Chapitre 5 : Sécurité Réseau
DoS/DDoS, Firewalls, IDS/IPS

Cours de Sécurité Informatique - Niveau Universitaire
Partie 3 : Network Security

12 janvier 2026

Table des matières

1 Attaques par déni de service (DoS/DDoS)

1.1 Définitions

Définition

Déni de service (DoS) : Attaque visant à rendre un service indisponible en saturant ses ressources.
DDoS (Distributed Denial of Service) : DoS distribué depuis de multiples sources (botnet).

1.2 Types d'attaques DoS

1. **Bandwidth exhaustion** : Saturer la bande passante
   - UDP flood, ICMP flood
   - Amplification attacks (DNS, NTP, Memcached)
2. **Resource exhaustion** : Épuiser CPU/mémoire/connexions
   - SYN flood (TCP half-open connections)
   - Slowloris (connexions HTTP lentes)
   - HTTP POST flood
3. **Application layer attacks** : Cibler des fonctions coûteuses
   - Requêtes complexes sur BDD
   - Regex DoS (ReDoS)
   - Algorithmic complexity attacks

1.3 Amplification attacks

Principe : Exploiter des protocoles permettant l'amplification du trafic.
Exemple DNS amplification :

- Attaquant envoie requête DNS avec IP source spoofée (victime)
- Serveur DNS envoie réponse (50x plus grande) à la victime
- Facteur d'amplification : jusqu'à 50x

Autres protocoles vulnérables :

- NTP (amplification 556x)
- Memcached (amplification 51,000x !)
- SNMP, SSDP, CharGen

1.4 Défenses contre DoS/DDoS

Prévention :

- Rate limiting (limiter requêtes par IP)
- SYN cookies (contre SYN flood)
- Filtrage BCP 38 (bloquer IP source spoofing)
- Désactiver services amplifiables non nécessaires

Détection :

- Monitoring du trafic (patterns anormaux)
- Anomaly detection

— SIEM (Security Information and Event Management)

Mitigation :

— CDN (Content Delivery Network) : Cloudflare, Akamai

— Scrubbing centers : Filtrer trafic malveillant

— Elastic scaling (cloud auto-scaling)

— BGP blackholing

2 Firewalls (pare-feu)

2.1 Définition et rôle

Définition

Firewall : Dispositif de sécurité qui filtre le trafic réseau selon des règles prédéfinies.
Objectif : Séparer réseaux de confiance (interne) et non-confiance (Internet).

2.2 Types de firewalls

1. **Packet filtering firewall** (couche 3-4)
   — Filtre basé sur IP source/dest, ports, protocole
   — Rapide mais peu intelligent
   — Exemple : iptables, pf
2. **Stateful firewall**
   — Suit l'état des connexions TCP
   — Comprend les sessions (connexions établies vs nouvelles)
   — Plus sécurisé que packet filtering simple
3. **Application layer firewall / WAF** (couche 7)
   — Inspecte contenu des requêtes HTTP/HTTPS
   — Détecte SQLi, XSS, CSRF
   — Exemple : ModSecurity, CloudFlare WAF
4. **Next-Generation Firewall (NGFW)**
   — Combine firewall + IPS + inspection SSL + threat intelligence
   — Deep packet inspection (DPI)
   — Exemple : Palo Alto, Fortinet

2.3 Règles firewall : bonnes pratiques

Principe du moindre privilège : Tout bloquer par défaut, autoriser explicitement.
Exemple iptables :

```
# Politique par défaut : DROP tout
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

# Autoriser connexions établies
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

```
# Autoriser SSH (port 22) depuis IP admin
iptables -A INPUT -p tcp -s 192.168.1.100 --dport 22 -j ACCEPT

# Autoriser HTTP/HTTPS
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

2.4 Limitations des firewalls

Avertissement

Ce que les firewalls NE protègent PAS contre :

- Attaques sur trafic autorisé (ex : exploitation web sur port 443)
- Malware téléchargé par utilisateur légitime
- Menaces internes (insider threats)
- Zero-day exploits
- Chiffrement malveillant (exfiltration sur HTTPS)

Discussion critique : Les firewalls ne sont qu'une couche de défense parmi d'autres (defense in depth).

3 Systèmes de détection/prévention d'intrusion (IDS/IPS)

3.1 IDS vs IPS

Définition

IDS (Intrusion Detection System) : Surveille le trafic et alerte sur activités suspectes.
IPS (Intrusion Prevention System) : IDS + capacité de bloquer automatiquement les attaques.

Différence :

- IDS : Mode passif (alerte)
- IPS : Mode actif (bloque)

3.2 Types de détection

1. **Signature-based detection**
   - Compare trafic à base de signatures d'attaques connues
   - Rapide et précis pour attaques connues
   - Vulnérable aux zero-days et évasion
   - Exemple : Snort, Suricata
2. **Anomaly-based detection**
   - Détecte déviations par rapport au comportement normal
   - Peut détecter attaques inconnues (zero-days)
   - Taux élevé de faux positifs
   - Nécessite apprentissage (baseline)
3. **Hybrid approach**
   - Combine signatures + anomaly detection
   - Machine Learning pour améliorer détection

3.3 Network-based vs Host-based

NIDS/NIPS (Network) :

— Surveille tout le trafic réseau
— Positionné stratégiquement (DMZ, backbone)
— Peut être contourné par chiffrement (HTTPS)

HIDS/HIPS (Host) :

— Installé sur chaque machine
— Surveille logs, fichiers, processus
— Détecte rootkits, malware
— Exemple : OSSEC, Wazuh

3.4 Limitations et discussion critique

Avertissement

Problèmes des IDS/IPS :

— **Faux positifs** : Alertes légitimes classées comme attaques
— **Faux négatifs** : Attaques non détectées
— **Performance** : Deep packet inspection coûteuse
— **Évasion** : Techniques pour contourner (fragmentation, polymorphisme)
— **Chiffrement** : HTTPS/TLS rend inspection difficile

Discussion : L'efficacité dépend de la qualité des signatures et du tuning. Nécessite expertise et maintenance continue.

4 Architectures de sécurité réseau

4.1 DMZ (Demilitarized Zone)

Principe : Zone tampon entre Internet et réseau interne.
Architecture typique :

```
Internet <--> Firewall externe <--> DMZ (serveurs web, mail)
              <--> Firewall interne <--> LAN interne
```

Avantages :

— Isoler services publics du réseau interne
— Double protection (deux firewalls)
— Limiter surface d'attaque

4.2 Defense in Depth

Principe : Multiples couches de sécurité.
Couches :

1. Périmètre : Firewall, IPS
2. Réseau : Segmentation VLAN, micro-segmentation
3. Endpoints : Antivirus, HIPS, EDR
4. Application : WAF, input validation
5. Données : Chiffrement, contrôle d'accès
6. Utilisateurs : MFA, formation

5 Conclusion

Points clés :

— DoS/DDoS : Menace majeure, défense par CDN + rate limiting

— Firewalls : Nécessaires mais insuffisants seuls

— IDS/IPS : Complémentaires, nécessitent tuning

— Defense in depth : Approche recommandée

Tendances : Zero Trust Architecture, SASE (Secure Access Service Edge), ML pour détection d'anomalies.