FIREWALL

I - Objectives

In this lab we use a firewall to connect a corporate network to Internet. Several aspects are studied:

- Definition of the various corporate networks
- Routing and interconnection
- Installation of the translation rules
- Definition of the security requirements
- Supervision of the firewall and analysis of the logs
- Connection by virtual private Network (VPN) of remote clients

II - Presentation of the platform

1 - General description

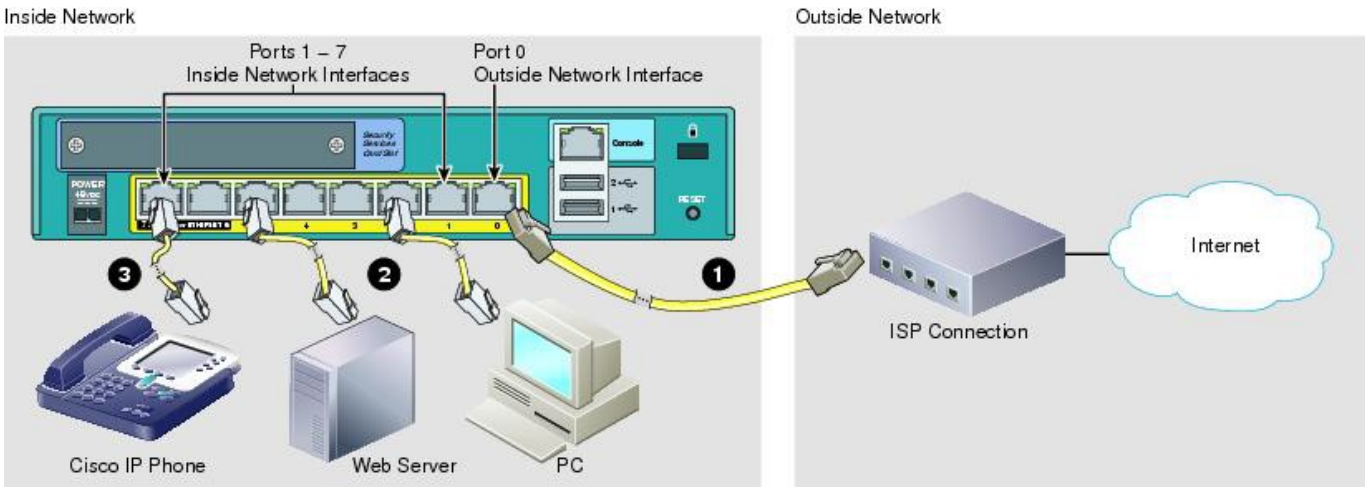
For this lab, you have:

- 2 hosts on a local area network
- 1 Web server host
- 1 external user host
- 1 CISCO ASA 5505 Firewall

You will need to use the following software (to download directly from Internet):

- Wireshark and Winpcap library: Software for the analysis of frames
- Kiwi_syslog: log server
- Putty: text mode console for telnet and SSH (Secure Shell) accesses

The ASA 5505 firewall come from the CISCO company. **CISCO** proposes several ranges of routers, switches and firewalls. The more recent firewalls are named **ASA Range 5500** (models 5505, 5510 ou 5515). ASA 5505 is the smallest model. The license used is the “Security Plus” license (see in the appendix the differences between the basic license and the “Security Plus”). The performances of this firewall allows its use in relatively large installations (tens of users). The price is about € 1000 without VAT with different licenses. On the rear panel, there are 8 ports, as you can see on the figure, from the Cisco documentation.

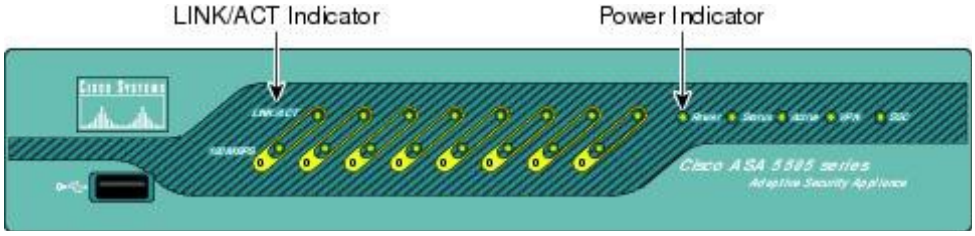


Port 0 will be used for **external** interface
Ports 1 to 7 are used to connect intern equipments
Ports 6 to 7 are POE compliant (IP phone or camera for example).
It's possible to set some VLANS on the internal switch, 3 for internal and external networks or for DMZ.
Notice the reset button on the right.

BEWARE : the power connector is very fragile !!!! Handle with caution.

The panel is classic, with LEDs to indicate different states. The system is installed with the firmware version 8.3.

The front panel equipment looks like this:

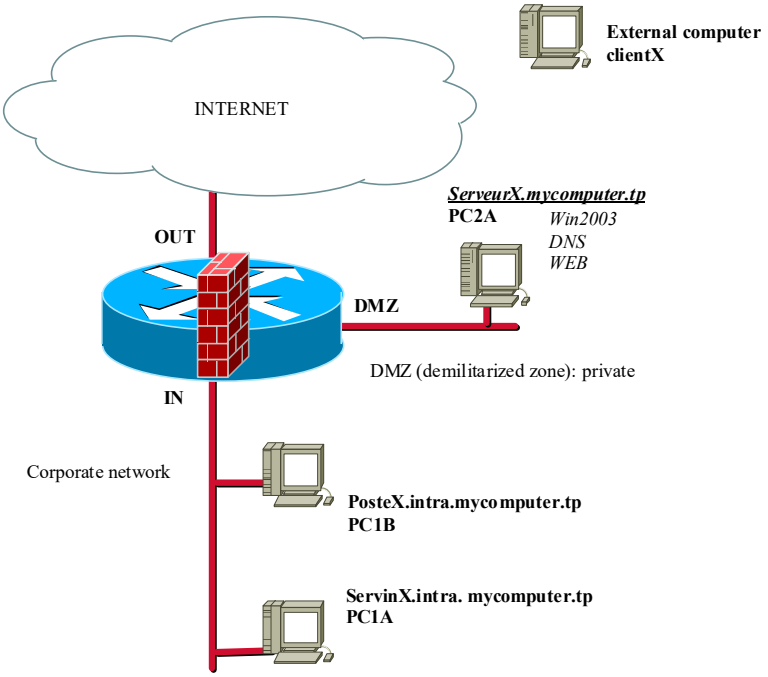


IMPORTANT REMARK:
We choose here a DMZ with a range of private address. This choice is good for understanding but not really interesting for a real installation. We will see why during the LAB.

The network address is the first address of a network. In our table, the public address is 152.77.65.192 / 26 and therefore the useful first address is 152.77.65.193 / 26

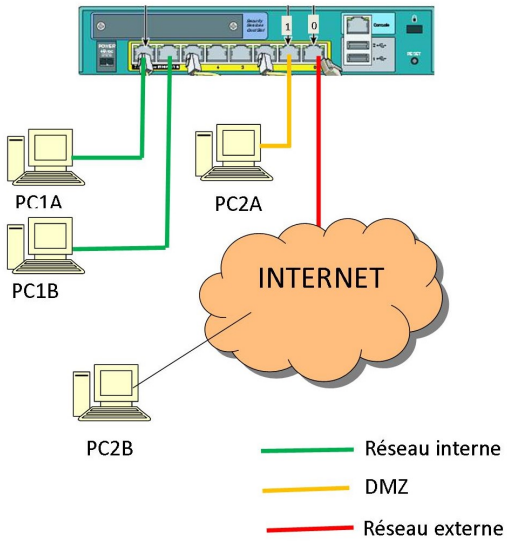
Whenever you see X in the part below, enter your group number (1, 2 or 3).

Name and IP addresses	Group 1	Group 2	Group 3
Mycompany	duchemin	durand	dupont
IN	10.1.0.0 /16	10.2.0.0 /16	10.3.0.0/16
OUT	**152.77.65.232 /26**	**152.77.65.234 /26**	152.77.65.236 /26
DMZ	172.16.1.0 /24	172.16.2.0 /24	172.16.3.0 /24
clientX external Post	**client1** **152.77.65.233 /24**	**client2** **152.77.65.235 /24**	**client3** **152.77.65.237 /24**
PosteX.intra.mycompany.tp	Poste1.intra.duchemin.tp	Poste2.intra.durand.tp	Poste3.intra.dupont.tp
servinX.intra.mycompany.tp	servin1.intra.duchemin.tp	servin2.intra.durand.tp	servin3.intra.dupont.tp
ServeurX.mycompany.tp	Serveur1.duchemin.tp	Serveur2.durand.tp	Serveur3.dupont.tp



2 - Installation of the network

Let's cable the network in accordance with the indications of the teacher.



The plan of room is as follows:

pc1A (**servinX**, internal DNS Server and Active Directory) is a Windows server and pc2A hosts (**serveurX**, Web and DNS server) is a CentOS server. Servers will be installed from Ghost images with Toto123 (or toto) as the password.

Optionnal : pc1B will be used as a client. Install the client with Windows 10.

pc2B will be installed in the same way as pc1B. It will be connected on the external network.

☝ De-activate Windows firewalls, because Windows firewalls prevent the computers to answer to pings.

III - Elementary configuration of the Firewall

1 - Basic configuration

a. Configure the administration tools of the Netasq Firewall.

On the USB key get Putty programm and copy it on your internal network computers (PC1A ou PC1B)
Use a console CISCO cable from a computer to the ASA. Then with « **putty** », with a « **Serial** » link, establish a connection to the device.

Here are the reset commands (please, no mistake when you enter the commands!!!!) :

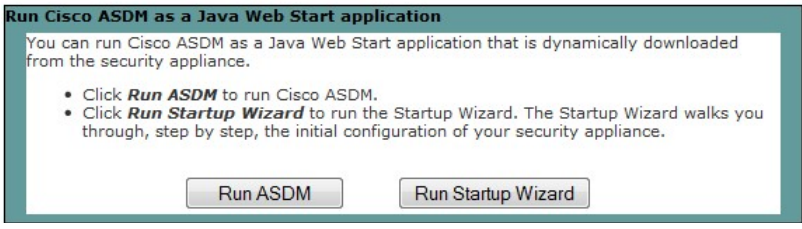
- **enable** (empty passwor or **Toto123**)
- **configure terminal**
- **clear configure all**
- **crypto key zeroize rsa**
- **revert webvpn all**
- **config factory-default 10.X.0.254 255.255.255.0**
- **reload save-config noconfirm**

Those commands reset the device to factory default parameters. The password is set and an IP address is configured for internal interface.

2 - First connection to the firewall:

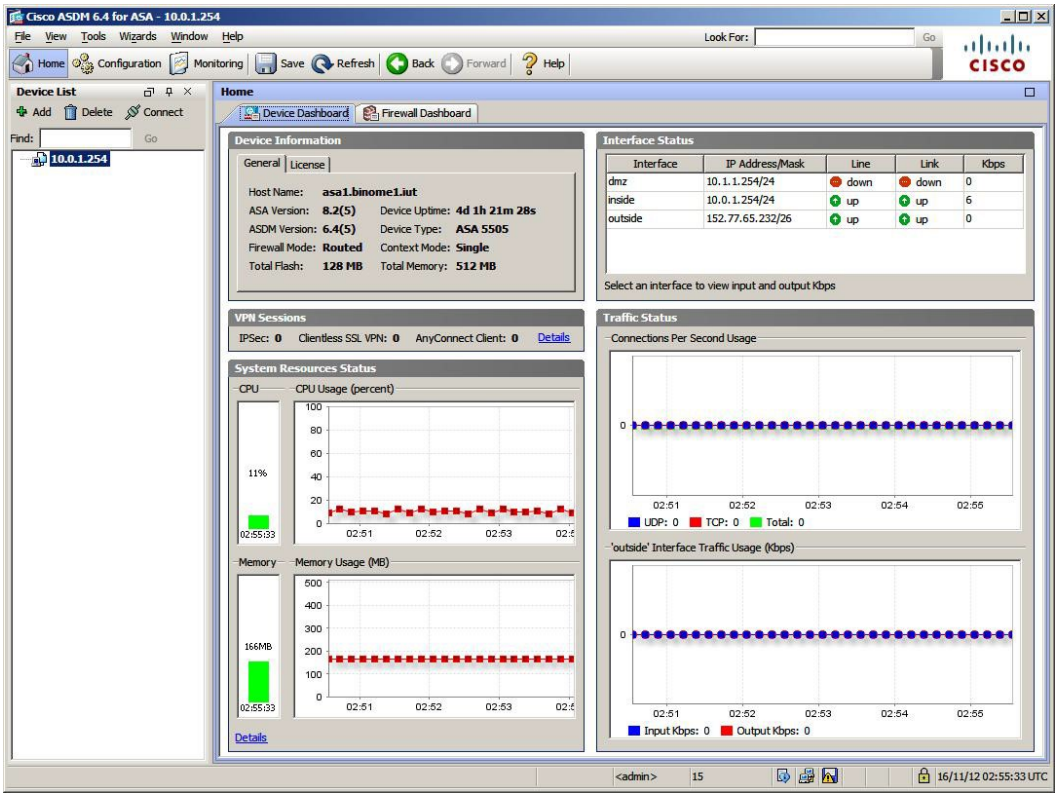
Now you had to install Java environnment on your computer. Get JRE.
Firewall is now reachable with a web browser to the address https://10.X.0.254 . ASA password is empty or Toto123.

Install the administration interface ASDM then Run ASDM (no account, no password or **Toto123**).

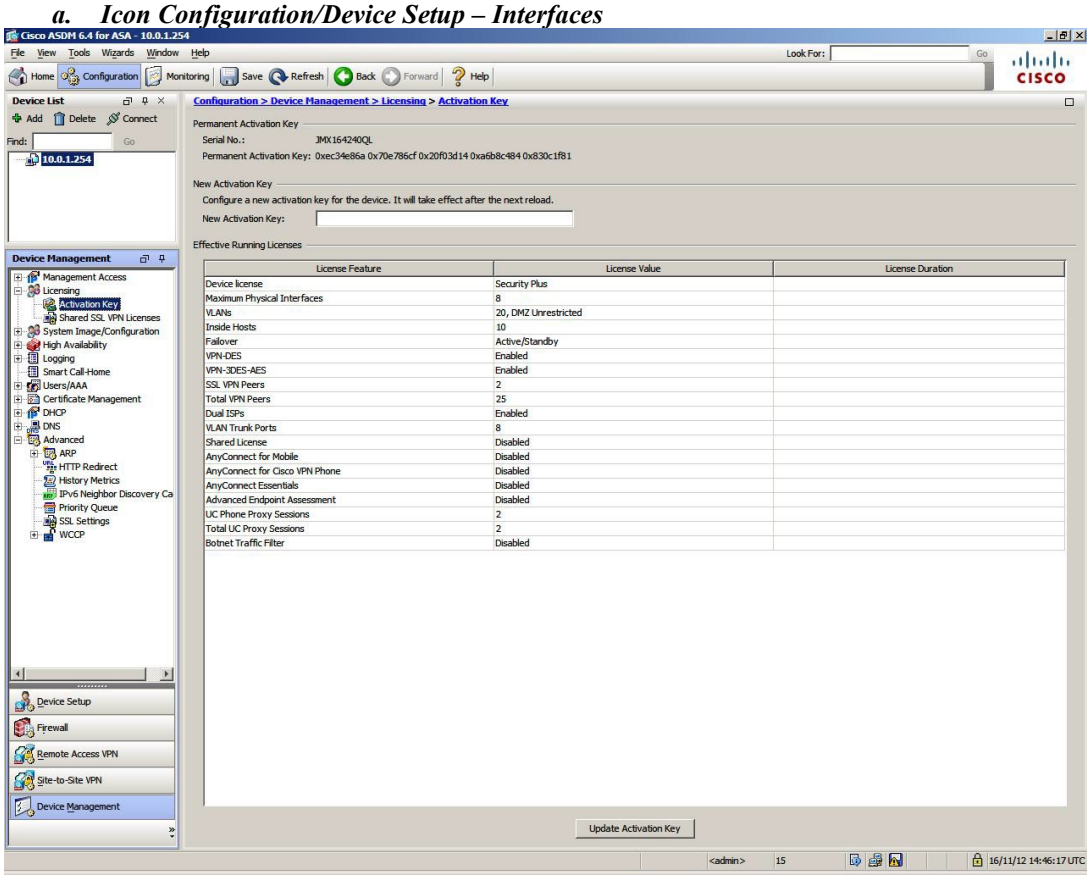


When you'll have the question « **Cisco smart Call home** », select : « **Do not enable Smart Call Home** ».

