IPSec client to site

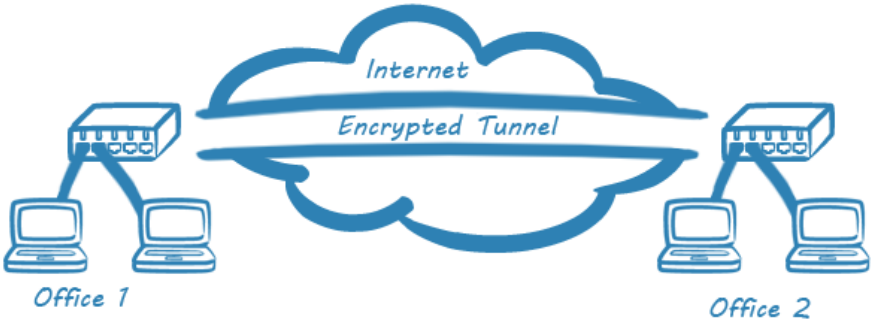
Miguel Frade

Department of Informatics Engineering
Polytechnic Institute of Leiria

Introduction

There are 2 types of IPSec VPN connections

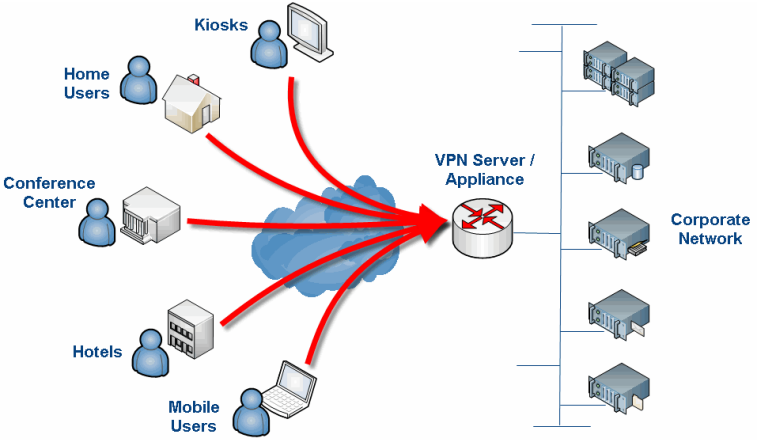
- Site-to-site (implemented in previous classes)



Introduction

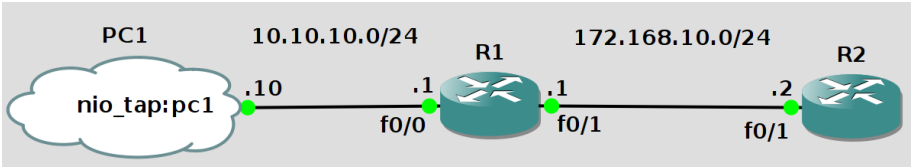
There are 2 types of IPSec VPN connections

- and client-to-site



Introduction

Our goal is to configure this network



1. be able to ping from PC1 to R2
2. create an IPSec tunnel between **PC1** and **R1**

R1 IPSec configurations

```
# Enable and configure AAA service
R1(config)$ aaa new-model                                  # enable AAA service
R1(config)$ aaa authentication login VPNAUTHEN local      # use local database for logins
R1(config)$ aaa authorization network VPNAUTHOR local     # allow network services
R1(config)$ username vpnstudent password cisco             # create user vpnstudent

# Set IP address pool for clients, this can limit the amount of simultaneous clients
R1(config)$ ip local pool IPPOOL 11.0.11.20 11.0.11.30

R1(config)$ crypto isakmp policy 5                         # configure ISAKMP policy
R1(config-isakmp)$ encryption des
R1(config-isakmp)$ hash md5
R1(config-isakmp)$ authentication pre-share
R1(config-isakmp)$ group 2
R1(config-isakmp)$ exit
```

R1 IPSec configurations (continuation)

```
# Specify group policy profile
R1(config)$ crypto isakmp client configuration group SALES
R1(config-isakmp-group)$ key cisco123
R1(config-isakmp-group)$ pool IPPOOL
R1(config-isakmp-group)$ domain lab.org
R1(config-isakmp-group)$ exit

# IPSec protocols configuration
R1(config)$ crypto ipsec transform-set MYSET esp-des esp-md5-hmac
R1(cfg-crypto-trans)$ exit

# Create a dynamic crypto map
R1(config)$ crypto dynamic-map DYNMAP 10
R1(config-crypto-map)$ set transform-set MYSET
R1(config-crypto-map)$ reverse-route
R1(config-crypto-map)$ exit
```

