Network Segmentation Strategy

William Pascoe

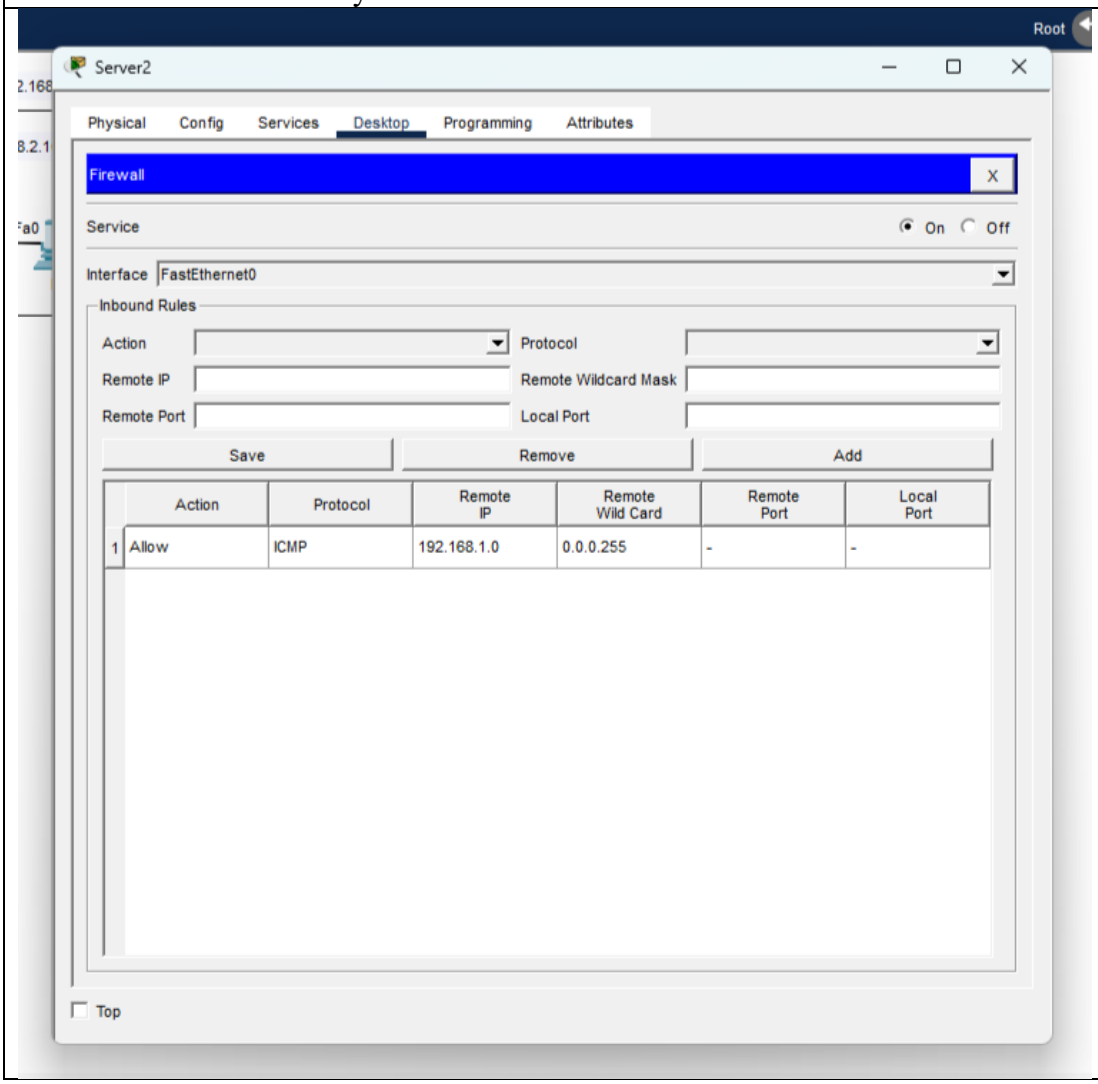
CYB-220 Network Security

Jonathon Schumaker

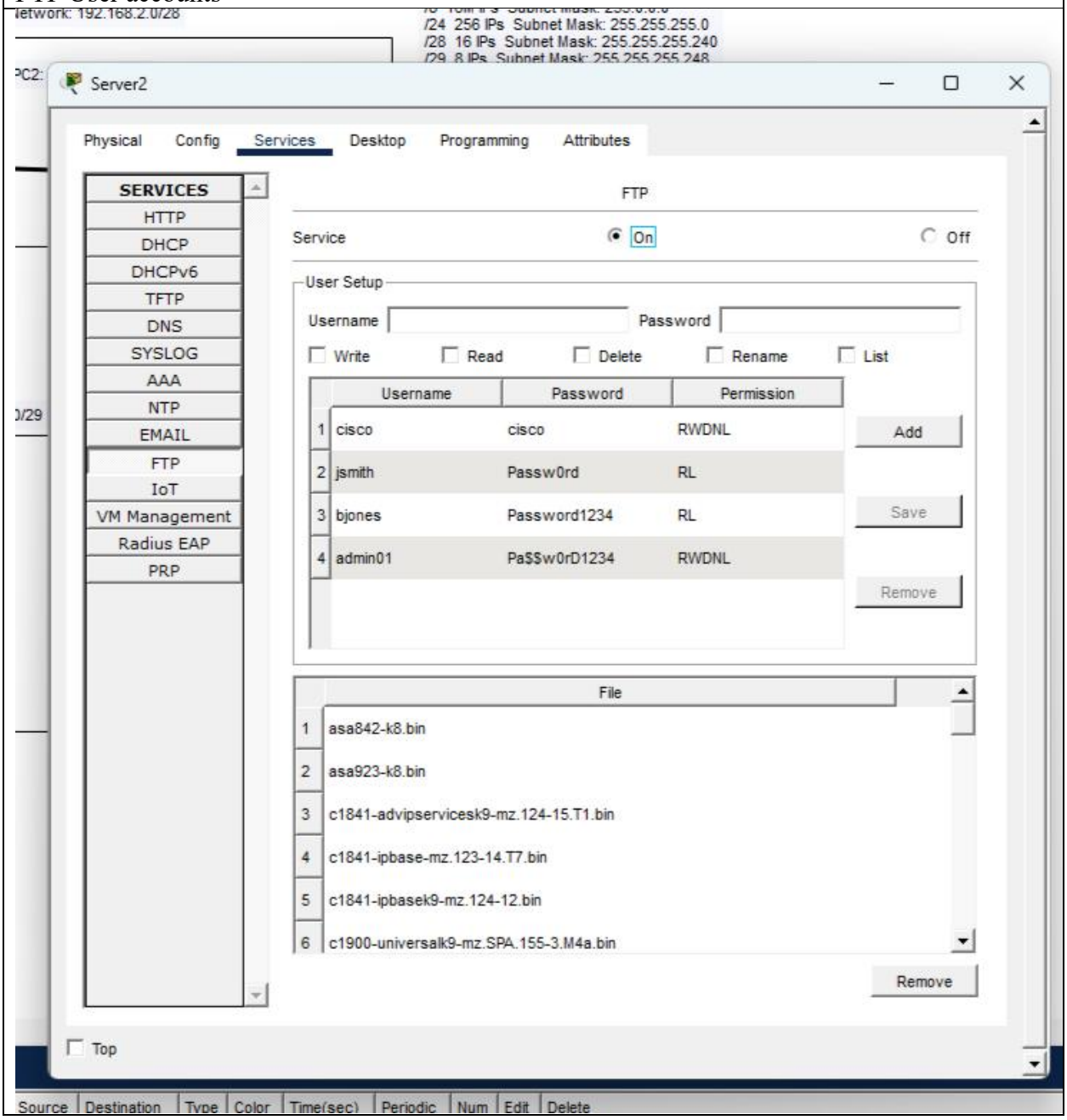
December 6, 2025

Network Segmentation Strategy

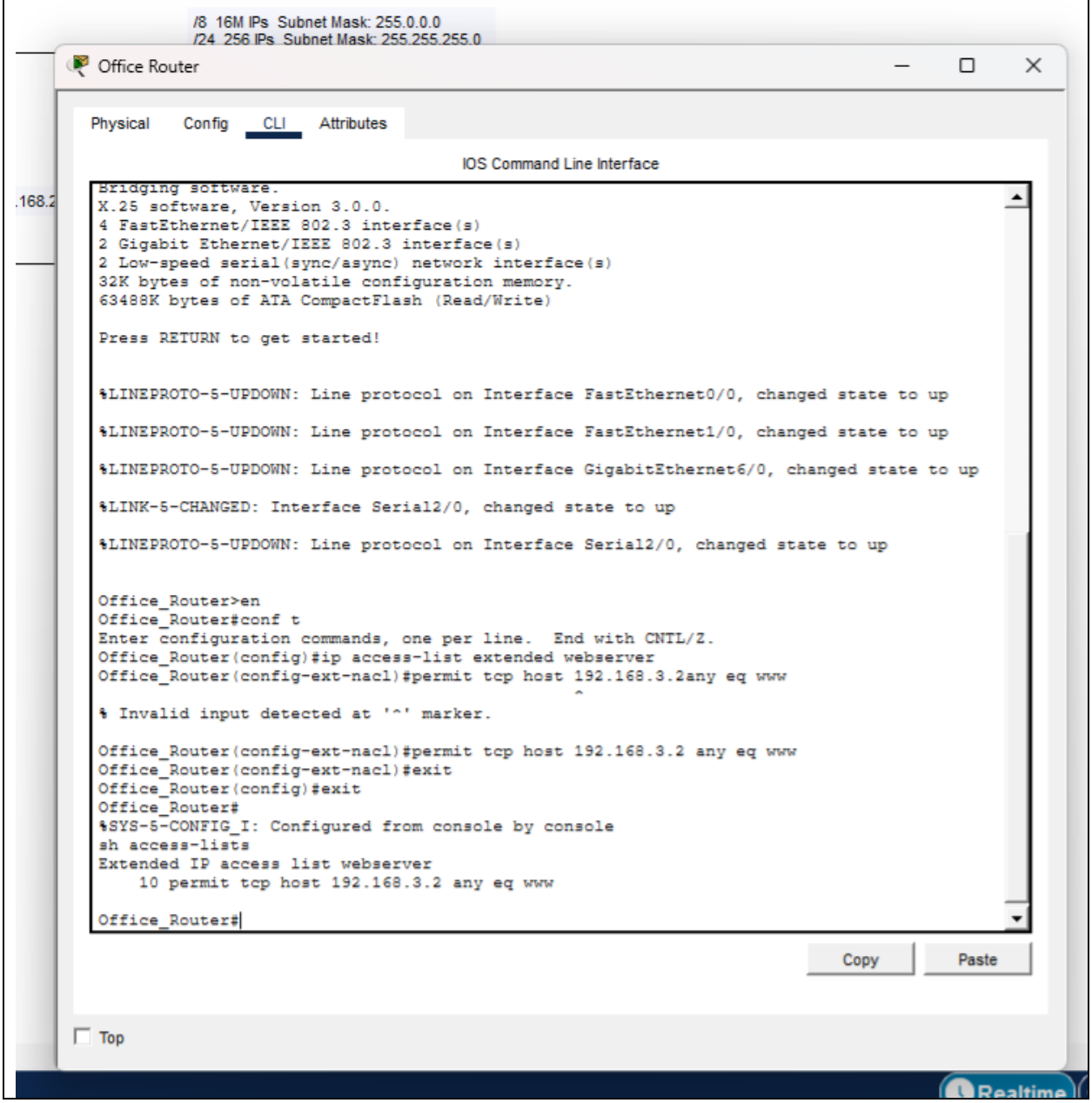
Configuration

Host Based Firewall Policy


FTP User accounts



Router Configuration



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 incoporate VLAN's to help aid in the isolation but firewalls do a better job of segmenting traffic more than VLAN's do.

References: