SatNAG

Satellite **N**etwork **A**dvisory **G**roup

2019

Next Generation Firewall

1. Seamless arbitration of multiple WANs
    a. Load balancing preferred.
    b. Multipath routing preferred.
    c. Preserved institutional IP space preferred.
2. Good visualization of state of affairs of the WAN connections and use. Easy to understand at a glance.
    a. Web UI
3. Programmable API / REST / SNMP for collecting status and usage data
4. Configuration Manageable import / export configuration files
5. LDAP / RADIUS Integrated Authentication
6. Reporting and Querying
7. QoS
    a. FUTURE: QoS best applied at egress, so ship->shore is best done at the ship, shore->ship best done at the shore.
    b. Shaping is better than Policing

Software Defined Wide Area Network (SD-WAN)

- A software-defined approach to managing the wide-area network, or WAN.
- Uses a centralized control function to securely and intelligently direct traffic across the WAN.
  - This allows a single access point to dynamically direct traffic off-ship to whatever connection is available at that moment.
  - This can allow traffic to be aggregated across multiple connections at the same time
    - E.g. traffic can be divided over both HSN and FX at the same time to increase effective bandwidth between ship and shore.

SD-WAN Strategies

Prioritized WAN

Traffic flows over one WAN connection at a time, based on a WAN link status and priority

Overflow

Traffic flows over multiple WAN connections simultaneously, with spillover from one to another if the link becomes saturated.

Load Balancing

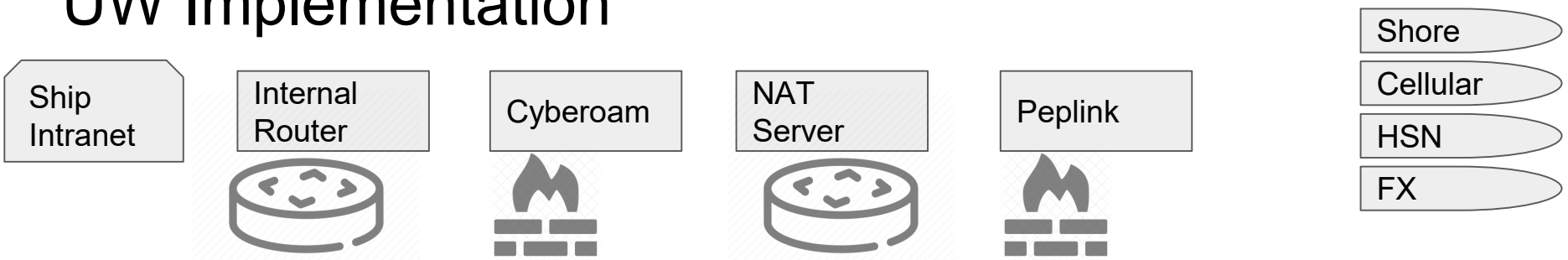
Approaches use dynamic routing and can be:

- Round Robin packets (bad for diverse latency)
- Round robin flows (different WAN used for each traffic flow)

Current Implementation

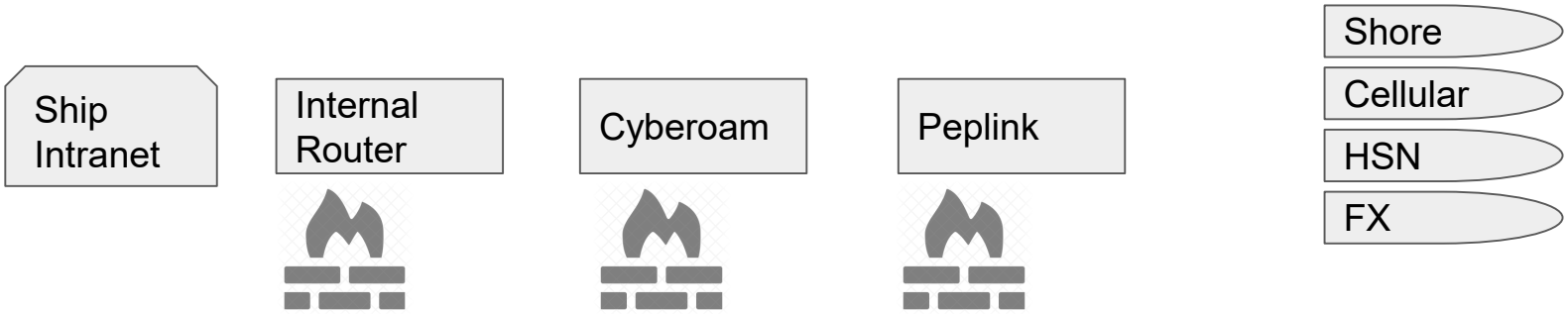
- We are using a combination of Peplink and Cyberoam devices to manage the connections from ship to outside world
  - Currently each institution implements this solution a little differently
- With the next generation firewall solution, SatNAG seeks to combine this functionality into a single device to promote a more unified implementation and more widespread adoption across the UNOLS fleet.
  - Details on the next generation firewall can be found in the Next Generation Firewall presentation

