

Simplifying Operations with FTP Passive Mode



Nick Russo

NETWORK ENGINEER

@nickrusso42518 www.njrusmc.net



Agenda



Why do we need it?

FTP passive mode operations

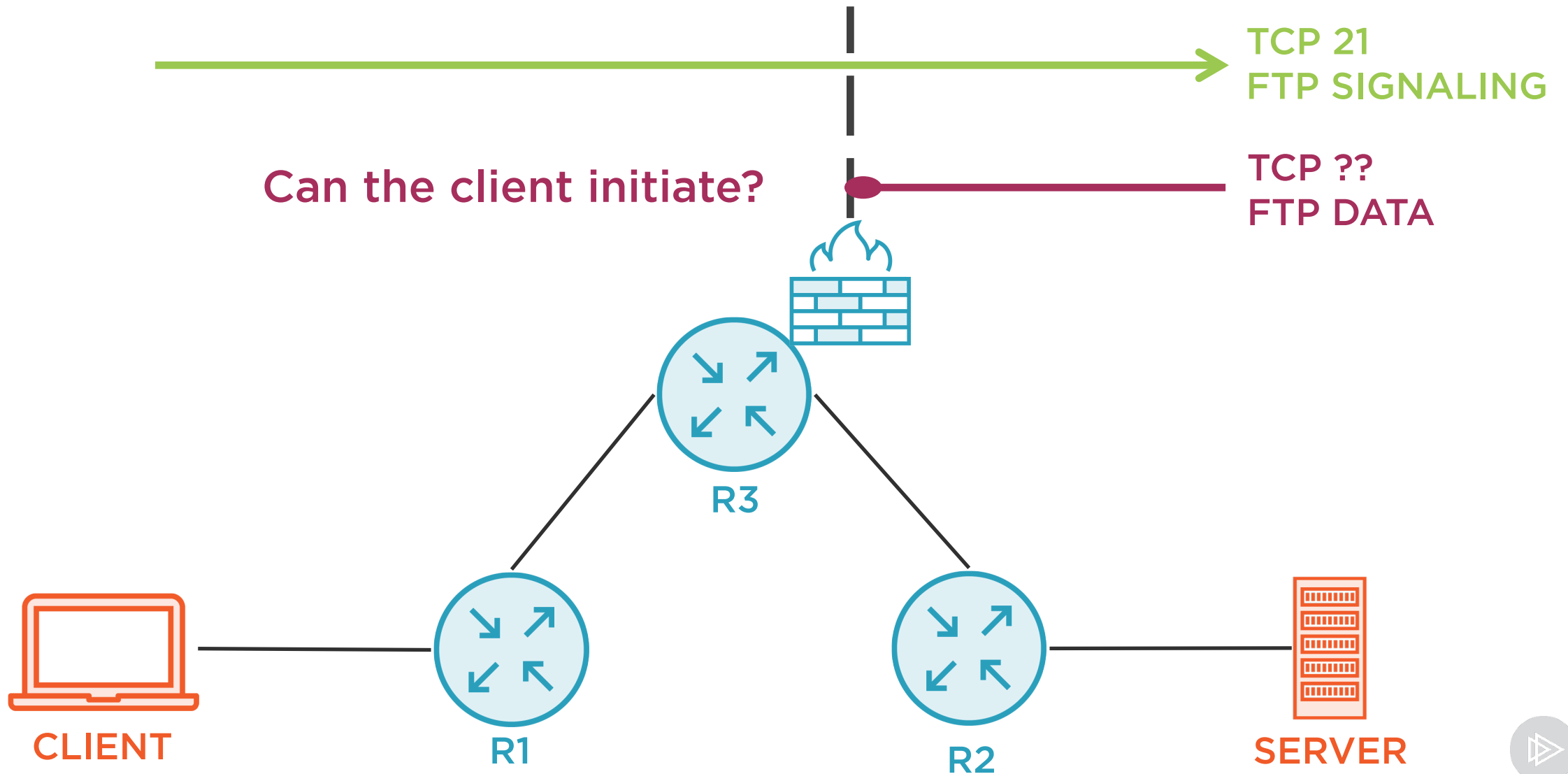
Demo and packet analysis

Securing passive FTP

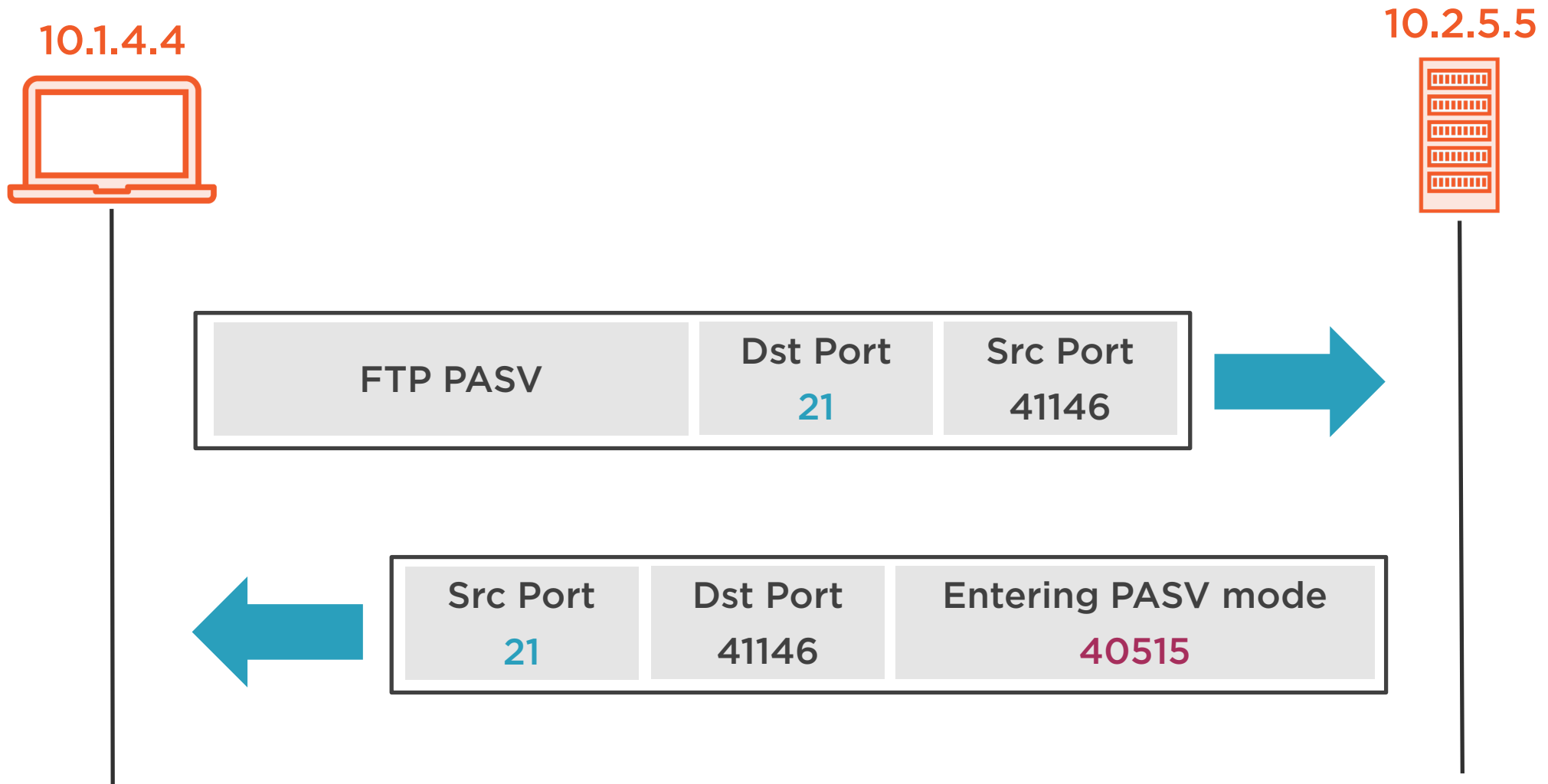
Comparing active and passive modes



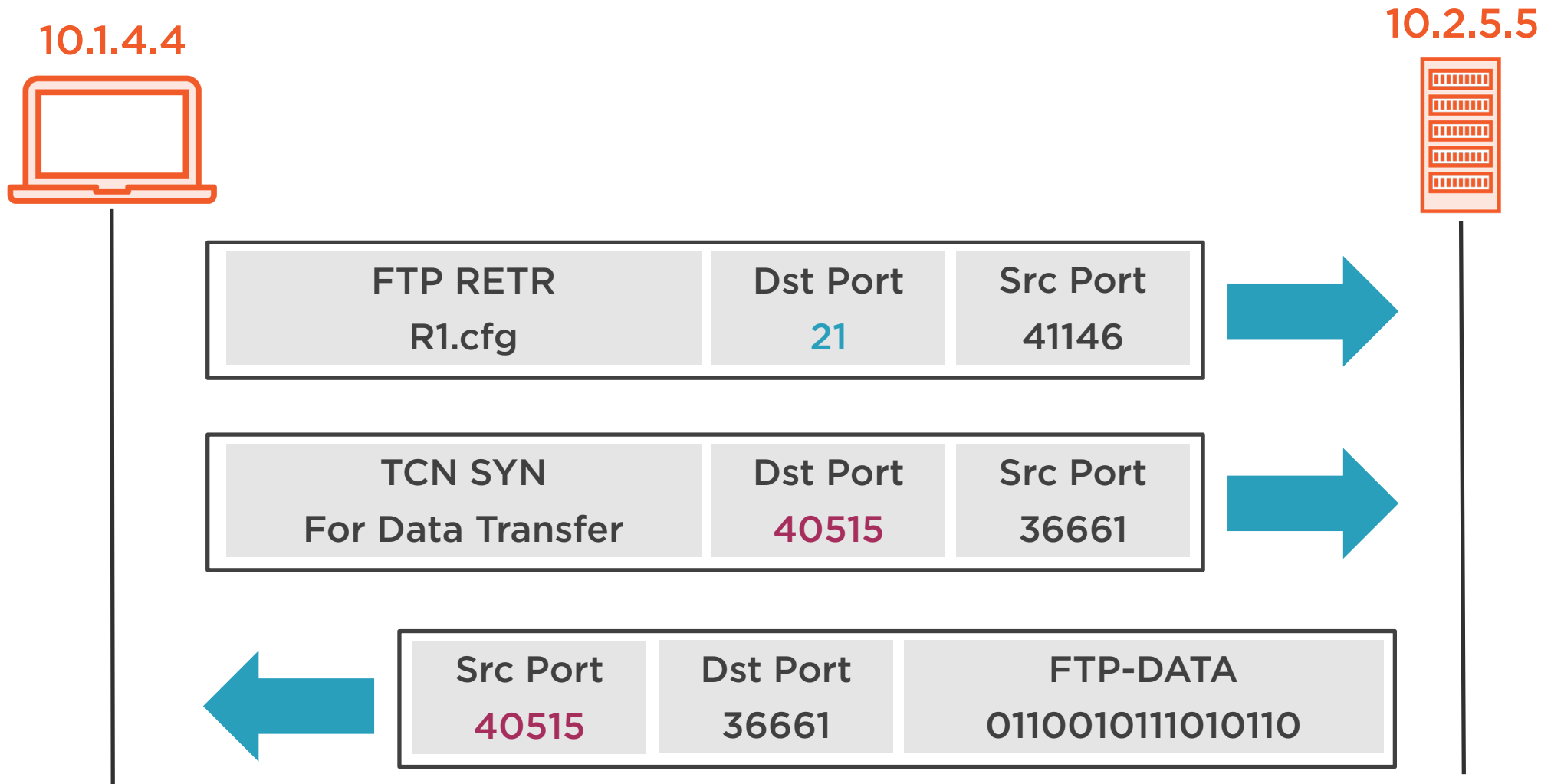
FTP Active Mode Security Challenge



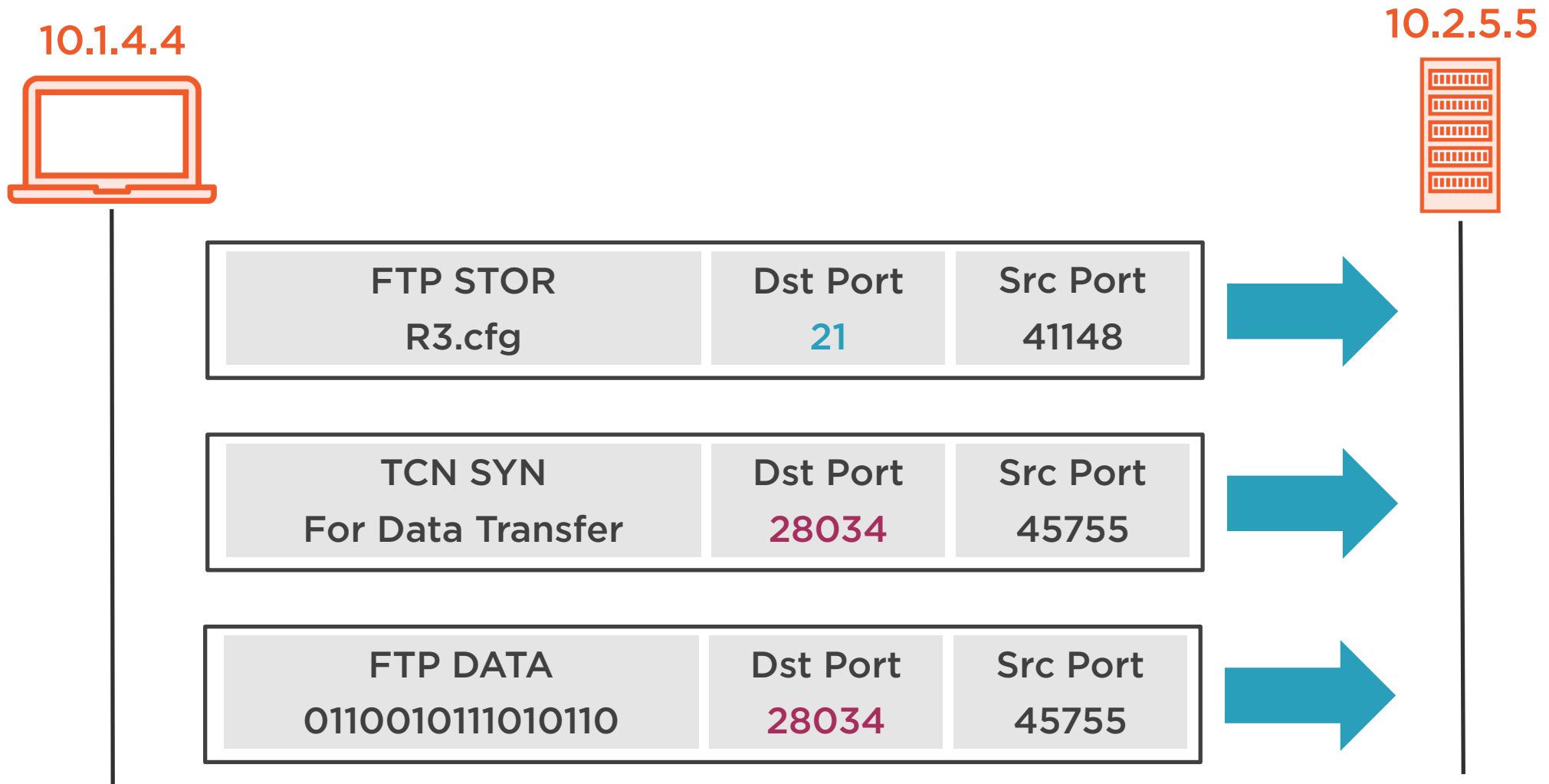
The FTP PASV Command



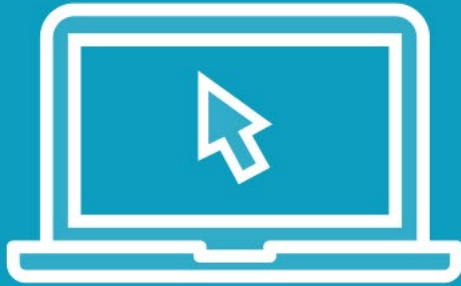
FTP Passive Mode Download



FTP Passive Mode Upload



Demo



Re-downloading with passive mode



