10.4.1.1 Packet Tracer - Skills Integration Challenge

** חלק מהערכים בתרגיל (שמות וכתובות ip) הם <u>רנדומליים,</u> שלבי הפתרון יהיו זהים אך יש להיעזר בטבלת הניתוב ובהוראות.

Sw

Configure remote management access including IP addressing and SSH:

- Domain is cisco.com
- User CAdmin with password itsasecret
- Crypto key length of 1024
- SSH version 2, limited to 2 authentication attempts and a 60 second timeout
- Clear text passwords should be encrypted.

Configure, name and assign VLANs. Ports should be manually configured as access

ports.

Implement port security:

On F0/1, allow 2 MAC addresses that are automatically added to the configuration file when detected. The port should not be disabled, but a syslog message should be captured if a violation occurs.

Cnt-Sw(config)#ip domain-name cisco.com Cnt-Sw(config)#user CAdmin password itsasecret Cnt-Sw(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 Cnt-Sw(config)#ip ssh version 2 Cnt-Sw(config)#ip ssh authentication-retries 2 Cnt-Sw(config)#ip ssh time-out 60 Cnt-Sw(config)#service password-encryption

Cnt-Sw(config)#vlan 15 Cnt-Sw(config-vlan)#name Servers * לחזור עבור כל Vlan

Cnt-Sw(config)#int range f0/11-f0/20 Cnt-Sw(config-if-range)#switchport mode access PCs ו Management לחזור עבור *

Cnt-Sw(config)#int vlan 60 Cnt-Sw(config-if)#ip address 192.168.45.34 255.255.255.240

Cnt-Sw(config)#ip default-gateway 192.168.45.33

Cnt-Sw(config)#int g0/0 Cnt-Sw(config-if)#switchport mode trunk Cnt-Sw(config-if)#switchport trunk native vlan 45

[show vlan brief, show int status, show int trunk]

Cnt-Sw(config-if)#int f0/1

Cnt-Sw(config-if)#switchport port-security Cnt-Sw(config-if)#switchport port-security mac-address sticky

Cnt-Sw(config-if)#switchport port-security maximum 2

Cnt-Sw(config-if)#switchport port-security violation restrict

Cnt-Sw(config)#int g0/2 Cnt-Sw(config-if)#shutdown Disable all other unused ports. Cnt-Sw(config-if)#int range fa0/21-24 Cnt-Sw(config-if-range)#shutdown Cnt-Sw(config)#line vty 0 15 Cnt-Sw(config-line)#transport input ssh Configure VTY lines to be accessible via SSH Cnt-Sw(config-line)#login local only ROUTER Configure inter-VLAN routing. Central(config)#int g0/0.15 Central(config-subif)#encapsulation dot1Q <u>15</u> Central(config-subif)#ip address 192.168.45.65 255.255.255.192 * לחזור עבור כל ** Central(config-subif)#int g0/0.45 Central(config-subif)#encapsulation dot1Q 45 native Central(config-subif)#ip address 192.168.45.17 255.255.255.240 Central(config)#int g0/0 Central(config-if)#no shutdown Configure DHCP services for VLAN 30. Central(config)#ip dhcp pool LAN Use **LAN** as the case-sensitive name for the Central(dhcp-config)#default-router pool. 192.168.45.129 Central(dhcp-config)#network <u>192.168.45.128</u> 255.255.255.192 Central(dhcp-config)#domain-name cisco.com ** click on vlan 30 PC and change ip settings to dhcp. PC should receive address from router

· Implement routing:

- Use RIP version 2

- Disable automatic summarization
- Configure one network statement for the entire **192.168.45.0/24** address space

- Configure a default route to the Internet.

Central(config)#router rip Central(config-router)#version 2 Central(config-router)#no auto-summary Central(config-router)#default-information originate

Central(config-router)#network <u>192.168.45.0</u> Central(config)#ip route 0.0.0.0 0.0.0.0<u>serial</u> 0/1/0

[show ip rip database, show ip route]

Implement NAT:

- Configure a standard, one statement ACL number 1. All IP addresses belonging to the 192.168.45.0/24 address space are allowed.

Central (config)#ip access-list standard <u>1</u> Central (config-std-nacl)#permit 192.168.45.0 0.0.0.255

- Refer to your documentation and configure static NAT for the File Server.

Central(config)#ip nat inside source static 192.168.45.66 64.100.32.58

- Configure dynamic NAT with PAT using a pool name of your choice, a /30 mask, and these two public addresses:

64.100.32.56 and 64.100.32.57

- Bind the NAT pool to ACL 1 and configure PAT. Packet Tracer does not grade this command.

- Activate NAT on all appropriate interfaces.

Central(config)#ip nat pool pool1 64.100.32.56 64.100.32.57 netmask 255.255.255.252

Central(config)#ip nat inside source list <u>1</u> pool <u>pool1</u> **overload**

[show ip route connected]

Central(config)#int se0/1/0 Central(config-if)#ip nat Central(config-if)#ip nat ou Central(config-if)#ip nat outside

Central(config-if)#int gi0/0.45 Central(config-subif)#ip nat Central(config-subif)#ip nat inside

*להגדיר על כל הממשקים