CSCI 6708 NETWORK SECURITY
ASSIGNMENT NO. 2

QUESTION NO.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 IP any any
interface E0
ip-access-group 1 out
```

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

```
access-list 2 deny 192.168.3.1 0.0.0.0
access-list 2 permit IP any any
interface E1
ip-access-group 2 out
```

(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 E0
ip access-group 101 out
```

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

```
access-list 101 deny TCP 192.168.3.1 0.0.0.0 192.168.2.1 0.0.0.0 eq 20
access-list 101 deny TCP 192.168.3.1 0.0.0.0 192.168.2.1 0.0.0.0 eq 21
access-list 101 deny TCP 192.168.3.1 0.0.0.0 192.168.2.1 0.0.0.0 eq 22
access-list 101 permit IP any any
Interface E0
ip access-group 101 out
```

QUESTION NO.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 172.16.0.0 0.0.255.255
access-list 1 permit IP any any
interface CalgaryE0
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 1 deny 172.16.80.0 0.0.0.255
access-list 1 permit 172.16.0.0 0.0.255.255
access-list 1 permit IP any any
interface EdmontonE0
ip access-group 1 out
```

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

```
access-list 101 deny TCP 172.16.50.75 0.0.0.0 172.16.70.2 0.0.0.0 eq 80
access-list 101 deny TCP 172.16.50.7 0.0.0.0 172.16.70.2 0.0.0.0 eq 80
access-list 101 permit ip 172.16.0.0 0.0.255.255 172.16.70.2 0.0.0.0
access-list 101 permit IP any any
```

interface RedDeerE1
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.

access-list 101 deny TCP 172.16.80.0 0.0.0.255 172.16.40.89 0.0.0.0 eq 23
access-list 101 permit TCP 172.16.80.16 0.0.0.0 172.16.40.89 0.0.0.0 eq 23
access-list 101 permit TCP 172.16.0.0 0.0.255.255 172.16.40.89 0.0.0.0 eq 23
access-list 101 permit IP any any
interface CalgaryE1
ip access-group 101 in

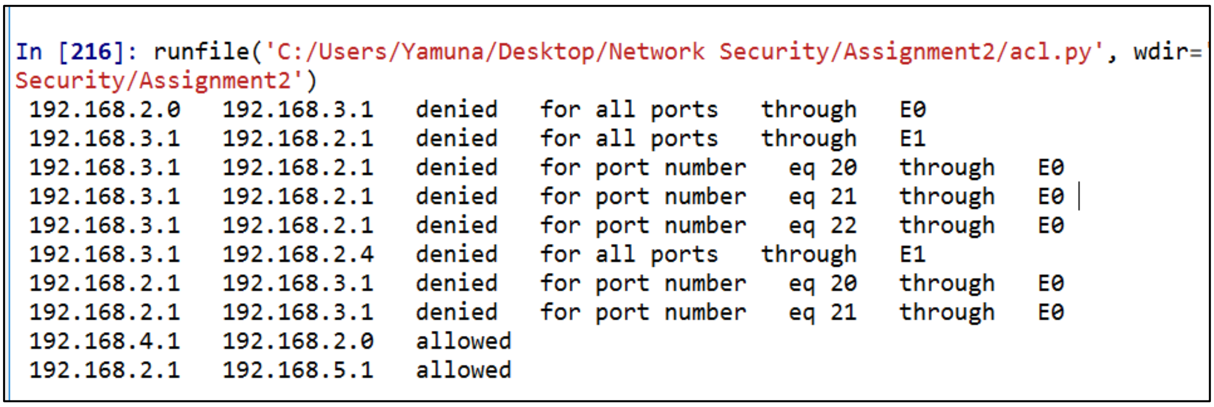
(e) 70.5 can ftp to the Edmonton router. No other host can.

access-list 101 permit TCP 172.16.70.5 0.0.0.0 172.16.30.1 0.0.0.0 eq 20
access-list 101 permit TCP 172.16.70.5 0.0.0.0 172.16.30.1 0.0.0.0 eq 21
access-list 101 deny IP 172.16.0.0 0.0.255.255 172.16.30.1 0.0.0.0
access-list 101 permit IP any any
interface CalgaryE0
ip access-group 101 out

QUESTION NO.3 – ACL SIMULATION

Simulation code is written in python, code attached “acl.py”
Input files “acl.csv” contains the Access Control List and “packets.py” has the source and destination addresses. The input files are also attached to run with the code.

OUTPUT



```
In [216]: runfile('C:/Users/Yamuna/Desktop/Network Security/Assignment2/acl.py', wdir=
Security/Assignment2')
 192.168.2.0   192.168.3.1   denied   for all ports   through   E0
 192.168.3.1   192.168.2.1   denied   for all ports   through   E1
 192.168.3.1   192.168.2.1   denied   for port number   eq 20   through   E0
 192.168.3.1   192.168.2.1   denied   for port number   eq 21   through   E0
 192.168.3.1   192.168.2.1   denied   for port number   eq 22   through   E0
 192.168.3.1   192.168.2.4   denied   for all ports   through   E1
 192.168.2.1   192.168.3.1   denied   for port number   eq 20   through   E0
 192.168.2.1   192.168.3.1   denied   for port number   eq 21   through   E0
 192.168.4.1   192.168.2.0   allowed
 192.168.2.1   192.168.5.1   allowed
```

QUESTION NO.4

INTRODUCTION

Gateway firewalls also known as Proxy firewall are used to maintain the transparency between server and client. Gateway firewalls work in application layer and hence provide better inspection capability. This firewall stands between the user and network, hence the name Gateway firewall. All packets entering the network passes through this firewall. The difference between the conventional firewall and the gateway firewall is that, gateway firewall works in the application layer, hence these firewalls can be programmed to allow or deny filtering traffic based on service. Even specific functions of applications can be filtered using this functionality, one such example is Squid Proxy server.

BENEFITS OF PROXY FIREWALL

1. The gateway understands the application as it works in application layer, hence the packet inspection is deeper.
2. This firewall can be used to control traffic both ways, external to internal and internal to external.
3. Since it is a single point of contact, it provides better access control to the services of network and internet.
4. Extensive logs are collected that helps the network administrator.
5. Traffic filtering can be done on the content of data as well, based on some rules.
6. Network infrastructure and information about the workstations and servers is protected from moving outside.

DISADVANTAGES OF PROXY FIREWALL

1. For the proxy firewalls to understand the applications in a deeper level, that many number of proxy server applications has to be installed as number of services that it needs to understand.
2. Since proxy firewalls are the single point of contact to the external clients, if this server fails, the entire network is considered down. Hence it needs a backup server for failovers.
3. All clients in the network should be configured to go through the proxy firewall. This has to be set as the Gateway IP in browser configurations.

USERGATE PROXY FIREWALL

UserGate Proxy Firewall is an affordable and user friendly software. It is a software alternative to many of the hardware gateway firewalls. It is used by 40,000 businesses and enterprises across the globe. UserGate Proxy Firewall is a one stop gateway firewall solution combining a network firewall, gateway antivirus, router, intrusion detection and prevention, web filtering, VPN server and other important functions. It allows user to manage optimize bandwidth, network traffic and provide Internet access control.

UserGate Proxy Firewall can be used on any Windows operating system and works as a gateway. It provides web security, Internet access sharing and traffic management. UserGate works based on the user’s account and security policies. It lets administrators to control the flow of traffic and track web pages accessed by employees. Many policies can be set to filter traffic in this firewall.

Advanced Firewall

UserGate firewall provides LAN protection against attacks from hacker and other types of protocol based intrusions by filtering traffic through particular ports. Ports specified in the proxy settings as well as ports specified in Port Mapping, are added in automatically generated firewall rules. UserGate’s firewall also process packets not processed by NAT rules. If a packet is already processed by the NAT driver, it will be ignored by the UserGate firewall.

Web Filtering and Access Control

User-based access management

UserGate Proxy Firewall creates user accounts for which Internet access is allowed or denied, rules to filter traffic are applied for the same statistics are calculated. User settings are created based on some specific parameters line IP or MAC address, username/password, Windows login.

To make traffic management simple, users are combined into groups by using the "Groups" feature. One another way to create groups is through one of the authorization methods. Network

Administrators can choose any of the above methods to manage multiple users, or computers, and sub-networks.

Categorized URL filtering

In order avoid users using internet in a wrong way, or to minimize problems caused by illegal use of the Internet, web filtering otherwise known as content-filtering is strongly recommended as a part of a company's security defences.

Entensys URL Filtering module of this gateway firewall helps to add extra security to local network. It is designed to provide administrative control over Internet downloads and also restricting access to all dangerous web sites.

Application Firewall

Many real-time communications like instant messaging, chat applications such as IRC, web conference and networking tools are used regularly in many organizations. Application filtering is created to protect against all possible security threats posed by such Internet based applications. The purpose of it is two-fold, which helps administrators restrict personal use of Internet like instant messengers or peer-to-peer clients also by protecting a local network from application based Internet threats.

Speed limitations and traffic quotas

UserGate is designed flexible in a way it allows network administrators to control traffic speed. There are two modules in where speed limits can be specified one is "Traffic policy" and other is "Bandwidth management". Traffic policy is used to define rules which can be applied to certain users and user groups. Bandwidth management is used to restrict traffic based on certain parameters like a specific adapter, protocols like TCP or UDP, based on source and destination IP address, and/or port.

Traffic quotas and time restrictions are defined to user-based management and it allows to set the limits for a particular user or user group. When defining a traffic quota, a network administrator has plenty of ways to define a rule that fits a situation. For example, a rule can be set to activate when some of the requirements such as a particular protocol or time of day, are met.

Threat Protection

To filter viruses, worms, Trojan horses, ransomware and spyware from infesting a network with the following three integrated AV engines - Kaspersky, Panda, and Avira. These antivirus programs can scan all web traffic, FTP traffic, email attachments and downloads. They are updated automatically with the latest virus definitions.

Traffic Management

It helps guarantee the bandwidth levels that are essential to serve business critical applications. A complete library of pre-defined applications united with granulated user and time based rules make it easy to control non business related applications in real-time to guarantee optimal quality of service.

REFERENCES

[1] World of Security!!!, “Proxy Firewall and Gateway Firewall Introduction: world of securtiy” 2010, http://securityworld.worldiswelcome.com/proxy-firewall-and-gateway-firewall-introduction.

[2] Entensys, “UserGate Proxy & Firewall”, https://www.entensys.com/products/usergate-proxy-and-firewall/benefits