Protecting Data with FTP Secure (FTPS)

Nick Russo
NETWORK ENGINEER

@nickrusso42518 www.njrusmc.net

Agenda

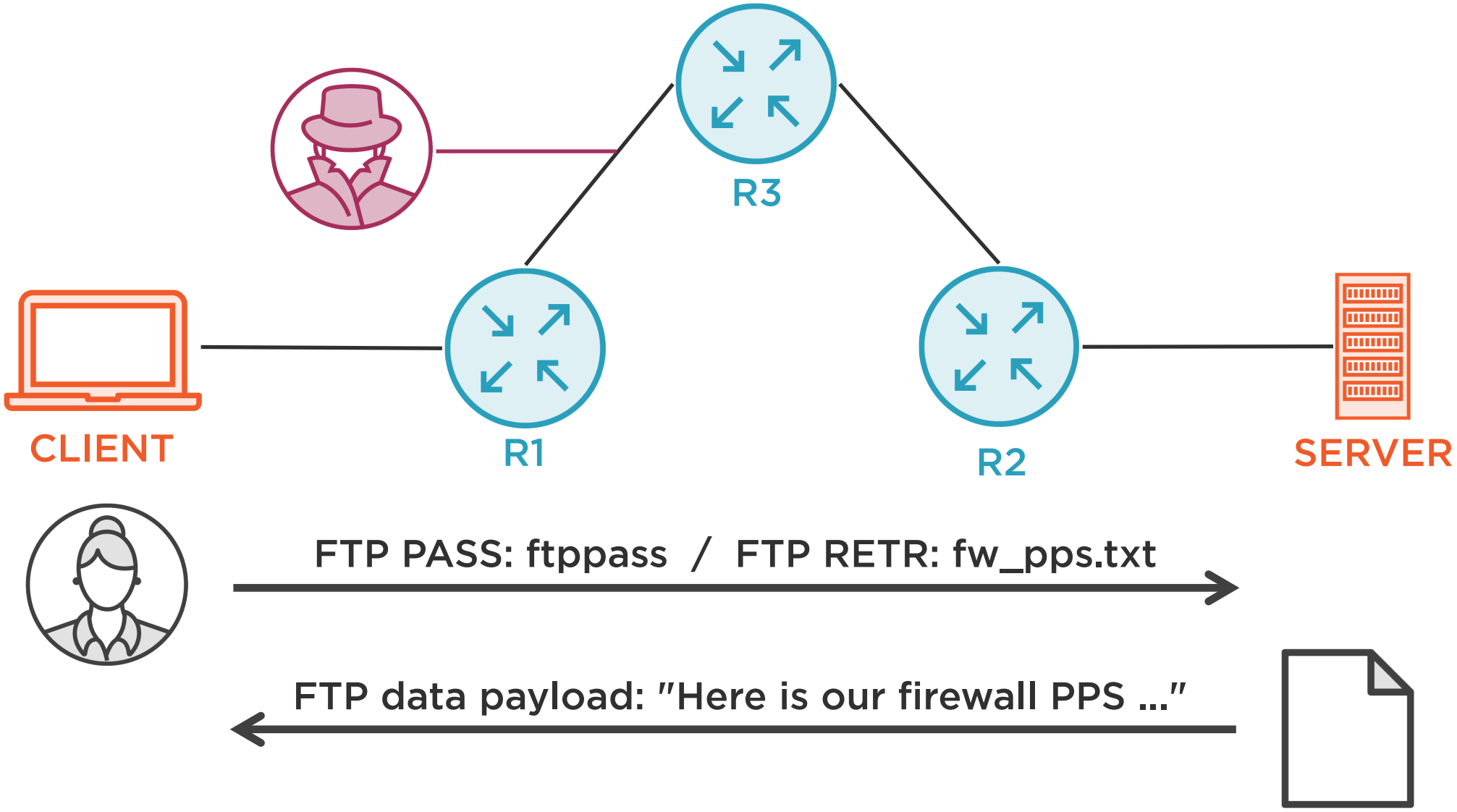
How FTPS works

Introducing digital certificates and PKI

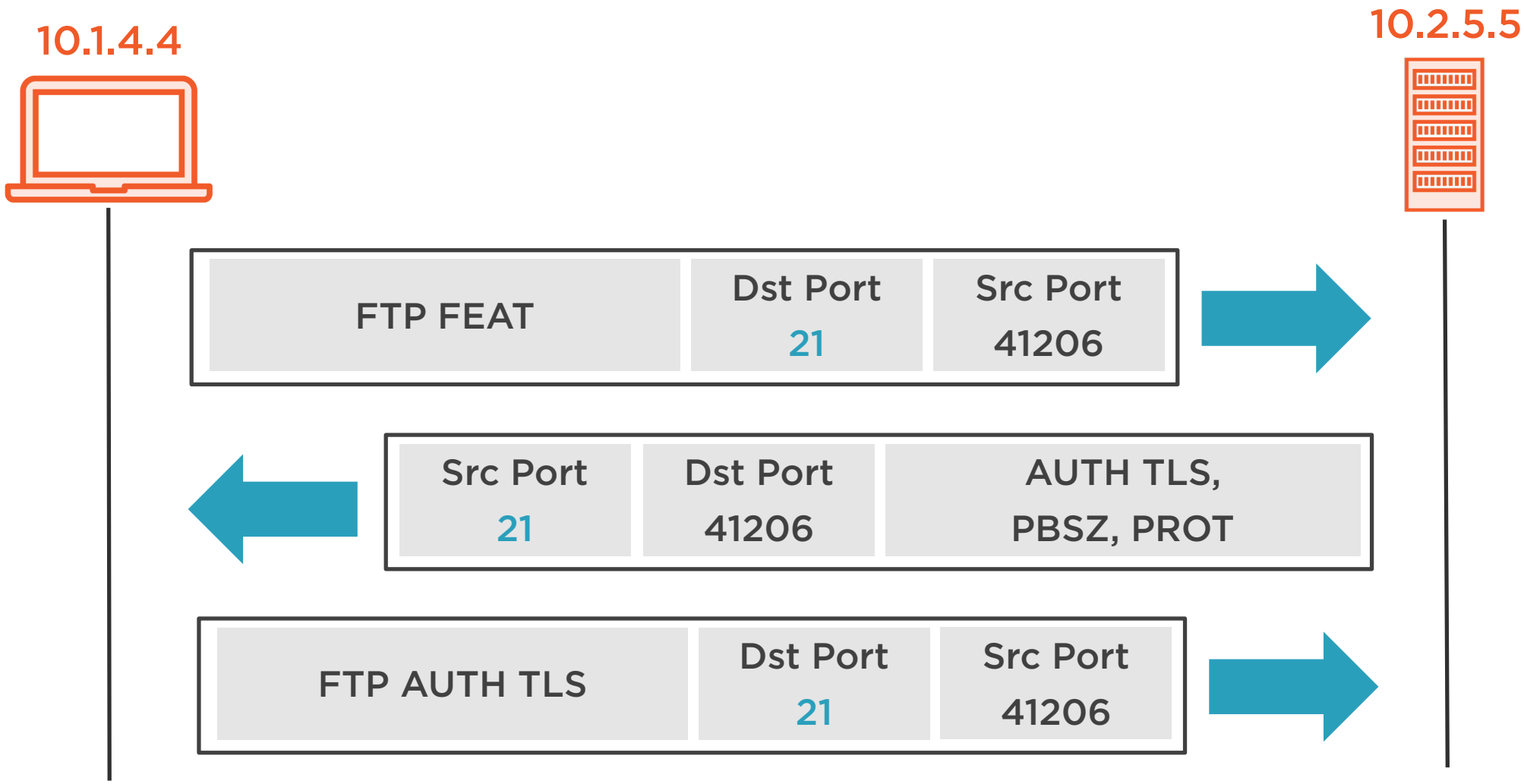
Configuring and testing FTPS

Does our firewall policy still work?

