Improving Confidentiality with SSH FTP (SFTP)

Nick Russo
NETWORK ENGINEER

@nickrusso42518 www.njrusmc.net

Agenda

- Introducing secure shell (SSH)
- How SFTP works
- Configuring and testing SFTP
- Firewall will need updates!

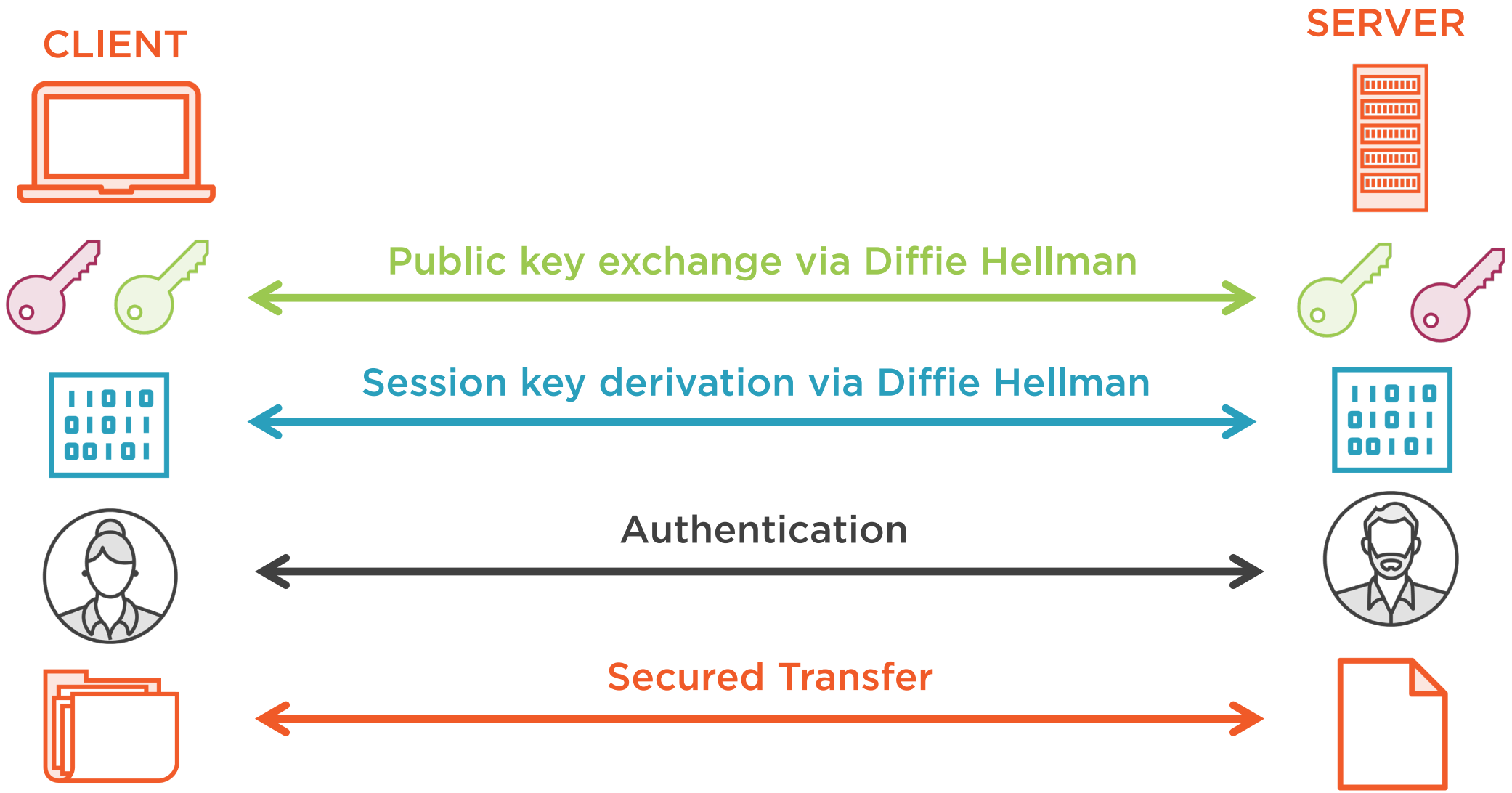
SFTP Characteristics

No official RFC

SSH-based transport

Difficult to decrypt

Protecting Traffic Using SSH



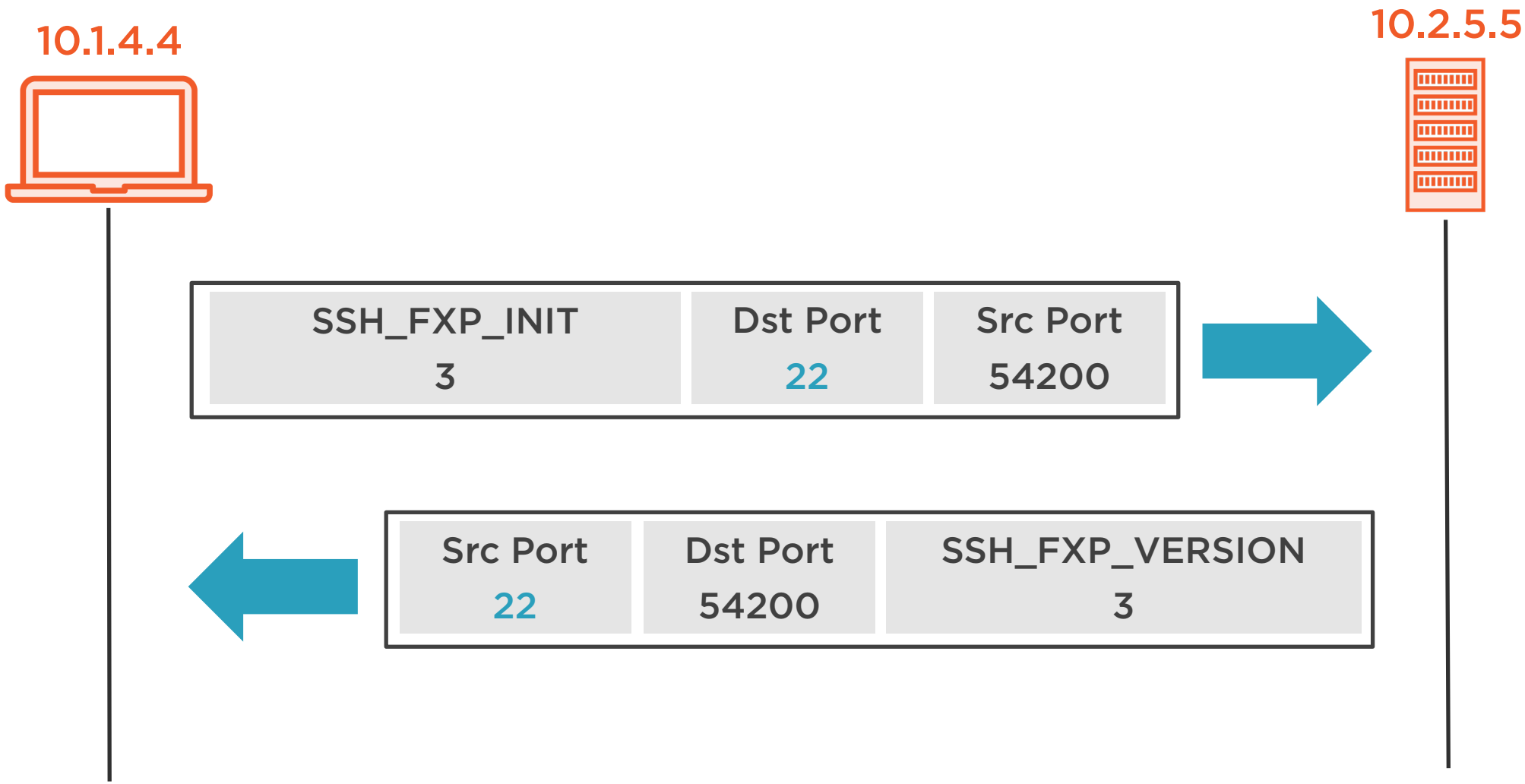
Wait! What About SCP?

