Simplifying Operations with FTP Passive Mode

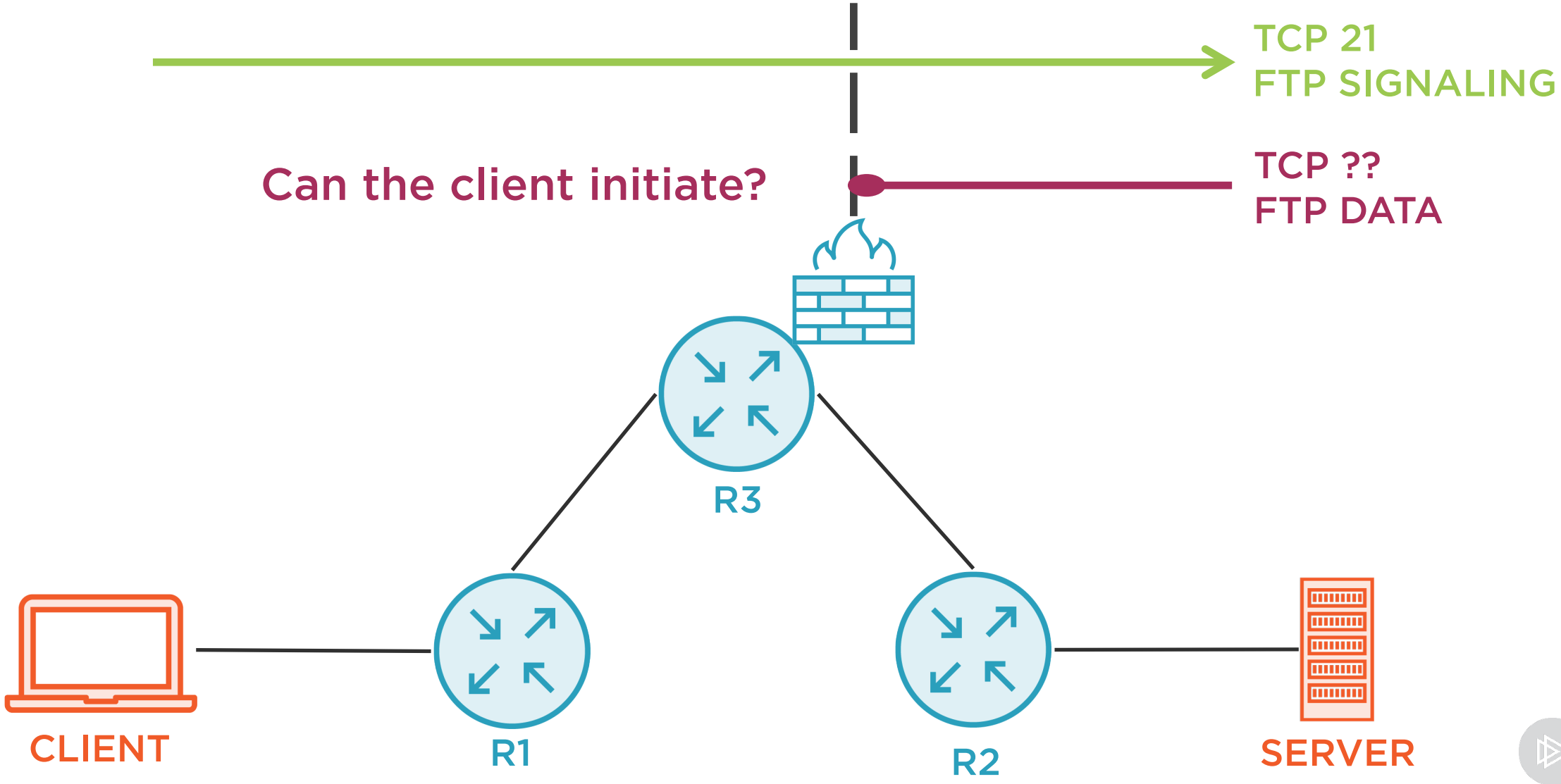
Nick Russo
NETWORK ENGINEER

@nickrusso42518 www.njrusmc.net

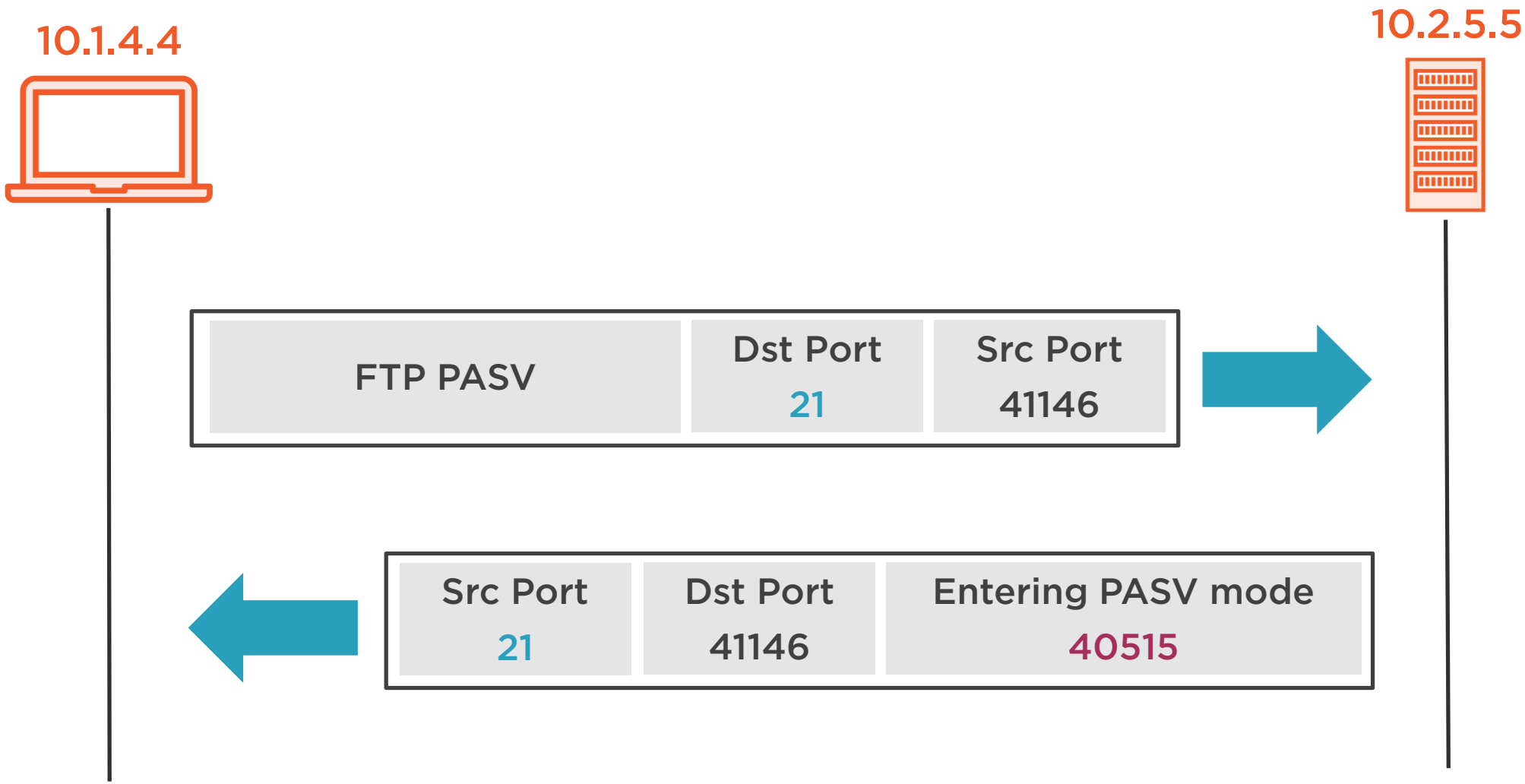
Agenda

- Why do we need it?
- FTP passive mode operations
- Demo and packet analysis
- Securing passive FTP
- Comparing active and passive modes

