

Network Segmentation Strategy

Andree Salvo

Southern New Hampshire University

CYB 220-10030 – 6-2 Project Two

Instructor: Wesley Buchan

Network Segmentation Strategy

I. Configuration

A. Host-based firewall policy

Andree Salvo
Course: CYB 220-10030
Instructor: Wesley Buchanan

Server2

Physical Config Services **Desktop** Programming Attributes

Firewall [X]

Service ☐ On ☒ Off

Interface: FastEthernet0

Inbound Rules

Action: [Dropdown] Protocol: [Dropdown]

Remote IP: [Text] Remote Wildcard Mask: [Text]

Remote Port: [Text] Local Port: [Text]

[Save] [Remove] [Add]

Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1 Allow	ICMP	192.168.1.96	0.0.0.0	-	-

B. FTP Server

Andree Salvo
Course: CYB-220-10030
Instructor: Wesley Buchanan

Server2

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP**
- IoT
- VM Management
- Radius EAP

FTP

Service ☐ On ☒ Off

User Setup

Username: [Text] Password: [Text]

☐ Write ☐ Read ☐ Delete ☐ Rename ☐ List

	Username	Password	Permission
1	cisco	cisco	RWDNL
2	jsmith	PassW0rd	RL
3	bjones	Password1234	RL
4	admin01	Pa\$\$w0rD1234	RWDNL

[Add] [Save] [Remove]

C. Network-based firewall policy

Andree Salvo
Course: CYB 220-10030
Instructor: Wesley Buchan

Office Router

Physical Config CLI Attributes

IOS Command Line Interface

```

Switching Software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet6/0, changed state to up
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Office_Router>enable
Office_Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Office_Router(config)#ip access-list extended webserver
Office_Router(config-ext-nacl)#permit tcp host 192.168.3.2 any eq www
Office_Router(config-ext-nacl)#exit
Office_Router(config)#exit
Office_Router#
%SYS-5-CONFIG_I: Configured from console by console

Office_Router#show access
Extended IP access list webserver
    10 permit tcp host 192.168.3.2 any eq www
Office_Router#

```

II. Rationale

- A. The network was separated from the FTP server, this rule was created by only allowing traffic from the IP address from the admin network through its firewall. When this rule is in place the server will only allow traffic from the admin network. Moreover, this would block sorts of traffic from the other IP addresses.
- B. The least privilege is only assigned to users based on their role, whether its granting access or denying access. From the configuration FTP server, “Jsmith and Bjones” were the only two

people who only had read/list access, while “admin01” has full administrative access rights. This helps minimize risk and prevents anyone trying to tamper with the network.

- C. A firewall based on a network helps isolate traffic by determining what devices can communicate with each other. In this case, the firewall rules (ACLs) is intended that only the admin network can only reach the FTP server and that only the kiosk can communicate with the web server on port 80. This keeps the services separated and reduces the chances that someone will log in and mess around with something they shouldn't.