Table of Contents

Assignment 1

This project will result in topology assembly, NAT and Zone-based firewall configuration.

Requirements

Network will have several subnetworks. Each subnetwork will represent either certain department in the company or remote, untrusted networks. In this case there will be following subnetworks: Internet, DMZ, Administrative, Production, Guest, IT. Administrative staff will have web access to the DMZ and to the Internet, and DNS access to the DMZ. Production employees will have web and DNS access to the DMZ. Guests will have web and DNS access to the Internet. IT staff will have all access to all the hosts. Remote hosts will have web access to the DMZ.

All internal subnetworks will be hidden behind the NAT.

Design

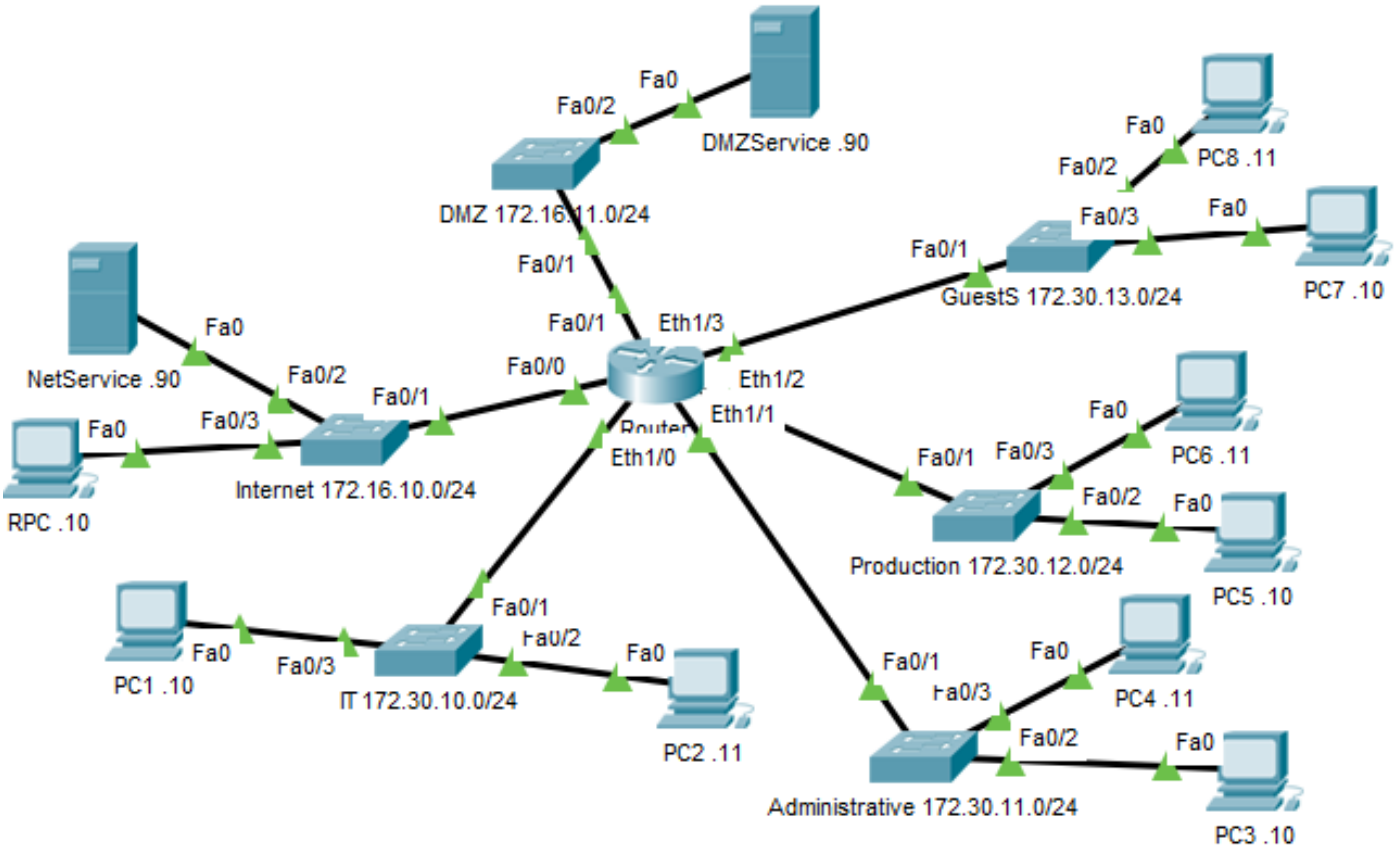

Figure 1. Topology

Built topology is shown on the (Figure 1). All subnetworks have several hosts, and one switch that can be accessed via Telnet. DMZ and Internet subnetworks also have Web servers. Detailed description of each node in the network can be found in (Table 2).

First of all, card with four addittional Ethernet ports was inserted into the router. Now, it is possible to connects all devices into the single network. After that, each device obtained an IP address according to the requirements. Then, Telnet was configured on the switches. After checking connectivity, security policies can be implemented.

Three combinations of protocols can be highlighted: HTTP and HTTPS; HTTP, HTTPS and DNS; ICMP, TCP and UDP. First case results in HTTP_SB class map, which covers web traffic. Next case results in INTERNET_PROTOCOLS_SB class map, which covers web and DNS traffic. Last case results in ALL_PROTOCOLS_SB class map, which covers all the traffic.

After that, security zones were created and assigned to interfaces: IT_SB (Ethernet1/0), ADMINISTRATIVE_SB (Ethernet1/1), PRODUCTION_SB (Ethernet1/2), GUEST_SB (Ethernet1/3), DMZ_SB (FastEthernet0/1), INTERNET_SB (FastEthernet0/0). Then, following zone pairs and policy maps were created (Table 1). Each policy map inspects corresponding class map.

Table 1. Zone pairs, policy maps and class maps

Zone pair	Policy map	Class map
ADMINISTRATIVE->DMZ_SB	ADMINISTRATIVE_TO_DMZ_SB	INTERNET_PROTOCOLS_SB
ADMINISTRATIVE->INTERNET_SB	ADMINISTRATIVE_TO_INTERNET_SB	HTTP_SB
PRODUCTION->DMZ_SB	PRODUCTION_TO_DMZ_SB	INTERNET_PROTOCOLS_SB
GUEST->INTERNET_SB	GUEST_TO_INTERNET_SB	INTERNET_PROTOCOLS_SB
INTERNET->DMZ_SB	INTERNET_TO_DMZ_SB	HTTP_SB
IT->ADMINISTRATIVE_SB	IT_TO_ADMINISTRATIVE_SB	ALL_PROTOCOLS_SB
IT->PRODCUTION_SB	IT_TO_PRODCUTION_SB	ALL_PROTOCOLS_SB
IT->GUEST_SB	IT_TO_GUEST_SB	ALL_PROTOCOLS_SB
IT->DMZ_SB	IT_TO_DMZ_SB	ALL_PROTOCOLS_SB
IT->INTERNET_SB	IT_TO_INTERNET_SB	ALL_PROTOCOLS_SB

In order to comply with NAT requirements, address pool POOL_SB was created with start and end address 172.16.10.1/24 – router outter interface address. Standard ACL PERMIT_ALL_SB permits all traffic from network 172.30.0.0/20. This ACL is needed for NAT configuration, it covers all existing internal subnetworks, except DMZ, that must not have access to any other network. Another NAT rule was created to map 80 port of outter router interface to 80 port of the DMZ server.

Table 2. Nodes description

Device	Interface	IP address	Default gateway	Desciption
Router	FastEthernet0/0	172.16.10.1/24	N/A	Internet interface
	FastEthernet0/1	172.16.11.1/24	N/A	DMZ interface
	Ethernet1/0	172.30.10.1/24	N/A	IT interface
	Ethernet1/1	172.30.11.1/24	N/A	Administrative interface
	Ethernet1/2	172.30.12.1/24	N/A	Production interface
	Ethernet1/3	172.30.13.1/24	N/A	Guest interface
PC1	FastEthernet0	172.30.10.10/24	172.30.10.1	IT host
PC2	FastEthernet0	172.30.10.11/24	172.30.10.1	IT host
IT Switch	Vlan 1	172.30.10.2/24	172.30.10.1	Switch, listens on Telnet port
PC3	FastEthernet0	172.30.11.10/24	172.30.11.1	Administrative host
PC4	FastEthernet0	172.30.11.11/24	172.30.11.1	Administrative host
Administrative Switch	Vlan 1	172.30.11.2/24	172.30.11.1	Switch, listens on Telnet port
PC5	FastEthernet0	172.30.12.10/24	172.30.12.1	Production host
PC6	FastEthernet0	172.30.12.11/24	172.30.12.1	Production host
Production Switch	Vlan 1	172.30.12.2/24	172.30.12.1	Switch, listens on Telnet port
PC7	FastEthernet0	172.30.13.10/24	172.30.13.1	Guest host
PC8	FastEthernet0	172.30.13.11/24	172.30.13.1	Guest host
Guest Switch	Vlan 1	172.30.13.2/24	172.30.13.1	Switch, listens on Telnet port
DMZService	FastEthernet0	172.16.11.90/24	172.16.11.1	DMZ Web server
DMZ Switch	Vlan 1	172.16.11.2/24	172.16.11.1	Switch, listens on Telnet port
NetService	FastEthernet0	172.16.10.90/24	172.16.10.1	Remote Web server
RPC1	FastEthernet0	172.16.10.10/24	172.16.10.1	Remote host
Remote Switch	Vlan 1	172.16.10.2/24	172.16.10.1	Switch, listens on Telnet port

Demonstration

Due to imperfection of the Cisco Packet Tracer NAT and Zone-based firewall cannot be demonstrated together. It will be shown that both NAT and firewall work as expected separately. However, when combined, they cause problems. ~~Video demonstration can be seen here~~ ~~https://www.youtube.com/watch?v=ugolKPHZOwg~~. (however, source video still exists)