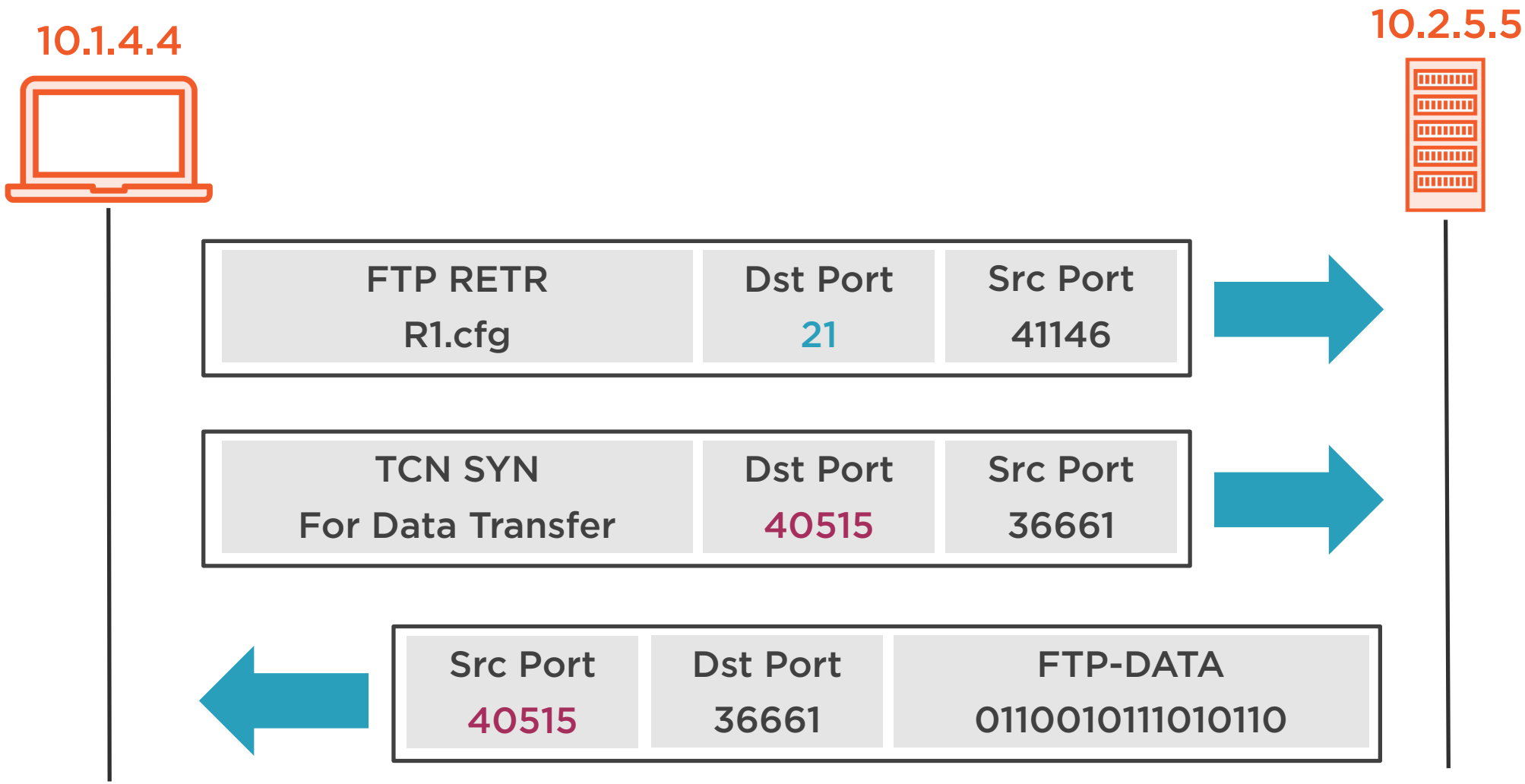
FTP Active Mode Security Challenge



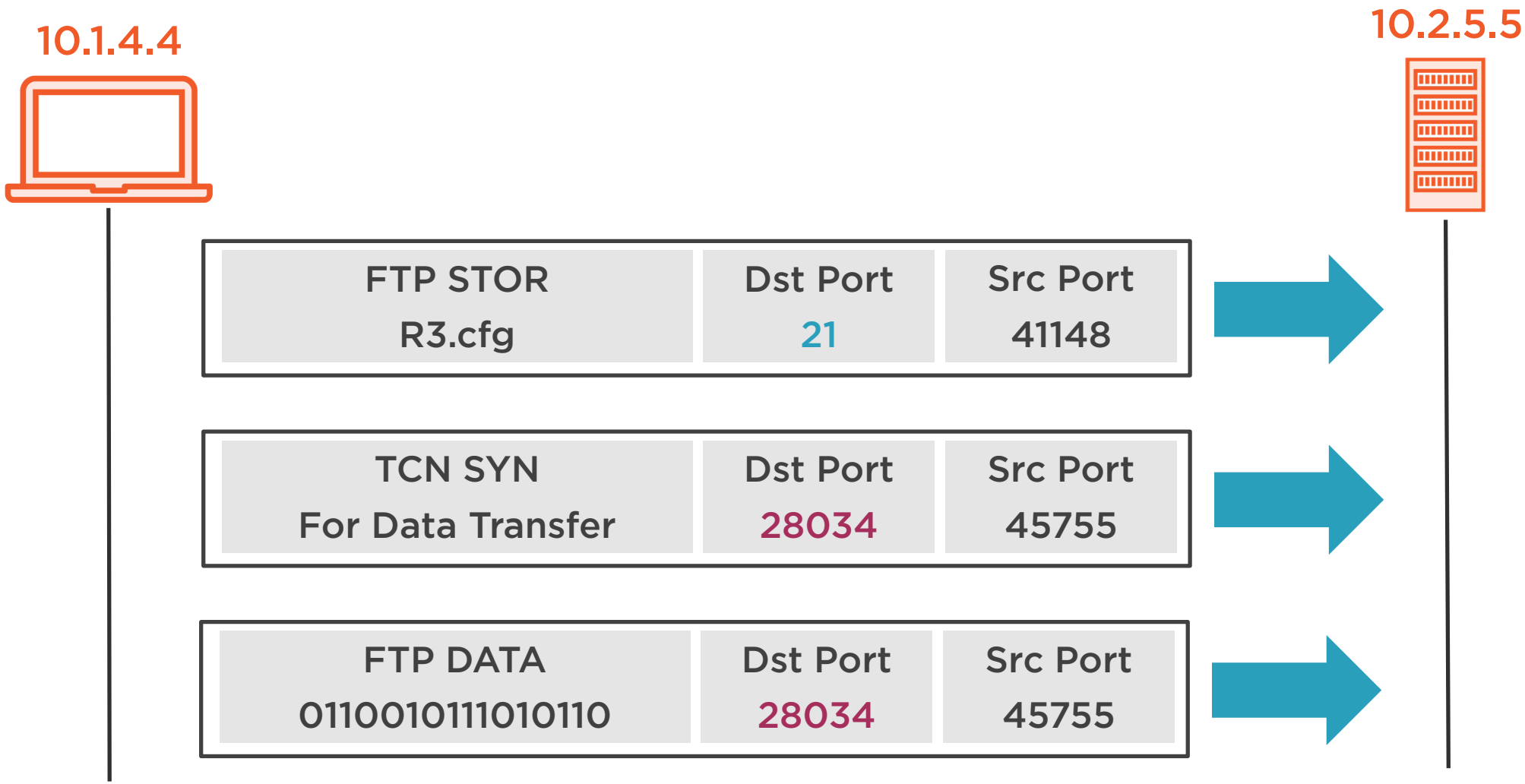
The FTP PASV Command



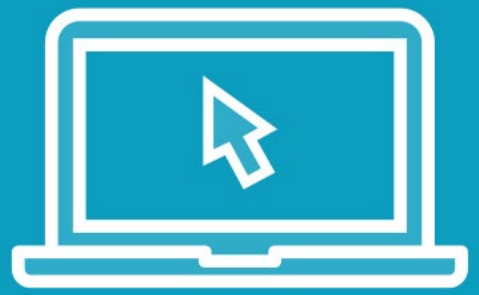
FTP Passive Mode Download



FTP Passive Mode Upload

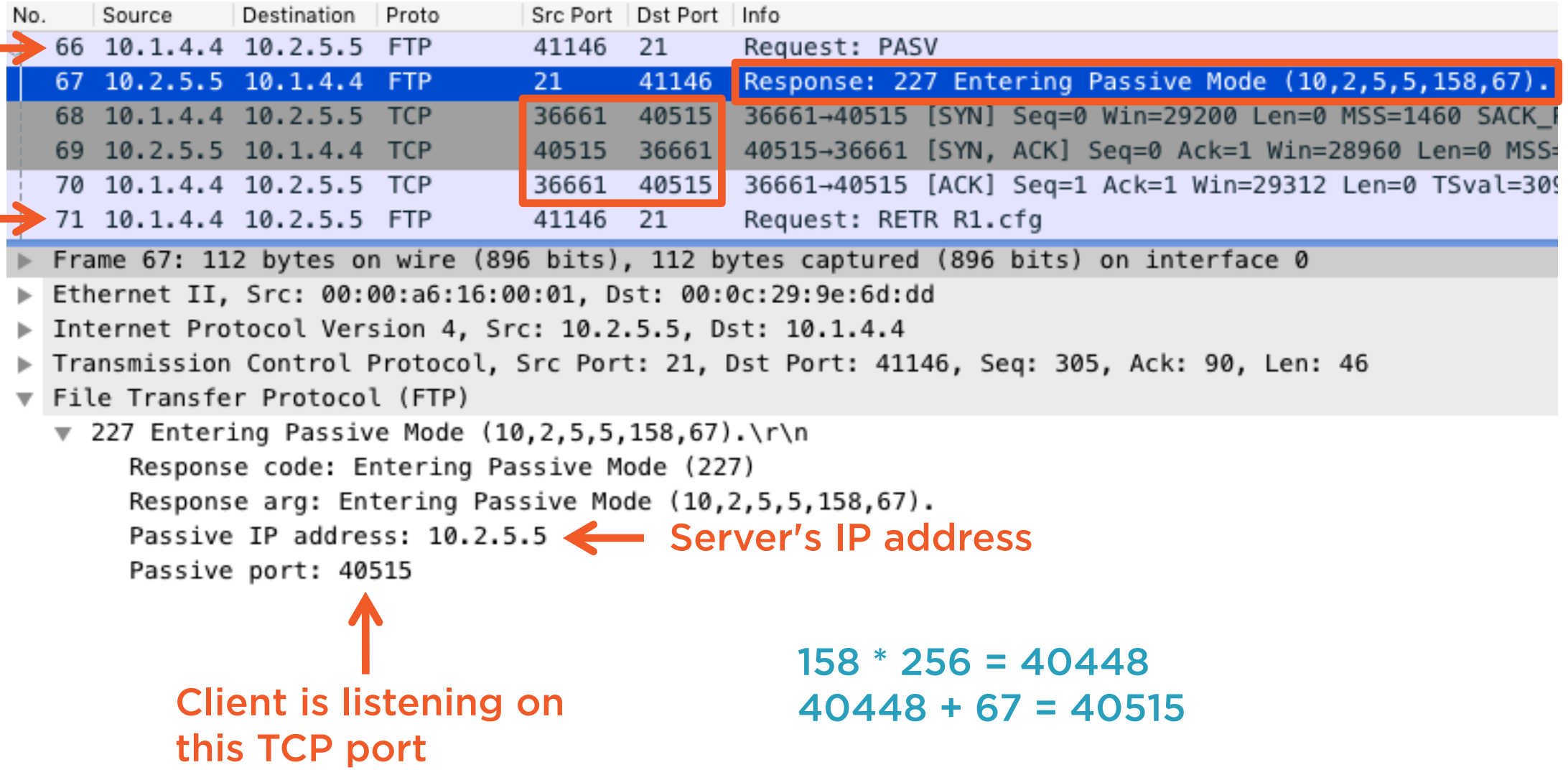


Demo

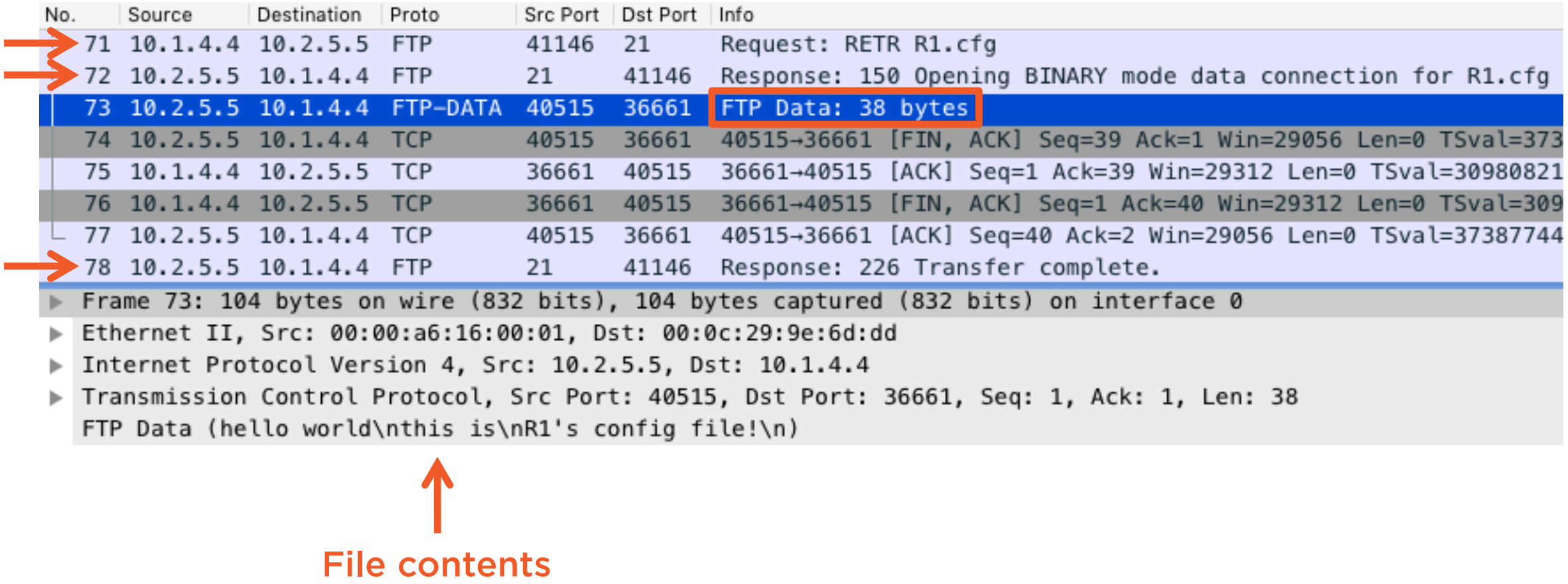


Re-downloading with passive mode

