МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

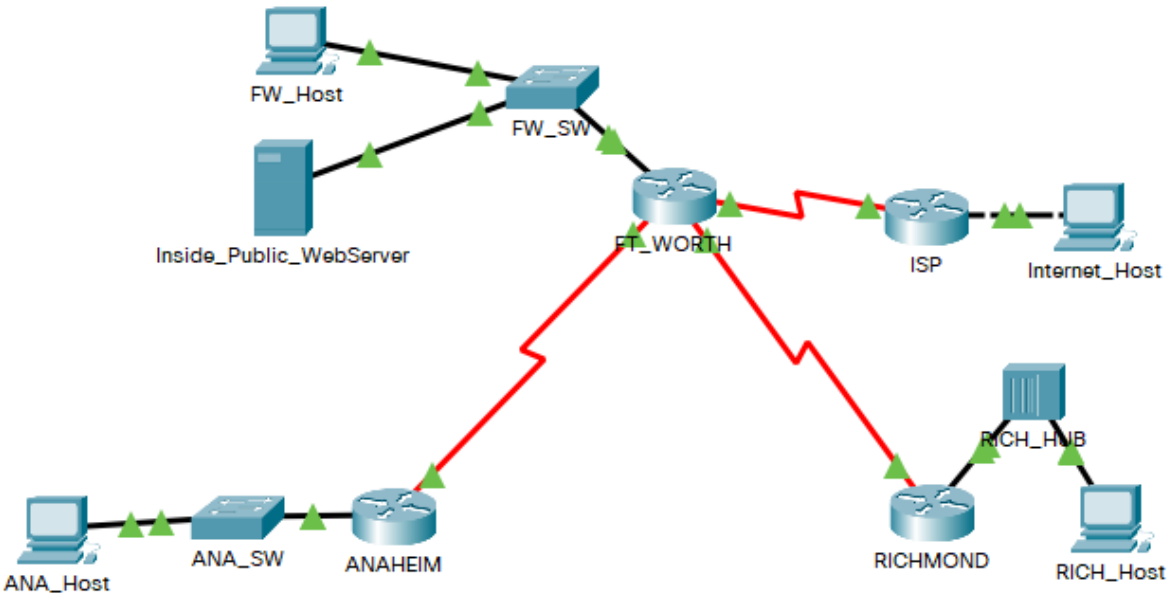
Step 5 Configure Access Control Lists (ACLs)

Отчет по лабораторной работе № 14
по дисциплине «Компьютерные сети»

студента 2 курса группы ИВТ-б-о-202(1)
Шор Константина Александровича

Направления подготовки 09.03.01«Информатика и вычислительная техника»

Симферополь, 2022



1. **ANAHEIM** security policy using ACL number 100:
Hosts attached to the 192.168.1.0/24 LAN should be allowed HTTP and FTP access to all destinations. Configure the HTTP port first, then FTP-data, then FTP. Any other order and you will not get credit.
ANAHEIM hosts should also be able to send ICMP messages to any destination.
All other access is implicitly denied; however, configure the **deny any** statement for documentation purposes.

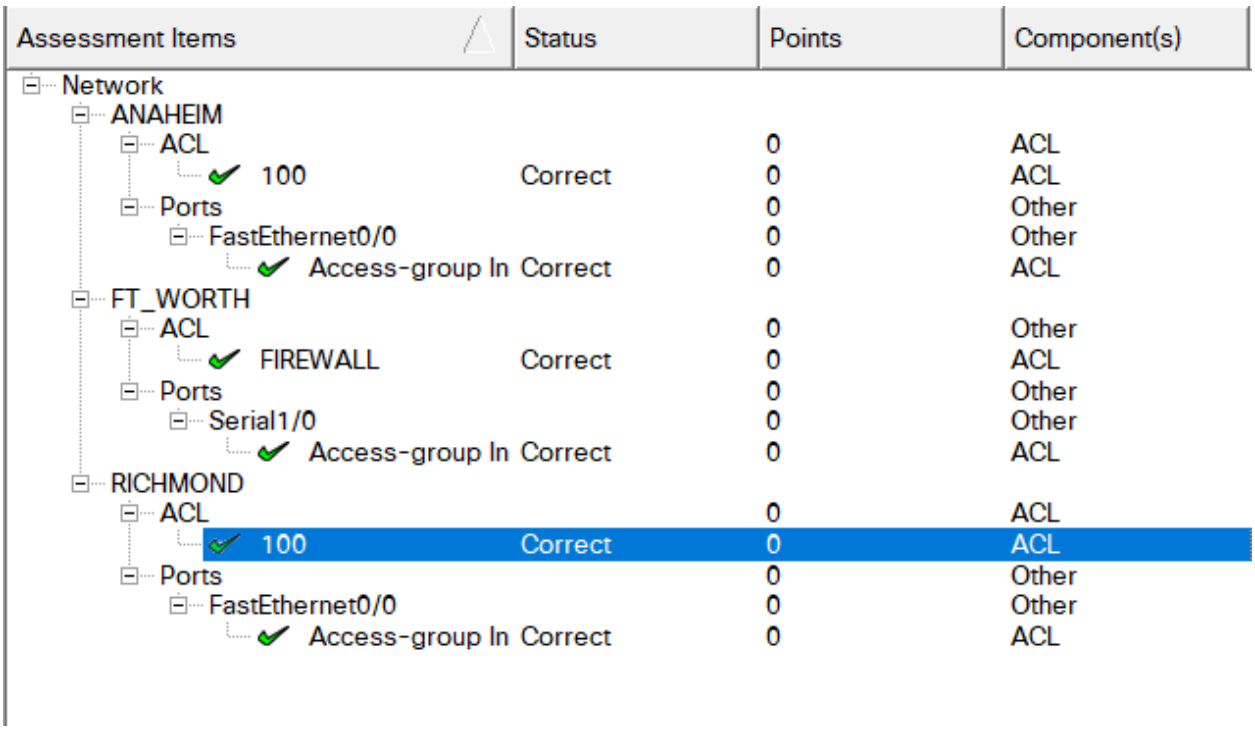
```
ANAHEIM(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 any eq www
ANAHEIM(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 any eq 20
ANAHEIM(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 any eq 21
ANAHEIM(config-ext-nacl)#permit icmp 192.168.1.0 0.0.0.255 any ?
  <0-256>               type-num
  echo                  Echo (ping)
  echo-reply            Echo reply
  host-unreachable      Host unreachable
  net-unreachable       Net unreachable
  port-unreachable      Port unreachable
  protocol-unreachable  Protocol unreachable
  ttl-exceeded          TTL exceeded
  unreachable           All unreachables
  <cr>
ANAHEIM(config-ext-nacl)#permit icmp 192.168.1.0 0.0.0.255 any
ANAHEIM(config-ext-nacl)#deny ip any any
ANAHEIM(config-ext-nacl)#exit
ANAHEIM(config)#fa
ANAHEIM(config)#int
ANAHEIM(config)#interface fa
ANAHEIM(config)#interface fastEthernet 0/0
ANAHEIM(config-if)#ac
ANAHEIM(config-if)#ip ac
ANAHEIM(config-if)#ip access-group 100 in
ANAHEIM(config-if)#
```

2. **RICHMOND** security policy using ACL number 100:
All access from the 192.168.5.0/24 LAN to the 192.168.1.0/24 LAN should be blocked.
All other traffic from the 192.168.5.0/24 LAN should be allowed.

```
RICHMOND>ena
RICHMOND#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RICHMOND(config)#ip ac
RICHMOND(config)#ip access-list ex
RICHMOND(config)#ip access-list extended 100
RICHMOND(config-ext-nacl)#deny ip 192.168.5.0 0.0.0.255 192.168.1.0 0.0.0.255
RICHMOND(config-ext-nacl)#permit ip 192.168.5.0 0.0.0.255 any
RICHMOND(config-ext-nacl)#exit
RICHMOND(config)#int
RICHMOND(config)#interface fa
RICHMOND(config)#interface fastEthernet 0/0
RICHMOND(config-if)#ip ac
RICHMOND(config-if)#ip access-group 100 in
RICHMOND(config-if)#
```

3. **FT_WORTH** security policy using an ACL named **FIREWALL** to filter all inbound traffic from **ISP (Hint:** ACL names are cAsE-sEnSiTiVe):
Allow all ICMP traffic.
Allow inbound HTTP requests for the Inside_Public_WebServer only.
All other access is implicitly denied; however, configure the **deny any** statement for documentation purposes.

```
FT_WORTH>ena
FT_WORTH#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
FT_WORTH(config)#ip ac
FT_WORTH(config)#ip access-list ex
FT_WORTH(config)#ip access-list extended FIREWALL
FT_WORTH(config-ext-nacl)#permit icmp any any
FT_WORTH(config-ext-nacl)#permit tcp any host 137.38.39.40 eq www
FT_WORTH(config-ext-nacl)#deny ip any any
FT_WORTH(config-ext-nacl)#exit
FT_WORTH(config)#int
FT_WORTH(config)#interface se
FT_WORTH(config)#interface serial 1/0
FT_WORTH(config-if)#ip ac
FT_WORTH(config-if)#ip access-group in
% Incomplete command.
FT_WORTH(config-if)#ip access-group FIREWALL in
```



Assessment Items	Status	Points	Component(s)
Network			
ANAHEIM			
ACL		0	ACL
100	Correct	0	ACL
Ports		0	Other
FastEthernet0/0		0	Other
Access-group In	Correct	0	ACL
FT_WORTH			
ACL		0	Other
FIREWALL	Correct	0	ACL
Ports		0	Other
Serial1/0		0	Other
Access-group In	Correct	0	ACL
RICHMOND			
ACL		0	ACL
100	Correct	0	ACL
Ports		0	Other
FastEthernet0/0		0	Other
Access-group In	Correct	0	ACL