

# Analyzing Common Attack Signatures of Suspect Traffic

---

## Module Overview



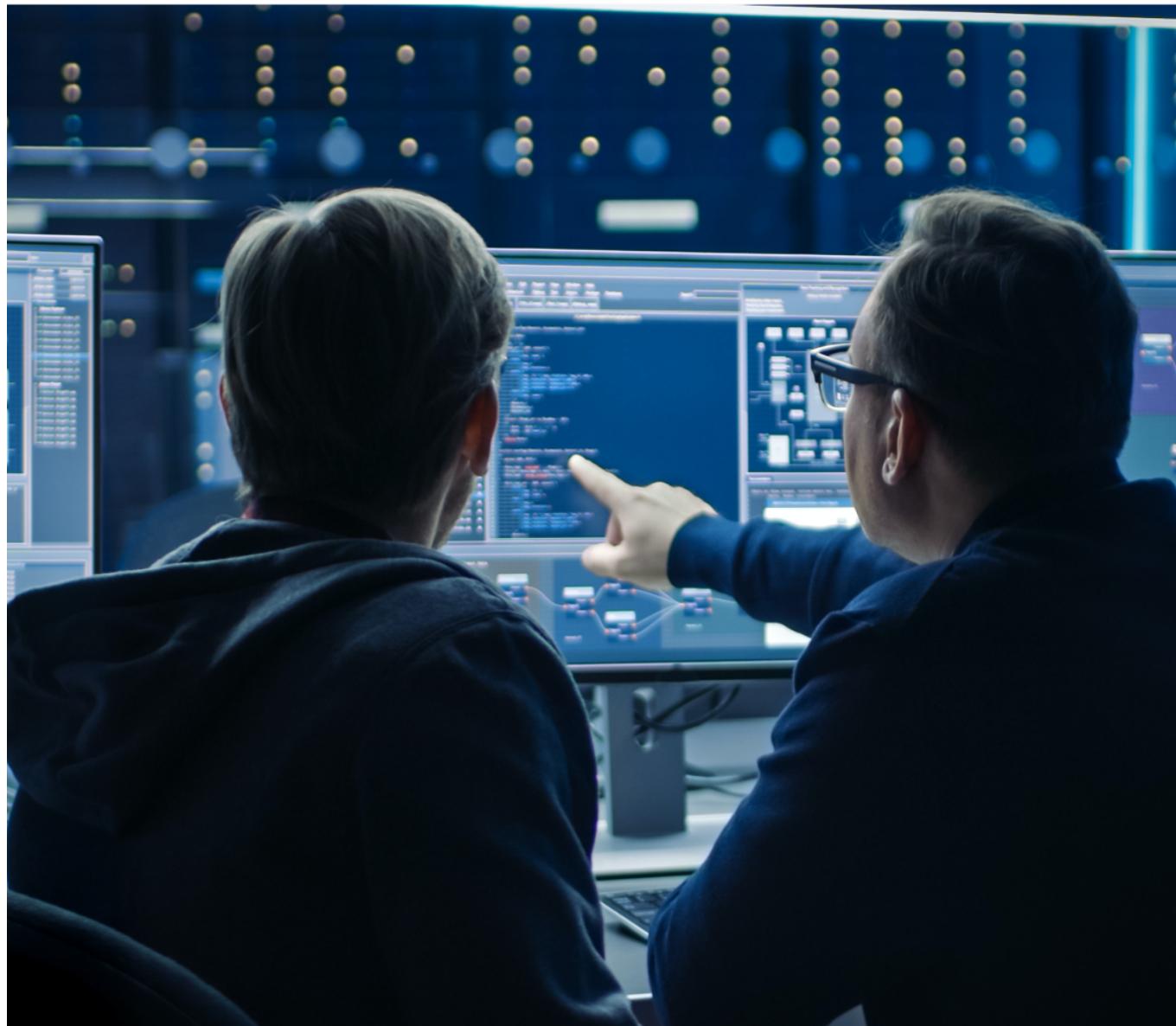
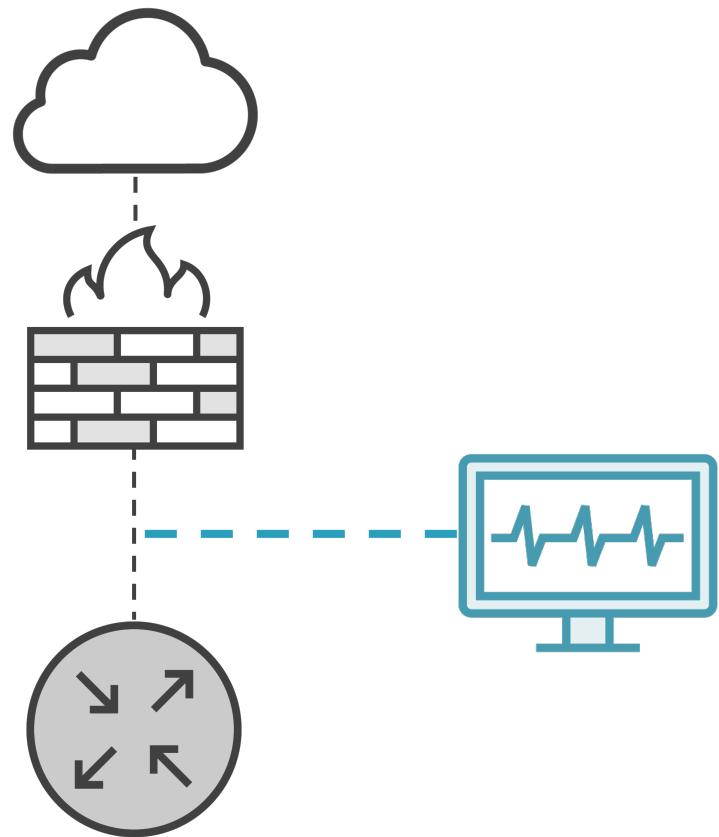
**What Does “Suspect Traffic” Look Like?**

**What is a Signature?**

**Top 10 Things to Look For in the Packets**

**Wireshark Filters to Catch This Behavior**

# Know What “Normal” Looks Like



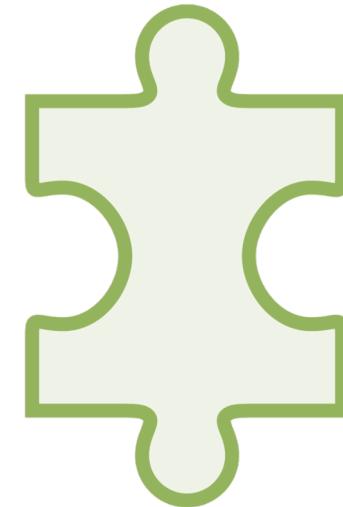
# How Do We Know What to Look For?



**Start with Alerts**



**Ask Plenty of  
Questions**



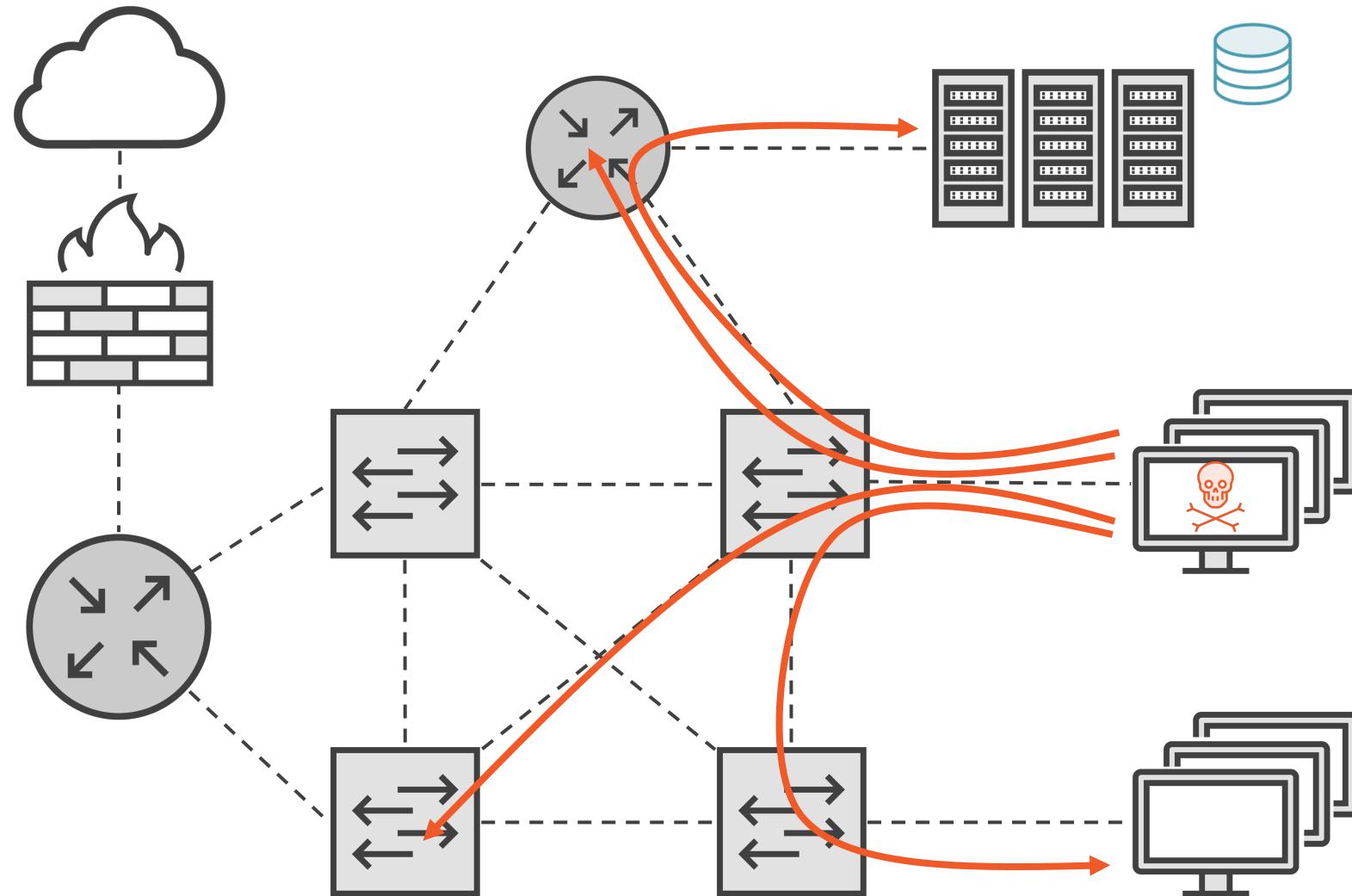
**Keep It Simple**

Before we go further, make sure to  
create a Security profile in Wireshark.  
Ok, let's dig!

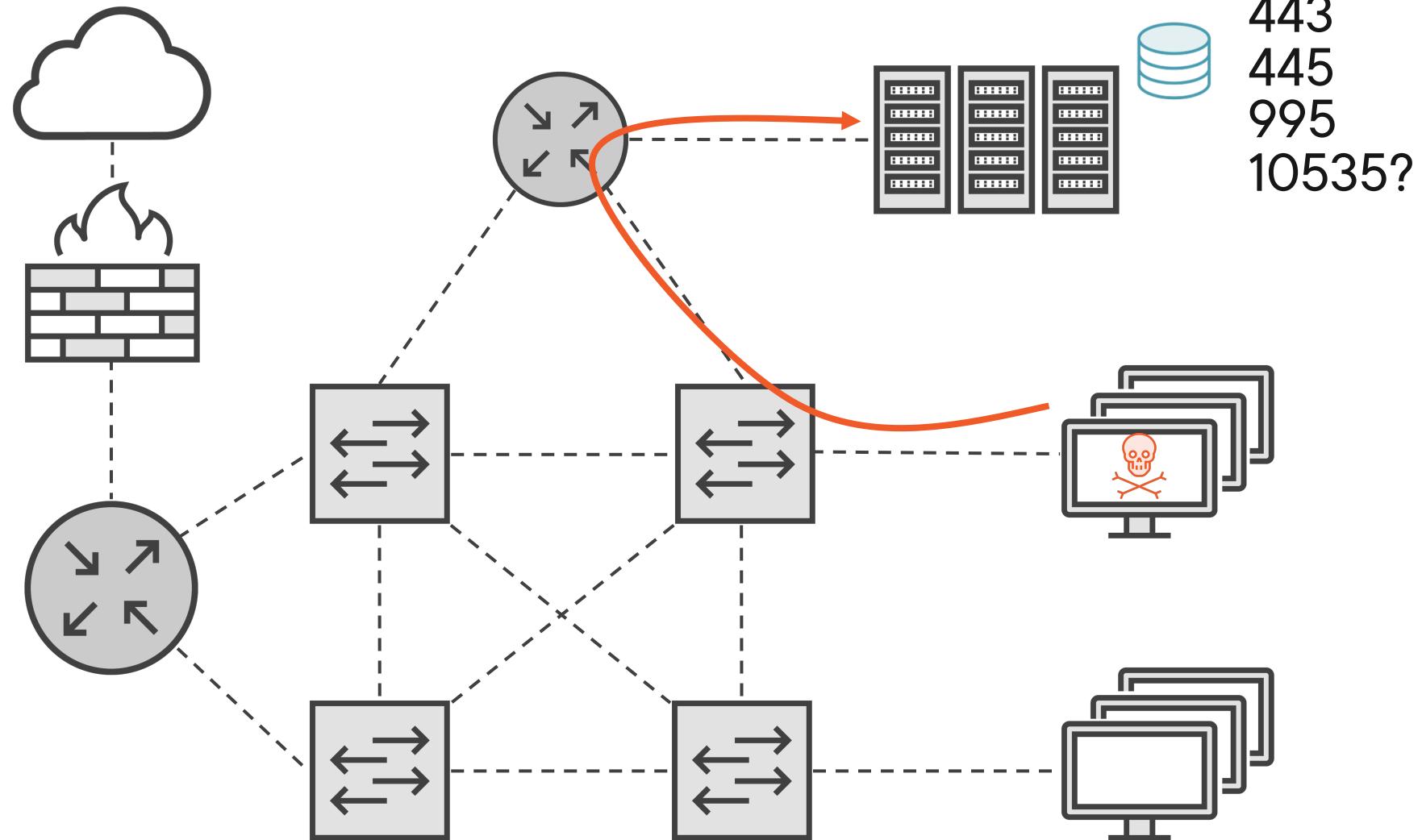
# The Top Ten Things to Look for When Analyzing Suspect Traffic

---

# 1. TCP SYN Scan



## 2. Unusual Port Numbers



# Useful Wireshark Filters

Attack Method	Wireshark Filter
TCP SYN Scan	<code>tcp.flags.syn==1 and tcp.flags.ack==0</code>
Unusual Port Numbers	<code>!tcp.port in {443 1433 445 995 8000..8005}</code>
Nmap Stealth Scan	<code>tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window_size &lt;=1024</code>

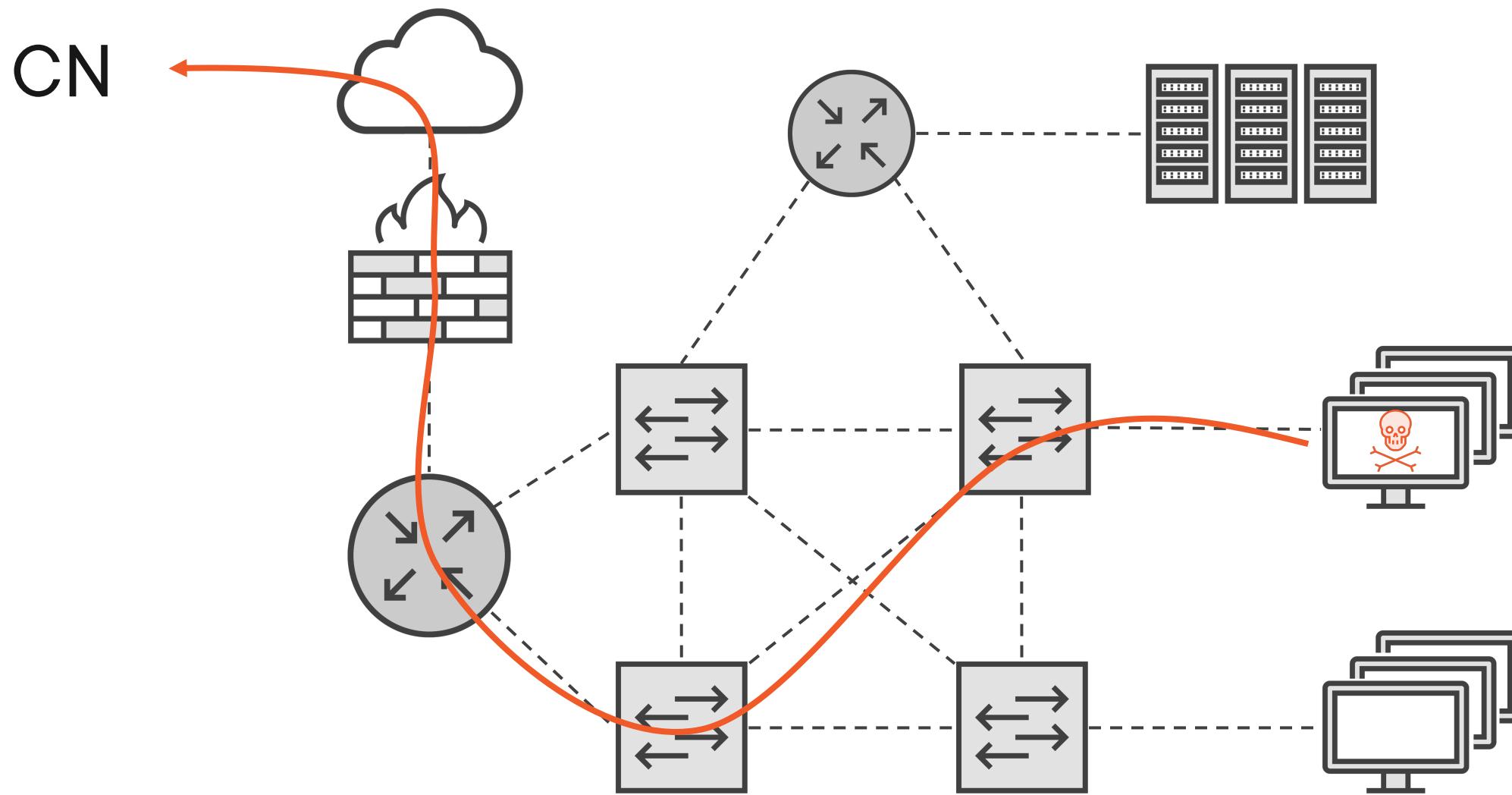
Be careful with these filters. Just because something matches the filter does not mean it is malicious.

Demo

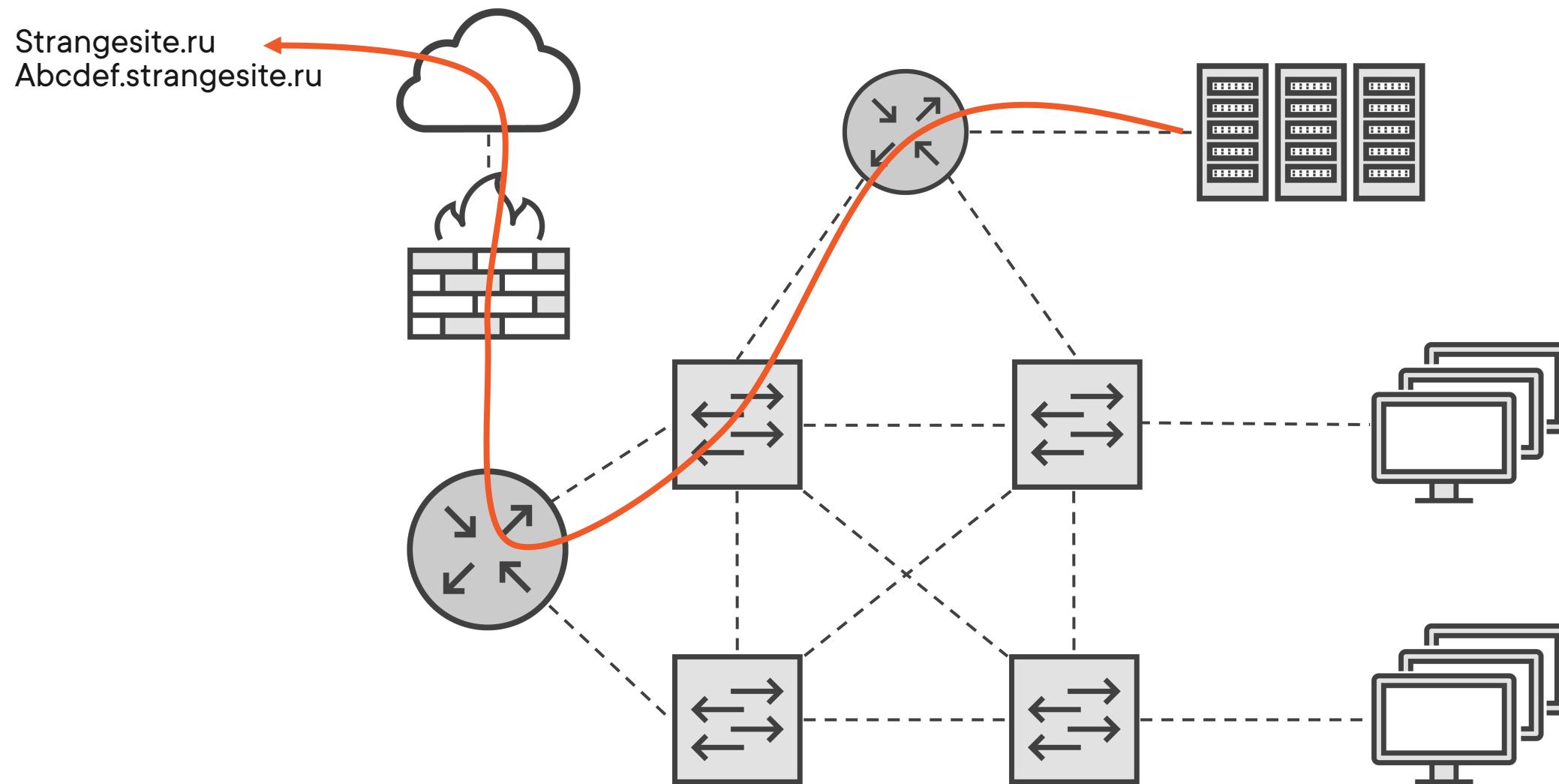


## **Lab 6 – Detecting Unusual TCP SYN Behavior and Unusual Port Numbers**

### 3. GeoIP Location to Suspect Country Codes



## 4. Domain Calls Including Suspect Countries



# Useful Wireshark Filters

Attack Method	Wireshark Filter
Suspect Geolocated IP Country	<code>ip.geoip.country == Russia</code>
Country Code	<code>ip.geoip.country_iso == CN</code>
Everything but a Country	<code>ip and !ip.geoip.country_iso == US</code>
Strange DNS	<code>dns.qry.name matches "(us mx cr)"</code>

Demo



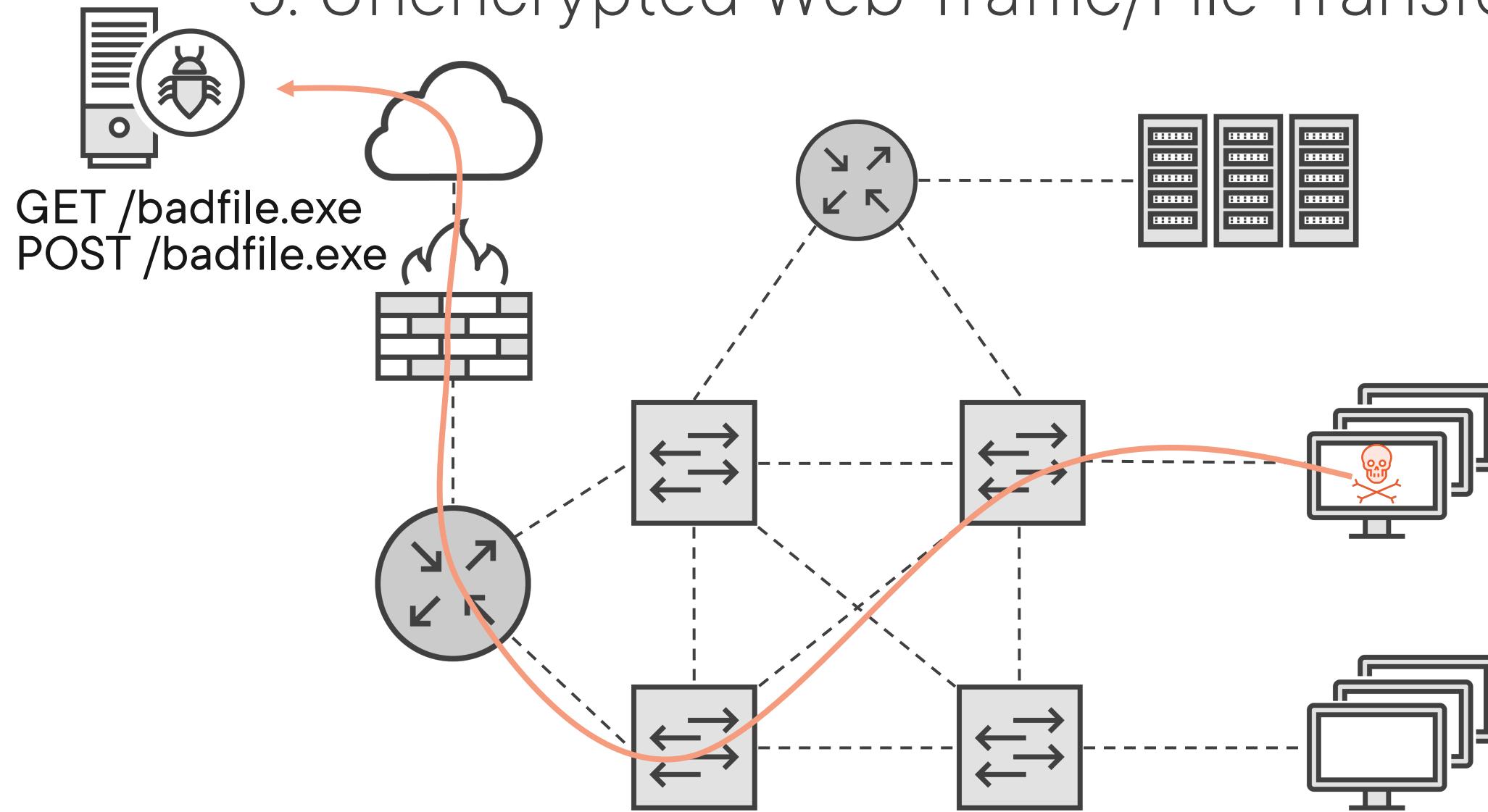
## Lab 7 – Finding Unusual Conversations to Remote Countries

Demo

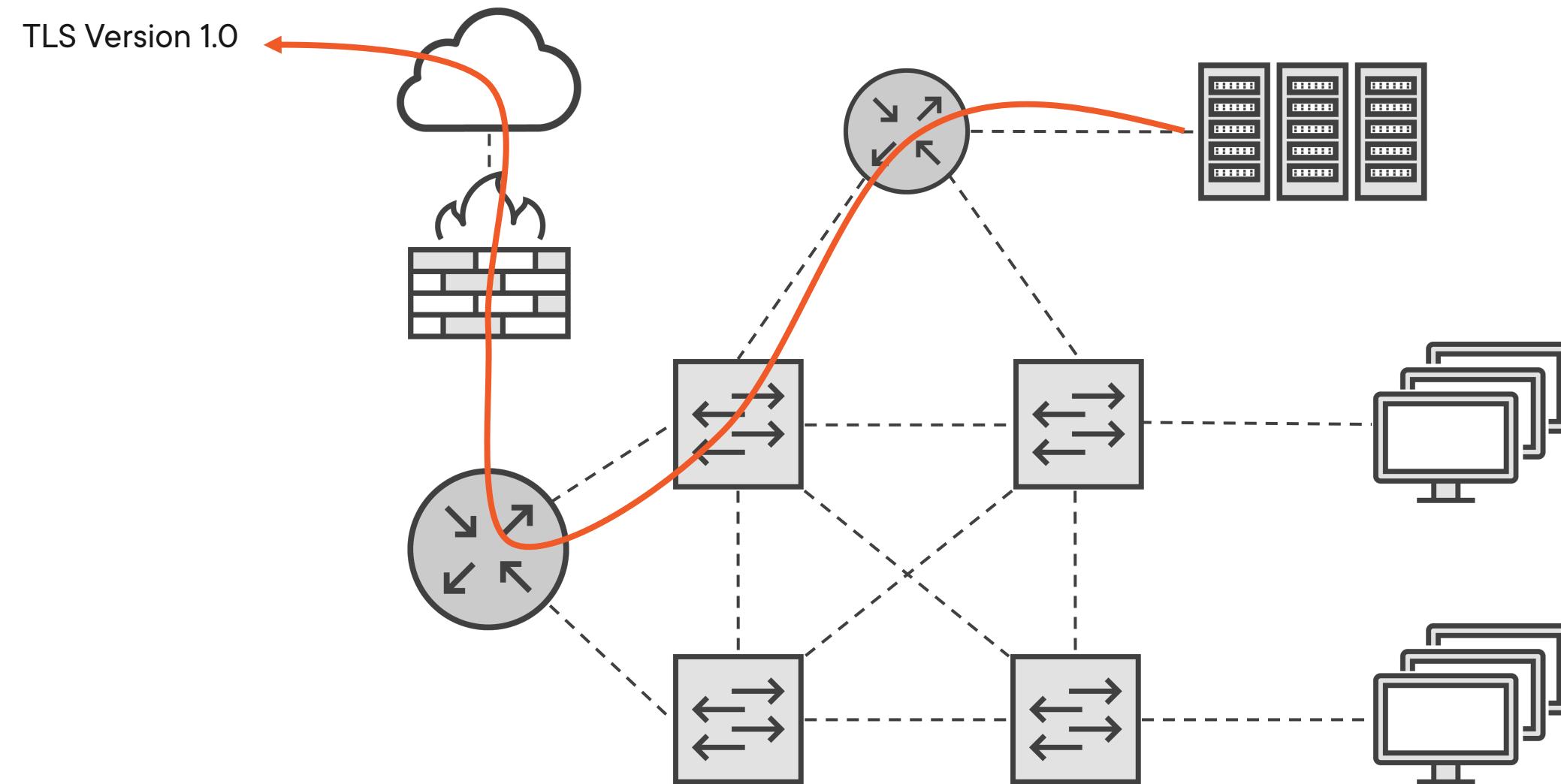


## Lab 8 – Spotting Suspect Domain Names

## 5. Unencrypted Web Traffic/File Transfers



# 6. Outdated TLS / Bad User Agents



# Useful Wireshark Filters

Attack Method	Wireshark Filter
Malware Downloads .bin/.exe/.php	<code>http.request.uri matches "(tar exe zip pdf bin php)"</code>
FTP File Transfers	<code>ftp.request.command == "RETR"</code>
Unencrypted Strings	<code>frame contains torrent</code>
Old TLS Versions	<code>tls.handshake.extensions.supported_version in {0x0300 0x0301 0x0302}</code>

Demo



## Lab 9 – Analyzing Unencrypted File Transfers in Wireshark

# Top Ten Things to Look For



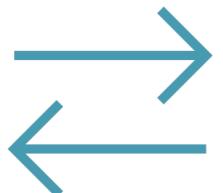
**7. Large DNS (Or Other) Packets for Sustained Periods – Data Exfiltration**



**8. Outbound SYN/ACK Replies (SYN Came from Outside Network)**



**9. Brute Force Password Behavior (FTP, SSH, RDP, HTTP)**



**10. Reverse Shell Behavior – TCP Port 4444, 1337, 1234, 6001, 8080**

# Useful Wireshark Filters

Attack Method	Wireshark Filter
DNS Exfiltration	DNS and ip.len > 200
Outbound SYN/ACK	tcp.flags.syn==1 and tcp.flags.ack==1 and (!ip.dst==10.0.0.0/8) <b>(insert local IP range)</b>
Brute Force Attacks	frame contains admin
Reverse Shell Behavior	tcp.port in {1234 4444 1337 6001}

Demo



## Lab 10 – Analyzing A Brute Force Attack on an FTP Server

## Module Overview



**What Does “Suspect Traffic” Look Like?**

**What is a Signature?**

**Top 10 Things to Look For in the Packets**

**Wireshark Filters to Catch This Behavior**