FTP PASV Command and Response

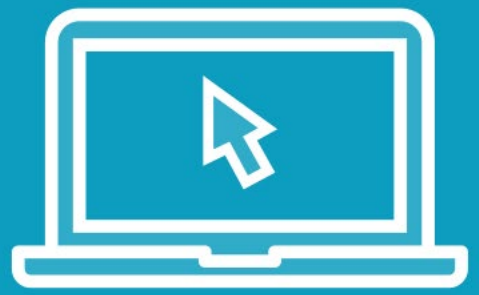


FTP Passive Mode Download



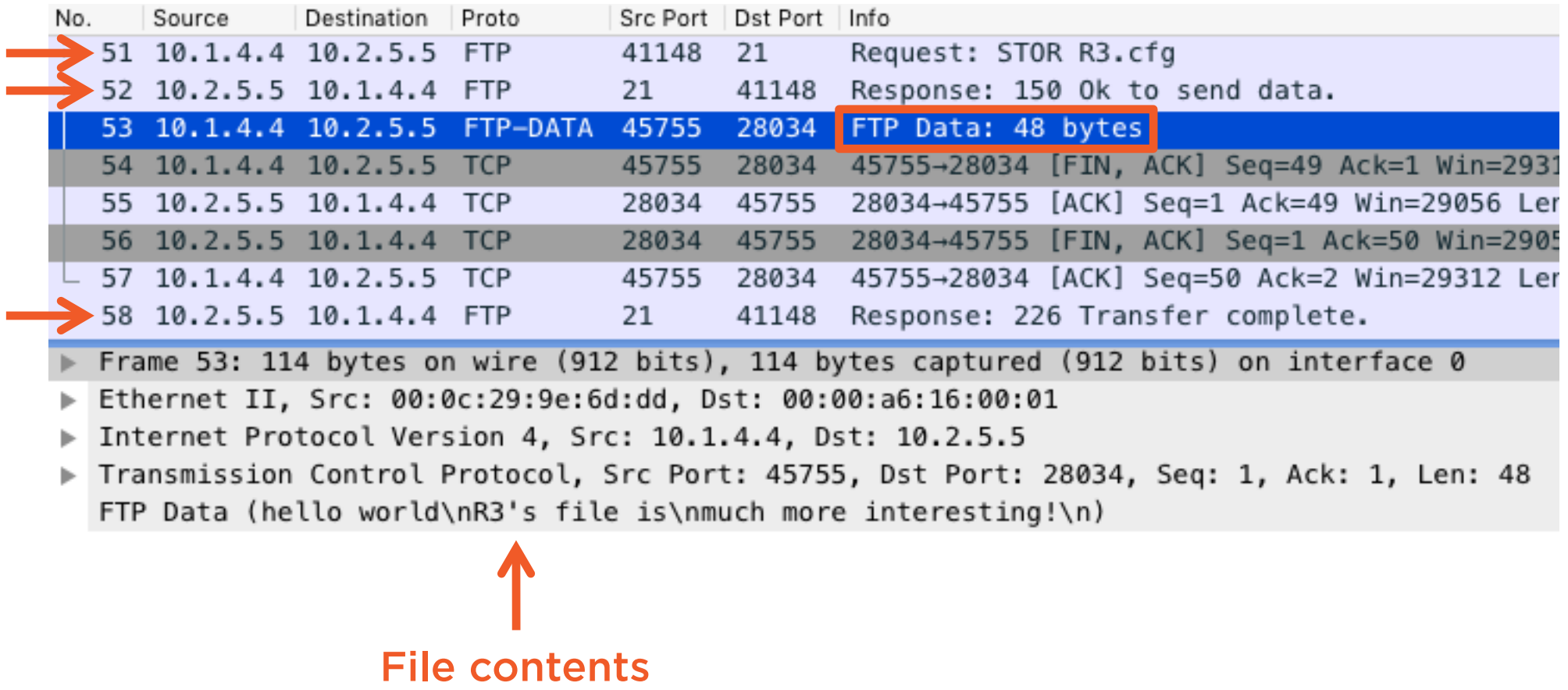
File contents

Demo



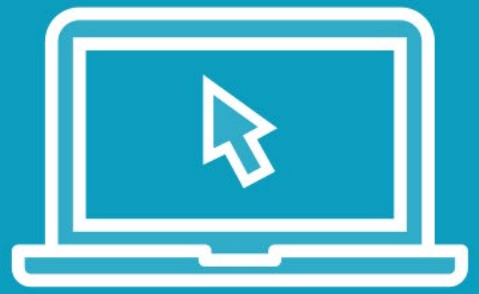
We should test uploads too!