Transfer files inside SSH

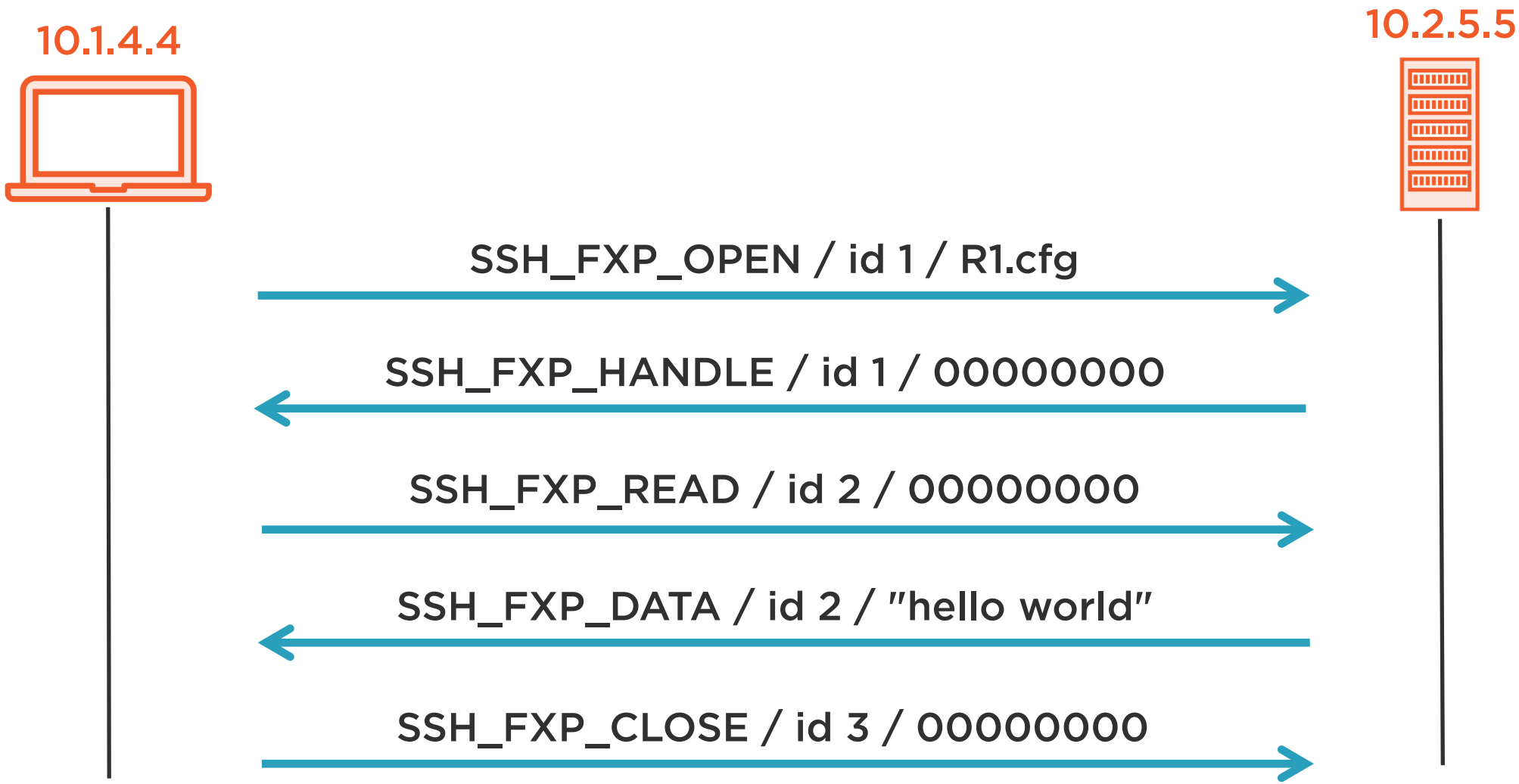
SCP can only transfer files

SFTP is technically superior

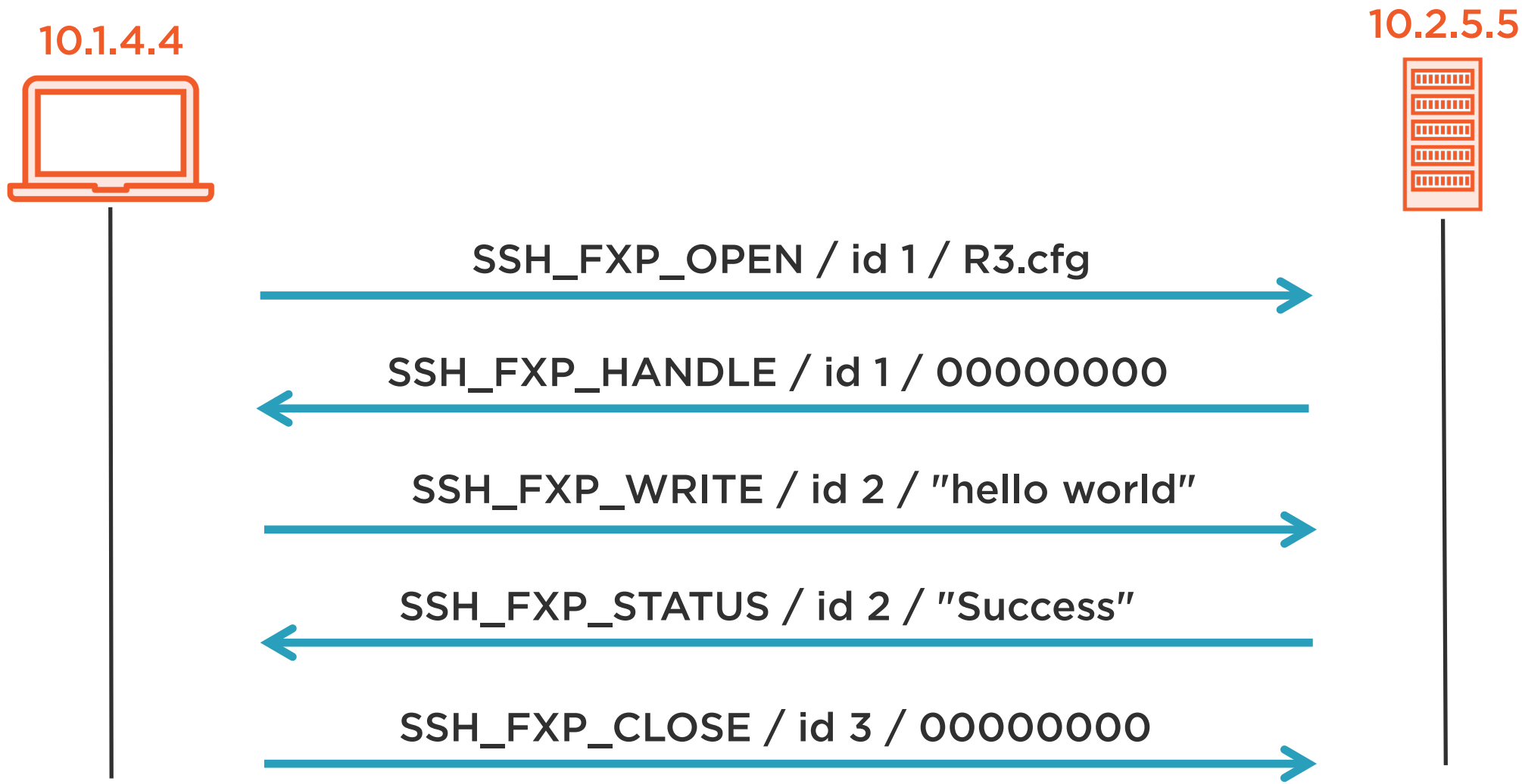
SFTP Initialization



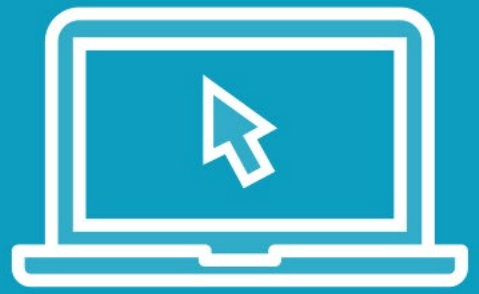
SFTP File Download



SFTP File Upload



Demo



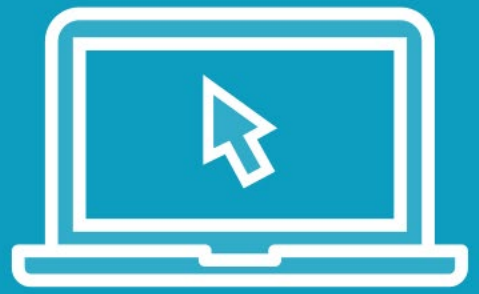
Using SFTP for downloading files

SFTP Codes Quick Reference

SFTP Client Message	Code
SSH_FXP_INIT	1
SSH_FXP_VERSION	2
SSH_FXP_OPEN	3
SSH_FXP_CLOSE	4
SSH_FXP_READ	5
SSH_FXP_WRITE	6
SSH_FXP_STATUS	101
SSH_FXP_HANDLE	102
SSH_FXP_DATA	103