UW Implementation



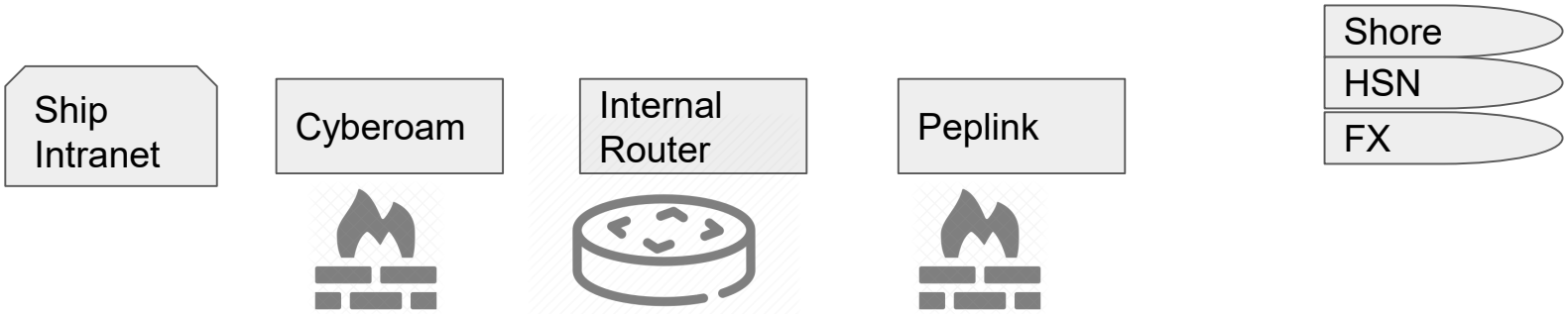
- From internal router all traffic bound for off-ship passes to Cyberoam
- Cyberoam passes traffic out to one of 3 IP addresses on NAT Server:
  - One for HSN only traffic
  - One for FX only traffic
  - One for traffic over best available transport
- NAT Server masquerades internal IP addresses and passes to Peplink
  - Bases masquerade address on which of it's IP addresses received the traffic
  - Does not masquerade externally accessible IP addresses
- Peplink passes traffic to Shore or Cell if available, or if at sea:
  - Sends over HSN and FX, load balanced, based on source address

UAF Implementation



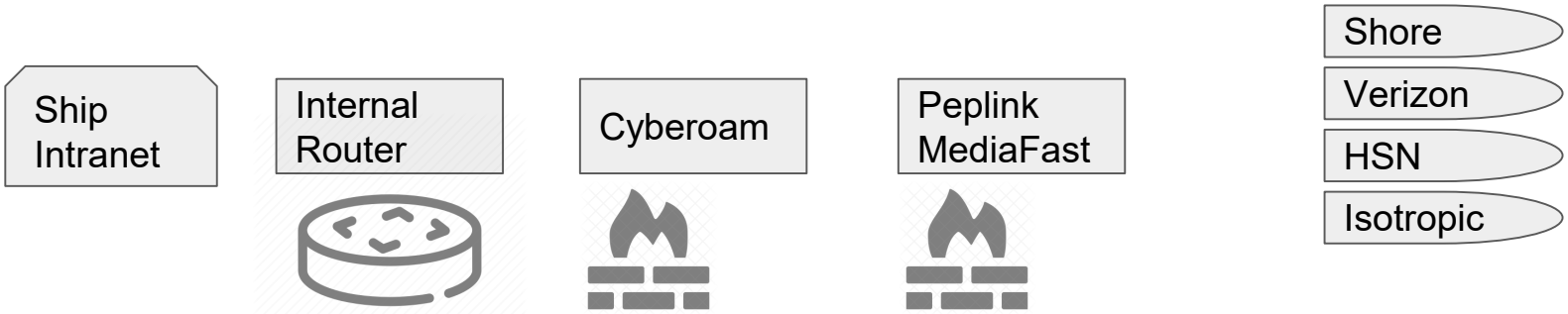
- From internal router all traffic bound for off-ship passes to Cyberoam
- Cyberoam passes traffic to Peplink
- Peplink passes traffic to Shore if available, or if at sea:
  - Sends over HSN and FX based on specific rules
- Uses Weighted Load Balanced SD-WAN

WHOI Implementation



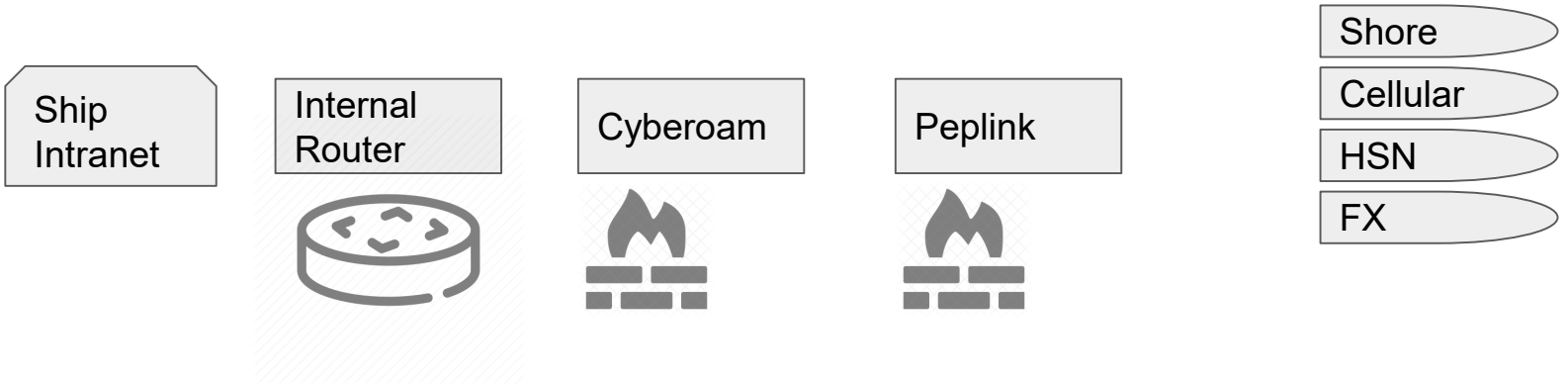
- From internal router all traffic bound for off-ship passes to Cyberoam
- Cyberoam passes traffic to the internal router
- Peplink passes traffic to Shore if available, or if at sea:
  - Sends over HSN and FX based on specific rules

URI Implementation



- From internal router all traffic bound for off-ship passes to Cyberoam
- Cyberoam passes traffic to Peplink
- Peplink passes traffic to Shore if available, or if at sea:
  - Sends over HSN OR Verizon OR Isotropic (whomever we're contracting with)

SIO Implementation



- From internal router all traffic bound for off-ship passes to Cyberoam
- Cyberoam passes traffic to Peplink
- Peplink passes traffic to Shore if available, or if at sea:
  - Sends over HSN and FX based on specific rules

