#sf21veu

Trace File Case Files

Jasper Bongertz
Team Packet-Foo

Hello!

I am Jasper Bongertz

I am here because I love analyzing packets ☺

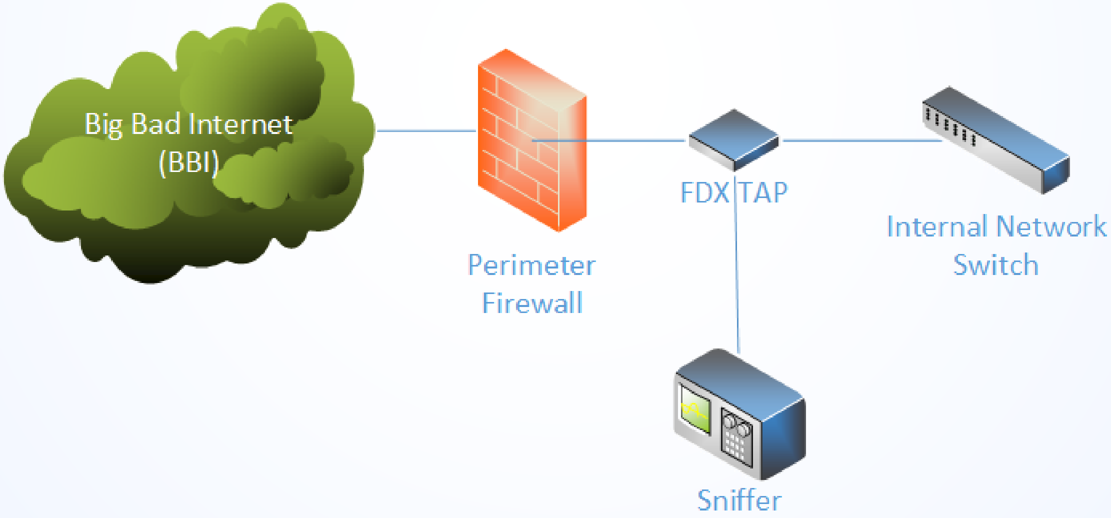
You can find me at @packetjay

Case 1: Beachhead

#sf21veu

- Ransomware Victim
- Possible ongoing attacker activities
- Task: try to find malicious traffic

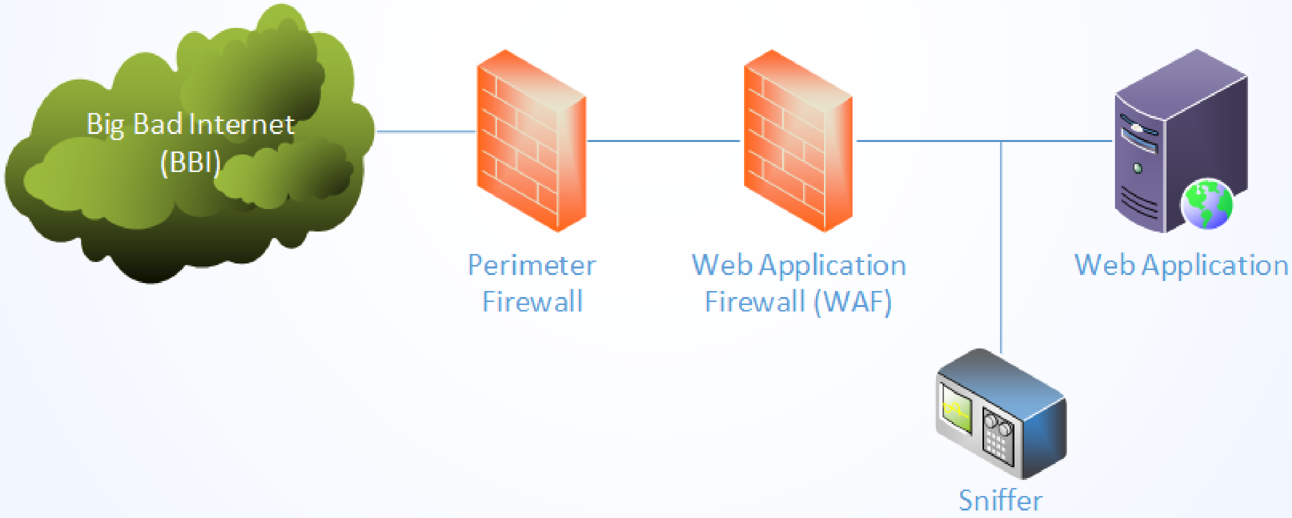
Case 1: Beachhead



Case 2: Defended?

