Architecture sécurisées

Notion d'architectures

E. Leblond[1]

[1] INL SARL

Module sécurité, Intech'info

Outline

E. Leblond
Autobiographie

- Concepteur et développeur principal de NuFW
- Contributeur Netfilter
- Fondateur et co-gérant d'INL

E. Leblond
Autobiographie

- Concepteur et développeur principal de NuFW
- Contributeur Netfilter
- Fondateur et co-gérant d'INL

E. Leblond
Autobiographie

- Concepteur et développeur principal de NuFW
- Contributeur Netfilter
- Fondateur et co-gérant d'INL

Outline

Modèle OSI
L'effet oignon

C'est le schéma classique de décomposition du réseau :

- Une décomposition en couche
- Du physique à l'application
- Basée sur l'encapsulation et fragmentation

Intérêt pratique notamment au niveau du développement.

Décomposition du modèle OSI

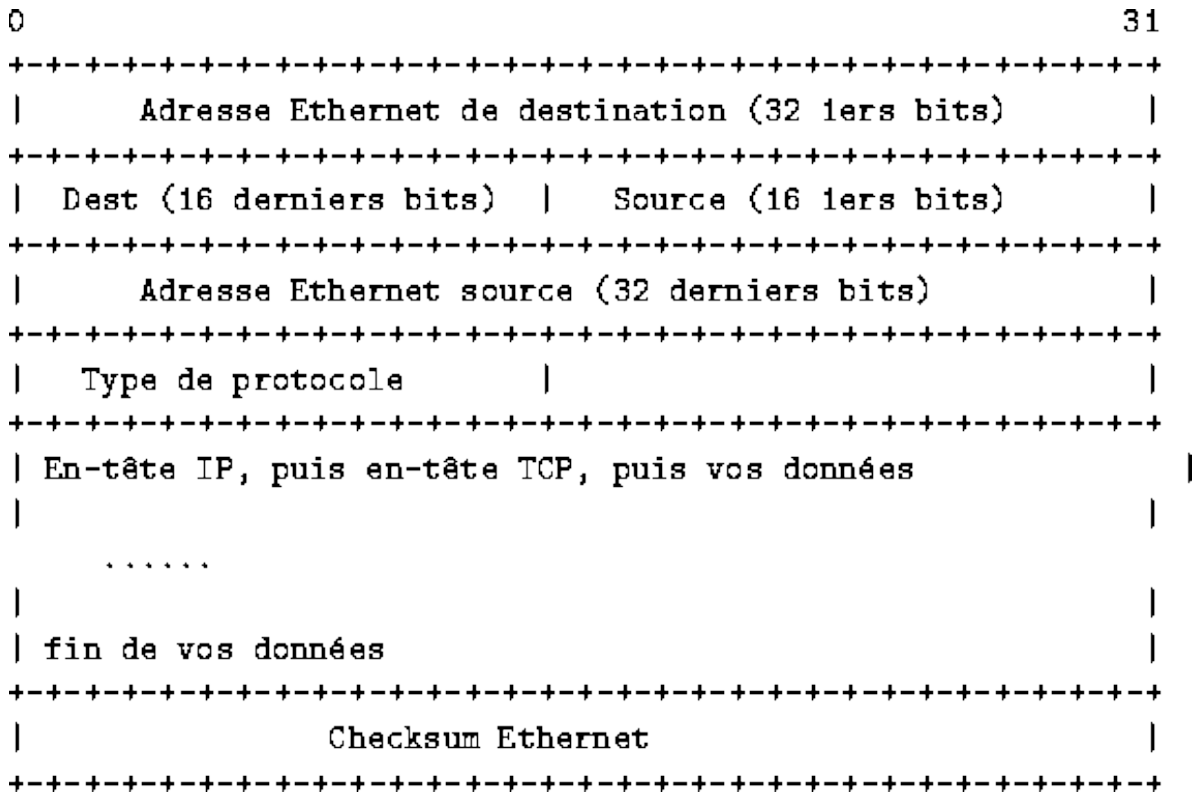
1. Couche physique : 100base-TX, Wireless
2. Couche de liaison : Ethernet, ATM, TokenRing, Wi-Fi
3. Couche de réseau : ARP, IPv4, IPv6
4. Couche de transport : TCP, UDP, ICMP, SCTP
5. Couche de session : L2TP, PPTP, RPC
6. Couche de présentation : Unicode, MIME, HTML, XML
7. Couche application : SSH, NNTP, DNS, HTTP