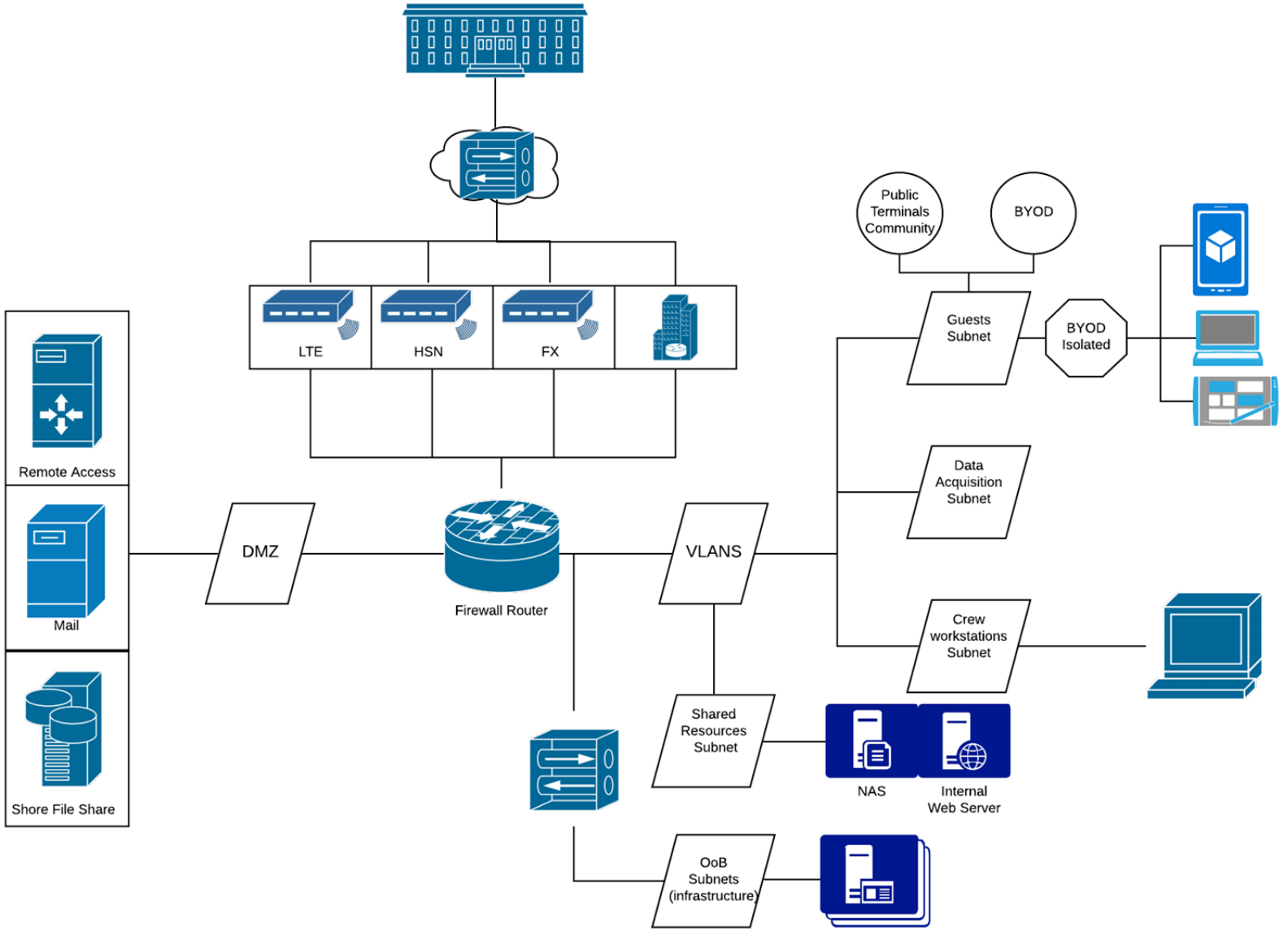
LAN Topology

USCG Safety Alert 06-19
Marine Safety Alert Inspections and Compliance Directorate

https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf

Segment Networks. “Flat” networks allow an adversary to easily maneuver to any system connected to that network. Segment your networks into “subnetworks” to make it harder for an adversary to gain access to essential systems and equipment.

Example WAN LAN Topology

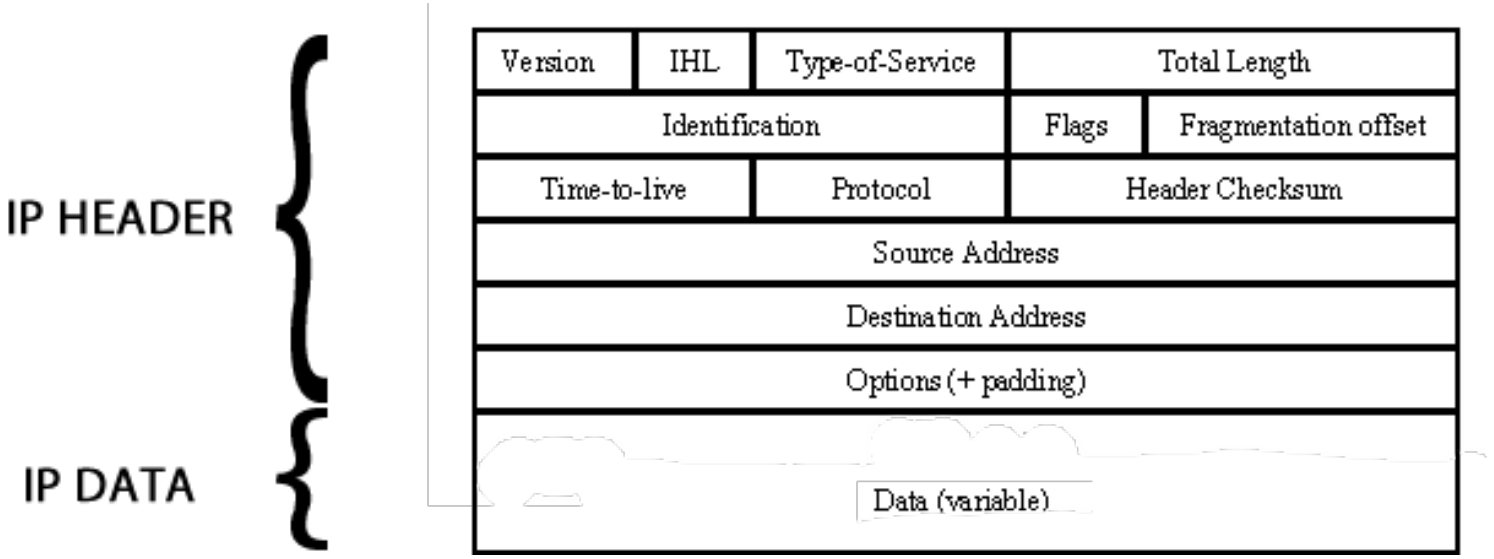


Captive Portal

- Bandwidth Quotas vs QoS Rate Limiting
- Most nextGen are utilizing QoS, will this work on the current bandwidth

Deep Packet Inspection

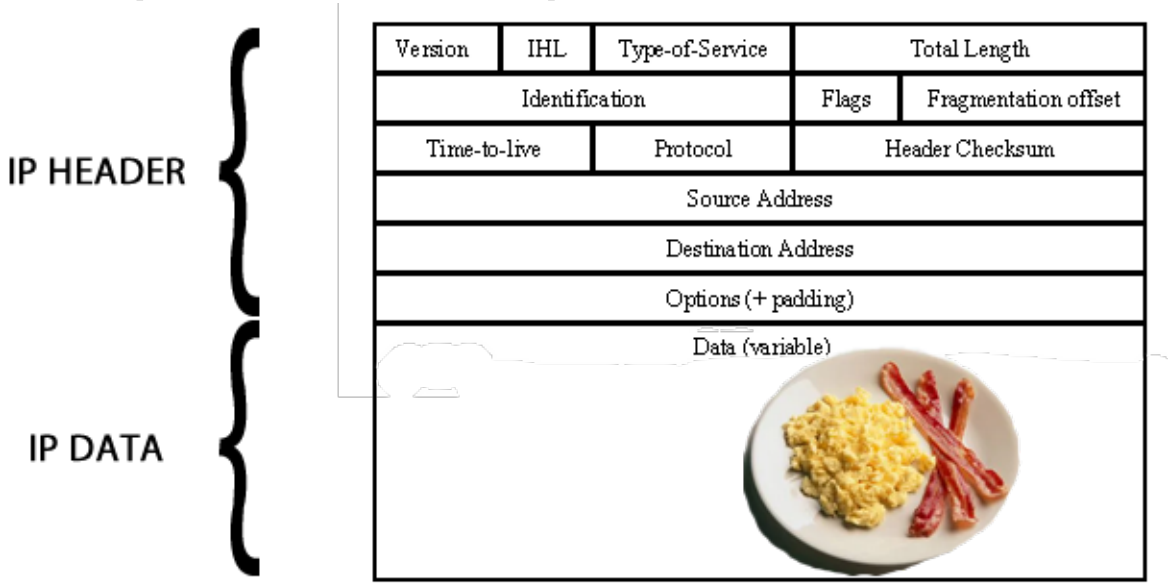
Your basic router operates at layer 3 of the OSI model, meaning the IP information in the packet header is inspected and *routed* accordingly...



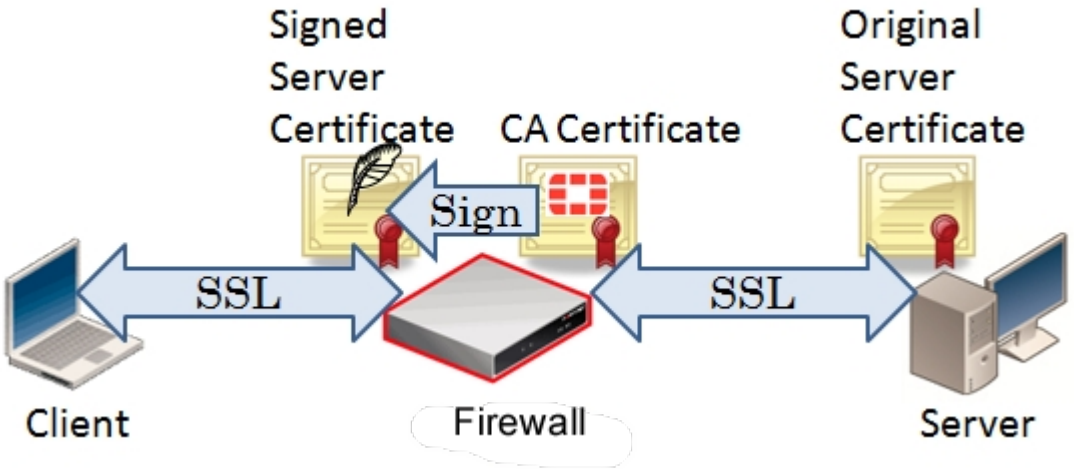
DEEP PACKET INSPECTION, as the name implies, allows the router to inspect the IP data to make routing decisions and perform other higher level functions. Most modern routers and all network security devices perform some level of DPI.

DPI becomes a complicated technical and philosophical issue as encrypted network traffic inches towards 100%.

Deep Packet Inspection



To inspect encrypted traffic the router has to somehow decrypt the IP data. The most common way of doing this is by acting as an SSL Certificate Proxy. This is otherwise known as a ***Man in the Middle*** interception.



Deep Packet Inspection

Implicit trust and installation of root certificates

In practice it becomes a major logistical issue.

- How do you prevent errors on any number of devices, OS'es, browsers, apps, etc. that detect the interception?
- How do you handle devices that don't have a certificate store?
- How do you handle devices which are locked down and won't work with an encryption error?
- Can we be implicitly trusted?
- How does NSF handle this as a larger organization?

PROS	CONS
• Enforce content policy • Cache content on the vessel • Prevent viruses and network intrusion • Route different content/protocols effectively • Better insight into bandwidth usage • More user friendly captive portals	• Logistically complicated • Some cost involved • Some maintenance involved • Some organizations/devices may have issues (NAVY, NOAA, etc)

Other Features

.. Other things we are looking into...

- Metrics Data Mining API
- Lifecycle Device and Firmware Updates
- Link State Aware Firewalls
- Zero Trust Networks

Current State of NextGen FW

An enterprise-grade solution is desired because:

- When it comes to firewalls, you tend to get what you pay for
- A common approach in firewall and technique across the fleet will give better uniformity for what is, in 2019, an expected resource
- Enterprise firewalls have easy-to-set up high-availability options for robust installation of critical infrastructure for Internet.
- Enterprise firewalls have a planned lifecycle that is published and able to be planned around, which is important for working at scale -- EG outfitting the whole fleet could mean 36 firewalls…
- Planned life cycle means that hardware replacement strategy is well defined
- Reliable and accessible vendor support

Decided to proof of concept test 2 vendor solution, Palo Alto and Fortinet to demonstrate all required features.

- Let the facts speak for how best to proceed
- Balance between features, capabilities, performance and cost
- Testing on Armstrong with 820 PA and 2x2Mbps link (Verizon)
- Testing on Sproul with Fortigate 100F

SatNAG DokuWiki

https://satnag.unols.org/

Thank You!

Questions?