

Protecting Data with FTP Secure (FTPS)



Nick Russo

NETWORK ENGINEER

@nickrusso42518 www.njrusmc.net



Agenda



How FTPS works

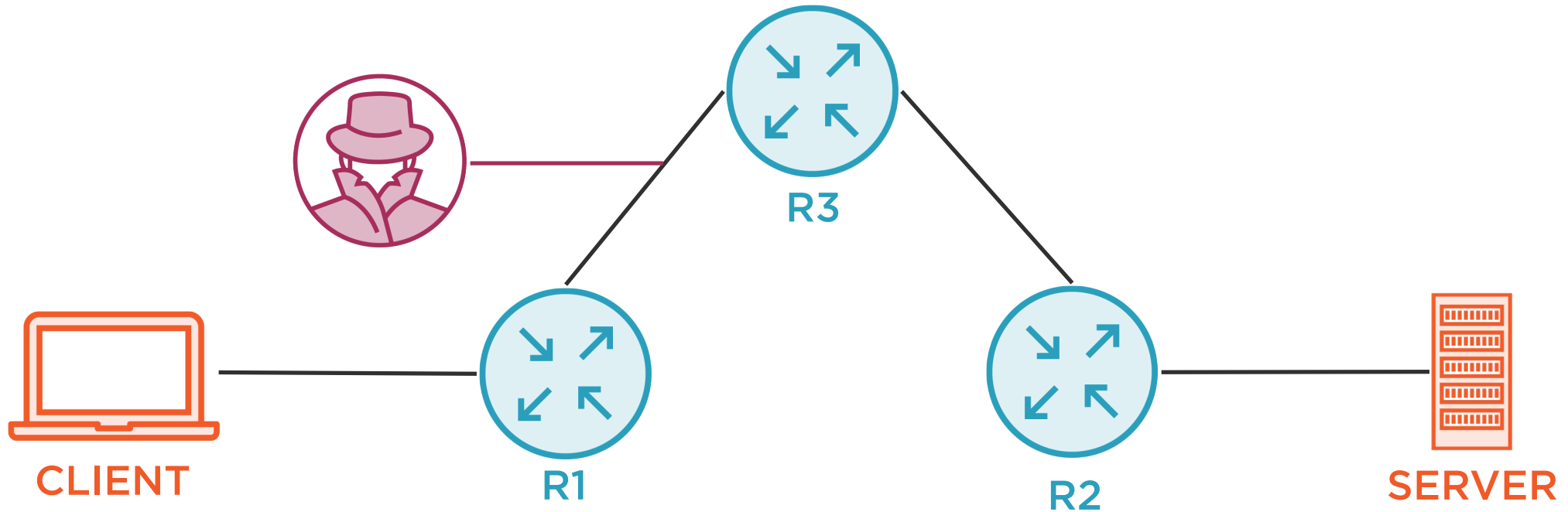
Introducing digital certificates and PKI

Configuring and testing FTPS

Does our firewall policy still work?



