Laboratoire de téléinformatique

VPN LAN to LAN

Auteurs : Gilles-Etienne Vallat, Alexandre Délez

Professeur : Fabien Bruchez

Version : 1.6 20/05/2009

Groupe No : _____

Elèves : _____

_____

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Table des matières

Introduction

Le but de ce travail est de pratiquer et mesurer toutes les étapes nécessaires à l'établissement d'un VPN IPsec.

Le laboratoire va permettre à l'étudiant de se familiariser avec tous les aspects du VPN de réseau à réseau (LAN to LAN) de manière à mieux comprendre la théorie. Ces aspects sont :

- Configuration IKE et IPsec
- Etablissement de la Phase I IKE
- Négociation de la Phase II IKE
- Capture des échanges IKE entre deux routeurs VPN
- « debug crypto » sur un routeur Cisco
- Overhead ajouté par IPsec aux paquets
- Gestion du MTU/MSS et de la fragmentation
- Interfaçage du VPN avec les fonctions de NAT nécessaires pour Internet
- Eventuellement tunnel GRE et routage au travers des VPN

Matériel

Chaque poste de travail est composé des éléments suivants :

- 2 clients Windows XP (PC1xx et 2xx) avec:
  - Un analyseur réseau Wireshark (au minimum la version 0.10.x)
  - Un serveur TFTP
    Compte: **`labo`**, mot de passe: **`labo`**
- 2 routeurs CISCO (modèles 2811 et 2821)
- Un Petit HUB
- Bornier : prises vertes et prises HUB salle (prises 7 et 8)

Structure du laboratoire et VPN en 2 mots

Présentation

Un VPN (Virtual Private Network) sert principalement à relier deux entités distantes pouvant partager un adressage commun au travers d'un réseau tiers. Ceci doit permettre de communiquer entre ces deux entités comme si elles n'étaient séparées que par un simple routeur.

Des critères ont été définis afin de répondre à ce besoin. Les trois principaux (séparation de l'espace d'adressage, du trafic et du routage) définissent un VPN. Afin d'obtenir un VPN sécurisé, il faut en ajouter trois autres (authentification, chiffrement et intégrité des données).
Ce laboratoire va principalement traiter des VPN sécurisés.

Critères définissants un VPN :

- Séparation de l'espace d'adressage
- Séparation du trafic
- Séparation du routage

} VPN

- Authentification
- Chiffrement
- Intégrité des données

} VPN Sécurisé

Il y a deux types de connexion possibles :

- LAN 2 LAN : permettant de connecter deux sites distants (que nous allons traiter dans ce laboratoire)
- Remote access VPN : permettant de connecter une machine distante à un site

Les VPN peuvent se trouver à plusieurs niveaux du modèle OSI (PPTP en couche 3, SSL en couche 4, …). Nous allons travailler avec IPsec qui est un protocole de couche 3.

Pour établir un tunnel sécurisé LAN to LAN, un mécanisme d'échange de clés est nécessaire. Il y a deux solutions envisageables.

La première consiste à placer sur chacun des sites une clé figée configurée statiquement. La seconde repose sur le protocole IKE. Il échange et renouvelle les clés périodiquement. C'est donc cette solution que nous allons utiliser.

IKE fonctionne en deux phases :

- La phase 1 permet de générer une première SA (Security Association : correspond à un ensemble de paramètres et de clés pour un lien) servant à communiquer de manière sécurisée sur IKE.
- La phase 2 permet de générer une paire de SA pour la communication IPsec.

Il y a deux types de phase 1 possibles :

