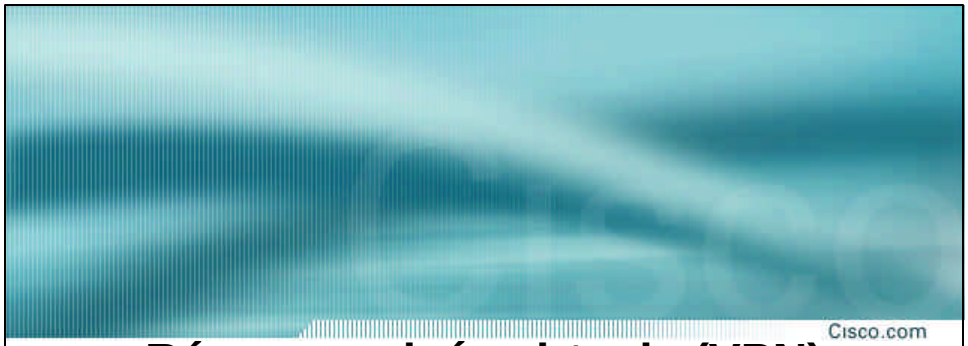


Réseaux privés virtuels (VPN)

Comment fonctionne le PATH MTU dans les tunnels GRE et IPSec?

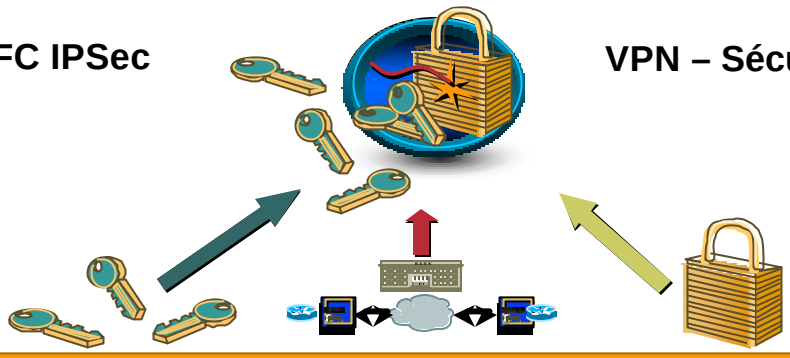
Martin Langlois

malanglo@cisco.com

Les VPNs

Cisco.com

RFC IPSec



VPN – Sécurité

Tunnels	Chiffrement	Authentification	Intégrité
• IPsec • GRE • L2TP/PPTP	• DES • 3 DES • AES	• RSA Digital Certificats • Clef partagée	• HMAC-MD5 • HMAC-SHA-1

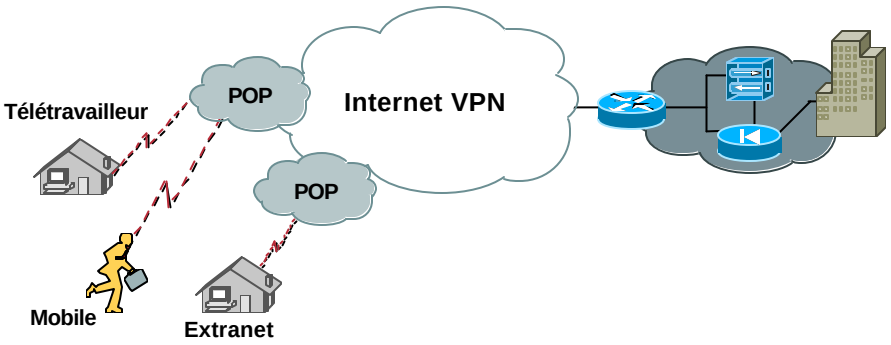
Agenda

Cisco.com

- Applications
- Considérations lors du design
- VPN site à site
- Interaction avec d’autres technologies

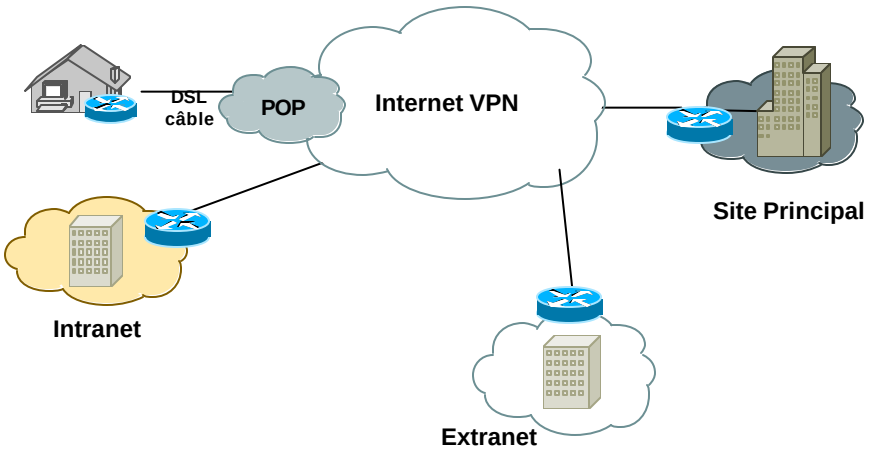
Accès Distant

Cisco.com



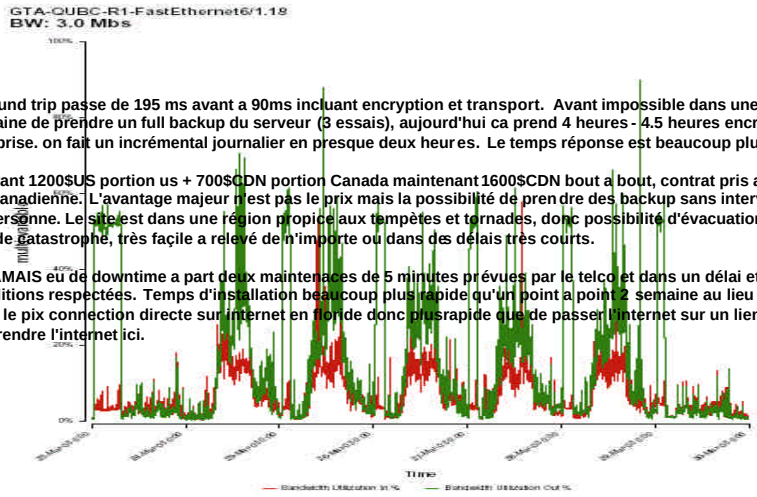
Replacement du lien WAN

Cisco.com



Replacement du lien WAN

Cisco.com



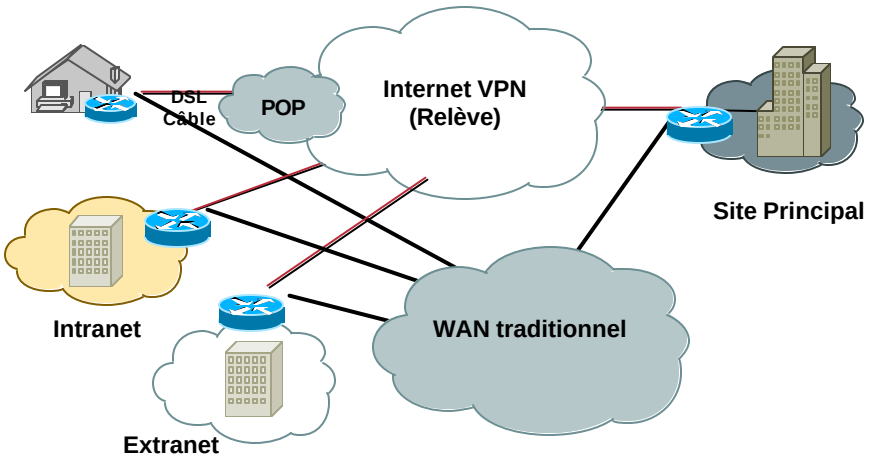
a) round trip passe de 195 ms avant a 90ms incluant encryption et transport. Avant impossible dans une fin de semaine de prendre un full backup du serveur (3 essais), aujourd'hui ca prend 4 heures - 4.5 heures encryption comprise. on fait un incrémental journalier en presque deux heures. Le temps réponse est beaucoup plus vite.

b) avant 1200$US portion us + 700$CDN portion Canada maintenant 1600$CDN bout a bout, contrat pris auprès de cie canadienne. L'avantage majeur n'est pas le prix mais la possibilité de prendre des backup sans intervention de personne. Le site est dans une région propice aux tempêtes et tornades, donc possibilité d'évacuations. En cas de catastrophe, très façile a relevé de n'importe ou dans des délais très courts.

c) JAMAIS eu de downtime a part deux maintenaces de 5 minutes prévues par le telco et dans un délai et conditions respectées. Temps d'installation beaucoup plus rapide qu'un point a point 2 semaine au lieu de 8 et avec le pix connection directe sur internet en floride donc plusrapide que de passer l'internet sur un lien dédié et de prendre l'internet ici.

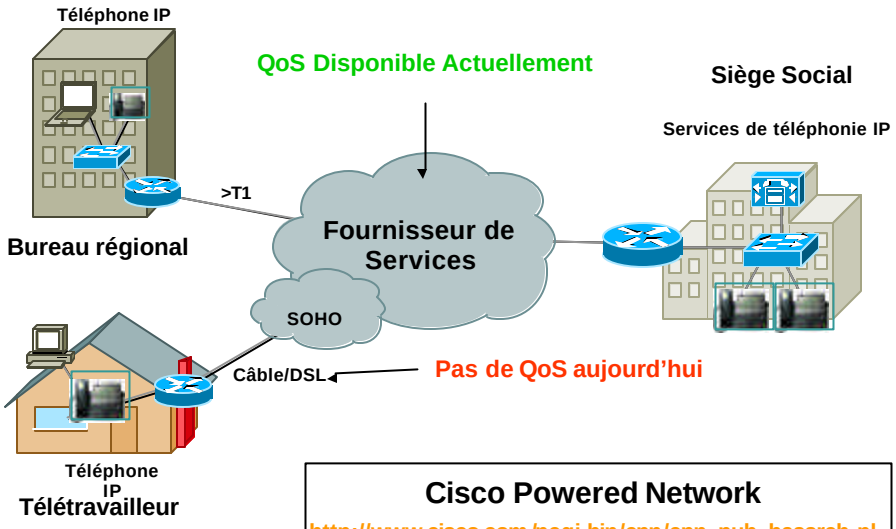
Relève du lien principal

Cisco.com



V³PN (VoIP/Video Enabled IPSec VPN)

Cisco.com



Cisco Powered Network

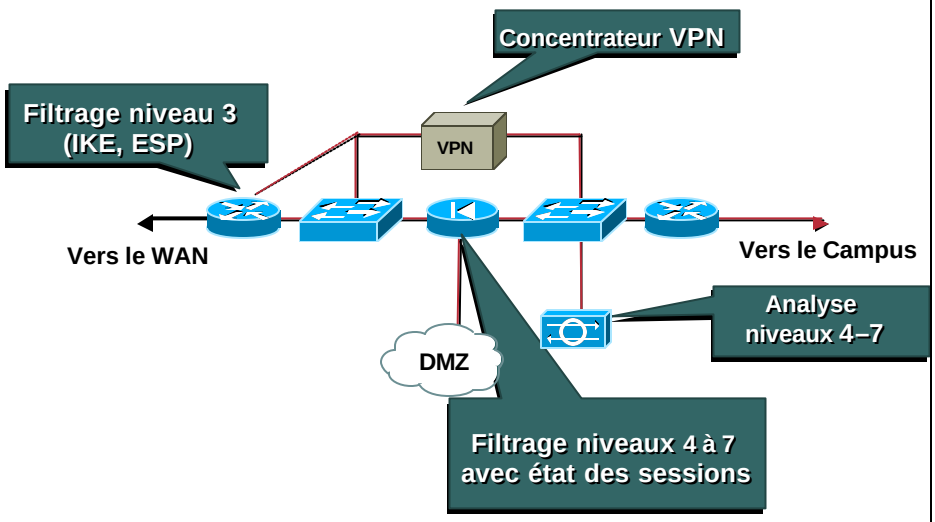
http://www.cisco.com/pcgi-bin/cpn/cpn_pub_bassrch.pl

Agenda

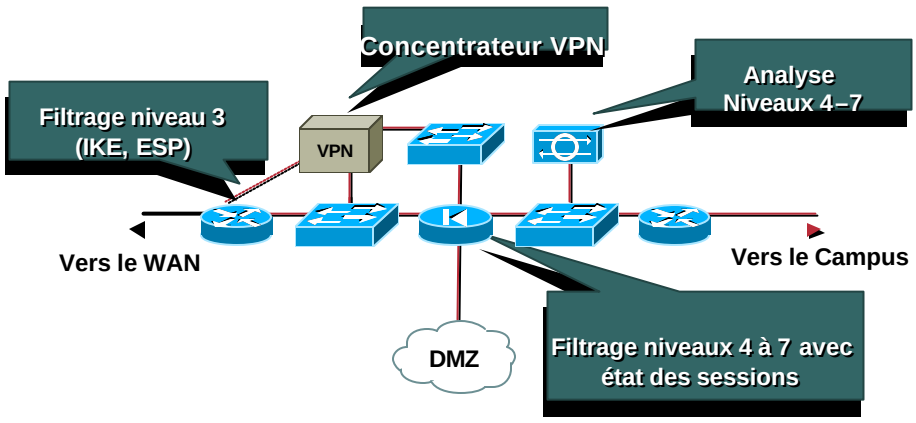
Cisco.com

- Applications
- Considérations lors du design
- VPN site à site
- Interaction avec d'autres technologies