FTP Without Confidentiality

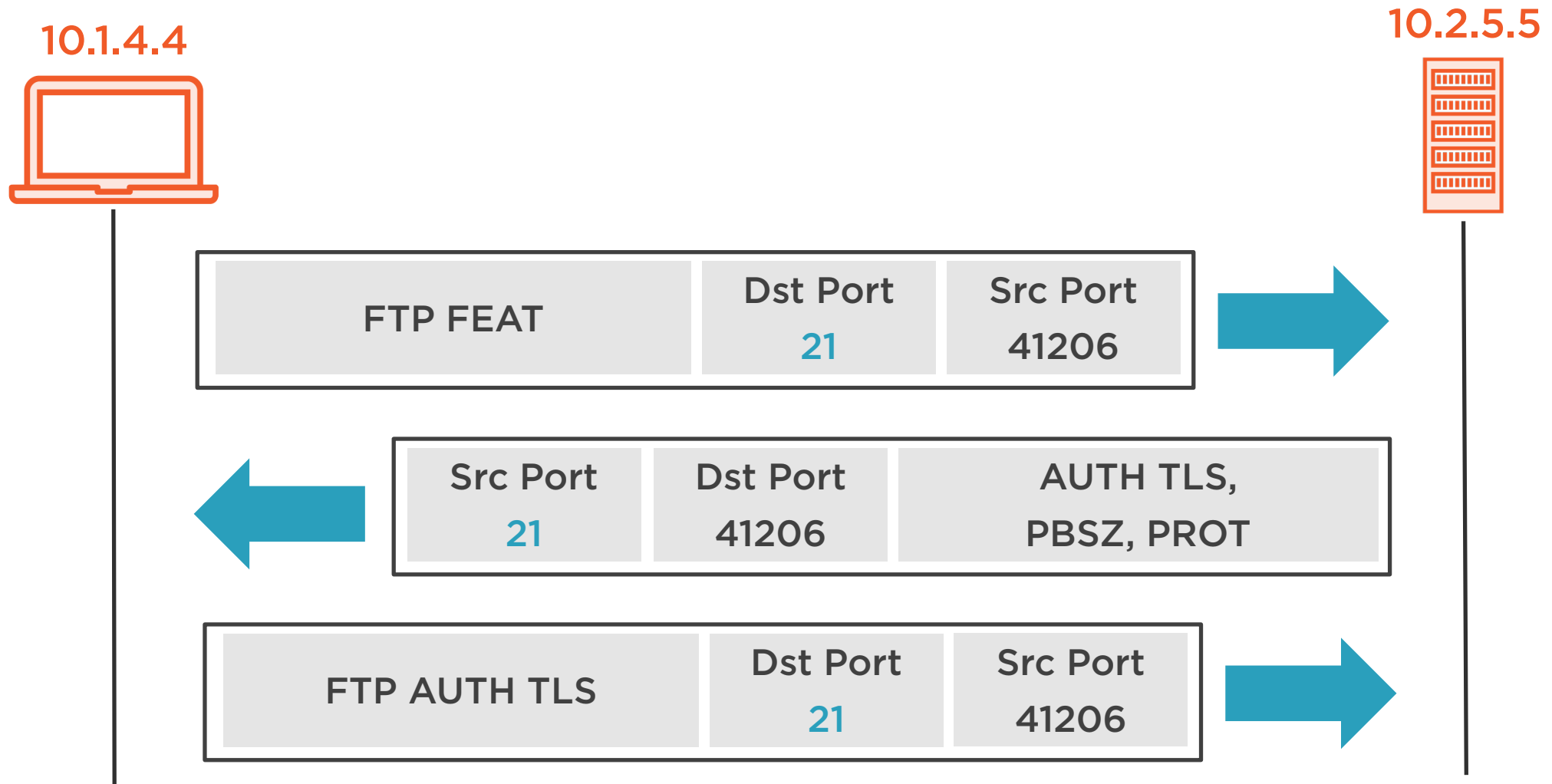


FTP PASS: ftppass / FTP RETR: fw_pps.txt

FTP data payload: "Here is our firewall PPS ..."



Initial Setup Changes for FTPS



Introduction to Digital Certificates

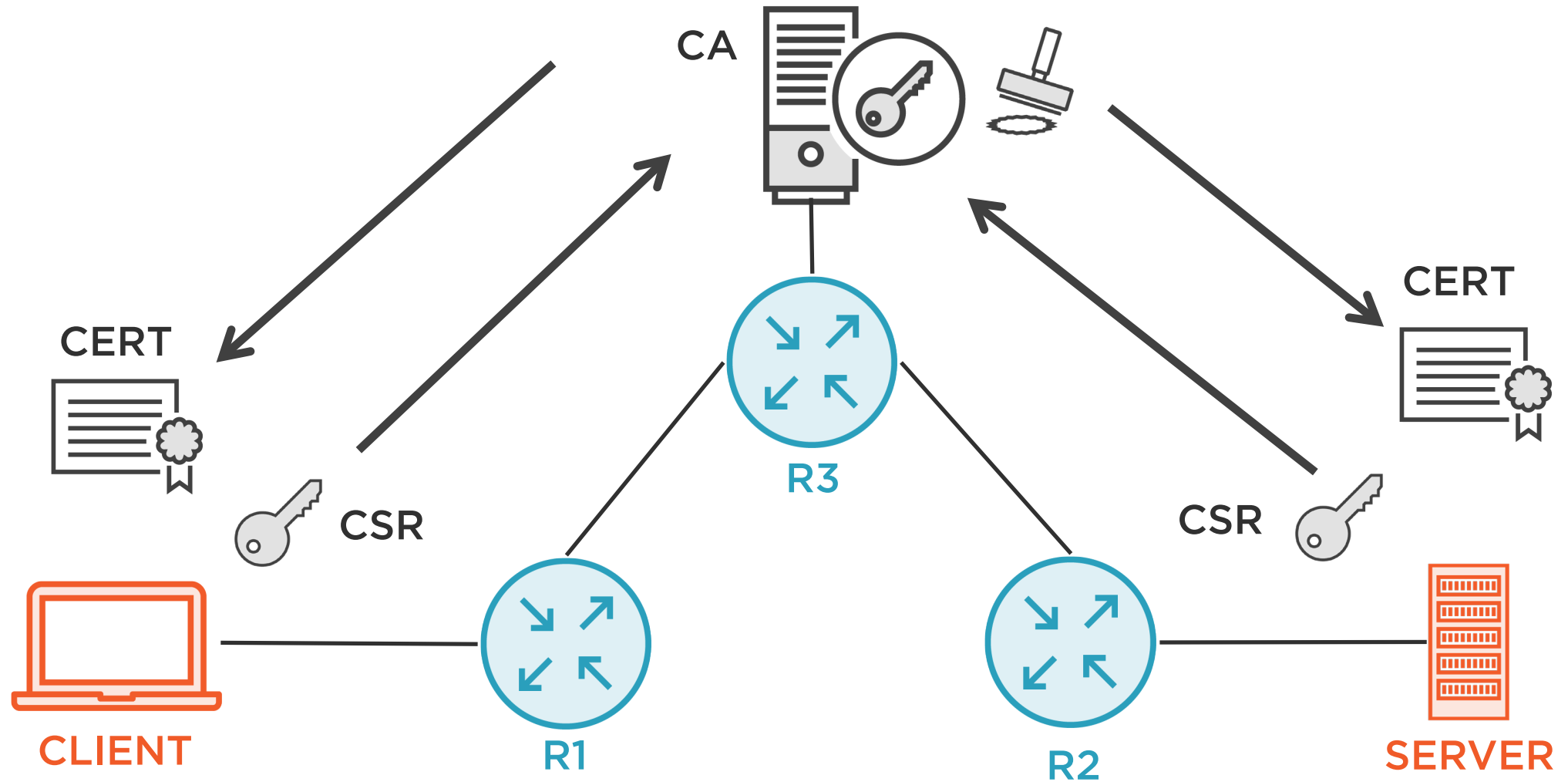
**Stronger
authentication**

**Encrypted
communications**

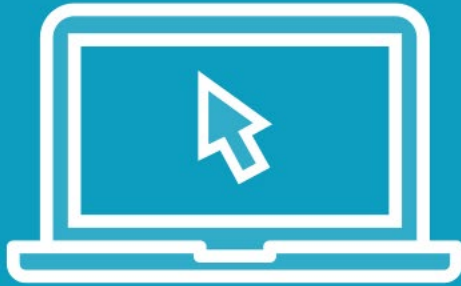
**Many moving
parts**



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\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/\300\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\10.2.5.5\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

