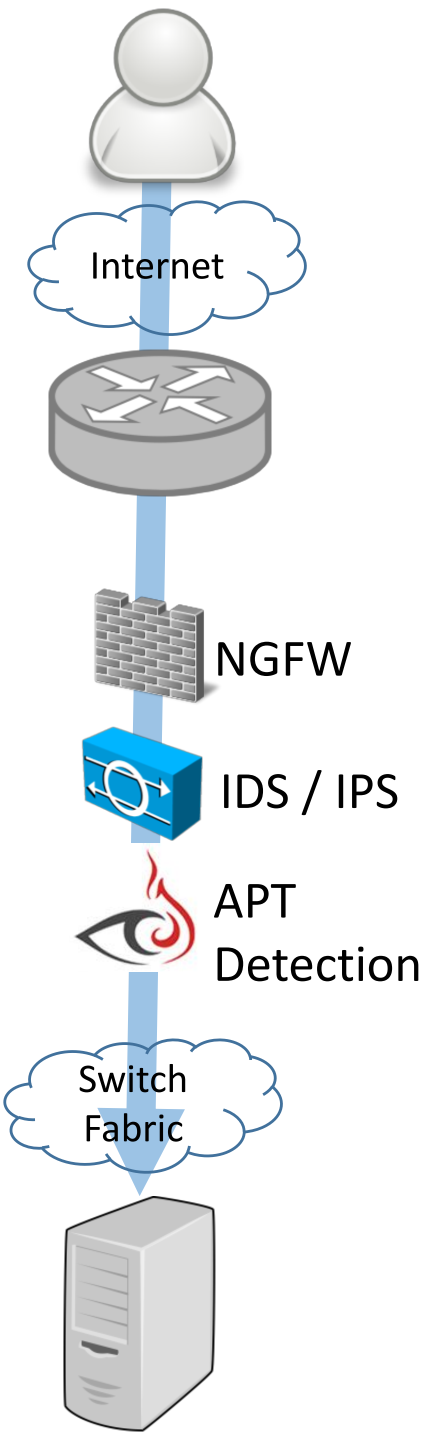
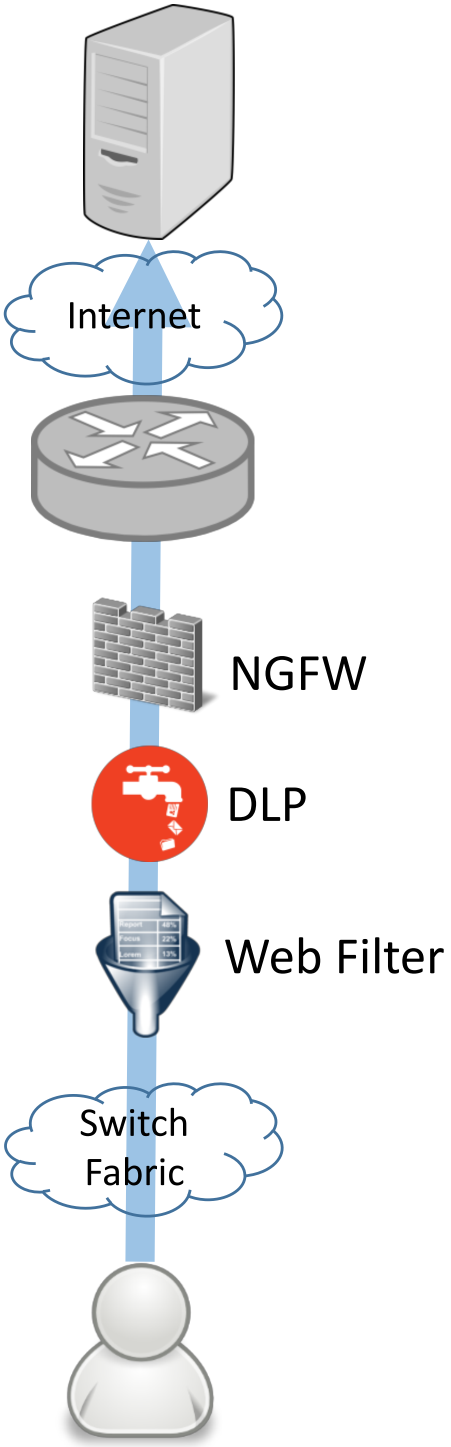
Next-Gen Network Architecture
SSL Everywhere

CURRENT COMMON PRACTICE

Logical Inbound


Internet
NGFW
IDS / IPS
APT Detection
Switch Fabric

Logical Outbound


Internet
NGFW
DLP
Web Filter
Switch Fabric

Limitations

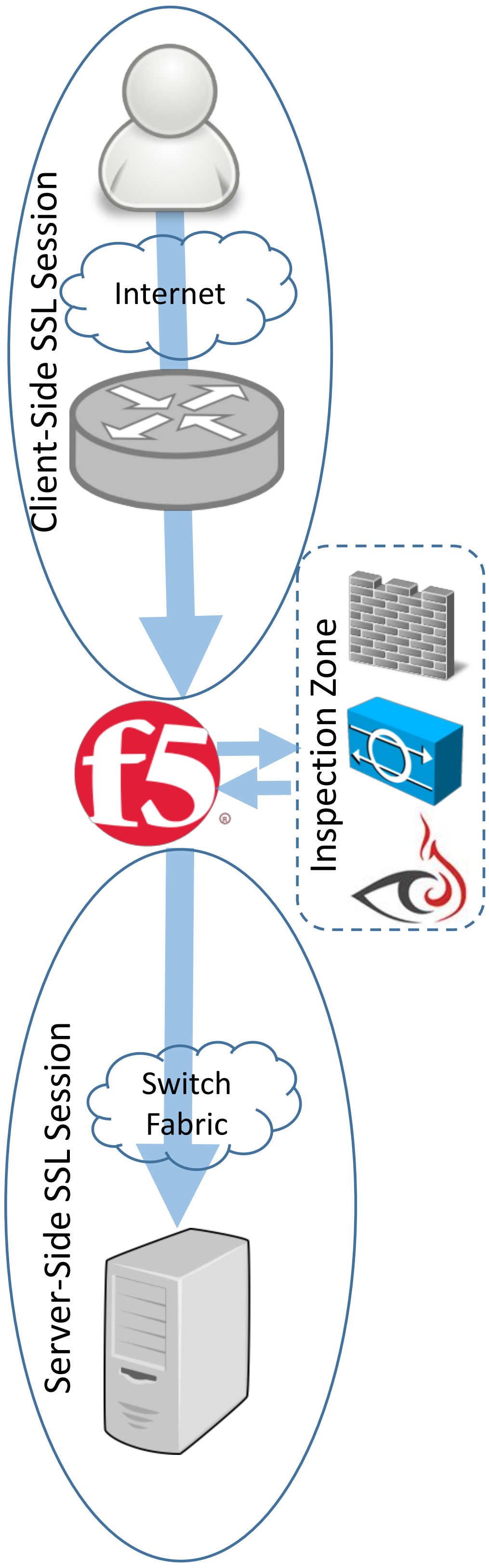
- If inspection devices are performing SSL inspection with a man-in-the-middle (MITM) attack, they are taking a 70-90% performance penalty.
- If inspection devices are not performing SSL inspection, they are blind to 50%+ of the traffic.
- ***TLS 1.3+ will not support MITM inspection.***
- Perfect Forward Secrecy (PFS) does not allow MITM inspection due to Diffie-Hellman use of temporary keys.
- If traffic exceeds inspection device capacity, the device must be forklift upgraded.

Rapid changes in the SSL / TLS landscape are quickly making this architecture obsolete.

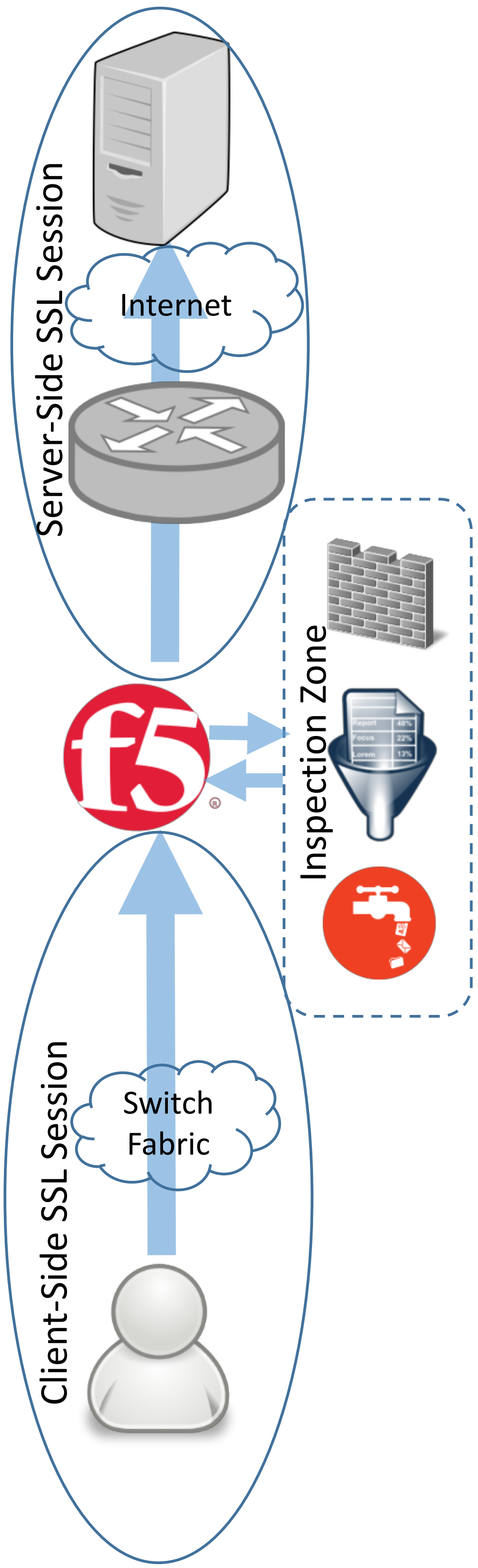
Next-Gen Network Architecture
SSL Everywhere

NEXT-GEN BEST PRACTICE

Logical Inbound



Logical Outbound



Benefits

- Maximum threat mitigation, data protection and AUP enforcement via total traffic visibility.
- User privacy preserved via URL category bypass.
- Scale inspection device performance via load balancing.
  (No more forklifts!)

Why F5?

- Only full-proxy can provide total flexibility with unique client-side vs server-side configuration.
- Best in class SSL / TLS
- PFS fully supported
- ICSA Certified and hardened appliance designed to be exposed to the Internet.
- Future opportunities to consolidate data center services to improve efficiencies.
- Programmability via iRules provides total data-plane flexibility.
- DevCentral User Community
- Free Online Training

Next-Gen Network Architecture
SSL Everywhere

NSS Labs Analyst Brief
"SSL Performance Problems for Next Generation Firewalls"
June 12, 2013

*"Ironically, increased use of SSL in attempt to make our online lives more secure can create **"blind spots"** that can actually **reduce security** on corporate networks because network security products and other defenses may not be able to monitor SSL traffic effectively or efficiently."*

Average SSL performance penalty among 7 NGFW vendors:
- 92.28% TPS decrease (2k ciphers)
- 81% performance decrease (2k ciphers)

NIST Publication
"Developing a Framework to Improve Critical Infrastructure Cybersecurity"
John Kindervag, Forrester Research
April 8, 2013

*"Cybersecurity professionals must stop trusting packets as if they were people. In Zero Trust, **all network traffic is untrusted**."*