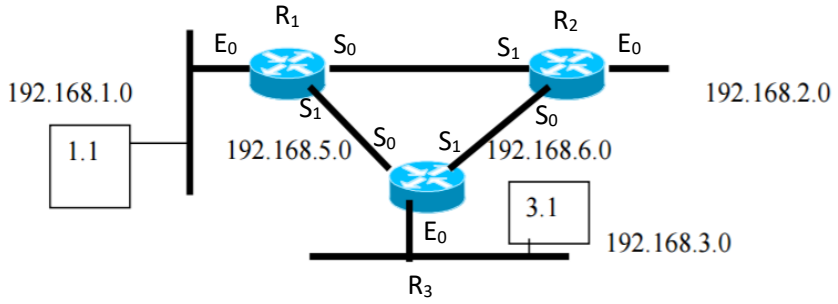
Assignment 2

Zehao Ba(B00732676)

1.



(a) Prevent all traffic from 192.168.2.0 from going to 192.168.1.0

Access-list 1 deny 192.168.2.0 0.0.0.255
Access-list 1 permit any any
Interface E_0 # R_1
Ip access-group 1 out

(b) Prevent all traffic from 192.168.3.1 from going to 192.168.2.1

Access-list 104 deny ip 192.168.3.1 0.0.0.0
192.168.2.1 0.0.0.0
Access-list 104 permit ip any any
Interface E_0 # R_3
Ip access-group 104 in

(c) Prevent FTP access from 2.1 to 3.1

Access-list 101 deny tcp 192.168.2.1 0.0.0.0
192.168.3.1 0.0.0.0 eq.20
Access-list 101 deny tcp 192.168.2.1 0.0.0.0
192.168.3.1 0.0.0.0 eq.21
Access-list 101 permit ip any any
Interface E_0 # R_2
Ip access-group 101 in

(d) Prevent Telnet and FTP access from 3.1 to 1.1

Access-list 102 deny tcp 192.168.3.1 0.0.0.0
192.168.1.1 0.0.0.0 eq.23
Access-list 102 deny tcp 192.168.3.1 0.0.0.0
192.168.1.1 0.0.0.0 eq.20
Access-list 102 deny tcp 192.168.3.1 0.0.0.0
192.168.1.1 0.0.0.0 eq.21
Access-list 102 permit ip any any
Interface E_0 # R3
Ip access-group 102 in

(e) Prevent any SNMP traffic from 2.1 from leaving the network 192.168.2.0

Access-list 103 deny udp 172.168.2.1 0.0.0.0

Any any eq. 161

Access-list 103 permit ip any any

Interface E_0 # R_2
Ip access-group 103 in

2. (a) Prevent traffic from workstation 20.163 from reaching the workstation 70.5 and the tower box 70.2. Traffic from all other hosts/networks should be allowed.

Access-list 1 deny 172.16.20.163 0.0.0.0
Access-list 1 permit any any
Interface E_0 # Calgary
Ip access-group 1 out

(b) Prevent traffic from 80.0 network from reaching 10.0 network. All other traffic must be allowed.

Access-list 2 deny 172.16.80.0 0.0.0.255

Access-list 2 permit any any

Interface E_0 # Edmonton

Ip access-group 2 out

(c) Workstations 50.75 and 50.7 should not be allowed web access on tower box 70.2. All other workstations can.

According to the assumption, there is no new network or host:

Access-list 101 deny tcp 172.16.50.0 0.0.0.255

172.16.70.2 0.0.0.0 eq. 80

Access-list 101 permit tcp any any eq. 80

Interface E1 # Red Deer

Ip access-group 101 in

(d) 80.16 can telnet to 40.89. No one else from 80.0 can telnet to 40.89. Any other host from any other subnet can telnet to 40.89.

Assumption: other protocols are not allowed to 40.89

Access-list 102 permit tcp 172.16.80.16 0.0.0.0

172.16.40.89 0.0.0.0 eq. 23

```
Access-list 102 deny tcp 172.16.80.0 0.0.0.255
                                172.16.40.89 0.0.0.0 eq. 23
Access-list 102 permit tcp 172.16.0.0 0.0.255.255
                                172.16.40.89 0.0.0.0 eq. 23
Interface E0 # Red Deer
Ip access-group 102 out
```

(e) 70.5 can ftp to the Edmonton router. No other host can.

```
Access-list 103 permit tcp 172.16.70.5 0.0.0.0
                                172.16.30.1 0.0.0.255 eq. 20
Access-list 103 permit tcp 172.16.70.5 0.0.0.0
                                172.16.30.1 0.0.0.255 eq. 21
Access-list 103 deny tcp 172.16.0.0 0.0.255.255
                                172.16.30.1 0.0.0.255 eq. 20
Access-list 103 deny tcp 172.16.0.0 0.0.255.255
                                172.16.30.1 0.0.0.255 eq. 21
Access-list 103 permit tcp 172.16.70.5 0.0.0.0
                                172.16.20.1 0.0.0.255 eq. 20
Access-list 103 permit tcp 172.16.70.5 0.0.0.0
                                172.16.20.1 0.0.0.255 eq. 21
Access-list 103 deny tcp 172.16.0.0 0.0.255.255
                                172.16.20.1 0.0.0.255 eq. 20
Access-list 103 deny tcp 172.16.0.0 0.0.255.255
                                172.16.20.1 0.0.0.255 eq. 21
Access-list 103 permit tcp 172.16.70.5 0.0.0.0
                                172.16.10.1 0.0.0.255 eq. 20
Access-list 103 permit tcp 172.16.70.5 0.0.0.0
                                172.16.10.1 0.0.0.255 eq. 21
Access-list 103 deny tcp 172.16.0.0 0.0.255.255
```

172.16.10.1 0.0.0.255 eq. 20

Access-list 103 deny tcp 172.16.0.0 0.0.255.255

172.16.10.1 0.0.0.255 eq. 21

Interface S_0 # Edmonton

Ip access-group 103 in

Interface E_0 # Edmonton

Ip access-group 103 in

Interface E_1 # Edmonton

Ip access-group 103 in

3. For question 3, input the acl file name and the packet file name
   1) ACL1.txt is:
   access-list 1 deny 172.16.4.13 0.0.0.0
   access-list 1 deny 172.16.5.0 0.0.0.255
   access-list 1 permit 172.16.3.0 0.0.0.255
   interface EO
   ip access-group 1 out

   packet1.txt is:
   172.16.4.13 172.16.3.2
   172.16.3.3 172.16.3.1
   172.16.5.2 172.16.3.4

   The output is:

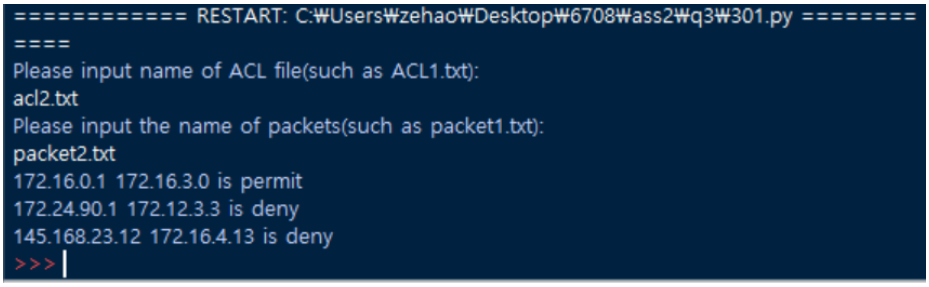
```
========== RESTART: C:₩Users₩zehao₩Desktop₩6708₩ass2₩q3₩301.py ========
====
Please input name of ACL file(such as ACL1.txt):
acl1.txt
Please input the name of packets(such as packet1.txt):
packet1.txt
172.16.4.13 172.16.3.2 is deny
172.16.3.3 172.16.3.1 is permit
172.16.5.2 172.16.3.4 is deny
>>>
```

   2) ACL2.txt is:
   access-list 2 permit 172.16.0.0 0.0.255.255
   interface E0
   ip access-group 1 out

   packet2.txt is:
   172.16.0.1 172.16.3.0
   172.24.90.1 172.12.3.3

145.168.23.12 172.16.4.13

The output is:



Etc.