FTP PASV Command and Response

No.	Source	Destination	Proto	Src Port	Dst Port	Info
66	10.1.4.4	10.2.5.5	FTP	41146	21	Request: PASV
67	10.2.5.5	10.1.4.4	FTP	21	41146	Response: 227 Entering Passive Mode (10,2,5,5,158,67).
68	10.1.4.4	10.2.5.5	TCP	36661	40515	36661→40515 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_
69	10.2.5.5	10.1.4.4	TCP	40515	36661	40515→36661 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=
70	10.1.4.4	10.2.5.5	TCP	36661	40515	36661→40515 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=309
71	10.1.4.4	10.2.5.5	FTP	41146	21	Request: RETR R1.cfg

▶ Frame 67: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0

▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:0c:29:9e:6d:dd

▶ Internet Protocol Version 4, Src: 10.2.5.5, Dst: 10.1.4.4

▶ Transmission Control Protocol, Src Port: 21, Dst Port: 41146, Seq: 305, Ack: 90, Len: 46

▼ File Transfer Protocol (FTP)

▼ 227 Entering Passive Mode (10,2,5,5,158,67).\r\n

Response code: Entering Passive Mode (227)

Response arg: Entering Passive Mode (10,2,5,5,158,67).

Passive IP address: 10.2.5.5 ← Server's IP address

Passive port: 40515

Client is listening on
this TCP port

$$158 * 256 = 40448$$