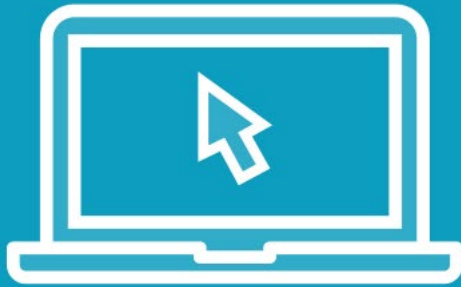
No.	Source	Destination	Proto	Src Port	Dst Port	Info
75	10.2.5.5	10.1.4.4	TCP	20	48163	20→48163 [SYN] Seq=0 Win=29200 Len=0 MSS=1
76	10.1.4.4	10.2.5.5	TCP	48163	20	48163→20 [SYN, ACK] Seq=0 Ack=1 Win=28960
77	10.2.5.5	10.1.4.4	TCP	20	48163	20→48163 [ACK] Seq=1 Ack=1 Win=29312 Len=0
78	10.2.5.5	10.1.4.4	FTP	21	41206	Response: \027\003\003\000X\276A\214(\261\
79	10.1.4.4	10.2.5.5	FTP-DATA	48163	20	FTP Data: 463 bytes
80	10.2.5.5	10.1.4.4	TCP	20	48163	20→48163 [ACK] Seq=1 Ack=464 Win=30336 Len
81	10.2.5.5	10.1.4.4	FTP-DATA	20	48163	FTP Data: 141 bytes

▶ Frame 81: 207 bytes on wire (1656 bits), 207 bytes captured (1656 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: 20, Dst Port: 48163, Seq: 1, Ack: 464, Len: 141
FTP Data (141 bytes data)

0000	00 0c 29 9e 6d dd 00 00	a6 16 00 01 08 00 45 08	..).m... ..E.
0010	00 c1 11 aa 40 00 3d 06	0e 7a 0a 02 05 05 0a 01@.=. .z.....
0020	04 04 00 14 bc 23 7f 18	bb 62 ad 26 96 7f 80 18#.. .b.&....
0030	00 ed 0f 15 00 00 01 01	08 0a de f4 62 65 01 f4be..



Demo



Can FTPS handle PASV and/or uploads?



