Designing Network Security for ICMP

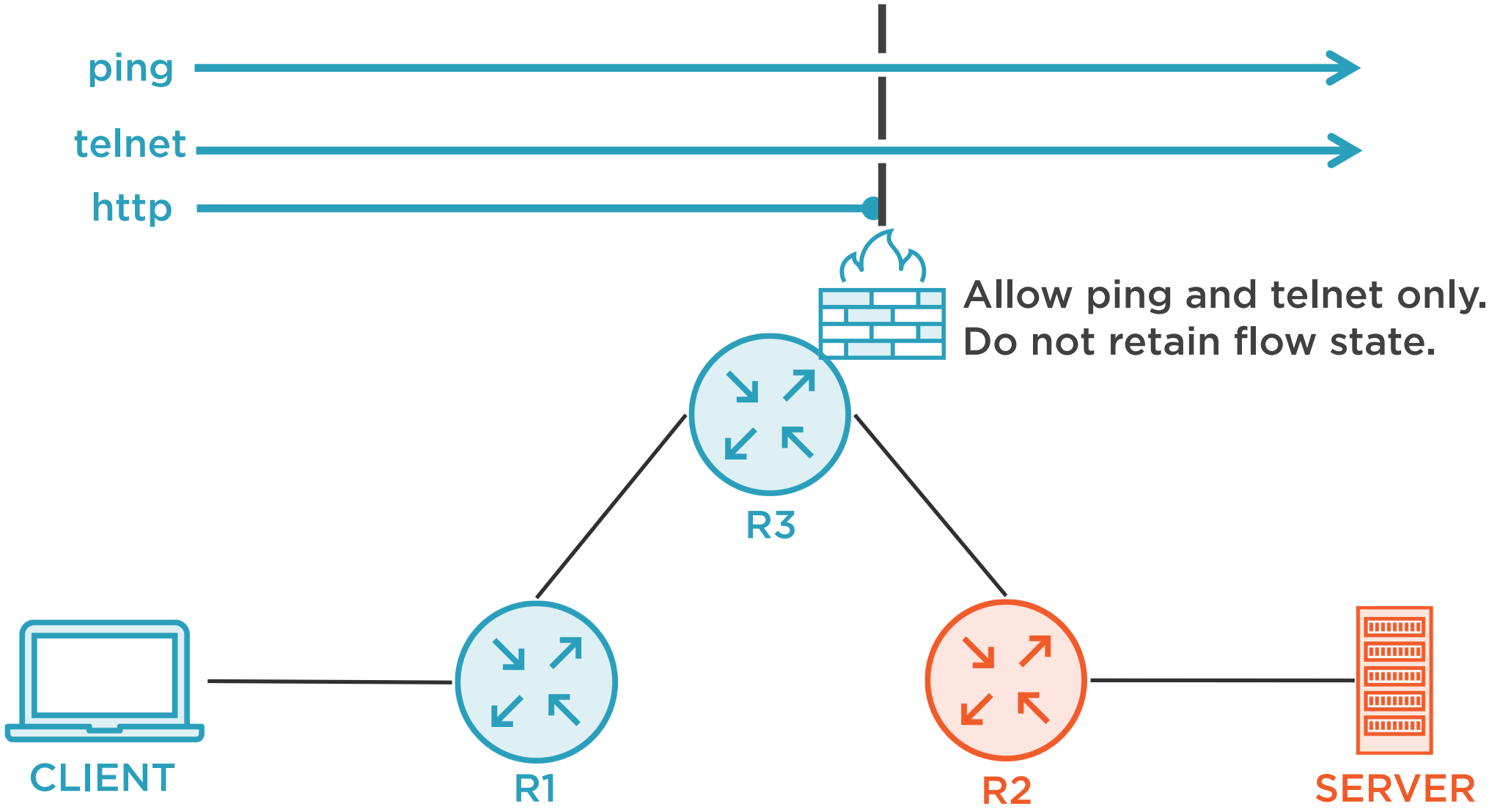
Nick Russo
NETWORK ENGINEER

@nickrusso42518 www.njrusmc.net

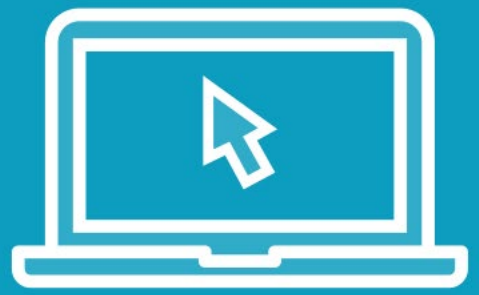
Agenda

- Stateless firewall basics
- Watching traceroute fail
- High Level ICMP firewall design
- Report firewall drops with ICMP
- Packet analysis