Ethernet
Le protocole de tous les jours

- Solution à bas coût et haute performance
  - Connecteur et concentrateur bon marché
  - Gamme très variée
- Atteint des bandes passantes élevées (de 10M à 10G)
- Filaire ou WiFi
- Switch de paquets

Ethernet

Décomposition d'un datagramme ethernet



Ethernet

- La destination d'abord pour l'optimisation
- Le datagramme contient toutes les informations nécessaires au routage
- La taille du datagramme est variable et est limitée par le médium physique:
  - 1500 bytes : la norme et le chiffre à retenir
  - 9000 bytes : jumbo frame

Ethernet
Principe

- Adresse MAC des cartes, identifiant unique
- Communication par adresse MAC
- Mécanisme d'annonce

Ethernet
ARP

Recherche correspondance IP<->Adresse Mac :

```
arp who-has 192.168.1.128 tell 192.168.1.2
arp reply 192.168.1.128 is-at 00:0c:f1:5c:47:91
```

Ethernet
ARP

Basé sur la confiance et donc soumis à de nombreuses attaques. Cette couche n'offre aucune sécurité.

- arp-spoofing
- arp-poisonning

Introduction à TCP/IP

- Famille de protocoles incontournables
- Beaucoup plus complexe qu'il n'y parait
- Coexistence avec les autres piles et les RFCs
  - Contournement des bugs
  - Violation des RFC

Principe

- Architecture du datagramme semblable à Ethernet
- Espace d'adresses de 32bit
- Construit pour l'encapsulation

Le paquet IPv4
Propriétés notables

- Taille variable
- Mécanisme de fragmentation
- Protocole de contrôle icmp
  - Vérification de connectivité : ping
  - Mécanisme d'information : reject
  - Indication de routage : redirect

IP
Décomposition du datagramme

+	Bits 0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Version	Header length	Type of Service (now DiffServ and ECN)	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	Header Checksum	
96	Source Address				
128	Destination Address				
160	Options				
160/192+	Data				

IP / Exemple de fragmentation

Ping de 1500 sur un lien à MTU 400

```
IP (tos 0x0, ttl  64, id 5503, offset 0, flags [+], proto: ICMP (1), length: 396) 127.0.0.1
> 127.0.0.1: ICMP echo request, id 49167, seq 1, length 376
IP (tos 0x0, ttl  64, id 5503, offset 376, flags [+], proto: ICMP (1), length: 396) 127.0.0.1
> 127.0.0.1: icmp
IP (tos 0x0, ttl  64, id 5503, offset 752, flags [+], proto: ICMP (1), length: 396) 127.0.0.1
> 127.0.0.1: icmp
IP (tos 0x0, ttl  64, id 5503, offset 1128, flags [none], proto: ICMP (1), length: 400) 127.0
> 127.0.0.1: icmp
IP (tos 0x0, ttl  64, id 5504, offset 0, flags [+], proto: ICMP (1), length: 396) 127.0.0.1
> 127.0.0.1: ICMP echo reply, id 49167, seq 1, length 376
IP (tos 0x0, ttl  64, id 5504, offset 376, flags [+], proto: ICMP (1), length: 396) 127.0.0.1
> 127.0.0.1: icmp
IP (tos 0x0, ttl  64, id 5504, offset 752, flags [+], proto: ICMP (1), length: 396) 127.0.0.1
> 127.0.0.1: icmp
IP (tos 0x0, ttl  64, id 5504, offset 1128, flags [none], proto: ICMP (1), length: 400) 127.0
> 127.0.0.1: icmp
```

Routage
Principe générique

- Directives de direction
  - Réseau segmenté
  - Comment atteindre une destination ?
  - Passerelle pour le réseau
- Routage : du plus spécifique au plus général