FTP Passive Mode Upload



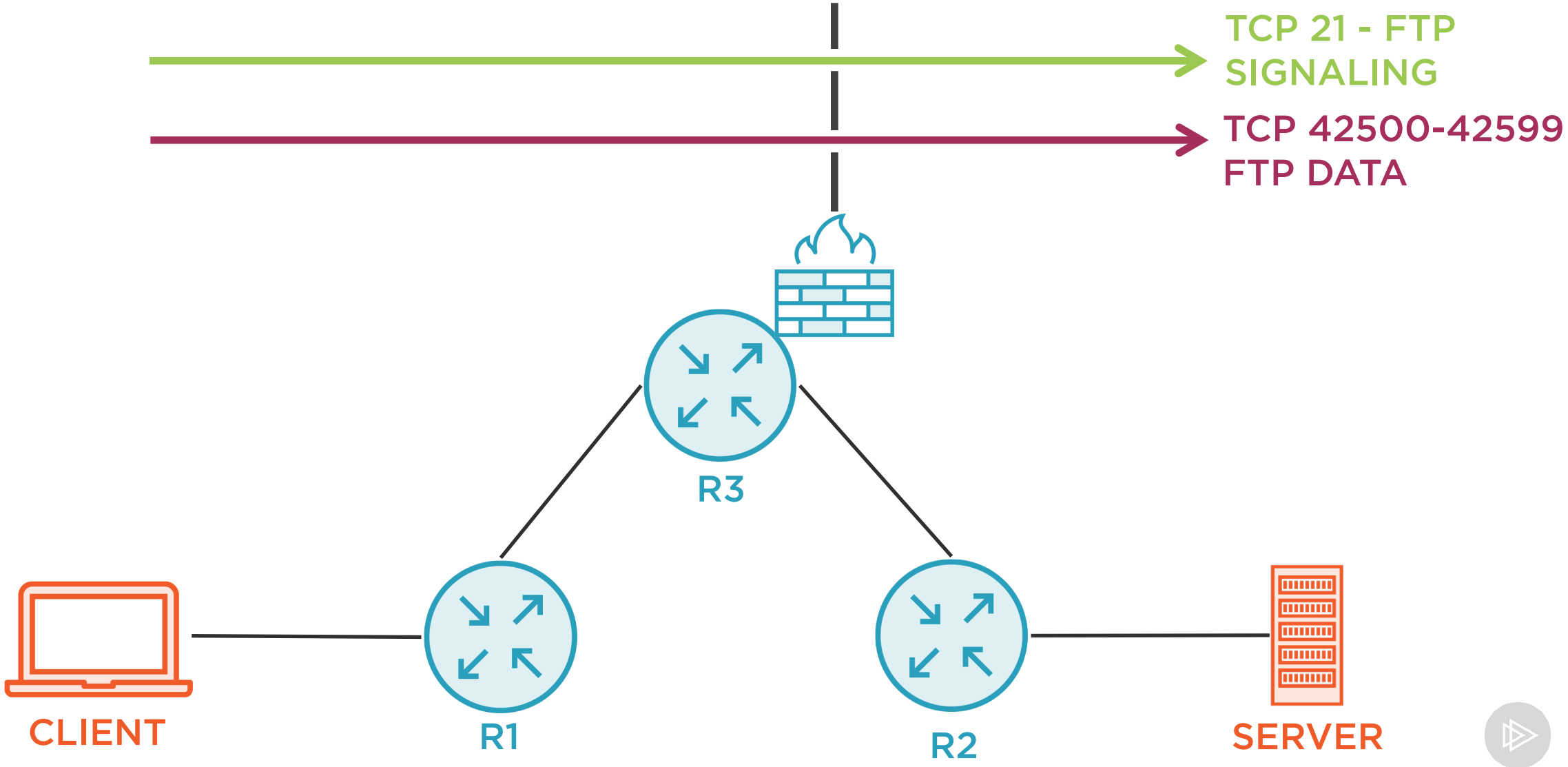
File contents

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	Passive Mode
Client sends PORT command	Client sends PASV command
Server opens session to client	Client opens session to server
Simpler server-side firewall	Simpler client-side firewall
NAT is complex	NAT "just works"
Legacy method	Preferred method