

Network Segmentation Strategy

William Pascoe

CYB-220 Network Security

Jonathon Schumaker

December 6, 2025

Network Segmentation Strategy

Configuration

Host Based Firewall Policy

Server2

Physical Config Services Desktop Programming Attributes

Firewall

Service

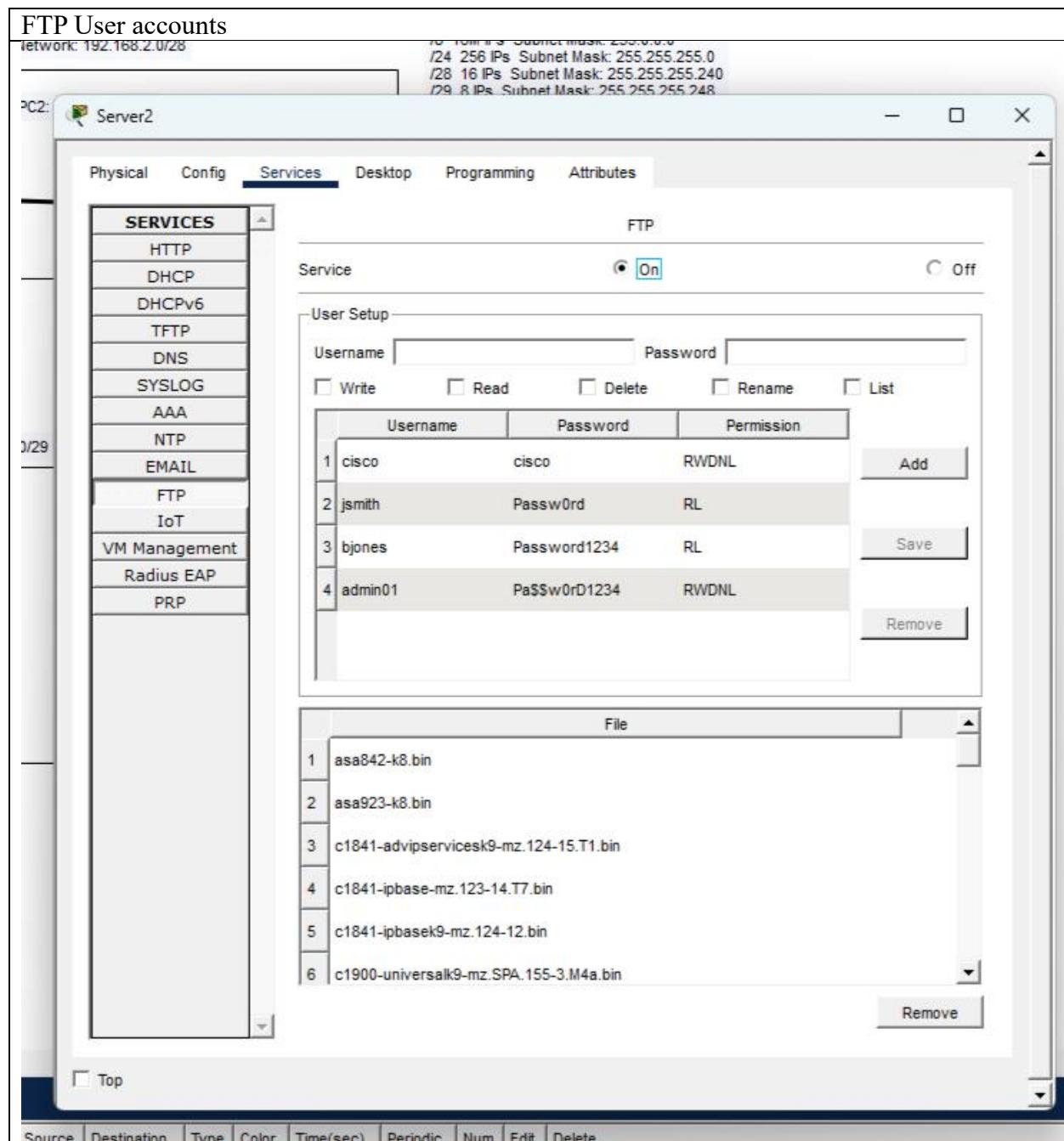
Interface FastEthernet0

Inbound Rules

Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1 Allow	ICMP	192.168.1.0	0.0.0.255	-	-

Save Remove Add

Top



Router Configuration

The screenshot shows a window titled "Office Router" with the tab "CLI" selected. The window displays the following text:

```

/8 16M IPs Subnet Mask: 255.0.0.0
/24 256 IPs Subnet Mask: 255.255.255.0

Physical Config CLI Attributes

IOS Command Line Interface

Bridging 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>en
Office_Router#conf t
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
^
* Invalid input detected at '^' marker.

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
sh access-lists
Extended IP access list webserver
  10 permit tcp host 192.168.3.2 any eq www

Office_Router#

```

At the bottom of the window, there are "Copy" and "Paste" buttons, and a "Top" link.

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: