Sécurité et réseaux : mythes et réalités

Olivier Levillain

ANSSI/CyberEdu

Journée CyberEdu à Nantes
19 avril 2018

Table des matières

Présentation du LRP (1/2)

Activités du laboratoire Sécurité des réseaux et protocoles de l'ANSSI

- l'Observatoire de la résilience de l'Internet en France
  - analyse des annonces BGP
  - détection d'usurpations de préfixe
  - analyse des zones DNS du `.fr` (avec l'Afnic)
  - un rapport annuel sur les résultats

- DDoS (*Distibuted Denial of Service*)
  - compréhension des vecteurs d'attaque (ex. : amplification DNS et NTP)
  - recommandations
  - participation au développement de contremesures (*Advanced Blackholing*)

Présentation du LRP (2/2)

Activités du LRP (suite)

- systèmes industriels (SCADA)
  - préprocesseur Modbus dans Suricata
  - mise en place d'une plateforme pour tester les équipements
  - recommandations (classification, architecture)
- sécurité des applications web
- étude des protocoles et technologies
  - SSL/TLS
  - OpenFlow
  - ...

Table des matières

Table des matières

Rappels sur la démarche en général

- L'objectif n'est *pas* l'analyse fine des protocoles cryptographiques ni l'implémentation de piles TLS sécurisées
- Comme pour les autres volets de la formation, l'idée est de proposer aux étudiants une vision qui va au-delà de l'approche fonctionnelle
- Cela repose sur le développement d'un esprit critique

Le canal de communication : idéal

Derrière un réseau, il y a toujours une notion de bus/canal de communication partagé entre les interlocuteurs

Le canal de communication : idéal

Derrière un réseau, il y a toujours une notion de bus/canal de communication partagé entre les interlocuteurs

Souvent, le canal de communication est idéalisé

- on ne s'intéresse qu'aux participants *légitimes*
- on modélise les échanges par l'envoi et la réception de *messages* bien délimités et formatés

Le canal de communication : réalité

En réalité, la transmission repose sur une couche physique :

- des variations de tension/d'intensité sur une paire de cuivre
- des signaux lumineux au sein d'une fibre optique
- des signaux électromagnétiques transmis sur une fréquence donnée

Le canal de communication : réalité

En réalité, la transmission repose sur une couche physique :

- des variations de tension/d'intensité sur une paire de cuivre
- des signaux lumineux au sein d'une fibre optique
- des signaux électromagnétiques transmis sur une fréquence donnée

Dès lors, on peut se demander :

- comment se fait l'accès au canal physique
  - possibilités d'interception et de modification des messages ?

Le canal de communication : réalité

En réalité, la transmission repose sur une couche physique :

- des variations de tension/d'intensité sur une paire de cuivre
- des signaux lumineux au sein d'une fibre optique
- des signaux électromagnétiques transmis sur une fréquence donnée

Dès lors, on peut se demander :

- comment se fait l'accès au canal physique
  - possibilités d'interception et de modification des messages ?
- comment sont encodés/décodés les échanges ?
  - découpage des trames (attaques de type *packet-in-packet*)
  - *parsing* des messages

Le canal de communication : réalité

En réalité, la transmission repose sur une couche physique :

- des variations de tension/d'intensité sur une paire de cuivre
- des signaux lumineux au sein d'une fibre optique
- des signaux électromagnétiques transmis sur une fréquence donnée

Dès lors, on peut se demander :

- comment se fait l'accès au canal physique
  - possibilités d'interception et de modification des messages ?
- comment sont encodés/décodés les échanges ?
  - découpage des trames (attaques de type *packet-in-packet*)
  - *parsing* des messages

Combien d'étudiants ont cette vision d'un paquet IP ?

Description des protocoles

Souvent, l'objectif principal est de décrire les besoins fonctionnels.

Description des protocoles

Souvent, l'objectif principal est de décrire les besoins fonctionnels.

Au-delà de la description des protocoles par les standards, comment réagir à des stimuli inhabituels ?

- fragments IP se recouvrant de manière incohérente
- longueur de segment maximum (MSS) nulle dans TCP
- en-têtes redondants dans une requête HTTP

Description des protocoles

Souvent, l'objectif principal est de décrire les besoins fonctionnels.

Au-delà de la description des protocoles par les standards, comment réagir à des stimuli inhabituels ?

- fragments IP se recouvrant de manière incohérente
- longueur de segment maximum (MSS) nulle dans TCP
- en-têtes redondants dans une requête HTTP

Quand on parle de sécurité, le principe de robustesse « *Be liberal in what you accept, and conservative in what you send* » est **dangereux** !

Illustrations

- Les planches à venir sont des illustrations
  - il ne s'agit pas d'un cours
  - l'objectif n'est pas l'exhaustivité
- Présentation de quelques aspects de la sécurité attenant aux notions présentées
- Contenu à adapter aux sujets traités

Table des matières

Analyse de trafic réseau

Wireshark, un outil très puissant pour analyser un protocole avec les étudiants.

En sécurité, on se posera des questions telles que

- quelles sont les informations circulant en clair sur le réseau ?
- dépendance entre les protocoles (ARP, DNS, HTTP par exemple)
- quid d'un protocole X tournant sur le port du protocole Y ?

Dissection et création de paquets

D'autres outils, tels que Scapy, permettent non seulement d'analyser le trafic reçu, mais également de forger des paquets pour interagir avec des implémentations réelles.

Au-delà du fonctionnel, ces outils permettent de mieux comprendre la nature des messages échangés, et de les modifier.

Exemples de manipulations simples avec Scapy

- test de règles de *firewall*
- rejeu de paquets (avec des modifications)

L'attaquant réseau

Grâce à ces outils, les étudiants peuvent prendre conscience de ce que peut faire un attaquant réseau ayant accès au canal de communication :

- écoute du trafic
- émission de trafic en usurpant des champs source/identité
- modification, insertion, destruction de messages

L'idée souvent répandue est que les messages réseau ne peuvent être échangés que par des acteurs légitimes. Ce mythe a la vie dure, et il est utile de retirer le côté magique des échanges réseau.

Quelques cas non triviaux

- Protocoles propriétaires non documentés
  - là encore, une idée reçue est qu'ils sont moins vulnérables que les protocoles ouverts
  - en pratique, il reste souvent possible de forger des messages corrects
  - des méthodes d'analyse permettent de décortiquer les protocoles (outils tels que Netzob)
  - protocole peu connu = protocole souvent fragile (car pas regardé)

Quelques cas non triviaux

- Protocoles propriétaires non documentés
  - là encore, une idée reçue est qu'ils sont moins vulnérables que les protocoles ouverts
  - en pratique, il reste souvent possible de forger des messages corrects
  - des méthodes d'analyse permettent de décortiquer les protocoles (outils tels que Netzob)
  - protocole peu connu = protocole souvent fragile (car pas regardé)
- Protocoles utilisant de la cryptographie
  - sujet abordé plus tard
  - on peut déjà dire que la cryptographie peut être contournée dans de (trop) nombreux cas

Pour aller plus loin

Pour aller plus loin

- la vision que les outils nous apportent est-elle fidèle ?
- en particulier, quid des vulnérabilités des dissecteurs eux-mêmes ?

CVE Wireshark

CVE Details
The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register Reset Password Activate Account

Vulnerability Feeds & W

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View BID :
Go
(e.g.: 12345)
Search By Microsoft

Wireshark » Wireshark : Vulnerability Statistics

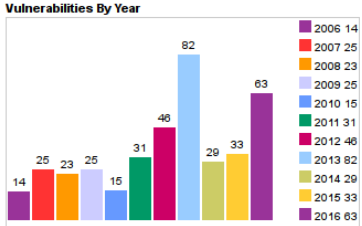
Vulnerabilities (386) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules
Related OVAL Definitions : Vulnerabilities (435) Patches (109) Inventory Definitions (1) Compliance Definitions (0)
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2006	14	12	1												
2007	25	25	4	5											1
2008	23	22	1	1							3				1
2009	25	23	3	4											1
2010	15	11	3	6	1										4
2011	31	29	4	9	1							1			2
2012	46	42	4	15							1				
2013	82	82		18	1										1
2014	29	29	2	17	2										1
2015	33	33		5	1										
2016	63	62		23								1			
Total	386	370	22	103	6						4	2			11
% Of All		95.9	5.7	26.7	1.6	0.0	0.0	0.0	0.0	0.0	1.0	0.5	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they m
those years.)

Vulnerabilities By Year



Vulnerabilities By Type

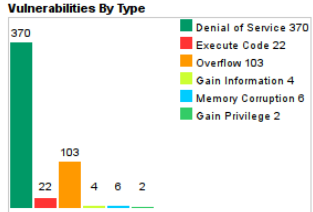


Table des matières

Spoofing ARP

Le principe d'ARP est le suivant :

- « Qui a l'adresse IP A.B.C.D ? Merci de répondre à <MAC> ? »
- « J'ai l'adresse IP A.B.C.D et mon adresse MAC est... »

Cette adresse MAC sera ensuite utilisée pour échanger les messages au sein du sous-réseau.

Spoofing ARP

Le principe d'ARP est le suivant :

- « Qui a l'adresse IP A.B.C.D ? Merci de répondre à <MAC> ? »
- « J'ai l'adresse IP A.B.C.D et mon adresse MAC est... »

Cette adresse MAC sera ensuite utilisée pour échanger les messages au sein du sous-réseau.

Que se passe-t-il si

- une machine répond alors qu'aucune question ne lui a été posée ?
- une machine répond à une requête ne lui étant pas destiné ?
- une machine pose une question en mentant sur son adresse IP ?

Protection par adresse MAC

De nombreux équipements réseau proposent d'autoriser uniquement des messages provenant d'une liste blanche d'adresses MAC

- *boxes* ADSL
- commutateurs
- filtrage de l'accès à l'interface d'administration

Protection par adresse MAC

De nombreux équipements réseau proposent d'autoriser uniquement des messages provenant d'une liste blanche d'adresses MAC

- *boxes* ADSL
- commutateurs
- filtrage de l'accès à l'interface d'administration

De tels mécanismes sont très facilement contournables, car malgré une idée reçue qui a la vie dure, changer son adresse MAC est trivial sur de nombreux systèmes.

```
ifconfig eth0 hw ether 01:02:03:04:05:06
```

Protection ARP

Il existe d'autres techniques pour limiter ces problèmes, mais elles ne sont pas toujours robustes du point de vue de la sécurité :

- limiter le nombre maximum d'entrée par interface (détournable)
- vlan (vlan hoping)
- pvlan
- 802.1x (compliqué à mettre en oeuvre)
- DHCP snooping
- IP source guard

Usurpation d'adresses IP

Qu'est-ce qui empêche un attaquant de modifier l'adresse IP source ?

Usurpation d'adresses IP

Qu'est-ce qui empêche un attaquant de modifier l'adresse IP source ?

- BCP 38 (filtrage « au bord »)...
- ... rarement mis en oeuvre

Usurpation d'adresses IP

Qu'est-ce qui empêche un attaquant de modifier l'adresse IP source ?

- BCP 38 (filtrage « au bord »)...
- ... rarement mis en oeuvre

En pratique

- possibilité d'émettre en aveugle
- fonctionnement de base de nombreuses attaques DDoS

Usurpation d'adresses IP

Qu'est-ce qui empêche un attaquant de modifier l'adresse IP source ?

- BCP 38 (filtrage « au bord »)...
- ... rarement mis en oeuvre

En pratique

- possibilité d'émettre en aveugle
- fonctionnement de base de nombreuses attaques DDoS
- dans certains cas, il a même été possible de dérouter la réponse
  - source route option (IPv4)
  - type 0 routing headers (IPv6)

Fragmentation IP

Pour supporter des canaux des liens réseaux plus étroits, les paquets IP peuvent être amenés à être fragmentés.

Comment analyser de tels fragments au niveau d'un IDS/IPS ?

Fragmentation IP

Pour supporter des canaux des liens réseaux plus étroits, les paquets IP peuvent être amenés à être fragmentés.

Comment analyser de tels fragments au niveau d'un IDS/IPS ?

- mettre en attente les paquets jusqu'au dernier
  - risque de déni de service sur l'IDS/IPS

Fragmentation IP

Pour supporter des canaux des liens réseaux plus étroits, les paquets IP peuvent être amenés à être fragmentés.

Comment analyser de tels fragments au niveau d'un IDS/IPS ?

- mettre en attente les paquets jusqu'au dernier
  - risque de déni de service sur l'IDS/IPS
- traiter le contenu à la volée
  - risque d'imprécision (fragments désordonnés)
  - a priori, l'IDS « verra » autre chose que le service destinataire

Analyse de la structure de l'internet

BGP : le protocole fondateur d'internet

- différents acteurs (les AS) sont interconnectés par BGP
- échange d'informations sur les routes connues
- pas ou peu d'imputabilité formelle

Analyse de la structure de l'internet

BGP : le protocole fondateur d'internet

- différents acteurs (les AS) sont interconnectés par BGP
- échange d'informations sur les routes connues
- pas ou peu d'imputabilité formelle

Qu'est-ce qui empêche un AS d'annoncer des préfixes arbitraires ?

- a priori, rien
- la détection d'incidents
- les bonnes pratiques
- quelques initiatives (aujourd'hui essentiellement déclaratives)

Messagerie électronique (SMTP)

On comprend bien à quoi sert le champ destinataire (RCPT TO), mais quid de l'émetteur (MAIL FROM) ?

Messagerie électronique (SMTP)

On comprend bien à quoi sert le champ destinataire (RCPT TO), mais quid de l'émetteur (MAIL FROM) ?

Même question dans les en-têtes d'un e-mail (From : et To :).

Messagerie électronique (SMTP)

On comprend bien à quoi sert le champ destinataire (RCPT TO), mais quid de l'émetteur (MAIL FROM) ?

Même question dans les en-têtes d'un e-mail (From : et To :).

Quelques questions :

- que se passe-t-il si on modifie les champs « émetteur » ?
- qu'arrive-t-il lorsque MAIL FROM et From disent des choses différentes ?
- même chose avec RCPT TO et To ?
- existe-t-il des cas légitimes ?

Un peu de recul sur les manipulations de réseau

Usurpation d'identité

- ARP, adresses MAC
- IP, adresses IP
- SMTP, émetteur
- ...

Empoisonnement / détournement

- BGP, préfixes IP annoncés
- ARP, correspondance MAC/IP
- DNS, correspondance IP/noms de domaine
- Google, quel serait l'impact d'un empoisonnement du cache de recherche ?
- ...

Messagerie électronique (POP/IMAP)

POP

```
user toto
pass querty12
...
```

IMAP (LOGIN)

```
. authenticate login toto querty12
...
```

IMAP (PLAIN)

```
. authenticate plain dGVzdAB0b3RvAHF1ZXJ0eTEy
...
```

Messagerie électronique (POP/IMAP)

POP

```
user toto
pass querty12
...
```

IMAP (LOGIN)

```
. authenticate login toto querty12
...
```

IMAP (PLAIN)

```
. authenticate plain dGVzdAB0b3RvAHF1ZXJ0eTEy
...
```

```
dGVzdAB0b3RvAHF1ZXJ0eTEy =
base64(test<NUL>toto<NUL>querty12)
```

Messagerie électronique (MIME)

Les clients mail ont aujourd'hui tout le confort moderne (inclusion de pièces jointes, d'images, de contenu HTML).

Messagerie électronique (MIME)

Les clients mail ont aujourd'hui tout le confort moderne (inclusion de pièces jointes, d'images, de contenu HTML).

Questions :

- peut-on parler de visualisation de confiance ?
- la version textuelle est-elle « identique » à la version HTML ?
- que « voit » une passerelle qui analyse les mails (anti-virus) ?

Gestion des types de contenu (SMTP)

Le standard MIME décrit des « types » de ressources.

Que se passe-t-il si une pièce jointe `toto.exe` est annoncé comme de type `image/png` ?

Gestion des types de contenu (SMTP)

Le standard MIME décrit des « types » de ressources.

Que se passe-t-il si une pièce jointe `toto.exe` est annoncé comme de type `image/png` ?

- sur quelle base se font les tests sur les serveurs mail (anti-virus) ?

Gestion des types de contenu (SMTP)

Le standard MIME décrit des « types » de ressources.

Que se passe-t-il si une pièce jointe `toto.exe` est annoncé comme de type `image/png` ?

- sur quelle base se font les tests sur les serveurs mail (anti-virus) ?
- comment le fichier est-il interprété in fine sur le poste de l'utilisateur dans le client ?

Gestion des types de contenu (SMTP)

Le standard MIME décrit des « types » de ressources.

Que se passe-t-il si une pièce jointe `toto.exe` est annoncé comme de type `image/png` ?

- sur quelle base se font les tests sur les serveurs mail (anti-virus) ?
- comment le fichier est-il interprété in fine sur le poste de l'utilisateur dans le client ?
  - une fois le fichier sauvé ?

Gestion des types de contenu (HTTP)

Même question si un site web A inclut une resource en provenance du site B. Qui décide le type du fichier :

- la balise d'inclusion du site A ?
- le Content-Type du site B ?
- l'heuristique du navigateur ?

Gestion des types de contenu (HTTP)

Même question si un site web A inclut une resource en provenance du site B. Qui décide le type du fichier :

- la balise d'inclusion du site A ?
- le Content-Type du site B ?
- l'heuristique du navigateur ?

En pratique, dès que ces trois types ne sont pas alignés (ou qu'un des en-tête est absent), on court au devant de problèmes.

Vérification côté client ou serveur

De nombreux formulaires web contraignent le type des entrées saisies

- format spécifique attendu pour une adresse électronique
- champs obligatoires

Vérification côté client ou serveur

De nombreux formulaires web contraignent le type des entrées saisies

- format spécifique attendu pour une adresse électronique
- champs obligatoires

Où faire les vérifications ?

- traditionnellement, ces vérifications étaient faites côté serveur

Vérification côté client ou serveur

De nombreux formulaires web contraignent le type des entrées saisies

- format spécifique attendu pour une adresse électronique
- champs obligatoires

Où faire les vérifications ?

- traditionnellement, ces vérifications étaient faites côté serveur
- pour éviter un aller-retour sur le réseau, JavaScript est désormais utilisé pour faire les tests sur le client

Vérification côté client ou serveur

De nombreux formulaires web contraignent le type des entrées saisies

- format spécifique attendu pour une adresse électronique
- champs obligatoires

Où faire les vérifications ?

- traditionnellement, ces vérifications étaient faites côté serveur
- pour éviter un aller-retour sur le réseau, JavaScript est désormais utilisé pour faire les tests sur le client
- quelle est la robustesse de ces tests faits uniquement sur le client ?

Table des matières

Qu'est-ce qu'une architecture ?

Un ensemble comprenant

- des machines : postes clients, serveurs
- des équipements réseaux : switches, routeurs
- des équipements de sécurité : firewalls, terminaisons VPNs, antivirus

Une architecture *sécurisée*

- vise à fournir un ensemble de services
- en prenant en compte certaines menaces
  - défiguration de sites web
  - compromission de machines
  - fuite de données...

Flux et politique de filtrage

Matrice des flux

Avant toute mise en place d'un pare-feu, il est nécessaire d'élaborer une matrice des flux qui décrit les échanges réseaux légitimes entre les différents équipements.

Cette matrice des flux sert ensuite à écrire la politique de filtrage

Dans les cas classiques :

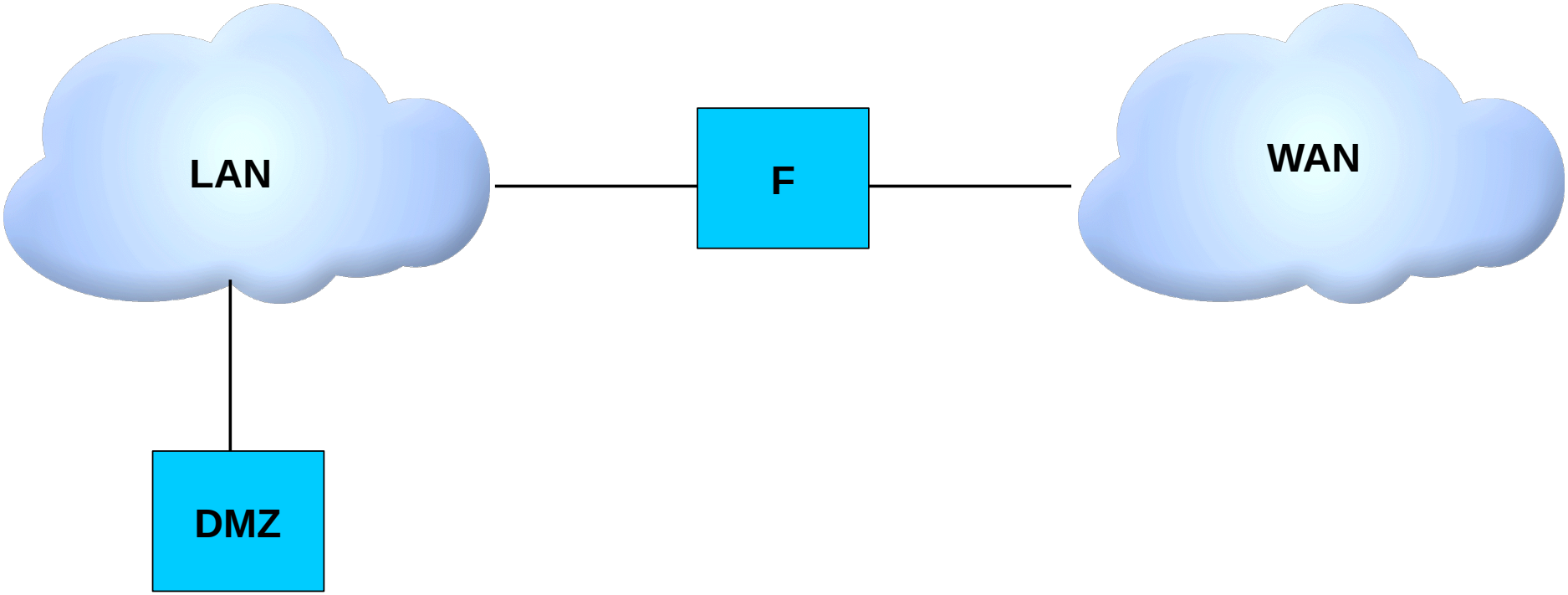
1. tout trafic est interdit
2. le trafic du LAN vers Internet est autorisé
3. le trafic d'Internet vers DMZ est autorisé

Légende des schémas

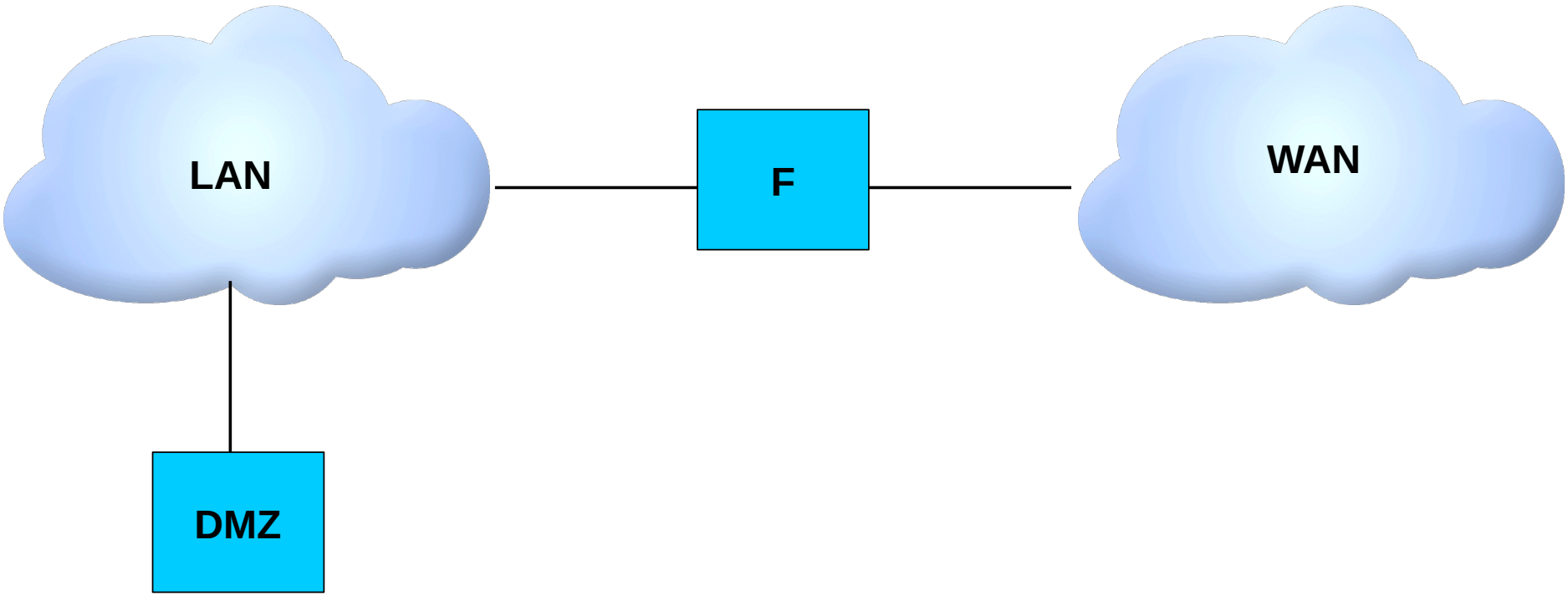
LAN	réseau interne, maîtrisé (*Local Area Network*)
WAN	réseau externe, non maîtrisé (*Wide Area Network*)
F	Pare-feu
DMZ	services opérationnels ou de sécurité (*DeMilizarized Zone*)
VPN	chiffreur IP (*Virtual Private Network*)
RAS	serveur d'accès distant (*Remote Access Server*)
S	station de supervision

Note : Les équipements de niveau 2 (commutateurs ethernet) ne sont pas représentés sur les schémas

Cas 0 : connexion directe (filtrée)



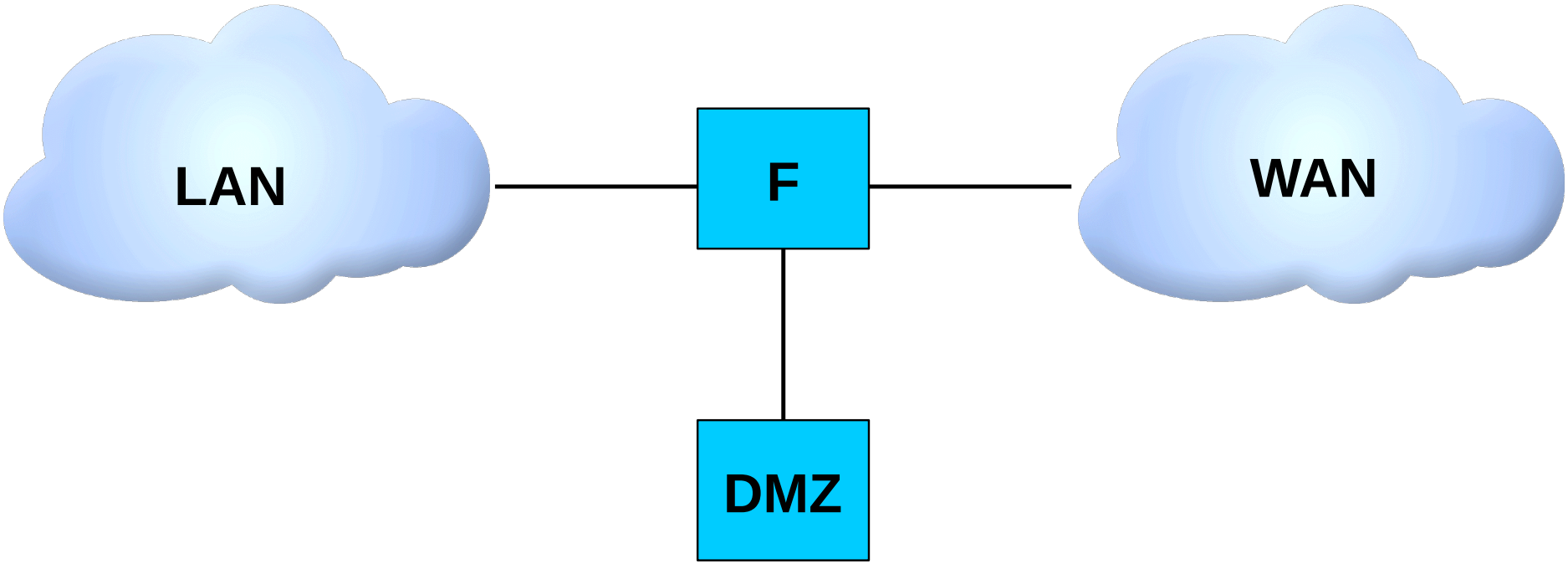
Cas 0 : connexion directe (filtrée)



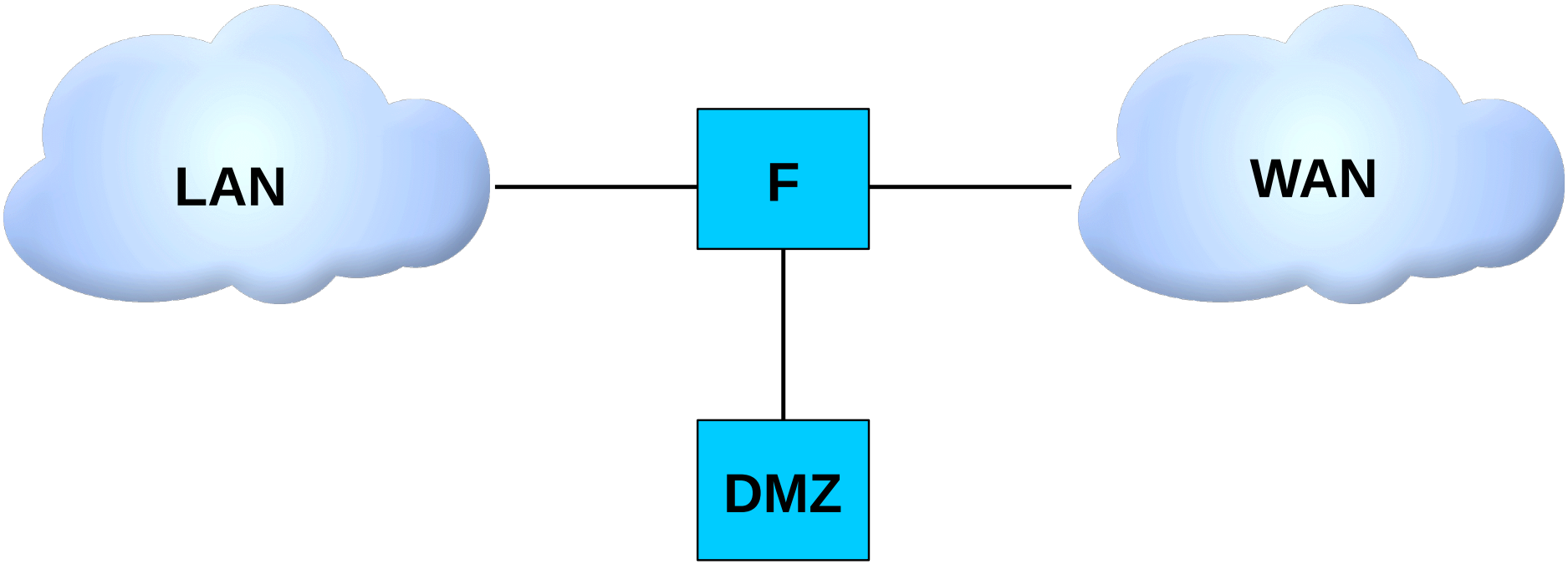
Cette architecture souffre de plusieurs problèmes

- le pare-feu est l'unique rempart
- les flux WAN à destination de la DMZ transitent par le LAN
- tous les services sont connectés directement à Internet

Cas 1 : isolement de la DMZ



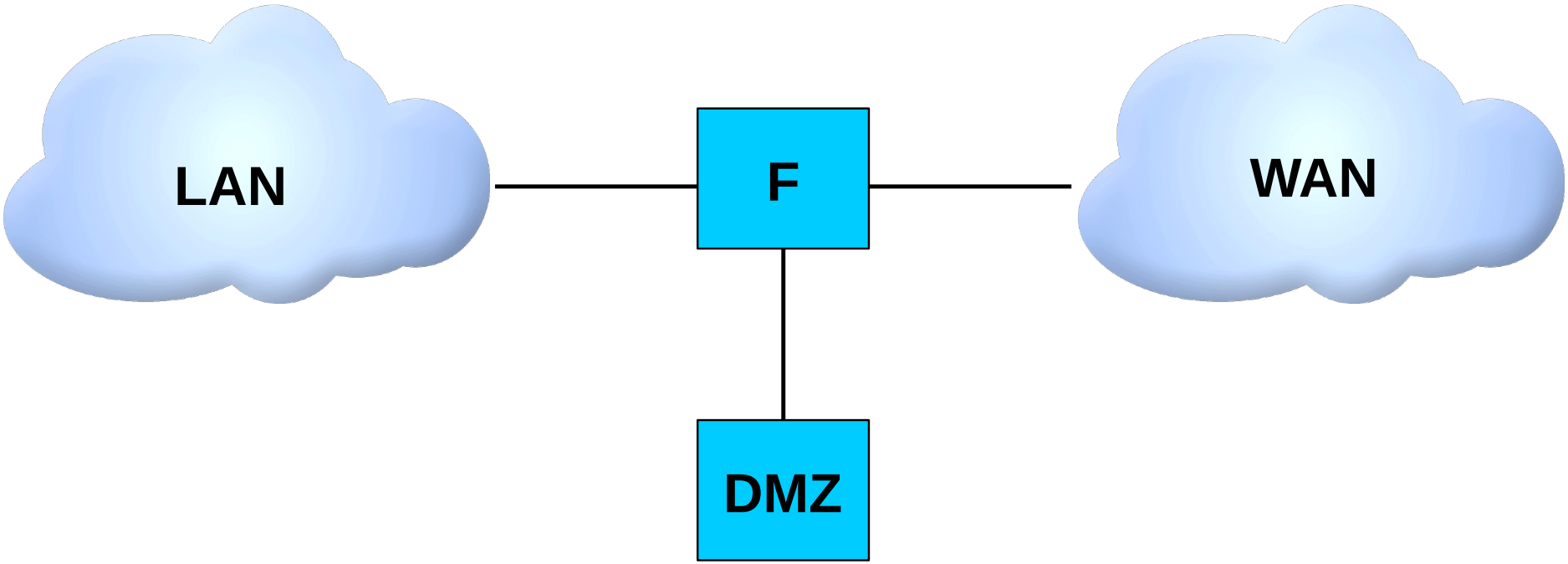
Cas 1 : isolement de la DMZ



Améliorations :

- les flux WAN à destination de la DMZ ne passent plus par le LAN

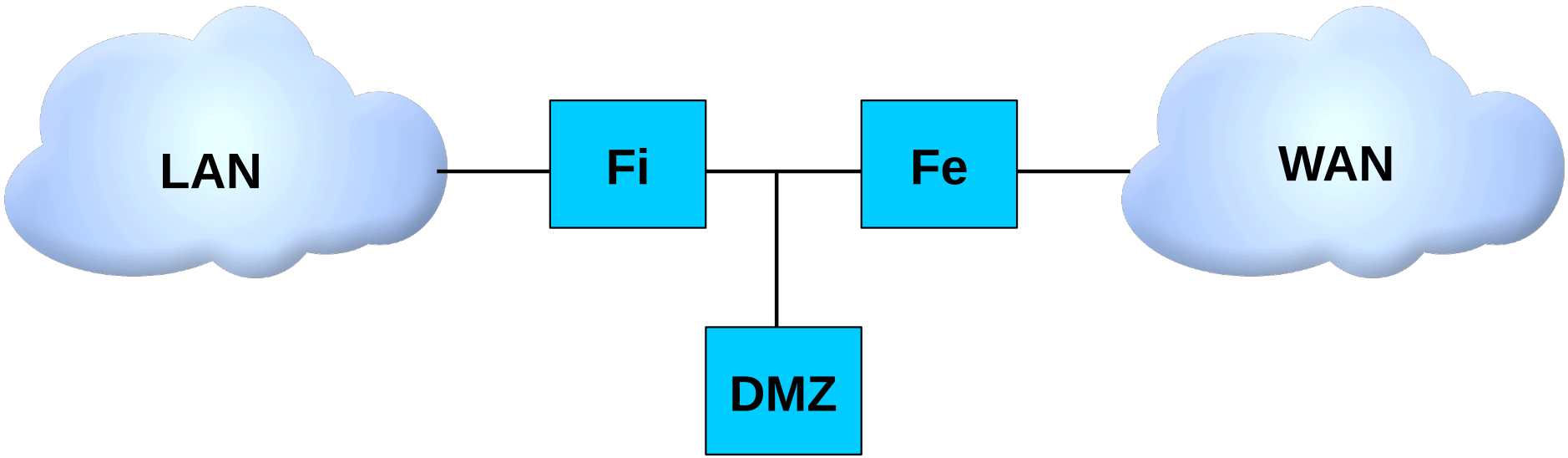
Cas 1 : isolement de la DMZ



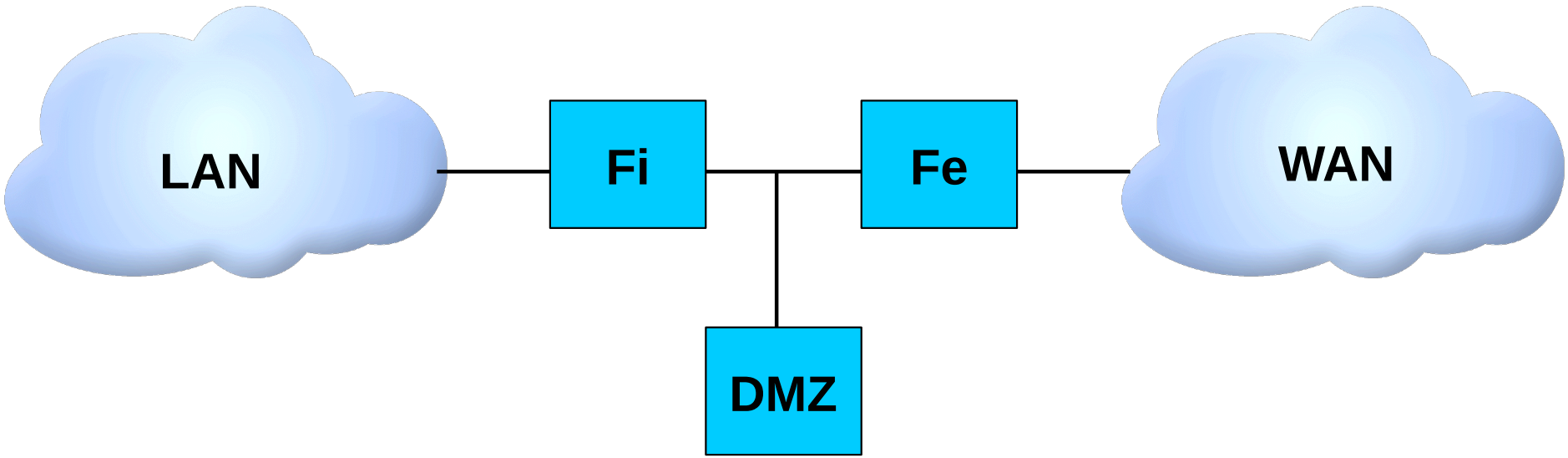
Problèmes persistants :

- le pare-feu est l'unique rempart
- tous les services sont connectés directement à Internet

Cas 2 : double filtrage



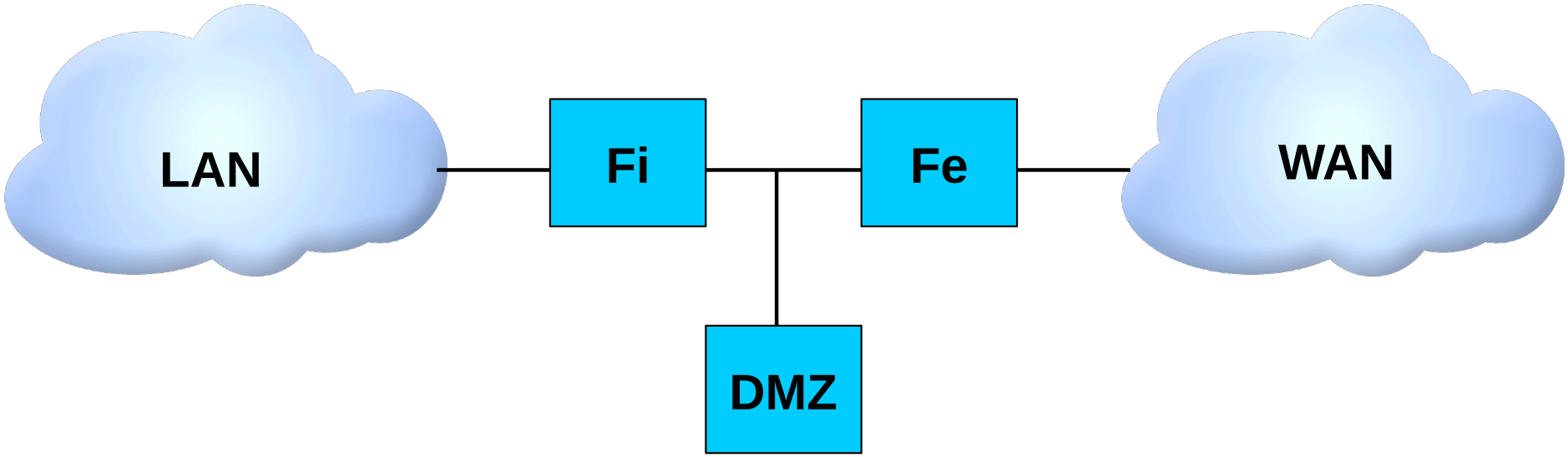
Cas 2 : double filtrage



Améliorations :

- la compromission de Fe ne permet pas d'attaquer directement le LAN
- la configuration de Fi est simplifiée

Cas 2 : double filtrage



Problèmes persistants :

- tous les services sont connectés directement à Internet

Pour aller plus loin : diversification technologique

Diversification à plusieurs niveaux

- logiciel :
  - système : Linux, OpenBSD, etc.
  - services
- matériel :
  - processeurs/architecture : x86, ARM, PowerPC etc.
  - périphériques (tels que les cartes réseau)

L'architecture ne fait pas tout

Le soin apporté à la définition d'une architecture robuste pour une passerelle d'interconnexion doit être complété par :

une sélection des composants individuels qui la composent

en fonction de :

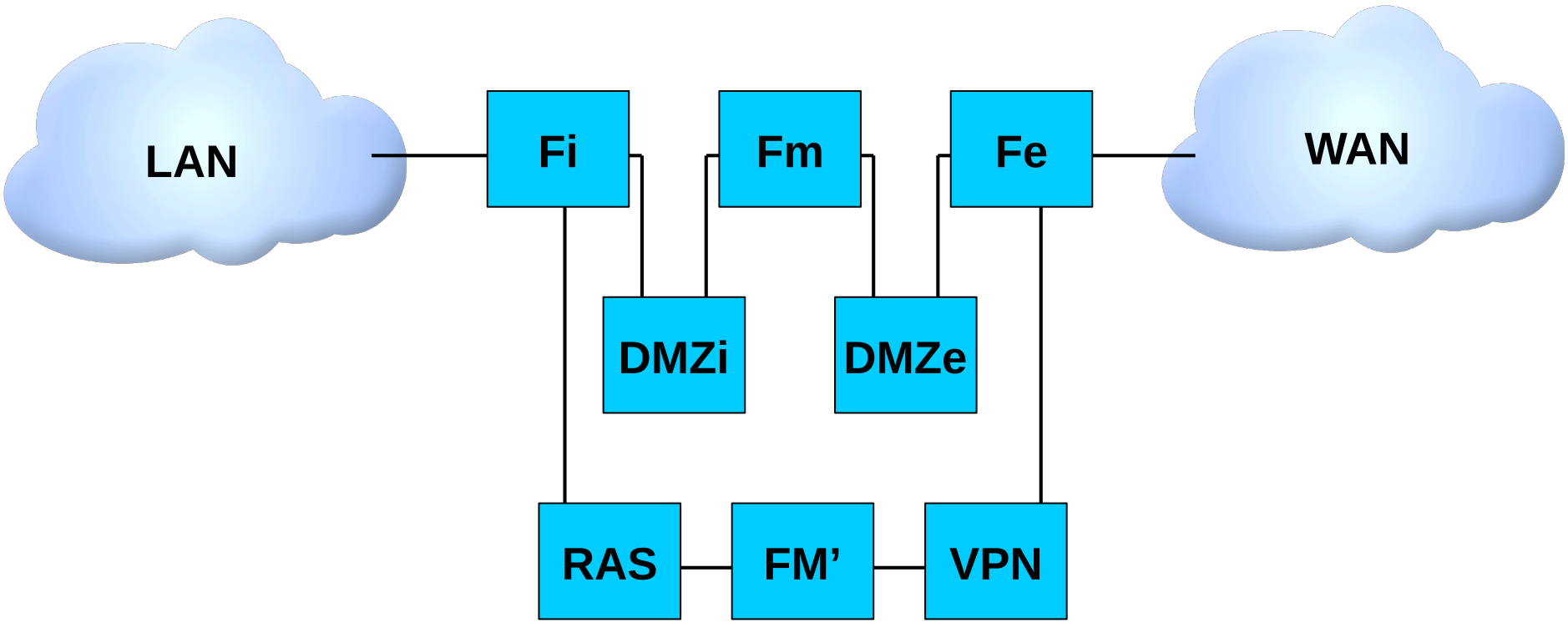
- leurs apports en terme de sécurité
- leur propre robustesse

un travail de maîtrise et de durcissement des équipements

pour assurer :

- une défense en profondeur contre les attaques non bloquées
- une protection contre les attaques internes

Autre exemple : double DMZ en coupure et accès distant



Détails de l'architecture

- les services peuvent être protégés par un *reverse proxy*
- les flux du tunnel chiffré arrivent sur une branche différente de l'architecture
- le *firewall* median (FM') traite les flux déchiffrés et limite les vecteurs d'attaque possibles
- le serveur d'accès distant peut être mis en place pour fournir un accès restreint aux postes nomades

Gestion des utilisateurs nomades

L'architecture précédente amène certaines questions :

- faut-il autoriser les postes nomades à se connecter au LAN ?
- doivent-ils passer par l'entreprise pour accéder à Internet ?

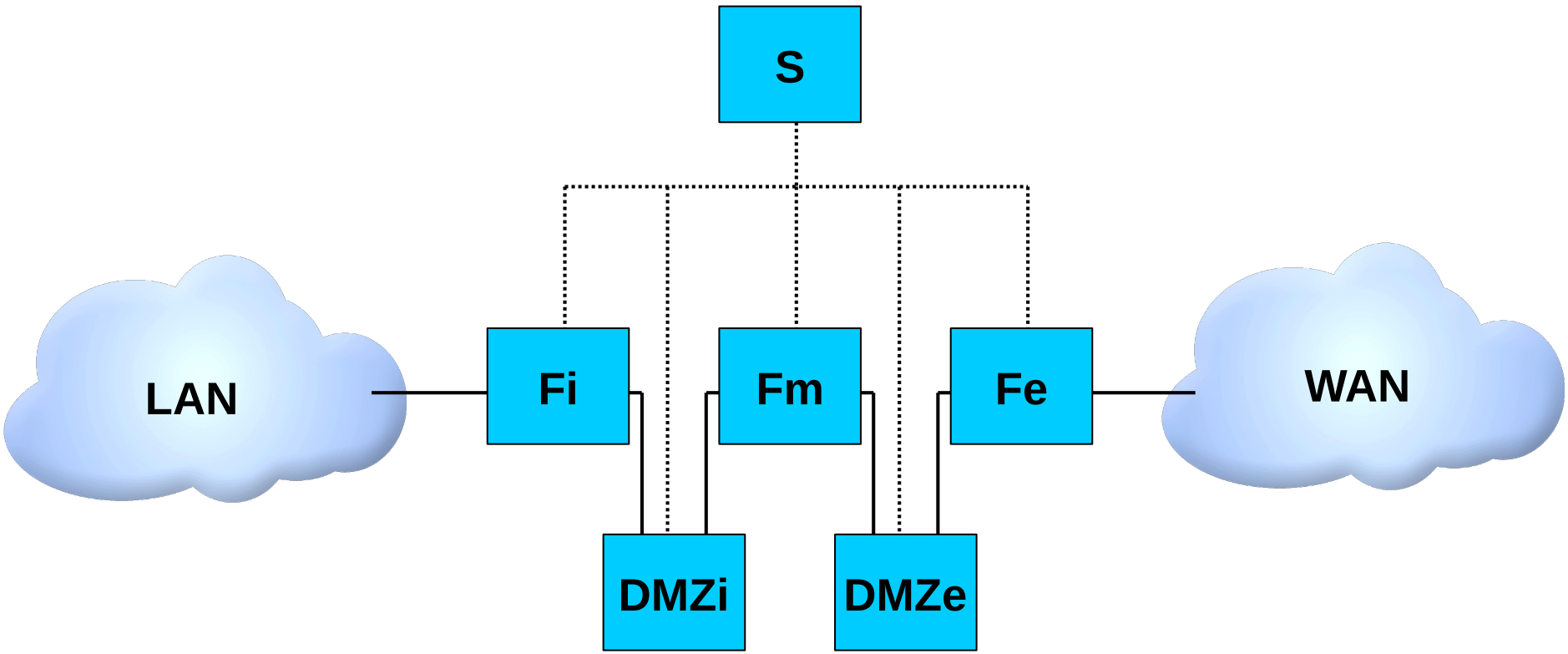
Au minimum il convient de

- durcir leur configuration (au moins autant que les postes fixes)
- les garder à jour

Se pose aussi la question de la confidentialité des données

- chiffrement des disques (en cas de perte ou vol)
- pas de consultation dans des lieux publics
  - transports en commun, cafés, etc.

Autre exemple : administration/supervision centralisée



Problèmes liés à l'administration centralisée

Les postes des administrateurs sont très sensibles

- éviter les rebonds (depuis FWe vers le LAN)
  - empêcher les flux initiés depuis les équipements vers les machines d'administration
- protéger les postes d'administration encore plus que les autres
- pas d'accès à Internet

À côté de l'architecture

Il convient de respecter différentes règles élémentaires

Notamment :

- la mise à jour des équipements et logiciels ;
- des privilèges limités ;
- la suppression des services inutiles ;
- un pare-feu local sur chaque machine ;
- la prise en compte des supports de stockage amovibles et des périphériques externes ;
- la sensibilisation des utilisateurs.

Voir aussi :

`http://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/`

Mises à jour

- De nombreux sites diffusent des informations sur les vulnérabilités connues
  - CERT-FR : `http://www.cert.ssi.gouv.fr`
- Parfois, aucune mise à jour n'existe, mais des solutions préventives sont données
- Il est important d'avoir connaissance des vulnérabilités résiduelles
  - Par exemple sur une fonctionnalité non utilisée, ou couverte par une mesure organisationnelle

Appliances et équipements divers

- Ce ne sont pas des boîtes magiques

Appliances et équipements divers

- Ce ne sont pas des boîtes magiques

- Quels sont les protocoles supportés ?
- Quels sont les flux légitimes ?

Appliances et équipements divers

- Ce ne sont pas des boîtes magiques

- Quels sont les protocoles supportés ?
- Quels sont les flux légitimes ?

- Ces questions semblent naturelles pour des serveurs, des passerelles ou des *firewalls*

Appliances et équipements divers

- Ce ne sont pas des boîtes magiques

- Quels sont les protocoles supportés ?
- Quels sont les flux légitimes ?

- Ces questions semblent naturelles pour des serveurs, des passerelles ou des *firewalls*

- Mais pour une imprimante réseau ?
- Ou une caméra IP ?
- Quelle doit être leur configuration réseau ?
- Est-ce normal que de tels périphériques émettent du *spam* ?

Configuration des équipements

- Restreindre la myriade de protocoles généralement supportés
- Modifier les mots de passe par défaut
- Supposer que les services souvent vulnérables
- Restreindre les clients potentiels (quitte à filtrer ou faire passer les requêtes par un proxy)

- Pour certains équipements, seule l'architecture permet de sécuriser l'ensemble

Lignes directrices

Quelques principes à respecter

- briser les flux entre le LAN et le WAN
  inversion du sens des flux et/ou analyse en couche applicative
- cloisonner les fonctions
  limitation des risques et des conséquences d'une compromission
- diversifier les technologies
  dans les limites permises par la maintenabilité du parc

Dans la durée

- effectuer les mises à jour de sécurité pertinentes
- suivre les journaux d'exploitation

Table des matières

GSM, 3G, 4G

- Un bel exemple de protocoles restés longtemps obscurs
  - spécifications complexes...
  - pas toujours accessibles librement/gratuitement

GSM, 3G, 4G

- Un bel exemple de protocoles restés longtemps obscurs
  - spécifications complexes...
  - pas toujours accessibles librement/gratuitement
- Lorsque les spécifications ont été regardées, de nombreux problèmes ont été mis au jour
  - connexions authentifiées de manière asymétriques
  - possibilité de négociation à la baisse
  - combinés ne rendant pas compte de l'état réel de la sécurité

GSM, 3G, 4G

- Un bel exemple de protocoles restés longtemps obscurs
  - spécifications complexes...
  - pas toujours accessibles librement/gratuitement
- Lorsque les spécifications ont été regardées, de nombreux problèmes ont été mis au jour
  - connexions authentifiées de manière asymétriques
  - possibilité de négociation à la baisse
  - combinés ne rendant pas compte de l'état réel de la sécurité
- En l'absence d'analyse concrète et poussée, un protocole ne doit pas être considéré comme sûr a priori !

WiFi

Un autre exemple fourmillant d'exemples liés à la sécurité :

- le standard de protection des flux n'étant pas prêt à temps, WEP a été bricolé

WiFi

Un autre exemple fourmillant d'exemples liés à la sécurité :

- le standard de protection des flux n'étant pas prêt à temps, WEP a été bricolé
- et cassé rapidement
- certaines variantes de WPA (et WPA2) sont cassées

WiFi

Un autre exemple fourmillant d'exemples liés à la sécurité :

- le standard de protection des flux n'étant pas prêt à temps, WEP a été bricolé
- et cassé rapidement
- certaines variantes de WPA (et WPA2) sont cassées
- mais que se passe-t-il si on offre un réseau ouvert avec le bon nom à votre portable ?

WiFi

Un autre exemple fourmillant d'exemples liés à la sécurité :

- le standard de protection des flux n'étant pas prêt à temps, WEP a été bricolé
- et cassé rapidement
- certaines variantes de WPA (et WPA2) sont cassées
- mais que se passe-t-il si on offre un réseau ouvert avec le bon nom à votre portable ?
- surtout que de nombreux systèmes annoncent à tout vent le nom des réseaux auxquels ils font confiance...