Design Classique

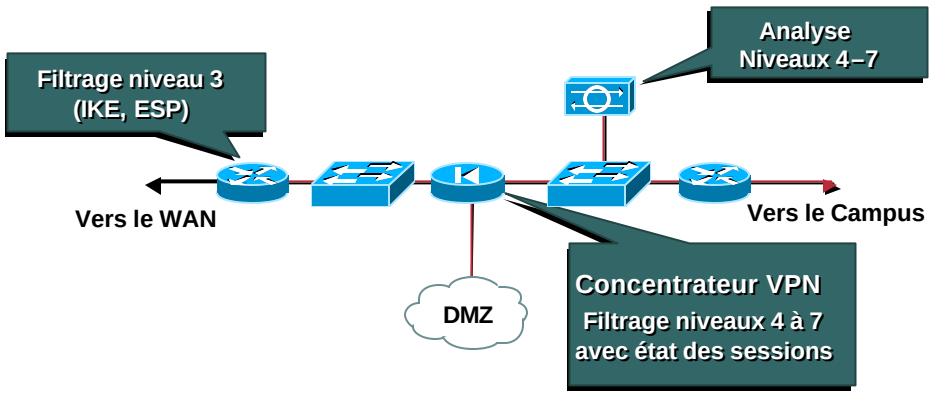


Concentrateur VPN sans pare-feu intégré



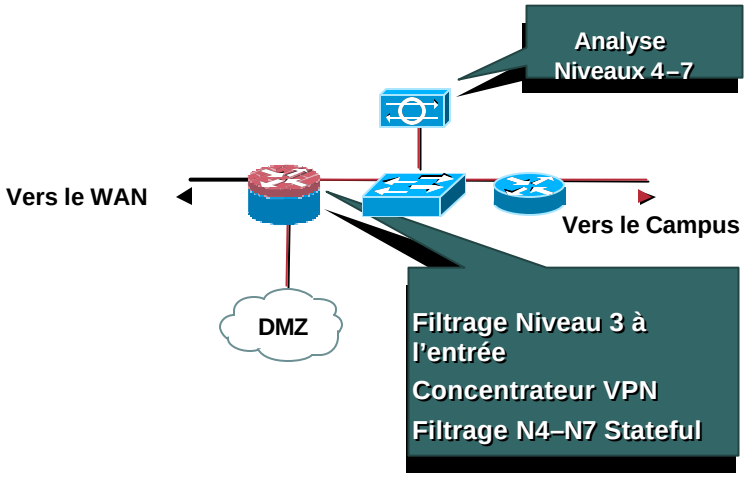
Pare-feu avec concentrateur VPN intégré

Cisco.com



VPN/Pare-feu intégré au Routeur

Cisco.com



Points à considérer lors du Design

Cisco.com

- Adressage IP
- Routage
- Sécurité
- Évolutivité
- QoS
- Gestion
- Migration
- Les composantes
- La politique de Sécurité
- Contrôle d'accès
- Haute disponibilité
- Performance
- Interopérabilité
- Authentification, autorisation, et la comptabilité
- Balancement de la charge

Le positionnement des composantes

Cisco.com

- Plan d'adressage IP
  - Les composantes VPN sont généralement placées à la frontière entre le réseau publique et privé
  - Les composantes qui terminent le VPN doivent avoir une adresse IP routable dans le réseau publique
  - Le NAT n'est pas forcément requis puisque les adresses internes sont maintenant cachées par IPSec
  - Les pare-feu et la politique de sécurité vont probablement avoir un impact.
- Routage
  - Il faut pouvoir router du trafic chiffré et non chiffré
  - Le routage dynamique est nécessaire pour les grands déploiements.

Le positionnement des composantes - II

Cisco.com

- **Sécurité**
  - **Comment ajuster les pare-feu et les règles de filtrage**
  - **Intranet vs Extranet**
- **Évolution**
  - **Les composantes doivent supportée l'augmentation de la charge**
  - **Composante multifonctions ou dédiée**
  - **Routage, robustesse, balancement de la charge et les options pour se relié au WAN**

Le positionnement des composantes - III

Cisco.com

- **QoS**
  - **Les paquets devraient maintenir l'étiquette de QoS en place et les composantes doivent pouvoir l'honorer**
- **Gestion**
  - **Composantes dédiées sont plus simple à dépanner vs nombre de composantes.**
  - **Plusieurs groupes peuvent être impliqués**

Agenda

Cisco.com

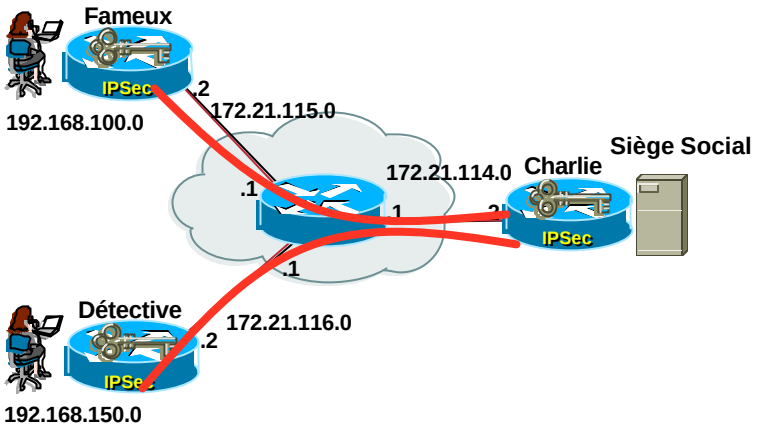
- Applications
- Considérations lors du design
- VPN site à site
- Interaction avec d'autres technologies

Qu'est ce qu'un Tunnel

Cisco.com

- Contrat entre deux parties sur une politique de sécurité incluant:
  - Algorithme de chiffrement
  - Algorithme d'authentification
  - Clefs partagées pour la session
  - Durée de vie des SA
  - Quelles données doivent être protégées (IPsec SAs seulement)
- Types de SAs
  - Bidirectionnel pour la gestion (IKE SA)
  - Unidirectionnel pour les données (IPsec SA)
  - 1 "Tunnel" = 1 IKE SA + 2 IPsec SAs

Topologie en étoile

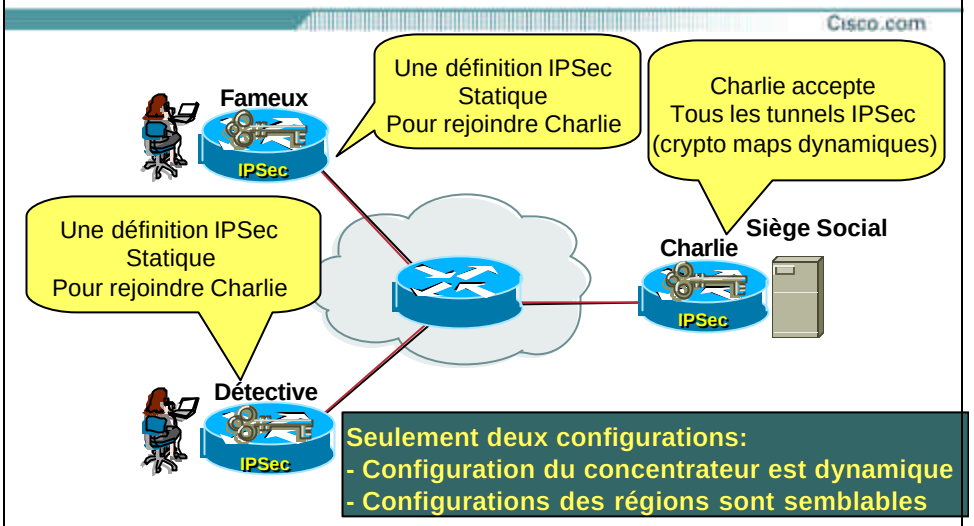


Topologie en étoile: Routeur Charlie Cfg 1


```
! Soyons courageux et entrons un
! crypto map par voisin
! ...
crypto map HQ 10 ipsec-isakmp
 set peer 172.21.115.2
 set transform-set encrypt-des
 match address 101

crypto map HQ 20 ipsec-isakmp
 set peer 172.21.116.2
 set transform-set encrypt-des
 match address 102
```


Topologie en étoile simplifiée



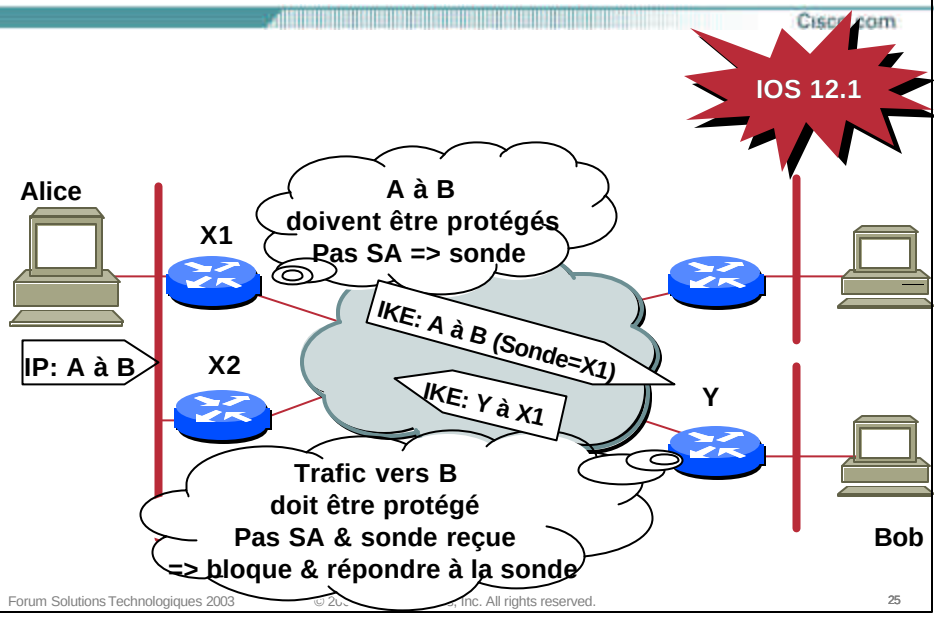
Topologie en étoile: Routeur Charlie– Cfg 2

Cisco.com

```
! Plaçons plutôt une commande unique de
! Dynamic crypto map
!
crypto map DYNAMIC 10 ipsec-isakmp dynamic TEMPLATE

! Template est utilisé pour définir: transforms, lifetime,
! Identities, ...
crypto dynamic-map TEMPLATE 10
     set transform-set ...
```

Tunnel Endpoint Discovery (TED)



TED – Configuration

```
! Template pour définir: transforms, lifetime,
! Identities, ...
crypto dynamic-map TEMPLATE 10
     set transform-set ...

crypto map TED 10 ipsec-isakmp dynamic TEMPLATE discover
```

TED a été déployé sur un réseau de 120 nœuds
Avec une interconnexion totale (Fully Mesh)

Limitations de TED

Cisco.com

- **Adressage**
  - **Comme la sonde utilise les adresses des composantes protégées (A, B), ces adresses doivent être routables.**
  - **TED n'est donc pas applicable pour du VPN sur Internet**
- **Déploiement**
  - **Tous les routeurs IPSec doivent avoir TED actif**
  - **Le déploiement sur tous les routeurs doit être réalisé simultanément ...**

IPSec *Passive* Mode

12.2(13)T

- **Le but est de simplifier les grands déploiements d'IPSec**
- **Sans "passive mode"**
  - **Tous les routeurs doivent avoir IPSec actifs au même moment**
  - **Pas de communications jusqu'à ce que les deux bouts du tunnel soient actifs**
- **Passive mode**
  - **Utilise IPSec lorsque les deux bouts ont activé IPSec**
  - **Utilise aucun chiffrement si un des bouts n'est pas configuré pour IPSec**

Fonctionnement de IPSec Passive Mode

Cisco.com

Routeur Transmet:

- IKE pour le trafic à chiffrer

  S'il y a une réponse, le tunnel est établi comme d'habitude

  S'il n'y a pas de réponse (après délai):

  + Création d'un "passive SA": SA normal, avec une bit "passive"
    Pas de chiffrement! Durée de vie très courte pour ce SA

Routeur qui reçoit:

- Répond à IKE et établi le tunnel
- Paquets chiffrés: Tout est normal
- Paquets non chiffrés: Transmet, ne pas "droppé"
  - Même si un SA (pour les Peers redondant)

(bleu pour le changement de comportement)

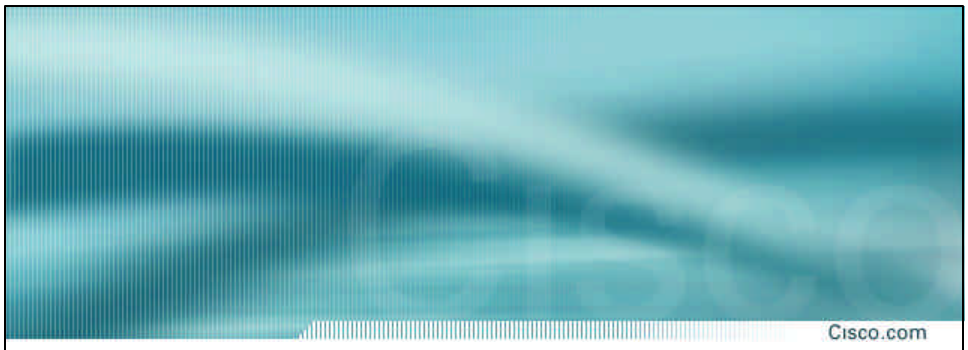
Passive IPSec: CLI

Cisco.com

- IPSec Passive n'est pas actif par défaut !
- Commandes Globales :

```
crypto ipsec optional
crypto ipsec optional retry Secondes
```