Routage
Exemple de table de routage

```
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.0.0     192.168.1.2     255.255.255.0   UG    0      0        0 eth1
0.0.0.0         192.168.1.254   0.0.0.0         UG    0      0        0 eth1
```

Protocoles de plus haut niveau
DNS

- En charge de la résolution des noms
- Mécanisme de cascade :
  - Décomposition des noms : home.regit.org
  - Serveur root
  - Serveur
- Des enregistrements différents
  - A : adresse
  - CNAME : alias
  - TXT : divers usages
  - ...
- UDP port 53 (et TCP port 53)

Protocoles de plus haut niveau
DNS

- En charge de la résolution des noms
- Mécanisme de cascade :
  - Décomposition des noms : home.regit.org
  - Serveur root
  - Serveur
- Des enregistrements différents
  - A : adresse
  - CNAME : alias
  - TXT : divers usages
  - ...
- UDP port 53 (et TCP port 53)

Protocoles de plus haut niveau
SMTP

- Protocole d'échange des mails entrant
- Repose sur le principe des MXs :
  - Liste de serveurs supportant le relayage
  - Le serveur de poids le plus faible prime
  - Chaque relais essaye de relayer au MX de poids plus faible
- Protocole simple avec échange en ascii

Protocoles de plus haut niveau
SMTP

Envoi d'un mail en telnet :

```
telnet "IP" smtp
HELO "domaine"
250 OK
MAIL From : <"foo@debian.org">
250 OK - mail from
RCPT To : <"email@cible">
250 OK - Recipient <"email@cible">
DATA
354 Send data. End with CRLF.CRLF

blablah
.
```

Protocoles de plus haut niveau
HTTP

- Le protocole !
- Repose sur un système de requêtes
  - GET : Récupération d'objet
  - POST : Envoi de formulaires
  - Autres : webdav
- Intimement lié aux entrées DNS textuelles
- Support de plusieurs sites sur un même IP
- Encapsule un grand nombre de protocoles :
  - XML-RPC
  - Web Services
- TCP port 80 (port 8080)
- HTTPS : encapsulation SSL

Protocoles de plus haut niveau
HTTP

- Le protocole !
- Repose sur un système de requêtes
  - GET : Récupération d'objet
  - POST : Envoi de formulaires
  - Autres : webdav
- Intimement lié aux entrées DNS textuelles
- Support de plusieurs sites sur un même IP
- Encapsule un grand nombre de protocoles :
  - XML-RPC
  - Web Services
- TCP port 80 (port 8080)
- HTTPS : encapsulation SSL

Protocoles de plus haut niveau
HTTP

- Requête :

```
GET http://www.commentcamarche.net HTTP/1.0
Accept : text/html
If-Modified-Since : Saturday, 15-January-2000 14:37:11 GMT
User-Agent : Mozilla/4.0 (compatible; MSIE 5.0; Windows 95)
```

- Réponse :

```
HTTP/1.0 200 OK
Date : Sat, 15 Jan 2000 14:37:12 GMT
Server : Microsoft-IIS/2.0
Content-Type : text/HTML
Content-Length : 1245
Last-Modified : Fri, 14 Jan 2000 08:25:13 GMT
```

Outline

Arp spoofing
Confiance ...

- La relation MAC<->IP est basée sur la confiance
- Prise en main d'une IP sur le réseau
  - Annonces en rafale
  - Sûr de polluer le cache des machines du réseau
  - Communication du poste visé impossible

Arp poisonning
Confiance ...

- Deni de service :
  - Envoi d'arp reply faux
  - Pollution des caches ARP
  - Déstabilisation du réseau
- arpwatch : monitoring et alerting sur comportement anormal

Arp poisonning
Confiance ...

- Deni de service :
  - Envoi d'arp reply faux
  - Pollution des caches ARP
  - Déstabilisation du réseau
- arpwatch : monitoring et alerting sur comportement anormal

Man in the middle
Confiance ...

- Le trafic entre deux machines passent par plusieurs points
- Le contenu des échanges peut être connus par un intermédiaire
- Il peut aussi être modifié
- C'est vrai pour les protocoles cryptés au démarrage

Man in the middle
Confiance ...

- Le trafic entre deux machines passent par plusieurs points
- Le contenu des échanges peut être connus par un intermédiaire
- Il peut aussi être modifié
- C'est vrai pour les protocoles cryptés au démarrage

Man in the middle
Confiance ...

- Le trafic entre deux machines passent par plusieurs points
- Le contenu des échanges peut être connus par un intermédiaire
- Il peut aussi être modifié
- C'est vrai pour les protocoles cryptés au démarrage

Man in the middle
Confiance ...

- Le trafic entre deux machines passent par plusieurs points
- Le contenu des échanges peut être connus par un intermédiaire
- Il peut aussi être modifié
- C'est vrai pour les protocoles cryptés au démarrage

DNS spoofing
Confiance ...

1. Réponse DNS falsifiée
2. Requête protocolaire dirigée vers une machine attaquante
3. Exploitation :
   - Récupération d'informations (phishing)
   - Injection de données corrompues (windows update)

Outline

Phase 1
Tout IP publique

- Le réseau des pionniers
- En mode routage pur
- Protection des services par `tcp-wrapper`
  - Contrôle de l'accès au niveau userland
  - liste d'accès contrôlée sur la machine

Phase 1
Tout IP publique

- Le réseau des pionniers
- En mode routage pur
- Protection des services par `tcp-wrapper`
  - Contrôle de l'accès au niveau userland
  - liste d'accès contrôlée sur la machine

Phase 1
Tout IP publique

- Cas du grand public
- Cas des backbone opérateurs
  - Accessibilité
  - Protocole BGP
    - Peu sécurisé
    - Écroulement en cascade
    - AS7007 : Coupure d'internet en 1997

Phase 1
Tout IP publique

- Cas du grand public
- Cas des backbone opérateurs
  - Accessibilité
  - Protocole BGP
    - Peu sécurisé
    - Écroulement en cascade
    - AS7007 : Coupure d'internet en 1997

Phase 1
Tout IP publique

- Cas du grand public
- Cas des backbone opérateurs
  - Accessibilité
  - Protocole BGP
    - Peu sécurisé
    - Écroulement en cascade
    - AS7007 : Coupure d'internet en 1997

Phase 1
Tout IP publique

- Cas du grand public
- Cas des backbone opérateurs
  - Accessibilité
  - Protocole BGP
    - Peu sécurisé
    - Écroulement en cascade
    - AS7007 : Coupure d'internet en 1997

Phase 2
Cloisonnement

- Centralisation du filtrage
  - Éparpillement des mesures de protections dangereux
  - Responsabilité et rôles variés des intervenants
  - Plus efficace et exhaustif : DROP par défaut
- Transformation des routeurs en filtre
  - Mise en place de contrôle d'accès à l'entrée des réseaux
  - Isolation des réseaux internes

Filtrage IP
Historique

- Filtre de paquets
  - Par rapport au contenu
  - Jeu de régles linéaire
  - Gestion des allers retours
- Implémentations :
  - Routeurs/pare-feu
  - Switchs niveau 3

Traduction d'adresse
source NAT

- Pénurie d'adresse : 2^{32} c'est peu
- Dépôt de classes d'adresses privées
- Le routeur de sortie masque les adresses
- Nécessité de maintenir une table
  - Analyse du paquet retour
  - Réécriture de l'adresse source
- Limitations :
  - 65535 ports pour une adresse
  - Gestion des protocoles complexes

Traduction d'adresse
source NAT

- Pénurie d'adresse : 2^{32} c'est peu
- Dépôt de classes d'adresses privées
- Le routeur de sortie masque les adresses
- Nécessité de maintenir une table
  - Analyse du paquet retour
  - Réécriture de l'adresse source
- Limitations :
  - 65535 ports pour une adresse
  - Gestion des protocoles complexes

Traduction d'adresse
source NAT

- Pénurie d'adresse : 2^{32} c'est peu
- Dépôt de classes d'adresses privées
- Le routeur de sortie masque les adresses
- Nécessité de maintenir une table
  - Analyse du paquet retour
  - Réécriture de l'adresse source
- Limitations :
  - 65535 ports pour une adresse
  - Gestion des protocoles complexes

Traduction d'adresse
source NAT

- Pénurie d'adresse : 2^{32} c'est peu
- Dépôt de classes d'adresses privées
- Le routeur de sortie masque les adresses
- Nécessité de maintenir une table
  - Analyse du paquet retour
  - Réécriture de l'adresse source
- Limitations :
  - 65535 ports pour une adresse
  - Gestion des protocoles complexes

Traduction d'adresse
source NAT

- Pénurie d'adresse : 2^{32} c'est peu
- Dépôt de classes d'adresses privées
- Le routeur de sortie masque les adresses
- Nécessité de maintenir une table
  - Analyse du paquet retour
  - Réécriture de l'adresse source
- Limitations :
  - 65535 ports pour une adresse
  - Gestion des protocoles complexes

Traduction d'adresse
source NAT

- Pénurie d'adresse : 2^{32} c'est peu
- Dépôt de classes d'adresses privées
- Le routeur de sortie masque les adresses
- Nécessité de maintenir une table
  - Analyse du paquet retour
  - Réécriture de l'adresse source
- Limitations :
  - 65535 ports pour une adresse
  - Gestion des protocoles complexes

Traduction d'adresse
Destination NAT

- Pénurie d'adresse : une c'est peu
- Redirection des services de l'IP publique vers d'autres serveurs
- Conforme au principe de séparation des services
- Modification de la visibilité sur le réseau
- Attention aux abus :
  - Accès direct aux machines internes depuis l'extérieur
  - Prise de contrôle possibles des machines cibles

Traduction d'adresse
Destination NAT

- Pénurie d'adresse : une c'est peu
- Redirection des services de l'IP publique vers d'autres serveurs
- Conforme au principe de séparation des services
- Modification de la visibilité sur le réseau
- Attention aux abus :
  - Accès direct aux machines internes depuis l'extérieur
  - Prise de contrôle possibles des machines cibles

Suivi de connexions

- Ajout de la notion de session
  - Maintien d'une table des connexions
  - Filtrage des paquets suivant l'état de leur connexion relative
  - Plus besoin de spécifier les allers retours
- Renforcement de la sécurité
  - On autorise un vrai retour
  - Plus de contournements possible
- Meilleure efficacité

Phase 3
Architecture n-tiers

- Limitation des accès directs aux ressources
- Découpage fonctionnel
  - Internet
  - DMZ
  - User
- Raffinement :
  - Zone serveur
  - Zone WiFi

Phase 3
Architecture n-tiers

- Limitation des accès directs aux ressources
- Découpage fonctionnel
  - Internet
  - DMZ
  - User
- Raffinement :
  - Zone serveur
  - Zone WiFi

Phase 3
Architecture n-tiers

- Limitation des accès directs aux ressources
- Découpage fonctionnel
  - Internet
  - DMZ
  - User
- Raffinement :
  - Zone serveur
  - Zone WiFi

Architecture n-tiers
Avantages

- Séparation des réseaux :
  - Attaque basée sur IP impossible
  - Possibilité de contenir une surcharge réseau
- Contrôle des accès
- Limitation des propagations virales

Architecture n-tiers
Protection des données

- Problématique de la publication
  - Mettre à disposition des partenaires des données sensibles
  - Accès depuis internet aux données vitales ?
- Quelques solutions :
  - Contrôle d'accès fin aux ressources internes
    - Contrôle d'accès des bases de données
  - Réplication partielle des données

Architecture n-tiers
Protection des données

- Problématique de la publication
  - Mettre à disposition des partenaires des données sensibles
  - Accès depuis internet aux données vitales ?
- Quelques solutions :
  - Contrôle d'accès fin aux ressources internes
    - Contrôle d'accès des bases de données
  - Réplication partielle des données

