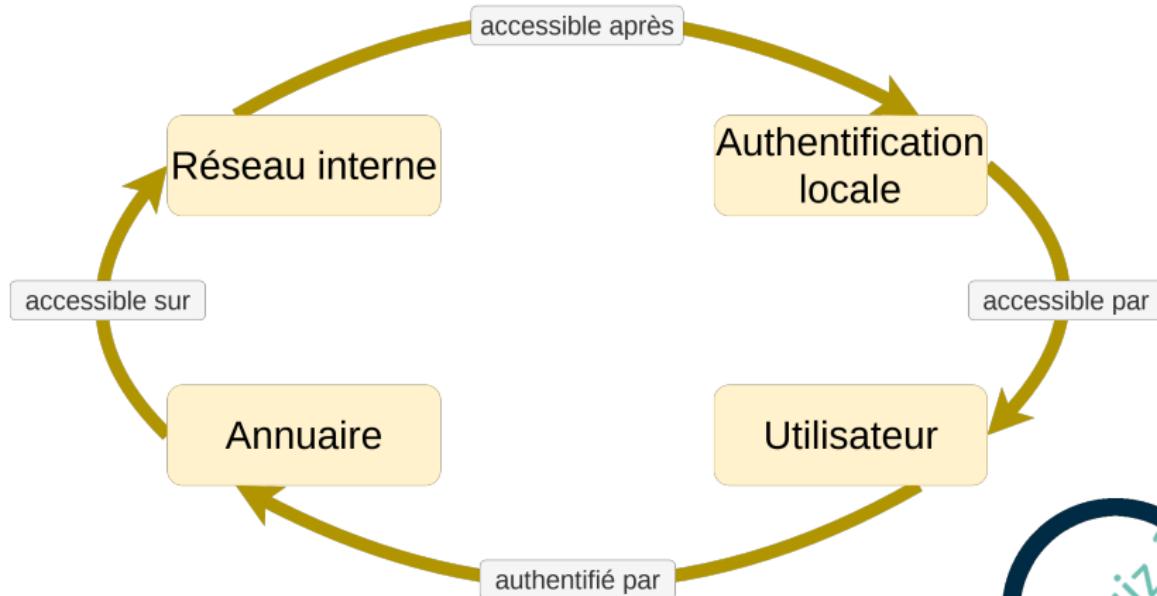


Figure – Dépendance circulaire : connexion au réseau avant authentification

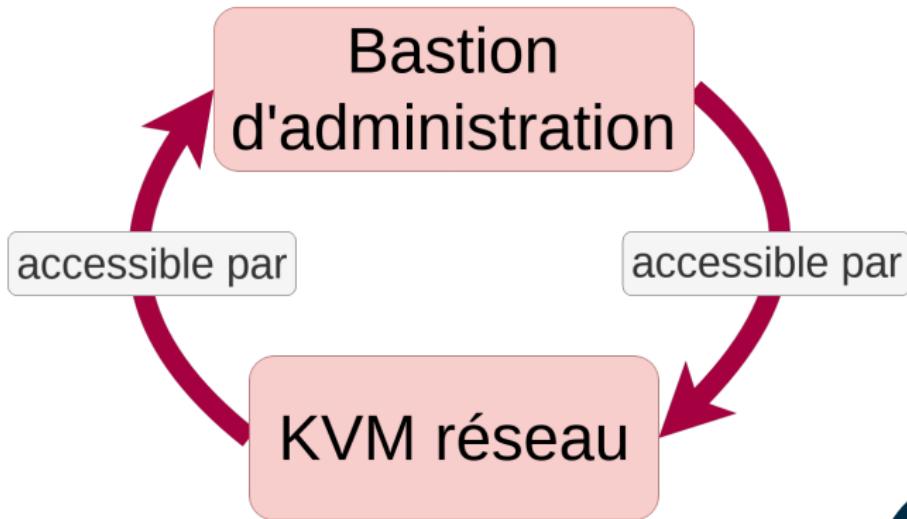


Figure – Dépendance circulaire : administration *out-of-band* via un bastion







• Redondez !

- One Multiple rings to rule them all.
- Les liaisons télécoms, les interfaces réseau, les hyperviseurs, les serveurs, les composants réseau, les composants de stockage, les disques, les alimentations électriques... (sans oublier les personnes !)
- En somme : tout (pour une architecture ayant des besoins importants en disponibilité)

Architectures spécifiques

mars 2021



Hervé Schauer Sécurité



©Hervé Schauer Sécurité 2021

Wenyoung WANG

487

En résumé...

C'est là où on discute de spécificités d'architecture notamment liées à la virtualisation, au *cloud* ou à d'autres types de sous-traitants.

1	Virtualisation de l'infrastructure	489
2	Architectures cloud	503
3	Systèmes industriels	514
4	Gestion technique des bâtiments	525
5	To be continued...	532

- Exécution de plusieurs systèmes sur les même ressources physiques
⇒ Mutualisation
 - Meilleur taux d'utilisation
 - Meilleure disponibilité
 - Répartition de charge
 - RéPLICATION
 - Sauvegarde / *snapshots*

- Émulation
 - JVM (Java Virtual Machine)
- Virtualisation complète ("type 2")
 - Oracle VM Virtualbox, VMware Fusion
- Virtualisation assistée par le matériel ("type 1")
 - Xen, VMware ESX, KVM
- Para-virtualisation
 - Xen, VMware ESX, Microsoft Hyper-V
- Cloisonnement / isolation
 - BSD Jail, LXC, Docker, OpenVZ

- Ressources mutualisées



SPOF

- Défaut de cloisonnement entre systèmes invités ou entre hôte et invités



Compromission

- "Déplacement" de données entre composants physiques



- Localisation des données difficile
 - Complexité de la suppression



Défense en profondeur : pas de confiance dans les mécanismes de cloisonnement
⇒ un hôte ↔ systèmes invités d'un niveau de sécurité homogène (même bulle)

- Segmentation des hôtes
 - Production / hors production
 - Production / administration
 - Métier / interne
 - Fournisseur / client
 - ...
- Idem pour les ressources réseau virtualisées
⇒ Exactement comme on le ferait sur une architecture non virtualisée

Que pensez-vous de cette situation ?

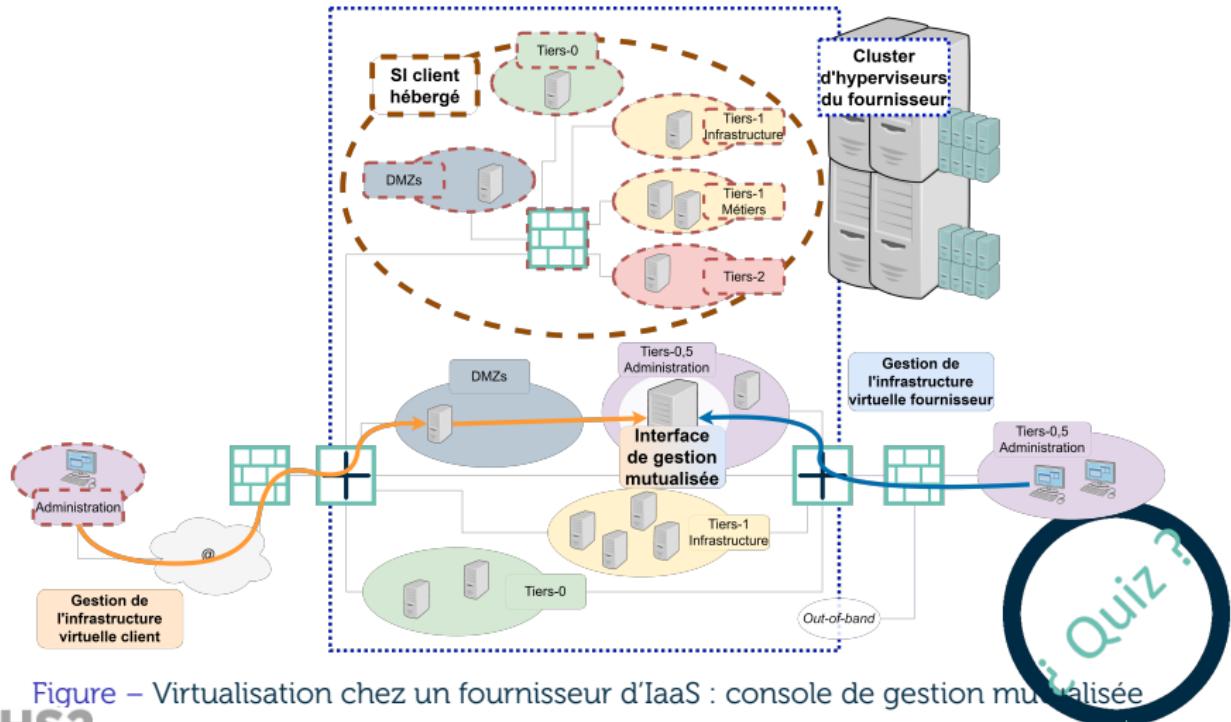


Figure – Virtualisation chez un fournisseur d'IaaS : console de gestion mutualisée

- Probablement une mauvaise idée
 - Vraie vie : le client peut éteindre le serveur de supervision du fournisseur d'IaaS
 - Donc un attaquant ayant compromis le client aussi
- Réflexion selon les mécanismes disponibles (et qui ont été audités)
 - De contrôle d'accès et de gestion des privilèges
 - De limitation d'accès aux ressources (quotas)
 - [...]
- Cela n'empêche pas le cloisonnement des hyperviseurs
 - D'autant plus s'il existe plusieurs clients hébergés

- Est-il possible qu'une machine virtuelle "hors production" monte le stockage d'une machine virtuelle de production?
 - Si oui : perdu.



- Ressources de stockage physiquement dédiées au même titre que les hyperviseurs selon un niveau de sécurité homogène
 - Sinon, mesures de sécurité complémentaires possibles : authentification iSCSI, *Fibre Channel zoning*, etc.

- Exemple : VMware ESXi
 - vCenter / vCSA
 - Interface Web + CLI + API
 - Platform Services Controller (PSC)
 - Interface Web + CLI
 - Virtual Appliance Management Interface (VAMI)
 - Interface Web
 - ESX
 - Interface Web + CLI + API + console

Total : 10 interfaces différentes à sécuriser

Certif défaut

Question

Quel risque implique le clonage d'une machine virtuelle template ?

MAJ , creuds déporté
Compromis → Worm





Attention aux éléments répliqués

- Certificat d'authentification machine
 - /etc/ssh/ssh_host_rsa_key
- Mot de passe des comptes locaux
 - Administrator, root
- Mot de passe de chiffrement
 - `cryptsetup luksChangeKey --key-slot
/dev/mapper/encrypted-device`
- Clefs d'API ou comptes de services déjà configurés

- Installation des correctifs de sécurité
 - Implique de multiples systèmes invités
 - Autant pour installer qu'en n'installant pas
- Quotas d'utilisation des ressources
- Séparation des tâches : distinction des administrateurs hôtes/invités
- Durcissement, journalisation, etc.
- Protection de l'intégrité des *templates*



- Restez cohérents dans la segmentation des hyperviseurs/VM/réseaux/interfaces

1	Virtualisation de l'infrastructure	489
2	Architectures cloud	503
3	Systèmes industriels	514
4	Gestion technique des bâtiments	525
5	To be continued...	532

Cloud (ISO/IEC 17788 :2014)

Paradigme pour l'accès réseau à une réserve extensible et flexible de ressources physiques ou virtuelles avec un approvisionnement en libre-service et une administration sur demande.

Caractéristiques

- Accès global par le réseau
- Mesure du service
- Multi-entité
- Libre-service sur demande
- Élasticité et extensibilité rapide
- Approvisionnement de ressources (stockage, mémoire, capacité de calcul, réseau)

- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- IaaS (Infrastructure as a Service)

- CaaS (Communications as a Service)
- DaaS (Data as a Service)
- Daas (Desktop as a Service)
- IDaaS (IDentity as a Service)
- SecaaS (Security as a Service)
- StaaS (Storage as a Service / DSaaS (Data Storage as a Service))
- NaaS (Network as a Service)
- [...]

