Chapitre 05 Sécurité des adresses IPv6

Introduction

L'adoption croissante du protocole IPv6 répond à l'épuisement des adresses IPv4, mais elle introduit également de nouveaux défis en matière de sécurité.

Ce chapitre détaille les vulnérabilités des adresses IPv6 et les mécanismes permettant d'assurer leur sécurité dans les réseaux modernes.

1. Spécificités de l'adressage IPv6

IPv6 introduit plusieurs types d'adresses et de mécanismes d'auto-configuration qui diffèrent fondamentalement d'IPv4 :

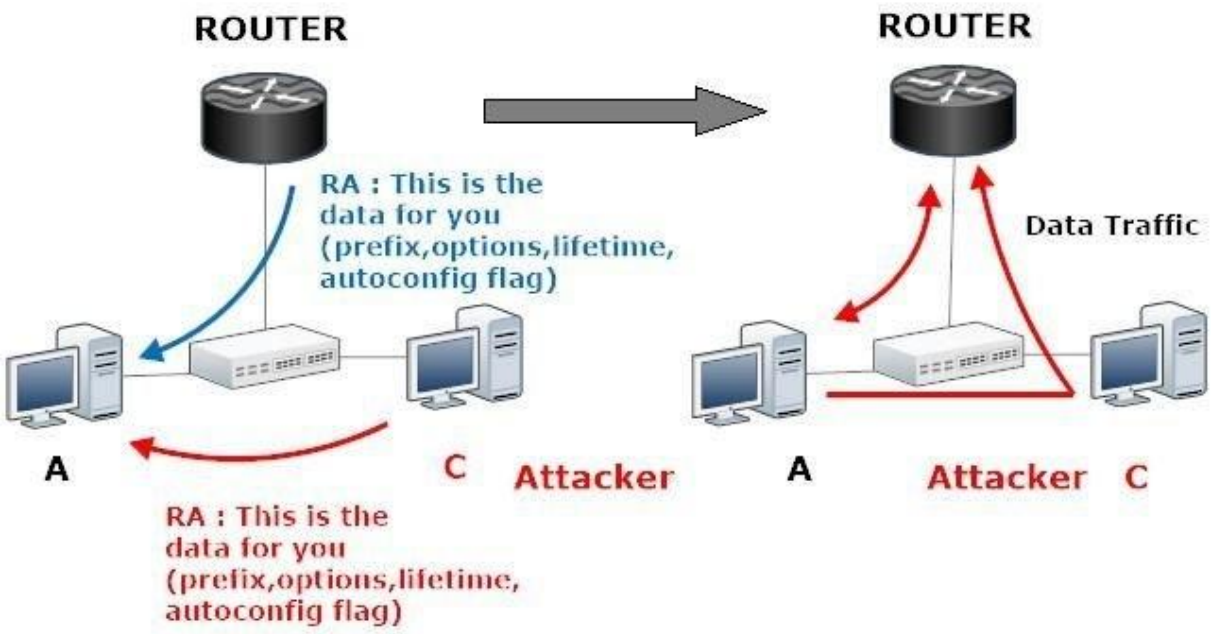
- **Longueur de l'adresse :** 128 bits contre 32 bits en IPv4.
- **Types d'adresses :** unicast, multicast, anycast (pas de broadcast).
- **Auto-configuration Stateless (SLAAC)** et **DHCPv6**.
- **Présence obligatoire d'IPSec** (dans la spécification, mais pas toujours activée).

2. Attaques IPv6 : Détails et Mécanismes

1. Attaques sur le Neighbor Discovery Protocol (NDP)

1.1. NDP Spoofing / Poisoning

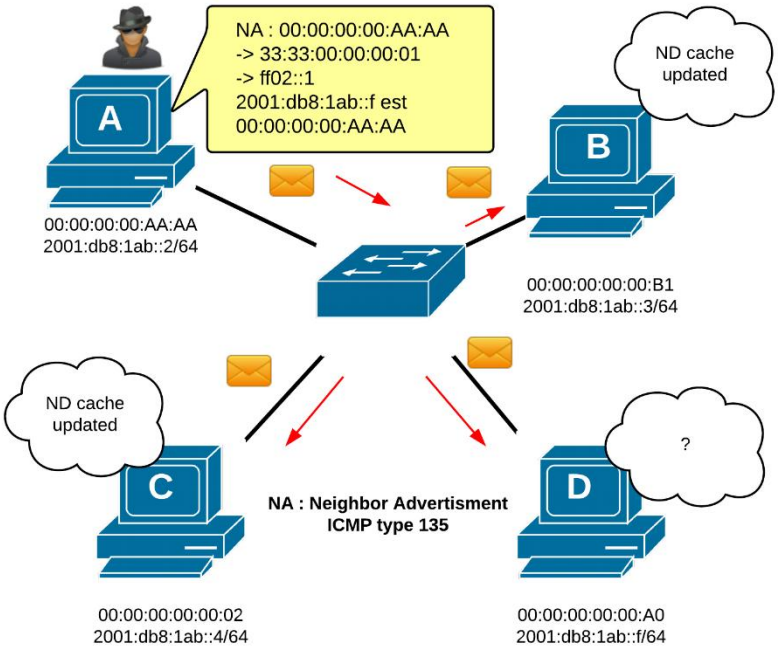
- **Description :** L’ attaquant envoie de fausses réponses NDP (Neighbor Advertisement) pour lier une adresse IPv6 à sa propre adresse MAC.



- **Conséquence :** Redirection du trafic vers l’ attaquant (MITM), déni de service, usurpation d’ identité.
- **Comparable à :** ARP Spoofing en IPv4.

1.2. NDP DoS (Cache Exhaustion)

- **Description :** L’ attaquant envoie des milliers de faux paquets NDP avec des adresses IPv6 aléatoires.

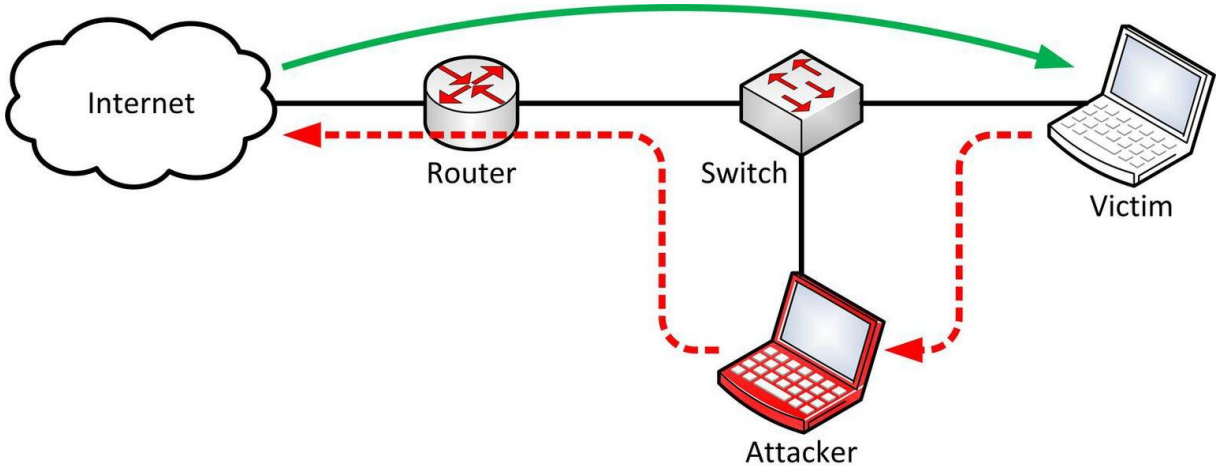


- **Conséquence :** Remplissage du cache NDP du routeur ou de la machine cible → saturation mémoire → crash ou ralentissement du système.
- **Outil :** THC-IPv6 (fake_router6, flood_advertise6).

2. Attaques sur Router Advertisement (RA)

2.1. RA Spoofing

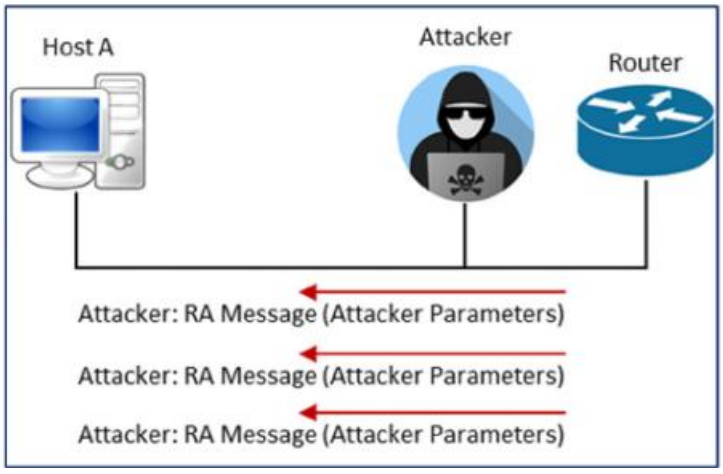
- **Description :** Un attaquant envoie de faux paquets RA (Router Advertisement) pour annoncer sa machine comme routeur par défaut.



- **Effet :** Les hôtes sur le réseau peuvent rediriger leur trafic vers l'attaquant.
- **Utilisation :** MITM, interception de trafic.
- **Contre-mesure :** RA Guard, contrôle du port.

2.2. RA Flooding

- **Description :** Bombardement du réseau avec des RA contenant des préfixes ou paramètres falsifiés.



- **Effet :** Création massive d'adresses IPv6, surcharge CPU et mémoire → déni de service.

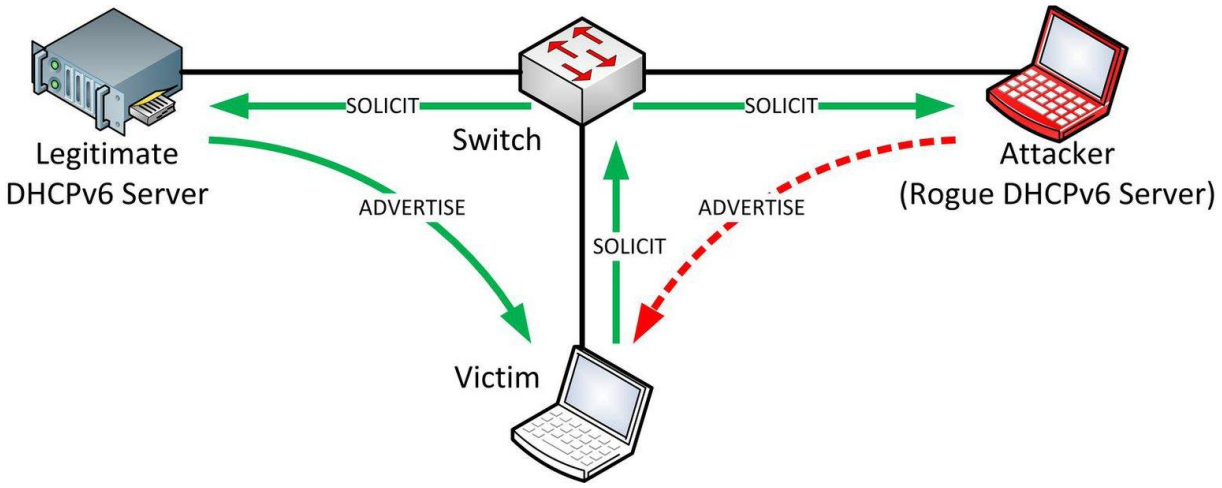
3. SLAAC (Stateless Address Auto-Configuration) Attacks

3.1. Faux préfixe IPv6

- **Description :** L'attaquant insère un nouveau préfixe via RA, provoquant la génération d'une fausse adresse IPv6.
- **Effet :** L'hôte peut devenir inaccessible ou rediriger le trafic.

3.2. Attaque de type Rogue DHCPv6 Server

- **Description :** Un faux serveur DHCPv6 fournit des informations incorrectes (ex. DNS, routeur, passerelle).

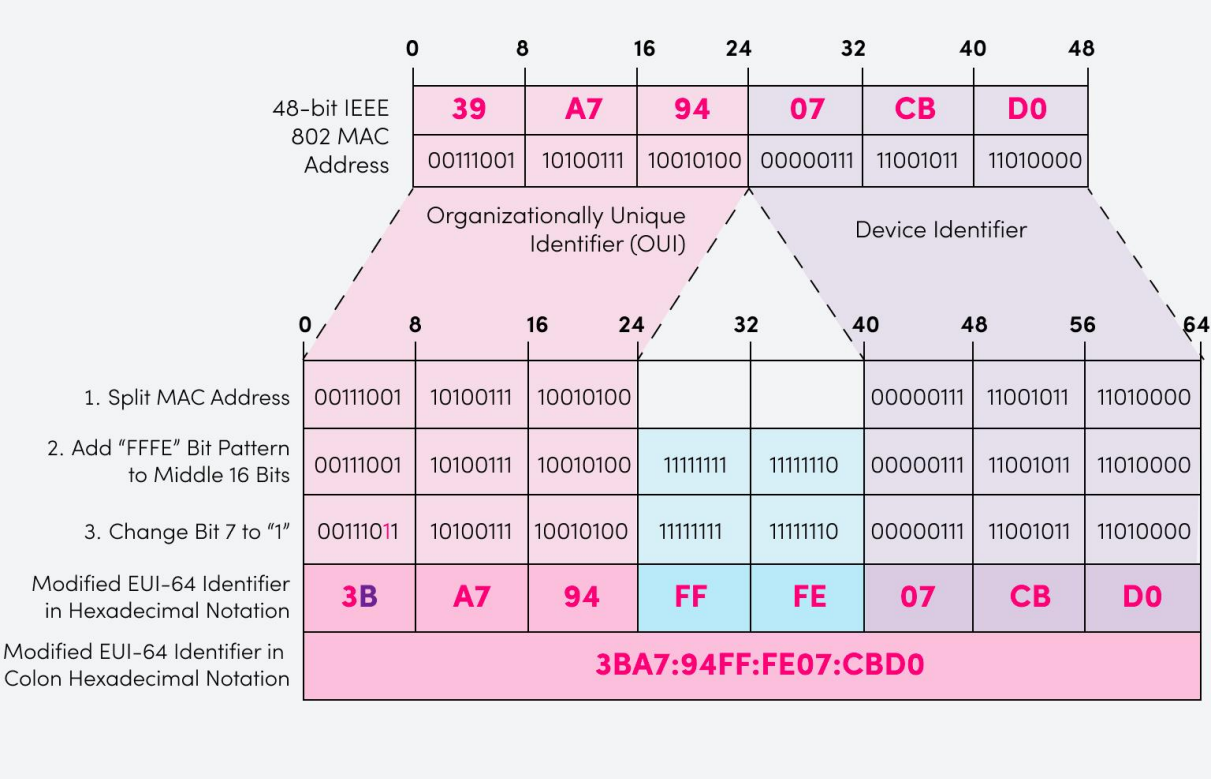


- **Effet :** Redirection vers des serveurs malveillants.

4. Attaques sur l'Interface Identifier (IID)

4.1. EUI-64-Based Tracking

- **Description :** L'adresse IPv6 est calculée automatiquement à partir de l'adresse MAC → traçabilité permanente de l'appareil.



- **Effet :** Atteinte à la vie privée, surveillance inter-réseaux.
- **Solution :** Activer les adresses temporaires (RFC 4941), désactiver EUI-64.

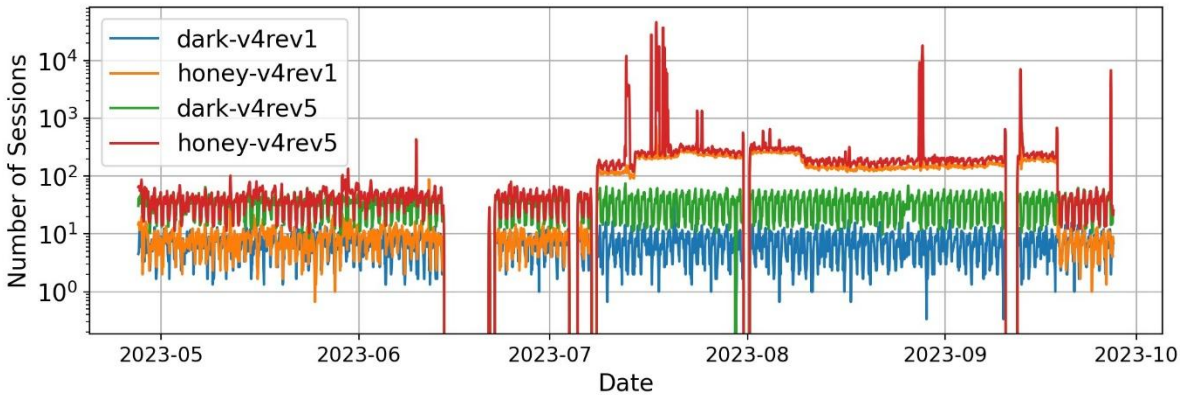
5. Attaques sur le multicast et scanning

5.1. Multicast Flooding

- **Description :** Utilisation d'adresses multicast (ff02::1, ff02::2) pour envoyer des paquets à tous les hôtes/routeurs du lien.
- **Effet :** Saturation de la bande passante, CPU élevé sur les hôtes.

5.2. IPv6 Scanning

- **Difficulté :** Impossible de scanner l'espace entier (2^64 adresses par sous-réseau), mais...

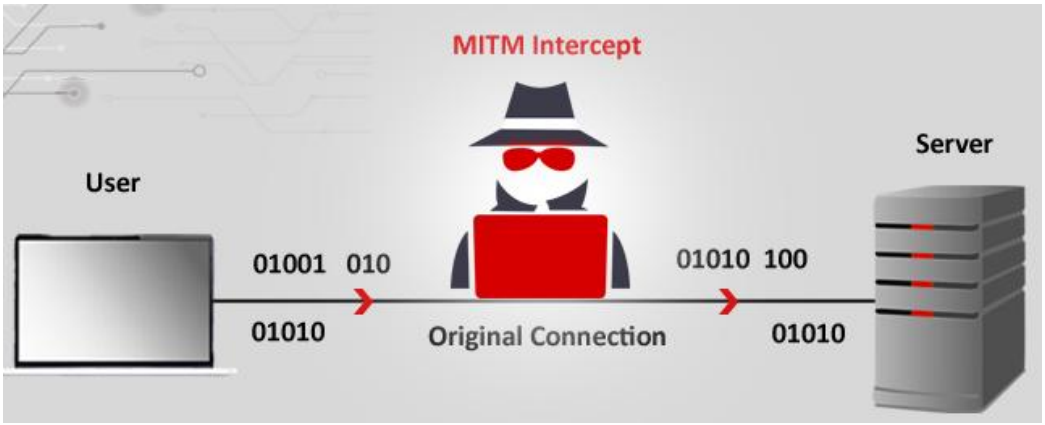


- **Méthodes utilisées :**
  - Scans ciblés (ex. adresses avec suffixes connus comme ::1, ::2, etc.).
  - Analyse des adresses générées par EUI-64.
  - Utilisation d' heuristiques et de dictionnaires.
- **Outils :** nmap, zmap, scan6.

6. Attaques Man-in-the-Middle (MITM)

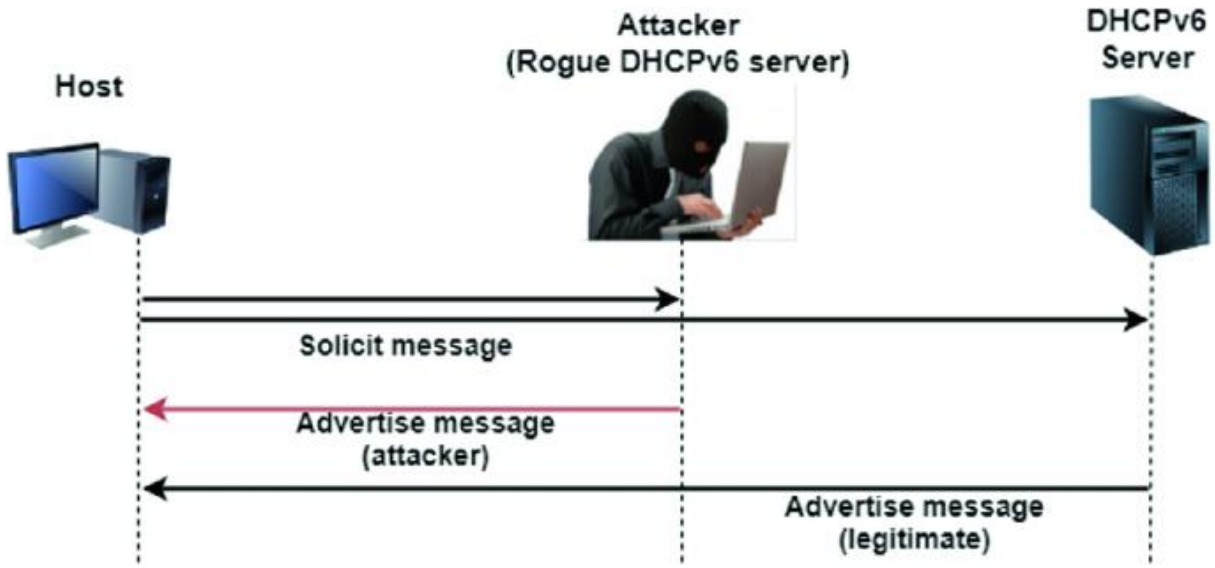
6.1. MITM via RA/NDP Spoofing

- Redirection du trafic à travers l' attaquant.
- Possibilité de modification, inspection ou suppression de paquets.



6.2. MITM avec DHCPv6

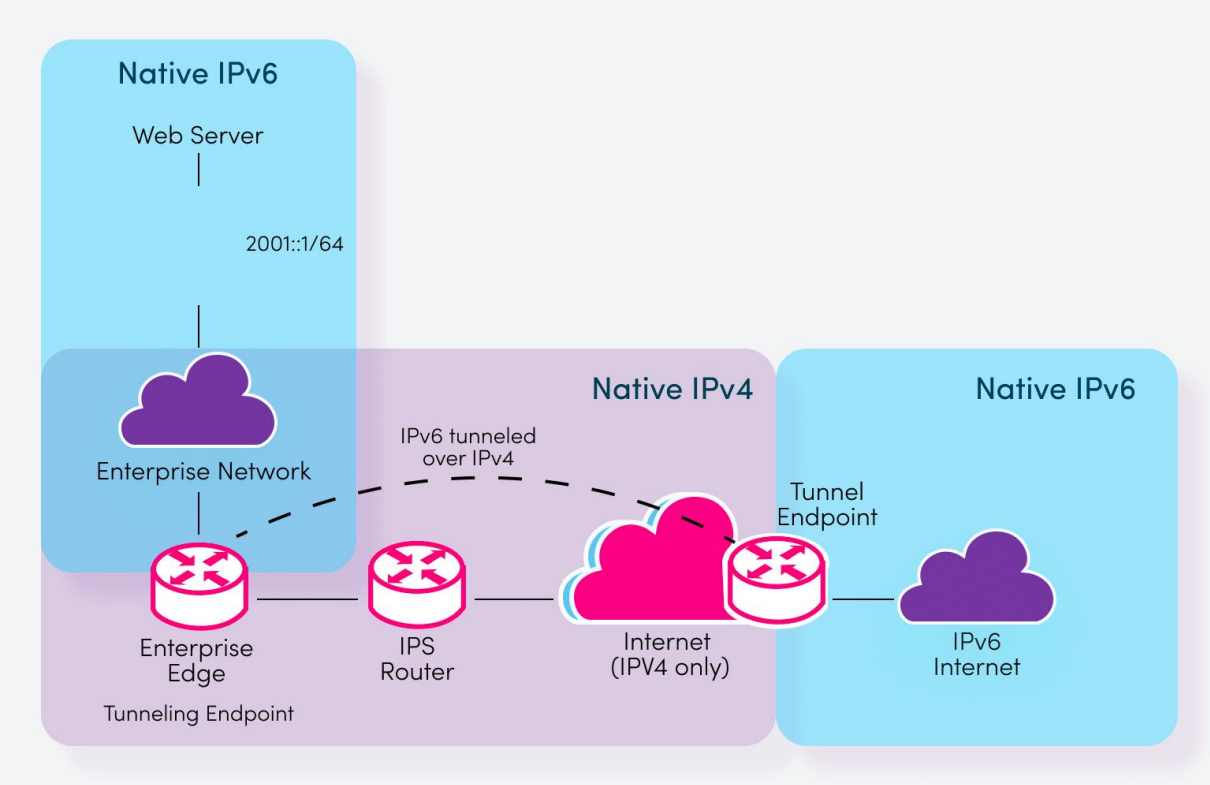
- Attribution de DNS ou routeurs malveillants → détournement de navigation, phishing.



7. Abus d' IPSec et fragmentation

7.1. Tunneling malveillant (IPv6-in-IPv4)

- **Description :** Utilisation abusive de tunnels automatiques (6to4, Teredo, ISATAP) pour contourner les règles de sécurité.



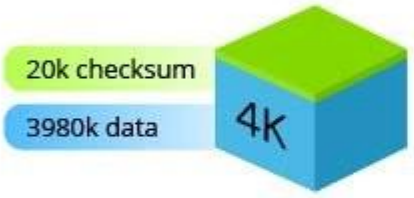
- **Effet :** Infiltration dans le réseau IPv6 via une couche IPv4, souvent non surveillée.

7.2. Fragmentation abuse

- IPv6 permet la fragmentation uniquement à l' hôte émetteur.

- =

IP Fragmentation and Reassembly
(Example)



length	ID	fragflag	offset
4000	X	0	0

MTU = 1500 Bytes, Offset = 1480/8

length	ID	fragflag	offset
1500	X	1	0

length	ID	fragflag	offset
1500	X	1	185

length	ID	fragflag	offset
1040	X	0	370

Length - The size of the fragmented datagram

ID - The ID of the datagram being fragmented

Fragflag - Indicates whether there are more incoming fragments

Offset - Details the order the fragments should be placed in during reassembly

- Des fragments mal formés ou délibérément séparés peuvent **bypasser les systèmes de détection d’ intrusion (IDS)**.

Outils courants d'attaque IPv6

Outil	Fonction
THC-IPv6	Suite complète d'attaques NDP, RA, SLAAC
Metasploit IPv6	Modules d'exploitation IPv6
Scapy6	Forge de paquets IPv6 personnalisés
Nmap/Zmap	Scan IPv6
Chiron	Génération et manipulation de paquets IPv6 (attaque et fuzzing)

Résumé des vulnérabilités et vecteurs d'attaque

Vecteur	Attaque	Impact
NDP	Spoofing / DoS	MITM, déni de service
RA	Falsification	Redirection, crash
SLAAC	Faux préfixes	Hijacking, perte de connectivité
Multicast	Flooding	Ralentissement réseau
Tunneling	Bypass de sécurité	Intrusion
IID	Tracking	Atteinte à la vie privée
Fragmentation	IDS evasion	Contournement sécurité

3. Contre-mesures et bonnes pratiques

3.1. Filtrage et pare-feu

- Utiliser des **firewalls compatibles IPv6**.
- Bloquer les **RAs non autorisées** sur les réseaux clients.
- Restreindre les paquets NDP aux segments de réseau local.

3.2. Sécurisation de NDP

- **SeND (Secure Neighbor Discovery)** : ajout de certificats cryptographiques à NDP.
- **RA Guard** : blocage de RAs suspects.
- **ND Inspection** (ou ND Protection) : analyse des messages NDP dans les commutateurs de niveau 2.

3.3. Adressage sécurisé

- Activer les **adresses temporaires** pour la confidentialité.
- Désactiver SLAAC ou EUI-64 si non nécessaire.
- Mettre à jour et **durcir les configurations DHCPv6**.

3.4. Surveillance et journalisation

- Activer la journalisation IPv6 sur tous les équipements réseau.
- Mettre en place une détection d'intrusion IPv6-aware.
- Surveiller l'usage abusif des adresses multicast (ex. ff02::1, ff02::2).

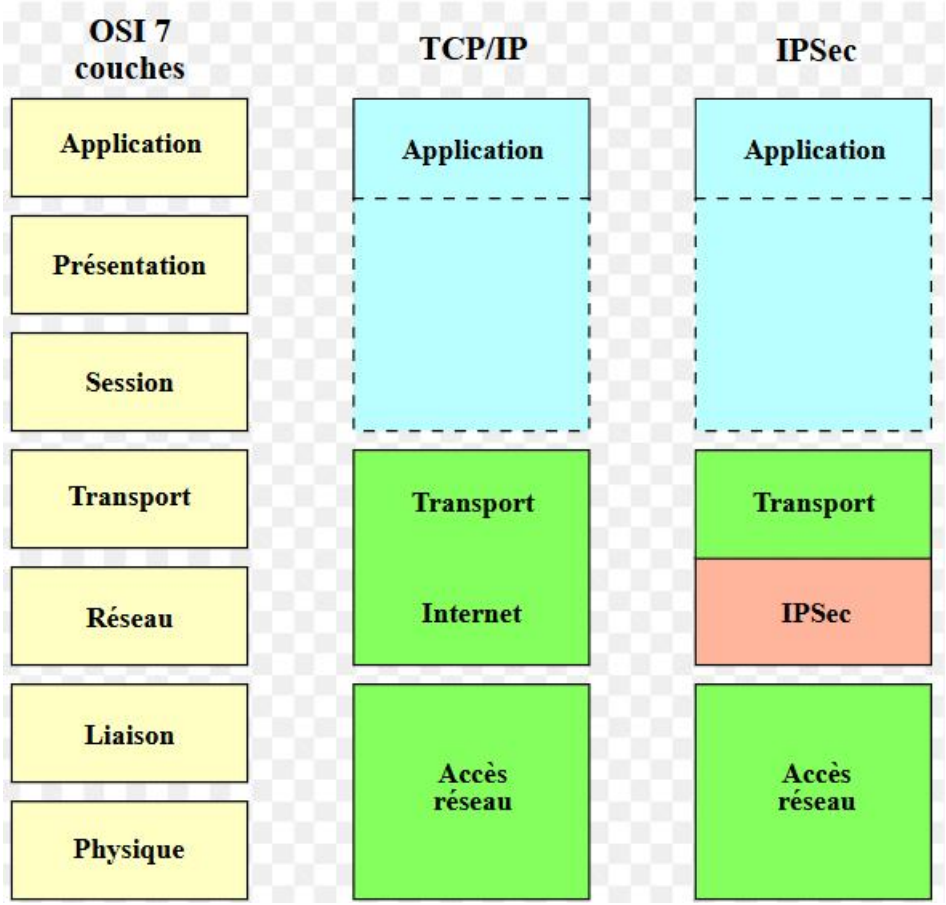
4. Bonnes pratiques pour les administrateurs

Recommandation	Détail
Formation IPv6	Former les équipes aux spécificités IPv6.
Test de sécurité	Réaliser des audits réguliers et des tests de pénétration.
Mise à jour	Maintenir à jour les firmwares des équipements réseau.
Dual Stack	Assurer la sécurité des deux piles (IPv4/IPv6).

IPSEC

IPSEC est un standard ouvert de l'IETF pour sécuriser les réseaux IP.

Il s'agit d'une technologie VPN de couche 3 qui transmet les données via un canal sécurisé établi entre deux points de terminaison (par exemple, deux passerelles de sécurité). Ce canal sécurisé est généralement appelé tunnel IPsec.



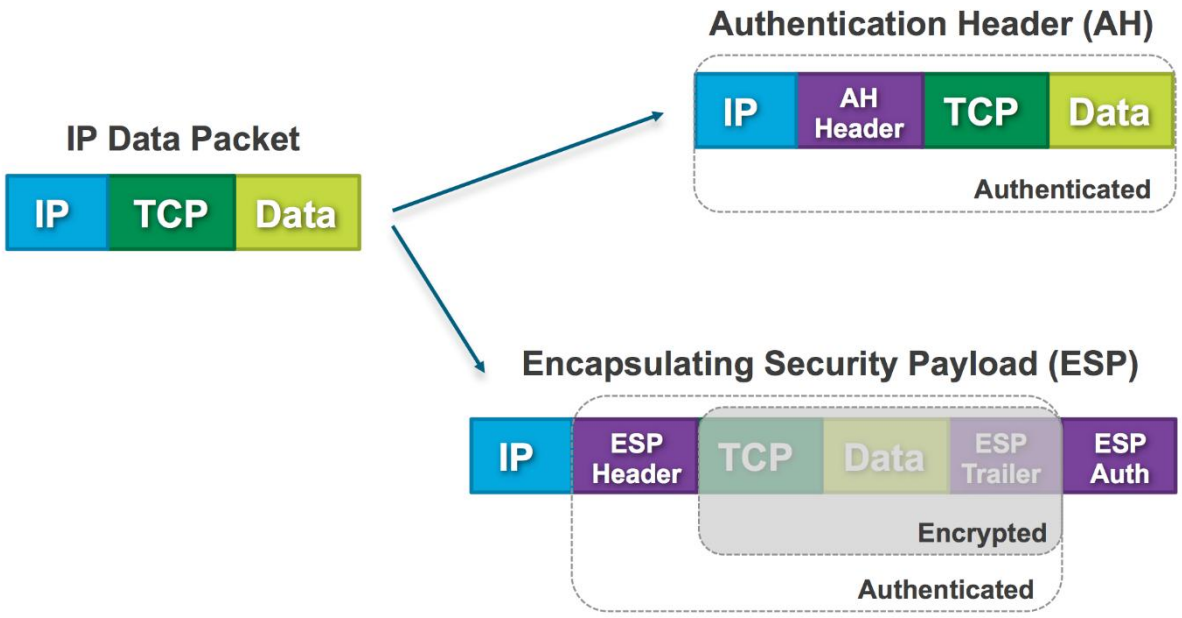
Il assure les fonctions de sécurité suivantes :

Service	Description	Méthode
Confidentilité des données	Des algorithmes de chiffrement confidentialisent le trafic	DES, 3DES, AES
Intégrité des données	Empêche les attaques d' homme-du-milieu et s' assure que les données n' ont pas été modifiée lors de leur transport	HMAC : MD5 ou SHA
Authentification de l' origine	Vérifie l' identité des pairs par un mécanisme d' authentification	PSK, certificats ou nonces

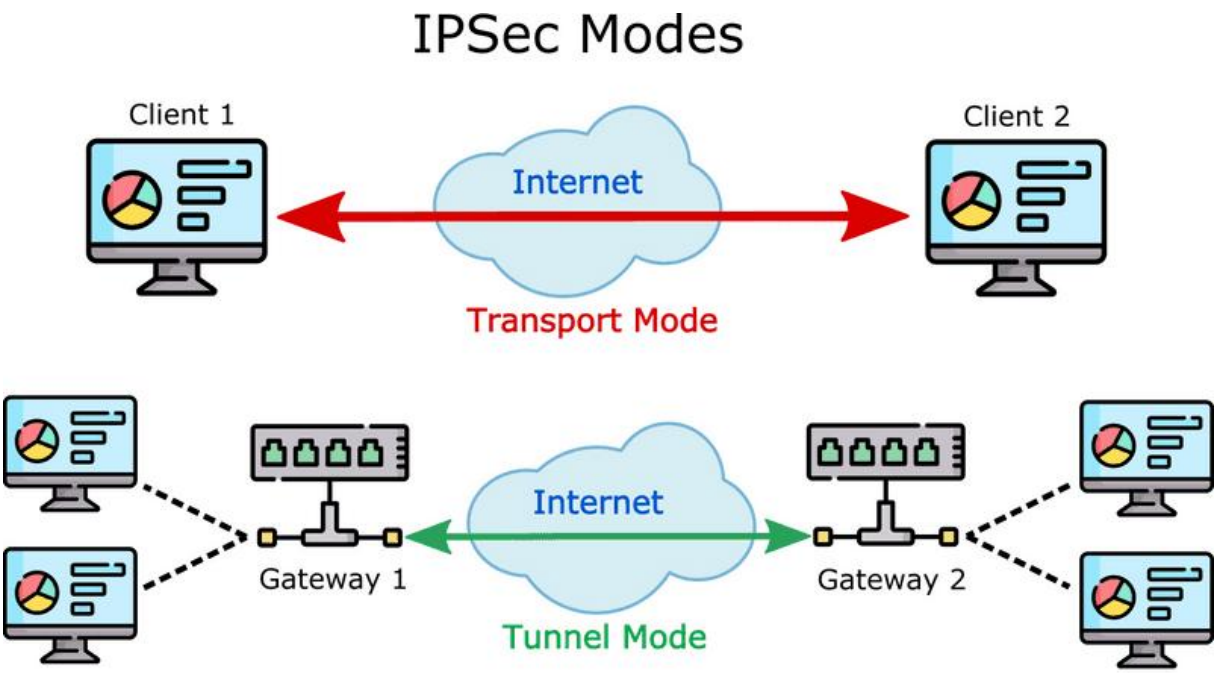
		RSA, signatures ECDSA
Protection anti-rejeu	-	-
Gestion des clés secrètes	Algorithme de chiffrement asymétrique	Diffie-Hellman (DH) ou ECDH