Architecture n-tiers
Protection des données

- Problématique de la publication
  - Mettre à disposition des partenaires des données sensibles
  - Accès depuis internet aux données vitales ?
- Quelques solutions :
  - Contrôle d'accès fin aux ressources internes
    - Contrôle d'accès des bases de données
  - Réplication partielle des données

Phase 4
Rupture des flux sortants

- Le danger vient de l'extérieur
- Connexion directe :
  - Toujours à double sens
  - Attaque et prise de contrôle
- Méthode de contournement :
  - Tunneling
  - port 80 ne veut pas dire HTTP

Rupture des flux sortants
Cas de HTTP

- Serveur mandataire
  - Gestion du cache
  - Validation du protocole
  - QoS sur les flux
- Contrôle d'accès :
  - Support du protocole HTTP 1.1
  - Filtrage par site
  - Analyse des logs fines

Rupture des flux sortants
Cas de HTTP

- Serveur mandataire
  - Gestion du cache
  - Validation du protocole
  - QoS sur les flux
- Contrôle d'accès :
  - Support du protocole HTTP 1.1
  - Filtrage par site
  - Analyse des logs fines

Phase 5
Rupture des flux entrants

- Les ressources internes doivent être protégées
  - Un serveur de mail héberge des données confidentielles
  - Il ne doit pas être accédé en direct
  - L'intermédiaire permet de masquer l'architecture interne
- Un contrôle des flux avant accès est souhaitable
  - Conformité protocolaire
  - Filtrage d'accès

Phase 5
Rupture des flux entrants

- Les ressources internes doivent être protégées
  - Un serveur de mail héberge des données confidentielles
  - Il ne doit pas être accédé en direct
  - L'intermédiaire permet de masquer l'architecture interne
- Un contrôle des flux avant accès est souhaitable
  - Conformité protocolaire
  - Filtrage d'accès

Rupture des flux entrants
Cas de SMTP

- Mise en place d'un relai vers l'interne
  - Permet de s'ajuster à l'architecture interne
  - Point de contrôle central
- Tâches de vérification :
  - liste de domaines supportés
  - Antivirus
  - Greylisting
  - Vérification des adresses destinataires

Rupture des flux entrants
Cas de SMTP

- Mise en place d'un relai vers l'interne
  - Permet de s'ajuster à l'architecture interne
  - Point de contrôle central
- Tâches de vérification :
  - liste de domaines supportés
  - Antivirus
  - Greylisting
  - Vérification des adresses destinataires

Rupture des flux entrants
Cas de HTTP

- Reverse Proxy :
  - Serveur frontal
  - Possibilité de cache
  - Répartition de charge
- Reverse proxy filtrant :
  - Validation des URLs
  - Bloquage des requêtes non conformes
  - Utilisation d'une base de signatures

Outline

Connexions de sites distants

- Liaisons louées
  - Connexions point à point entre les sites
  - Dépassé et trop cher
- IPsec
  - Établissement d'un tunnel entre deux passerelles
  - Visibilité directe des réseaux privés
  - Encryption des échanges
  - Protocole ratifié IETF
- MPLS
  - Isolation sur la backbone opérateur
  - Pas d'encryption
  - Facile à mettre en oeuvre

Connexions de sites distants

- Liaisons louées
  - Connexions point à point entre les sites
  - Dépassé et trop cher
- IPsec
  - Établissement d'un tunnel entre deux passerelles
  - Visibilité directe des réseaux privés
  - Encryption des échanges
  - Protocole ratifié IETF
- MPLS
  - Isolation sur la backbone opérateur
  - Pas d'encryption
  - Facile à mettre en oeuvre

Connexions de sites distants

- Liaisons louées
  - Connexions point à point entre les sites
  - Dépassé et trop cher
- IPsec
  - Établissement d'un tunnel entre deux passerelles
  - Visibilité directe des réseaux privés
  - Encryption des échanges
  - Protocole ratifié IETF
- MPLS
  - Isolation sur la backbone opérateur
  - Pas d'encryption
  - Facile à mettre en oeuvre