- Privé
- Communautaire
- Public
- Hybride



- Peu importe le modèle :
 - Il subsiste toujours des équipements à gérer
 - Il faut concevoir l'architecture et l'interconnexion des deux environnements

- Multi-fournisseurs
 - Assurer la disponibilité
- Automatisation
 - Accélérer le *time-to-market*

- Multi-fournisseurs



- Compétences
- Interconnexion
 - Cloud brokers
- Reprise sur panne / répartition de charge

- Automatisation



- Serveurs ont des comptes d'API
 - Prise de contrôle du compte chez le fournisseur de cloud
 - Rebond



La mise en œuvre diffère mais les concepts restent identiques !

- Serveurs/services autonomes dans le cloud (SaaS, PaaS ou IaaS) et interconnexion par Internet



Filtrage supplémentaire au niveau des serveurs dans le cloud

- Architecture mise en œuvre dans le cloud



SDN (Software-Defined Network)

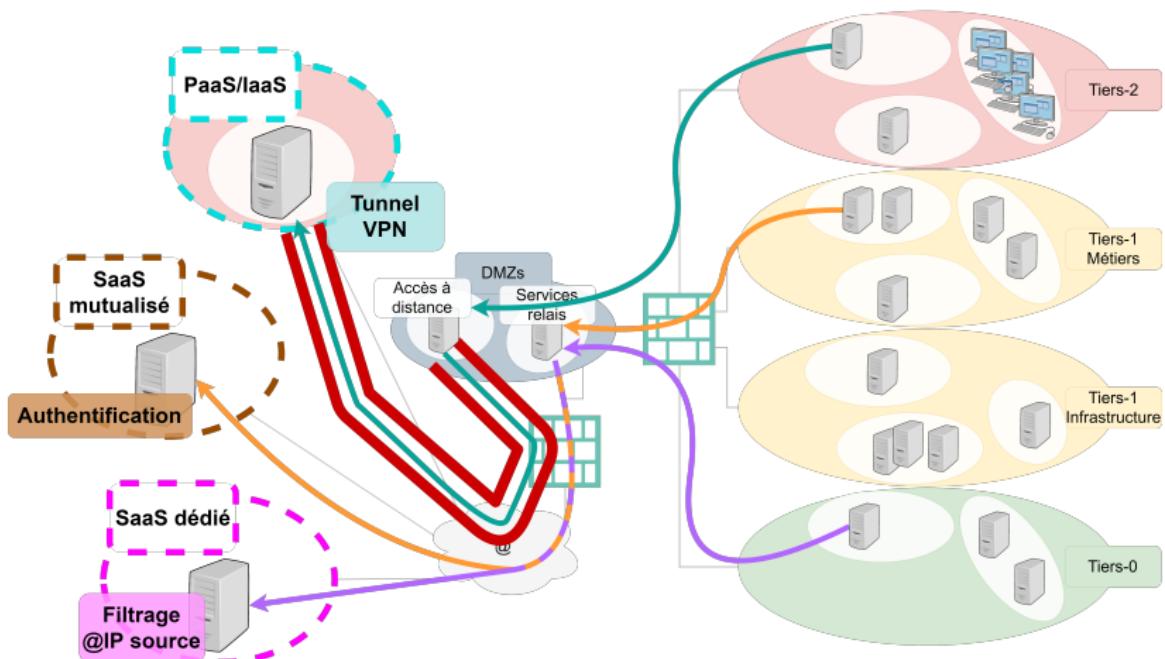


Figure – Architecture cloud : interconnexion avec des services autonomes

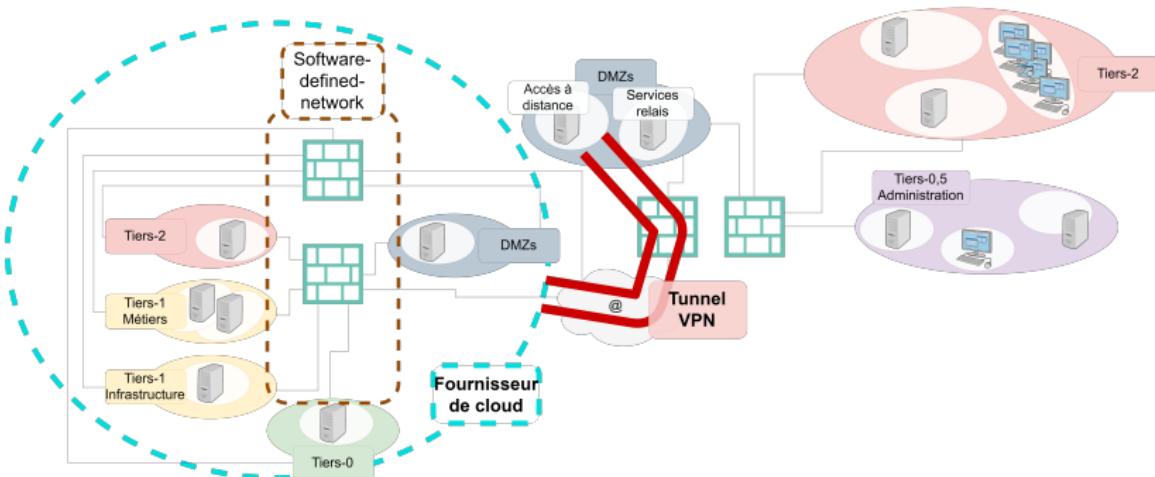


Figure – Architecture cloud : externalisation complète



- Suivez les recommandations du fournisseur
- Auditez, corrigez, recommencez

1	Virtualisation de l'infrastructure	489
2	Architectures cloud	503
3	Systèmes industriels	514
4	Gestion technique des bâtiments	525
5	To be continued...	532

- Les systèmes industriels ont des contraintes et des objectifs différents des systèmes *IT* classiques
 - Temps réel, sûreté, disponibilité
 - Environnement physique difficile, voire extrême



- Mesures de sécurité minimales, voire absentes
 - Voir inclusion flagrante de vulnérabilités
 - Mots de passe d'administration en dur ⇒ "Ceci est une fonctionnalité"
 - Sécurité par l'obscurité... :(
- Difficulté/impossibilité de mise à jour
 - "Obsolescence imposée"
 - Maintenance très coûteuse ("Veuillez rebooter votre usine")
- Systèmes exposés physiquement
- Communications sans fil nécessaires

- Niveau 4-5 : Réseau d'entreprise
 - Planification, ordonnancement, logistique, systèmes "IT"
- Niveau 3.5 : DMZ industrielle
 - Relais, antivirus, bastions, historian, patch management...
- Niveau 3 : Gestion des opérations et de la fabrication
 - Backup, DC, serveurs d'applications, DHCP, DNS, NTP...
- Niveau 2 : Contrôle et supervision
 - Console opérateurs locaux, SCADA²⁴...
- Niveau 1 : Equipements de terrain
 - Actionneurs, PLC (Programmable Logic Controller), VFD (Variable-Frequency Drive)...
- Niveau 0 : Equipements contrôlés
 - Equipements contrôlés : capteurs, pompes, valves...

24. Supervisory Control And Data Acquisition

25. International Society of Automation

- Quid des **systèmes critiques** vs. systèmes peu importants?
 - Ex : SIS (Safety Instrumented Systems)
 - Capteurs, IHM, contrôleurs dédiés
- Quid des **systèmes exposés**
 - Sécurité physique, média de communication "à risque"...



- Systèmes dans une couche avec des criticités / expositions différentes



- Cloisonnement horizontal
- Evolution vers un modèle par **zones et conduits** (IEC 62443)

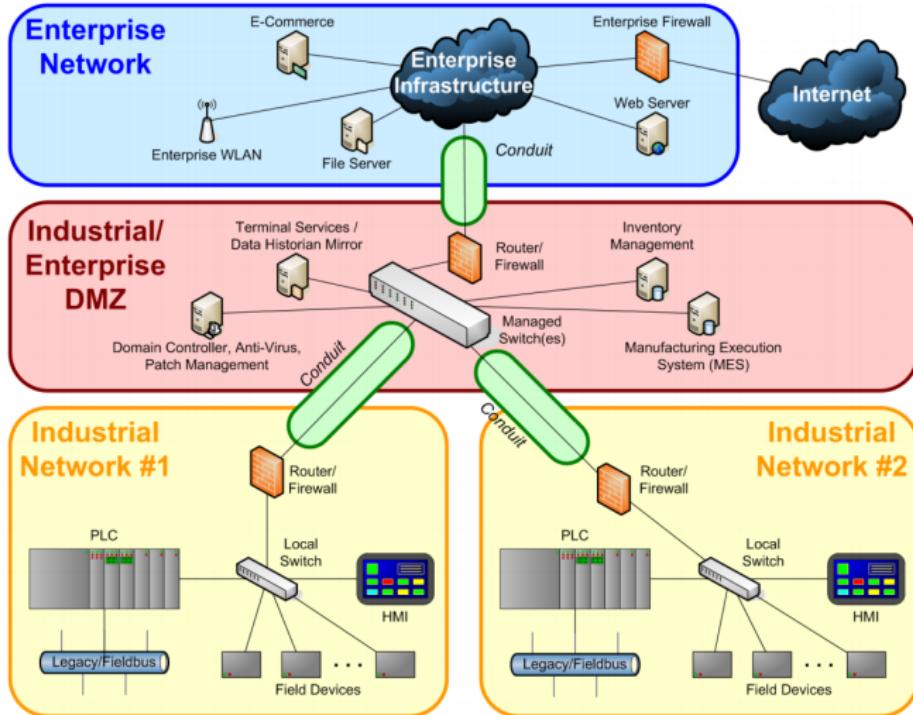


Figure – Modèle zones et conduits
 src : ISA (International Society of Automation)

- Assigner un niveau de criticité/exposition

Ex. proposé par l'ANSSI :

- Calcul basé sur plusieurs caractéristiques
 - L'**Impact** (1 :insignifiant.. 3 :catastrophique)
 - La **Complexité** (1 :minimal.. 3 :très complexe)
 - La **Connectivité** (1 :isolé.. 5 :internet)
 - L'**Accessibilité** (1 :autorisés/habilités/contrôlés.. 4 :public)

- Résultat : la **Classe**

- 1 : risque ou impact faible
- 2 : risque ou impact significatif
- 3 : risque ou impact critique

- **Minimum vital :**
 - SI industriel vs. Réseaux publics
 - SI industriel vs. Réseau d'entreprise
- Mais ne pas oublier...
 - Interactions entre les différentes classes
 - Flux unidirectionnels du plus critique vers le moins critique
 - Processus de télédiagnostic / télémaintenance
 - Protection des communications
- Et plus généralement :
 - Accès physique aux équipements
 - Attention aux médias amovibles !

	1	2	3
Réseaux publics	<-> Pare-feu	<- Pare-feu	Non!
SI d'entreprise	<-> Pare-feu	<- / <-> Pare-feu	<- Diode
SI industriel (classe inférieure)	n/a	<- Pare-feu	<- Diode
SI industriel (même classe)	<-> Pare-feu	<-> Pare-feu	<-> Pare-feu

	1	2	3
Sans-fil	- Authent. client+AP - Isolation	Idem, + IDS conseillé	- Idem, + IDS oblig. - <u>Interdit</u> si besoin en dispo. important
Télémaintenance	ok	Déconseillée	<u>Interdit</u> Ou depuis un site de classe 3)
Télédiagnostic	ok	ok	<- (aucune interaction)
Surveillance	Journaux	IDS (péph + critiques)	IDS (péph + critiques)

Exemple d'architecture industrielle

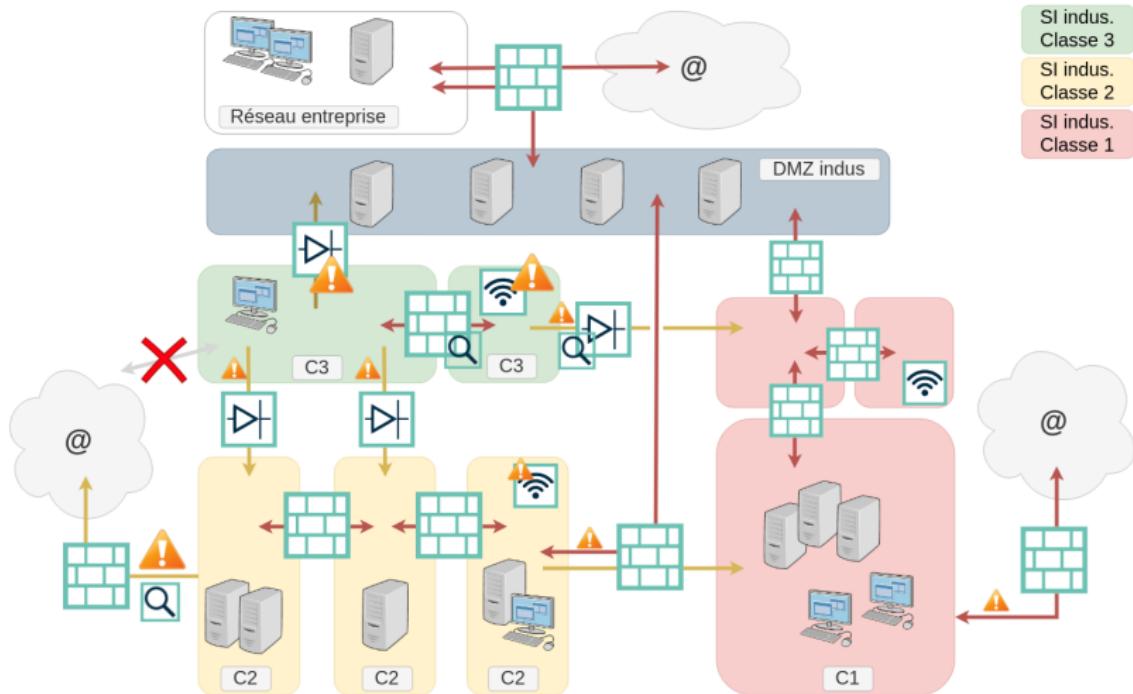


Figure – Exemple d'architecture industrielle



- Identifiez la sensibilité de vos SI industriels
- Isolez tous les SI le permettant
- Cloisonnez chacun des autres selon sa sensibilité
- Supprimez toute communication entrante vers un SI de classe 3
 - puis installez des diodes pour les communications sortantes vers des SI de classe inférieure
- Concevez une DMZ entre les SI industriels et de gestion
- Surveillez (corrélation de journaux, sondes, IDS/IPS, etc.)
 - au plus proche des systèmes critiques
 - et au niveau de la DMZ (positionnement parapluie)

1	Virtualisation de l'infrastructure	489
2	Architectures cloud	503
3	Systèmes industriels	514
4	Gestion technique des bâtiments	525
5	To be continued...	532

- Téléphonie d'urgence



Indisponibilité : réaction aux incidents/gestion de crise perturbée

- Alarmes
- Contrôle d'accès physique
- Centrales de détection incendies
- Vidéosurveillance



- Indisponibilité/altération : intrusion physique non détectée
- Altération : intrusion dans un système d'information interconnecté
- Confidentialité : dépend de leur positionnement



- Isolation réseau physique complète vis-à-vis des autres systèmes d'information
- Segmentation selon l'exposition
 - Des différents systèmes (vidéosurveillance vs. contrôle d'accès physique)
 - Voir entre externe et interne
 - Des différentes types d'équipements
 - Capteurs (boîtiers, caméras, etc.), serveurs de contrôle et de collecte, postes de supervision
 - Entre les capteurs
 - Type PVLAN ou segmentation par zones (au sens physique)



- Privilégier le filaire (coaxial ou paire torsadée)
 - Contrôle d'accès au réseau
 - Authentification réseau (802.1X), par exemple
 - Chiffrement et authentification des flux
 - Et **mécanismes anti-rejet**
 - Désactivation des interfaces d'administration locales
 - Sécurité physique des boîtiers et des câbles
-
- Référentiels APSAD R7 (déttection automatique d'incendie), R81 (déttection d'intrusion), R82 (vidéosurveillance)