$$40448 + 67 = 40515$$



FTP Passive Mode Download

No.	Source	Destination	Proto	Src Port	Dst Port	Info
71	10.1.4.4	10.2.5.5	FTP	41146	21	Request: RETR R1.cfg
72	10.2.5.5	10.1.4.4	FTP	21	41146	Response: 150 Opening BINARY mode data connection for R1.cfg
73	10.2.5.5	10.1.4.4	FTP-DATA	40515	36661	FTP Data: 38 bytes
74	10.2.5.5	10.1.4.4	TCP	40515	36661	40515→36661 [FIN, ACK] Seq=39 Ack=1 Win=29056 Len=0 TSval=373
75	10.1.4.4	10.2.5.5	TCP	36661	40515	36661→40515 [ACK] Seq=1 Ack=39 Win=29312 Len=0 TSval=30980821
76	10.1.4.4	10.2.5.5	TCP	36661	40515	36661→40515 [FIN, ACK] Seq=1 Ack=40 Win=29312 Len=0 TSval=309
77	10.2.5.5	10.1.4.4	TCP	40515	36661	40515→36661 [ACK] Seq=40 Ack=2 Win=29056 Len=0 TSval=37387744
78	10.2.5.5	10.1.4.4	FTP	21	41146	Response: 226 Transfer complete.

▶ Frame 73: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0

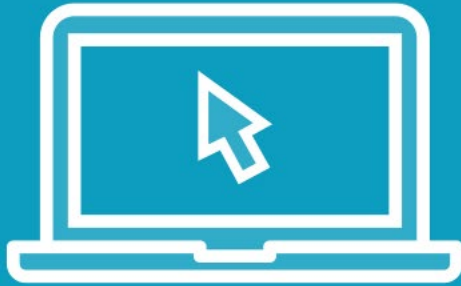
- ▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:0c:29:9e:6d:dd
- ▶ Internet Protocol Version 4, Src: 10.2.5.5, Dst: 10.1.4.4
- ▶ Transmission Control Protocol, Src Port: 40515, Dst Port: 36661, Seq: 1, Ack: 1, Len: 38

FTP Data (hello world\nthis is\nR1's config file!\n)

↑
File contents



Demo



We should test uploads too!



FTP Passive Mode Upload

No.	Source	Destination	Proto	Src Port	Dst Port	Info
51	10.1.4.4	10.2.5.5	FTP	41148	21	Request: STOR R3.cfg
52	10.2.5.5	10.1.4.4	FTP	21	41148	Response: 150 Ok to send data.
53	10.1.4.4	10.2.5.5	FTP-DATA	45755	28034	FTP Data: 48 bytes
54	10.1.4.4	10.2.5.5	TCP	45755	28034	45755→28034 [FIN, ACK] Seq=49 Ack=1 Win=29312 Len=0
55	10.2.5.5	10.1.4.4	TCP	28034	45755	28034→45755 [ACK] Seq=1 Ack=49 Win=29056 Len=0
56	10.2.5.5	10.1.4.4	TCP	28034	45755	28034→45755 [FIN, ACK] Seq=1 Ack=50 Win=29056 Len=0
57	10.1.4.4	10.2.5.5	TCP	45755	28034	45755→28034 [ACK] Seq=50 Ack=2 Win=29312 Len=0
58	10.2.5.5	10.1.4.4	FTP	21	41148	Response: 226 Transfer complete.

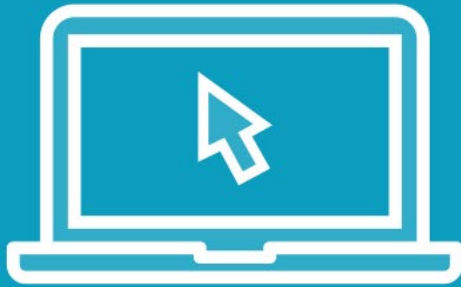
▶ Frame 53: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0

- ▶ Ethernet II, Src: 00:0c:29:9e:6d:dd, Dst: 00:00:a6:16:00:01
- ▶ Internet Protocol Version 4, Src: 10.1.4.4, Dst: 10.2.5.5
- ▶ Transmission Control Protocol, Src Port: 45755, Dst Port: 28034, Seq: 1, Ack: 1, Len: 48
FTP Data (hello world\nR3's file is\nmuch more interesting!\n)