R1 IPSec configurations (continuation)

```
# Configure the router to initiate or reply to mode configuration requests
R1(config)$ crypto map CLIENTMAP client configuration address respond

# Configure AAA to local, as defined in the aaa authorization network command
R1(config)$ crypto map CLIENTMAP isakmp authorization list VPNAUTHOR

# Authentication as defined in the aaa authentication login command
R1(config)$ crypto map CLIENTMAP client authentication list VPNAUTHEN

# Assign the dynamic crypto map to CLIENTMAP
R1(config)$ crypto map CLIENTMAP 10 ipsec-isakmp dynamic DYNMAP

# Assign the crypto map to the outside interface
R1(config)$ interface f0/0
R1(config-if)$ crypto map CLIENTMAP
R1(config-if)$ exit
```

Check R1 IPSec configurations

```
R1$ show crypto isakmp policy

Global IKE policy
Protection suite of priority 5
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

```
R1$ show crypto map

Crypto Map "CLIENTMAP" 10 ipsec-isakmp
        Dynamic map template tag: DYNMAP
        Interfaces using crypto map CLIENTMAP:
                FastEthernet0/0
```

```
R1$ show crypto ipsec transform-set

Transform set MYSET: { esp-des esp-md5-hmac  }
    will negotiate = { Tunnel,  },
```

Client configuration

It is possible to configure:

- Windows clients
  - Download and install `VPN Cisco Client`:
    `http://intranet.ipleiria.pt/servicos/si/servicos_wiki/Paginas%20Wiki/VPN.aspx`
- Linux clients
  - Download and install `vpnc`:

    ```
    sudo apt-get install vpnc
    ```

Linux client configuration

Start `vpnc`

```
me@Linux:~$ sudo vpnc-connect
(...)
This algorithm is considered too weak today
If your vpn concentrator admin still insists on using DES
use the "--enable-1des" option.

me@Linux:~$ sudo vpnc-connect --enable-1des
Enter IPSec gateway address: 10.10.10.1                 # R1 IP address
Enter IPSec ID for 10.10.10.1: SALES                    # as specified in client configuration command
Enter IPSec secret for SALES@10.10.10.1: cisco123       #
Enter username for 10.10.10.1: vpnstudent               # as specified in username command
Enter password for vpnstudent@10.10.10.1: cisco         #
VPNC started in background (pid: 31258)...              # connection successful
```

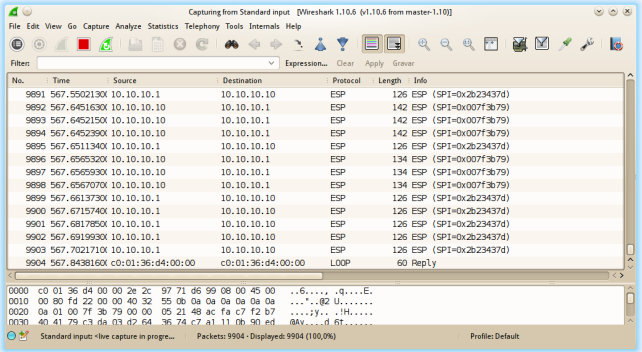
Note

This will route all your IP packets to R1, so you'll lose Internet connectivity until you terminate the IPSec tunnel!

Linux client configuration

Now, test configuration:

- view new `TUN` virtual interface: `ip a`
- test with `ping` from PC1 to R1
- then do `show crypto ipsec sa`
- capture packets with Wireshark



Linux client configuration

Terminate VPN connection

```
me@Linux:~$ sudo vpnc-disconnect
[sudo] password for me:
Terminating vpnc daemon (pid: 31258)
```

Create configuration file

```
me@Linux:~$ sudo nano /etc/vpnc/r1vpn.conf  # must end with .conf
```

```
Enable Single DES                    # write this line only if --enable-1des is required
IPSec gateway 10.10.10.1
IPSec ID SALES
IPSec secret cisco123                # NOTE the password is stored in plain text!
Xauth username vpnstudent
Xauth password cisco                 # NOTE the password is stored in plain text!
```

```
me@Linux:~$ sudo vpnc-connect r1vpn          # much easier now!
VPNC started in background (pid: 472)...
```

Exercise 1 – For the same network scenario

Set up an client-to-site IPSec tunnel between `PC1` and `R1` to protect all network traffic

Data confidentiality must be ensured by `AES 192` and authentication through the `SHA` algorithm. To authenticate himself, the user `ss` uses the password `xpto10`. The integrity of ISAKMP communications should be guaranteed by `MD5`, the confidentiality with `3DES` and and key exchange through the DH algorithm group `5`. The domain is `super-fun.pt` with group ID `IPLeiria` and key `IwantMore`.

For paramaters not specified above, use the defaults values.

Exercise 2 – Windows client

Repeat the previous exercise, but with a Windows client:

- by means of a virtual machine,
- or setup GNS3 on Windows and install a `Microsoft Loopback Interface`

Recommended reading

Cisco example:

- Configure Remote Access Using Cisco Easy VPN (available on Moodle)