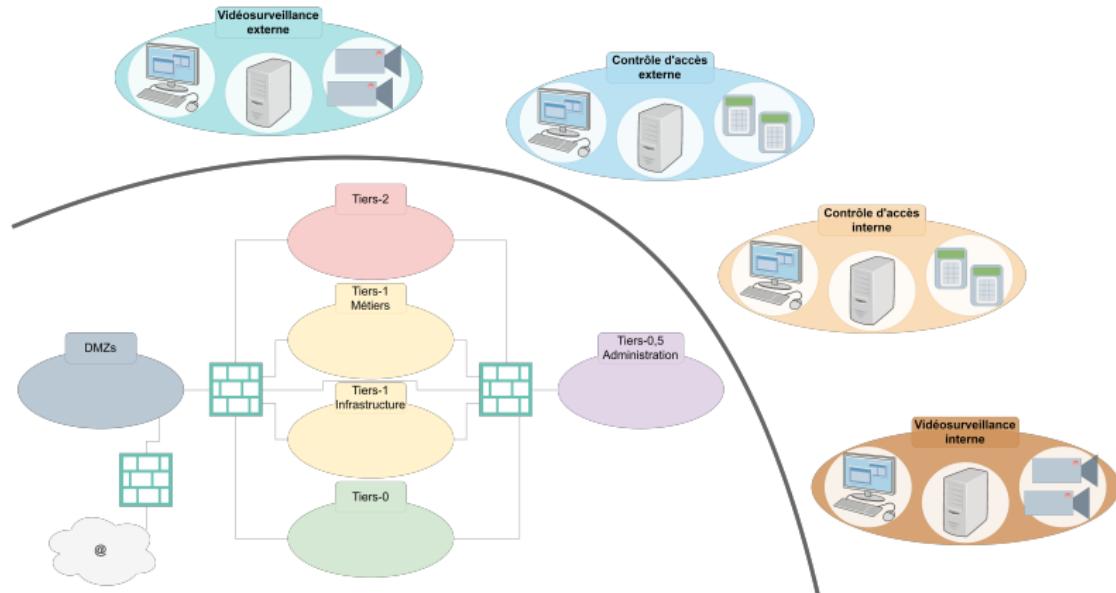


Figure – Gestion des bâtiments : isolation des réseaux

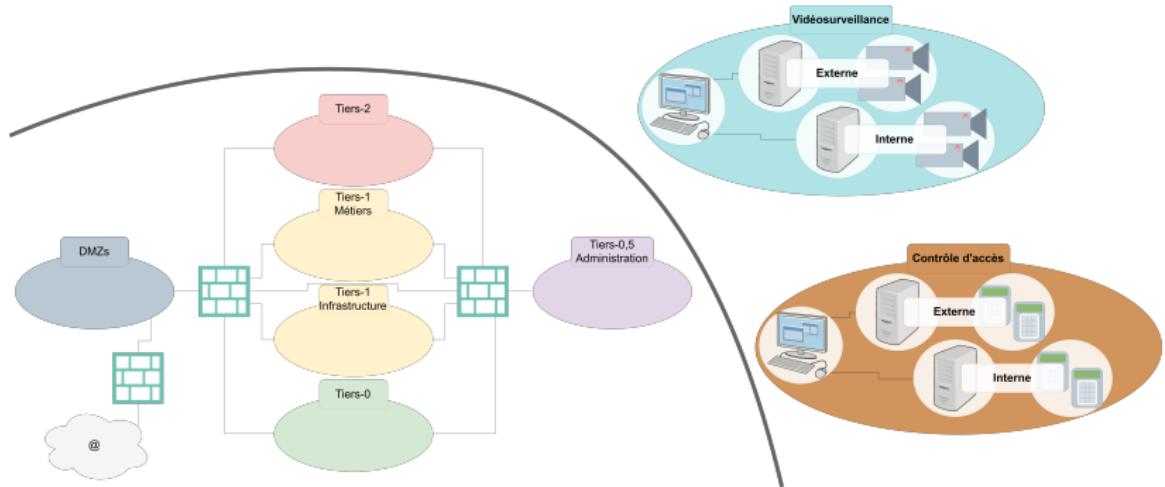


Figure – Gestion des bâtiments : mutualisation des réseaux internes et externes



- Isolez les SI de gestion technique
 - des SI "métiers"
 - entre les différentes fonctions
 - selon leur exposition
- Ne les abandonnez pas...
 - mettez en œuvre les mêmes mesures d'hygiène que sur vos SI métiers
 - gestion des vulnérabilités, durcissement...

1	Virtualisation de l'infrastructure	489
2	Architectures cloud	503
3	Systèmes industriels	514
4	Gestion technique des bâtiments	525
5	To be continued...	532

- Besoin en disponibilité très variable selon les usages
 - Redondance
 - Serveurs applicatifs, serveurs d'appels, passerelles et IPBX
 - Liens opérateurs
- Besoin en confidentialité et en intégrité dans tous les cas

- Quelques mesures essentielles :
 - Isolation complète physique ou logique
 - Si l'administration n'est pas dédiée, pas réellement complète
 - Segmentation en zones par type de composants (applicatifs, passerelles, etc.)
 - Privilégier le filaire
 - Authentification sur le réseau des téléphones IP
 - Durcissement des commutateurs de desserte (PVLAN, *port security*, etc.)
 - Chiffrement des flux (SRTP, SIP-TLS)
⇒ Jusqu'ici, identique à la gestion technique des bâtiments
- Mesures spécifiques supplémentaires :
 - Sécurité périphérique au niveau des *trunks SIP*
 - Déploiement de SBC (Session Border Controller)
 - Durcissement des commutateurs PoE (notamment désactivation des ports inutilisés)

- Krack^{aa}, WPA3 DragonBlood^{ab}
 - Si possible : se passer du sans-fil
- Sinon, essentiellement trois groupes de mesures
 - Tenir à jour les différents composants
 - Pilotes sur les postes, firmware des points d'accès
 - Sécuriser le point d'accès
 - PVLAN au niveau des réseaux sans fil
 - Interface d'administration inaccessible depuis les réseaux Wi-Fi
 - Pare-feu entre les points d'accès et le réseau interne
 - Désactivation du WPS (Wi-Fi Protected Setup)
 - (Limitation de la portée du signal - antennes directionnelles)
 - Sécuriser la connexion
 - Bannir le PSK ⇒ WPA-Entreprise
 - Indisponibilité suite au renouvellement de la clef partagée
 - WPA2 (/WPA3) + AES-CCMP
 - Isoler les réseaux "invités"

- Répartition d'une partie des traitements d'une application sur une grappe de machines
 - L'application doit être découpée pour réaliser des traitements parallèles indépendants
- Essentiellement utilisé dans le domaine de la recherche scientifique et pour du calcul financier et industriel (simulations)
 - Mais pas seulement!
 - SETI²⁶@home
 - Cryptominage

- Problématiques essentiellement applicatives
 - Intégrité du calcul
 - Confidentialité de l'information
 - ⇒ Traitement d'un tout petit morceau qui n'a pas de valeur seul
- Problématiques d'architecture
 - ⇒ Services applicatifs
 - ⇒ Ascendant/descendant

- Quelle différence avec une architecture distribuée ?
 - Orchestration et architectures en micro-services
 - Conteneurisation
 - ⇒ Exemple : kubernetes + docker
- Problématiques d'architecture
 - ⇒ Services applicatifs
 - ⇒ Virtualisation
 - Sensibilité de l'orchestrateur vs. console de gestion
 - Cloisonnement des équipements physiques/virtuels
 - on-premises/cloud* supportant les déploiements
 - Plus généralement : partage de ressources entre composants de sensibilité hétérogène
 - Partage et stockage de secrets (mots de passe, clefs de chiffrement, clefs d'API, etc.)
 - Privilèges des conteneurs
 - *Software-defined network*
 - [...]

Internet des objets (ISO/IEC 20924 :2018)

Infrastructure d'entités, personnes, systèmes et ressources informationnelles interconnectées avec des services qui traitent et réagissent à des informations du monde physique et du monde virtuel.

