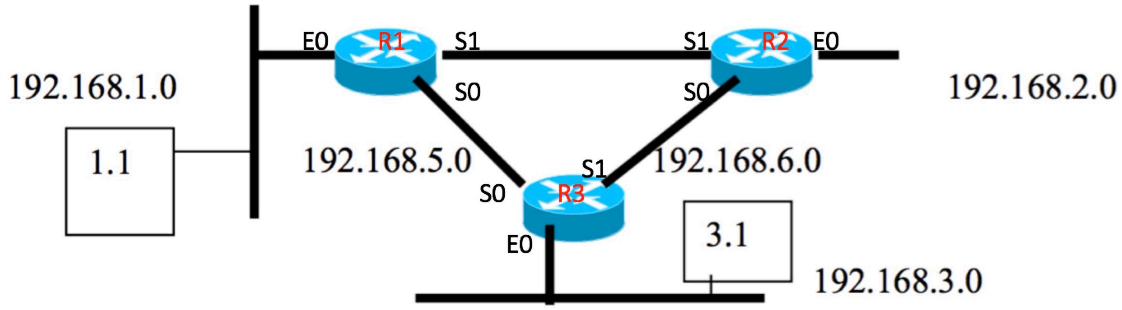
# Assignment02
# B00756586
# Zewen Wang

**Q1**:

I added interfaces and router names for routers, which is shown from the picture below. The access-list is based this picture.



a)standard

```
Access-list      1      deny      192.168.2.0      0.0.0.255
Access-list      1      permit    any
interface E0 # R1
ip access-group 1    out
```

b)extended

```
Access-list     101     deny      IP      192.168.3.1      0.0.0.0      192.168.2.1      0.0.0.0
Access-list     101     permit    IP                   any                           any
interface E0 # R3
ip access-group 101 in
```

c)extended

```
Access-list    102     deny      TCP     192.168.2.1     0.0.0.0     192.168.3.1     0.0.0.0  eq 20
Access-list    102     deny      TCP     192.168.2.1     0.0.0.0     192.168.3.1     0.0.0.0  eq 21
Access-list    102     permit    IP                  any                         any
interface E0 # R2
ip access-group 102 in
```

d)extended

```
Access-list    103     deny      TCP     192.168.3.1     0.0.0.0     192.168.1.1     0.0.0.0  eq 23
Access-list    103     deny      TCP     192.168.3.1     0.0.0.0     192.168.1.1     0.0.0.0  eq 20
Access-list    103     deny      TCP     192.168.3.1     0.0.0.0     192.168.1.1     0.0.0.0  eq 21
Access-list    103     permit    IP                  any                         any
interface E0 # R3
ip access-group 103 in
```

e)extended

```
Access-list    104     deny      UDP     192.168.2.1     0.0.0.0                 any      eq 161
Access-list    104     permit    IP                  any                         any
interface E0 # R2
ip access-group 104 in
```

## Q2:

a)standard:

```
Access-list    1    deny     172.16.20.163    0.0.0.0
Access-list    1    permit                    any
interface E0 # Calgory
ip access-group 1   out
```

b)standard:

```
Access-list    2    deny     172.16.80.0      0.0.0.255
Access-list    2    permit                    any
interface E0 # Edmonton
ip access-group 2   out
```

c)extended

```
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   IP               any                        any
interface E1 # Red Deer
ip access-group 101 in
```

d) extended: Assuming all other protocols are permitted

```
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   IP                 any                       any
interface E1 # Calgory
ip access-group 102 in
```

e)extended:

```
Access-list   103   permit   TCP   172.16.70.5   0.0.0.0   any    eq 20
Access-list   103   permit   TCP   172.16.70.5   0.0.0.0   any    eq 21
Access-list   103   deny     TCP                 any       any    eq 20
Access-list   103   deny     TCP                 any       any    eq 21
Access-list   103   permit   IP                  any       any
interface S0 # Edmonton
ip access-group 103 in
```

extended:

```
Access-list   104   deny     TCP                 any       any    eq 20
Access-list   104   deny     TCP                 any       any    eq 21
Access-list   104   permit   IP                  any       any
interface E0 # Edmonton
ip access-group 104 in
```

extended:

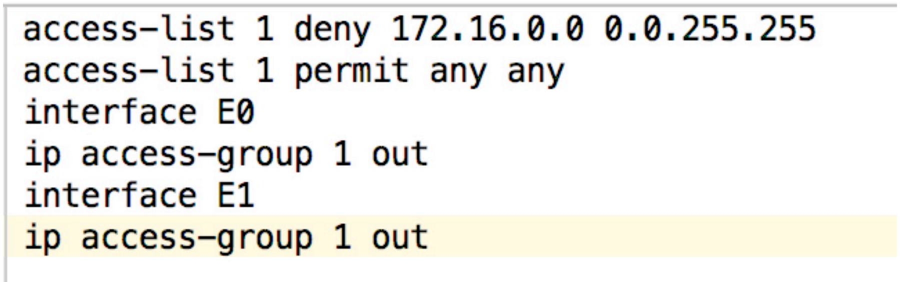
```
Access-list    105    deny      TCP                  any          any      eq 20
Access-list    105    deny      TCP                  any          any      eq 21
Access-list    105    permit     IP                  any          any
interface E1 # Edmonton
ip access-group 105 in
```

Q3:

I use python to perform ACL operation. Standard.py is to perform standard ACL, and extended.py is to perform extended ACL. I just write some examples for standard and extended.

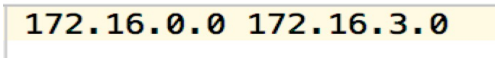
**Standard:**

**Sample 1)** The file file01.txt is to store standard access-list



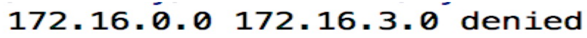
```
access-list 1 deny 172.16.0.0 0.0.255.255
access-list 1 permit any any
interface E0
ip access-group 1 out
interface E1
ip access-group 1 out
```

The file file02.txt is to store the standard packet



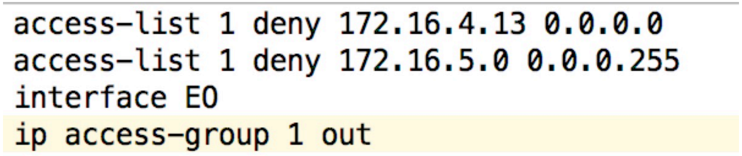
```
172.16.0.0 172.16.3.0
```

The result of this sample is shown below:



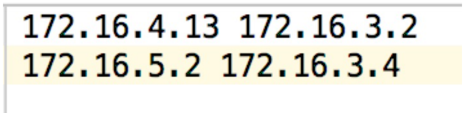
```
172.16.0.0 172.16.3.0 denied
```

**Sample 2)** The file file01.txt is to store standard access-list



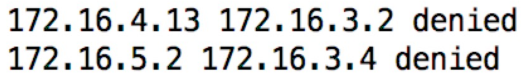
```
access-list 1 deny 172.16.4.13 0.0.0.0
access-list 1 deny 172.16.5.0 0.0.0.255
interface E0
ip access-group 1 out
```

The file file02.txt is to store the standard packet



```
172.16.4.13 172.16.3.2
172.16.5.2 172.16.3.4
```

The result of this sample is shown below:



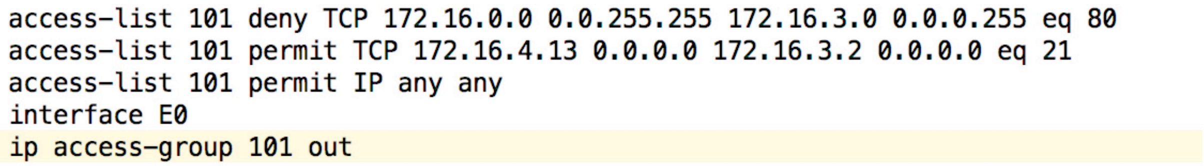
```
172.16.4.13 172.16.3.2 denied
172.16.5.2 172.16.3.4 denied
```

**extended:**

For extended ACL, we have to consider protocol, but because of limited space, I just consider several protocols, FTP, SSH, Telnet, HTTP, SNMP and IP.

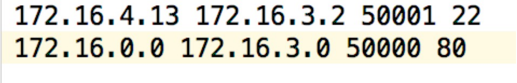
**Sample:**

**The file extended_file01.txt is to store extended access-list**



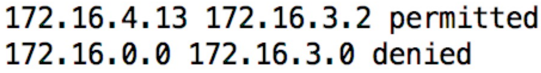
```
access-list 101 deny TCP 172.16.0.0 0.0.255.255 172.16.3.0 0.0.0.255 eq 80
access-list 101 permit TCP 172.16.4.13 0.0.0.0 172.16.3.2 0.0.0.0 eq 21
access-list 101 permit IP any any
interface E0
ip access-group 101 out
```

**The file extended_file02.txt is to store the extended packet, the third column is source port number and the fourth column is the destination port number.**



```
172.16.4.13 172.16.3.2 50001 22
172.16.0.0 172.16.3.0 50000 80
```

**The result of this sample can be seen below:**



```
172.16.4.13 172.16.3.2 permitted
172.16.0.0 172.16.3.0 denied
```

Q4:

**(1)One commercially available gateway firewall**

**Cisco Virtual Security Gateway Firewall**

The Cisco Virtual Security Gateway (VSG)[1] is a virtual firewall appliance that provides trusted access to virtual data and cloud environments. It enables a broad set of workloads which have varied security profiles to share a common compute infrastructure in a virtual data center private cloud or in a public cloud. The features of this firewall are as followed[2]:

- Help reduce errors and improve cooperation across server, network, and security teams while performing separate administrative responsibilities.
- Flexible deployment. This firewall supports Layer 3 and Layer 2 modes and protects multiple physical servers.
- Performance acceleration**.** This firewall offloads packet-intensive processing to optimize performance.
- High availability**.** Deploying this firewall in active-standby mode helps ensure high availability.
- Cloud security**.** This firewall supports dynamic provisioning of security policies and trust and extends zone-based firewalling service to virtual machines on VXLAN through updated segmentation features.

**(2) New trends in firewall design—Next-Generation Firewall**

**Definition:**

A Next-Generation Firewall (NGFW) [3] is an integrated network platform that is a part of the third generation of firewall technology, it is also an enterprise firewall.

**Technical Features:**

1. **Next-Generation Firewall VS. Traditional Firewall[3]**

   The goal of next-generation firewalls is to include more layers of the OSI model, improve filtering of network traffic which depends on the packet contents.

   - Compared with traditional firewall, NGFWs include the typical functions of traditional firewall, such as packet filtering, NAT, URL blocking, stateful inspection and virtual private network(VPN) support.
   - Protect against viruses, spam, spyware, intrusions and other threats with a proven and high-performance in NGFWs. [4]
   - Perform deeper inspection compared to stateful inspection by the previous generation firewalls.
   - NGFWs use a more thorough inspection style, checking packet payloads and matching signatures for harmful activities such as exploitable attacks and malware. [5]
   - NGFWs combines a traditional firewall with other network device filtering functionalities, such as an intrusion prevention system (IPS).

2. **Features of Next-Generation Firewall[6]**

   **(1) Central, Powerful Management**

   A more centralized management system can aggregate data across security defenses and give security team the ability to respond quickly.

**(2) User and Application Control**
User and Application Control is still important for NGFWs because of Internet continues to offer myriad places to lure employees away from productive activities.

**(3) High Availability**
The key feature to achieve high availability and resiliency is the use of active-active clustering of NGFWs.

**(4) Plug and Play Deployment**
If an enterprise has a lot of distributed locations, Plug and Play Deployment is a must-have feature for firewall.

**(5) Deep Packet Inspection**
Deep Packet Inspection ensures the various pieces of each packet are thoroughly examined to identify malformed packets, errors, known attacks and any other anomalies.

**(6) AET Protection**
Advanced evasion techniques, AET protection technologies remove obfuscations, so traffic can be thoroughly inspected across multiple protocols and layers, providing full-stack, multi-layer traffic. When AET protection is built right into the core of the NGFW, even the most thorough data analysis and normalization does not impact network performance.

**(7) Multi-Tenancy**
This feature, Multi-Tenancy, ensures distinction between domains to properly secure end users without sacrificing efficiency.

**(8) Adaptable, Convertible Architecture**
The architecture of NGFW needs to be adaptable and convertible so people can most effectively deploy security as they need it.

**(9) Enterprise level VPN**
NGFWs can add even more power to your VPN by combining IPsec VPN with other advanced technologies, such as those that may combine links or tunnels to produce a cost-effective and highly available VPN connection.

**(10) Virtualization**
With virtual appliances, people can easily and independently deploy a comprehensive security infrastructure using virtual machines.

Compared with new trends of firewalls, Cisco Virtual Security Gateway Firewall incorporate several features of NGFWs, which are High Availability, Virtualization Adaptable, Convertible Architecture, Deep Packet Inspection, Central, Powerful Management and high-performance.

# Reference:

[1](2017) Cisco Virtual Security Gateway. In: Cisco. http://www.cisco.com/c/en/us/products/switches/virtual-security-gateway/index.html. Accessed 27 Feb 2017

[2] (2014) Cisco Virtual Security Gateway Overview. In: Cisco. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/vsg/sw/4_2_1_VSG_1_1/vsg_configuration/guide/VSG_Config_Guide/vsg_config_intro.html#pgfId-1056592. Accessed 27 Feb 2017

[3] (2017) Next-Generation Firewall. In: Wikipedia. https://en.wikipedia.org/wiki/Next-Generation_Firewall. Accessed 27 Feb 2017

[4]Next-Generation Firewall Security Solutions | SonicWall. In: Next-Generation Firewall Security Solutions | SonicWall. https://www.sonicwall.com/solutions/next-generation-firewall/. Accessed 27 Feb 2017

[5] What is next-generation firewall (NGFW)? - Definition from WhatIs.com. In: SearchSecurity. http://searchsecurity.techtarget.com/definition/next-generation-firewall-NGFW. Accessed 27 Feb 2017

[6] 10 Must-Have Features for Your Next Generation Firewall Buyers Checklist. In: Information Security News, IT Security News & Expert Insights: SecurityWeek.Com. http://www.securityweek.com/10-must-have-features-your-next-generation-firewall-buyers-checklist. Accessed 27 Feb 2017