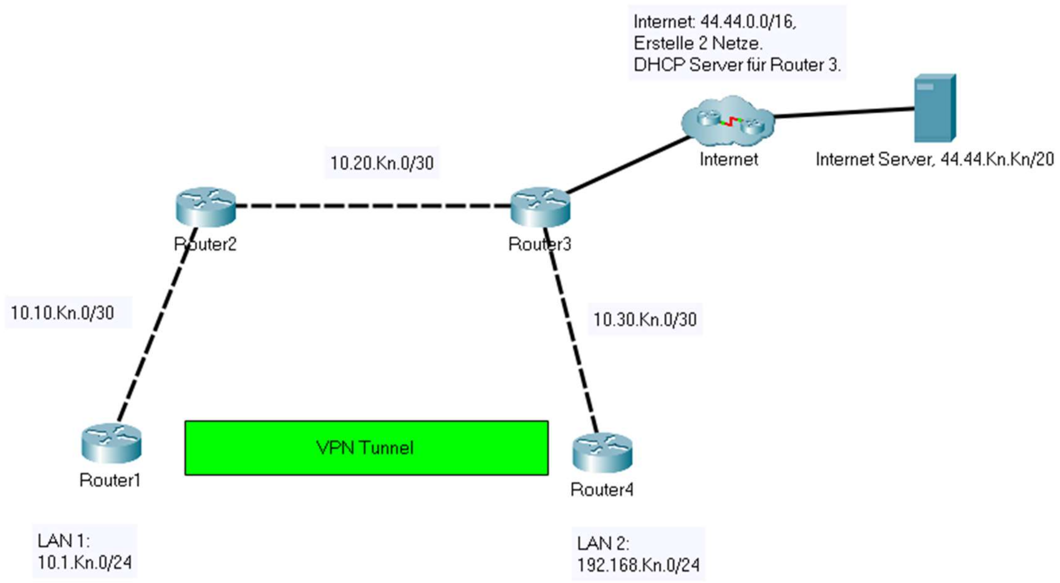
Packet Tracer - Configure and Verify a Site-to-Site IPsec VPN, ACL, NAT, OSPF, DHCP

Topology, Kn = siehe File



VPN_Prüfung4Router_V3.pkt

Addressing Table (optional)

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1			255.255.255.0		
			255.255.255.252		
R2			255.255.255.0		
			255.255.255.252		
			255.255.255.252		
R3			255.255.255.0		
			255.255.255.252		
			255.255.255.252		
R4			255.255.255.0		
			255.255.255.252		
PC-A	NIC		255.255.255.0		
PC-B	NIC		255.255.255.0		
Internet Server	NIC				

Objectives

- Verify connectivity throughout the network.
- Configure R1 to support a site-to-site IPsec VPN with R4.

ISAKMP Phase 1 Policy Parameters

Parameters		R1	R4
Key Distribution Method	Manual or **ISAKMP**	**ISAKMP**	**ISAKMP**
Encryption Algorithm	**DES**, 3DES, or AES	AES 256	AES 256
Hash Algorithm	MD5 or **SHA-1**	**SHA-1 or better**	**SHA-1 or better**
Authentication Method	Pre-shared keys or **RSA**	pre-share	pre-share
Key Exchange	DH Group best available	DH best available	DH best available
IKE SA Lifetime	86400 seconds or less	**86400**	**86400**
ISAKMP Key		FirstName	FirstName

IPsec Phase 2 Policy Parameters

Parameters	R1	R4
Transform Set Name	VPN-SET-FirstName	VPN-SET-FirstName
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authentication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	tbd	tbd
Traffic to be Encrypted	tbd	tbd
Crypto Map Name	VPN-MAP-FirstName	VPN-MAP-FirstName
SA Establishment	ipsec-isakmp	ipsec-isakmp

Part 1: Configure IP Addresses and OSPF

Step 1: IP Addresses as shown in the network diagram.

Step 2: Configure OSPF as follows:

- **One static route to Internet propagated by OSPF.**
- **OSPF Area Kn.**

Part 2: Configure Internet

Step 1: Configure Internet as shown in the network diagram.

Part 3: Configure IPsec Parameters on R1

Step 1: Enable the Security Technology package.

Step 2: Identify interesting traffic on R1.

Step 3: Configure the IKE Phase 1 ISAKMP policy on R1.

Step 4: Configure the IKE Phase 2 IPsec policy on R1.

Step 5: Configure the crypto map on the outgoing interface.

Part 4: Configure IPsec Parameters on R4

Step 1: Enable the Security Technology package.

Step 2: Configure router R3 to support a site-to-site VPN with R1.

Step 3: Configure the IKE Phase 1 ISAKMP properties on R4.

Step 4: Configure the IKE Phase 2 IPsec policy on R4.

Step 5: Configure the crypto map on the outgoing interface.

Part 5: Configure NAT on R3

Step 1: Configure NAT only for LAN1 and LAN2.

Part 6: Configure ACLs on R3

Step 1: Configure ACL1 as follows: Allow for LAN1 and LAN2 only HTTP, HTTPS, DNS, Protokoll “Kn” and ICMP.

Step 2: Configure ACL2 as follows: Allow only connections from the Internet that were already established or originated within LAN1 or LAN2.

Part 7: Configure DHCP for LAN1 und LAN2

Step 1: Configure an DHCP as follows: static IP addresses from 1 to Kn.

Part 8: Verify and Trouble Shoot the IPsec VPN 30%

Step 1: Verify the tunnel prior to interesting traffic.

Issue the **show crypto ipsec sa** command on R1. Notice that the number of packets encapsulated, encrypted, decapsulated, and decrypted are all set to 0.

Step 2: Create interesting traffic.

Step 3: Verify the tunnel after interesting traffic.

On R1, re-issue the **show crypto ipsec sa** command. Notice that the number of packets is more than 0, which indicates that the IPsec VPN tunnel is working.

Step 4: Create uninteresting traffic.

Step 5: Verify the tunnel after uninteresting traffic.

On R1, re-issue the **show crypto ipsec sa** command. Notice that the number of packets has not changed, which verifies that uninteresting traffic is not encrypted.

Part 9: Verify NAT. 15%

Use appropriate **show and debug commands** to prove the proper functionality.
Annotate and interpret the outputs.

Part 10: Verify the ACLs. 15%

Use appropriate **show commands** to prove the proper functionality.
Annotate and interpret the outputs.

Part 11: Verify OSPF with proper static route distribution. 15%

Use appropriate **show and debug commands** to prove the proper functionality. Interpret the outputs.
Annotate and interpret the outputs.

Part 12: Verify the Internet connectivity. 15%

Use the command **traceroute** and the **Browser** to verify the connectivity to the Internet Server.

Part 13: Verify the DHCP on LAN1 und LAN2. 15%

Use appropriate **show commands** to prove the proper functionality on the routers.
Annotate and interpret the outputs.