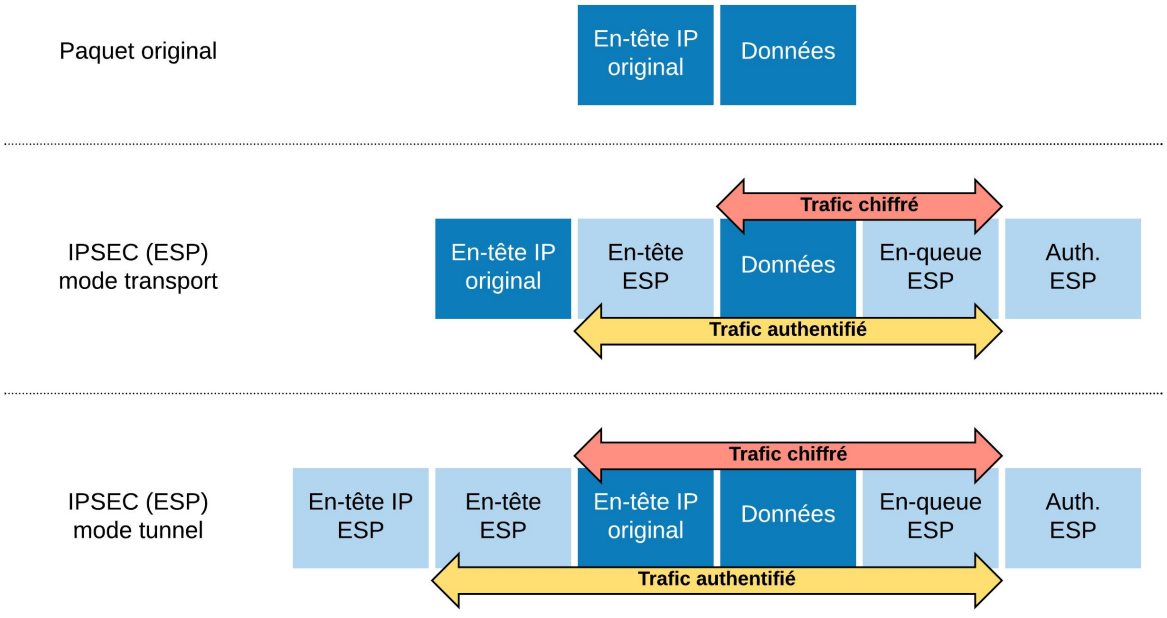
Principe de fonctionnement

IPSEC propose deux protocoles de couche 3 pour encapsuler le trafic de manière sécurisée : **AH (Authentication Header, IP51)** et **ESP (Encapsulating Security Payload, IP50)**.



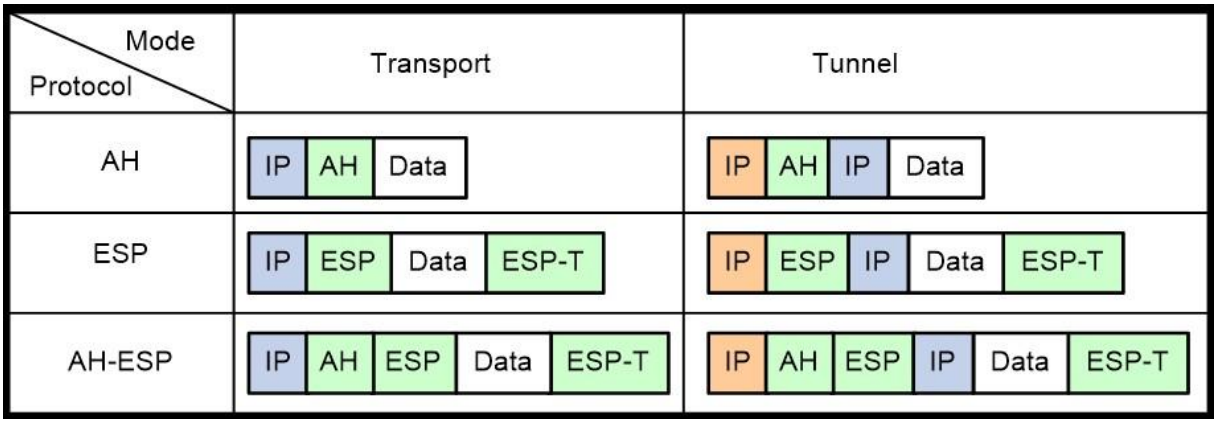
Mode de fonctionnement


IPSec Modes
Client 1
Internet
Client 2
Transport Mode
Gateway 1
Internet
Gateway 2
Tunnel Mode


Paquet original
En-tête IP original
Données
IPSEC (ESP) mode transport
Trafic chiffré
En-tête IP original
En-tête ESP
Données
En-queue ESP
Auth. ESP
Trafic authentifié
IPSEC (ESP) mode tunnel
Trafic chiffré
En-tête IP ESP
En-tête ESP
En-tête IP original
Données
En-queue ESP
Auth. ESP
Trafic authentifié

Transport Mode	Tunnel Mode
IP payload is encrypted	IP payload is encrypted
IP header is not encrypted	IP header is encrypted
Original IP header is used for routing decisions	New IP packet encapsulates the encrypted one with a new header that is used for routing decisions
Provides protection for the payload from end to end	

Encapsulation ipsec



Conclusion

IPv6 apporte des améliorations majeures, mais introduit aussi de nouvelles vulnérabilités.

Une approche proactive combinant pare-feux, chiffrement (IPsec) et surveillance (IDS) est essentielle pour sécuriser les réseaux IPv6. Les administrateurs doivent également suivre les bonnes pratiques de configuration et de mise à jour pour minimiser les risques.