La mobilité
Accès distant

- Ipsec
  - Connexion Road-warrior
  - Complexité du client
- OpenVPN
  - Plus léger
  - Passage des proxy
- VPN-SSL
  - Sans client
  - Version Web 2.0 du VPN

Défense passive
Protection du réseau interne

- IDS
  - analyse des flux
  - remontée d'alerte
- Honey Pot
  - Simulation de machine vulnérable
  - Découverte de nouvelles attaques
  - Détournement des pirates des vraies cibles

IDS
Principe

- Écoute des trames réseaux
- Analyse sur base de signature

```
alert udp $EXTERNAL_NET any -> $SQL_SERVERS any (msg:"MS-SQL probe \
response overflow attempt";
content:"|05|"; depth:1; byte_test:2,>,512,1; content:"|3B|"; \
distance:0; isdataat:512,relative;\
content:!"|3B|"; within:512; reference:bugtraq,9407; reference:cve,2003-0903; \
reference:url,www.microsoft.com/technet/security/bulletin/MS04-003.mspx;\
classtype:attempted-user; sid:2329; rev:6;)
```

- Analyse comportementale

IDS
Difficulté

- Performance
  - Analyse complexe
  - Surcharge CPU
- Fragmentation
  - Découpage du protocole IP (niveau 3)
  - Découpage du protocole (niveau 7)
  - Exemples : RPC
  - Reconstruction nécessaire à tous les niveaux

IDS
Difficulté

- Performance
  - Analyse complexe
  - Surcharge CPU
- Fragmentation
  - Découpage du protocole IP (niveau 3)
  - Découpage du protocole (niveau 7)
  - Exemples : RPC
  - Reconstruction nécessaire à tous les niveaux

IDS
Difficulté

- Performance
  - Analyse complexe
  - Surcharge CPU
- Fragmentation
  - Découpage du protocole IP (niveau 3)
  - Découpage du protocole (niveau 7)
  - Exemples : RPC
  - Reconstruction nécessaire à tous les niveaux

Outline

Analyse protocolaire
pare-feu niveau 7

- Analyse des protocoles
- Vérification de conformité
  - Décomposition du début des paquets
  - Découverte du protocole
  - Bloquage si non conformité
- Méthode d'échappement
  - Encapsulation respectueuse : nstx
  - Dissimulation d'information dans le protocole

Analyse protocolaire
IPS

- Antivirus de flux
- Difficulté d'équilibrage
  - Faux positifs deviennent dangereux
  - Problématiques de la performance

Le poste client
Protection du réseau interne

- Contrôle des accès
  - Introduction des machines sur le réseau (802.1x)
  - Validation des identités (NuFW)
- Vérification des postes
  - Isolation au niveau du switch
  - Vérification du poste par un agent
  - Problème de confiance

Le poste client
Protection du réseau interne

- Contrôle des accès
  - Introduction des machines sur le réseau (802.1x)
  - Validation des identités (NuFW)
- Vérification des postes
  - Isolation au niveau du switch
  - Vérification du poste par un agent
  - Problème de confiance

Le poste client
Protection du réseau interne

- Contrôle des accès
  - Introduction des machines sur le réseau (802.1x)
  - Validation des identités (NuFW)
- Vérification des postes
  - Isolation au niveau du switch
  - Vérification du poste par un agent
  - Problème de confiance

Le poste client
Protection du réseau interne

- Contrôle des accès
  - Introduction des machines sur le réseau (802.1x)
  - Validation des identités (NuFW)
- Vérification des postes
  - Isolation au niveau du switch
  - Vérification du poste par un agent
  - Problème de confiance

Fin du cloisonnement ?

Un monde trop dangereux

- Attaque sur les protocoles de haut niveau
- Problèmes des postes mobiles
  - Contamination externe
  - Réinjection dans le réseau interne
- Arrivée d'IPV6
  - Globalisation des adresses
  - IPV6 mobile

Fin du cloisonnement ?

Un monde trop dangereux

- Attaque sur les protocoles de haut niveau
- Problèmes des postes mobiles
  - Contamination externe
  - Réinjection dans le réseau interne
- Arrivée d'IPV6
  - Globalisation des adresses
  - IPV6 mobile