- Par défaut, le routeur va essayer aux 5 minutes de chiffrer la session

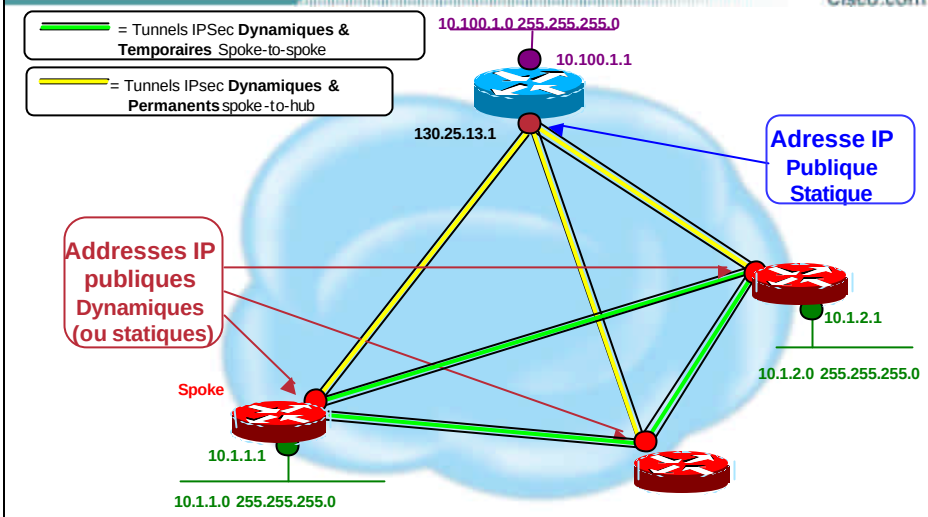


Dynamique Multipoint VPN DMVPN

VPNs avec IPSec

- Topologie en étoile
  - + Tout le trafic doit passer par le site central
  - + Facile à déployer
  - × Deux chiffrements
  - × Besoin de plus de bande passante vers le site central
  - × Peut donner des configurations très longues…
- Interconnexion complète (Full Mesh)
  - + Communication directe entre les régions
  - × Petits routeurs n'ont pas les ressources pour maintenir les connexions
  - × Ajout d'un site = beaucoup de planification
  - × Un casse-tête d'évolution, donc la plupart des entreprises utilisent une topologie en étoile

Dynamique Multipoint VPN - DMVPN



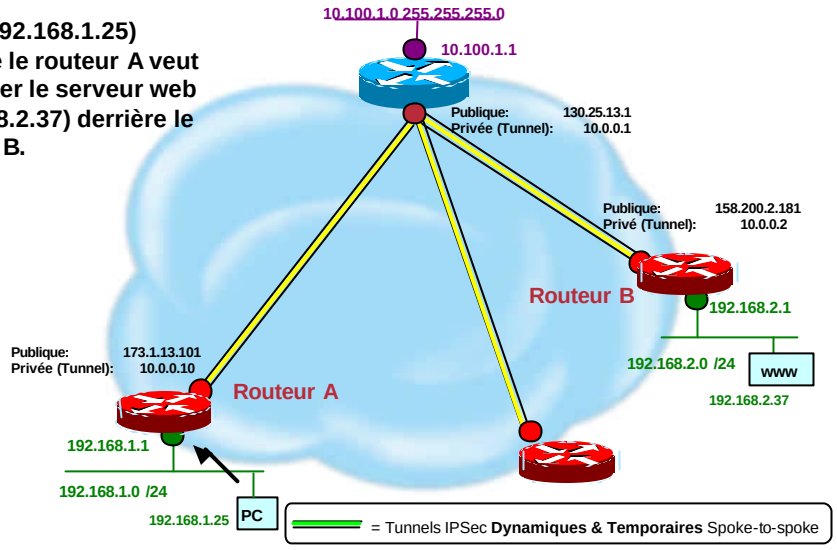
DMVPN – Comment ça marche

- Basé sur deux technologies
  - –NHRP – Next Hop Resolution Protocol
    - Client/serveur: Site central est le serveur; Régions sont clients
    - Site central maintien la BD (NHRP) pour toutes les adresses publiques des régions
      - – Chaque région enregistre son adresse publique au démarrage
      - – Régions demandent à la BD NHRP pour l'adresse publique de la destination pour établir le tunnels
  - –Interface Tunnel Multipoint GRE (mGRE) – RFC2547
    - Permet à une interface GRE de supporter plusieurs tunnels IPSec

Dynamique Multipoint VPN - Exemple

Cisco.com

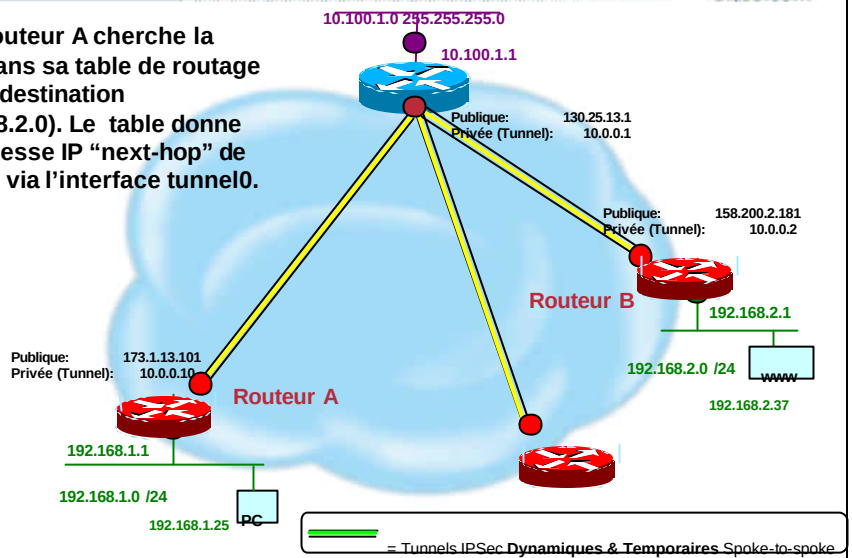
1. PC (192.168.1.25) derrière le routeur A veut contacter le serveur web (192.168.2.37) derrière le routeur B.



Dynamique Multipoint VPN - Exemple

Cisco.com

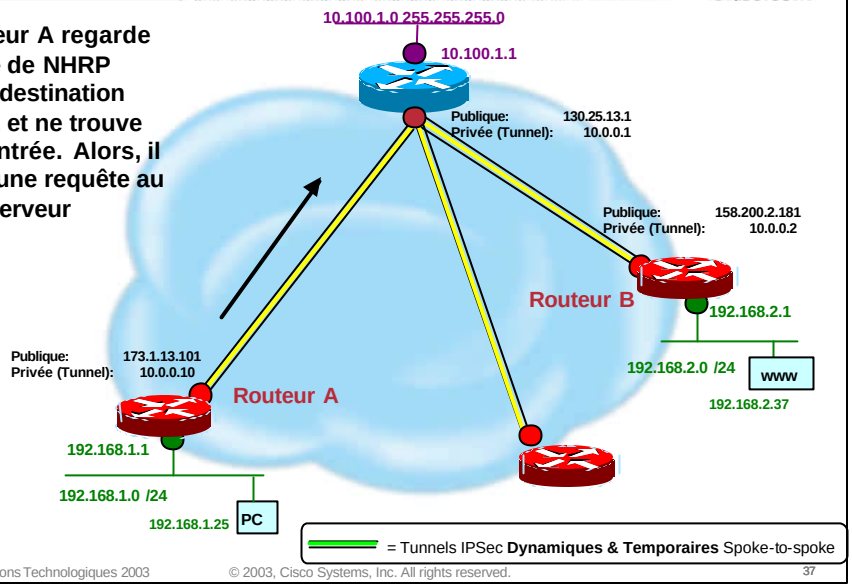
2. Le routeur A cherche la route dans sa table de routage pour la destination (192.168.2.0). Le table donne une adresse IP "next-hop" de 10.0.0.2 via l'interface tunnel0.



Dynamique Multipoint VPN - Exemple

Cisco.com

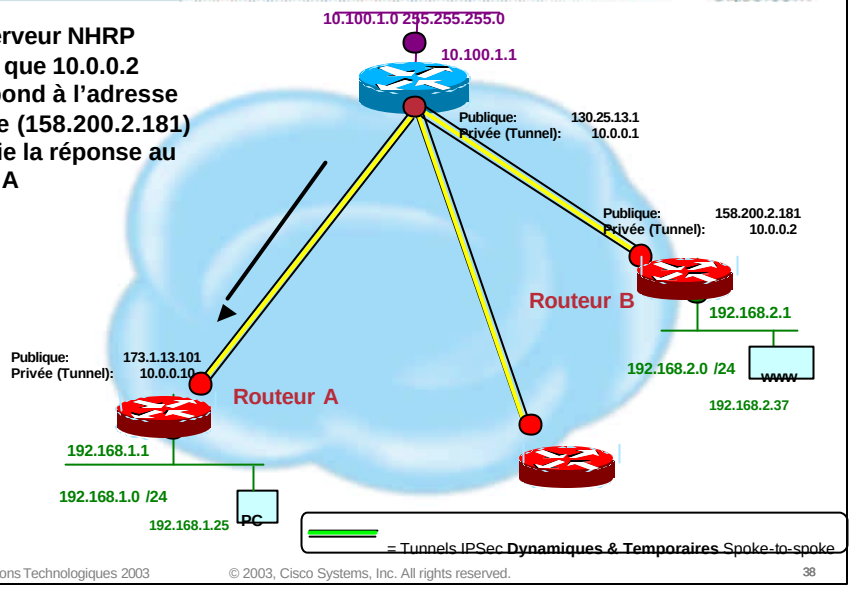
3. Routeur A regarde sa table de NHRP pour la destination 10.0.0.2 et ne trouve pas d'entrée. Alors, il envoie une requête au NHRP serveur



Dynamique Multipoint VPN - Exemple

Cisco.com

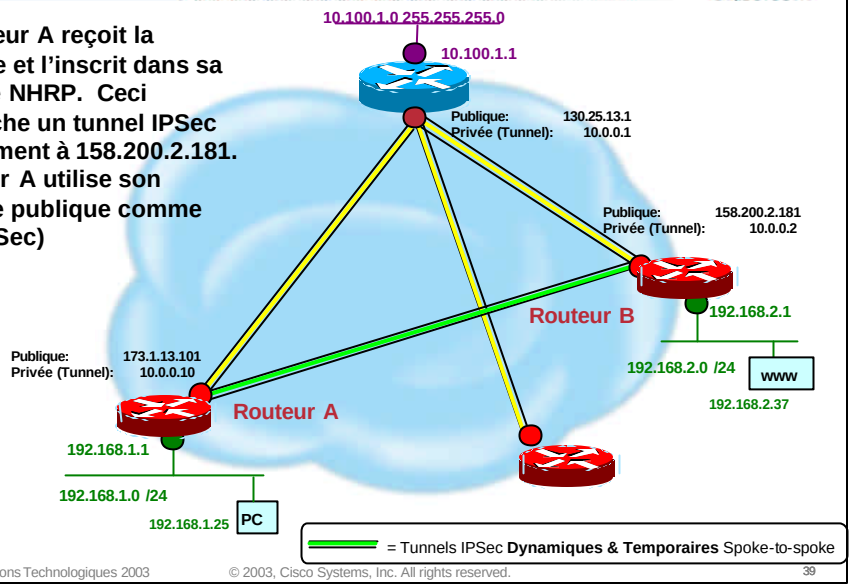
4. Le Serveur NHRP indique que 10.0.0.2 correspond à l'adresse publique (158.200.2.181) et envoie la réponse au routeur A



Dynamique Multipoint VPN - Exemple

Cisco.com

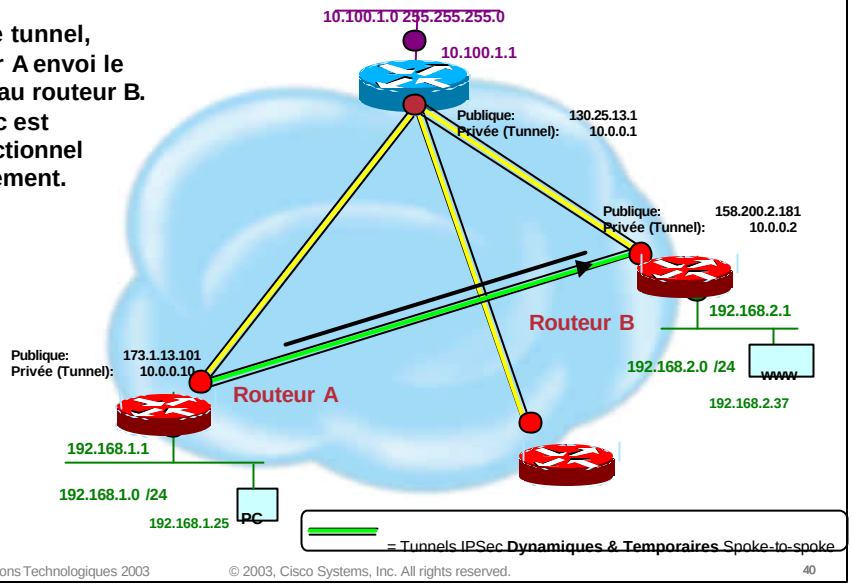
5. Routeur A reçoit la réponse et l'inscrit dans sa table de NHRP. Ceci déclanche un tunnel IPSec directement à 158.200.2.181. (Routeur A utilise son adresse publique comme peer IPSec)



Dynamique Multipoint VPN - Exemple

Cisco.com

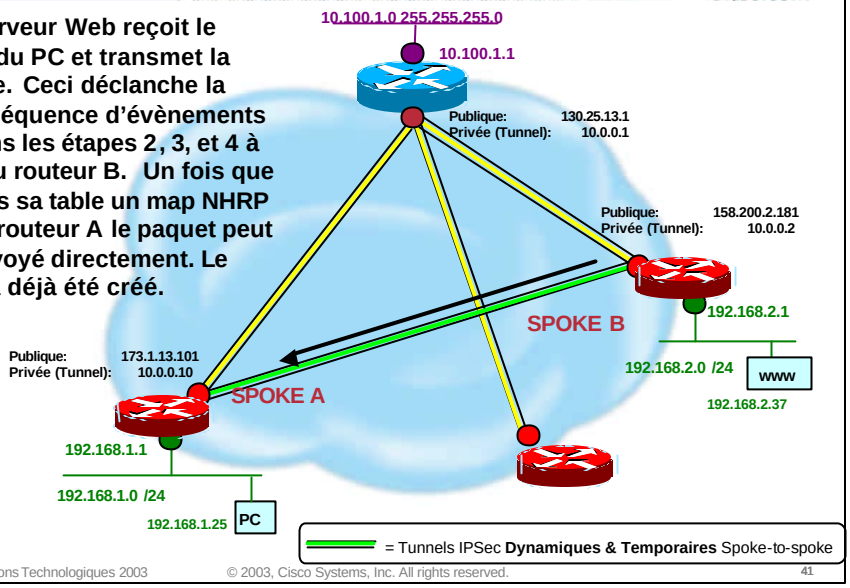
6. Par le tunnel, Routeur A envoi le paquet au routeur B. Le trafic est unidirectionnel actuellement.



Dynamique Multipoint VPN - Exemple

Cisco.com

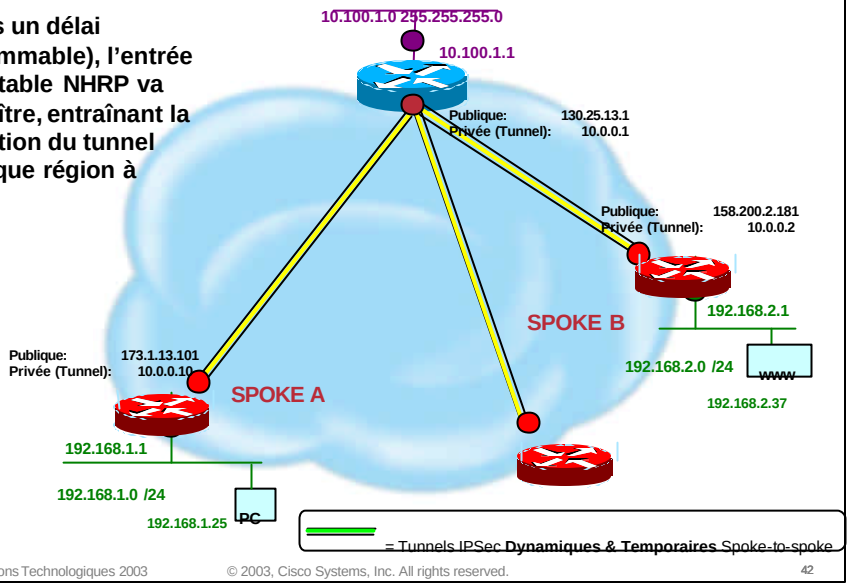
7. Le serveur Web reçoit le paquet du PC et transmet la réponse. Ceci déclanche la même séquence d'évènements que dans les étapes 2, 3, et 4 à partir du routeur B. Un fois que B à dans sa table un map NHRP pour le routeur A le paquet peut être envoyé directement. Le tunnel a déjà été créé.



Dynamique Multipoint VPN - Exemple

Cisco.com

8. Après un délai (programmable), l'entrée dans la table NHRP va disparaître, entraînant la destruction du tunnel dynamique région à région.



Configuration – Site Central

Cisco.com

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto IPsec transform-set trans2 esp-des esp-md5-hmac
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
```


Configuration – Site Central – suite

Cisco.com

```
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1416
 ip nhrp authentication donttell
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

Configuration – Site Central – Suite.

Cisco.com

```
interface Ethernet0
 ip address 130.25.13.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!
```

Pas de configuration particulière pour les Régions!!!

Configuration – Régions

Cisco.com

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto IPsec transform-set trans2 esp-des esp-md5-hmac
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
```

Configuration – Régions – Suite

Cisco.com

```
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.3 255.255.255.0
 ip mtu 1416
 ip nhrp authentication donttell
 ip nhrp map 10.0.0.1 130.25.13.1
 ip nhrp network-id 99
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```


Configuration – Régions – Suite

Cisco.com

```
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
```

Toutes les régions possèdent la même configuration à l'exemption des adresses sur l'interface du tunnel et celle du réseau local.

Recommandations

Cisco.com

- Certificats/PKI

  Si vous utilisez des clef partagées et que la clef est compromise, il faut changer les clefs dans tous les régions.
- L'authentification avec NHRP
  - NHRP Network ID et mot de passe
  - mGRE Network ID
- Ces paramètres sont transmis par le tunnel IPSec entre le site central et les régions et sont chiffrés
- Il est possible de configurer plusieurs serveurs NHRP sur plusieurs sites centraux pour la redondance

Plateformes et version d'IOS

Cisco.com

- 12.2(15)T

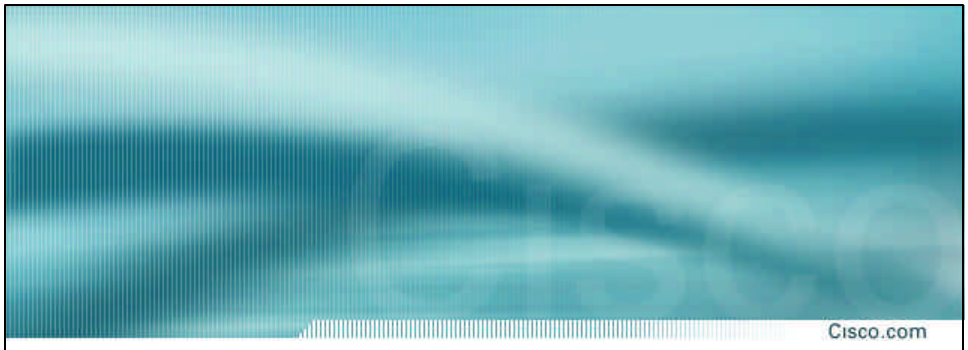
  7200, 37xx, 36xx, 26xx, 17xx
- 12.2.(13)ZG

  Pour les 831, 836 et 837

www.cisco.com/go/fn

Agenda

- Applications
- Considérations lors du design
- VPN site à site
- **Interaction avec d'autres technologies**
  - **Fragmentation des paquets IP**
  - **Path MTU Discovery**
  - **Impact de GRE**
  - **Impact de IPSec**
  - **Impact de GRE et IPSec**
  - **Impact de IPSec sur la QoS**



Fragmentation des paquets IP

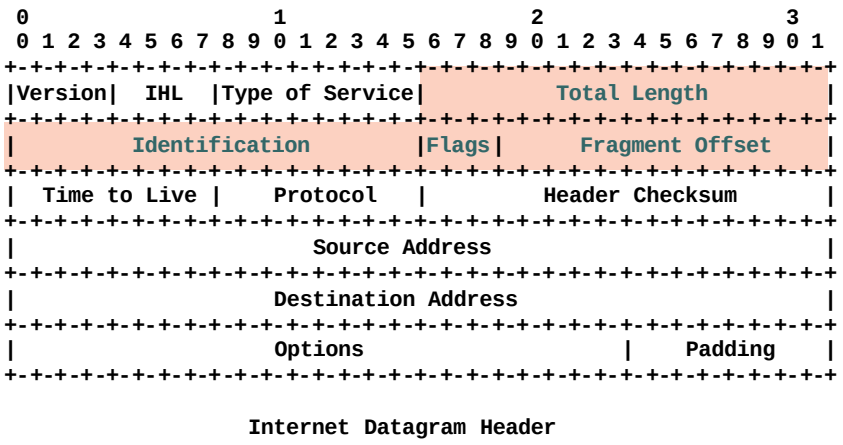
Grosseur d’un paquet IP

Cisco.com

- Un paquet IP peut avoir 65536 octets
- Les couches 1 et 2 offrent normalement une grandeur limite aux trames
  - MTU: Maximum Transmission Unit
  - Habituellement, 1500 octets pour Ethernet
- Les hôtes ou les routeurs doivent fragmenter lorsque la trame IP est plus grande que le MTU
- Les fragments sont transmis comme des paquets IP (routage, fragmentation additionnelle, etc..)

Un paquet IP

Cisco.com



Internet Datagram Header

Les champs d'un paquet fragmenté

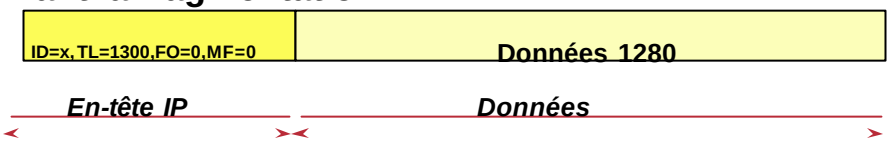
Cisco.com

- Tous les fragments conservent le champ *identification* original
- Les fragments sont identifié par un *fragment offset*
- *Flags* peut contenir:
  - MF: D'autres Fragments (More Fragments)
  - DF: Ne pas fragmenter (Do not Fragment)

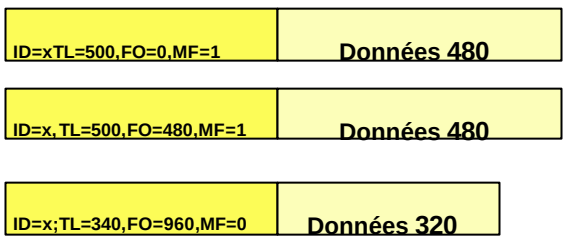
Fragmentation IP

Cisco.com

Avant la fragmentation:



Après la fragmentation (MTU = 500):



Pour reconstruire la trame

Cisco.com

- *L'hôte de Destination reconstruite la trame en se basant sur*
  - Adresse IP de Source
  - Le champ "identification"
  - Les Fragments
  - MF flags
- Les routeurs ne devraient jamais reconstruire une trame sauf s'ils sont la destination
- Fragments perdu = Perte complète de la trame IP

Impact de la Fragmentation

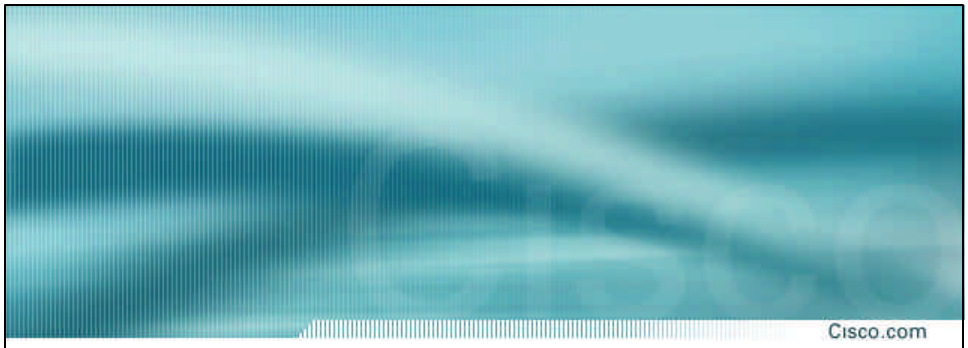
Cisco.com

- La fragmentation doit être évitée à tout prix:
  - Augmente le nombre de paquets perdus
  - Consommation du CPU des hôtes
- Certains produits (PAT boxes) sont incapables de fonctionner avec des fragments
  - ➔ La communication ne fonctionne simplement pas
- Les Routeurs perdent leur efficacité
  - Ils doivent allouer des gros bloques de mémoire
  - Toujours "process-switched"

Qui Fragmente?

Cisco.com

- **Actuellement, c'est plutôt commun:**
  - **ADSL avec PPPoE offre un MTU de 1492 octets**
  - **MPLS over Ethernet réduit aussi le MTU**



Path MTU Discovery (PMTUD)

Path MTU Discovery (PMTUD)

Cisco.com

- Path MTU Discovery essai de mesurer le plus petit MTU disponible et la source va pouvoir ajuster la grosseur de ses paquets
- PMTUD est principalement utilisé par TCP

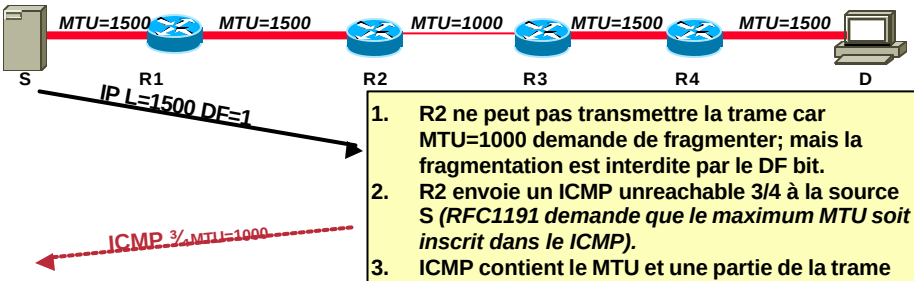
Path MTU Discovery/1

Cisco.com

- Selon le RFC 1191
- Le plus petit MTU est 1000 octets ⇒ S ne devrait pas envoyer de trame IP de plus de 1000 octets
- Pour découvrir le plus petit MTU, S et D vont envoyer des trames IP selon leur MTU avec le DF bit initialisé

Path MTU Discovery/2

Cisco.com



1. R2 ne peut pas transmettre la trame car MTU=1000 demande de fragmenter; mais la fragmentation est interdite par le DF bit.
2. R2 envoie un ICMP unreachable 3/4 à la source S *(RFC1191 demande que le maximum MTU soit inscrit dans le ICMP).*
3. ICMP contient le MTU et une partie de la trame

1. A la réception du ICMP unreachable, S met à jour une table interne
2. S transmet seulement des trames <= 1000 à D

Les problèmes avec PMTUD

Cisco.com

- **PMTUD utilise une signalisation négative:**
  - **Pas de nouvelle, bonne nouvelle**
- **Mais, les ICMP sont:**
  - **Bloqués par les pare-feu ou les règles de sécurité indésirables (devraient permettre ICMP code 3 type 4 en entrée)**
  - **Ignoré par certain système de balancement de charge**
    - **(LD et WebNS 4.1 sont OK)**