Stateless Firewall Operation

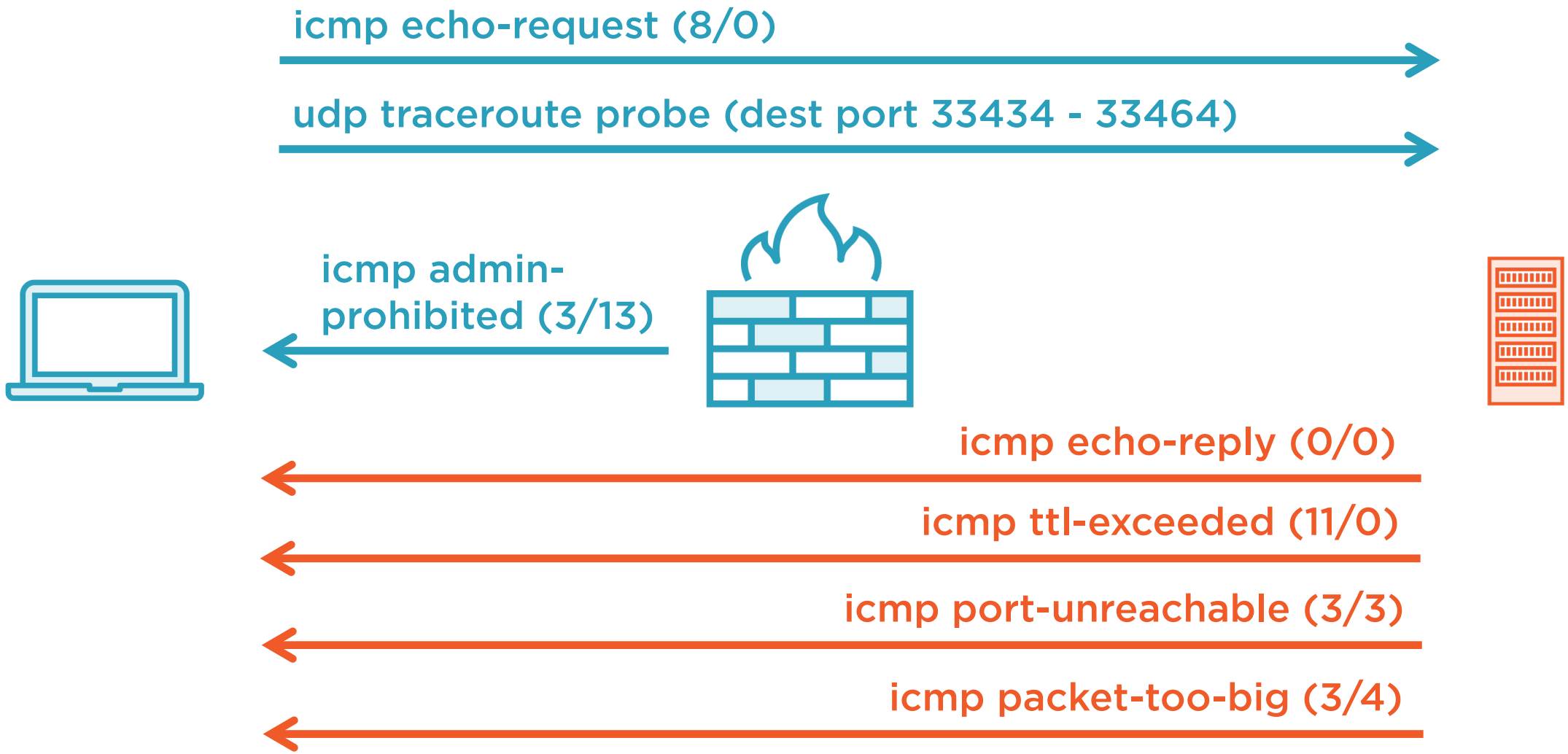


Demo

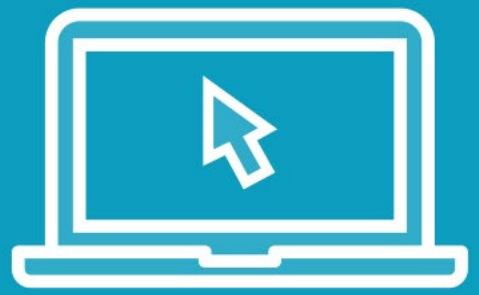


Watching traceroute fail

Firewall Design for ICMP



Demo



Let's test our firewall policy!

ICMP "Admin-prohibited"

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.1.4.4	10.2.5.5	TCP	26876→80 [SYN] Seq=0 Win=4128 Len=0 MSS=536
2	0.000902	10.1.3.3	10.1.4.4	ICMP	Destination unreachable (Communication administratively filtered)

```
▶ Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:00:a6:16:00:04
▶ Internet Protocol Version 4, Src: 10.1.3.3, Dst: 10.1.4.4
▼ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 13 (Communication administratively filtered)
    Checksum: 0x5a61 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ▶ Internet Protocol Version 4, Src: 10.1.4.4, Dst: 10.2.5.5
  ▶ Transmission Control Protocol, Src Port: 26876, Dst Port: 80
```

Type 3 is "unreachable"
Code 13 is "traffic denied"

Encapsulates original packet

Less Common ICMP Permits to Consider

Redirect

Type 5

All codes

Time-exceeded

Type 11

Frag reassembly

Code 1

Timestamp

Type 12

Timestamp-reply

Type 13

ICMP Security Design Recap

Permit some ICMP messages

Start with the basic design

ICMP for IPv4 complete!