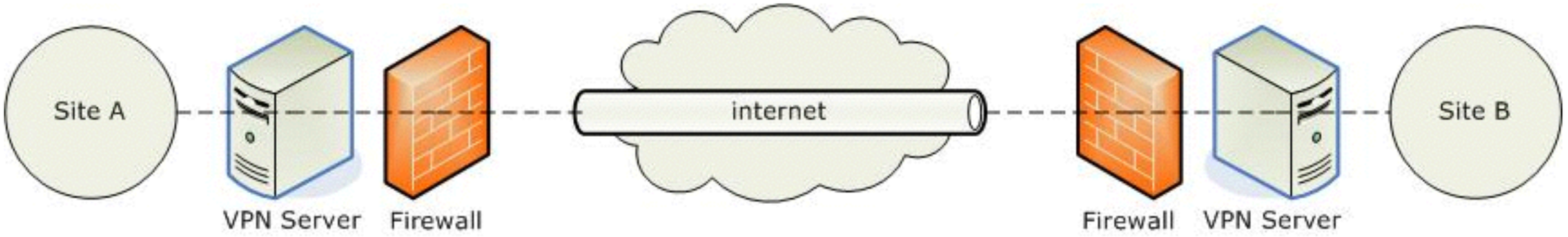
VPN avec IPsec

Nicolas Ollinger, Université d'Orléans

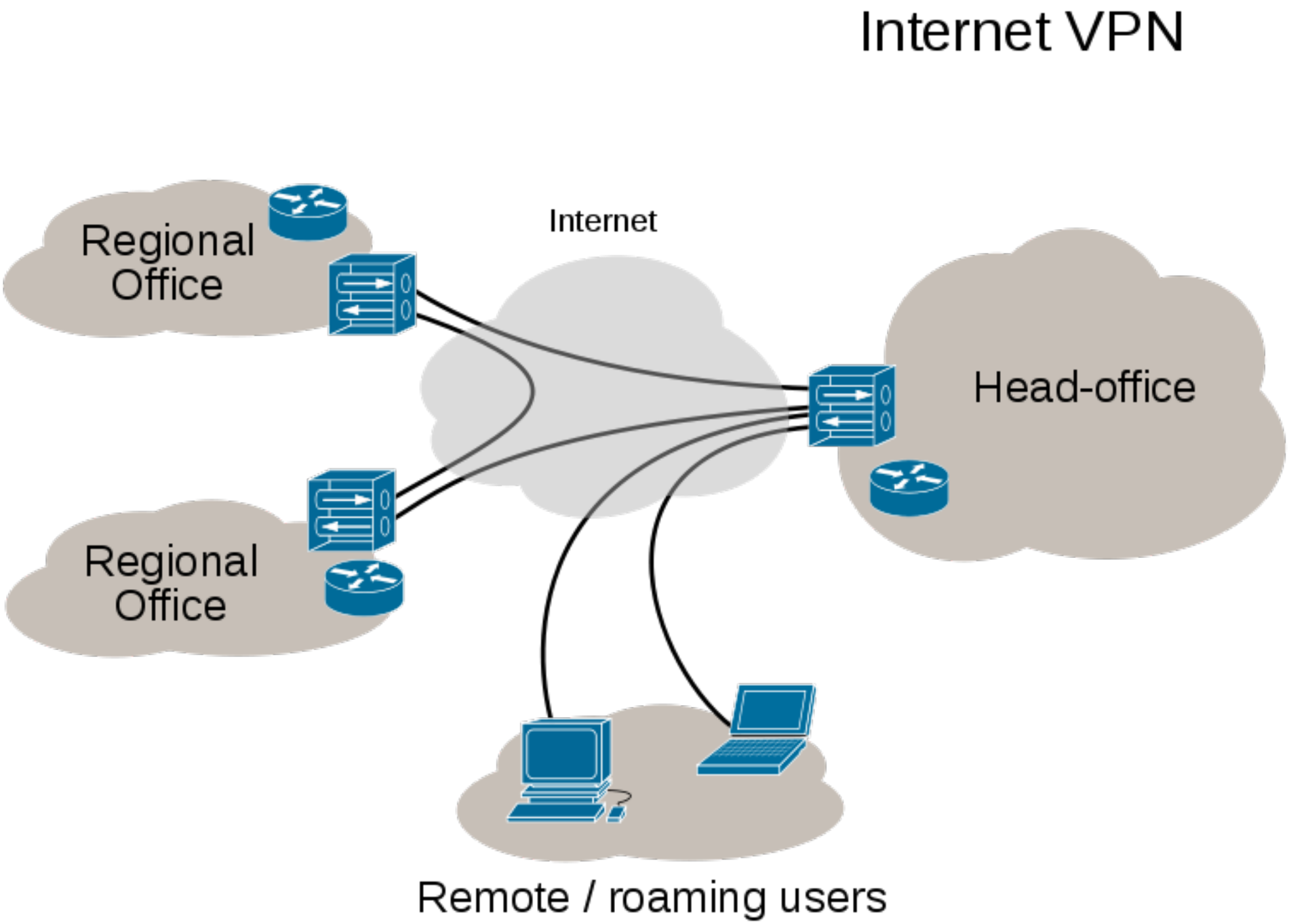
M2 SIR Sécurité des réseaux — **S4** 2015/2016

Virtual **P**rivate **N**etwork

- Un **VPN** permet de créer une **liaison sécurisée** entre deux réseaux distants à travers un réseau non sûr (par exemple l'internet public).
- Se substitue (ou complète !) à la location d'une liaison spécialisée entre deux routeurs éloignés.



lan-to-lan, host-to-lan



Fonctionnalités

Authentification Vérifier l'identité des deux extrémités du VPN par authentification mutuelle.

Contrôle d'intégrité Empêcher la modification du flux réseau qui traverse le VPN (prévenir l'ajout de paquets ou la modification du contenu des paquets).

Confidentialité Empêcher l'écoute des données.

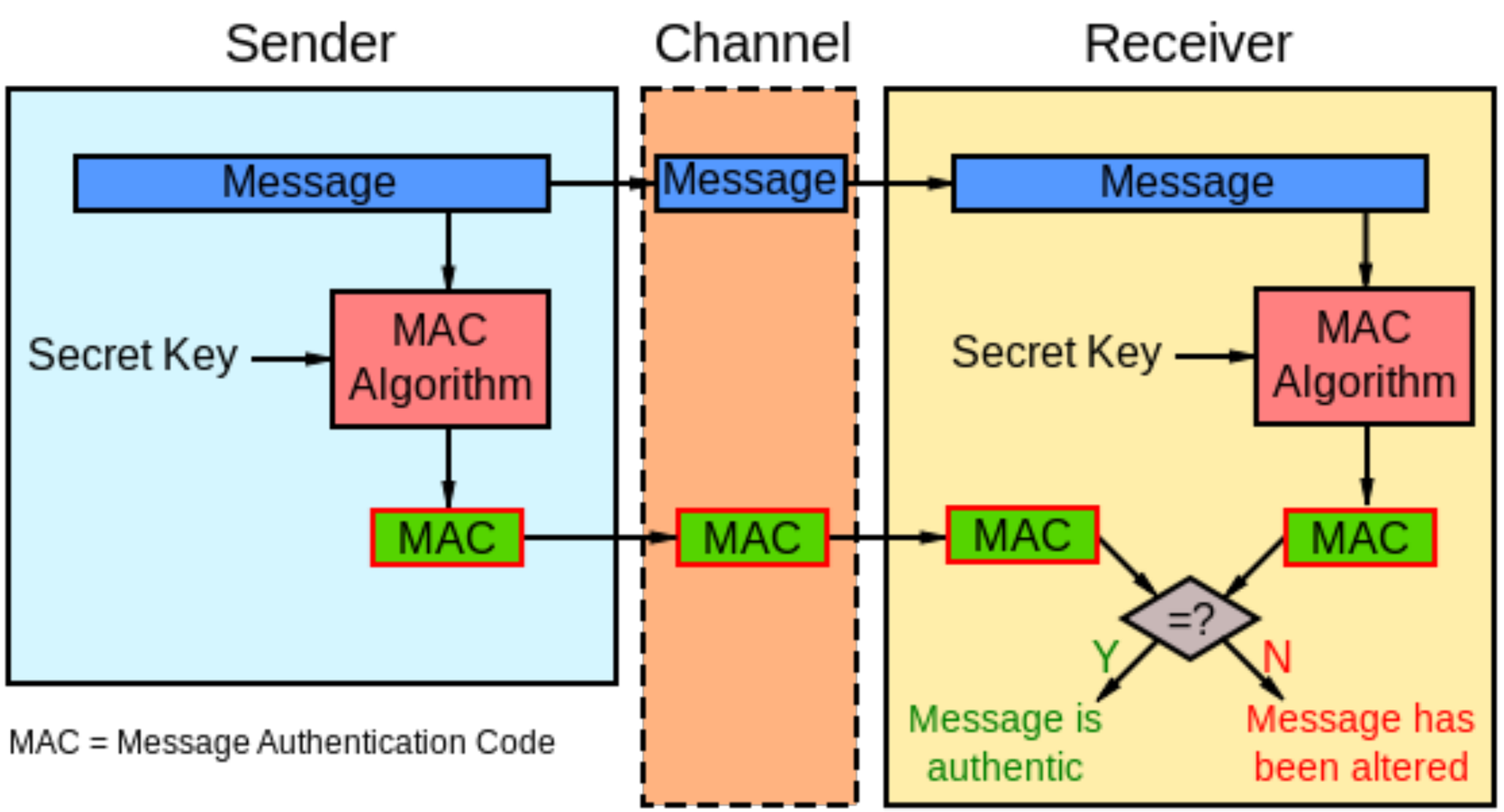
Authentification

- Connexion lan-to-lan :
  - ➡ mot de passe (**P**re-**S**hared **K**ey)
  - ➡ certificats numériques (**P**ublic **K**ey **I**nfrastructure)

- Connexion remote access :
  - ➡ login + mot de passe (voire **O**ne **T**ime **P**assword)
  - ➡ certificats numériques (**P**ublic **K**ey **I**nfrastructure)

Contrôle d'intégrité

Utilisation de codes d'authentification de message (**MAC**) combinant fonction de hachage cryptographique et clé secrète (par exemple HMAC).



Confidentialité

- Chiffrement des messages à l'aide de primitives cryptographiques normalisées.
- Chiffrement symétrique : 3DES, AES, Blowfish, RC4, …
- Chiffrement asymétrique : RSA, DSA, …
- cf cours **Sécurité et Protocoles**

Technologies

- Protocoles ad hoc propres à une technologie :
  - ➡ OpenSSH (PermitTunnel + -w)
  - ➡ OpenVPN (tunnels SSL sur UDP/TCP)

- Protocoles normalisés :
  - ➡ IPsec en mode transport ou tunnel
  - ➡ IPsec/GRE : couche 3 + multicast + …
  - ➡ IPsec/L2TP : couche 2

IP security (IPsec)

RFC 4301

« (…) IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, detection and rejection of replays (a form of partial sequence integrity), confidentiality (via encryption), and limited traffic flow confidentiality. (…) »

Une solution normalisée pour le déploiement de VPN IP interopérables mise en œuvre par la quasi-totalité des acteurs du marché : Cisco, Juniper, SUN, HP, Microsoft, Checkpoint, GNU/Linux, OpenBSD, *etc*

Composants d'IPsec

- Des protocoles pour le transport des paquets qui transitent à l'intérieur du VPN :
  - ➡ Authentification Header (**AH**)
  - ➡ Encapsulating Security Payload (**ESP**)

- Une famille d'algorithmes cryptographiques normalisés à combiner à ces protocoles.

- Un protocole (optionnel) de gestion automatique de clés : Internet Key Exchange (**IKEv2**) Protocol.

- Un mécanisme type pare-feu pour décider des paquets qui passent par le tunnel et doivent être encapsulés par AH ou ESP.

AH et **ESP**

- Encapsulation de chaque paquet IP qui transite par le VPN, nouvelle entête IP + entête AH/ESP +
  - ➡ la charge utile du paquet IP en **mode transport** ;
  - ➡ le paquet IP complet en **mode tunnel**.

- Information présente dans l'entête :
  - ➡ **SPI** (Security Parameters Index)
  - ➡ **SN** (Sequence Number)
  - ➡ **ICV** (Integrity Check Value) si contrôle d'intégrité

- Pour en savoir plus : **An Illustrated Guide to IPsec**

Security **P**olicy **D**atabase

- Détermine la politique d'encapsulation IPsec du flux réseau entrant et sortant.
- Règle type pare-feu qui décide sur quels paquets appliquer quelle type d'encapsulation IPsec (AH vs ESP vs ESP+AH, transport vs tunnel).

```
spdadd 10.0.0.0/24 10.0.1.0/24 any -P in
  ipsec esp/tunnel/100.10.10.10-100.20.20.20/require;
spdadd 10.0.1.0/24 10.0.0.0/24 any -P out
  ipsec esp/tunnel/100.20.20.20-100.10.10.10/require;
```

Security **A**ssociation **D**atabase

- Détermine la politique de sécurité à partir du SPI, du type de protocole IPsec (AH, ESP) et éventuellement d'adresses IP.

- **S**ecurity **A**ssociation = protocoles + clés + …

```
add 100.10.10.10 100.20.20.20 esp 1337
                -E des-cbc 0xcafebabec00170ad
                -A hmac-md5 "there is no cake";
```

Gestion des clés

- Gestion **manuelle** : configuration statique des SA à l'aide de clés ou de certificats statiques.

- Gestion **automatique** des clés avec **IKE** : génération à la volée de clés pour chaque session IPsec (4 clés si ESP+AH bidirectionnel).

IKE et **IKEv2**

RFC 7296

1. Négociation sur la protection d'IKE
   (Diffie-Hellman à partir d'un secret partagé, …)

2. Négociation sur la protection IPsec
   (choix des protocoles et génération de clés)

3. Session IPsec jusqu'à expiration

sous GNU/Linux

- **https://wiki.debian.org/IPsec**

- ipsec-tools + racoon

- Configuration :
  racoon. conf + psk.txt + ipsec-tools.conf

sous OpenBSD

- Clés manuelles ou IKEv1 : **ipsec.conf**

- IKEv2 : **iked.conf**

Sur PIX/ASA

```
access-list 90 permit ip 10.0.0.0 255.255.255.0 10.0.1.0 255.255.255.0
sysopt connection permit-ipsec
crypto ipsec transform-set strong esp-3des esp-sha-hmac
crypto map rt 20 ipsec-isakmp
crypto map rt 20 match address 90
crypto map rt 20 set peer 100.20.20.20
crypto map rt 20 set transform-set strong
crypto map rt interface outside
isakmp enable outside
isakmp key cisco1234 address 100.20.20.20 netmask 255.255.255.255
isakmp identity address
isakmp policy 9 authentication pre-share
isakmp policy 9 encryption 3des
isakmp policy 9 hash sha
isakmp policy 9 group 1
isakmp policy 9 lifetime 86400
```

Voir doc Cisco + **recherche web**

Sur routeur Cisco

```
access-list 90 permit ip 10.0.0.0 255.255.255.0 10.0.1.0 255.255.255.0

crypto isakmp policy 11
  crypto 3des
  hash md5
  authentification pre-share
crypto isakmp key cisco1234 address 100.20.20.20

crypto ipsec transform-set blop esp-3des esp-md5-hmac

crypto map nolan 11 ipsec-isakmp
  set peer 100.10.10.10
  set transform-set blop
  match address 90

interface Gi0/0
  crypto map nolan
```

- voir doc Cisco + **recherche web**

Partie TP

- **En salle E09, le TP3 sous Netkit.**
- **En salle E11, autour d'un switch avec écoute SPAN, déployer des hôtes et des LANs avec VPN IPsec + IKEv1/IKEv2 hétérogènes :**
  - ➡ **routeurs Cisco ;**
  - ➡ **pare-feux Cisco PIX/ASA ;**
  - ➡ **Debian GNU/Linux + racoon ;**
  - ➡ **OpenBSD.**