https://tools.ietf.org/html/draft-ietf-secsh-filexfer-13#section-4.3

Demo

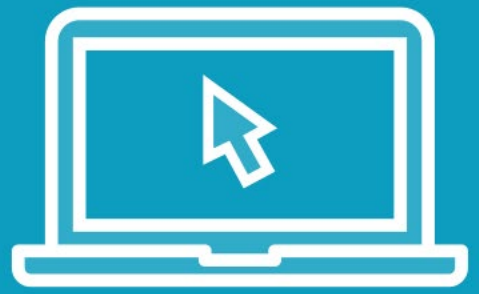


Using SFTP for uploading files

SSH and SFTP Chatter

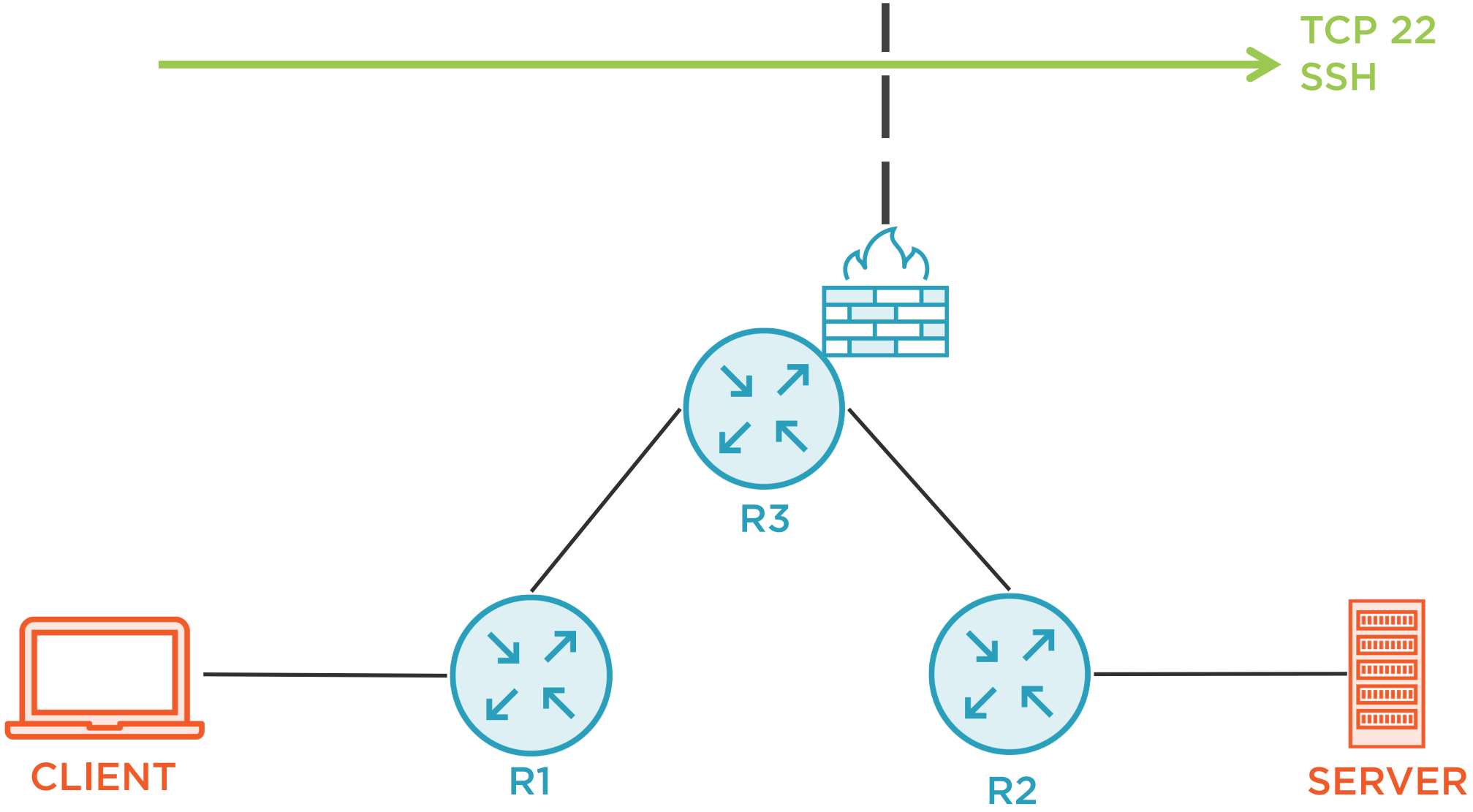
No. ▲	Source	Destination	Proto	Src Port	Dst Port	Info
4	10.1.4.4	10.2.5.5	SSHv2	54200	22	Client: Protocol (SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3)
5	10.2.5.5	10.1.4.4	TCP	22	54200	22→54200 [ACK] Seq=1 Ack=42 Win=29056 Len=0 TSval=37454196
6	10.2.5.5	10.1.4.4	SSHv2	22	54200	Server: Protocol (SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3)
7	10.1.4.4	10.2.5.5	TCP	54200	22	54200→22 [ACK] Seq=42 Ack=42 Win=29312 Len=0 TSval=3764267
8	10.2.5.5	10.1.4.4	SSHv2	22	54200	Server: Key Exchange Init
9	10.1.4.4	10.2.5.5	TCP	54200	22	54200→22 [ACK] Seq=42 Ack=1122 Win=31360 Len=0 TSval=37642
10	10.1.4.4	10.2.5.5	SSHv2	54200	22	Client: Key Exchange Init
11	10.2.5.5	10.1.4.4	TCP	22	54200	22→54200 [ACK] Seq=1122 Ack=1402 Win=31872 Len=0 TSval=374
12	10.1.4.4	10.2.5.5	SSHv2	54200	22	Client: Diffie-Hellman Key Exchange Init
13	10.2.5.5	10.1.4.4	TCP	22	54200	22→54200 [ACK] Seq=1122 Ack=1450 Win=31872 Len=0 TSval=374
14	10.2.5.5	10.1.4.4	SSHv2	22	54200	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encry
15	10.1.4.4	10.2.5.5	SSHv2	54200	22	Client: New Keys
16	10.2.5.5	10.1.4.4	TCP	22	54200	22→54200 [ACK] Seq=1574 Ack=1466 Win=31872 Len=0 TSval=374
17	10.1.4.4	10.2.5.5	SSHv2	54200	22	Client: Encrypted packet (len=44)
18	10.2.5.5	10.1.4.4	TCP	22	54200	22→54200 [ACK] Seq=1574 Ack=1510 Win=31872 Len=0 TSval=374
19	10.2.5.5	10.1.4.4	SSHv2	22	54200	Server: Encrypted packet (len=44)
20	10.1.4.4	10.2.5.5	SSHv2	54200	22	Client: Encrypted packet (len=68)

Demo



Updating the firewall policy for SFTP

Simplified Firewall Policy



FTP Secure vs. SSH FTP

FTP Secure (FTPS)	SSH FTP (SFTP)
Requires multiple flows and TCP ports	Requires only TCP port 22
Unique network profile	Looks just like SSH
Integrates with existing PKI	SSH key management can be hard
Good on the intranet	Good on the Internet or extranets