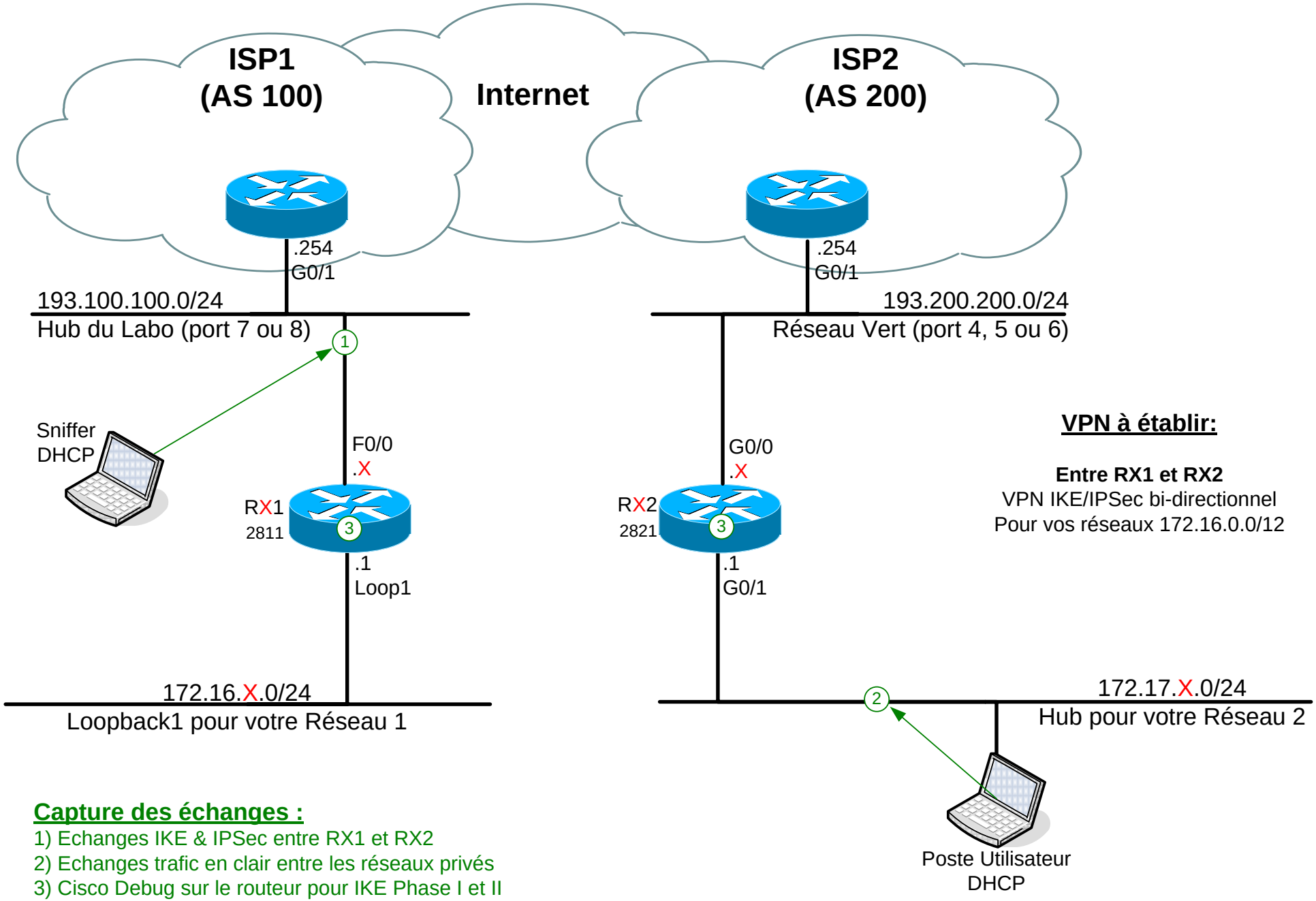
- Main mode : se compose de six paquets permettant de chiffrer l'identité du client, ce qui le rend à cet égard plus sécurisé.
- Agressive mode : se compose de trois paquets, ce qui le rend plus rapide, mais l'identité du client passe en clair sur le réseau. Ceci peut être nécessaire dans certains cas.

L'échange peut se faire avec une clé partagée dite PSK (Pre-Shared Key) ou en DSA (Digital Signature Authentication).
Dans notre cas, nous utiliserons le Main mode en PSK.

La phase 2, Quick mode, sert à échanger les paramètres et les clés de la connexion IPsec. Elle se compose de trois paquets.

IPsec est un protocole de couche 3 permettant de chiffrer des données. Ses paramètres (clés, algorithmes de chiffrement, …) ont déjà été échangés lors de la phase 2 de IKE.

Une fois la phase 2 de IKE terminée, le tunnel est donc opérationnel. Chaque paquet empruntant le tunnel sera chiffré par IPsec, transmis par le tunnel au destinataire qui le déchiffrera et le routera sur son réseau.



VPN à établir:

Entre RX1 et RX2
VPN IKE/IPSec bi-directionnel
Pour vos réseaux 172.16.0.0/12

Capture des échanges :

1) Echanges IKE & IPSec entre RX1 et RX2
2) Echanges trafic en clair entre les réseaux privés
3) Cisco Debug sur le routeur pour IKE Phase I et II

Manipulations

Préparation

Téléchargez les fichiers nécessaires à ce laboratoire. Ils se trouvent sur:
\\Eint20\Profs\FBZ\Cours ADN\Lab VPN\

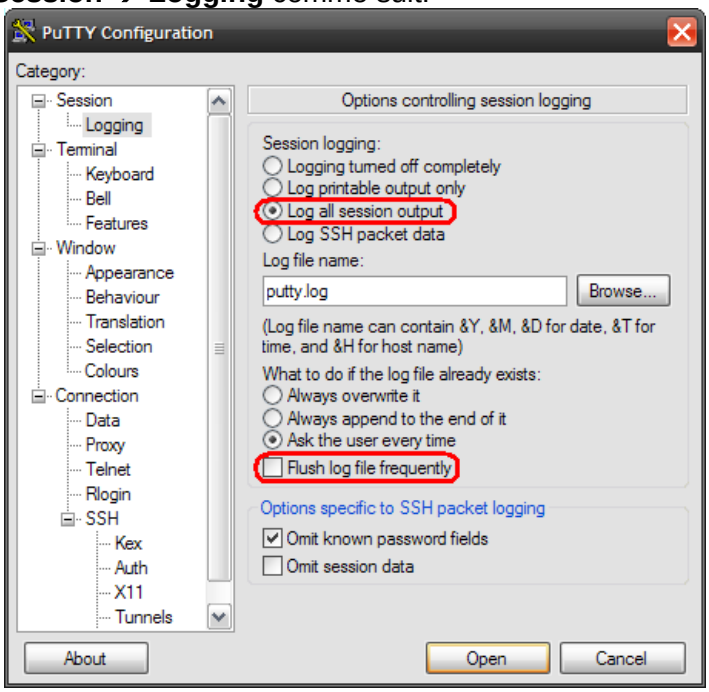
Branchez vos deux routeurs comme décrit sur le schéma ci-dessus.

Branchez aussi les deux stations comme illustré sur le schéma. La station « sniffer » est capable d'aller sur Internet à tout moment (documentation Cisco ou autre). Par contre la station « poste utilisateur » ne sera capable d'aller sur Internet qu'à l'issue d'une configuration VPN avec NAT pour votre réseau (exercice 4).

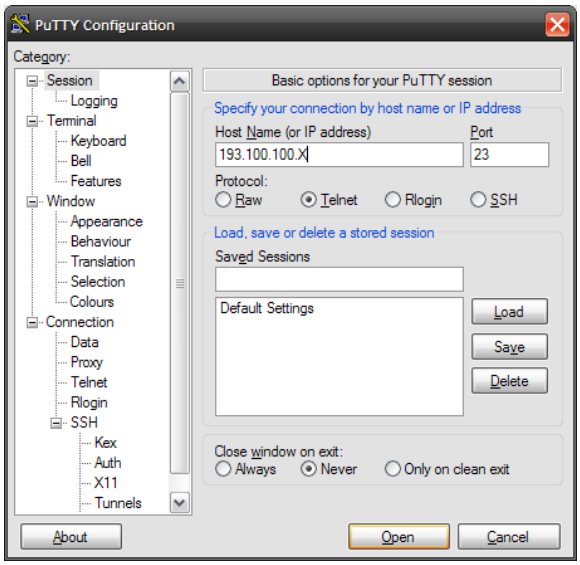
Partout où figure la lettre « X » dans ce document, elle devra être remplacée par votre numéro de groupe durant toute la réalisation.

Dans ce laboratoire, il faudra se connecter aux routeurs avec une connexion rapide. Pour ce faire, l'utilitaire "Putty" sera utilisé pour se connecter aux routeurs par telnet. Il est disponible sur tous les postes du laboratoire ou téléchargeable sur le site http://www.putty.nl/ (Pour le télécharger directement: http://www.putty.nl/latest/x86/putty.exe).

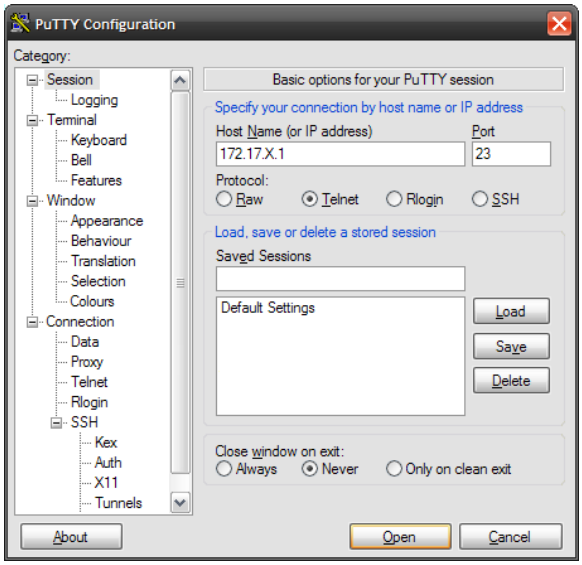
Il faudra lui demander d'enregistrer dans un fichier ce qui sera affiché dans un fichier en modifiant le menu **Session → Logging** comme suit:



Pour se connecter aux routeurs, il suffit de préciser le protocole (en l'occurrence telnet) ainsi que son adresse IP et son port:



Pour RX1



Pour RX2

Configuration de base des routeurs

Effacez la configuration actuelle du routeur avec la commande

`erase nvram:`, puis **`reload`**
Abandonnez le « wizard » de configuration

Modifiez puis importez les configurations suivantes dans chacun des deux routeurs

RX1 - 2811 cisco2811-base.cfg

RX2 - 2821 cisco2821-base.cfg

Dans ces fichiers, il faut remplacer la chaîne « !!!X!!! » par le numéro de votre groupe. Vous pourrez ensuite coller le contenu de vos configurations modifiées à la console de chacun des deux routeurs (<configure terminal> puis cut&paste). Le mot de passe d'accès ainsi que le mot de passe « enable » sont préconfigurés à la valeur « cisco ». Merci de ne pas changer cela.

Pour différencier les deux routeurs sans chercher trop longtemps l'étiquette où est noté le modèle, vous pouvez vous rappeler que le routeur 2821 (2RU) est plus haut que le 2811 (1RU). « RU » veut dire « Rack Unit » qui une hauteur standardisée pour les racks informatiques, qui vaut environ 4.5cm.

Contrôlez la connectivité sur toutes les interfaces à l'aide de pings.

RX2 (172.17.X.1) à votre poste utilisateur

RX1 vers ISP1 (193.100.100.254) et votre Sniffer en DHCP

RX2 vers ISP2 (193.200.200.254)

Afin que les **debug** soient visibles sur votre interface par telnet, il faut activer le **terminal monitor** en mode Enable sur vos routeurs.

1. Configuration VPN LAN 2 LAN

Nous allons établir un VPN IKE/IPsec entre le réseau de votre « loopback 1 » sur RX1 (172.16.X.0/24) et le réseau de votre hub sur RX2 (172.17.X.0/24). Les étapes de configuration seront les suivantes :

Configuration des « proposals » IKE sur les deux routeurs
Configuration des clefs « preshared » pour l'authentification IKE
Activation des « keepalive » IKE
Configuration du mode d'encryption IPsec
Configuration du trafic à encrypter
Activation de l'encryption

1.1) Configuration IKE

Sur le routeur RX1 nous activons un « proposal » IKE avec les éléments suivants :

Encryption	AES 256 bits
Signature	Basée sur SHA-1
Authentification	Preshared Key
Diffie-Hellman	avec des nombres premiers sur 1536 bits
Renouvellement	des SA de la Phase I toutes les 30 minutes
Keepalive	toutes les 30 secondes avec 3 « retry »
Preshared-Key	pour l'IP du distant avec le texte « cisco-1 »
	Notez que dans la réalité nous utiliserions un texte plus compliqué.

Les commandes de configurations sur RX1 ressembleront à ce qui suit :

```
crypto isakmp policy 20
  encr aes 256
  authentication pre-share
  hash sha
  group 5
  lifetime 1800
crypto isakmp key cisco-1 address 193.200.200.X no-xauth
crypto isakmp keepalive 30 3
```

Sur le routeur RX2 nous activons un « proposal » IKE supplémentaire comme suit :

```
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  hash md5
  group 2
  lifetime 1800
crypto isakmp policy 20
  encr aes 256
  authentication pre-share
  hash sha
  group 5
  lifetime 1800
crypto isakmp key cisco-1 address 193.100.100.X no-xauth
crypto isakmp keepalive 30 3
```

Vous pouvez consulter l'état de votre configuration IKE avec les commandes suivantes et faites part de vos remarques :

show crypto isakmp policy
show crypto isakmp key

1.2) Configuration IPsec

Nous allons maintenant configurer IPsec de manière identique sur les deux routeurs. Pour IPsec nous allons utiliser les paramètres suivants :

IPsec avec IKE	IPsec utilisera IKE pour générer ses SA
Encryption	AES 192 bits
Signature	Basée sur SHA-1
Proxy ID RX1	172.16.X.0/24
Proxy ID RX2	172.17.X.0/24
Fonction PFS	active avec du DH sur 1024 bits

Changement de SA toutes les 5 minutes ou tous les 2.6MB
Si inactifs les SA devront être effacés après 15 minutes

Les commandes de configurations sur RX1 ressembleront à ce qui suit :

```
crypto ipsec security-association lifetime kilobytes 2560
crypto ipsec security-association lifetime seconds 300
crypto ipsec transform-set STRONG esp-aes 192 esp-sha-hmac
ip access-list extended TO-CRYPT
 permit ip 172.16.X.0 0.0.0.255 172.17.X.0 0.0.0.255
crypto map MY-CRYPTO 10 ipsec-isakmp
 set peer 193.200.200.X
 set security-association idle-time 900
 set transform-set STRONG
 set pfs group2
 match address TO-CRYPT
```

Les commandes de configurations sur RX2 ressembleront à ce qui suit :

```
crypto ipsec security-association lifetime kilobytes 2560
crypto ipsec security-association lifetime seconds 300
crypto ipsec transform-set STRONG esp-aes 192 esp-sha-hmac
 mode tunnel
ip access-list extended TO-CRYPT
 permit ip 172.17.X.0 0.0.0.255 172.16.X.0 0.0.0.255
crypto map MY-CRYPTO 10 ipsec-isakmp
 set peer 193.100.100.X
 set security-association idle-time 900
 set transform-set STRONG
 set pfs group2
 match address TO-CRYPT
```

Vous pouvez contrôler votre configuration IPsec avec les commandes suivantes :

show crypto ipsec security-association
show crypto ipsec transform-set
show access-list TO-CRYPT
show crypto map

1.3) Activation IPsec & test

Pour activer cette configuration IKE & IPsec il faut appliquer le « crypto map » sur l'interface de sortie du trafic où vous voulez que l'encryption prenne place. Avant d'activer cette configuration vous ne devez pas être capable de pinger vos adresses privées sur RX1 (Ex : 172.16.X.1) depuis votre station utilisateur derrière RX2. Validez cela et donnez votre explication sur : « pourquoi vos adresses privées ne sont pas routées sur Internet ».

Sur RX1 il s'agit, selon le schéma, de l'interface « FastEthernet0/0 » et la configuration sera :

```
interface FastEthernet0/0
 crypto map MY-CRYPTO
```

Sur RX2 il s'agit, selon le schéma, de l'interface « GigabitEthernet0/0 » et la configuration sera :

```
interface GigabitEthernet0/0
 crypto map MY-CRYPTO
```

Après avoir entré cette commande, normalement le routeur vous indique que IKE (ISAKMP) est activé. Vous pouvez contrôler que votre « crypto map » est bien appliquée sur une interface avec la commande « **show crypto map** ».

Analysez le retour de la commande « **show crypto engine configuration** » et faites part de toutes vos constatations et remarques dans votre rapport. Une petite recherche sur le site de Cisco peut s'avérer utile pour compléter votre explication.

Pour tester si votre VPN est correctement configuré vous pouvez maintenant lancer un « ping » sur la « loopback 1 » de votre routeur RX1 (172.16.X.1) depuis votre poste utilisateur (172.17.X.100). De manière à recevoir toutes les notifications possibles pour des paquets ICMP envoyés à un routeur comme RX1 vous pouvez activer un « debug » pour cela. La commande serait :

```
debug ip icmp
```

Pensez à démarrer votre sniffer sur le poste utilisateur avant de démarrer votre ping, collectez aussi les éventuels messages à la console des différents routeurs. Ensuite faites part de vos remarques dans votre rapport.

Merci de reporter dans votre rapport une petite explication concernant les différents « timers » utilisés par IKE et IPsec dans cet exercice.

2. Analyse détaillée de l'établissement du VPN

Dans cette question nous voulons mettre en lumière toutes les étapes de l'établissement d'un VPN. Ce qui comprend l'établissement de la phase I (6 paquets) et de la phase II (trois paquets) avant l'échange de paquet ESP encrypté.

2.1) Captures Phase I et Phase II fonctionnelles

Vous allez capturer tous les échanges IKE et IPSec entre vos deux routeurs VPN fonctionnels. Cette capture doit englober les éléments suivants :

Les paquets ICMP qui sortent de votre poste utilisateur (ping 172.16.X.1 -n 2)

Les paquets IKE et ESP échangés entre les deux routeurs (depuis votre sniffer)

Les messages de « debug » sur la crypto activés sur les deux routeurs

Pour activer tous les « debug » intéressants sur vos routeur, vous devez entrer les commandes suivantes :

debug ip icmp	! pour tous les paquets ICMP émis par le routeur
debug crypto isakmp	! pour tous les messages IKE
debug crypto engine	! pour tous les messages venant du crypteur
debug crypto ipsec	! pour tous les messages à propos d'IPSec

Au vu du nombre de messages générés par les commandes « debug » ci-dessus il est conseillé de travailler en telnet sur les différents routeurs (sniffer → RX1, poste utilisateur → RX2). La console qui risque d'être surchargée à 9600, c'est pour cela qu'il est préférable de ne pas envoyer de message de debug sur celle-ci, la commande serait : **« logging console informational »**.

Identifier dans vos traces et « debug » les différentes étapes de l'établissement de la Phase I et de la Phase II IKE. En vous reportant au cours, pointez sur les messages/paquets importants à relever en cas de bon fonctionnement de chaque étape et expliquer brièvement ce qui se passe.

Exemple (incomplet) :

```
...
ISAKMP (0:0): received packet from 193.200.200.15 dport 500
...                                              sport 500 Global (I) MM_NO_STATE
ISAKMP:(0:0:N/A:0):found peer pre-shared key matching 193.200.200.15
...
ISAKMP:(0:0:N/A:0):atts are acceptable. Next payload is 0
...
ISAKMP:(0:1:SW:1):Old State = IKE_I_MM6  New State = IKE_P1_COMPLETE
...
```

2.2) Captures avec erreurs en Phase I

Maintenant que vous avez des captures de la phase I et de la phase II IKE fonctionnelles, vous pouvez introduire volontairement certaines erreurs pour comparer les informations capturées et pointer sur le message qui vous permet de confirmer l'erreur introduite. Vous pouvez vous inspirer du fichier PDF suivant « ipsec_debug.pdf » (disponible sur le partage réseau du laboratoire) pour vous aider à expliquer les situations d'erreur ci-dessous.

a) Erreur à introduire en phase I pour les groupes **pairs**

Entrer les commandes de configuration suivantes sur votre routeur RX1 :

crypto isakmp policy 20

group 2

lifetime 600

b) Erreur à introduire en phase I pour les groupes **impairs**

Entrer la commande de configuration suivante sur votre routeur RX1 :

no crypto isakmp key cisco-1 address 193.200.200.X no-xauth

crypto isakmp key cisco-2 address 193.200.200.X no-xauth

Dès que l'erreur est introduite, il est nécessaire d'effacer vos clefs (SA) IKE et IPsec avec les commandes suivantes avant de redémarrer le test d'établissement du VPN:

clear crypto isakmp

clear crypto sa

Toujours avec les « debug » actifs, faites remonter le tunnel VPN IPsec (ping de 172.16.X.1 depuis votre station utilisateur) et comparez les traces et messages collectés sur les deux routeurs avec celles de la question 2.1 (cas fonctionnel). Etayez ces contrôles dans votre rapport (capture Wireshark si possible, debug Cisco, show commandes) de manière à bien montrer la différence. Faites ensuite part de vos remarques sur les différences, indiquez quelle ligne de message de quel routeur vous permet d'affirmer la source de votre erreur.

Une fois cette partie d'analyse terminée, vous pouvez corriger votre configuration pour qu'elle soit à nouveau fonctionnelle (le ping doit fonctionner avant que vous passiez à la question suivante).

2.3) Captures avec erreurs en Phase II

a) Erreur à introduire en phase II pour les groupes **pairs**

Entrer les commandes de configuration suivantes sur votre routeur RX1 :

ip access-list extended TO-CRYPT

permit ip 172.16.X.0 0.0.0.255 172.17.X.128 0.0.0.127

no permit ip 172.16.X.0 0.0.0.255 172.17.X.0 0.0.0.255

b) Erreur à introduire en phase II pour les groupes **impairs**

Entrer la commande de configuration suivante sur votre routeur RX1 :

crypto ipsec transform-set STRONG esp-aes 192 esp-md5-hmac

Dès que l'erreur est introduite, il est nécessaire d'effacer vos clefs (SA) IKE et IPsec avec les commandes suivantes avant de redémarrer le test d'établissement du VPN :

clear crypto isakmp

clear crypto sa

Toujours avec les « debug » actifs, faites remonter le tunnel VPN IPsec (ping de 172.16.X.1 depuis votre station utilisateur) et comparez les traces et messages collectés sur les deux routeurs avec celles de la question 2.1 (cas fonctionnel). Etayez ces contrôles dans votre rapport (capture Wireshark si possible, debug Cisco, show commandes) de manière à bien montrer la différence. Faites ensuite part de vos remarques sur les différences, indiquez quelle ligne de message de quel routeur vous permet d'affirmer la source de votre erreur.

Une fois cette partie d'analyse terminée, vous pouvez corriger votre configuration pour qu'elle soit à nouveau fonctionnelle (le ping doit fonctionner avant que vous passiez à la question suivante).

3. Gestion du MTU avec les VPN

3.1) « Overhead » ajouté par IPsec aux paquets

A l'aide de captures Wireshark démarrées sur vos deux postes, montrer l' « overhead » IPsec dans votre configuration actuelle.

Pour cela faites des pings en réglant la taille des données que l'ICMP ECHO enverra vers sa destination. La commande DOS « ping » avec l'option « -l » permet de changer cette valeur mise par défaut sous la plupart des OS à 32 Bytes. Comme le header IP est de 20 bytes et le header ICMP est de 8 bytes la taille totale du paquet IP qui sera envoyé sur le réseau sera de 60 Bytes.

Faites des pings consécutifs pour des tailles de paquets IP allant de 250 à 500 Bytes par incrément de 1 byte (il est très aisé de faire un petit batch pour tous ces pings, vous le trouverez sur le partage du laboratoire avec le nom « ping-size.bat »).

ping 172.16.X.1 -n 1 -l 222

ping 172.16.X.1 -n 1 -l 223

…

ping 172.16.X.1 -n 1 -l 472

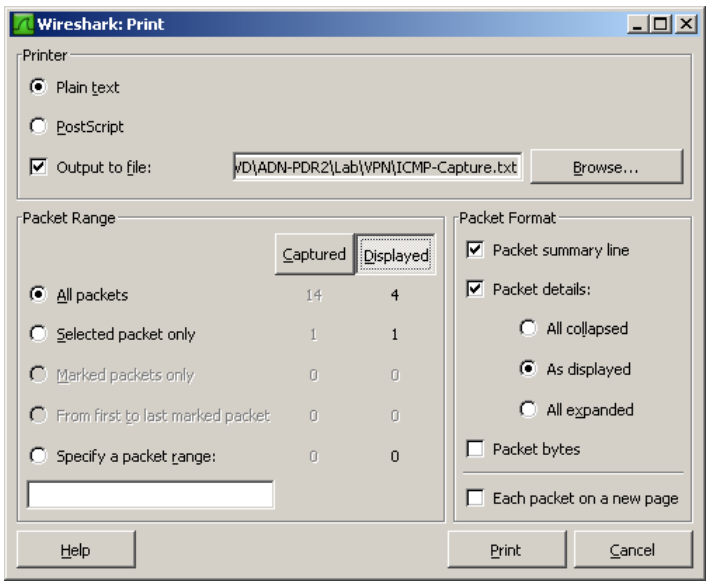
Trafic en clair : filtrez sur « icmp.type == 8 && ip.src == 172.17.X.100 »

Trafic encrypté : filtrez sur « ip.proto == 0x32 && ip.src == 193.200.200.X »

Sauvez le résultat de la capture au mode texte

Trafic en clair : fichier ICMP-Capture.txt

Trafic encrypté : fichier ESP-Capture.txt



```
No.     Time            Source              Destination           Protocol Info
      1 10:23:18.124439 172.17.172.17       172.17.172.254        ICMP     Echo (ping) request
Frame 1 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:a0:d1:be:03:ad, Dst: 00:0c:85:66:6f:69
Internet Protocol, Src: 172.17.172.17 (172.17.172.17), Dst: 172.17.172.254 (172.17.172.254)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 60
    Identification: 0xc736 (50998)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (0x01)
    Header checksum: 0xc257 [correct]
    Source: 172.17.172.17 (172.17.172.17)
    Destination: 172.17.172.254 (172.17.172.254)
Internet Control Message Protocol
```

findstr "Total Length" ICMP-Capture.txt > ICMP-len.txt

findstr "Total Length" ESP-Capture.txt > ESP-len.txt

Relevez les différences entre la taille du paquet IP/ICMP et la taille du paquet IP/ESP (comparez le champ « IP total length »). Représentez ceci dans un graphique et faites part de vos remarques dans votre rapport.