FTPS Passive Mode Upload

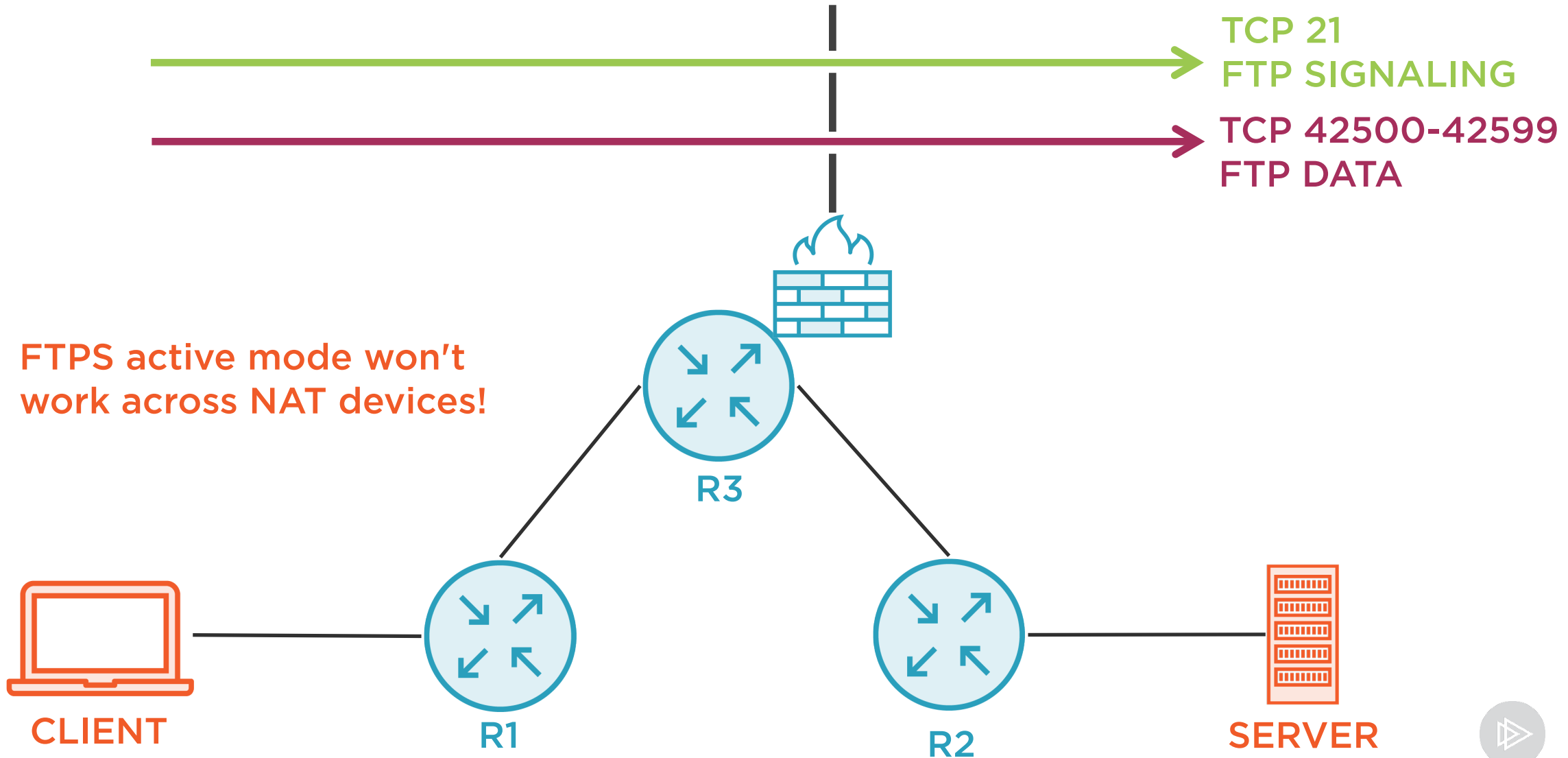
No.	Source	Destination	Proto	Src Port	Dst Port	Info
55	10.1.4.4	10.2.5.5	TCP	41695	42592	41695→42592 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 S
56	10.2.5.5	10.1.4.4	TCP	42592	41695	42592→41695 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
57	10.1.4.4	10.2.5.5	TCP	41695	42592	41695→42592 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSva
58	10.1.4.4	10.2.5.5	FTP	41208	21	Request: \027\003\003\000%\000\000\000\000\000\000
59	10.2.5.5	10.1.4.4	FTP	21	41208	Response: \027\003\003\000.\301p`\031\365]\207\244
60	10.1.4.4	10.2.5.5	TCP	41695	42592	41695→42592 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=4
61	10.2.5.5	10.1.4.4	TCP	42592	41695	42592→41695 [ACK] Seq=1 Ack=464 Win=30080 Len=0 TS
62	10.2.5.5	10.1.4.4	TCP	42592	41695	42592→41695 [PSH, ACK] Seq=1 Ack=464 Win=30080 Len
63	10.1.4.4	10.2.5.5	TCP	41695	42592	41695→42592 [ACK] Seq=464 Ack=142 Win=30336 Len=0
64	10.1.4.4	10.2.5.5	TCP	41695	42592	41695→42592 [PSH, ACK] Seq=464 Ack=142 Win=30336 L

▶ Frame 64: 117 bytes on wire (936 bits), 117 bytes captured (936 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: 41695, Dst Port: 42592, Seq: 464, Ack: 142, Len: 51
▼ Data (51 bytes)
Data: 1403030001011603030028000000000000000000c5f55b5cb6...
[Length: 51]

0000	00 00 a6 16 00 01 00 0c	29 9e 6d dd 08 00 45 00).m...E.
0010	00 67 02 c3 40 00 40 06	1a c3 0a 01 04 04 0a 02	.g..@.@.
0020	05 05 a2 df a6 60 96 d2	f8 d4 8f 21 73 54 80 18 \. . . !sT..
0030	00 ed 31 2f 00 00 01 01	08 0a 01 f5 64 3d de f5	..1/.....d=..



Does Our Firewall Need Updates?



Unsecure FTP vs. FTPS

Unsecure FTP

Authentication via user/pass

Signaling insecure

Data insecure

Active mode across NAT with SW

Faster and lighter weight

FTPS

User/pass or client-side certs

Signaling always secure

Data optionally secure (PROT)

Active mode never works across NAT

Cert exchange and more traffic overall