4. Research

- **Features**

  In 2016, Cisco published Firepower Next-Generation Firewall (NGFW) which can block more malicious threats and keep your system secure. The new generation firewall can block more malware no matter known or unknown. It operates better by combining other Cisco products, for example Advanced Malware Protection. Trust anchor technologies provides Cisco highly secure foundation. The trust anchor provides three features, image signing, secure boot, and trust anchor module. Image signing is a set of cryptographically signed images which insure the authentication and non-modification of firmware, BIOS, etc. Secure boot uses on layer protection to prevent illegal modified firmware. Last one is trust anchor module, it is a strong cryptographic solution, which provides authentic hardware assurance so that the resources can be identified by Cisco. [1]

- **New trends and NGFW corporation:**
  - Central, powerful management.

    Too much firewalls or management components will block the usage of rare resources. A centralized management system is available to gather the data from security defences and help the security team to give the responses faster. Central management means a system which can be controlled, watched and set up by a glass pane. Besides, it can also provide the routine selection automatically, element reuse, and other functions so that it can give the most efficient with less effort. [2]

  - User and application control

    Keep human out of the loop is a key concept during the product design because the employees may cause malicious unconsciously, which is called user control. For application control, it is not only ports and protocols' visible, but the characteristics of user's behaviours. Technologies have already abled to accomplish application control by accumulating user identity, human role and other policies. [2]

- High availability

  It is not allowed to shut the machine down even during the routine maintenance time within a company. An active-active clustering keeps the NGFW continuous operating during the updating and maintaining of system. Besides, this function can operate the process flexibility during the heavy traffic. Upgrading node-by-node is necessary for clusters without breaking services, different software versions or various hardware changes. [2]

- Plug and play deployment

  A NGFW has plug-and-play feature so that you can use it in different locations because it allows cloud installation and configuration. In this way, the NGFW can be installed remotely by anyone after plugging the power and connecting network physically. Updates and upgrades can also be done by automatically remote operate. [2]

- Deep packet inspection

  NGFW has deep packet inspection (DPI) to exam various pieces of every packet. It exam the malicious virus thoroughly, such as Trojans, spam and other violations during the protocol communications. There are several packet data analysis methods, such as data stream-based inspection, policy configurations, etc. NGFW which has DPI should also be updated automatically and regularly. [2]

- AET protection

  AET means advanced evasion techniques. AET is not useful because of its unstable and dangerous during the attack. Therefore, an AET protection is necessary to monitor the traffic within multiple protocols and layers. An AET protection can normalize the multi-layer traffic, provide full-stack services during deconstruct and decode the packet. It also applies on thorough data analysis without effecting the network performance. It is product into the core of NGFW. [2]

- Multi-tenancy

  A multi-tenancy NGFW allows large enterprises or network service providers so that it distinct the domains without influencing the end users' efficiency. It can be managed separately according to different business units, locations or user organizations. It can also make inter-operable, which mean keep the entities separately, at the same time, give the same managements. [2]

- Adaptable, convertible architecture

  This feature allows the user to operate the NGFW efficiency according to the deployment so that the NGFW can be a software of physical or virtual appliance with wider range of budget and flexible structure. What is more, this NGFW can also change by requirement to serve updated firewalls. [2]

- Enterprise level VPN

NGFW with a powerful VPN allows the connection be resilient and flexible. There are a lot of NGFWs use IPsec VPN to deal with security arrangements so that it is unnecessary to change manually. If the VPN can be part of the NGFW, combining with IPsec VPN, to provide an available VPN connection with more probabilities. [2]

- Virtualization

  The virtual appliance can run software or operating system, and security structures independently. Visualization makes the security gateway configurations are divided and managed separately on a physical NGFW device. This feature allows the managed security service providers to deal with multiple users' security problem in same physical NGFW. [2]

It can be found NGFW incorporates well with these features, especially, it must have bigger power and better central management, user application control, high availability, these are the lowest standards of NGFW. It is undoubted that NGFW will improve fast and satisfies all people need in the future. NGFW is much better and secure for industry to keep safe than traditional one. It is makeable that malicious application, botnet, worm and APT attack mention companies to improve the firewall function.

Bibliography

[1] "Cisco," Cisco NGFW, 2016. [Online]. Available: http://www.cisco.com/c/dam/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-736661.pdf.

[2] P. Calhoun, "Security week," Wired Business Media, 24 July 2014. [Online]. Available: http://www.securityweek.com/10-must-have-features-your-next-generation-firewall-buyers-checklist.