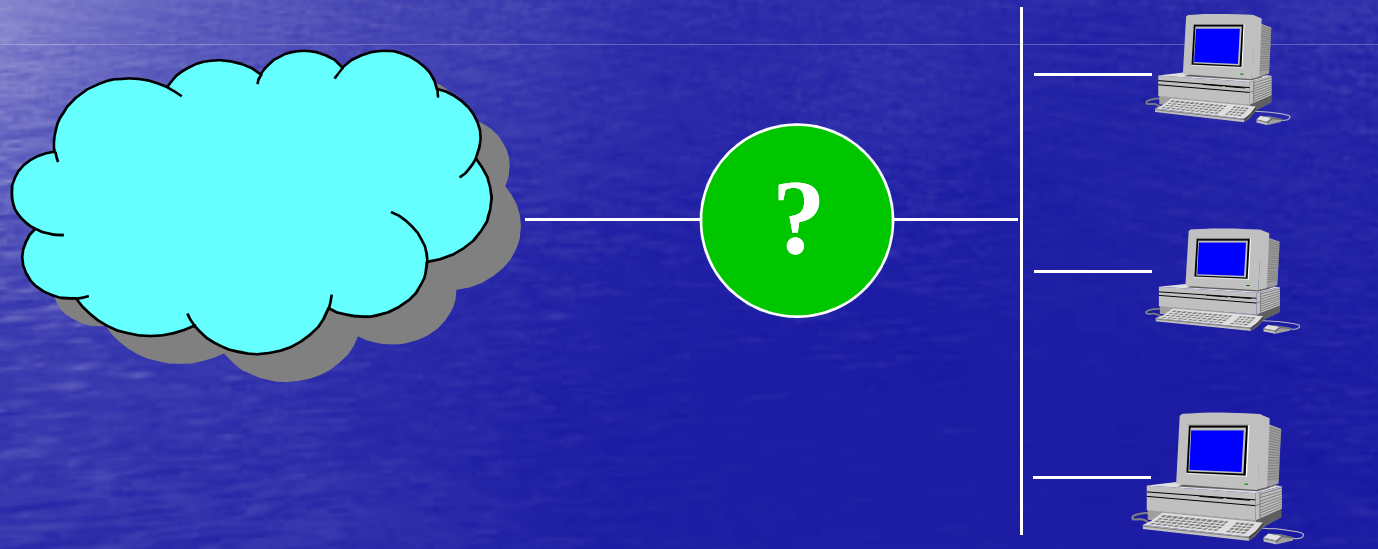
Sécurité des Réseaux

- Architectures de réseaux sécurisés
  - Routage, Filtrage
  - Pare-feu
  - Passerelle proxy
  - DMZ
  - Scanner et IDS
- IPSec et VPN
- Réseaux sans-fil

Architecture de Réseaux

- Quelle est la meilleure protection pour sécuriser le réseau local ?



Contrôle et Filtrage

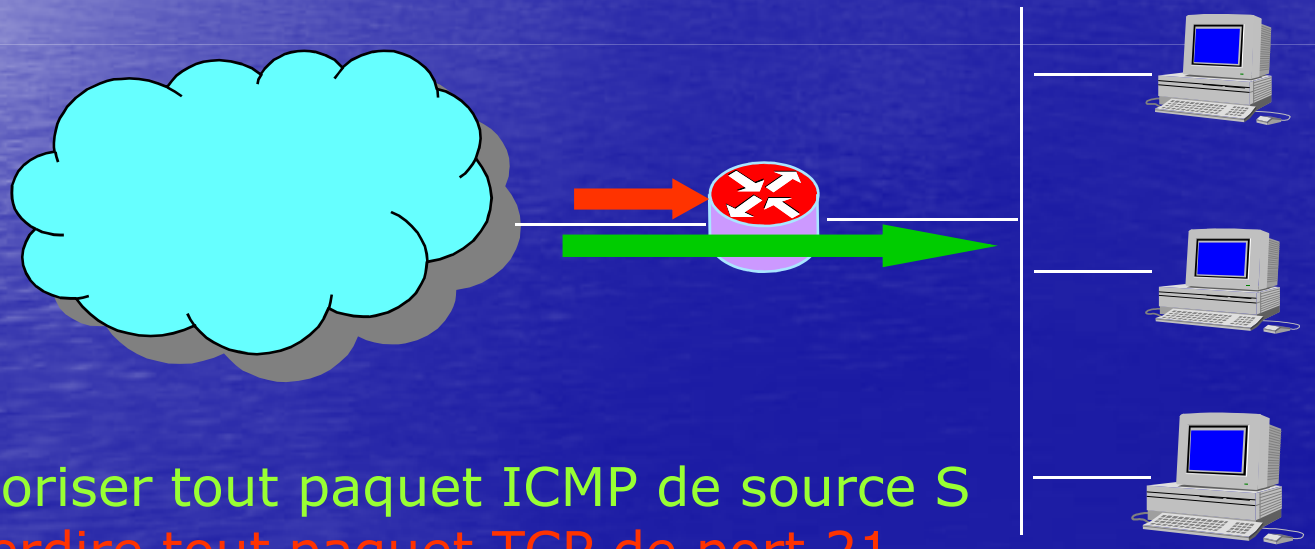
- Le routage avec ACL
- Le filtrage sans état
- Le filtrage avec état
- La translation d 'adresse
- Le proxy ou mandataire
- Le filtrage applicatif

Filtrage stateless ou sans état

- Filtrage portant sur :
  - les adresses IP source et destination
  - Le protocole transporté
  - les port TCP ou UDP
- Rapide et facile à mettre en œuvre (possible sur routeur)
- Les paquets sont filtrés un par un
- Pas de notion d'état (de mémoire)
- Règles ou Access-List

