



Firewall Refresher (Cisco)

Firewall Refresher (Cisco)

» Wireshark and firewalls

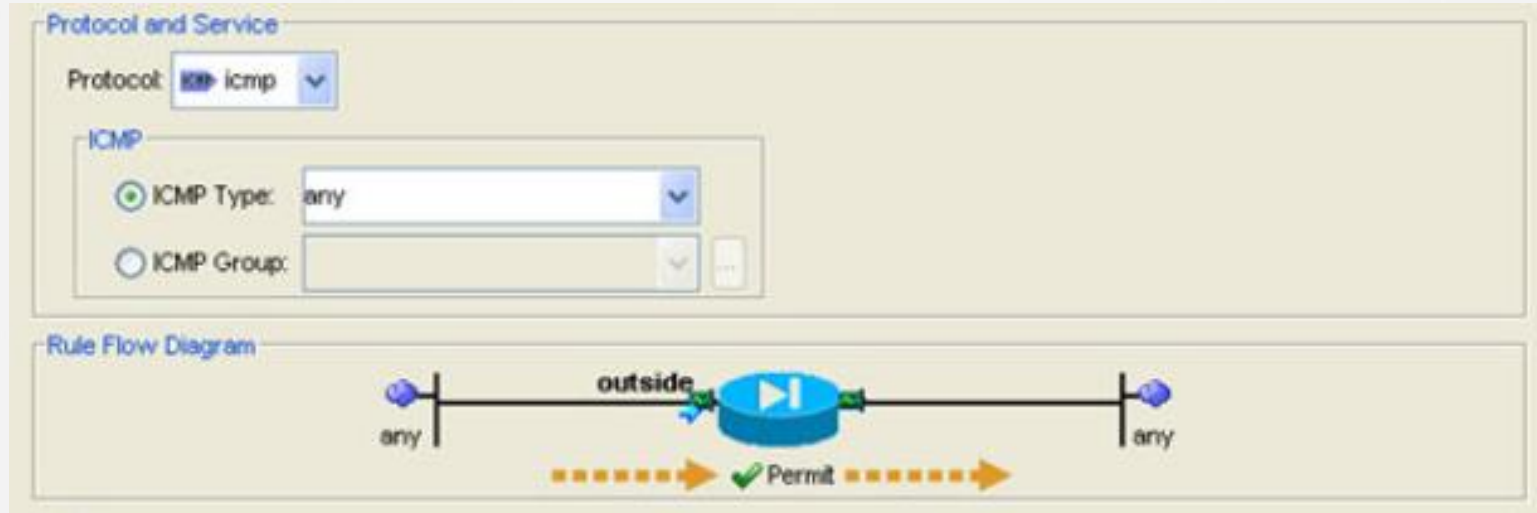
» How to analyze traffic

- Review capture for clues about firewalled segments
- Review network documentation
- Review with other tools (such as ping, traceroute, etc.)

» Common analysis outcome

- ICMP output

Firewall Refresher (Cisco)



Firewall Refresher (Cisco)

```

+ Frame 668: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
+ Ethernet II, Src: Cisco_56:dd:c8 (f0:f7:55:56:dd:c8), Dst: IntelCor_3b:35:4c (6c:88:14:3b:35:4c)
- Internet Protocol Version 4, Src: 10.121.68.1 (10.121.68.1), Dst: 10.121.68.41 (10.121.68.41)
  Version: 4
  Header Length: 20 bytes
+ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 60
  Identification: 0x477d (18301)
+ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: ICMP (1)
+ Header checksum: 0xd727 [correct]
  Source: 10.121.68.1 (10.121.68.1)
  Destination: 10.121.68.41 (10.121.68.41)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
- Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x535a [correct]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 513 (0x0201)
  Sequence number (LE): 258 (0x0102)
  [Request frame: 667]
  [Response time: 278.379 ms]
+ Data (32 bytes)
```

Questions?