- Traitement de données sensibles
 - Données à caractère personnel (dont données de santé)
 - Données de paiement
 - Données de l'environnement (capteurs)
- Physiquement non contrôlés
- Ressources limitées
 - La cryptographie coûte cher en temps processeur
- Environnements difficiles à sécuriser
 - Plateformes, systèmes et protocoles très hétérogènes

- Sur les produits finis : mesures de sécurité essentiellement sur le durcissement local
- Protocoles (de contrôle et locaux) intrinsèquement non sécurisés
 - Pas de chiffrement, pas d'authentification, parfois contrôle d'intégrité
 - Donc surcouches : TLS/DTLS, VPN
- Qualité de code généralement faible
 - Audit, mise à jour si disponible

- PKI (Public Key Infrastructure), KMS (Key Management System), HSM (Hardware Security Module)
- Cœur de réseau, MPLS (MultiProtocol Label Switching)
- Vidéoconférence, salles de réunions
- Copieurs multifonctions
- BYOD/AVEC, COPE, MDM, CYOD
- Protocoles non IP : X.25, série, IPX
- Déclinaisons spécifiques d'IoT
 - Véhicules connectés
 - Équipements industriels dispatchés (gestion de réseaux de distribution)
 - Domotique (pas vraiment dans la sphère professionnelle)
- Réseau SSI (sondes, gestion d'incident, ...)

^a IEEE 802.1D (LAN/MAN : MAC bridges)

https://standards.ieee.org/standard/802_1D-2004.html

^b RFC 826 (ARP)

<https://tools.ietf.org/html/rfc826>

^c IEEE 802.1Q (VLAN)

<http://www.ieee802.org/1/pages/802.1Q-2014.html>

^d RFC 7348 (VXLAN)

<https://tools.ietf.org/html/rfc7348>

^e VRF hopping sur routeur Huawei

<https://www.cvedetails.com/cve/CVE-2015-8087/>

^f VRF hopping sur composants HPE

<https://www.cvedetails.com/cve/CVE-2015-5434/>

^g NIST SP 800-63B (Digital Identity Guidelines-Authentication and Lifecycle Management)

<https://pages.nist.gov/800-63-3/sp800-63b.html>

h Échappement de machine virtuelle sur Oracle VM Virtualbox

<https://cvedetails.com/cve/CVE-2018-2698/>

i Échappement de machine virtuelle sur Oracle VM Virtualbox

<https://cvedetails.com/cve/CVE-2018-2844/>

j Échappement de machine virtuelle sur VMware Workstation Fusion

<https://cvedetails.com/cve/CVE-2017-4934/>

k Exécution de code à distance à travers rdesktop et xrdp

<https://research.checkpoint.com/>

[reverse-rdp-attack-code-execution-on-rdp-clients/](https://research.checkpoint.com/reverse-rdp-attack-code-execution-on-rdp-clients/)

l Exécution de code à distance à travers mstsc (client RDP de Microsoft)

<https://cvedetails.com/cve/CVE-2019-0887/>

m Exécution de code à distance à travers mstsc (client RDP de Microsoft)

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1333>

n Présentation WSUSPect (Black Hat 2015)

[https://www.blackhat.com/docs/us-15/materials/
us-15-Stone-WSUSpect-Compromising-Windows-Enterprise-Via-Windows-Update.pdf](https://www.blackhat.com/docs/us-15/materials/us-15-Stone-WSUSpect-Compromising-Windows-Enterprise-Via-Windows-Update.pdf)

- Papier WSUSpendu (SSTIC 2017)

[https://www.sstic.org/media/SSTIC2017/SSTIC-actes/wsus_pendu/
SSTIC2017-Article-wsus_pendu-coltel_le-provost.pdf](https://www.sstic.org/media/SSTIC2017/SSTIC-actes/wsus_pendu/SSTIC2017-Article-wsus_pendu-coltel_le-provost.pdf)

- Présentation WSUSpendu (Black Hat 2017)

[https://www.blackhat.com/docs/us-17/wednesday/
us-17-Coltel-WSUSpendu-Use-WSUS-To-Hang-Its-Clients.pdf](https://www.blackhat.com/docs/us-17/wednesday/us-17-Coltel-WSUSpendu-Use-WSUS-To-Hang-Its-Clients.pdf)

- RFC 5798 (VRRP)

<https://tools.ietf.org/html/rfc5798>

- RFC 2281 (HSRP)

<https://tools.ietf.org/html/rfc2281>

- RFC 2328 (OSPF)

<https://tools.ietf.org/html/rfc2328>

^t RFC 5340 (OSPF avec IPv6)

<https://tools.ietf.org/html/rfc5340>

^u RFC 1195 (IS-IS dans des environnements TCP/IP)

<https://tools.ietf.org/html/rfc1195>

^v RFC 1058 (RIP)

<https://tools.ietf.org/html/rfc1058>

^w RFC 2453 (RIPv2)

<https://tools.ietf.org/html/rfc2453>

^x RFC 4271 (BGP)

<https://tools.ietf.org/html/rfc4271>

^y RFC 2395 (TCP MD5 pour BGP)

<https://tools.ietf.org/html/rfc2385>

^z RFC 3704 (uRPF)

<https://tools.ietf.org/html/rfc3704>

^{aa} Vulnérabilité Krack (WPA2)

<https://www.krackattacks.com/>

^{ab} Vulnérabilité DragonBlood (WPA3)

<https://wpa3.mathyvanoef.com/>

Annexes

mars 2021



Hervé Schauer Sécurité



©Hervé Schauer Sécurité 2021

Wenyoung WANG

547

1 Liste des acronymes

548

- ACL : Access Control List
- AD : Active Directory
- API : Application Programming Interface
- ARP : Address Resolution Protocol
- AVEC : Apportez Votre Équipement personnel de Communication
- BSD : Berkeley Software Distribution
- BYOD : Bring Your Own Device
- CAM : Content Addressable Memory
- CARP : Common Address Redundancy Protocol
- CAS : Central Authentication Service
- CDN : Content Delivery Network
- CHAP : Challenge-Handshake Authentication Protocol
- CLI : Command-Line Interface
- COPE : Corporate Owned Personally Enabled