Architecture de Réseaux sécurisés

- **Filtrage : le routeur filtre les paquets sur les règles des « access-list »**



Autoriser tout paquet ICMP de source S
Interdire tout paquet TCP de port 21

Limites du Filtrage sans état

- Ne permet pas de tracer une session ou de détecter certaines attaques, car il ne mémorise pas d'état
- Ne détecte pas le DOS SYN-flooding
- Ne bloque pas les paquets malformés (ping of death, …)
- Pas de traitement des protocoles utilisant un port dynamique

Filtrage avec état (stateful)

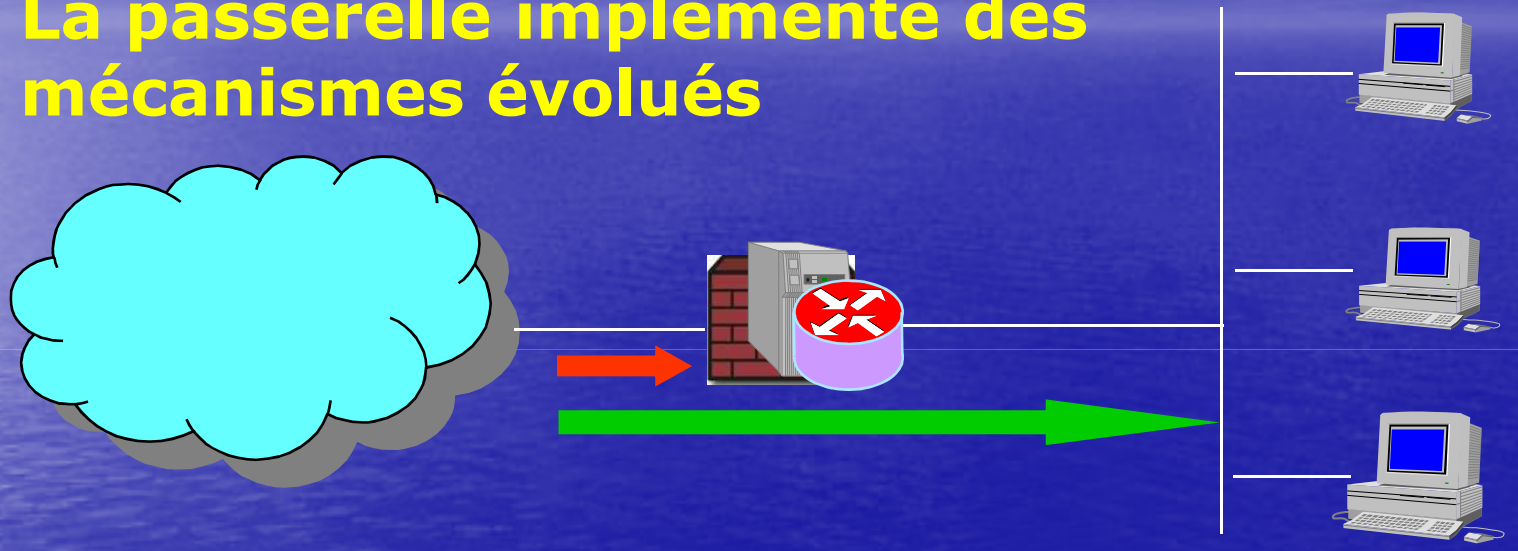
- Filtrage sur portant sur :
  - les adresses IP
  - les port TCP ou UDP
  - les flags TCP
- Filtrage des paquets avec contexte de sessions ou connexions TCP/UDP/ICMP (notion de mémoire).
- Plus dynamique et plus souple
- Protection de certaines attaques Déni de Service

Le pare-feu

- Passerelle pour toutes les communications et contrôle du trafic entre le réseau local et les réseaux externes
- Implémente de nombreuses fonctionnalités
  - Filtrage d'accès et de contenu
  - Réseau privé virtuel
  - La translation d'adresses réseau
  - Détection des intrusions
- Point de contrôle unique pour la protection du réseau
- Point névralgique de sécurité
- Firewalls Cisco PIX, CheckPoint ....

Architecture de Réseaux sécurisés

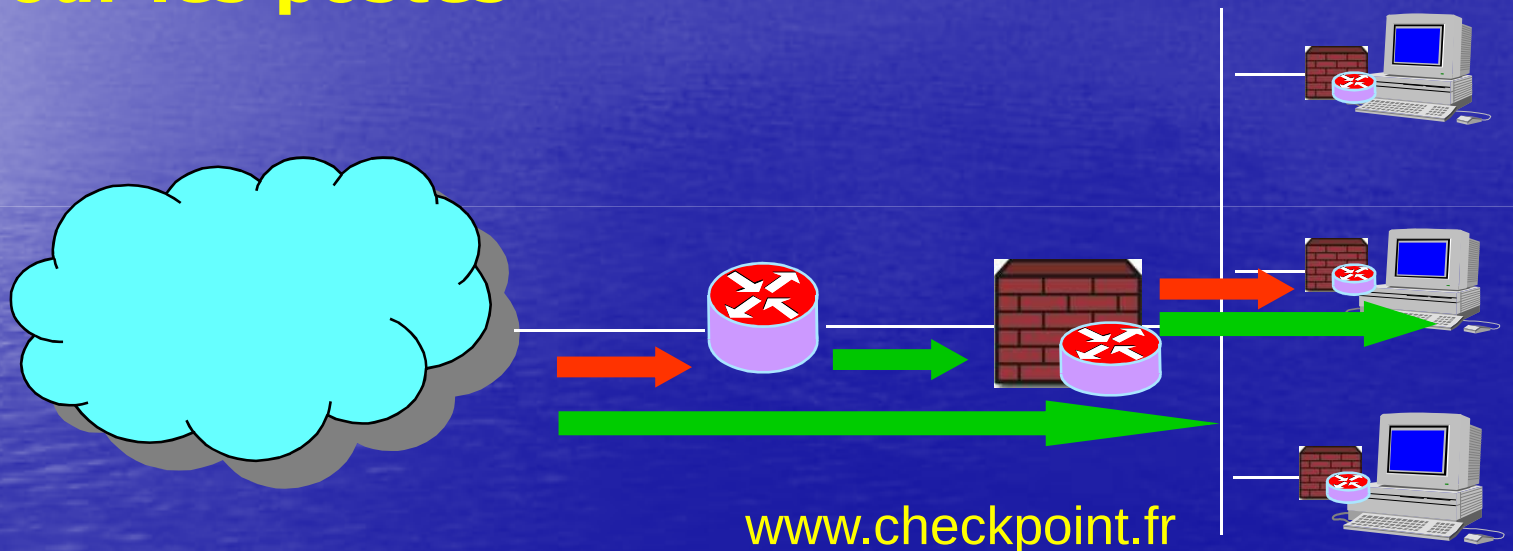
- La passerelle implémente des mécanismes évolués



- Translation NAT
- Filtrage du contenu des applications
- Anti-virus
- Authentification/autorisation des applications
- Chiffrement

Architecture de Réseaux sécurisés

- On peut choisir de dupliquer les pare-feus pour le réseau local et pour les postes

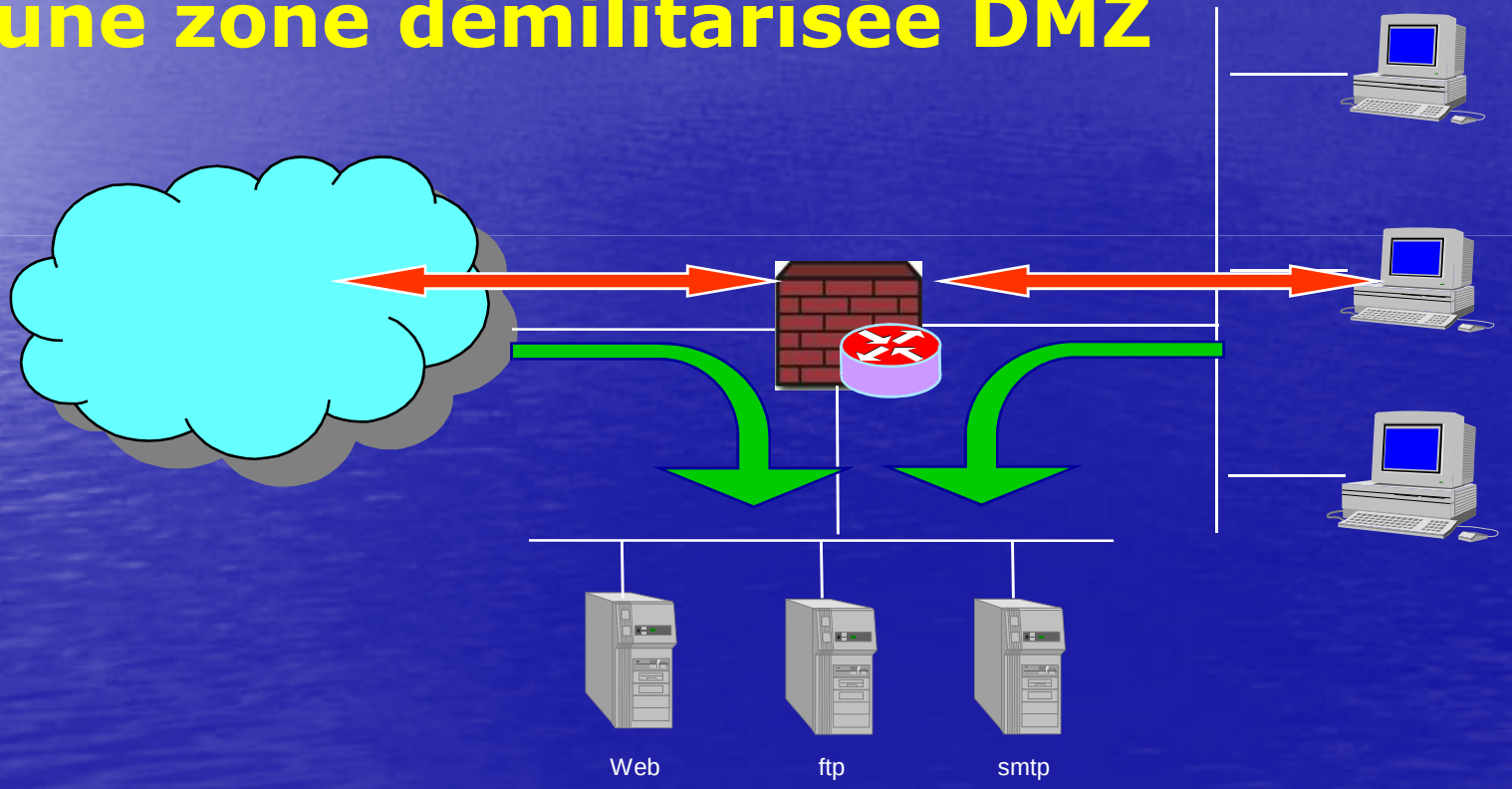


www.checkpoint.fr
www.cisco.fr

www.zonelabs.com
www.kerio.com

Architecture de Réseaux sécurisés

- Les serveurs sont isolés dans une zone démilitarisée DMZ



La passerelle proxy

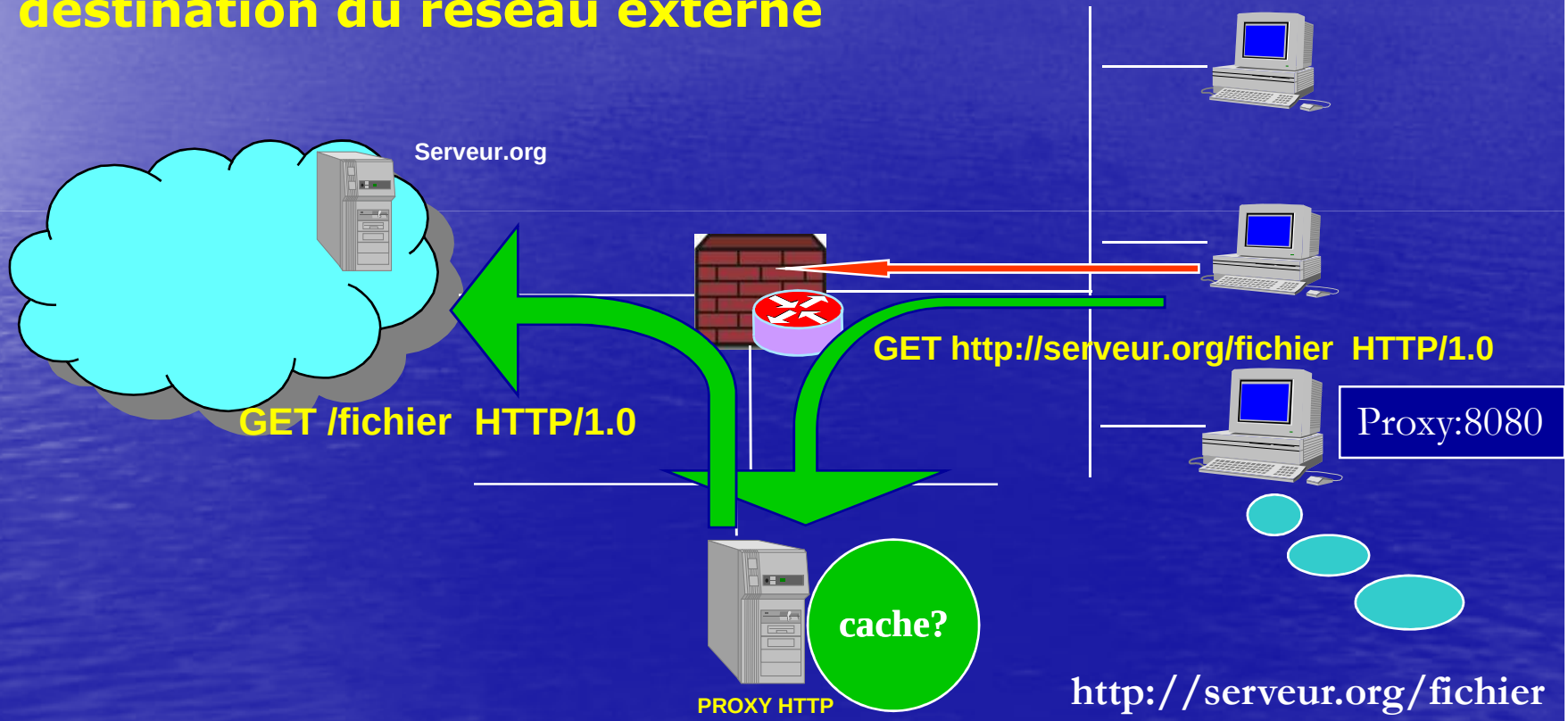
- Une passerelle joue le rôle de mandataire ou intermédiaire entre les postes du réseau local et les réseaux externes
- **Proxy générique** recopie le flux sans contrôle spécifique (proxy de circuit) ou implémente des mécanismes de filtrage
- Relais applicatif ou machine bastion dans une zone démilitarisée

La passerelle proxy

- Traitement des données niveau application
  - Permet une authentification des utilisateurs et une analyse du type de requêtes (filtrage d'url)
  - Un proxy par service offert : http, ftp, telnet, SMTP, etc
- Optimisation : Un proxy serveur HTTP implémente des mécanismes de cache d'URL

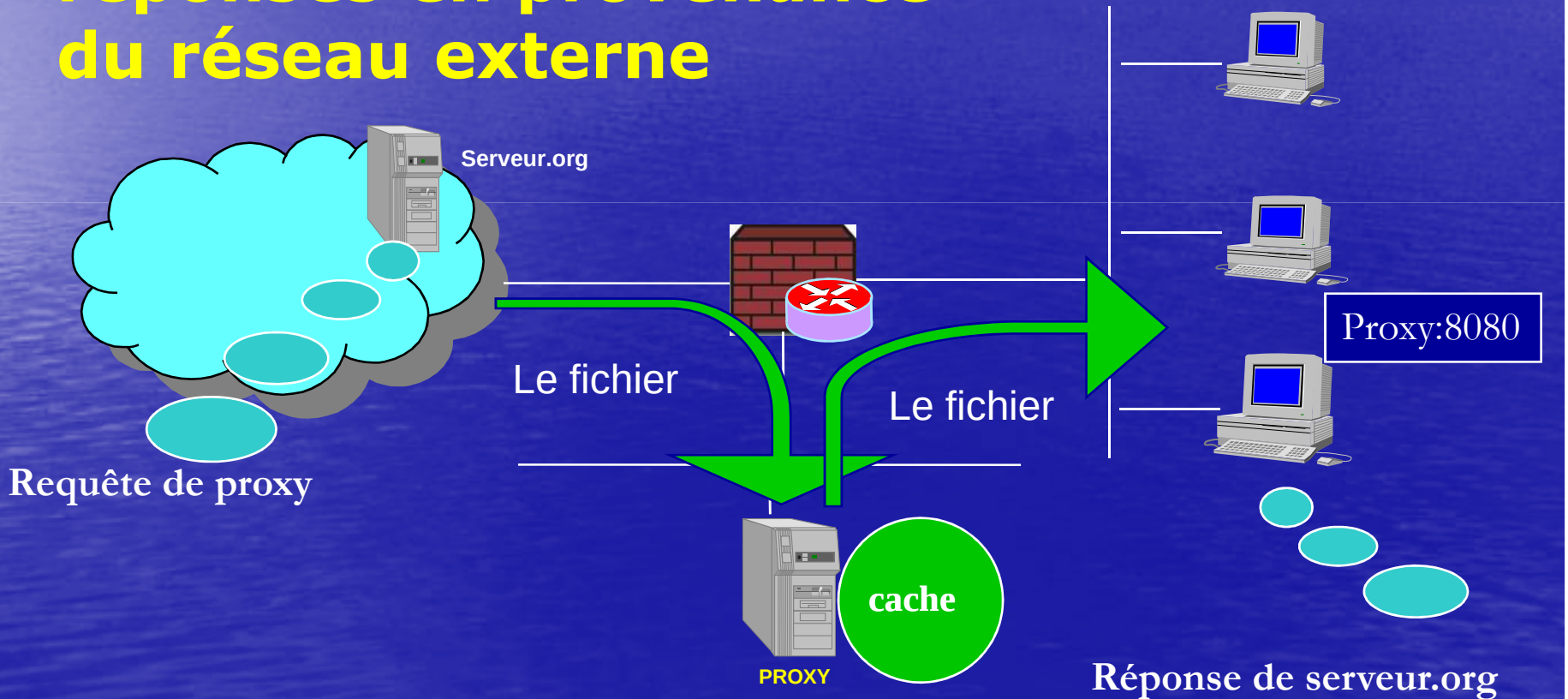
Architecture de Réseaux sécurisés

- Le serveur proxy relaie les requêtes à destination du réseau externe



Architecture de Réseaux sécurisés

- Le serveur proxy relaie les réponses en provenance du réseau externe



Les outils : scanner

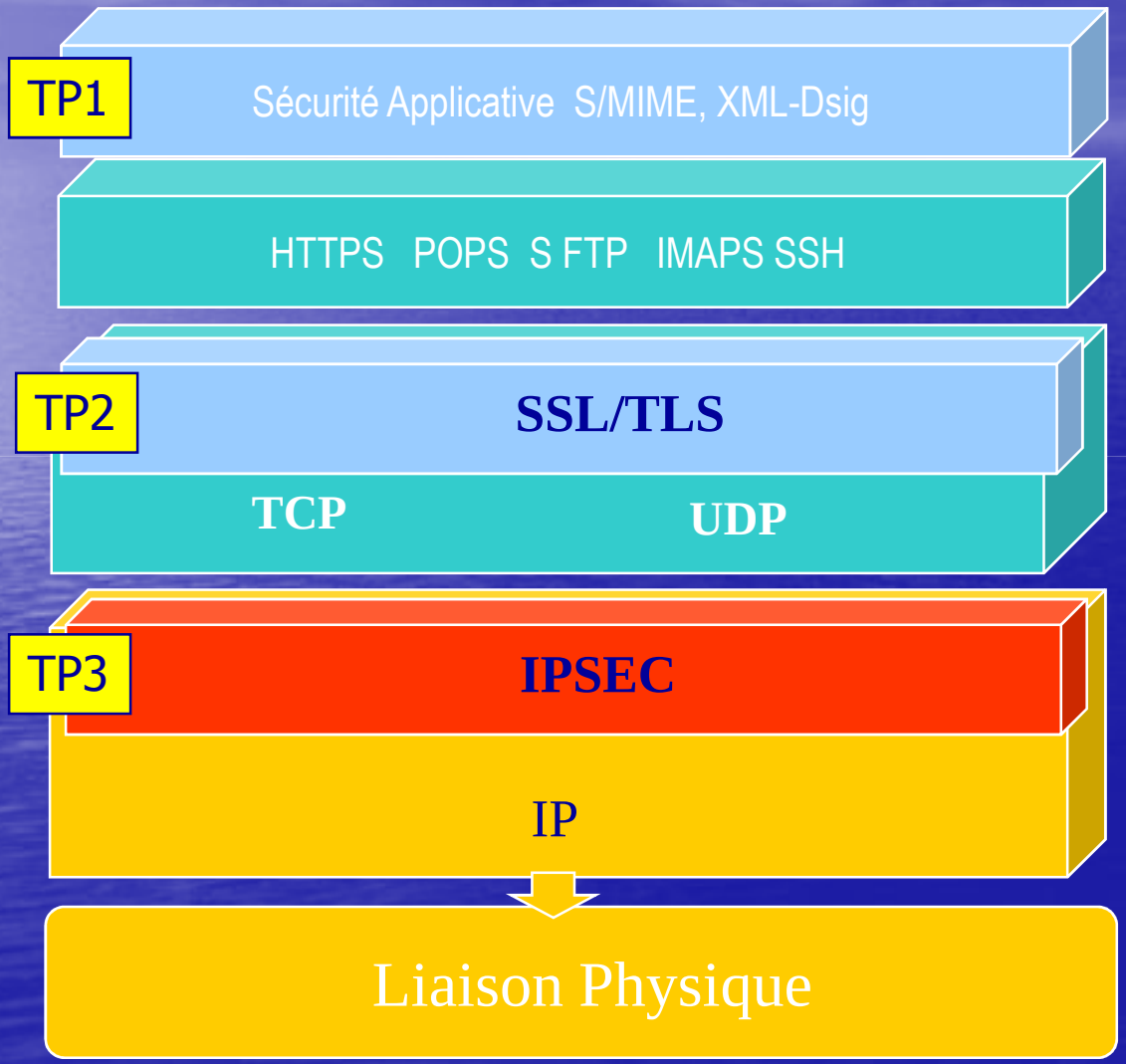
- Un scanner est un outil qui recherche les vulnérabilités d'un site
- La recherche doit être possible à distance
- A mettre entre les mains d'un administrateur
- Difficile d'être exhaustif et de rester dynamique face aux multiples annonces de vulnérabilités

IDS et détection d'intrusion

- Un détecteur d'intrusion ou IDS (*Intrusion Detection System*) est un programme permettant de détecter une intrusion
  - par analyse du trafic réseau (analyse des paquets, comparaison à des modèles)
  - par inspection des journaux, contrôle de l'activité du système
  - Par détection de signature (attaque connue)
  - Par détection d'anomalie (par rapport à un modèle d'activité)
  - Par vérification d'intégrité

Snort www.snort.org

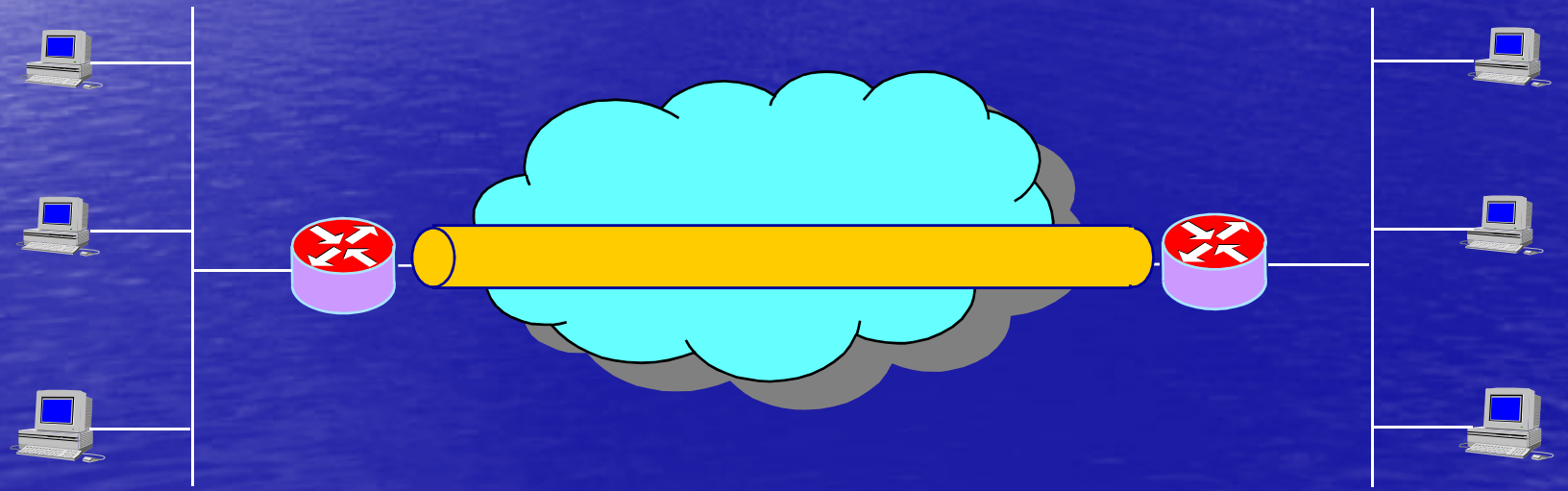
Modèle OSI et Sécurité : IPSEC



VPN : La couche Transport et toutes les applications sur UDP et TCP bénéficient de la sécurité IPSEC de manière transparente

IPSEC : Internet Protocol Security

- Développement initial dans IPv6
- Standardisé par l'IETF
- Traitement au niveau Réseau
  - Chiffrement et intégrité des paquets IP
  - Authentification des équipements
  - Toutes les applications en bénéficient



IPSEC : les composants

- Les protocoles
  - AH Authentication Header
  - ESP Encapsulating Security Payload
  - IKE Internet Key Exchange
- Les bases de données
  - SA Security Association
    - Paramètres : fonction, mode, clés, algorithmes…
  - SP Security Policy
    - Traitements à appliquer aux flux

IPSEC et SAD les fonctions

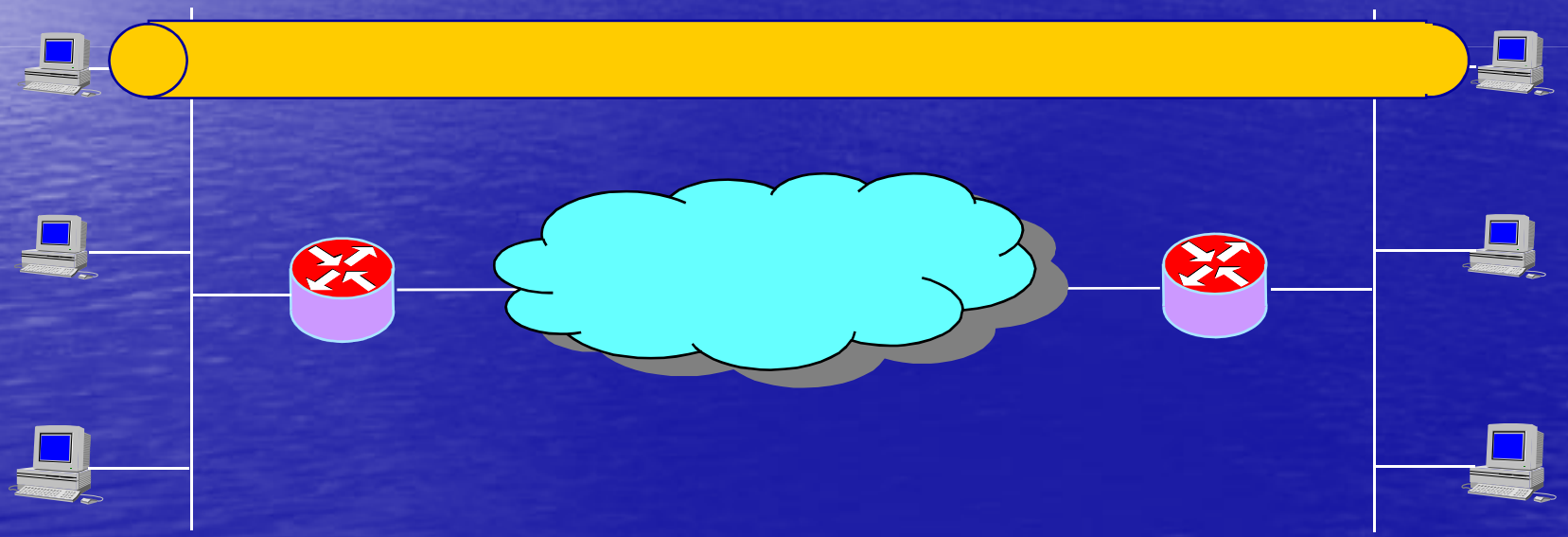
- AH
  - Authentification et intégrité
  - Insertion d'un en-tête
  - Le paquet IP (en-tête+data) transite en clair
  - Nécessite un secret partagé
- ESP
  - Chiffrement des données
  - Insertion d'un en-tête
  - Nécessite un secret partagé
- IPComp
  - Compression des données

IPSEC et SAD les modes

- Transport
  - Sécurité de bout en bout A - B
  - Seules les applications de A et de B bénéficient de la sécurité
  - Les adresses IP de A et B transitent en clair
- Tunnel
  - Établi entre 2 routeurs X - Y
  - Les applications de tous les postes des réseaux privés peuvent bénéficier de la sécurité (SPD)
  - Les adresses IP ne sont pas visibles, car encapsulées dans des paquets IP X – Y dont le contenu est chiffré

VPN avec IPSEC

- Mode transport
- Entre 2 équipements d'extrémité
- Indépendant des applications

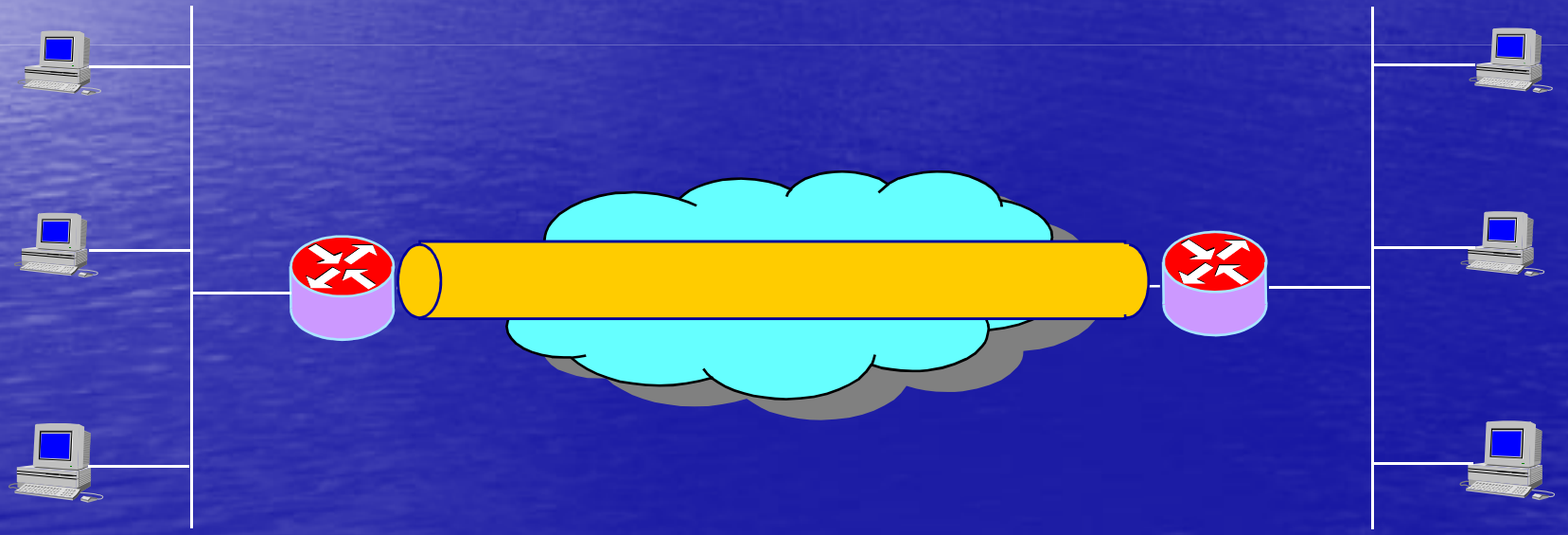


VPN et IPSEC

- Mode tunnel
- Entre 2 équipements d'interconnexion

→ Transparent au réseau local

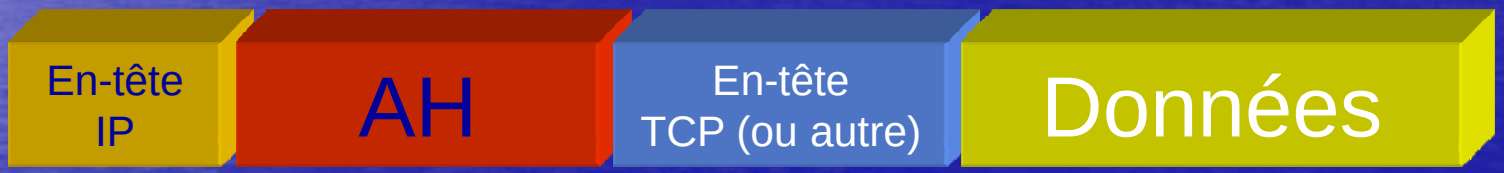
→ Tous les postes en bénéficient



Encapsulation AH

- **Paquet IP Original**

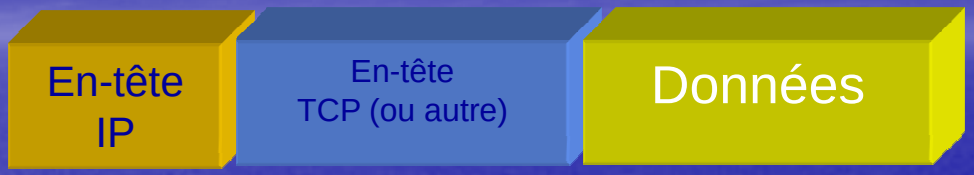
- **AH en mode Transport**



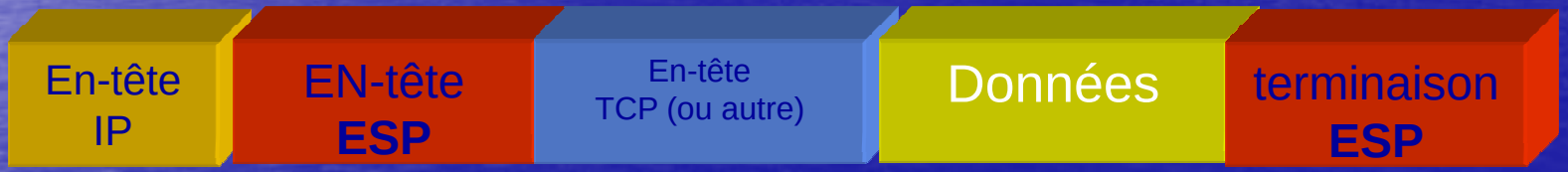
- **AH en mode Tunnel**

Encapsulation ESP

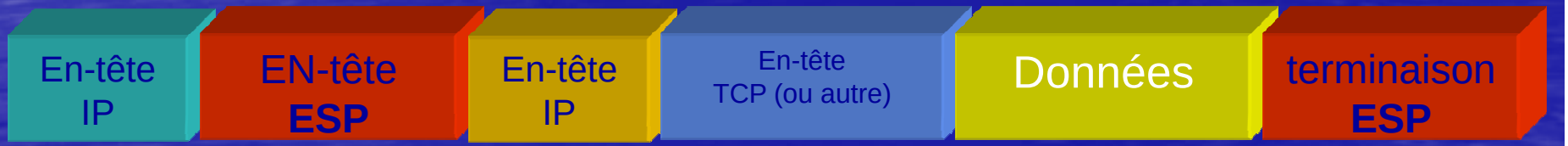
- **Paquet IP Original**



- **ESP en mode Transport**



- **ESP en mode Tunnel**



SAD : Algorithmes et clés

- 3 modes de partage du secret
  - Configuration initiale manuelle
  - IKE échange de clés
  - Certificats X509v3

Algorithmes AH

algorithm	(bits) keylen	comment
hmac-md5	128	ah: rfc2403 128
	128	ah-old: rfc2085
hmac-sha1	160	ah: rfc2404 160
	160	ah-old: 128bit ICV
keyed-md5	128	ah: 96bit ICV
	128	ah-old: rfc1828
keyed-sha1	160	ah: 96bit ICV
	160	ah-old: 128bit ICV
null	0 to 2048	for debugging

Algorithmes ESP

algorithm	(bits) keylen	comment
des-cbc	64	esp: rfc2405
3des-cbc	192	rfc2451
simple	0 to 2048	rfc2410
blowfish-cbc	40 to 448	rfc2451
cast128-cbc	40 to 128	rfc2451
rc5-cbc	40 to 2040	rfc2451
des-deriv	64	ipsec-ciph-des-
3des-deriv	192	no document

IPSEC et SAD : exemple

 # setkey –D ***// liste la SAD***

// syntaxe ajout SA

// setkey –c add

//<adr-src> <adr-dst>

//esp|ah

//<SPI>

//-E|-A

//<algo> <clé ascii ou hexa> ;

 # setkey –c
add 1.2.3.4 5.6.7.8 esp 55432 –E blowfish-cbc «AZERT» ;
 # setkey –c
add 1.2.3.4 5.6.7.8 ah 55432 –A hmac-md5 «12345678901234 56» ;

IPSEC et SPD
Politique de sécurité

- Décrit les règles de traitement des paquets
  - En fonction des adresses
  - En fonction des protocoles
  - Indique le traitement nul, abandon ou ipsec

- Ex: tout paquet du réseau 10.10.10/24 à destination de 20.20.20/24 doit emprunter le VPN IPSEC avec ESP et AH en mode tunnel entre 1.2.3.4 et 4.5.6.7

IPSEC et SPD : exemple

setkey –DP *// liste la SPD*

// syntaxe ajout SP
// setkey –c
// spdadd
// <adr-src> <adr-dst>
// any
// –P out | in
// ipsec ah | esp /
// tunnel | transport /
// [<src>-<dst>] /
// [require|use]]

```
# setkey –c
spdadd 10.10.10.0/24   20.20.20.0/24
any   –P   out  ipsec
esp/tunnel/1.2.3.4-5.6.7.8/use;
```

TP3 : Pare-feu et IPSEC