

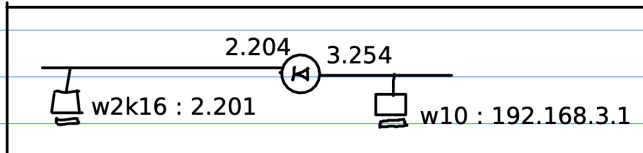
Network Security

Labs 9 ▢ Pratical Exam

9. ASAv (Lab11)

ASAv VPNs

Situation initiale : blade



Accès à w2k16 via RDP

W2k16 avec jre 1.8 et accès IE à https://_._.204 : install asdm launcher

Sur le router 22

----Mettre la configuration de base----

```
Router> en
Router# conf t
Router(config)# hostname router22
router22(config)# int g0/0
router22(config-if)# ip add 192.168.2.254 255.255.255.0
router22(config-if)# no shut
router22(config-if)# int g0/1
router22(config-if)# ip add 192.168.1.254 255.255.255.0
router22(config-if)# no shut
```

----telnet----

```
router22(config)# aaa new-model
router22(config)# username cisco password cisco
router22(config)# enable password cisco
router22(config)# line vty 0 4
router22(config-line)# transport input telnet
```

----dhcp pour 192.168.1.0/24 (côté pc client)----

```
router22(config)# ip dhcp excluded-address 192.168.1.254
router22(config)# ip dhcp pool POOL1
router22(dhcp-config)# network 192.168.1.0 255.255.255.0
router22(dhcp-config)# default-router 192.168.1.254
```

Sur le serveur W2K16 (rdp ▢ mstsc dans un terminal ou windows+R)

Dans la barre de recherche : <https://192.168.2.253>

Install ASDM Launcher

admin + P@ssw0rd -> ce qui télécharge dm-launcher.msi

intaller dm-launcher (next -> install)

Dans la fenêtre du Launcher :

Device Ip Address / Name : 192.168.2.253

admin + P@ssw0rd
❑ erreur de certificats -> sur internet explorer, aller dans Tools (la roue dentées en haut à droite), Internet Options
❑ dans l'onglet Security aller sur Trusted sites, sites et rajouter 192.168.2.253 dans la liste
Plus d'erreurs et l'application se lance

----Application----

Dans l'onglet Configuration, Device Setup -> Interface Settings -> Interfaces -> g0/1 EDIT

Interface Name: dmz1
Security Level: 50
Enable Interface
IP Address: 192.168.3.254
Subnet Mask: 255.255.255.0
OK

!Apply Changes! -> apparait lorsque l'on change d'onglet

Idem pour l'interface g0/2 qui est inside

Interface Name: inside
Security Level: 100
Enable Interface
IP Address: 192.168.4.254
Subnet Mask: 255.255.255.0
OK

Dans l'onglet Configuration, Firewall -> Objects -> Service Objects/Groups -> Add TCP Service Group

Group Name: RDP
Create new member:
Port/Range: 3389
ADD >>
OK

Dans l'onglet Configuration, Firewall -> Access Rules, Add

Interface outside -> car ça vient de l'extérieure
Action Permit
Source: 192.168.2.0/24
Destination: 192.168.3.1
Service: RDP
OK

Idem pour 192.168.4.1
Interface outside
Action Permit
Source: 192.168.2.0/24
Destination: 192.168.4.1
Service: RDP
OK

!!!! Sur outside et pas dmz ou inside, on met sur l'interface d'entrée

Rajoute les routes statiques via cmd

```
C:\Users\Administrator>route add 192.168.3.0 mask 255.255.255.0 192.168.2.253  
C:\Users\Administrator>route add 192.168.4.0 mask 255.255.255.0 192.168.2.253
```

Dans l'onglet Wizards, aller sur VPN wizards et sur Clientless SSL VPN Wizard

Connection Profile Name: clientlessProfile
SSL VPN Interface: outside
v Connection Group Alias/URL: CLIENTLESS

next

o Authenticate using the local user database

Username: cisco
Password: P@ssw0rd
Confirm Password: P@ssw0rd
Add >>

o Create new group policy: GPClientless

next

Bookmark List: manage -> Add

Bookmark List Name: List1

Add

o URL with GET or POST method

Bookmark Title: https

URL: http://192.168.3.1

Add

o URL with GET or POST method

Bookmark Title: cifs

URL: cifs://192.168.3.1/share

Assign: GPClientless

cisco

Finish

Configuration -> Remote Access VPN -> AAA/Local Users -> Local Users

cisco EDIT

Identity change user password -> cisco

VPN policy -> Connection Profile (Tunnel Group) Lock: x inherit (décoche)

clientlessProfile

Dans un browser https://192.168.2.253/CLIENTLESS

cisco/cisco

Sur la machine 192.168.3.1 créer un fichier partagé et activer le service http

Add role Web Server IIS

Dans l'onglet Wizards, aller sur VPN wizards et sur AnyConnect VPN Wizard

Télécharger l'image anyconnect-win-4.4.00243-webdeploy-k9.pkg sur l'EV et la copier coller dans le W2K16

Connection Profile Identification
 Connection Profile Name: AnyConnectProfile
 VPN Access Interface: outside
VPN Protocols
 v SSL
 x IPsec
Client Images
 Add -> l'image qu'on à copié collé
Authentication Methods
 Add cisco2/P@ssw0rd
Client Address Assignment
 IPv4 AddressPool Add
 POOL1
 192.168.3.2 -> 192.168.3.253
 255.255.255.0
Network Name Resolution Server
 On passe -> popup, mettre no
NAT Exempt
 v Exempt VPN traffic from network address translation
 inside & any4

Configuration -> Remote Access VPN -> AAA/Local Users -> Local Users
 cisco2 EDIT
 Identity change user password -> cisco2
 VPN policy -> Group Policy: GroupPolicy_AnyConnectProfile
 Connection Profile (Tunnel Group) Lock: x inherit

(décoche) clientlessProfile

Dans un browser <https://192.168.2.253/CLIENTLESS>

 cisco2/cisco2
 Télécharger anyconnect

Dans C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client
vpnu -> 192.168.2.253
Error -> Change Settings
 x Block connections to untrusted servers
rechanger le mdp en P@ssw0rd

FONCTIONNE PAS

Sur une autre machine (host ou de labo) installer
[anyconnect-win-4.4.00243-webdeploy-k9.pkg](#)

Lancer l'application anyconnect 192.168.2.253 -> enlever option Block...
cisco2/P@ssw0rd

On configure d'abord un routeur de notre côté :

```
# crypto isakmp policy 1
  encr aes 256
  hash sha
  authentication pre-share
  group 2

# crypto isakmp key SECRET address 192.168.2.253

# crypto ipsec transform-set MYSET esp-aes 256 esp-sha-hmac

# crypto map MYMAP 1 ipsec-isakmp
  set peer 192.168.2.253
  set transform-set MYSET
  match address 100

# access-list 100 permit ip 11.11.11.0 0.0.0.255 192.168.3.0 0.0.0.255

# int ...
  crypto map MYMAP
```

Il faut créer la même configuration mais en miroir sur ASA (le firewall) :

Wizards > Site-to-site VPN Wizard >

Configurer peer ip address (ip de notre routeur) :

The screenshot shows the 'Site-to-site VPN Connection Setup Wizard' window. On the left, a 'Steps' sidebar lists: 1. Introduction, 2. Peer Device Identification (highlighted), 3. Traffic to protect, 4. Security, 5. NAT Exempt, and 6. Summary. The main area is titled 'Peer Device Identification' and contains the text: 'This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.' Below this, there are two fields: 'Peer IP Address:' with a text input containing '192.168.2.50', and 'VPN Access Interface:' with a dropdown menu showing 'outside'. At the bottom, there are four buttons: '< Back' (disabled), 'Next >' (active/highlighted), 'Cancel', and 'Help'.

Configurer le trafic à protéger : Local network : 192.168.3.0/24 (dmz-network/24)

Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
- 3. Traffic to protect**
4. Security
5. NAT Exempt
6. Summary

Traffic to protect

This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.

Local Network:

Remote Network:

< Back Next > Cancel Help

Configurer une pre-shared key :

Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
3. Traffic to protect
- 4. Security**
5. NAT Exempt
6. Summary

Security

This step lets you secure the selected traffic.

☒ Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

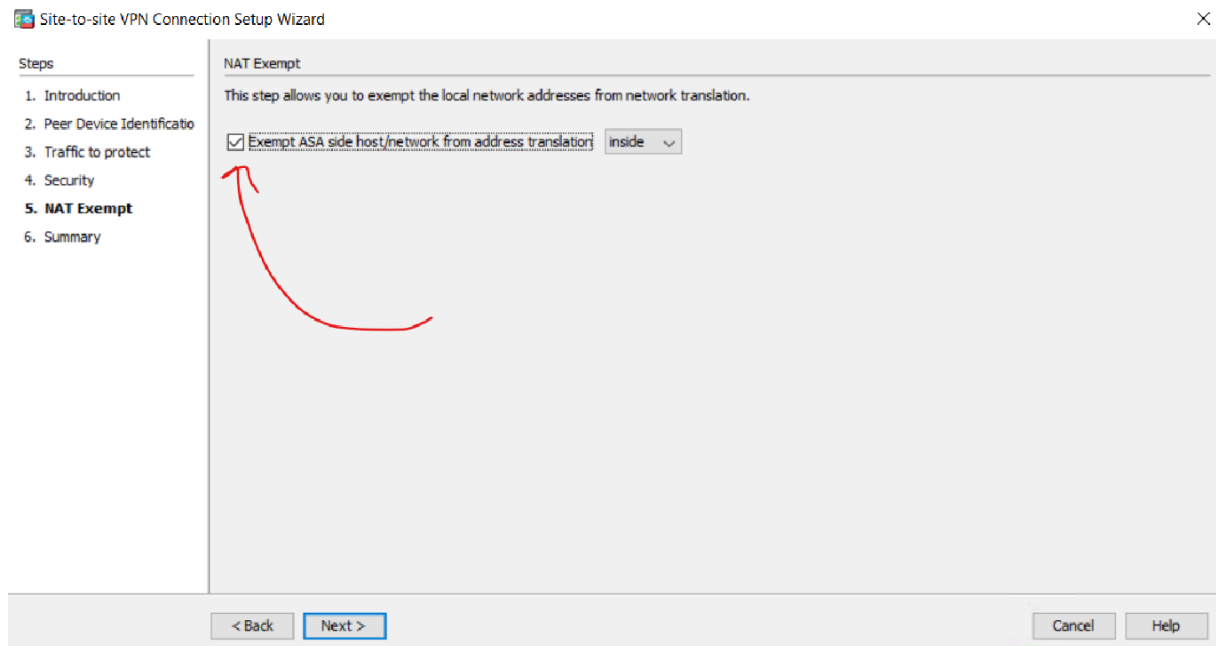
Pre-shared Key:

☐ Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

< Back Next > Cancel Help

NAT exempt : Exempt inside from translation :



Configurer ensuite le routeur en choisissant correctement les algorithmes (group 2 + sha).

```
R31(config)#int G0/0
R31(config-if)#ip addr 192.168.2.50 255.255.255.0
R31(config-if)#no shut
R31(config-if)#exit
R31(config)#int G0/1
R31(config-if)#ip addr 11.11.11.254 255.255.255.0
R31(config-if)#no shut
R31(config-if)#exit
R31(config)#
```

Pour vérifier que le tunnel fonctionne :

```
#debug crypto isakmp
```

On peut enfin vérifier que tout fonctionne avec une fonctionnalité appelée Paquet Tracer (Tools > Paquet Tracer) directement sur l'ASA :

Cisco ASDM Packet Tracer - 192.168.2.253

Select the packet type and supply the packet parameters. Click Start to trace the packet.

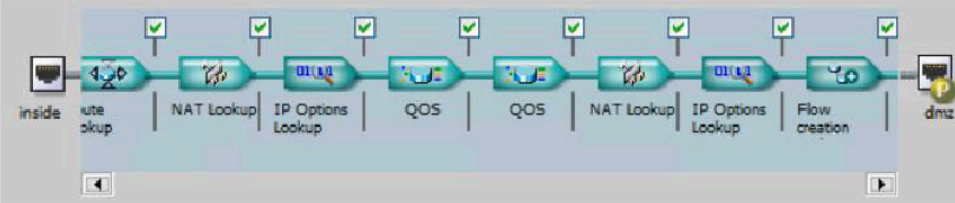
Interface: Packet Type: ☒ TCP ☐ UDP ☐ SCTP ☐ ICMP ☐ IP

☐ SGT number (0-65535)

Source: Destination:

Source Port: Destination Port:

☒ Show animation



Phase	Action	
+	ACCESS-LIST	✓
+	ROUTE-LOOKUP	✓
+	NAT	✓
+	IP-OPTIONS	✓
+	QOS	✓
+	QOS	✓
+	NAT	✓
+	IP-OPTIONS	✓
+	FLOW-CREATION	✓
[-]	RESULT - The packet is allowed.	✓

Input Interface: Line Link