Note : un zoom sur les 30 premiers paquets testés permettra certainement de mieux visualiser le comportement de l'encapsulation ESP.

3.2) Gestion du MTU et de la fragmentation

Toujours avec votre sniffer actif, pingez votre routeur RX2 depuis votre poste utilisateur avec un paquet IP de 1500 Bytes au total et regardez que cela fonctionne bien.

ping 172.17.X.1 –n 1 –l 1472

Ensuite Pingez la loopback 1 du routeur RX1 toujours avec un paquet IP de 1500 Bytes et regardez comment est encrypté votre paquet. Faites part de vos remarques dans votre rapport en les étayant de trace ou captures.

ping 172.16.X.1 –n 1 –l 1472

En agissant sur la configuration du routeur RX2 sur l'ordre des opérations concernant la fragmentation, comparez le ping ci-dessus avec les deux configurations suivantes activées. Faites part de vos remarques dans votre rapport en les étayant de traces ou captures suites à vos deux tests.

interface GigabitEthernet0/0

crypto ipsec fragmentation before-encryption

interface GigabitEthernet0/0

crypto ipsec fragmentation after-encryption

« after-encryption » indique que la fragmentation des grands paquets est faite après l'encapsulation dans IPsec.

« before-encryption » indique que la fragmentation des grands paquets est faite avant l'encapsulation dans IPsec.

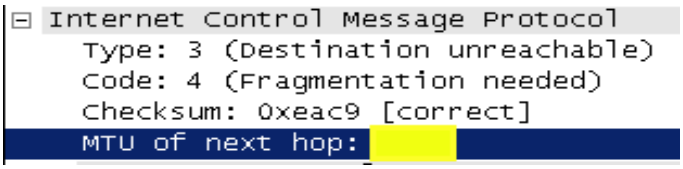
Quand ces mesures sont terminées revenez au mode de fragmentation par défaut. Puis testez le comportement du routeur VPN quand vous lui envoyez des paquets IP de 1500 Bytes avec interdiction de fragmentation. Vous pouvez envoyer des paquets ICMP avec interdiction de fragmentation (bit DF du header IP) avec l'option « -f ». Faites part de vos constatations à l'analyse des traces de vos deux sniffers. La commande ping ressemblera à :

ping 172.16.X.1 –n 1 -f –l 1472

Trouvez la taille maximale de paquet en bytes qui va passer le VPN sans être fragmenté.

ping 172.16.X.1 –n 1 -f –l 1...

Pour aller plus vite vous pouvez regarder plus en détail dans le header du paquet ICMP « destination unreachable » de code « fragmentation needed » pour observer la taille demandée par votre routeur RX2. Exemple :



3.3) MSS optimal en agissant sur la synchronisation TCP

Vous trouverez sur le partage réseau du laboratoire un fichier de 50KB ainsi qu'un petit serveur FTP (BabyFTP) à installer sur votre station utilisateur. Démarrez ce serveur FTP sur votre station et faites pointer le répertoire par défaut sur l'emplacement (en local sur votre machine) où se trouve le fichier de 50K.

Dès que vous êtes prêt avec votre serveur FTP et vos deux sniffers, démarrez le téléchargement de ce fichier sur le routeur RX1 depuis votre station utilisateur.

copy ftp://172.17.X.100/50K.bin null:

Afin de capturer un maximum d'information sur ce qui va se passer sur le routeur qui initie le téléchargement (RX1) et le routeur (RX2) qui va encapsuler dans IPsec votre session FTP, il est nécessaire de démarrer quelques « debug » que vous trouvez ci-dessous. De plus il faut s'assurer que le routeur RX1 utilise l'IP de la loopback 1 pour initier sa session FTP, ceci est configuré avec les commandes suivantes :

ip ftp source-interface loopback 1

ip ftp username anonymous

ip ftp password cisco@

ip tcp path-mtu-discovery

Debug à activer sur le routeur RX1 :

debug ip tcp transactions

debug ip icmp

debug ip ftp

Debug à activer sur le routeur RX2 :

debug ip icmp

Relevez toutes les informations nécessaires à décrire le comportement du transfert de ce fichier sur le routeur distant. Vous devez être capable de dessiner un diagramme en flèche et pointer sur tous les événements importants relatifs à la fragmentation de cette session TCP. Reportez-vous au cours pour expliquer ce qui se passe.

Maintenant que vous avez analysé le comportement d'un VPN pour la fragmentation des paquets, nous voulons être le plus optimal possible quant à la gestion des sessions TCP avec des paquets trop grands pour passer dans un tunnel VPN. Pour cela nous allons activer la fonction d'ajustement du MSS TCP (réf. Cours ADN).

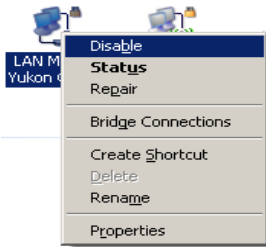
Pour cela nous pouvons activer la commande d'ajustement du MSS dans les paquets SYN envoyés. Attention cette commande doit être activée sur l'interface d'entrée du trafic en clair.

interface *votre_interface*

ip tcp adjust-mss votre_valeur_en_bytes

Une fois cette commande activée et toutes vos traces et debug en fonction, vous pouvez relancer l'opération de transfert du fichier FTP de 50K et reporter vos constatations dans votre rapport.

Note : pour effacer le cache de fragmentation de votre poste utilisateur et repartir sur une base saine il est nécessaire de désactiver l'interface réseau de votre station XP pour un bref instant.



4. Intégration VPN et NAT

Activez une configuration NAT classique dans votre routeur RX2. Contrôlez ensuite que votre poste utilisateur accède maintenant à Internet et au réseau de l'école.

La configuration NAT suivante est déjà présente dans votre routeur RX2, mais pas activée. Elle indique que toutes les adresses IP de votre réseau 172.17.X.0/24 seront masquées en PAT derrière l'adresse IP de l'interface GigabitEthernet0/0 de votre routeur.

```
ip nat inside source static tcp 172.17.X.100 23 interface GigabitEthernet0/0 2023
ip nat inside source route-map MY-NAT interface GigabitEthernet0/0 overload
ip access-list extended TO-NAT
 permit ip 172.17.X.0 0.0.0.255 any
route-map MY-NAT permit 20
 match ip address TO-NAT
route-map MY-NAT deny 50
```

Pour activer cette configuration NAT, vous devez indiquer quelle interface sera située en interne (**ip nat inside**) et laquelle sera située en externe (**ip nat outside**). Vous pouvez faire ça très simplement avec les commandes de configuration suivantes (une fois passée le NAT configuré sera actif).

```
interface GigabitEthernet0/0
 ip nat outside
interface GigabitEthernet0/1
 ip nat inside
```

Contrôlez maintenant que votre poste utilisateur accède maintenant au réseau de l'école.

Ceci constaté, regardez ce qui se passe au niveau de votre trafic VPN. Afin de préparer ce test il est nécessaire d'effacer vos clefs (SA) IKE & IPsec (c.f. 2.2) et d'activer le « debug » pour les opérations de NAT avec **« debug ip nat [detailed] »** et éventuellement consultez l'état de la table de translation NAT avec : **« show ip nat translations ».**

Avec les « debug » crypto et NAT activés analysez les traces et les messages collectés puis faites part de vos remarques. Etayez ces contrôles dans votre rapport (capture Wireshark si possible, debug Cisco, show commandes) de manière à bien montrer ce qui se passe.

Afin de corriger le problème constaté vous pouvez entrer les commandes de configuration suivantes pour opérer une exclusion du NAT pour les adresses de votre VPN :

route-map MY-NAT deny 10

match ip address TO-CRYPT

Notez qu'il est important d'effacer les translations de NAT actuellement actives afin de partir sur les nouvelle bases de votre configuration. Ceci peut être réalisé avec la commande :

clear ip nat translation *

Toujours avec les « debug » crypto et NAT activés analysez les traces et les messages collectés puis faites part de vos remarques sur ce qui a changé. Etayez ces contrôles dans votre rapport (capture Wireshark si possible, debug Cisco, show commandes) de manière à bien montrer ce qui se passe.

5. Routage au travers des VPN (extra)

Ajout d'une loopback2 avec 172.18.X.1/24 sur votre routeur RX1

Ajout d'une loopback2 avec 172.19.X.1/24 sur votre routeur RX2

Quelles seraient les modifications à opérer à votre configuration IKE/IPsec classique pour ajouter la nouvelle loopback 2 de RX1 dans votre VPN.

Plutôt que d'opérer ces modifications nous allons créer un tunnel GRE entre les deux routeurs RX1 et RX2 puis activer un routage OSPF entre ceux-ci pour permettre aux routeurs d'apprendre dynamiquement les nouveaux réseaux sans ne plus changer la configuration VPN.

Le subnet qui devra être utilisé pour le tunnel GRE entre RX1 et RX2 sera 172.20.X.0/24 avec RX1=172.20.X.1 et RX2=172.20.X.2

Sur RX1

```
interface tunnel 1
 ip address 172.20.x.1 255.255.255.0
 tunnel mode gre ip
 tunnel source loopback 1
 tunnel destination 172.17.X.1
```

Sur RX2

```
interface tunnel 1
 ip address 172.20.x.2 255.255.255.0
 tunnel mode gre ip
 tunnel source Giga 0/1
 tunnel destination 172.16.X.1
```

Contrôlez que l'OSPF préconfiguré pour vous soit établi et fonctionnel entre les deux routeurs. Il n'y a pas de raison de changer la configuration OSPF actuelle.

```
show ip ospf neighbor
show ip route ospf
ping 172.18.X.1 source 172.19.X.1      ! depuis RX2
```

Règles de Notation pour le laboratoire

2/3 de la note	Pertinence des résultats présentés
1/3 de la note	Contenu rédactionnel et qualité du rapport