Some Thoughts on MPTCP Proxies and Middleboxes

Ed Lopez – elopez@fortinet.com

Prologue

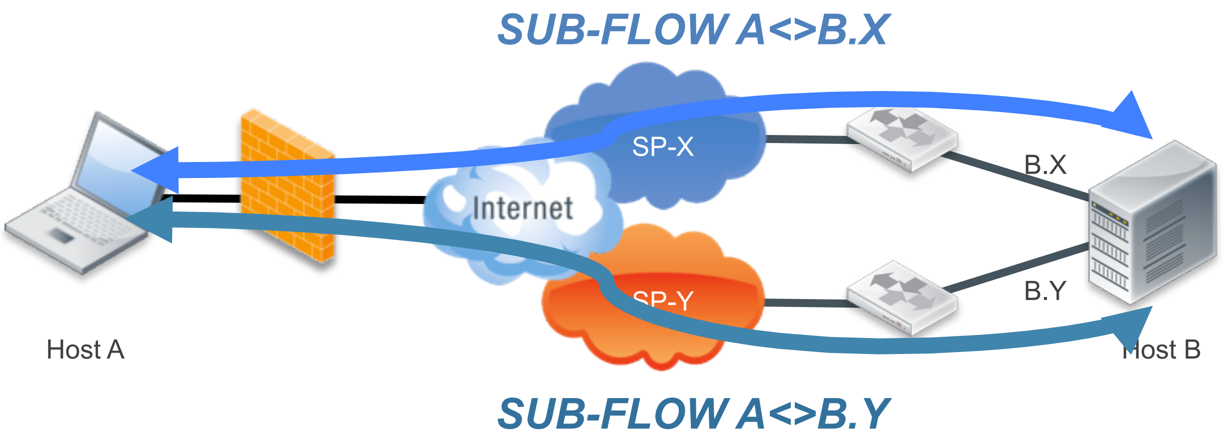
- Middleboxes (and proxies) break the end-to-end principal of Internet architecture
  - Stateful ones force single path architectures
  - Packet transforms, especially by encapsulation, NAT devices and proxies, are particularly problematic
- Unfortunately, middleboxes perform functions essential to their operators, often due to regulation and other non-technical requirements
  - Financial (PCI) and healthcare (HIPPA) compliance are good examples
  - Carrier-grade NAT (CGN) will become a permanent fixture, due to IPv6 mobility requirements
  - Encapsulation is everywhere!
- Much of what I will talk about is noted in 6824, but responses either provide flexibility in MPTCP protocol (i.e. less security), or force fallback to standard TCP
  - This discussion is about how middlebox vendors will actively respond to MPTCP threats over time

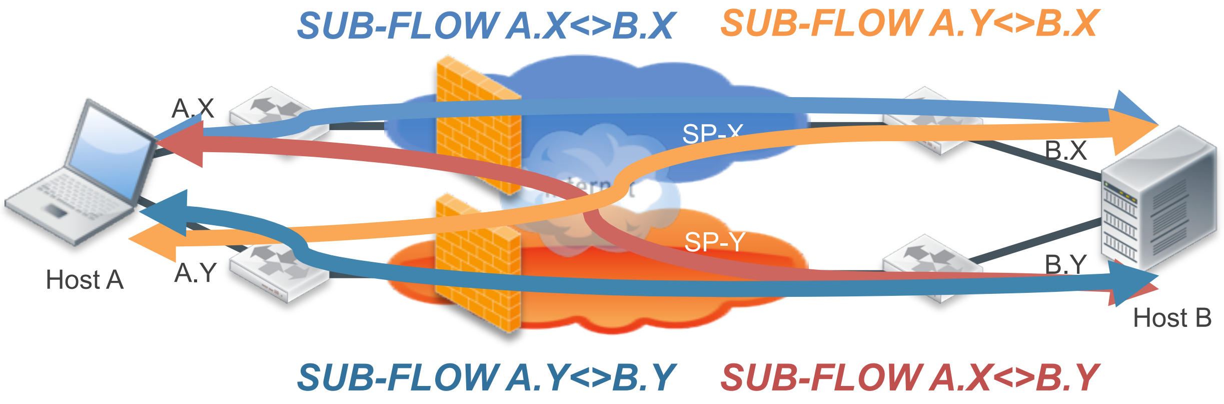
MPTCP Middlebox Issues

- FW/NAT – Will embedded addresses in MPTCP options be properly NAT'd?
  - Especially critical with CGN
- Application Layer Inspection Engines – Are biased to a single session paradigm
  - Engines using protocol decoders (i.e. reassembling traffic in context) will fail because they cannot properly reassemble an MPTCP session
  - Flow-based engines will suffer degradation due to false negatives, due to inability to match patterns in data across multiple sessions
- Proxy services will fail due to improper protocol statefulness
  - Especially transparent ones
- DNS/FQDN inspection solutions will degrade, since path joins occur after resolutions
  - Including DNSSEC
  - MPTCP open to Man-In-The-Middle attacks

MPTCP Middleboxes Issues (cont'd)

- Even if host has single link/path, the single session bias issues are still present
- Across multiple paths, how can application data be meaningfully inspected
- NAT issues abound!





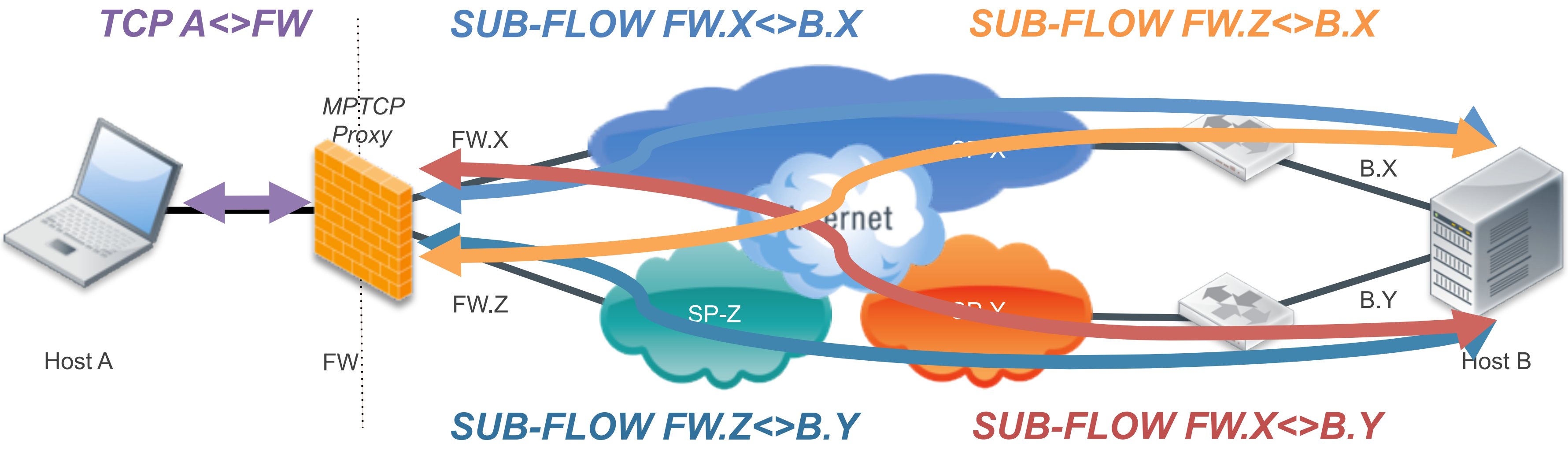
Solutions Middleboxes Will Create

- First, MPTCP will be seen as an attack vector
  - Create option to block the MPTCP options (or unknown TCP options), to force fallback to standard TCP
- DNS/FQDN inspection services (such as web filtering) will probe for sites using MPTCP, and include this information to enforcement devices
  - Better than broad option blocking, allows entities to choose which categories of sites are allowed for MPTCP

Solutions Middleboxes Will Create

- MPTCP application-layer gateway (ALG) capabilities will emerge
  - Ability to detect/inspect MPTCP option values, to look for MITM issues
  - Ability to block/limit undesirable paths
  - Properly translate IP addresses in MPTCP options across NAT devices
- MPTCP proxy devices
  - Initially edge devices, rather than cloud based
  - Path convergence is easier at the edge

Edge MPTCP Proxy



- Multi-path devices front end to user and/or server hosts to converge all MPTCP subflows
- As MPTCP Proxy has access to all subflows, it provides an inspection point
- High-availability and other resiliency mechanisms can be applied to MPTCP proxies

Summary

- The current state of middlebox support for MPTCP will limit its usefulness
- Middlebox creators will actively pursue methodologies to workaround or mitigate functional degradation effects of MPTCP
- Any information in the MPTCP options is subject to inspection and action by middleboxes
- MPTCP proxies will be developed, likely at first on the edge, then followed by cloud/carrier