الكلية المتعددة التخصصات - بني ملال
Faculté Polydisciplinaire - Beni Mellal

Polydisciplinary Faculty
Beni Mellal

جامعة السلطان مولاي سليمان
Université Sultan Moulay Slimane

Master :Telecommunications Systems and Computer Networks

Lab : Configure Clientless Remote Access SSL VPNs

Realized by :

EL MOTAMID Houria

2022 - 2023

Table des matières

1 | Required Resources

Downloading source of the software which will be required for this practical.
Processor for import the GNS3-VM, change the setting of it, and connectivity test from the Windows.
Setup the Local Server in GNS3.
Association of the GNS3-VM with GNS3.

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology Package license)
- 3 Switches (Cisco 2960 with cryptography IOS image for SSH support – Release 15.0(2)SE7 or comparable) (not required)
- 1 ASA 5506-X (OS version 9.10(1) and ASDM version 7.10(1) and Base license or comparable)
- 3 PCs (Windows, SSH Client and Java version compatible with installed ASDM version)
- Serial and Ethernet cables, as shown in the topology
- Console cables to configure Cisco networking devices

2 | Configure Basic Device Settings

2.1. Objectives:

- Cable the network and clear previous device settings, as shown in the topology.
- Configure basic settings for routers.
- Configure PC host IP settings.
- Verify connectivity.
- Save the basic running configuration for each router and switch.

At first you will set up the network topology and configure basic settings on the routers such as interface IP addresses and static routing.

2.2. Step 1: Cable the network and clear previous device settings

Attach the devices shown in the topology diagram and cable as necessary. Ensure that the routers and switches have been erased and have no startup configurations.

2.3. Step 2: Configure R1 using the CLI script

In this step, you will use the following CLI script to configure basic settings on R1. Copy and paste the basic configuration script commands listed below. Observe the messages as the commands are applied to ensure that there are no warnings or errors.

Note: Depending on the router model, interfaces might be numbered differently than those listed. You might need to alter the designations accordingly.

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

```
hostname R1
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
username admin01 algorithm-type scrypt secret admin01pass
ip domain name ccnasecurity.com
line con 0
 login local
 exec-timeout 5 0
 logging synchronous
exit
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0
 logging synchronous
exit
interface gigabitethernet 0/0
 ip address 209.165.200.225 255.255.255.248
 no shut
exit
int serial 0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 2000000
 no shut
exit
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
crypto key generate rsa general-keys modulus 1024
```

2.4. Step 3: Configure R2 using the CLI script.

The following CLI script to configure basic settings on R2.

```
hostname R2
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
username admin01 algorithm-type scrypt secret admin01pass
ip domain name ccnasecurity.com
line con 0
 login local
 exec-timeout 5 0
 logging synchronous
exit
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0
 logging synchronous
exit
interface serial 0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shut
```

```
exit
interface serial 0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 2000000
 no shut
exit
ip route 209.165.200.224 255.255.255.248 Serial0/0/0
ip route 172.16.3.0 255.255.255.0 Serial0/0/1
crypto key generate rsa general-keys modulus 1024
```

2.5. Step 4: Configure R3 using the CLI script.

The following CLI script to configure basic settings on R3.

```
hostname R3
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
username admin01 algorithm-type scrypt secret admin01pass
ip domain name ccnasecurity.com
line con 0
 login local
 exec-timeout 5 0
logging synchronous
exit
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0
 logging synchronous
exit
interface gigabitethernet 0/1
 ip address 172.16.3.1 255.255.255.0
 no shut
```

```
exit
int serial 0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shut
exit
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
crypto key generate rsa general-keys modulus 1024
```

2.6. Step 5: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A, PC-B, and PC-C.

2.7. Step 6: Verify connectivity.

PC-C and PC-D should be able to ping the R1 interface G0/0. If these pings are unsuccessful, troubleshoot the basic device configurations before continuing. The ASA is the focal point for the network zones and it has not yet been configured.

2.8. Step 7: Save the basic running configuration for each router and switch.

3 | Access the ASA Console and ASDM

3.1. Objectives:

- Access the ASA console.
- Clear the previous ASA configuration settings.
- Bypass Setup mode.
- Configure the ASA by using the CLI script.
- Access ASDM.

3.2. Step 1: Clear the previous ASA configuration settings.

To delete the startup-config file from flash memory, use the write erase command. To restart the ASA, issue the reload command. The ASA displays in CLI Setup mode as a result. If you notice that the System configuration has changed. Save?**[Y]es/[N]o**: message, type n, and press Enter.

3.3. Step 2: Bypass Setup mode.

When the ASA completes the reload process, it should detect that the startup configuration file is missing and go into Setup mode. If it does not come up in this mode, repeat Step 2. When prompted to preconfigure the firewall through interactive prompts (Setup mode), respond with no.
Enter privileged EXEC mode with the enable command. The password should be kept blank (no password).

3.4. Step 3: Configure the ASA by using the CLI script.

Configuring an SSL VPN is the first step in setting up a virtual private network (VPN) - you will need to copy and paste the Pre-VPN Configuration Script commands listed below at the ASA global configuration mode prompt to start configuring the SSL VPNs.

```
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password cisco12345
interface G1/2
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 no shutdown
interface G1/1
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
 no shutdown
interface G1/3
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
 no shutdown
object network inside-net
 subnet 192.168.1.0 255.255.255.0
object network dmz-server
 host 192.168.2.3
access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
object network inside-net
 nat (inside,outside) dynamic interface
object network dmz-server
 nat (dmz,outside) static 209.165.200.227
access-group OUTSIDE-DMZ in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
username admin01 password admin01pass
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
http server enable
http 192.168.1.0 255.255.255.0 inside
ssh 192.168.1.0 255.255.255.0 inside
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 10
ssh timeout 10
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
   inspect icmp
crypto key generate rsa modulus 1024
```

At the privileged EXEC mode prompt, issue the write mem (or copy run start) command to save the running configuration to the startup configuration and the RSA keys to non-volatile memory.

3.5. Step 4: Access ASDM.

On PC-B, start ASDM using the ASDM application or by using a browser and connecting to https://192.168.1.1 and then choosing Run ASDM.
Please refer to the previous lab for more detailed instructions. **Note:** If one of the choices is Install Java Web Start, you will need to input `https://192.168.1.1/admin/public/startup.jnlp` in a browser if you do not want to install the Launcher.
After the ASDM Launcher starts, log in as user **admin01** with password **admin01pass**.

4 | Configure Clientless SSL VPN Remote Access Using ASDM

4.1. Objectives:

- Start the VPN wizard.
- Configure the SSL VPN user interface.
- Configure AAA user authentication.
- Configure the VPN group policy.
- Configure a bookmark list (clientless connections only).
- Review the configuration summary and deliver the commands to the ASA.
- Verify the ASDM SSL VPN connection profile.
- Verify VPN access from the remote host.
- Access the web portal page.
- View the clientless remote user session using the ASDM Monitor.

4.2. Step 1: Start the VPN wizard.

On the ASDM main menu, click **Wizards > VPN Wizards > Clientless SSL VPN wizard**.

Click Next to continue and open the SSL VPN Interface window.

4.3. Step 2: Configure the SSL VPN user interface.

On the SSL VPN Interface screen, configure SSL-VPN as the Connection Profile Name, and specify outside as the interface to which outside users will connect.

The SSL VPN Interface screen provides links in the Information section. These links identify the URLs that need to be used for the SSL VPN service access (log in) and for Cisco ASDM access (to access the Cisco ASDM software).
Click Next to continue and open the User Authentication window.

4.4. Step 3: Configure AAA user authentication.

On the User Authentication screen, click Authenticate using the local user database.
Enter the user name **SSL-VPN-USER** with password **cisco12345**. Click Add to create the new user. Click Next to continue and open the Group Policy window.

4.5. Step 4: Configure the VPN group policy.

On the Group Policy screen, create a new group policy named SSL-VPN-POLICY. (When configuring a new policy, the policy name cannot contain any spaces.).
Click Next to continue and open the Clientless Connections Only window.
Note: By default, the created user group policy inherits its settings from the DfltGrpPolicy. These settings may be modified after the wizard has been completed by navigating to the **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies submenu.**

4.6. Step 5: Configure the bookmark list (clientless connections only).

A bookmark list is a set of URLs configured to be used in the clientless SSL VPN web portal. If there are bookmarks already listed, use the Bookmark List drop-down list, select the bookmark of choice, and click Next to continue with the SSL VPN wizard.

Note: There are no configured bookmark lists by default and, therefore, they must be configured by the network administrator.

On the Clientless Connections Only – Bookmark List screen, click Manage to create an HTTP server bookmark in the bookmark list. In the Configure GUI Customization Objects window, click Add to open the Add Bookmark List window. Name the list Web-Server.

The ASDM can create three types of bookmarks. Select the URL with GET or POST method, click OK.

Enter the bookmark title and enter the server destination IP address or hostname as the URL to be used with the bookmark entry. In this example, the Bookmark Title of Web-Mail is entered and an internal IP address of 192.168.2.3 (the DMZ server) is specified. If this server has HTTP web services with web mail installed and functional, the outside users are able to access the server from the ASA portal when they connect.

Click OK to continue

Verify Web-Server is selected, and click Next to continue.

4.7. Step 6: Review the configuration summary and deliver the commands to the ASA.

The Summary page is displayed next. Verify that the information configured in the SSL VPN wizard is correct. Click Back to make changes, or click Cancel and restart the VPN wizard.
Click Finish to complete the process and deliver the commands to the ASA.

4.8. Step 7: Verify the ASDM SSL VPN connection profile.

In ASDM, click **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**. In this window, the VPN configuration can be verified and edited.

4.9. Step 8: Verify VPN access from the remote host.

Open the browser on PC-C and enter the login URL for the SSL VPN into the address field (`https://209.165.200.226`). Use secure HTTP (HTTPS) because SSL is required to connect to the ASA.
The Logon window should display. Enter the previously configured username SSL-VPN-USER and password cisco12345, and click Login to continue. **Note:** If you were unable to log in, use the CLI to verify that the user SSL-VPN-USER is configured. If it is still not working, enter the command username SSL-VPN-USER password cisco12345 in the CLI.

4.10. Step 9: Access the web portal window.

After the user authenticates, the ASA SSL web portal page lists the various bookmarks previously assigned to the profile. If the Bookmark points to a valid server IP address or hostname that has HTTP web services installed and functional, the outside user will be able to access the server from the ASA portal. **Note:** In this lab, the web mail server is not installed.

4.11. Step 10: View the clientless remote user session using the ASDM Monitor.

While the remote user at PC-C is still logged in and on the ASA portal page, you can view the session statistics using ASDM monitor.
From the ASDM menu bar on PC-B, click Monitoring and then select **VPN > VPN Statistics > Sessions**. Click the Filter By pull-down list and select Clientless SSL VPN. You should see the SSL-VPN-USER session logged in from PC-C (172.16.3.3). **Note:** You may need to click Refresh to display the remote user session.

4.12. Step 11: Log out of the web portal page.

The user should log out of the web portal window on PC-C using the Logout button when done (See Step 10). However, the web portal will also time out if there is no activity. In either case a logout window will be displayed informing users that for additional security, they should clear the browser cache, delete the downloaded files, and close the browser window.

TOPOLOGY:

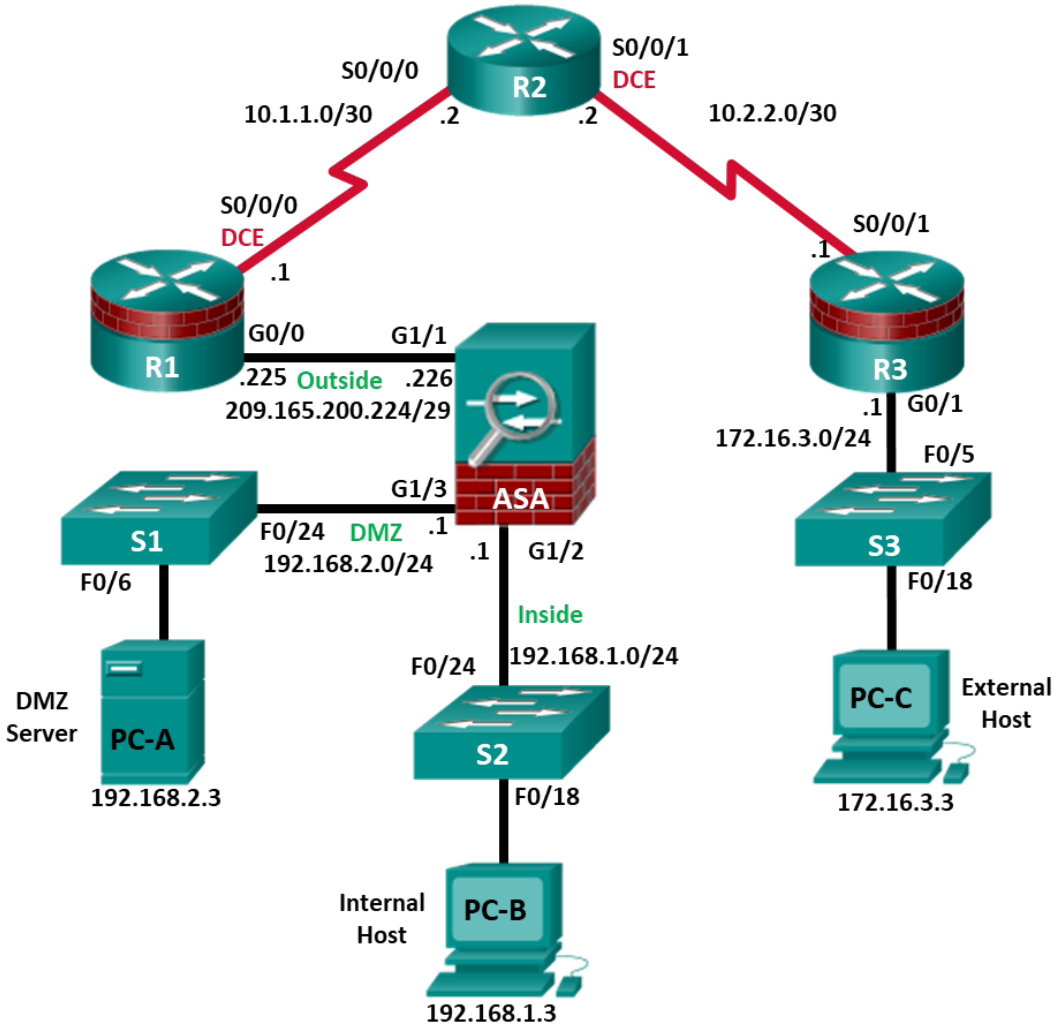

Figure 4.1: Topology