Solution: TCP MSS

Cisco.com

- TCP MSS (Maximum Segment Size) = maximum TCP payload
- Hôtes envoient leurs MSS dans le SYN
- MSS peut être configuré à MSS+40 <= plus petit MTU pour éviter la fragmentation.
- *Fonctionne seulement pour TCP*
- IOS (avec CSCds69577 à partir de 12.2(4)T fonctionne pour les SYN en entrée et en sortie)

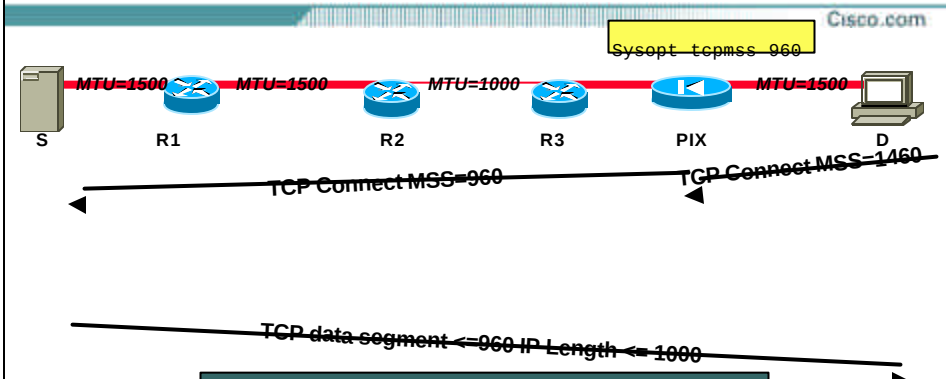
```
ip tcp adjust-mss 1400
```

- PIX

```
sysopt tcpmss 1400
```


Effet de réduire le MSS

Cisco.com



1. S n'envoie pas de trame IP > 1000 octets
2. Pas de fragmentation
3. Même si S utilise PMTUD, comme il n'y a pas de fragmentation, nous n'avons pas besoin de générer des ICMPs

Solution: Initialiser à zéro le DF bit

Cisco.com

- Dans IOS 12.1(6), policy based routing peut être utilisé pour initialiser à zéro le DF bit
- CPU va augmenter (Fragmentation et PBR)

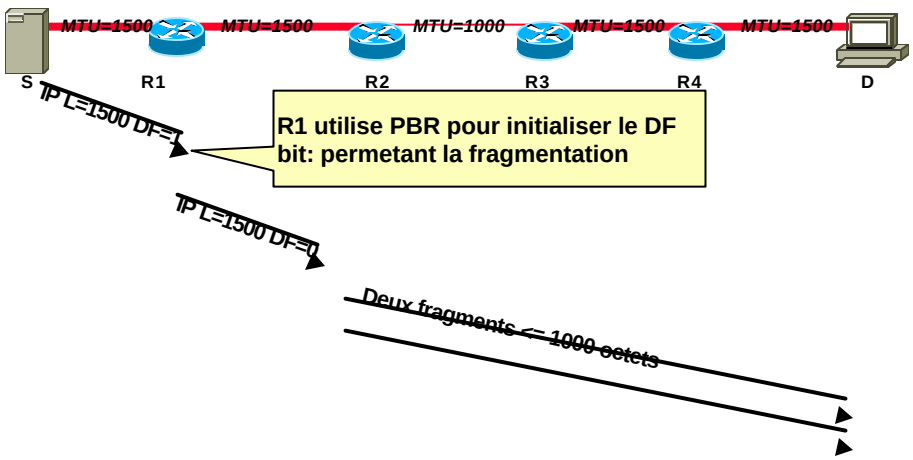
```
interface serial0
  ...
  ip policy route-map clear-df-bit

route-map clear-df-bit permit 10
  match ip address 111
  set ip df 0

access-list 111 permit tcp any any
```


Initialiser à zéro le DF bit

Cisco.com



Cisco.com

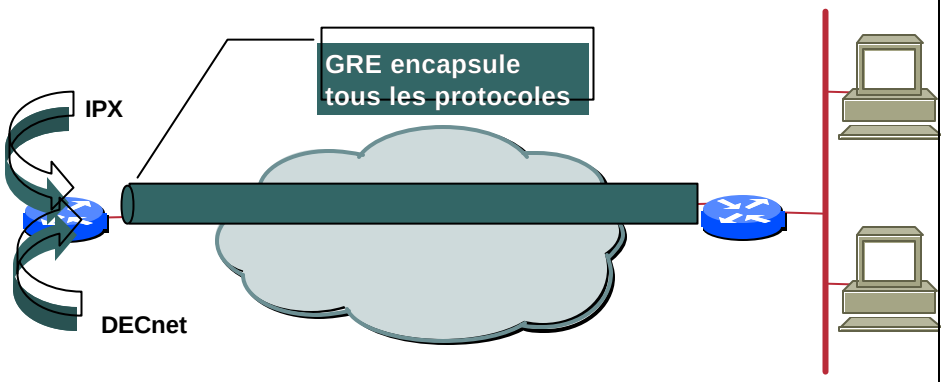
Impact de GRE

Generic Routing Encapsulation (GRE)

Cisco.com

GRE RFC 2784 *(standard: Cisco, Procket, Juniper Obsoletes RFC 1701)*
encapsules tous les protocoles dans IP

Dans l'IOS, le tunnel GRE est une interface (avec son propre MTU)



Encapsulation GRE

Cisco.com

Trame IP Initiale *(avant transmission)*

Encapsulation GRE *(après transmission dans un tunnel GRE)*

Paquet GRE avec en-tête: protocol 47 *(avec la nouvelle adresse de destination)*

GRE MTU

Cisco.com

- **Le MTU de l'interface tunnel GRE est par défaut le MTU de l'interface physique – 24 octets**

  Pour *Ethernet* le MTU de GRE est 1476 octets

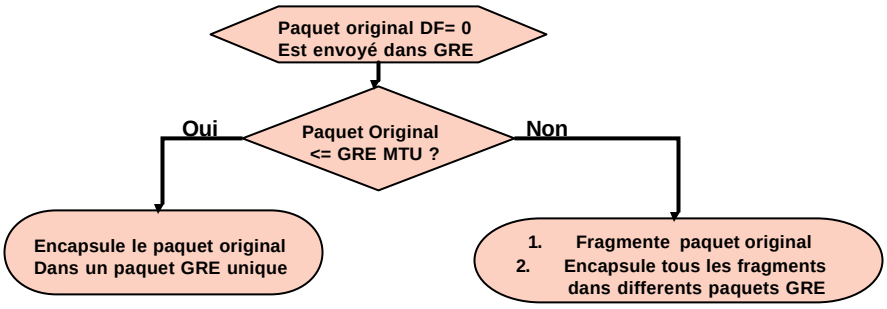
```
#show ip interface tunnel 0
Tunnel0 is up, line protocol is up
  …
  MTU is 1476 octets
```

- **Par défaut le DF bit de GRE est initialisé à 0**
- **Il est possible de changer le MTU de l'interface tunnel GRE avec la commande**

  `ip mtu …`

GRE et la fragmentation

Cisco.com

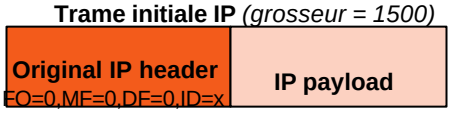


Encapsulation GRE avec Fragmentation /1

Cisco.com

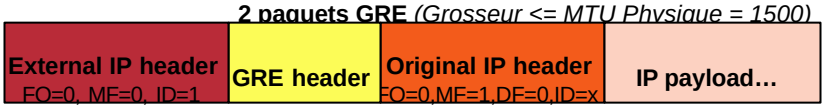
Par défaut:
MTU du tunnel GRE est de 1476
=> La trame initiale est fragmentée

Trame initiale IP *(grosseur = 1500)*



20 octets 1480 octets

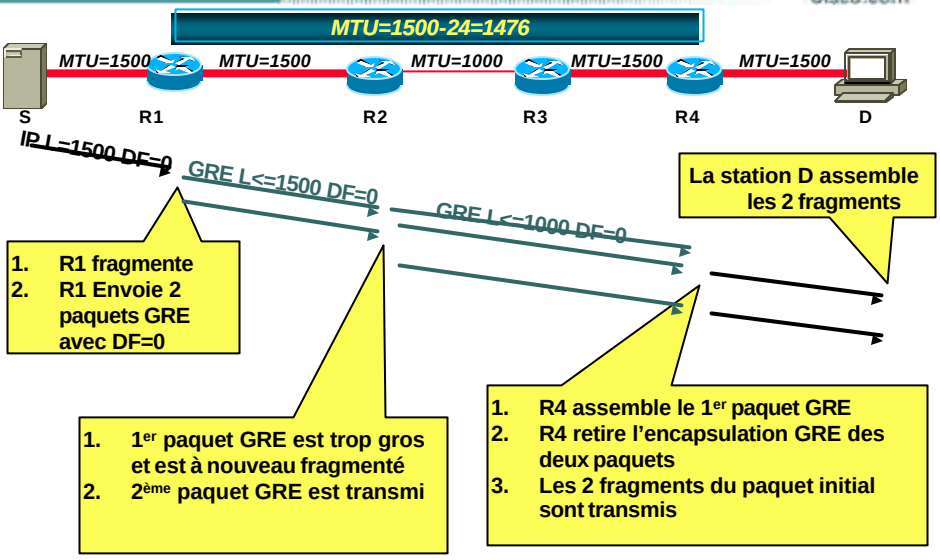
2 paquets GRE *(Grosseur <= MTU Physique = 1500)*



20 octets 4 octets 20 octets 1456 octets

20 octets 4 octets 20 octets 24 octets

Encapsulation GRE avec Fragmentation /2

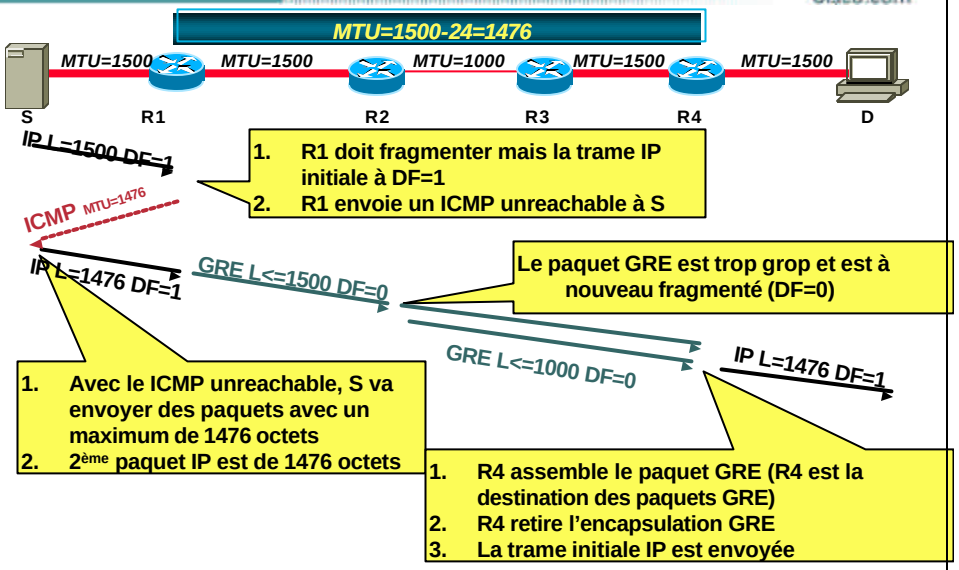


Encapsulation GRE avec Fragmentation /3 Conclusion lorsque le DF=0

Cisco.com

- **Tout fonctionne**
- **Mais, il y a 2 fragmentations**
  - **A l'entrée du tunnel**
  - **Dans le tunnel**

Encapsulation GRE avec Fragmentation /4 DF=1 (le cas des stations qui font PMTUD)



Encapsulation GRE avec Fragmentation /5 Conclusion lorsque le DF=1 (ou PMTUD)

Cisco.com

- **Tout fonctionne: les données passent**
  - **Si et seulement si les ICMPs ne sont pas filtrés**
- **Mais, il y a encore une fragmentation**
  - **Les paquets GRE ont DF=0 par défaut**

