Table of Contents

Assignment 2

This project will result in topology assembly, VPN and NAT configuration.

Requirements

Topology will emulate several remote offices. Each office has its own network with several subnetworks. Offices are connected over the Internet. Both Headquarters and branch offices have Staff and Guests subnetworks. HQ office also has Servers subnetwork. Hosts from Staff subnetwork have access to the Servers. Staff at the branch site access HQ Servers via VPN. Staff and Guests at both sites have access to the Internet.

All internal subnetworks at both sites are hidden behind the NAT.

Design

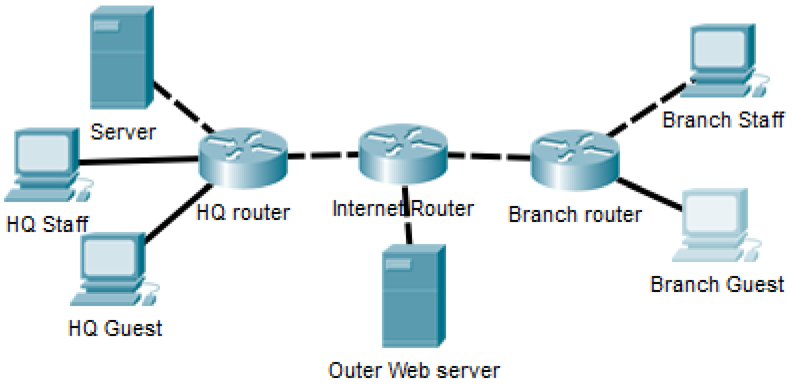

Figure 1. Topology

Built topology is shown on the (Figure 1). Due to limited resources all internal subnetworks have only one host. Detailed description of each node in the network can be found in (Table 2).

First of all, IP addresses were assigned to physical and virtual interfaces on all the routers. After that, static routes were added.

VPN was configured on both routers in the following way. ISAKMP protocol was confogured to use AES with 256bit key for encryption, SHA-512 for hashing; Secret55 was used as a pre-shared key. Transform set XFORM_SB uses AES for encryption and SHA-256 for hashing. On both routers, HQ and Branch, ACL ALLOW_VPN that allows any IP traffic from one site to another was created. More specifically it allows IP traffic from 172.30.0.0/16 to 172.31.0.0/16 and vise versa. This ACL as well as created earlier transfomr set were added to crypto maps IPSEC_TO_HQ(BR)_SB. VPN was then enabled on outside interfaces.

On both routers, class maps TRUSTED_PROTOCOLS_SB and WEB_PROTOCOLS_SB were created. They inspect TCP, UDP, ICMP and HTTP, HTTPS, DNS protocols respectively. ACL ALLOW_ACCES_TO_SERVERS was created on the HQ router. This ACL permits TCP, UDP and ICMP traffic from Branch Staff subnetwork to HQ Servers subnetwork. REMOTE_ACCESS_TO_SERVERS class map uses that ACL.

Security zones were created and assigned to the interfaces on both routers: INTERNET_SB(FastEthernet0/0), STAFF_SB(Vlan 11), GUESTS_SB(Vlan 12). HQ router has another one zone - SERVERS_SB(Vlan 10).

Zone pairs with policy maps and class maps are shown in (Table 1). STAFF->INTERNET and GUEST->INTERNET zone pairs are common for both routers.

Table 1. Zone pairs, policy maps and class maps

Zone pair	Policy map	Class map
INTERNET->SERVERS_SB	INTERNET_TO_SERVERS_SB	REMOTE_ACCESS_TO_SERVERS_SB
STAFF->SERVERS_SB	STAFF_TO_SERVERS_SB	TRUSTED_PROTOCOLS_SB
STAFF->INTERNET_SB	STAFF_TO_INTERNET_SB	TRUSTED_PROTOCOLS_SB
GUEST->INTERNET_SB	GUEST_TO_INTERNET_SB	WEB_PROTOCOLS_SB

In order to comply with NAT requirements, address pool POOL_SB was created with start and end address 172.16.10.2/24 – HQ router outside interface address and 172.16.11.3 – Branch router outside interface address. Extended ACL NAT_ADR_SB denies all taffic between the sites and allows any other traffic. Purpose of such complicated ACL is that routers will not perform address translation for secure traffic. Now all communications with the Internet will be performed via NAT.

Table 2. Nodes description

Device	Interface	IP address	Default gateway	Desciption
HQ Router	FastEthernet0/0	172.16.10.2/24	N/A	Outside interface
	Vlan 10(Fa0/1/0)	172.30.10.1/24	N/A	Servers subnet
	Vlan 11(Fa0/1/1)	172.30.11.1/24	N/A	Staff subnet
	Vlan 12(Fa0/1/2)	172.30.12.1/24	N/A	Guests subnet
VM1	N/A	172.30.10.10/24	172.30.10.1	HQ Server
Laptop	N/A	172.30.11.10/24	172.30.11.1	HQ Staff host
VM2	N/A	172.30.12.10/24	172.30.12.1	HQ Guest host
Internet Router	FastEthernet2/0/1	172.16.10.1/24	N/A	To HQ router
	FastEthernet2/0/2	172.16.11.1/24	N/A	To Branch router
	FastEthernet2/0/3	172.30.11.1/24	N/A	Internet subnet
VM3	N/A	172.16.1.90/24	172.16.1.1	Outer web server
Branch Router	FastEthernet0/0	172.16.11.2/24	N/A	Outside interface
	Vlan 11(Fa0/1/1)	172.31.11.1/24	N/A	Staff subnet
	Vlan 12(Fa0/1/2)	172.31.12.1/24	N/A	Guests subnet
VM4	N/A	172.31.11.10/24	172.31.11.1	Branch Staff host
VM5	N/A	172.31.12.10/24	172.31.12.1	Branch Guest host

Demonstration

Due to lack of time, demonstration video was made in Cisco Packet Tracer environment. Emulated topology was built and configured as closely as possible to the real one. ~~Video can be seen here https://youtu.be/qIjlcfLbaRo .~~