When you're connected you'll have this screen :



a. Icon Configuration/Device Setup – Interfaces

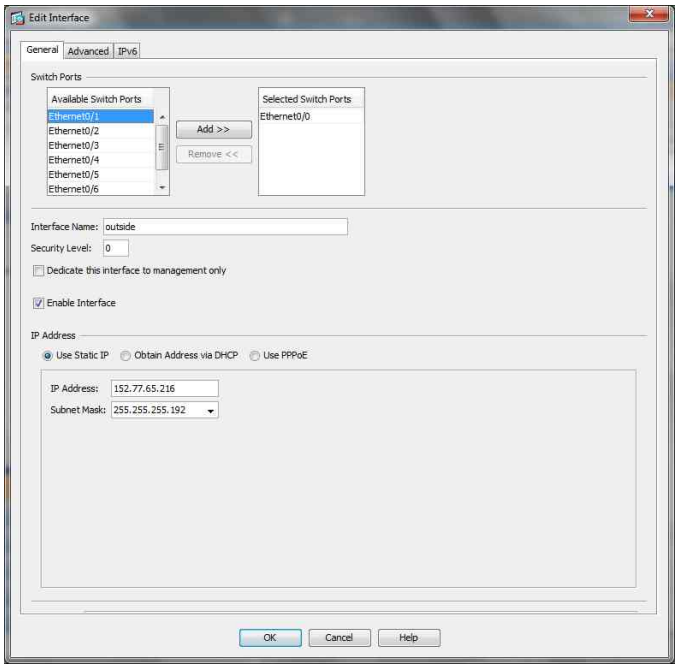


Init state :

- Ethernet0/0 interface is in Vlan 2, meaning on OUTSIDE network
- Ethernet0/1 to 7 interfaces are in Vlan 1, meaning on INSIDE network

We can now configure the interfaces :

- Interface Ethernet 0/0 is in OUTSIDE network
  - Select the interface then click on Edit button
  - Interface name must be outside an security option level set to 0. This is the trust level for this interface. 0 = untrusted
  - In IP Address, select « Use Static IP » Give an IP and a mask according to your team.



Click « OK » to validate the configuration, then change interface.

- Interface Ethernet 0/1 DMZ
  - Click « Add »
  - In menu « Switch Ports », select Ethernet 0/1 the click "Add"
  - Give it a name in Interface Name : DMZ
  - Set Security Level = 50
  - In IP Address, select « Use Static IP »
  - Give an IP address and a mask for your DMZ network

Click « OK » » to validate the configuration, then change interface.

- Interfaces Ethernet0/2 to 7 INTERNAL
  - Nothing more to do, interfaces were configured during init process
  - Notice Security Level is 100, the maximal value.

Apply configuration with "Apply" button.

☝ Save the firewall configuration from time to time.

b. Icon Configuration/Device Setup – Routing

- Have a look to the sub menu routing
  - Select StaticRoutes then « Add »
  - Select external interface
  - We want to set default network route, Network should be set to « any »
  - All the traffic had to be sent to UJF router on IP address 152.77.65.254
  - Click « OK »
  - Click « Apply »

c. Icôn Configuration/Firewall - Objects

Examine the different tabs available and preset values.

- Menu « Objects » then « Network Objects/Groups ».

For each server add an item. We can set an item for each service even if it's on the same computer (For example define : Serv_www and Serv_ftp with the same IP address)

i. Define **Serv_web**, **Serv_ftp**, **Serv_dns_dmz** and **Serv_dns_intra.**
ii. Define Syslog machine **Serv_syslog** with IP address 10.X.0.1

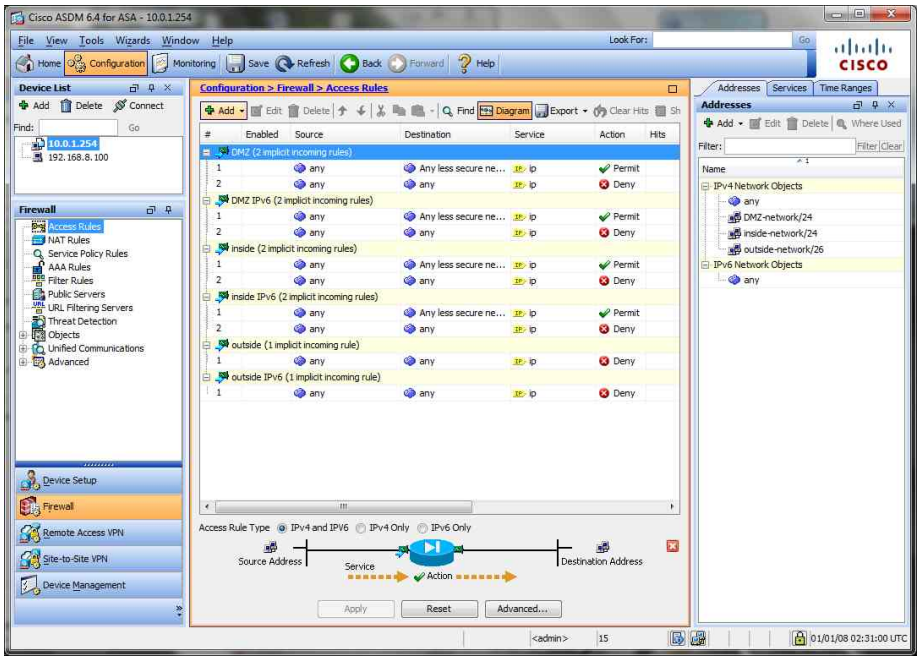
You add to create a device "router_ujf" with address 152.77.65.254 and on the main tab "routage", click on button and set it to "router_ujf".

d. Icon Configuration/Firewall – NAT Rules

- Create a rule allowing all internal network users to access Internet network.
- You had to had a NAT rule NAT for the entire internal network and also for DMZ network.
- By default, a NAT rule is set for internal network, create one for the DMZ.

e. Icon Configuration/Firewall – Acces Rules

- By default Cisco firewall allows all IP traffic from an interface with a high « Security Level » to another interface with a lower level.



In this state, internal network computers should connect to DMZ computers or Internet.

☞ See in appendix the various possibilities of address translation:

VALIDATION	- Hosts communication between them, and outside (for example towards 152.77.24.211) -

IV - Hosts configuration

1 - Servers configuration

a. Configure the Intern 2008 server.

- Configure the network:
  - Address IP: 10.X.0.1 /16, Gateway 10.X.0.254, DNS: 127.0.0.1,
  - host name **servinX.intra.mycompany.tp**

  Select **Start** => **Server Manager** to change the name of the computer
  With **X = 1 or 2 or 3** as a function of your group

- We will add the roles DHCP server, DNS server and active Directory with your server: (programs/tools of administration/ managing your server - *programmes/outils d'administration/gérer votre serveur*) (TAKE CARE! Not to use the default configuration and to prefer an installation of each element respecting the following order…)
  - Install first the DHCP Server role
    - Extended / *étendue*: **etendueX**
    - Range of addresses / *plage d'adresse* **10.X.0.100 to 10.X.0.255 /16**
    - Router / *routeur* **10.X.0.254**
    - Parent domain / *domaine parent*: **intra.mycompany.tp**
    - DNS: **dns.intra.mycompany.tp** (IP: **10.X.0.1**) DNS will be an alias for **servinX.intra.mycompany.tp**
    - Manage DHCP server and (in the action menu) authorize it to deliver addresses.

  - Add the controller role for the Active Directory domain.

Click in **Start** => **Execute =>** then write **dcpromo, then the installation will be automatic** => Click **OK**
Then you can follow the steps provided by the user interface:

- It is a new domain in a new forest.
- The domain will be called **intra.mycompany.tp**
- Choose authorizations in conformity with a Windows2008 model
- Validate the following proposals.
- Give a password for the restoration mode (choose toto)

- (N. B. One can open here a “mmc” management console and put inside the various utilities “DHCP”, “DNS”, “Events observer / *Observateur d'événements*”, “Active directory”…)

Note : Check the constraints regarding passwords and check their lenghts.
Netbios name = servinX
Forest root domain name = intra. mycompany.tp

At the end of the installation, the *Additional Domain Controller Options* page will appear, select the checkbox that appears and click **Next** for the installation to complete.
Then restart the system

- Install the DNS server role. (2008 server CDROM necessary)
  - Create a direct zone and a reverse zone (*zone inverse*) (principal zone): intra.mycompany.tp
  - Authorize the dynamic updates (*mise à jour dynamique*)
  - Create the reverse zone **X.10.in-addr.arpa**
  - Redirect the requests to the DNS server (in the DMZ) **172.16.X.1**
  - The server will not be able to find roots for the moment; please note the error message.
  - In the direct zone, give an alias to the **servinX** host (alias: **dns.intra.mycompany.tp**)

- In the Active Directory user database
  - Create an account **Albert Legrand**, login **alegrand**, password **Toto123** (a too simple password is refused by the system)
  - The study of Active Directory is a very large subject which will not be tackled today.

b. Configure the Serveur.mycompany.tp server.

On the Linux server in the DMZ, we are going to install A DNS and web server

- Configure the network:
  - Address IP: 172.16.X.1 /24, Gateway 172.16.X.254, DNS: 127.0.0.1,
  - Name of host **serveurX.mycompany.tp**

Install webmin from the USB key rpm –ivh webmin-XXXX.rpm

Some dependencies may be required (Perl SSL Lay)

Add the DNS server (Create a direct and reverse zone) : maboite.tp

Yum install bind
With webmin create the reverse zone **X.16.172.in-addr.arpa**
Forward the inside DNS traffic from the inside DNS server server to this one : **152.77.24.211**
Service named start

Configure the WEB server.

- Yum install httpd
- The server must be listenning on the IP address not the local one /etc/httpd/conf/httpd.conf ligne Listen 80
- Service httpd start

Configure iptables (pare-feu linux /etc/sysconfig/iptables) we want :

- DNS and web services reachable from inside and outside
- Webmin (port tcp/10000) and SSH services only reachable from the inside networkExemples iptables :
  -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
  -A INPUT -p tcp -m tcp --dport 53 -m state --state NEW -j ACCEPT
  -A INPUT -p icmp -s 213.251.184.9 -j ACCEPT
  Man iptables

Test locally that every services are running

2 - Configuration of the client

a. ***Configure XP PosteX host.***

b. ***Configure*** *PostX* ***(where X=1 or 2 or 3) using DHCP and recover its configuration*** *by ipconfig /renew.* ***(****Start* **=>** *Execute* **=> then type** *cmd* **=> Click** *OK* **to see the command interface)**

To change the name to posteX, domain and input of **alegrand** account **,** Click **Start** **=>my computer => system information**.
Integrate the host to the Windows 2008 domain.

Note : something like this will be needed **INTRA\alegrand** then the password **Toto123** (what is the name of this domain?). Note problem that may arises due to difference in French and English keyboard.

-

c. ***Then, after rebooting, log under the alegrand account.***

V - Security configuration (Step 1: pings and Web)

Note: You will always have to use the real host addresses even if the address translation is implemented.

Editing rule for each services could lead to hundred lines configuration code. To avoid this it's possible to create some service group objects and they are really usefull. We can by example creat a group with all web fonctions, or mail…

d. ***In*** *Configuration/Firewall/objects/Services groups*

- Create a group **services_intra** used by internal network users and add in http and https services, outside FTP access.
- Create a group **services_dmz** with the same properties.

e. ***Allow access from internal to outside.***

i. For service group **services_intra**
ii. For outside ping

f. ***Allow access from DMZ to outiside.***

i. For outside ping (not to internal network)
ii. For service group **services_dmz.**

QUESTION :
At this point, logically, with the security rules set, it shouldn't be possible to connect to the configuration tool, but it still works. What do you think ?

Security configuration (Step 2 : DNS)

Allow internal network computers to ask for a name resolution
Attention ! Those computers must user **servinX.intra.mycompany.tp** as DNS server.
ServinX.intra.mycompany.tp must redirect request to **dns.mycompany.tp**

It could be necessary to set up some debuging tools for exemple :
On DNS servers, activate logs (we will write logs in c:\logs\dns)

You also could download and install **Wireshark.**

NOW, all computers should access to the web – Call for a rules control !!!! Be sure to set **router_ujf** as the firewall default gateway.
VALIDATION - show "mmc" interface - show PosteX configuration (user, IP) - show that it's possible to ping domain names like mycompany.tp, intra.mycompany.tp

VI - Implementation of the logs of the Firewall - Monitoring

1 - Use of syslog

It is particularly useful thanks to a Firewall to be able to supervise its activity for the detection of attacks or for reasons of maintenance and debugging. The most traditional solution consists in using a logs server.

The Firewall will send the logs on the **serv_syslog.intra.mycompany.tp** server.

a. Syslog client configuration (on the firewall)

- On the firewall (Tab Configuration/Device Management/Logging/Syslog Servers), ask the logs to be send to an external log server (**servinX.intra.mycompany.tp)**. Log the maximum informations. Remind port number.

b. Syslog server configuration (on the Firewall)

- Install on **servinX.intra.mycompany.tp** « KIWI Syslog Daemon » (Download on the web).
- Install and configure (setup menu).

Check that the logs are posted in real time on the console of the server.

2 - Montoring from ASDM

In Cisco ASDM click on « Monitoring » then « Logging ». Select « Enable Logging » then « OK ». Click on « View »
We can now see all the connection crossing the firewall in real time.

- The reporter displays then the contents of the various logs files. Examine for example what are the packets refused by the Firewall (Which rule is responsible for that?).

This tool is very convenient for debugging and to monitor the Firewall.
N.B. Because of the existence of a proxy (port 3128) to reach the Internet (in some cases), it will be necessary to create and use a proxy "object".
Propose filtering rules allowing to join the UJF proxy server **(www-cache.ujf-grenoble.fr**).

for checking, prove the functioning of a rule using the reporter.

VII - A little further with the Firewall

1 - Implementation of the URL filtering: (Slots /WEB)

The preceding security rules were configured at the level of the third and fourth OSI model-layers. Specialized Firewall such as ASA 5505 offers also possibilities of filtering at the application level, by analysis of the messages exchanged at the highest layers. We will now remove the traffic from the Internet on port 80 which is not the real http traffic..

Go to "Configuration / Service Policy Rules" then use the button "Add". Select the appropriate interface (we will inspect traffic from the interface “inside”) and click "Next". Select the inspection of all the traffic, then click "Next." Now we will apply the inspection rules for the HTTP traffic, the "Configure" button is active, click. Now it is possible to define rules for a more advanced filtering. Choose the definition of custom rules and look through the menus the various possibilities. We note for example that it is possible to block traffic from peer-to-peer applications trying to use the port 80.