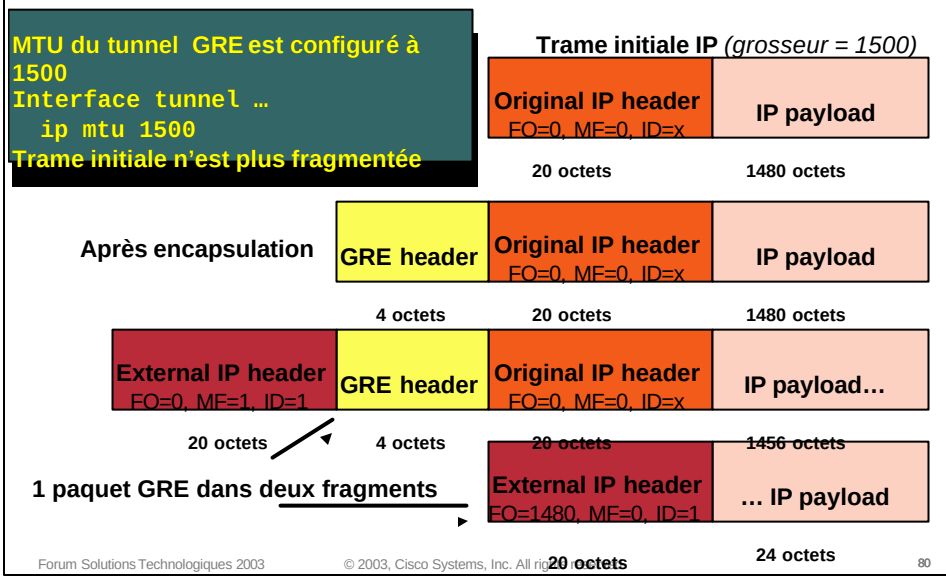
Solution: GRE MTU = 1500

Cisco.com

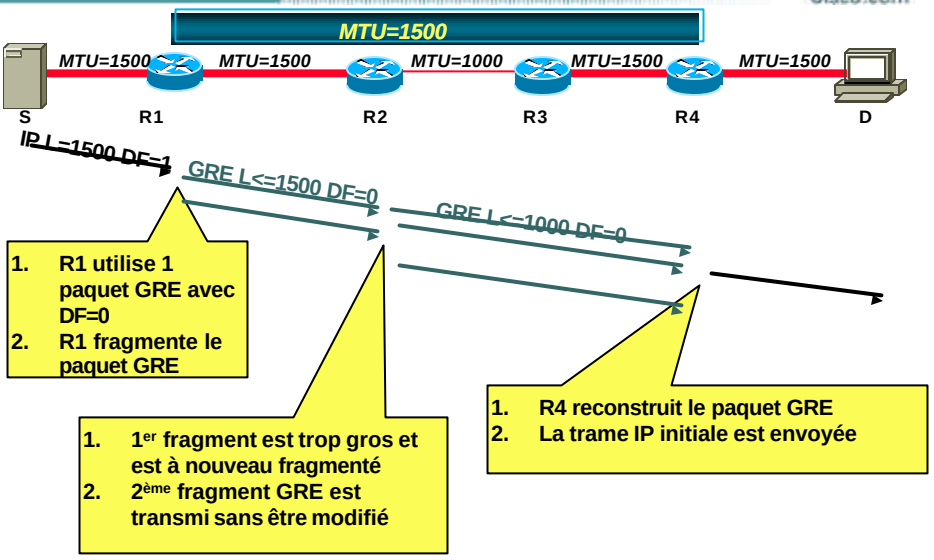
- **Configuration manuelle du MTU de l'interface GRE à 1500**
  - **Plus de fragmentation avant l'encapsulation GRE (pas de paquet ICMP envoyé)**
  - **Le paquet GRE à DF=0 et peut être fragmenté**

Encapsulation GRE avec Fragmentation /6

Cisco.com



PMTUD avec MTU de l'interface GRE=1500



PMTUD avec MTU de l'interface GRE=1500 Conclusion

Cisco.com

- **Plus de fragmentation avant l'encapsulation GRE**
  - **Le paquet GRE est fragmenté**
  - **Fonctionne même si les ICMP sont filtrés**

PMTUD dans tunnel GRE

Cisco.com

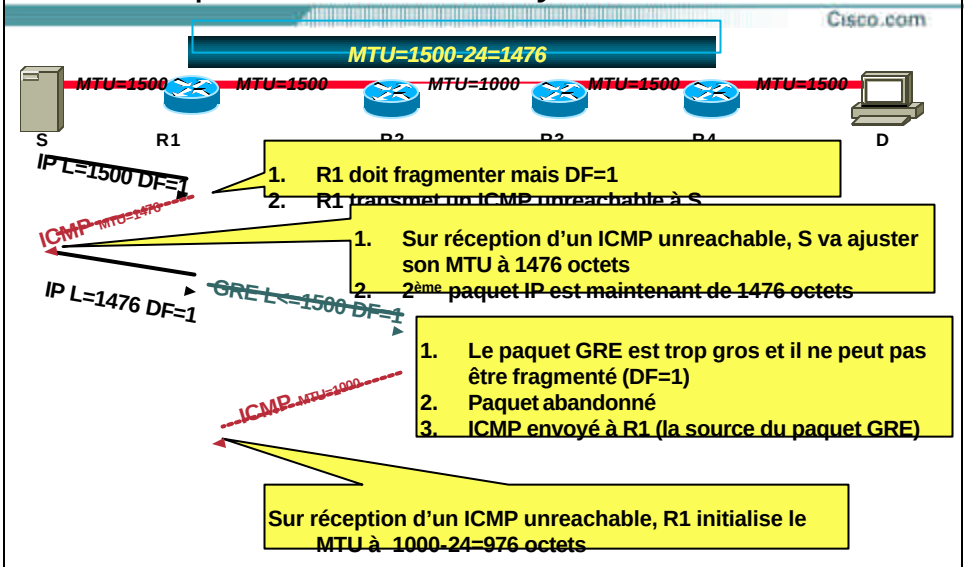
- **Depuis 12.0(5)T (mais pas documentée!)**

```
tunnel path-mtu-discovery
```

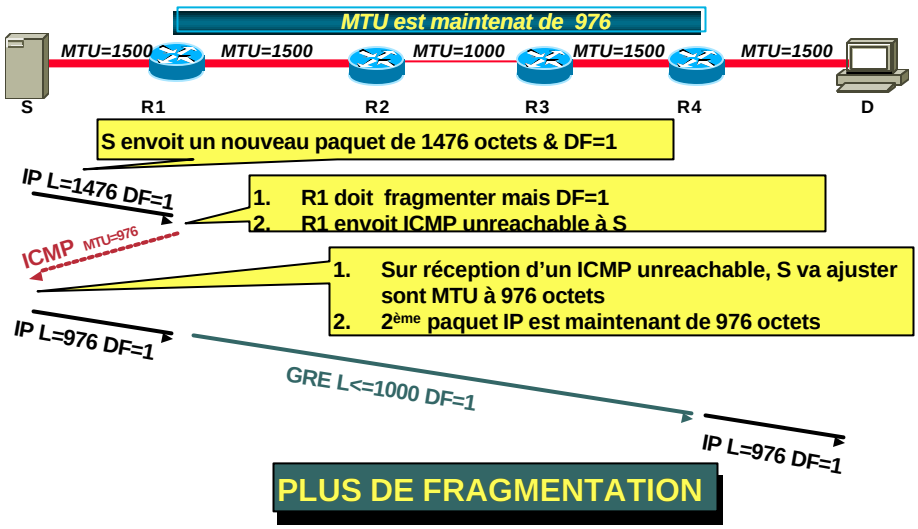
- **Changements**
  1. **Le DF bit est copié du paquet initial dans l'en-tête GRE**
  2. **Routeurs avec interface GRE écoutent pour les ICMPs unreachable**
  3. **Lorsqu'un routeur reçoit un ICMP unreachable, le MTU du tunnel GRE est mis à jour dynamiquement**

Tunnel path-mtu-discovery */1*

Cisco.com



Tunnel path-mtu-discovery */2*



Tunnel path-mtu-discovery */2*

```
show interface tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Description: Virtual interface to router C
  Internet address is 192.168.100.2/30
  MTU 1514 octets, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 194.194.194.1, destination 193.193.193.1
  Tunnel protocol/transport GRE/IP, key disabled,
  Checksumming of paquets disabled,  fast tunneling enabled
  Path MTU Discovery, ager 10 mins, MTU 976, expires 00:09:36
```

LE PMTUD tel que mise-à-jour par ICMP

Tunnel path-mtu-discovery: conclusion

Cisco.com

- **Avec `tunnel path-mtu-discovery`**
  - **Le MTU dans les tunnels GRE est appris dynamiquement**
  - **Plus de fragmentation**
  - **Un paquet IP est perdu**
  - **Les messages ICMP doivent être reçus par S et R1**
- **Sans `tunnel path-mtu-discovery`**

  Il est possible d'utiliser `ip mtu` pour initialiser l'interface au plus petit MTU sur le chemin – 24 octets

IPinIP: RFC 2003

Cisco.com

- **IPinIP est très proche de GRE**
- **IPinIP est utilisé par IPSec en mode tunnel**
- **Tous ce que nous venons de décrire pour GRE fonctionne pour IPinIP**

IPinIP Encapsulation

Cisco.com

IPinIP est défini dans le RFC2003
Utilise le protocole 4
Fonctionne seulement pour IP
Utilisé par IPsec en mode tunnel
Presque identique à GRE dans IOS

Trame IP Initiale

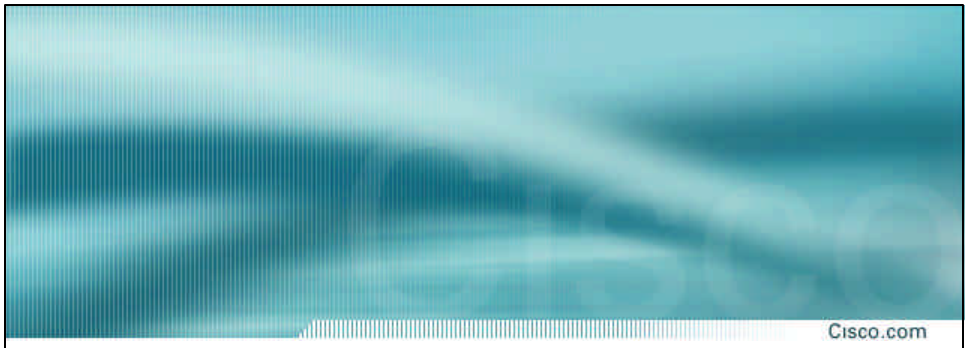
20 octets

Encapsulation IPinIP *(après le passage dans le tunnel)*

20 octets

Paquet IPinIP avec en-tête IP: protocol 4 *(avec la nouvelle adresse de destination)*

20 octets 20 octets



Impact de IPSec

IPSec

Cisco.com

IPSec RFC 2401 (et plusieurs autresRFC) encapsule IP dans des paquets chiffrés

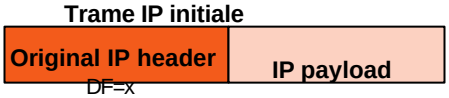
Avec l'IOS, le tunnel IPSec n'est pas un interface

Encapsulation IPSec en Mode Tunnel

Cisco.com

Par défaut:
DF bit est copié dans l'en-tête IP externe

Trame IP initiale



DF=x

20 octets

Encapsulation IPSec ESP

16 octets 20 octets 2-10 octets

Paquet IPSec avec une nouvelle en-tête IP

DF=x

20 octets 16 octets 20 octets 2-10 octets

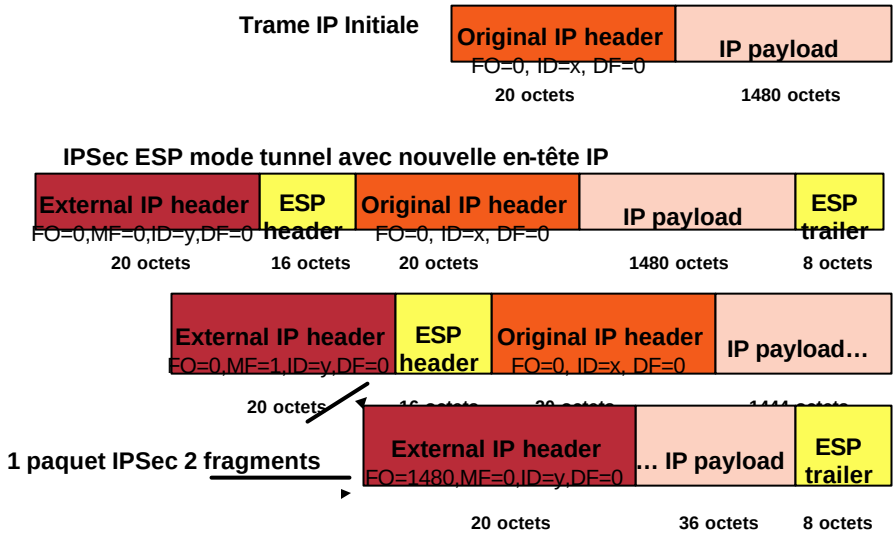
Différence entre GRE et IPSec mode Tunnel

Cisco.com

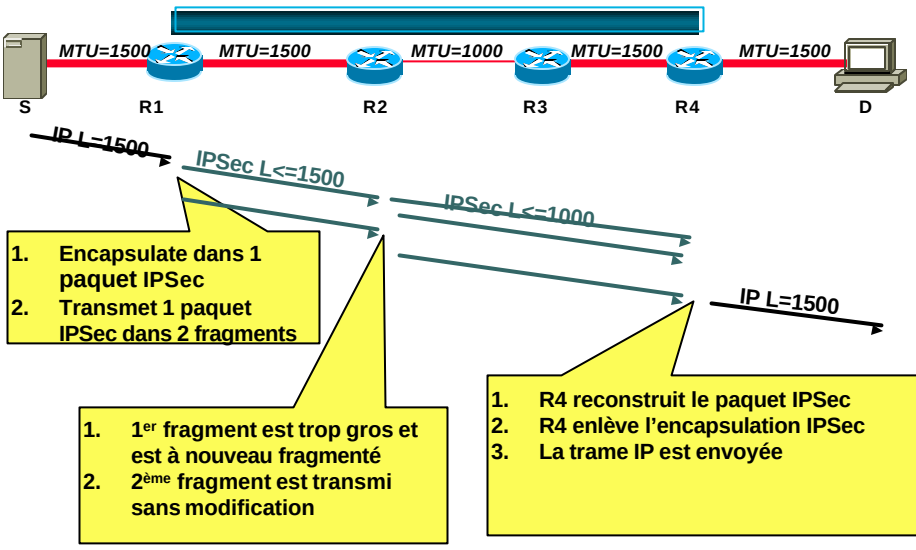
- **GRE fragmente avant l'encapsulation**
- **IPSec Mode Tunnel fragmente après l'encapsulation** *(sauf avec look-ahead)*

IPSec en Mode Tunnel et la Fragmentation

Cisco.com



IP fragmentation & IPSec



Performance IPSec avec Fragmentation

- **Si le paquet IPSec est fragmenté**

  Routeur qui termine le tunnel doit re-construire le paquet

  Baisse de performance de 50 à 90%

- **Si nous utilisons look-ahead (défaut)**

  Les paquets sont fragmentés avant d'entrer dans le tunnel, plus de paquets IPSec fragmentés

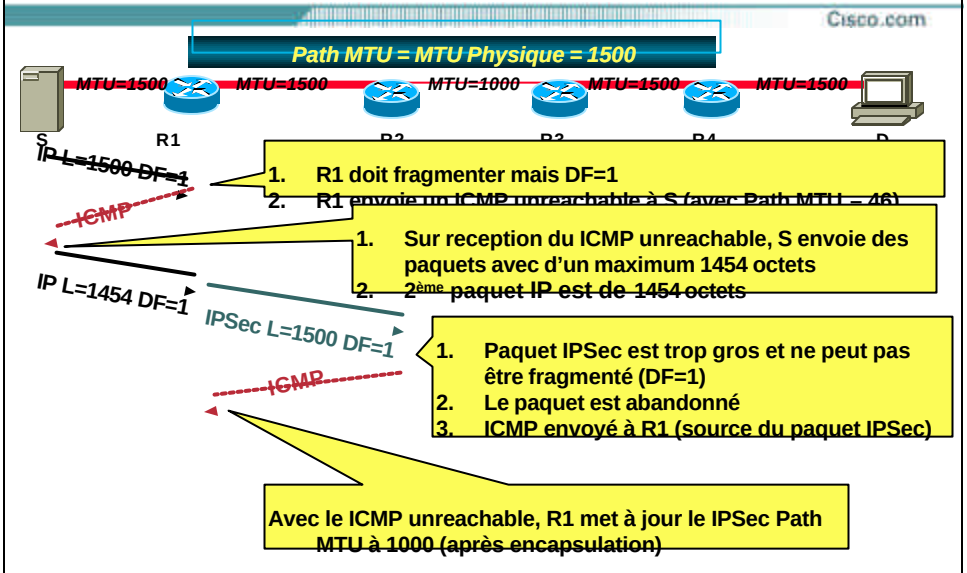
IPSec et PMTUD

Cisco.com

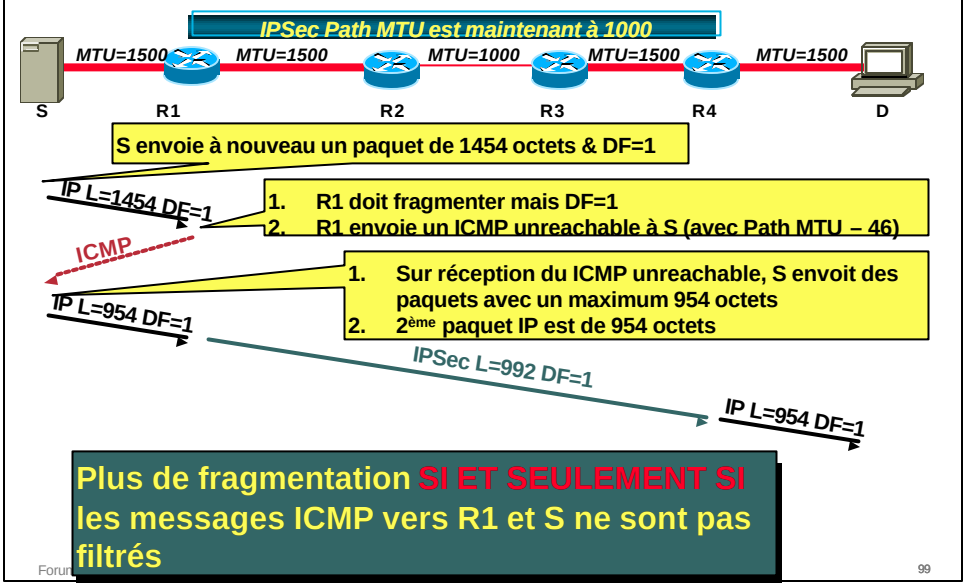
- **Encapsulation IPSec copie le DF bit dans l'en-tête externe (Selon le RFC 2401)**
- **IPSec suit l'état du path MTU du tunnel**
  - **Initialisé en rapport au MTU physique**
  - **Le MTU avant la fragmentation est le MTU physique– 46** *(20 IP externe, 16 l'en-tête ESP, max 10 pour le ESP trailer)*
  - **Mis à jour dynamiquement avec des ICMP unreachable**

PMTUD et IPSec/1

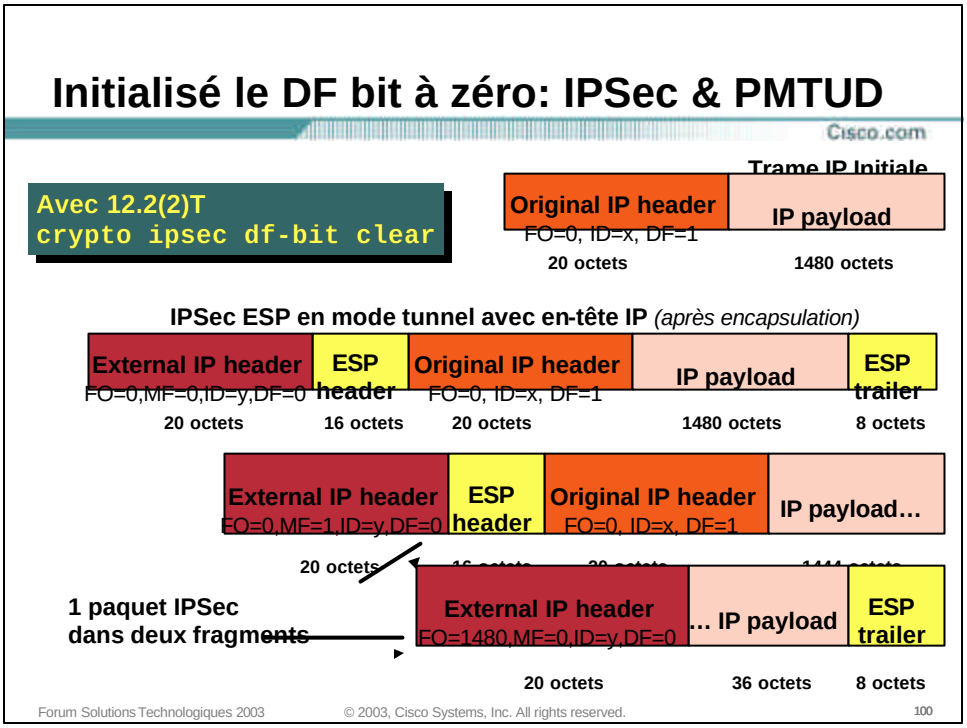
Cisco.com

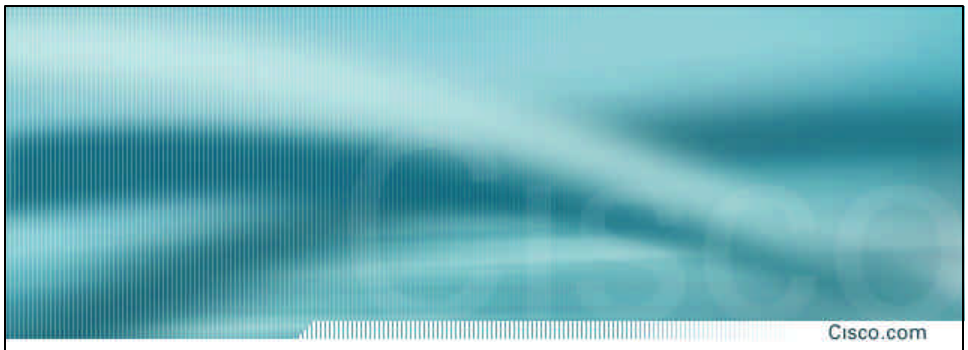


PMTUD et IPSec/2



Initialisé le DF bit à zéro: IPSec & PMTUD





GRE et IPSec

GRE + IPSec

- **L'association par excellence**
  - **GRE (ou IPinIP): pour les protocoles de routage, le multicast**
  - **IPSec : confidentialité, intégrité, authentification**

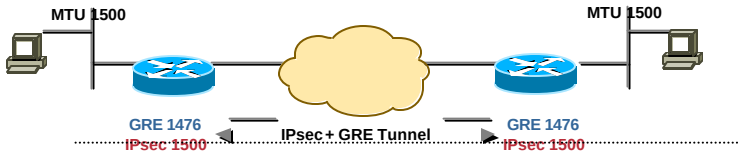
GRE + Ipsec et la Fragmentation

Cisco.com

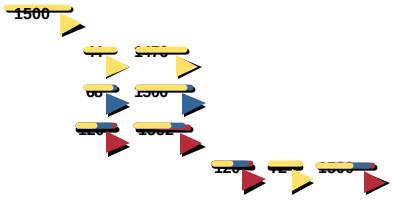
- **Fragmentation**
  - **GRE fragmente avant l'encapsulation**
  - **IPsec fragmente après le chiffrement**
  - **Nous pouvons avoir une double fragmentation**
- **Si nous ne pouvons l'éviter, il faut initialiser le MTU de l'interface GRE:**
  - **IPsec transport mode ⇒ 'ip mtu 1440'**
  - **IPsec tunnel mode ⇒ 'ip mtu 1420'**

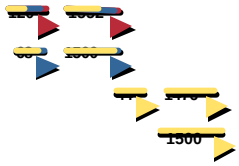
IPsec + GRE Fragmentation DF=0

Cisco.com

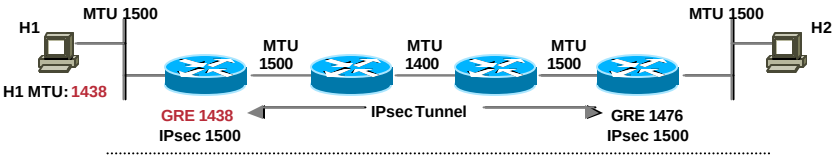


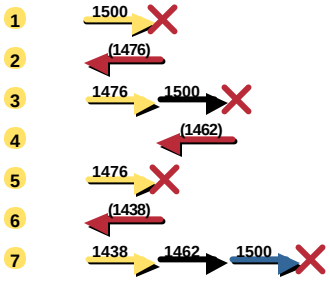
1. Données (DF bit = 0)
2. Fragmente le paquet GRE
3. Ajoute encapsulatation GRE
4. IPsec chiffre les paquets
5. Fragmente IPsec
6. Assemble le paquet IPsec
7. Retire le chiffrement IPsec
8. Retire l'encapsulation GRE
9. Hôte Assemble la trame





IPsec + GRE avec PMTUD – 1ère Partie





Trame IP; Abandonée par GRE

ICMP envoyé à la source (type=3, code=4)

Trame IP; Paquet GRE; Abandonné par IPsec

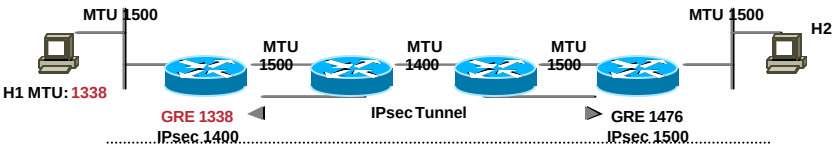
ICMP envoyé la source du tunnel GRE

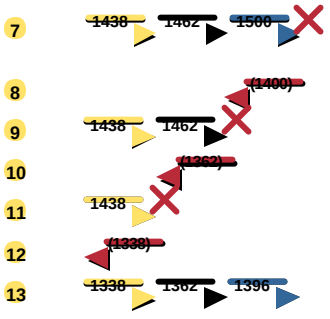
Trame IP Abandonnée par GRE

ICMP envoyé à la source (type=3, code=4)

Trame IP; Paquet GRE; Paquet IPSec; Abandonné par le router intermédiare

IPsec + GRE avec PMTUD- 2ème partie





Trame IP; Paquet GRE; Paquet IPSec; Abandonné par le router intermédiare

ICMP envoyé la source du paquet IPSec

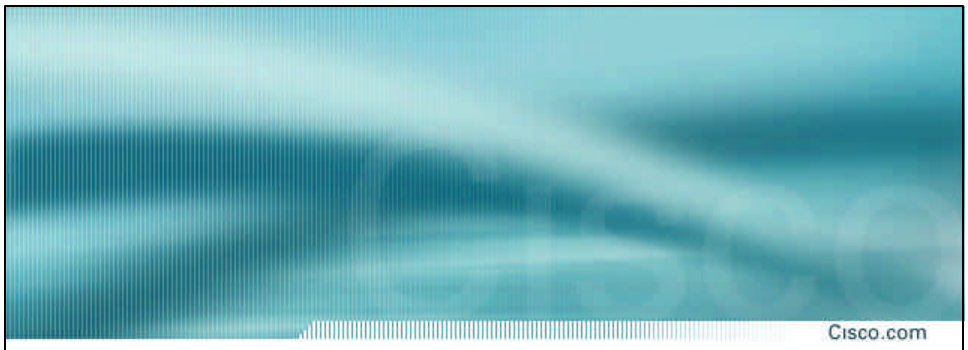
Trame IP; Paque GRE; abandonné par IPsec

ICMP envoyé à la source du tunnel GRE

Trame IP; Abandonnée par GRE

ICMP envoyé à la source (type=3, code=4)

Trame IP; Paquet GRE; Paquet Ipsec; Atteint finalement la destination

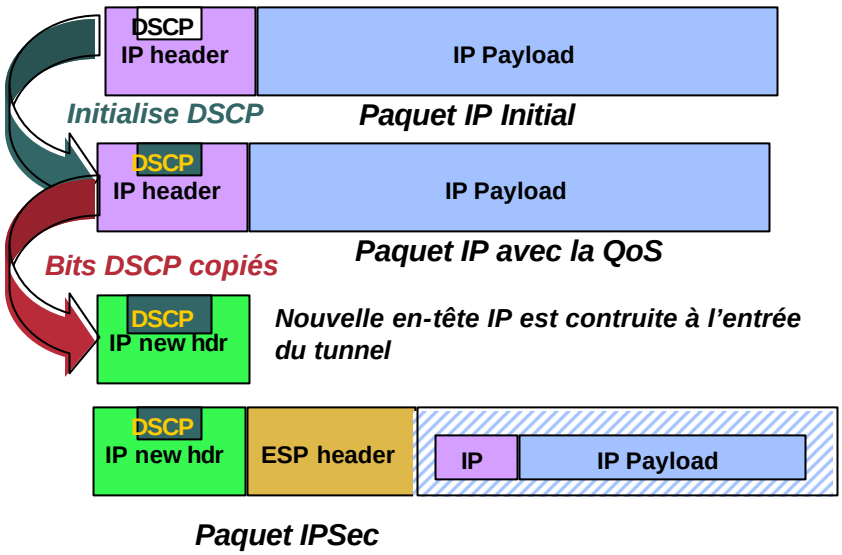


IPSec et la Qualité de Service (QoS)