↑
File contents



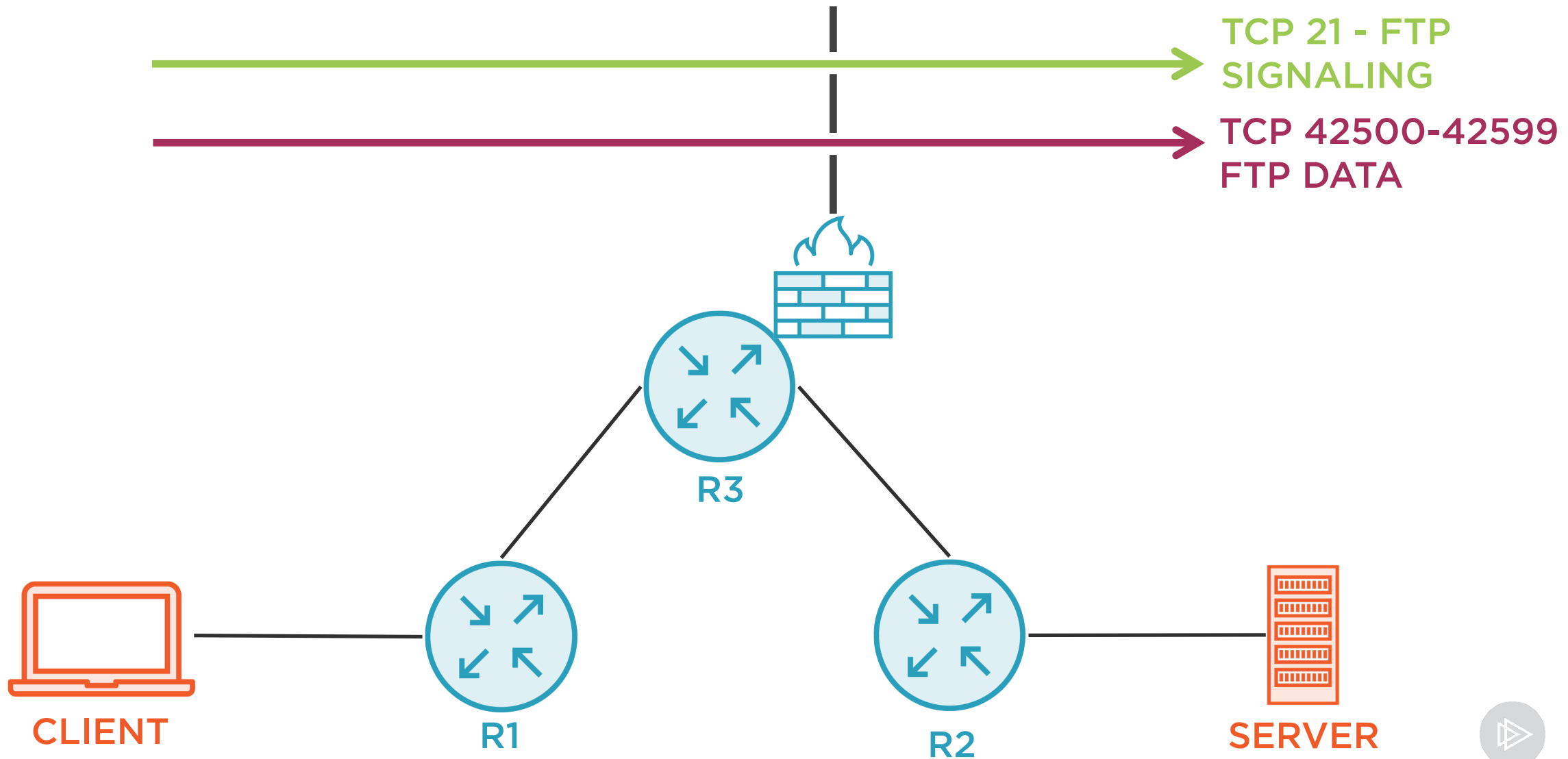
Demo



Securing passive FTP



FTP Passive Mode Security Improvement



FTP PASV Custom Ports

No.	Source	Destination	Proto	Src Port	Dst Port	Info
42	10.1.4.4	10.2.5.5	FTP	41154	21	Request: PASV
43	10.2.5.5	10.1.4.4	FTP	21	41154	Response: 227 Entering Passive Mode (10,2,5,5,166,70).
44	10.1.4.4	10.2.5.5	TCP	37103	42566	37103→42566 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_F
45	10.2.5.5	10.1.4.4	TCP	42566	37103	42566→37103 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=
46	10.1.4.4	10.2.5.5	TCP	37103	42566	37103→42566 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=313
47	10.1.4.4	10.2.5.5	FTP	41154	21	Request: RETR R1.cfg

- ▶ Frame 43: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0
- ▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:0c:29:9e:6d:dd
- ▶ Internet Protocol Version 4, Src: 10.2.5.5, Dst: 10.1.4.4
- ▶ Transmission Control Protocol, Src Port: 21, Dst Port: 41154, Seq: 305, Ack: 90, Len: 46
- ▼ File Transfer Protocol (FTP)
 - ▼ 227 Entering Passive Mode (10,2,5,5,166,70).\r\n
 - Response code: Entering Passive Mode (227)
 - Response arg: Entering Passive Mode (10,2,5,5,166,70).
 - Passive IP address: 10.2.5.5
 - Passive port: 42566

From our range of
42500 - 42599

$$166 * 256 = 42496$$
$$42496 + 70 = 42566$$



FTP Active Mode vs. Passive Mode

Active Mode

Client sends PORT command
Server opens session to client
Simpler server-side firewall
NAT is complex
Legacy method

Passive Mode

Client sends PASV command
Client opens session to server
Simpler client-side firewall
NAT "just works"
Preferred method