2 - Translations of destination addresses (« Configuration/Firewall/Nat Rules »)

We already saw how to allow the users of internal networks to have access to Internet. We will now see how to give the external world access to our Web server.

The access will be achieved for the external users thanks to a connection to the site 152.77.65.193 or 152.77.65.194 or 152.77.65.195
The router will be then charged to redirect the connection onto the internal server.

- Using the documentation of the Firewall, add the relevant rule in « Configuration/Firewall/NatRules »

- The public address of the Web site is 152.77.65.193 or 152.77.65.194 or 152.77.65.195, we would like to be able to give this address to the internal users, in particular through the DNS system. But a problem arises: Can an internal user reach the site through this address? Why?

We will correct this default, re-route the internal requests for the Web server 152.77.65.193 (or 194 or 195) towards the DMZ Web.

-
- Use a redirection to carry out that. (Be careful with the choice of the interface on which the redirection is carried out).
- Update the **DNS server of the DMZ** so that the server is accessible from the internal network by **www.mycompany.tp.**

Is it possible to make functioning the DNS resolution for the external users? Why?

3 - Configuration of the attack detection

ASA 5505 can block hosts attempting DoS or Scan type attacks..

a. Study of the ftp case.

By using a client host on your network, check in Internet Explorer that the client is configured in passive mode.
On the Firewall, de-activate the ftp plug-in of the ASQ.

Try to connect to the ftp://ftp.gtrgrenoble.fr site
What's the matter?
Reactivate the ftp plug-in. Check that ftp functions again. **Explain.**

b. Study of the HTTP case.

A lot of attacks take place by buffer overflow on the Web servers.
An unforeseen character string, (generally long) is sent to a form in order to starts an operation which is not in conformity of the server. To avoid this, it is possible to configure the Firewall to limit the size of a URL which passes on the network

- Start the Web server on the server host.
- Check that this server is accessible from the internal network.
- Configure the HTTP plug-in to limit the size of URL to 128 bytes.
- Then consult the following URL: http://172.16.X.1/123456189123456789 (sequence 123456789 to be repeated about fifteen time)
- Consult the logs and note the generation of an alarm.

Other Plug-in allow specific actions, in particular the checking of the conformity of the messages with RFCs.

VALIDATION
- Provide a convincing explanatory diagram of the functioning of the ftp plug-in.

- Show URLs filtering
- Show the access towards the DMZ web server from the outside, and the relative rules (translation, filtering).

VIII - Implementation of a VPN tunnel (pptp.)

There are several types of VPN:

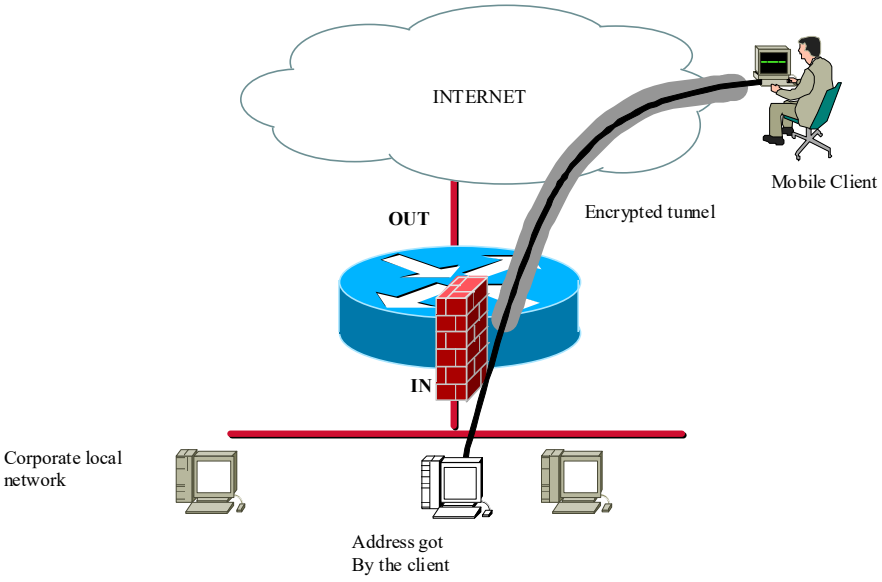
- site-to-site VPN
- VPN to provide access to a remote client so that it can access to the corporate network

Let's start with this second type of VPN, several possibilities have emerged since the introduction of VPNs:
- PPTP (Point to Point Tunneling Protocol) VPNs, are very simple to implement, but the level of security remains very basic. The advantage is the simplicity of implementation and the compatibility with many devices. PPTP was developed by Microsoft and comes with Windows systems from Windows 98. All Microsoft computers can natively establish PPTP connections. We will not use PPTP in this lab, the ASA firewall allows more interesting and much more secure configurations.
- L2TP VPNs, much more secure when used with IPsec (called tunnel L2TP/IPSec): they combined Cisco L2F and Microsoft PPTP protocols. They are quite more difficult to implement.
- SSL VPNs (also called VPNSSL). In this case, it is possible to use a dedicated client (Cisco Anyconnect in our case) or just a recent web browser. The possibilities can be really interesting if we use more advanced configurations, as we shall see.

Start by using VPNSSL:
Clientless ... so without dedicated client. The connection is done through the browser on the external host. The VPN connection will be allowed or not depending on access policies defined on the ASA. These strategies are applied to users:

- present in the ASA local database accounts
- configured on a server: in this case, the link between the ASA and the server can be done through several methods. Three methods are presented here:
  - Querying a local database accounts on the ASA
  - Querying the LDAP domain controller
  - Querying an authentication server, based on the RADIUS protocol.

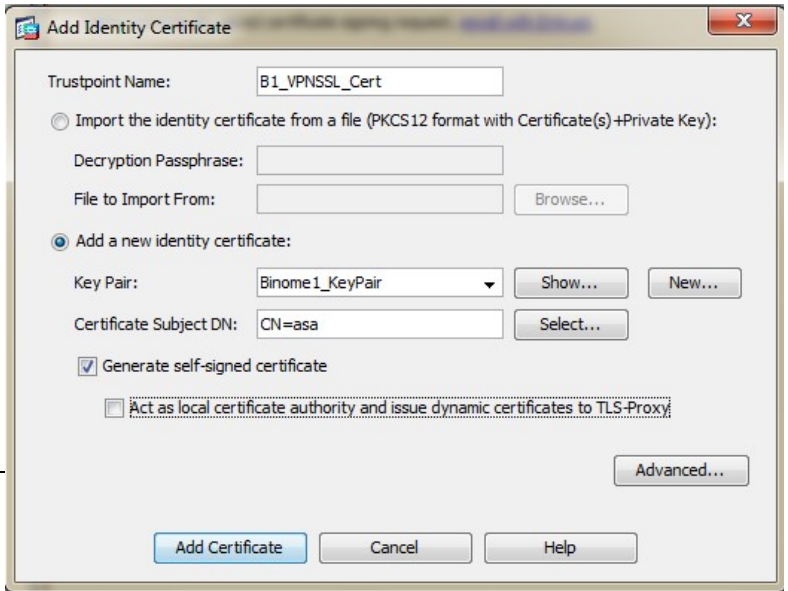
Start with the case of a local database



Step1 : Creation of a Certificate

SSL connections require the exchange of public keys through certificates. We need to configure and take care of the certificate used in SSL connections.
Let's create a certificate for this type of VPN .
In " Device Management ", " Certificate Management ", " Identity Certificates ". On the right there are two possibilities:

- Create your own certificate , which is not recognized as being issued by a certification authority



known by conventional browsers, but that will cost us nothing

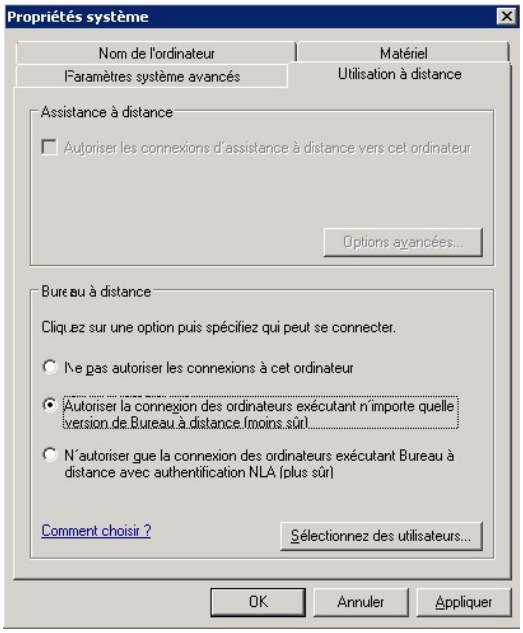
- go through a recognized certification authority (CA)..

Click on « **Add** », then, generate a new paris of keys (« New »), called « **BX_KeyPair** ».
Then enter on the top the name of a certificate (« **BX_Cert** »), select « **Generate self-signed certificate** » and click on « **Advanced** ». FQDN should have the value « **asa.binomeX.iut** ». Let the other fields empty. Click « **Ok** » then come back, then « **Add Certificate** ». Show the number of years of validity of the certificate.The certificate for our tunnels (among which the SSL tunnel), is ready. Let's continue the configuration steps.

Step2 : Preparation of the home page.
In "Remote Access VPN", "Clientless SSL VPN Access", many configuration options are available, two of them are called "Portal" and "Customization". The general idea is to offer a home page for users arriving via an SSL tunnel, giving them the choice of access to various servers: FTP, Windows, SSH and RDP (graphical connection to a Windows server).

Find how to provide users an access to shared data in the Active Directory server.

Creation of a local account and a strategy for this VPN.
Among the wizards « **Wizards** », « **SSL VPN Wizard** » select « **Clientless SSL VPN Access** », create a connection profile named « **BX_Profile_Connexion** », interface « **Outside** », using the certificate generated previously (figure on the right)
Locate the URLs to access the tunnel. Next step: indicate that you are going to use a local account you will have to create. The account will be named **USERSSL** (password **USERSSL**). Next step: create a new "Policy Group" named "**VPNSSL_PolicyGroup**."



Finally, the next step is to add our list of bookmarks.
The VPN is working, but first, a correction on the **USERSSL** account should be done. Check by editing this account (in "**AAA / Local Users**", "**Local Users**") the access rights granted to the account. We don't need the account to have a full access, so we will select "**No ASDM, SSH, Telnet or console access**".
Before testing on the 2008 server, log in as admin ("**BINOMEX \ Administrator**" after the installation of AD) and right-click on the "**Computer***/Ordinateur*" icon, then "**Properties***/Propriétés*".
The figure on the right shows you what to do to accept RDP sessions.

Test the good functioning of your VPN from the client browser, using the address **https://@ IP_externe**. Of course, the certificate presented is not recognized as trusted by the browser. Accept it. You can then edit the certificate sent and visualize the data of this certificate.
Accept its use, and you get the desired home page.

Port Redirection
Port redirection is another interesting possible improvement: it is for example possible to give an external host an remote access to a desk on the AD server.

To achieve this, the operations are very simple on the ASA:
In " **Remote Access VPN** ", " **Clientless SSL VPN Access** ", " **Portal** ", " **Port Forwarding** " , add a new list named for example " **BX_Ports** ."
In this list, add the redirection of the local port 10000 towards the port 3389 (port used by RDP) of the 2008 Server. Let's save the configuration.
With "**Assign**", apply the port redirection to the Group Policy " **VPNSSL_PolicyGroup** "
Save the modifications. Log back from the client. Sometimes the connections no longer work: it could be due to wrong disconnections which prevent new connections, because the quota has been reached.
In this case, "**Monitoring**" , "**VPN**" , "**VPN statistics** ", " **Sessions** " then filter the connections " **Clientless SSL VPN** ". Remove the old connections.

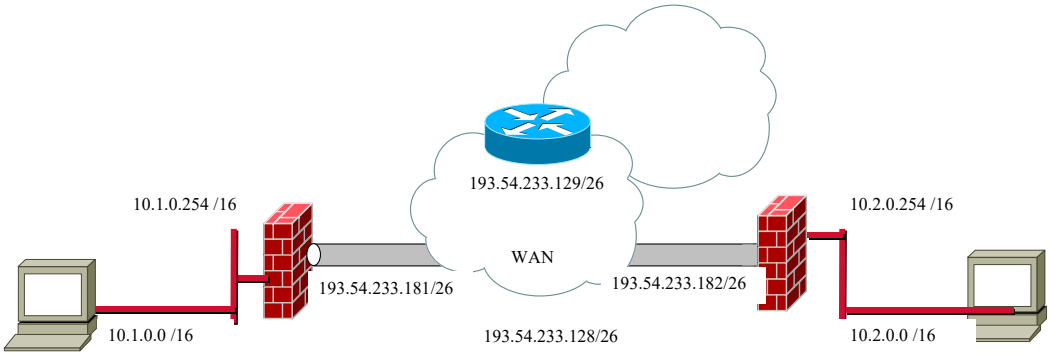
Once connected from the client, choose " **Application Access** " " **Start Application** ". The port redirection is working. Test from the " **Remote Desktop**/*Bureau à distance* " tool the RDP connection to the server . It is fully operational.

VALIDATION	- Functioning of the SSL tunnel.

IX - Interconnection of sites with a VPN IPsec tunnel

The objective is now to inter-connect the two private local area networks of the two sites of the two student groups through a protected tunnel. Through this tunnel, all the communications will be authorized.
The mechanism of security implemented is called IPsec. The principle consists as for PPTP in negotiating the security parameters, then to build an encrypted tunnel. However, IPsec has much more possibilities and is consequently more complex. (See course on security).
We will set up the following architecture in which the two networks preserve their usual access to Internet but will have to pass by the tunnel to communicate together directly.

We will build initially an IPsec link with pre-shared keys. In this mode, a secret password known from the two ends will be used for the mutual authentication.



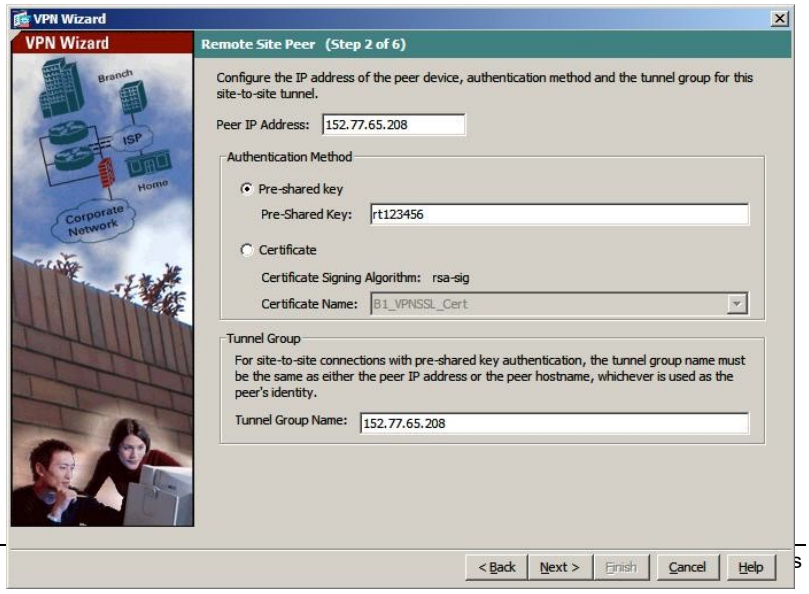
Several stages are necessary:

- Define the pre-shared key:
- IPsec being held in two phases, define the parameters of negotiation of phase 1 then those of phase 2
- Modify the routing and filtering rules to authorize the communication of IPsec flow.

Create first the following objects:

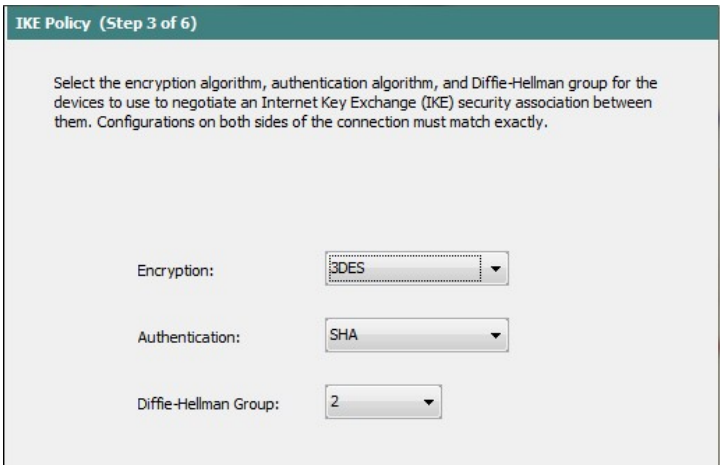
- **Firewall_distant** (public address of the other firewall)
- **Distant_network** (distant internal network)

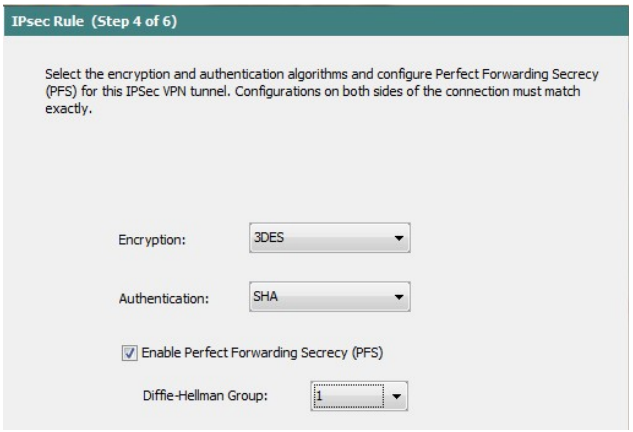
In « **Configuration** », « **Firewall** »,« **Objects** »,« **Network Objects/Groups** ». Click on "**Add**" then select « **Network Object** ».
Let's consider Y as the number of the remote binomial of students.
Enter the following information: name "**Reseau_BY**", IP Address « **10.0.Y.0** », Netmask « **255.255.255.0** ».
Don't forget to apply the modifications at the bottom of the window « **Apply** ». In the menu « **Wizards** », select the element « **IPsec VPN Wizard** ». Select « **Site-to-site** », then « **Next** ».
In the second window, you will give the address of the remote host with which you will create the tunnel. Insert a shared key "**rt123456**."



Perform a ping to the remote network. Normally it should work. Because of the time of establishment of the tunnel, it is possible that the first packet is lost.

CAUTION , you must have the same key on the other side of the tunnel. Do not touch the " **Tunnel Group Name** " proposed by the Wizard.
The next two steps are used to select the encryption protocols and authentication methods. Indeed, the use of IPsec implements two distinct phases.
- The first phase allows the recognition of the two entities exchange information and set up a first encrypted tunnel. The protocol used is called IKE (Internet Key Exchange). The choices here (3DES , SHA and Diffie -Hellman Group 2) are safe choices.
For information, the Diffie -Hellman algorithm allows the two entities to exchange a key in ensuring that only those two entities know the key exchanged (use of signatures) .
- The second phase is based on two protocols:
o The first protocol is called AH (Authentication Header), it can confirm with certainty the identity of the participants in the tunnel. AH does not encrypt data.
o The second protocol is called ESP (Encapsulating Security Protocol) which encrypts the data it two possible modes , tunnel mode is the most secure.
Many articles explain in detail these protocols. For more information on the encapsulation mechanisms for these protocols you can consult the article in the following site:
http://www.securiteinfo.com/cryptographie/IPSec.shtml
These protocols are configured by the following two steps : Leave the default values and click next. (Note that it is recommended not to use DES and MD5 (less secure because of the shorter sizes of the key for DES or of the hash for MD5) , and prefer to use 3DES , AES, Blowfish , SHA and other protocols available).





In step 5, select your local network and the remote LAN.
Let the last line checked. It allows not to NAT the addresses in the tunnel.
"**Next**"
In step 6, a summary of the configuration is presented. Check that everything is correct and click on **finish**.
In "**Site-to-Site VPN**" "**Connection Profiles**" look at the created profile, named from the IP address of the remote ASA. Check that it is "**Enabled**".
Take the opportunity to have a look on what the "wizard" recorded in "**Tunnel Group**" and "**Crypto Maps**".
This is where the different parameters and algorithms have been placed. In "**ACL Manager**", you can see that some rules have been added. Which ones?
TESTS
Now the **two extremities** of the tunnel have been configured, let's test if it works.

Test 1 : From your Windows server, send a ping towards the server of the other binomial of students. Observe at the same time the logs of the ASA (« **Monitoring** », « **Logging** », « **View** »). We can see that the packets are not authorised. Which ACL is blocking the icmp packets?
In the menu « **Tools** », select « **Packet Tracer** ». Chosse the « **inside** » interface, packet type : « **icmp** », source « **10.0.X.1** », destination « **10.0Y.1** » type « **echo** », code « **0** » ID « **1** » then click on « **start** ». See the blocking.

Test 2 : Test an RDP connection towards the server of the other binomial of students.

X - Internal mail service (Optional)

We will set up a simplified mail service at the DMZ level.
It will not be possible to receive e-mails from outside because the DNS does not allow it; but it will allow the exchange of messages through the Intranet.

Installation of the e-mail server on **serveurX.mycompany.tp**

- Manage the mail service server role (*rôle serveur de messagerie*)
  - For the authentication method, we will choose “local Windows accounts, to require the authentication by protected password” (SPA) ("*comptes Windows locaux, exiger l’authentification par mot de passe sécurisé"*) and “always create an associated user” ("*toujours créer un utilisateur associé*")
  - The managed domain will be **mycompany.tp**
- Create two e-mails boxes (**alegrand**, password **monmail**) and **bdupond**, password **monmail**.

Configuration of the client on the posteX host.

- Configure Outlook express with two distinct identities (alegrand and bdupond).
- Set up the security.

Test the sending of an e-mail from **bdupond** to **adurand**.

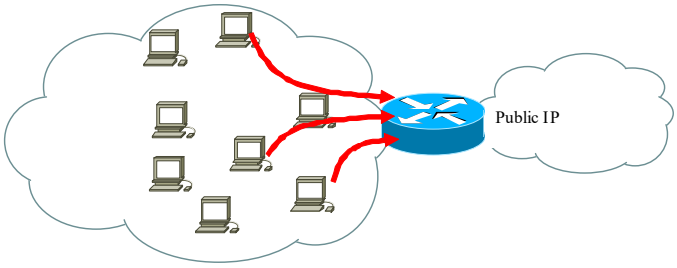
XI - Appendix:

1 - address translations.

The use of ranges of private addresses is an element of flexibility and security in the design of corporate networks.
But it is necessary to convert the private addresses into public addresses or reciprocally to allow the hosts of the private networks to communicate with outside. This is called address translation.

According to the context, various types of address translation will be used. Note that the terminology used can vary, depending on the manufacturers. We use the Netasq terminology here.

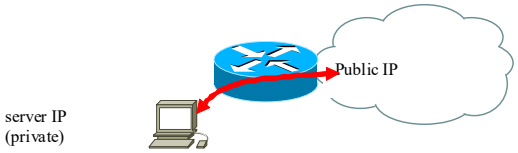
one-way address Translation (*Translation d'adresse unidirectionnelle*).
This type of translation is used to give the possibility to all the hosts of a network to have access to Internet



The hosts of the local area network use the common public IP address as the virtual address.
The connections are done at the request of an internal host. No host of the LAN can be contacted from outside.

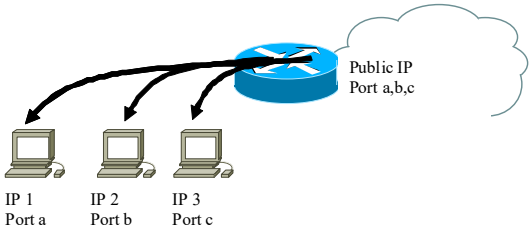
Original	Relocated
IP Address on the Internal network	public IP Address

bidirectional address Translation (*Translation d'adresse bidirectionnelle*):
The bidirectional address translation allows converting an address into another one. This is achieved at the time of the crossing through the firewall whatever the source of connection is. The bidirectional translation is generally used to give access from the outside to a server located on the private network of the company.



Original	Relocated
public IP Address	real server IP Address

Redirection of port
The redirection of port allows redirecting a couple (IP, port) towards another couple (IP, port). Thus various types of requests arriving to a public address (WEB, E-mail etc) could be redirected towards distinct servers and ports freely selected by the administrator.



2 - Comments on PPTP:

Generic Routing Encapsulation GRE (Rfc 2784)

The GRE tunnel allows encapsulating any IP network protocol (third layer of the OSI model). In practice, it is often used to set tunnels on IP networks.

<table>
<tr><td></td><td></td><td></td><td></td><td rowspan="4">IP Header</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>N°Proto</td><td></td><td></td></tr>
<tr><td colspan="4">@IP source</td></tr>
<tr><td colspan="4">@IP destination</td><td rowspan="4">GRE Header</td></tr>
<tr><td colspan="2">Flags</td><td colspan="2">Encapsulated Protocol
0x800 :IP
0x880B : PPP</td></tr>
<tr><td colspan="2">DATA length</td><td colspan="2">N°Session</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgement Number</td><td rowspan="2">Encapsulated Protocol</td></tr>
<tr><td colspan="4">.
.
.</td></tr>
</table>

It can be used to inter-connect networks with non routable protocols (Netbeui), private networks, networks other than Ipv4 (it is possible for example to connect two IPV6 networks through a GRE tunnel).
GRE allows neither authentication of the ends nor ciphering of the data.

In the example of the lab, the carrying protocol is IP, but other protocols can be used, in particular PPP in the case of a connection by modem. Take care not to confuse this connection with the PPP transport used inside the tunnel.

XII - PPTP Tunnel (Not to Point Tunnel Protocol) RFC 2637

PPTP is a protocol which allows building tunnels using PPP sessions above a GRE tunnel.

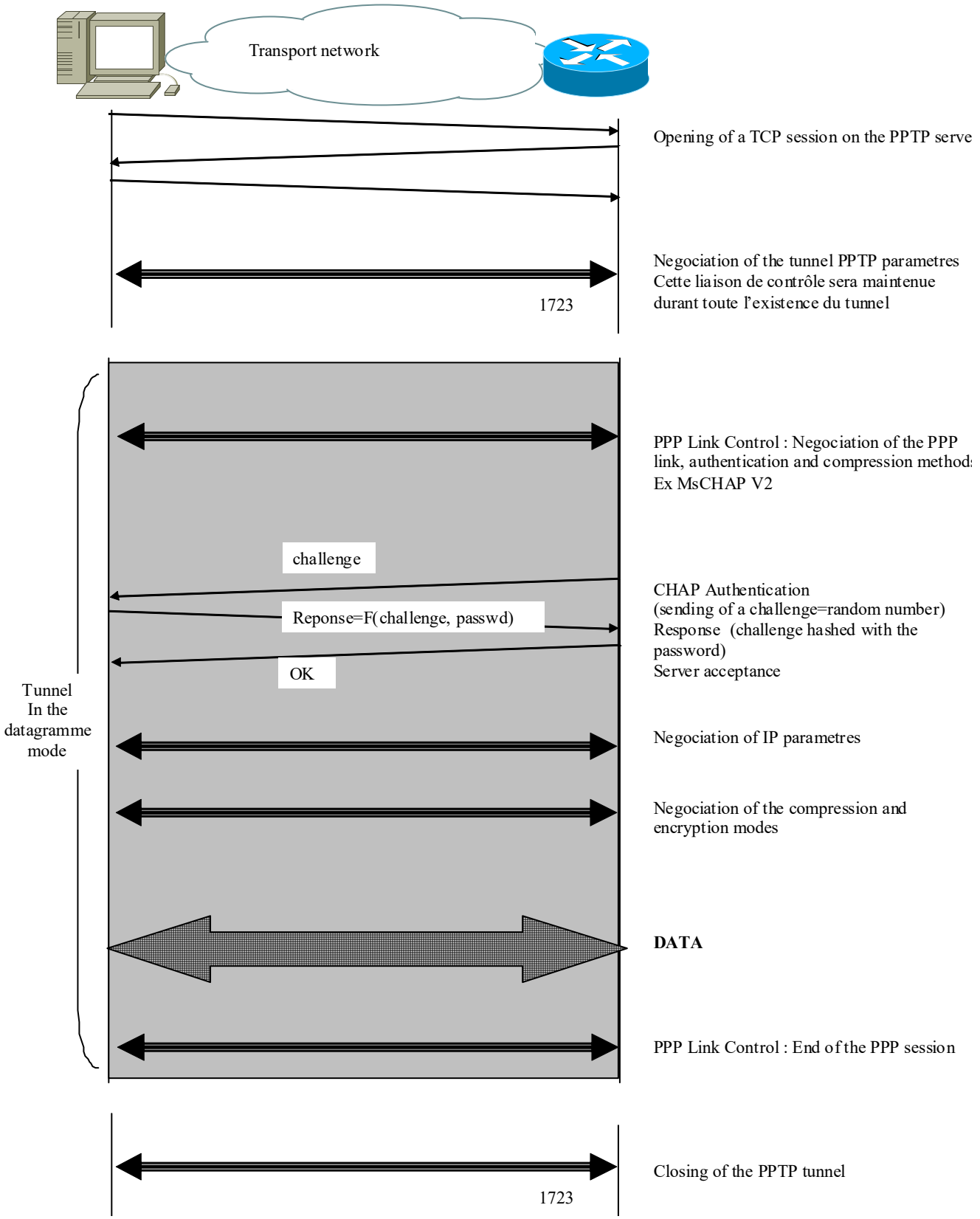
- The GRE tunnel extended for the transport of PPP datagrammes
- A TCP session allows controlling the tunnel

Neither the TCP connection nor the GRE tunnel is secured.

Two protocols respectively manage the authentication and ciphering: MS/CHAP and MPPE.

MS/CHAP is an extension of the CHAP (Challenge/Handshake Authentication Protocol) protocol already largely used to authenticate PPP connections between the clients and their ISP. This protocol gives the possibility not to send ciphered names of users and passwords.
Microsoft decided to add its own extension. Take care, there are some differences between classical CHAP and MS/CHAP protocols.

With regard to the coding of connection, protocol PPP did not offer any facility of this type. MPE or Microsoft Point-to-Point Encryption thus was born. This one uses an encryption algorithm RC4 into 40 or 128 bits.


Transport network
Opening of a TCP session on the PPTP serve
Negociation of the tunnel PPTP parametres
Cette liaison de contrôle sera maintenue
durant toute l'existence du tunnel
1723
PPP Link Control : Negociation of the PPP
link, authentication and compression method
Ex MsCHAP V2
challenge
Reponse=F(challenge, passwd)
OK
CHAP Authentication
(sending of a challenge=random number)
Response (challenge hashed with the
password)
Server acceptance
Tunnel
In the
datagramme
mode
Negociation of IP parametres
Negociation of the compression and
encryption modes
DATA
PPP Link Control : End of the PPP session
Closing of the PPTP tunnel
1723