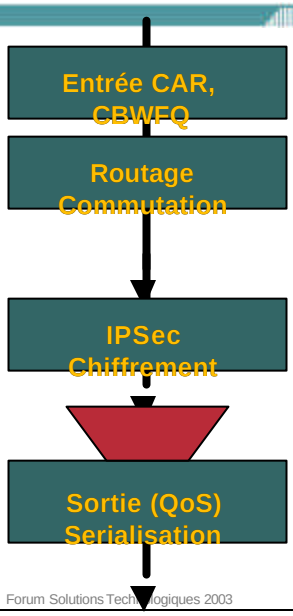
QoS diff-serv et IPSec

- **IPSec oblige qu'on copie les bits DSCP de l'en-tête IP initiale**
  - **QoS est préservée pour WRED, CBWFQ, ...**

Tunnels IPSec & QoS

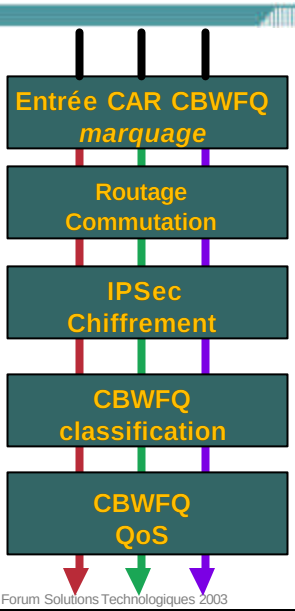


Le cheminement d'un paquet



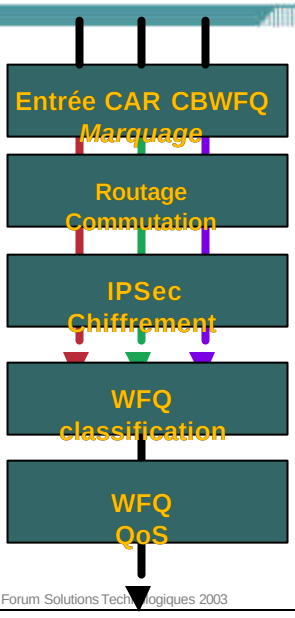
- **L'ordre dans les files d'entrée et sortie dépend de la QoS**
  - **WFQ: Une file par session**
  - **PQ/CQ: 4 où 16 queues (ACL)**
  - **CBWFQ: Queues multiples (ACL, NBAR, …)**

CBWFQ et IPSec



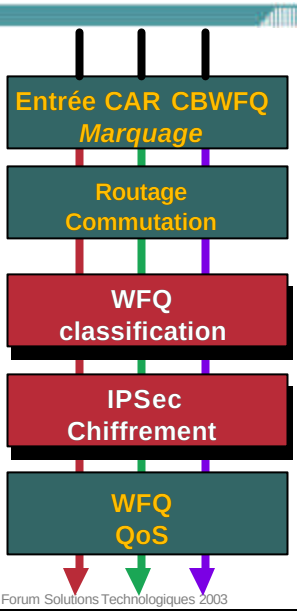
- Le marquage des paquets avec DSCP est réalisé avant le chiffrement
- CBWFQ
  - classification basée sur des “extended ACL”
  - => Plusieurs queues

WFQ and IPSec



- Le marquage des paquets avec DSCP est réalisé avant le chiffrement
- WFQ
  - Classification basée sur les adresses IP, protocoles, (ports IP)
  - Poids (weight) basé sur les bits de précédence IP
  - => Seulement un queue est utilisée

WFQ et IPSec



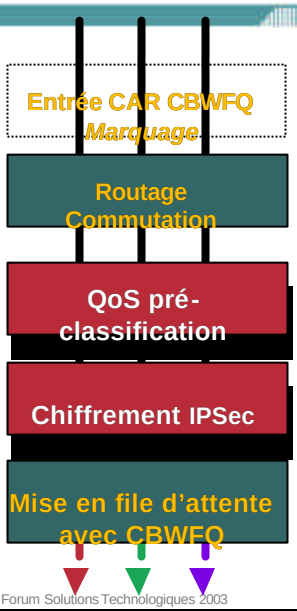
- Si

```
crypto map …
    qos pre-classify
```

IOS 12.2
IOS 12.1(5)T

- WFQ
  - **Classification** basée sur les adresses IP, protocoles, (ports IP)
  - **Poids (weight)** basé sur les bits de précédence IP
  - => Plusieurs queues sont utilisées

Une autre utilisation de QoS Pre-Classify

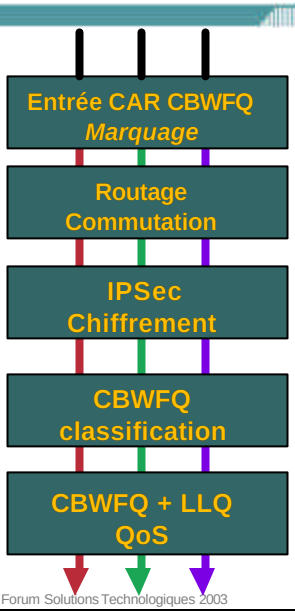


- Si

```
crypto map …
    qos pre-classify
```

- Le marquage des paquets IP peut être réalisé sur l'interface de sortie

Low Latency Queuing (LLQ) et IPSec




```
policy-map voice-policy
  class voice
    priority 64
```

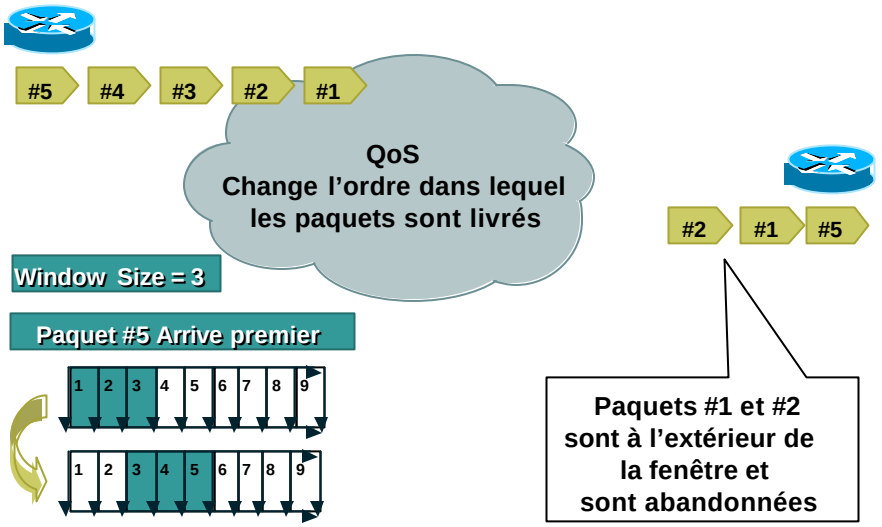
- **CBWFQ avec LLQ**
  - **Classification basée sur des extended ACL (DSCP) de paquets IPSec**
  - **⇒Multiple queues**
  - **⇒ Queue LLQ est toujours vidée en premier**

Anti-Replay avec IPSec

- **ESP (avec authentification) et AH possède des mécanisme “anti-reply”**
  - **Basé sur des numéros de séquence**
  - **Le RFC recommande 64 paquets, mais 32 paquets OK**
  - **La source augmente le numéro de séquence après chaque transmission**
  - **La destination vérifie le numéro de séquence et refuse le paquet s’il est hors séquence**
- **Devrait être négocié avec IKE**
- **Note: le numéro de séquence n’est pas utilisé pour ordonner la livraison des paquets**

QoS et Anti-Replay

Cisco.com



IOS et PIX

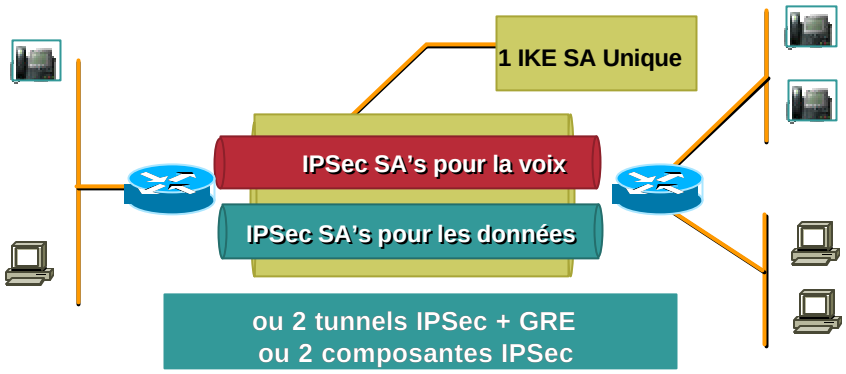
Cisco.com

- Anti-replay est toujours actif pour AH et ESP avec authentification
  - IOS window size est de 64 paquets
  - PIX window size est de 32 paquets
- Anti-replay est inactif pour ESP sans authentification

Pour annuler l'Anti-Replay

Cisco.com

- Il est possible d'utiliser un SA's dediés à la VoIP



Cisco.com

Références

IPSec et le PMTUD ou la QoS

Cisco.com

- **IP Fragmentation and PMTUD**

  http://www.cisco.com/warp/public/105/pmtud_ipfrag.html

- **Reference Guide to Implementing Crypto and QoS:**

  http://www.cisco.com/warp/public/105/crypto_qos.html

Cisco IOS – Nouvelles fonctions de sécurité

Cisco.com

Categorie	Fonction	Version
IPsec	AES SW support in IOS	12.2(13)T
	Dynamic Multipoint VPN (DMVPN)	12.2(13)T
	IPsec NAT Transparency	12.2(13)T
	IPsec Stateful Fail-over Phase 1	12.2(11)YX
	Easy VPN Remote Phase 1	12.2(13)T
	LLQ for IPsec	12.2(13)T
	IPsec Passive Mode	12.2(13)T
	Look-ahead fragmentation	12.2(13)T
	SADB Lookup Optimization	12.2(13)T
	SW IPComp with HW Crypto	12.2(13)T
	Clearing of IPsec SA without clearing the counters	12.2(13)T
	IKE Support for PKI multi-RSA key pair	12.2(13)T
	Tunnel Protection (IPsec around GRE)	12.2(13)T
	Aswan Phase 1.3	12.2(13)T1

Cisco IOS – Nouvelles fonctions de sécurité

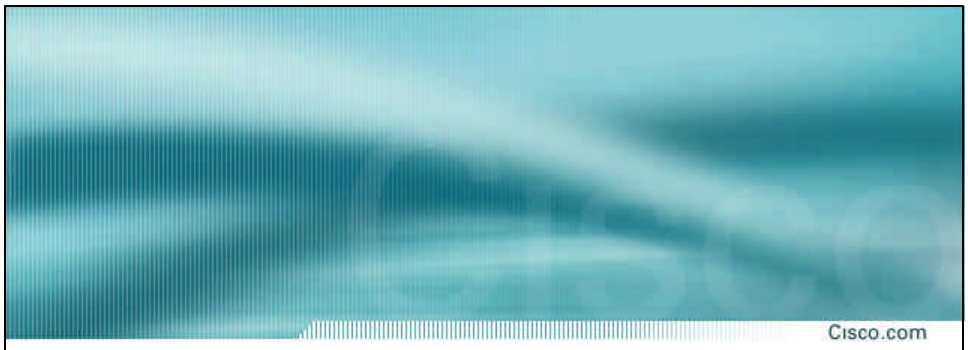
Cisco.com

Categorie	Fonctions	Version
Trust & Identity	Manual Cert. Enrollment (TFTP and Cut & Paste)	12.2(13)T
Firewall & IDS	IDS performance	12.2(13)T
	Websense/N2H2 Filtering	12.2(11)YU
	SIP Voice inspection	12.2(11)YU
	HTTPS support for Auth Proxy	12.2(11)YU
	ICMP Inspection	12.2(11)YU
	IDS Signatures (42)	12.2(11)YU
IP Services	Stateful NAT Phase 1	12.2(13)T
	VRF-Aware NAT Phase 1	12.2(13)T
	IPsec Pass-thru with Overload Phase 1	12.2(13)T
	Static NAT mapping on an interface	12.2(13)T
	NAT PT Phase 1	12.2(13)T

Cisco IOS – Nouvelles fonctions de sécurité

Cisco.com

Categorie	Fonctions	Version
~~IPsec~~	~~VRF-aware IPsec (IPsec/MPLS Integration)~~	~~12.2(15)T~~
	~~Easy VPN Remote Phase 2.0 & 3.0~~	~~12.2(15)T~~
	~~IPsec Accounting~~	~~12.2(15)T~~
	~~IPsec Timer Clean-up~~	~~12.2(15)T~~
~~Trust & Identity~~	~~N-Tier Certificate Chaining~~	~~12.2(15)T~~
	~~Certificate Security Attribute based Access Control~~	~~12.2(15)T~~
	~~Allow Source Int. Selection for HTTP Traffic~~	~~12.2(15)T~~
	~~SSL Server Support in Cisco IOS IOS~~	~~12.2(15)T~~
	~~Key Import/Export~~	~~12.2(15)T~~



Merci

N'oubliez pas de remplir votre formulaire d'évaluation.

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION