

Network Segmentation Strategy

William Pascoe

CYB-220 Network Security

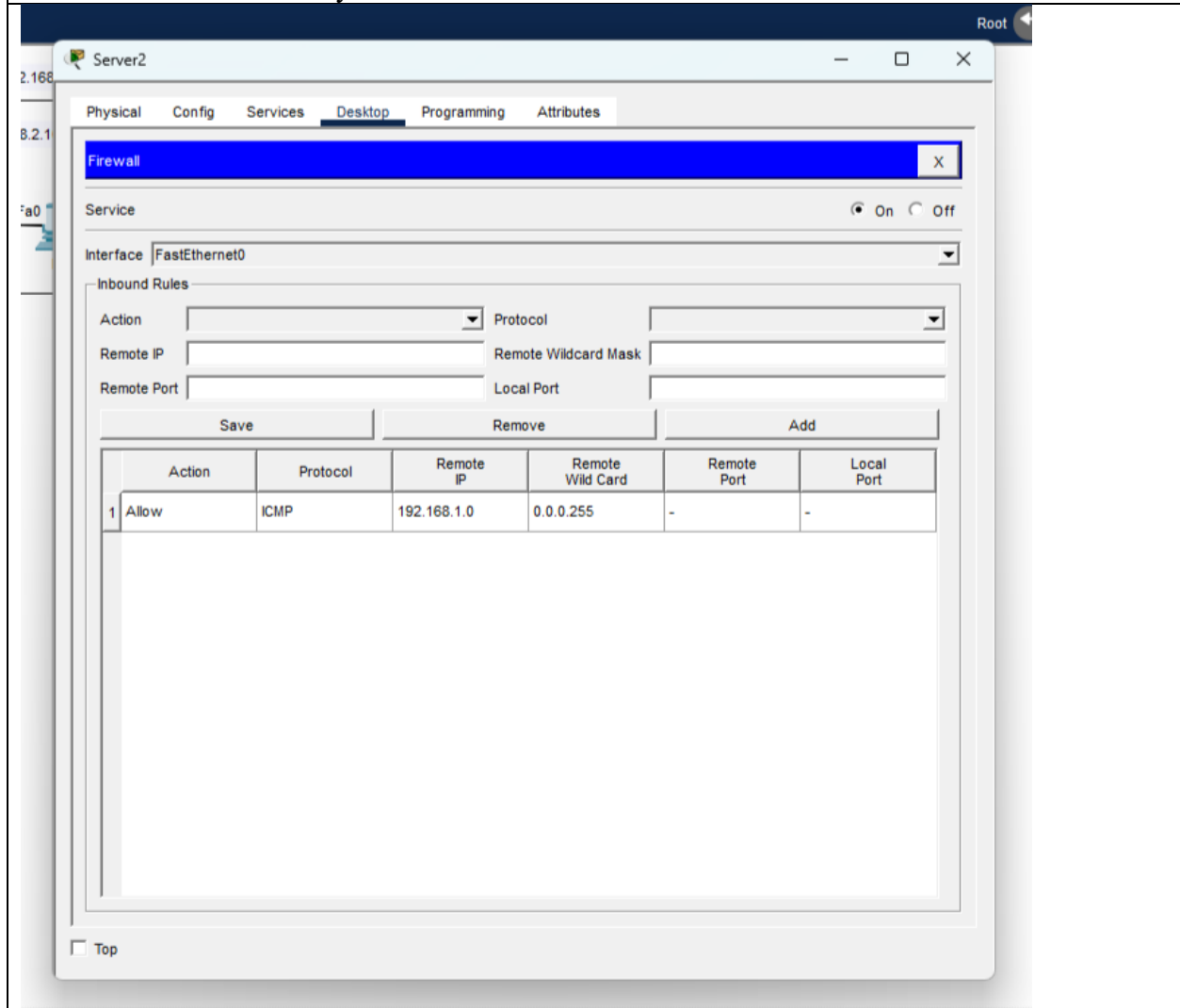
Jonathon Schumaker

December 6, 2025

Network Segmentation Strategy

Configuration

Host Based Firewall Policy



FTP User accounts

Network: 192.168.2.0/28

10.10.1.3 Subnet Mask: 255.0.0.0
 /24 256 IPs Subnet Mask: 255.255.255.0
 /28 16 IPs Subnet Mask: 255.255.255.240
 /29 8 IPs Subnet Mask: 255.255.255.248

PC2: Server2

Physical Config **Services** Desktop Programming Attributes

SERVICES

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

Service ☒ On ☐ Off

User Setup

Username Password

☐ Write ☐ Read ☐ Delete ☐ Rename ☐ List

	Username	Password	Permission	
1	cisco	cisco	RWDNL	Add
2	jsmith	Passw0rd	RL	Save
3	bjones	Password1234	RL	
4	admin01	Pa\$\$w0rD1234	RWDNL	
				Remove

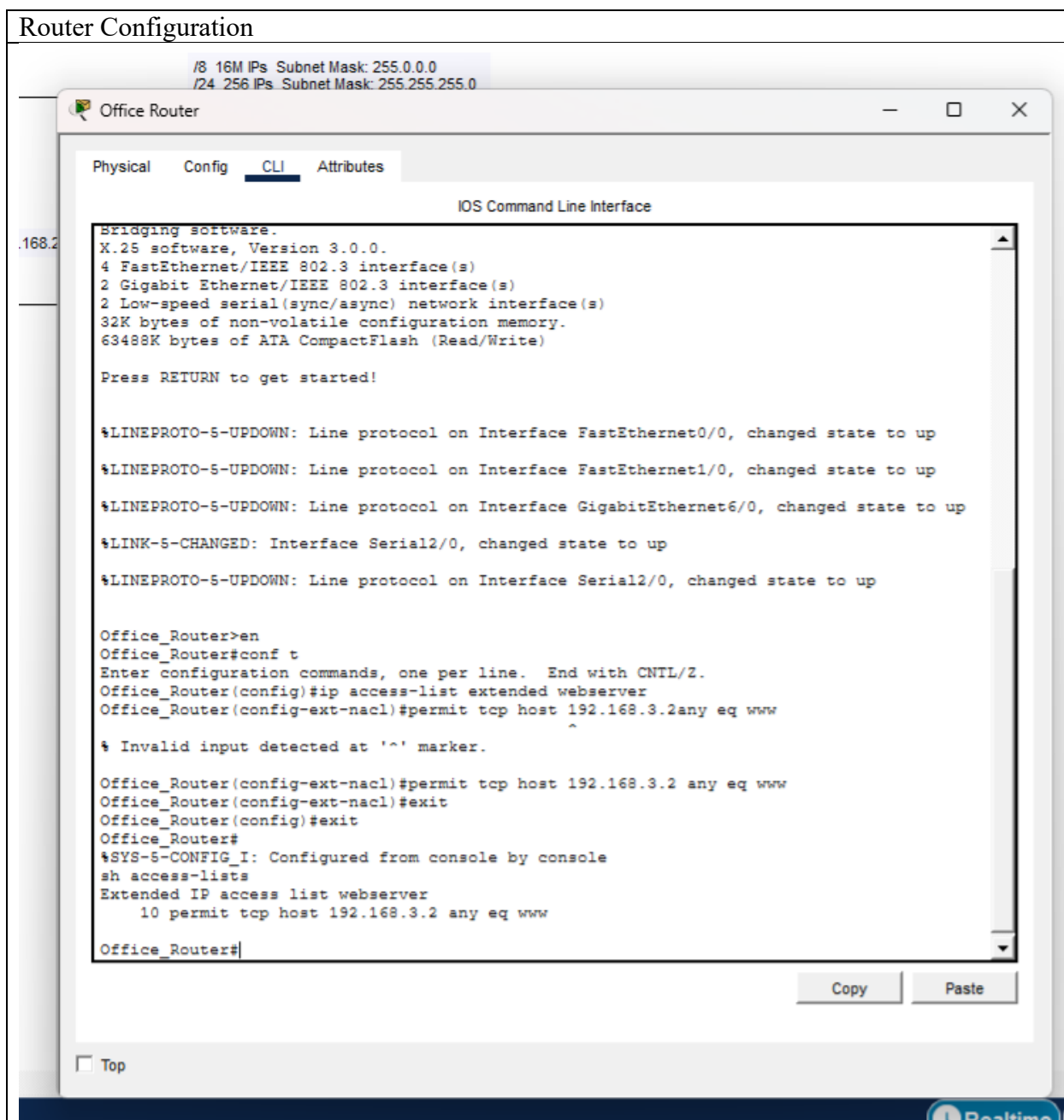
File

1	asa842-k8.bin
2	asa923-k8.bin
3	c1841-advipservicesk9-mz.124-15.T1.bin
4	c1841-ipbase-mz.123-14.T7.bin
5	c1841-ipbasek9-mz.124-12.bin
6	c1900-universalk9-mz.SPA.155-3.M4a.bin

Remove

☐ Top

Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
--------	-------------	------	-------	-----------	----------	-----	------	--------



Rationale

Network segmentation is the practice of dividing a computer network into smaller, isolated sections or segments to improve security and performance. For this scenario we wanted to achieve this because we only wanted the admin computers to be able to communicate with the

FTP server. The firewall was configured to only allow traffic coming from the admin subnet and block all other traffic.

The concept of least privilege is that personnel are only granted the minimum access that they need to achieve what they need to do on a particular network. In this scenario we only wanted jsmith and bjones to have read and lists privileges only. We did however want the admin account to be able to read, write, delete, rename, and list on the server. By separating these privileges we keep personnel from being able to see or interact with things that they may not need to.

The approach of adding in a network firewall would be to place a firewall in a part of the network where you want to separate the trusted part of the network from the untrusted part of the network. This would allow the monitoring of traffic coming into and going out of the network but doesn't really segment parts of the network from other parts. We could incorporate VLAN's to help aid in the isolation but firewalls do a better job of segmenting traffic more than VLAN's do.

References: