

**Course Code: ITEC1330**

**Course Title: Firewall & VPNs**

**Assignment**

Weight: 20%

Contents

[I- Rubrics: 1](#_Toc95580234)

[1. Firewall Plan 2](#_Toc95580235)

[2. VPN Plan 3](#_Toc95580236)

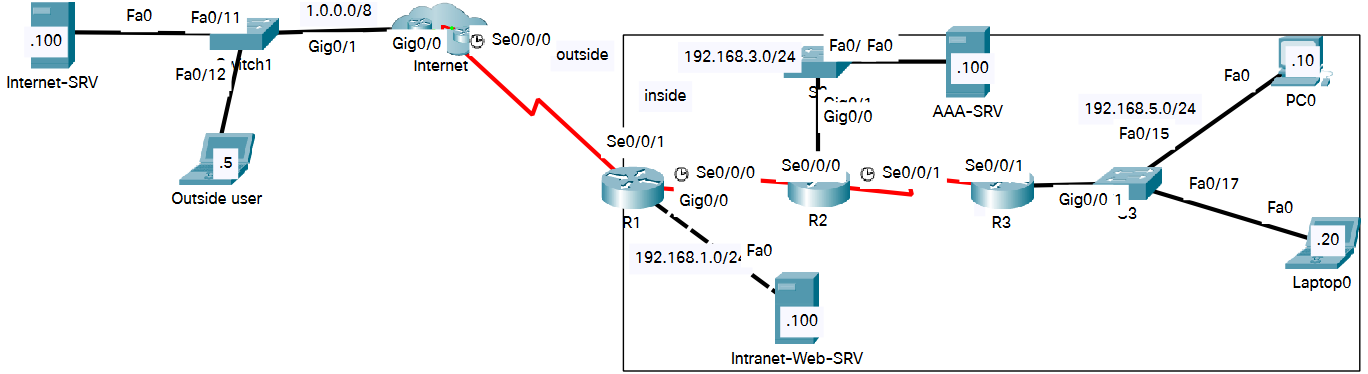
[3. Verification Plan 4](#_Toc95580237)

[II- How to Submit: 5](#_Toc95580238)

# Rubrics:

* ACL Plan: **8 marks**
* VPN Plan: **8 marks**
* Discussions: **4 marks**

This questions aims at building the ACL & VPN Policy for a network topology. **Figure A** shows the design of a network:



## Firewall Plan

The network traffic Requirements are in the below:

* **AAA-SRV:** is the AAA server to authenticate internal users accessing the 3 routers R1, R2 and R3. It runs Radius (udp-1645)
* **Intranet-Web-SRV** is a website to be accessed from inside and outside using HTTPS (tcp-443)
* **S3 LAN:** Internal users include one **IT admin PC0** who needs to securely manage routers and one normal user **(laptop0)** who needs to securely browse the Internet.

Suggest the convenient **filtering policie(s)** to allow legitimate communications as per the previous description while blocking unwanted ones. You might use one or more ACL, on one or more router. Fill in the below table with your choices and implement them on packet tracer file.

**Note:**

1. **Verify full network connectivity before any configuration**
2. **Use Extended named ACL only**

**Table 1: ACL Table**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Policy-1:  Protect server… | | | | | | | | | | Brief Justifications | | |
| Router | **Interface** | | **Direction** | | **ACL Name** | | | | ACL Entries |  | | |
| R3 | **G0/0** | | **IN** | | **sw3Lan** | | | | permit udp 192.168.5.0 0.0.0.255 host 192.168.3.100 eq 1645 | To allow to S3 Lan users to access and authenticate with AAA server | | |
| R3 | | **G0/0** | | **IN** | | **sw3Lan** | | permit tcp host 192.168.5.10 host 192.168.4.2 eq 22  permit tcp host 192.168.5.10 host 192.168.2.1 eq 22  permit tcp host 192.168.5.10 host 192.168.5.1 eq 22 | | | | To allow PC0 admin to securely manage routers(R1,R2,R3) using ssh protocol |
| R3 | | **G0/0** | | **IN** | | **sw3Lan** | permit tcp host 192.168.5.20 any eq 443 | | | | To allow normal user (laptop0) to connect with any web server using only https protocol. | |
| R3 | | **G0/0** | | **IN** | | **sw3Lan** | permit icmp any any echo  permit icmp any any echo-reply | | | | To allow incoming and outcoming ping. | |
| R3 | | **G0/0** | | **IN** | | **sw3Lan** | **permit tcp 192.168.5.0 0.0.0.255 host 192.168.1.100 eq 21** | | | | To allow internal users in lan3 using FTP server | |
| Policy-2: | | | | | | | | | |  | | |
| R1 | G0/0 | | OUT | | intraWebSRV | | | | permit tcp any host 192.168.1.100 eq 443 | To allow any accessing website from inside and outside using only https protocol | | |
| R1 | G0/0 | | Out | | intraWebSRV | | | | permit tcp 192.168.5.0 0.0.0.255 host 192.168.1.100 eq 21 | To allow inside users in lan3 using ftp server. | | |
| R1 | G0/0 | | Out | | intraWebSRV | | | | **deny tcp 192.168.1.0 0.0.0.255 any eq 22** | To Deny intra-web-server use ssh connection | | |
| R1 | S0/0/1 | | IN | | **denySSH** | | | | deny tcp any any eq 22 | To deny Outside users to connect with internal routers remotely using ssh. | | |
| R1 | S0/0/1 | | IN | | denySSH | | | | permit tcp any any eq 443  permit tcp any any | To allow accessing to intra web server using https protocol | | |
| R2 | G0/0 | | In | | AAALan | | | | deny tcp 192.168.3.0 0.0.0.255 any eq 22 permit udp ho 192.168.3.100 any  permit icmp any any echo  permit icmp any any echo-reply | To deny ssh connection, and only allow ping and radius authentication with AAA server | | |