Table des matières

S/MIME

S/MIME apporte la signature et le chiffrement des mails

S/MIME

S/MIME apporte la signature et le chiffrement des mails

- Qu'est-ce qui est réellement protégé, parmi l'enveloppe, les en-têtes et le corps du message ?
- Mieux vaut éviter de signer un message ne contenant que `oui`, ou d'utiliser un sujet trop explicite pour un mail chiffré...
- Signer une URL ou des références à des images externes est-il une bonne idée ?

S/MIME

S/MIME apporte la signature et le chiffrement des mails

- Qu'est-ce qui est réellement protégé, parmi l'enveloppe, les en-têtes et le corps du message ?
- Mieux vaut éviter de signer un message ne contenant que `oui`, ou d'utiliser un sujet trop explicite pour un mail chiffré...
- Signer une URL ou des références à des images externes est-il une bonne idée ?

- Quels sont les algorithmes utilisés ?
- *S/MIME Capabilities* implémentées correctement nulle part...

S/MIME

S/MIME apporte la signature et le chiffrement des mails

- Qu'est-ce qui est réellement protégé, parmi l'enveloppe, les en-têtes et le corps du message ?
- Mieux vaut éviter de signer un message ne contenant que `oui`, ou d'utiliser un sujet trop explicite pour un mail chiffré...
- Signer une URL ou des références à des images externes est-il une bonne idée ?

- Quels sont les algorithmes utilisés ?
- *S/MIME Capabilities* implémentées correctement nulle part...

- Et la gestion des clés ?

S/MIME

S/MIME apporte la signature et le chiffrement des mails

- Qu'est-ce qui est réellement protégé, parmi l'enveloppe, les en-têtes et le corps du message ?
- Mieux vaut éviter de signer un message ne contenant que `oui`, ou d'utiliser un sujet trop explicite pour un mail chiffré...
- Signer une URL ou des références à des images externes est-il une bonne idée ?

- Quels sont les algorithmes utilisés ?
- *S/MIME Capabilities* implémentées correctement nulle part...

- Et la gestion des clés ?

- Quid des alternatives (GnuPG par exemple) ?
- Quid des webmails ?

RDP, SSH

Il existe quelques protocoles d'administration à distance

- Telnet, qui n'offre aucune protection

RDP, SSH

Il existe quelques protocoles d'administration à distance

- Telnet, qui n'offre aucune protection
- SSH, censé remplacer Telnet
  - SSH-1 ? SSH-2 ?
  - Encrypt-and-MAC ?
  - modèle de confiance ?
  - pour garantir quelque chose, utiliser la dernière version d'OpenSSH

RDP, SSH

Il existe quelques protocoles d'administration à distance

- Telnet, qui n'offre aucune protection
- SSH, censé remplacer Telnet
  - SSH-1 ? SSH-2 ?
  - Encrypt-and-MAC ?
  - modèle de confiance ?
  - pour garantir quelque chose, utiliser la dernière version d'OpenSSH
- Remote Desktop
  - une usine à gaz très très difficile à analyser
  - le diable est dans l'interopérabilité
  - pour garantir quoi que ce soit, nécessité d'un parc homogène et à jour

HTTPS et TLS : le cadenas dans un navigateur (1/3)

HTTPS = HTTP dans TLS

HTTPS et TLS : le cadenas dans un navigateur (1/3)

HTTPS = HTTP dans TLS

- contournements possibles
  - réécriture des URLs `https` en `http`
  - problème des pages avec contenu mixte
  - pages de *login* en `http`

HTTPS et TLS : le cadenas dans un navigateur (1/3)

HTTPS = HTTP dans TLS

- contournements possibles
  - réécriture des URLs `https` en `http`
  - problème des pages avec contenu mixte
  - pages de *login* en `http`
- éléments visuels
  - le cadenas, et sa compréhension par l'utilisateur moyen
  - la barre verte et les certificats EV
  - peu de cohérence d'un navigateur à l'autre (ou d'une version à l'autre)

HTTPS et TLS : le cadenas dans un navigateur (2/3)

- vérification des certificats
  - la majorité des applications mobiles ne vérifient rien
  - même quand un client vérifie le certificat, sait-on à combien d'autorités la confiance est accordée ?
  - nettoyage du magasin de certificats parfois possible...
  - mais à refaire à chaque mise à jour !

HTTPS et TLS : le cadenas dans un navigateur (2/3)

- vérification des certificats
  - la majorité des applications mobiles ne vérifient rien
  - même quand un client vérifie le certificat, sait-on à combien d'autorités la confiance est accordée ?
  - nettoyage du magasin de certificats parfois possible...
  - mais à refaire à chaque mise à jour !
- interactions difficiles avec l'écosystème web
  - *virtual hosting*
  - accélérateurs SSL, *proxies* et autres équipements
  - gestion des clés et des certificats ?

HTTPS et TLS : le cadenas dans un navigateur (3/3)

2014 : l'année où toutes les piles TLS majeures ont fait l'objet de vulnérabilités critiques

HTTPS et TLS : le cadenas dans un navigateur (3/3)

2014 : l'année où toutes les piles TLS majeures ont fait l'objet de vulnérabilités critiques

- février : `goto fail` Apple

HTTPS et TLS : le cadenas dans un navigateur (3/3)

2014 : l'année où toutes les piles TLS majeures ont fait l'objet de vulnérabilités critiques

- février : `goto fail` Apple
- février : `goto fail` GnuTLS

HTTPS et TLS : le cadenas dans un navigateur (3/3)

2014 : l'année où toutes les piles TLS majeures ont fait l'objet de vulnérabilités critiques

- février : `goto fail` Apple
- février : `goto fail` GnuTLS
- avril : *Heartbleed* dans OpenSSL

HTTPS et TLS : le cadenas dans un navigateur (3/3)

2014 : l'année où toutes les piles TLS majeures ont fait l'objet de vulnérabilités critiques

- février : `goto fail` Apple
- février : `goto fail` GnuTLS
- avril : *Heartbleed* dans OpenSSL
- juin : *Early CCS* dans OpenSSL

HTTPS et TLS : le cadenas dans un navigateur (3/3)

2014 : l'année où toutes les piles TLS majeures ont fait l'objet de vulnérabilités critiques

- février : `goto fail` Apple
- février : `goto fail` GnuTLS
- avril : *Heartbleed* dans OpenSSL
- juin : *Early CCS* dans OpenSSL
- septembre : *Universal signature forgery* dans NSS (Mozilla)
- septembre : *Universal signature forgery* dans CyaSSL
- septembre : *Universal signature forgery* dans PolarSSL

HTTPS et TLS : le cadenas dans un navigateur (3/3)

2014 : l'année où toutes les piles TLS majeures ont fait l'objet de vulnérabilités critiques

- février : `goto fail` Apple
- février : `goto fail` GnuTLS
- avril : *Heartbleed* dans OpenSSL
- juin : *Early CCS* dans OpenSSL
- septembre : *Universal signature forgery* dans NSS (Mozilla)
- septembre : *Universal signature forgery* dans CyaSSL
- septembre : *Universal signature forgery* dans PolarSSL
- novembre : exécution de code arbitraire dans SChannel (MS)

HTTPS et TLS : le cadenas dans un navigateur (3/3)

2014 : l'année où toutes les piles TLS majeures ont fait l'objet de vulnérabilités critiques

- février : `goto fail` Apple
- février : `goto fail` GnuTLS
- avril : *Heartbleed* dans OpenSSL
- juin : *Early CCS* dans OpenSSL
- septembre : *Universal signature forgery* dans NSS (Mozilla)
- septembre : *Universal signature forgery* dans CyaSSL
- septembre : *Universal signature forgery* dans PolarSSL
- novembre : exécution de code arbitraire dans SChannel (MS)

- **la sécurité réseau ne s'arrête pas à la mise en place de SSL/TLS !**

Références

- Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

  `http://www.cert.ssi.gouv.fr`
- Guide de définition d'une passerelle d'interconnexion

  `http://www.ssi.gouv.fr/administration/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/`
- Guide d'hygiène informatique

  `http://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/`
- Guides et bonnes pratiques publiées par l'ANSSI

  `http://www.ssi.gouv.fr/administration/bonnes-pratiques/`
- Common Vulnerabilities and Exposures

  `https://cve.mitre.org/`

Questions ?

Merci de votre attention.