Test Project
ES2014_TP2010_HU

APPENDIX 3.
Description of project and tasks – DAY 3

Submitted by:
Name: Zoltán Sisák
Member Country: Hungary

Table of Content

Whenever a password is not specified, you should use **Lille2014** as password on all servers, clients and devices.

IMPORTANT! If you do not use the proper password, and your settings cannot be checked, you might not receive any points for your solution!

Please use the details on the topology (IP addresses, interfaces, etc.) accurately during your implementation.

The X in the IP-addresses and names represents your team-number.

1. THE SURROUNDINGS

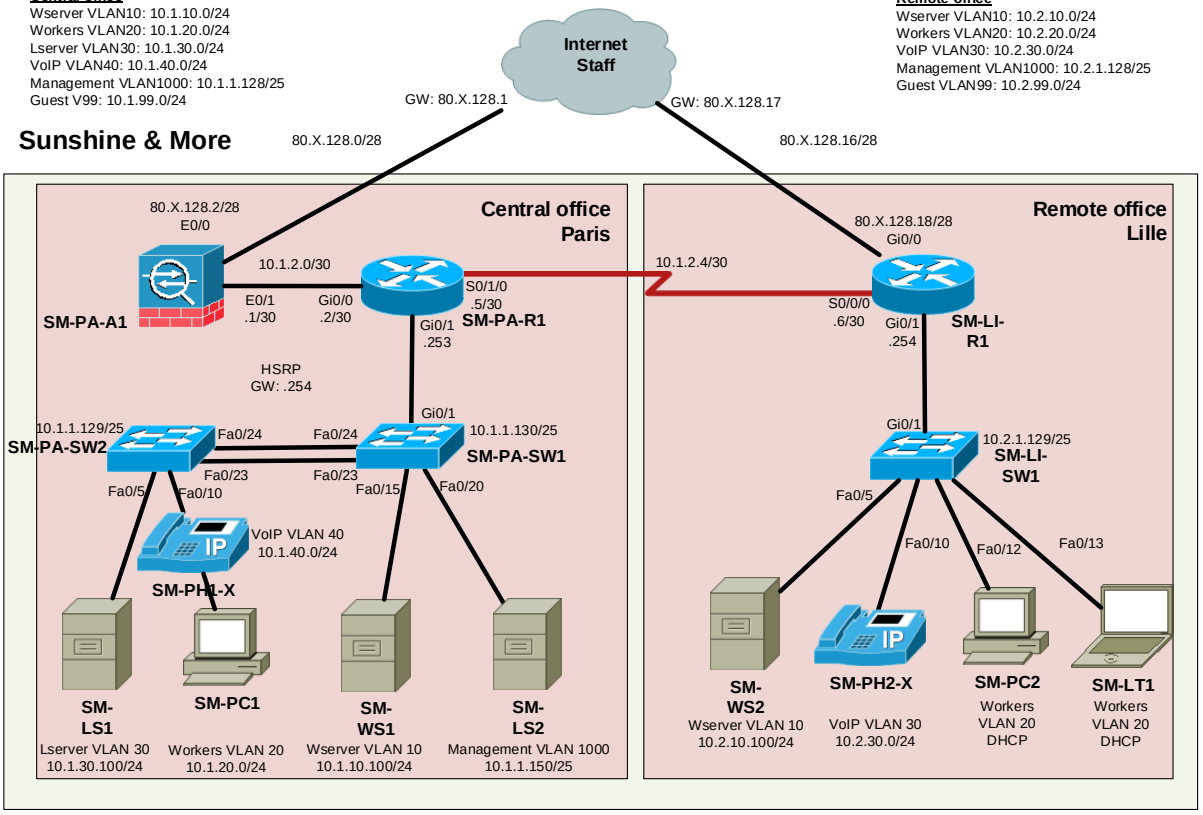
Your company and team experienced many intrusions during the last months so the leadership decided to build a more secure network. A new security plan was designed to ensure the protection of the company system. According to the plan a new equipment, a Cisco ASA 5505 device was purchased and several new requirements appeared.

Your team has been charged to implement the plan.

Central office
Wserver VLAN10: 10.1.10.0/24
Workers VLAN20: 10.1.20.0/24
Lserver VLAN30: 10.1.30.0/24
VoIP VLAN40: 10.1.40.0/24
Management VLAN1000: 10.1.1.128/25
Guest V99: 10.1.99.0/24

Remote office
Wserver VLAN10: 10.2.10.0/24
Workers VLAN20: 10.2.20.0/24
VoIP VLAN30: 10.2.30.0/24
Management VLAN1000: 10.2.1.128/25
Guest VLAN99: 10.2.99.0/24

Sunshine & More



2. YOUR TASKS AT SUNSHINE & MORE

2.1. NETWORK-ADMINISTRATOR TASKS

1. The physical infrastructure has to be rebuilt. The new ASA device will act as the firewall of the Paris office site.
2. It is important to ensure secure access to the company IT resources for the remote workers. Implement remote access VPN using the ASA and Cisco VPN Client. VPN group name should be *sunshinevpn.* The authentication should happen using Radius service on **SM-WS1**.
3. Previously the company already LAN-to-LAN VPN between the two sites using the border routers. One of the end devices was replaced by the ASA, so it needs reconfiguration. Make the necessary changes and configuration on **SM-PA-A1** and **SM-LI-R1**. The IPSec-L2L VPN should work by certificate based authentication. **SM-PA-A1** should get its certificate from the CA on **SM-LS1**, but **SM-LI-R1** certificate should come from the CA on **SM-WS2**.
4. Configure **SM-PA-A1** device to ensure that only RDWeb service and DNS service for sunshineX.eu domain could be reached from the outside network using 80.x.128.3 public IP address. Any other traffic should be refused.
5. Configure **SM-LI-R1** device to ensure that only RDWeb service and DNS service for sunshineX.eu domain could be reached from the outside network using 80.x.128.19 public IP address. Any other traffic should be refused.
6. Configure IEEE 802.1x on all switch ports which were previously assigned to VLAN20. On Paris site use Windows radius server, on Lille site use Linux radius server as authentication server. Depending whether the authentication was successful or not, the clients should be placed in different VLANs. You can find the details under the Windows and Linux tasks.
7. Configure the SNMP client on **SM-PA-R1** and **SM-LI-R1** to use **SM-LS1** as SNMP server.

2.2. WINDOWS TASKS

1. Requirements regarding Windows Clients authentication (IEEE 802.1x) in Paris site
   a) Only domain computers allowed access to corporation network.
   b) Windows clients should authenticate themselves by computer certificates. This rule and the necessary properties should come from GPO.
   c) During the authentication it needs to check the firewall status on the client. If the firewall is switched off the authentication should be refused.
   d) Depending whether the authentication was successful or not, the clients should be palced in different VLANs. The clients which are not able to authenticate themselves should assign to VLAN 99. All the others should go to VLAN 20.
2. Windows Clients authentication in Lille site
   a) Windows clients should authenticate themselves by domain user credentials.

b) Configure the client for 802.1x authentication. Configure to use automatically the Windows logon name and password. All 802.1x settings should come from GPO.

c) Depending whether the authentication was successful or not, the clients have to settle in different VLANs. The clients which are not able to authenticate themselves should assign to VLAN 99. All the others should go to VLAN 20.

3. Graphical user interface from **SM-WS2** should be removed.
4. Create a new sunshineX.eu DNS zone. Create the necessary records for accessing RDWeb service by rdweb.sunshineX.eu and remote access VPN service by vpn.sunshineX.eu.
5. Install IIS web server on **SM-WS2**. Install PHP framework and create a simple index file which show the actual server date and time. (Hint: use *date* PHP function.) Use *myfirstphppage.tmt* as file name of the index page.
6. Install Windows Server Update Services on **SM-WS1**.
7. Use Group Policy for configuring all client computers to use **SM-WS1** as Windows Update Server.
8. Ensure that all Windows machines (servers and clients) is “pingable” (reply to echo requests) Use Group Policy.

2.3. LINUX SERVER TASKS

1. Password policy must be implemented on **SM-LS1**. The minimum length of the passwords is 8 and it should contain lowercase character, uppercase character and number.
2. Prepare your existing radius server for receiving IEEE 802.1x requests. The server should use Active Directory database. Depending whether the authentication was successful or not, the clients should be placed in different VLANs. The clients which are not able to authenticate themselves should be assigned to VLAN 99. All the others should go to VLAN 20.
3. ICMP flood attack from the Internet on **SM-LI-R1** router should be detected. The ISP staff should receive an e-mail alert if an intrusion happens. Address: alert@tarhely.hu; Subject: TeamX Alert; From: smls2@sunshineX.eu
4. Install SNMP server on **SM-LS1**. When SNMP trap received, generate log message to system’s default log destination.
5. Backup SM-WS2 website data every ten minutes. Use backup_yyyy-mm-dd-hh-mm.tar as file name. Store the files in /var/backup folder.
6. User projectuser1 is only allowed to login between 8.00-12.00, from Monday till Saturday.
7. Configure firewall policy on **SM-LS1** ensuring that only the previously defined services of these servers could be accessed from the inside and outside network.
8. Join **SM-PC2** Debian client to the corporate Active Directory domain. Enable AD users’ login on **SM-PC2**.