## VPN Plan

The network traffic Requirements are in the below:

* **R2-R3:** is an untrusted ISP link, between two cities where R2 and R3 are physically located.
* **R1-R2:** is a trusted link between two adjacent buildings where R1 and R2 are physically located.
* **Internal FTP** (tcp 21) traffic **to Intranet-SRV** should be encrypted through VPN

**Table 2: VPN Table**

Suggest the convenient **VPN policie(s)** to allow legitimate communications as per the previous description while blocking unwanted ones. You might use one or more ACL, on one or more router. Fill in the below table with your choices and implement them on packet tracer file.

|  |  |  |
| --- | --- | --- |
| Policy-1:  Establish VPN Between… | | Brief Justifications |
| Routers | VPN configuration |  |
| R2 | R2  1- ACL:  access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255  2- IKE-Phase1  authentication pre-share  encryption aes  hash md5  group 5  exit  crypto isakmp key cisco123 address 192.168.4.1  3- IKE-Phase2  crypto ipsec transform-set MYSET esp-aes esp-sha-hmac  4- Create Cryptomap:  crypto map MYMAP 10 ipsec-isakmp  set peer 192.168.4.1  set transform-set MYSET  match address 110  5- Apply Cryptomap on Interface  int s0/0/1  crypto map MYMAP | Create ACL, and configure phase 1,phase2 with IKE protocol to encrypt data between routers and data of their LAN’s |
| R3 | R2  1- ACL:  access-list 110 permit ip 192.168.5.0 0.0.0.255 192.168.3.0 0.0.0.255  2- IKE-Phase1  authentication pre-share  encryption aes  hash md5  group 5  exit  crypto isakmp key cisco123 address 192.168.4.2  3- IKE-Phase2  crypto ipsec transform-set MYSET esp-aes esp-sha-hmac  4- Create Cryptomap:  crypto map MYMAP 10 ipsec-isakmp  set peer 192.168.4.2  set transform-set MYSET  match address 110  5- Apply Cryptomap on Interface  int s0/0/1  crypto map MYMAP | Create ACL, and configure phase 1,phase2 with IKE protocol to encrypt data between routers and data of their LAN’s |
| Policy-2:  Establish VPN Between… | |  |
| Router | VPN configuration |  |
| R1 | 1- ACL:  access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.5.0 0.0.0.255  2- IKE-Phase1  crypto isakmp policy 10  authentication pre-share  encryption aes  hash md5  group 5  exit  crypto isakmp key cisco123 address 192.168.4.1  3- IKE-Phase2  crypto ipsec transform-set MYSET2 esp-aes esp-sha-hmac  4- Create Cryptomap:  crypto map MYMAP2 10 ipsec-isakmp  set peer 192.168.4.1  set transform-set MYSET2  match address 110  5- Apply Cryptomap on Interface  int s0/0/1  crypto map MYMAP2 | Create ACL, and configure phase 1,phase2 with IKE protocol to encrypt data between routers and data of their LAN’s |
| R3 | 1- ACL:  access-list 110 permit ip 192.168.5.0 0.0.0.255 192.168.1.0 0.0.0.255  2- IKE-Phase1  crypto isakmp policy 10  authentication pre-share  encryption aes  hash md5  group 5  exit  crypto isakmp key cisco123 address 192.168.2.1  3- IKE-Phase2  crypto ipsec transform-set MYSET2 esp-aes esp-sha-hmac  4- Create Cryptomap:  crypto map MYMAP2 10 ipsec-isakmp  set peer 192.168.2.1  set transform-set MYSET2  match address 110  5- Apply Cryptomap on Interface  int s0/0/1  crypto map MYMAP2 | Create ACL, and configure phase 1,phase2 with IKE protocol to encrypt data between routers and data of their LAN’s |

## Verification Plan

* 1. **\*\*Include a Print Screen of the result for each step**
  2. Admin on PC0 to be able to securely mange router R1
  3. Admin on PC0 to be able to securely mange router R2
  4. Admin on PC0 to be able to securely mange router R3
  5. Laptop0 user to be able to securely browse Intranet-SRV
  6. Laptop0 user to be able to securely browse Internet-SRV
  7. Outside user to be able to securely browse Intranet-SRV
  8. VPN Traffic verification

# How to Submit:

* Please submit **TWO FILES** on **Blackboard** before the deadline: **WORD** and **PKT**
* **Follow the below naming convention, for example for Group-1:**
* **Group1-2330-Suggested-Policies.docx**
* **Group1-2330-Configured-Topology.pkt**
* **Any student can submit on behalf of the group**

**Good luck!**