- CRAM : Challenge-Response Authentication Mechanism
- CRC : Cyclic Redundancy Check
- CYOD : Choose Your Own Device
- CaaS : Communications as a Service
- DC : Domain Controller
- DES : Data Encryption Standard
- DMZ : DeMilitarized Zone
- DTLS : Datagram Transport Layer Security
- DTP : Dynamic Trunking Protocol
- DaaS : Data as a Service
- Daas : Desktop as a Service
- DoS : Denial of Services
- EAP : Extensible Authentication Protocol
- EGP : Exterior Gateway Protocol

- EIGRP : Enhanced Interior Gateway Routing Protocol
- ESAE : Enhanced Security Administrative Environment
- ESX : Elastic Sky X
- FAST : Flexible Authentication via Secure Tunneling
- FCS : Frame Check Sequence
- GLBP : Gateway Load Balancing Protocol
- HI(D/P)S : Host-based Intrusion Detection/Prevention System
- HSM : Hardware Security Module
- HSRP : Hot Standby Router Protocol
- ICS : Industrial Control System
- IDS : Intrusion Detection System
- IDaaS : IDentity as a Service
- IGRP : Interior Gateway Routing Protocol
- IKE : Internet Key Exchange

- IP : Internet Protocol
- IPFIX : IP Flow Information Export
- IPS : Intrusion Prevention System
- IPv4 : Internet Protocol v4
- IPv6 : Internet Protocol v6
- IS-IS : Intermediate System to Intermediate System
- ISA : International Society of Automation
- ISP : Internet Service Provider
- IT : Information Technology
- IaaS : Infrastructure as a Service
- IoT : Internet of Things
- JEA : Just Enough Admin
- JVM : Java Virtual Machine
- JiTA : Just in Time Admin

- KISS : Keep It Simple, Stupid !
- KMS : Key Management System
- KVM : Kernel-based Virtual Machine
- KVM : Keyboard-Video-Mouse (switch)
- LAN : Local Area Network
- LDAP : Lightweight Directory Access Protocol
- LM : LAN Manager
- LXC : LinuX Containers
- MAC : Media Access Control
- MD4 : Message Digest 4
- MD5 : Message Digest 5
- MDM : Mobile Device Management
- MIM : Microsoft Identity Management
- MIT : Massachusetts Institute of Technology

- MPLS : MultiProtocol Label Switching
- MSTP : Multiple Spanning-Tree Protocol
- NAT : Network Address Translation
- NDP : Neighbour Discovery Protocol
- NFS : Network File System
- NI(D/P)S : Network-based Intrusion Detection/Prevention System
- NPM : Network Performance Monitor
- NT : New Technology
- NTLM : NT LAN Manager
- NaaS : Network as a Service
- OSPF : Open Shortest Path First
- OUI : Organizational Unique Identifier
- PAP : Password Authentication Protocol
- PAT : Port Address Translation

- PEAP : Protected EAP
- PFS : Perfect Forward Secrecy
- PIM : Privileged Identity Management
- PKI : Public Key Infrastructure
- PLC : Programmable Logic Controller
- POP : Point Of Presence
- PPP : Point-to-Point Protocol
- PSC : Platform Services Controller
- PSK : Pre-Shared Key
- PVLAN : Private VLAN
- PaaS : Platform as a Service
- RADIUS : Remote Authentication Dial-In User Service
- RBAC : Role Based Access Control
- RCE : Remote Code Execution

- RDP : Remote Desktop Protocol
- RIP : Routing Information Protocol
- RODC : Read-Only Domain Controller
- RPKI : Resource Public Key Infrastructure
- RSTP : Rapid Spanning-Tree Protocol
- RTSP : Real-Time Streaming Protocol
- SAML : Security assertion markup language
- SAN : Storage Area Network
- SASL : Simple Authentication and Security Layer
- SBC : Session Border Controller
- SCADA : Supervisory Control And Data Acquisition
- SCP : Secure CoPy
- SCRAM : Salted Challenge Response Authentication Mechanism
- SCTP : Stream Control Transmission Protocol

- SDN : Software-Defined Network
- SETI : Search for Extra-Terrestrial Intelligence
- SFTP : SSH File Transfer Protocol
- SI : Système d'Information
- SIP : Session Initiation Protocol
- SIS : Safety Instrumented Systems
- SMTP : Simple Mail Transfer Protocol
- SPAN : Switched Port Analyzer
- SPB : Shortest Path Bridging
- SPNEGO : Simple and Protected GSSAPI Negotiation Mechanism
- SPOF : Single Point Of Failure
- SRTP : Secure Real-time Transport Protocol
- SSH : Secure Shell
- SSL : Secure Sockets Layer

- SSO : Single Sign-On
- STP : Spanning-Tree Protocol
- SaaS : Software as a Service
- SecaaS : Security as a Service
- StaaS : Storage as a Service / DSaaS
- TACACS : Terminal Access Controller Access-Control System
- TAP : Test/Terminal Access Point
- TCP : Transmission Control Protocol
- TLS : Transport Layer Security
- TRILL : TRansparent Interconnection of Lots of Links
- ToIP : Telephony over Internet Protocol
- UO : Unité d'Organisation
- URL : Uniform Resource Locator
- VACL : VLAN Access Control Lists

- VAMI : Virtual Appliance Management Interface
- VFD : Variable-Frequency Drive
- VIP : Virtual IP Address
- VLAN : Virtual Local Area Network
- VNC : Virtual Network Computing
- VRF : Virtual Routing and Forwarding
- VRRP : Virtual Router Redundancy Protocol
- VTP : VLAN Trunking Protocol
- VXLAN : Virtual eXtensible LAN
- WAF : Web Application Firewall
- WDM : Wavelength Division Multiplexing
- WIDS : Wireless Intrusion Detection System
- WPS : Wi-Fi Protected Setup
- WinRM : Windows Remote Management (Powershell remoting)

- eBGP : Exterior Border Gateway Protocol
- hmac : Keyed-hash Message Authentication Code
- iBGP : Interior Border Gateway Protocol
- iSCSI : Internet Small Computer Systems Interface
- pbkdf : Password-Based Key Derivation Function
- uRPF : Unicast Reverse Path Forwarding
- vCSA : vCenter Server Appliance