- Ransomware Victim. Yep. Another.
- Critical custom built web application
  - Initial breach vector?
  - Countermeasure: WAF
- Task: verification required

Case 2: Defended?

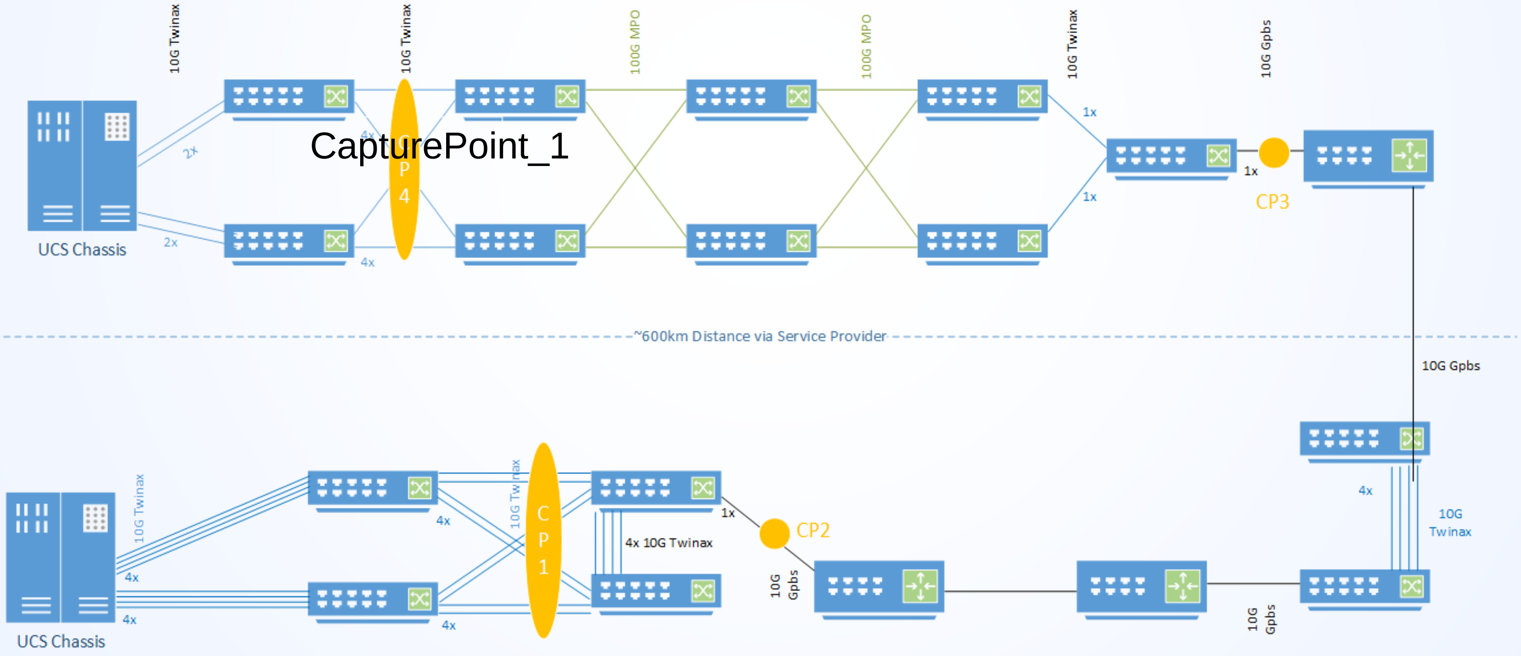


Case 3: SRSLY?

- Virtualization environments on 2 datacenters
- Connected via 10G fiber
- Distance: ~600km
- Problem: bad throughput when moving VMs from one site to the other

Case 3: SRSLY?

#sf21veu



Q&A

Mail:	jasper@packet-foo.com
Web:	blog.packet-foo.com
Twitter:	@packetjay