FTP Without Confidentiality



Initial Setup Changes for FTPS



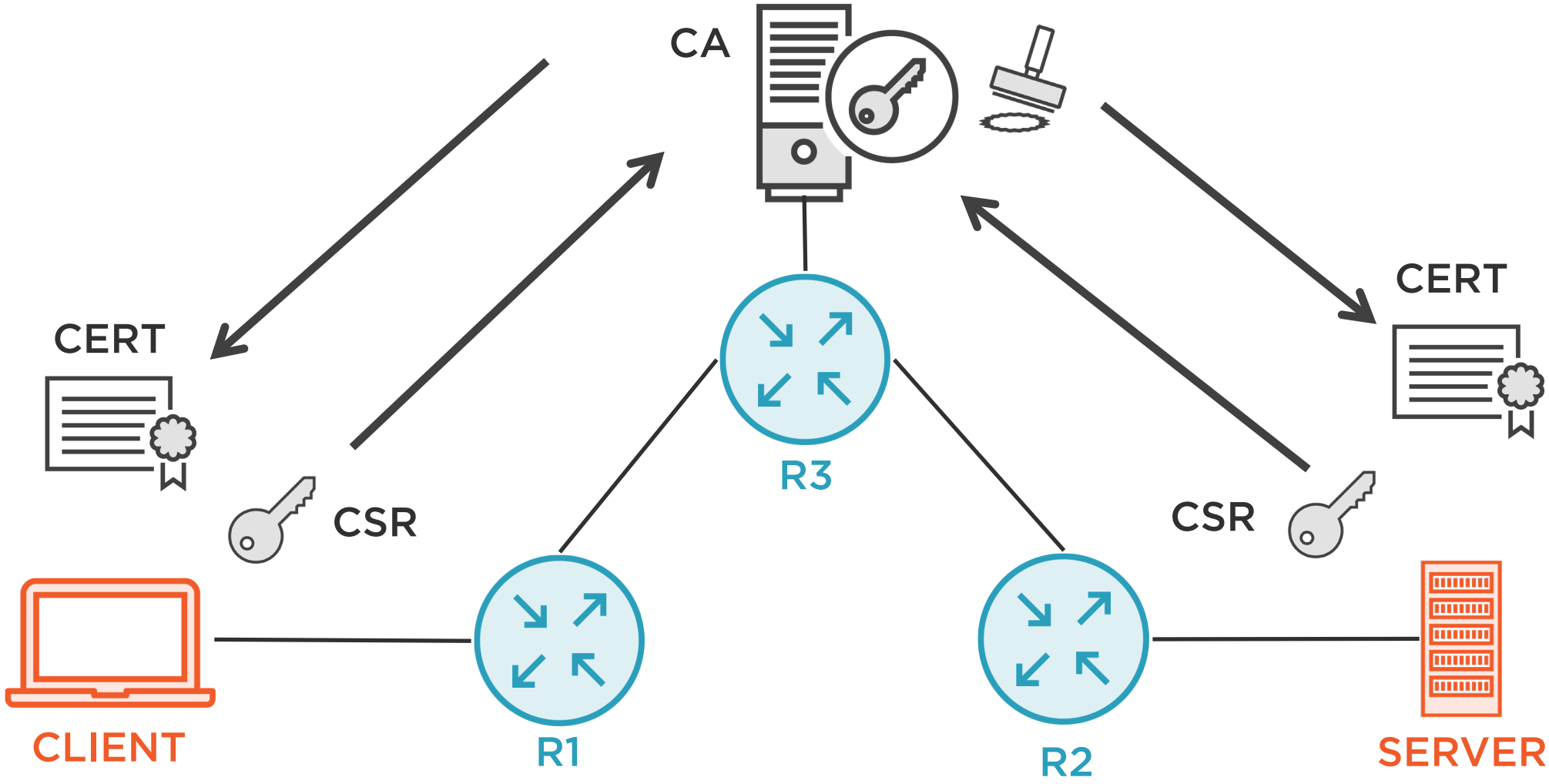
Introduction to Digital Certificates

Stronger authentication

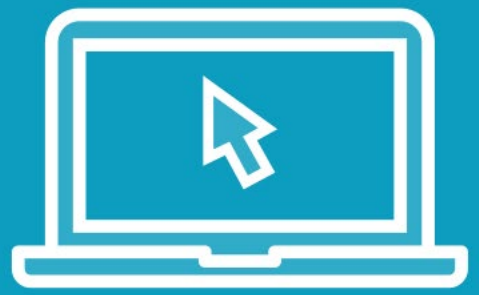
Encrypted communications

Many moving parts

High-level PKI Operations



Demo



Repelling the attackers with FTPS

FTPS Setup Actions

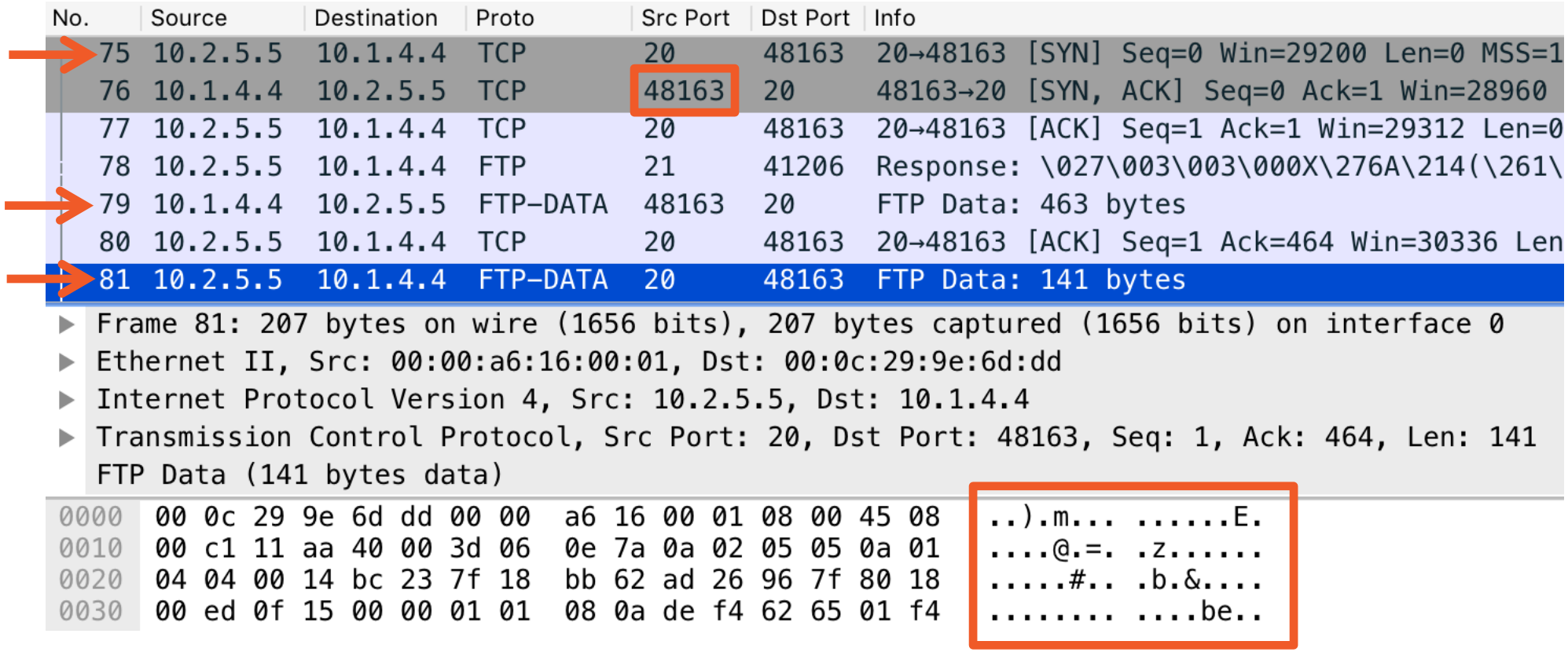
No.	Source	Destination	Proto	Src Port	Dst Port	Info
6	10.1.4.4	10.2.5.5	FTP	41206	21	Request: FEAT
7	10.2.5.5	10.1.4.4	TCP	21	41206	21→41206 [ACK] Seq=21 Ack=7 Win=29056 Len=0
8	10.2.5.5	10.1.4.4	FTP	21	41206	Response: 211-Features:
9	10.2.5.5	10.1.4.4	FTP	21	41206	Response: AUTH TLS
10	10.2.5.5	10.1.4.4	FTP	21	41206	Response: EPRT
11	10.2.5.5	10.1.4.4	FTP	21	41206	Response: EPSV
12	10.2.5.5	10.1.4.4	FTP	21	41206	Response: MDTM
13	10.2.5.5	10.1.4.4	FTP	21	41206	Response: PASV
14	10.1.4.4	10.2.5.5	TCP	41206	21	41206→21 [ACK] Seq=7 Ack=54 Win=29312 Len=0
15	10.2.5.5	10.1.4.4	FTP	21	41206	Response: PBSZ
16	10.2.5.5	10.1.4.4	FTP	21	41206	Response: PROT
17	10.2.5.5	10.1.4.4	FTP	21	41206	Response: REST STREAM
18	10.2.5.5	10.1.4.4	FTP	21	41206	Response: SIZE
19	10.1.4.4	10.2.5.5	TCP	41206	21	41206→21 [ACK] Seq=7 Ack=110 Win=29312 Len=0
20	10.2.5.5	10.1.4.4	FTP	21	41206	Response: TVFS
21	10.1.4.4	10.2.5.5	FTP	41206	21	Request: AUTH TLS
22	10.2.5.5	10.1.4.4	FTP	21	41206	Response: 234 Proceed with negotiation.

What's Happening?

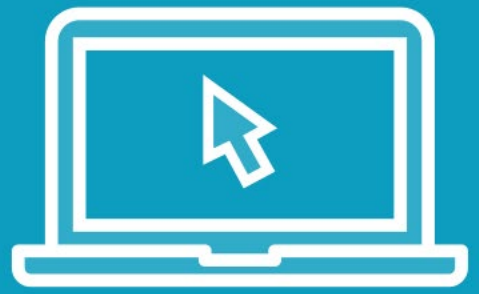
No.	Source	Destination	Proto	Src Port	Dst Port	Info
23	10.1.4.4	10.2.5.5	FTP	41206	21	Request: \026\003\001\000\372\001\000\000\366\003\003\\233
24	10.2.5.5	10.1.4.4	FTP	21	41206	Response: \026\003\003\000A\002\000\000=\003\003\004nDq\24
25	10.1.4.4	10.2.5.5	FTP	41206	21	Request: \026\003\003\000\a\v\000\000\003\000\000\000\026\
26	10.2.5.5	10.1.4.4	FTP	21	41206	Response: \026\003\003\000\272\004\000\000\266\177\377\377
27	10.1.4.4	10.2.5.5	FTP	41206	21	Request: \027\003\003\000&\000\000\000\000\000\000\000\001

```
▶ Frame 23: 321 bytes on wire (2568 bits), 321 bytes captured (2568 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: 41206, Dst Port: 21, Seq: 17, Ack: 157, Len: 255
▼ File Transfer Protocol (FTP)
  ▶ \026\003\001\000\372\001\000\000\366\003\003\\233v\243\313@\342\320.\000\260\362[\240\361\336\216\
    \300$\300s\300+\300\206\300\254\300\t\300#\300r\300\b\3000\300\213\314\250\300\024\300(\300w\300/\
    \000\237\300}\314\252\300\237\0009\000k\000\210\000\304\000\236\300|\300\236\0003\000g\000E\000\27
    \000\v\000\000\b10.2.5.5\377\001\000\001\000\000#\000\000\000\n
    \000\f\000\n
    \000\027\000\030\000\031\000\025\000\023\000\v\000\002\001\000\000\r
    \000\026\000\024\004\001\004\003\005\001\005\003\006\001\006\003\003\001\003\003\002\001\002\003
```

FTPS Active Mode Download

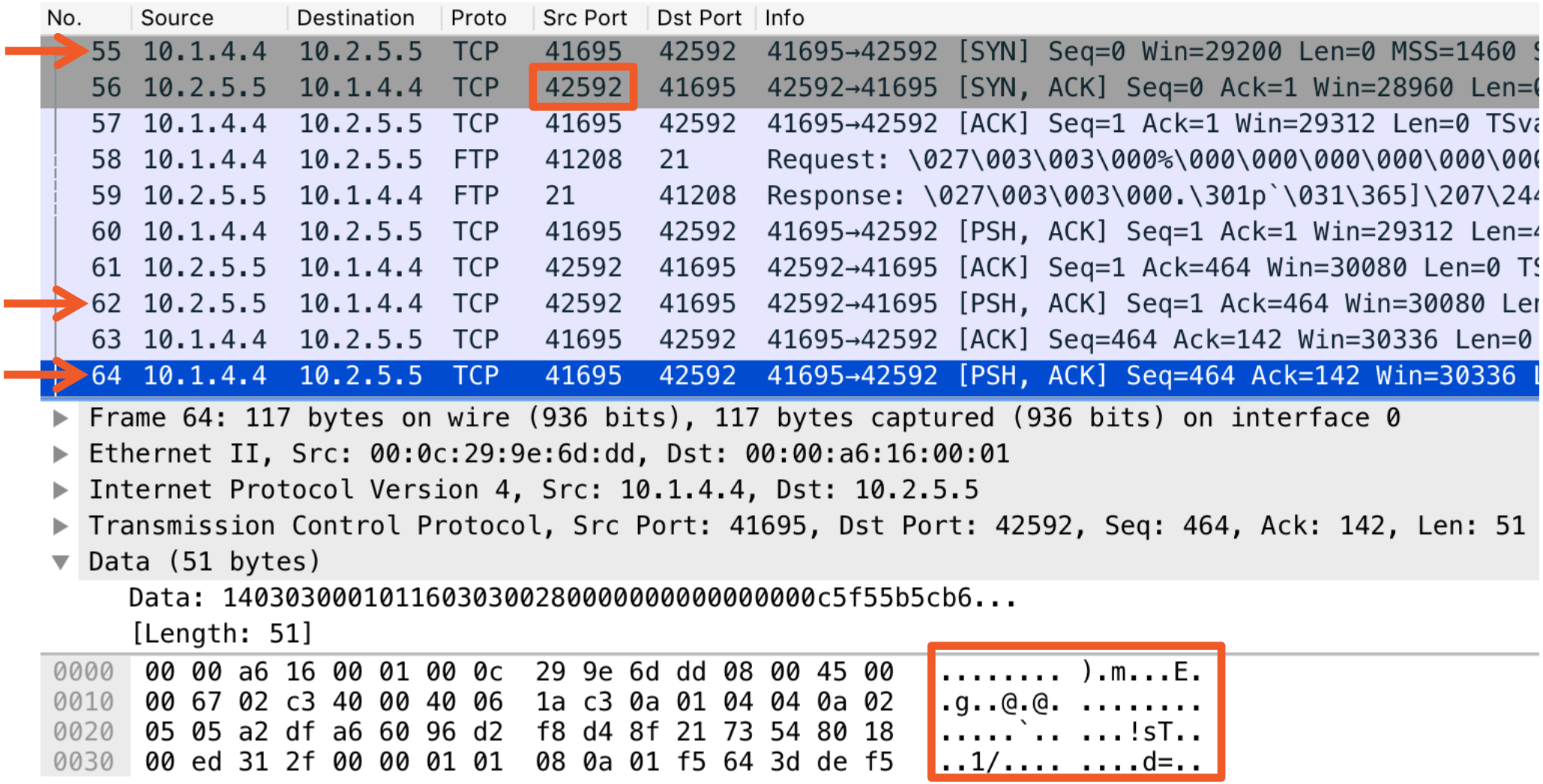


Demo

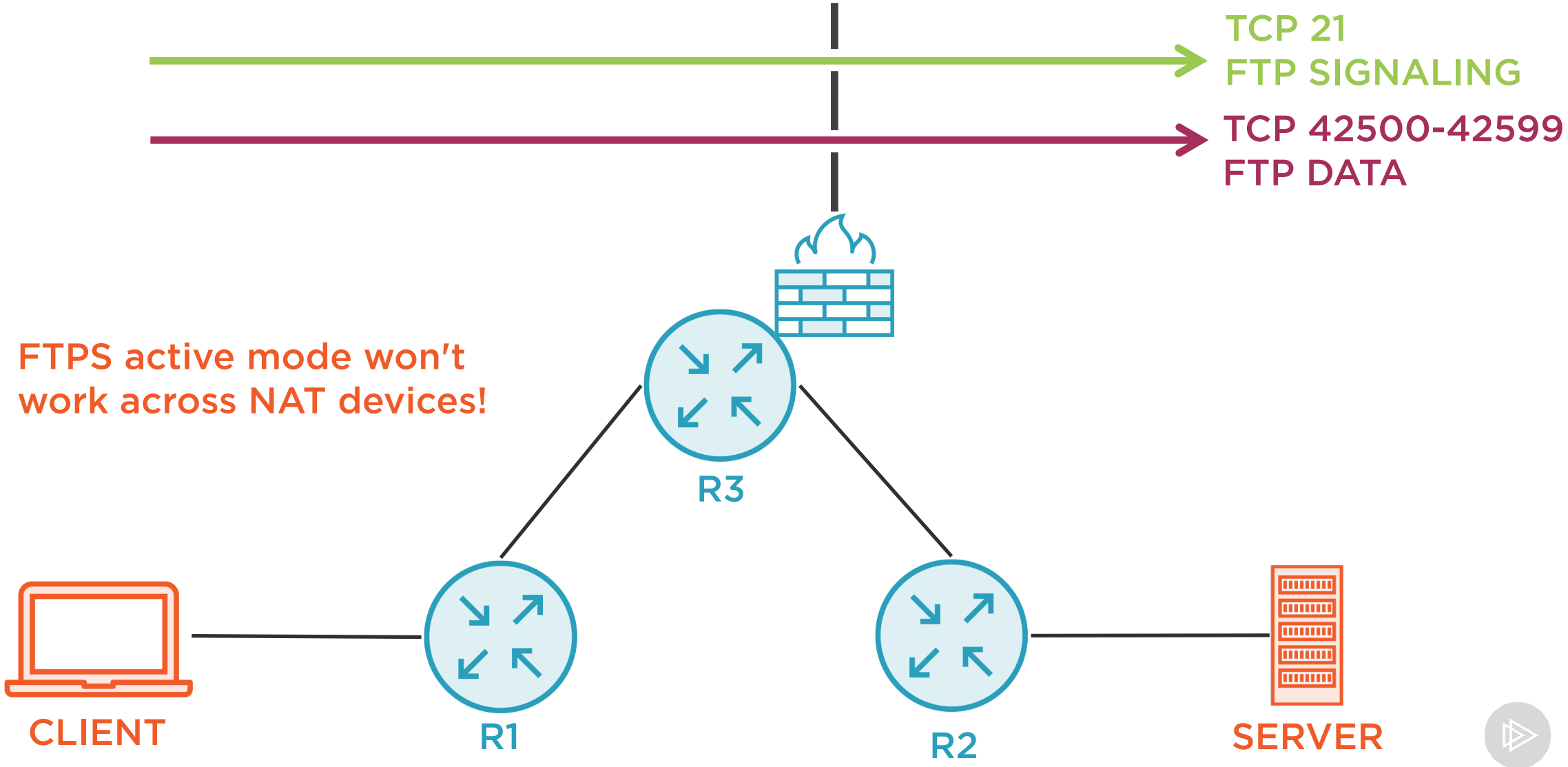


Can FTPS handle PASV and/or uploads?

FTPS Passive Mode Upload



Does Our Firewall Need Updates?



Unsecure FTP vs. FTPS

Unsecure FTP	FTPS
Authentication via user/pass	User/pass or client-side certs
Signaling insecure	Signaling always secure
Data insecure	Data optionally secure (PROT)
Active mode across NAT with SW	Active mode never works across NAT
Faster and lighter weight	Cert exchange and more traffic overall