Le Montage d'Amour
(2024 Fortigate Project Update)

Rachel Simon, 2024-10-22 09:00-09:20

Community Feedback

@martechmemes

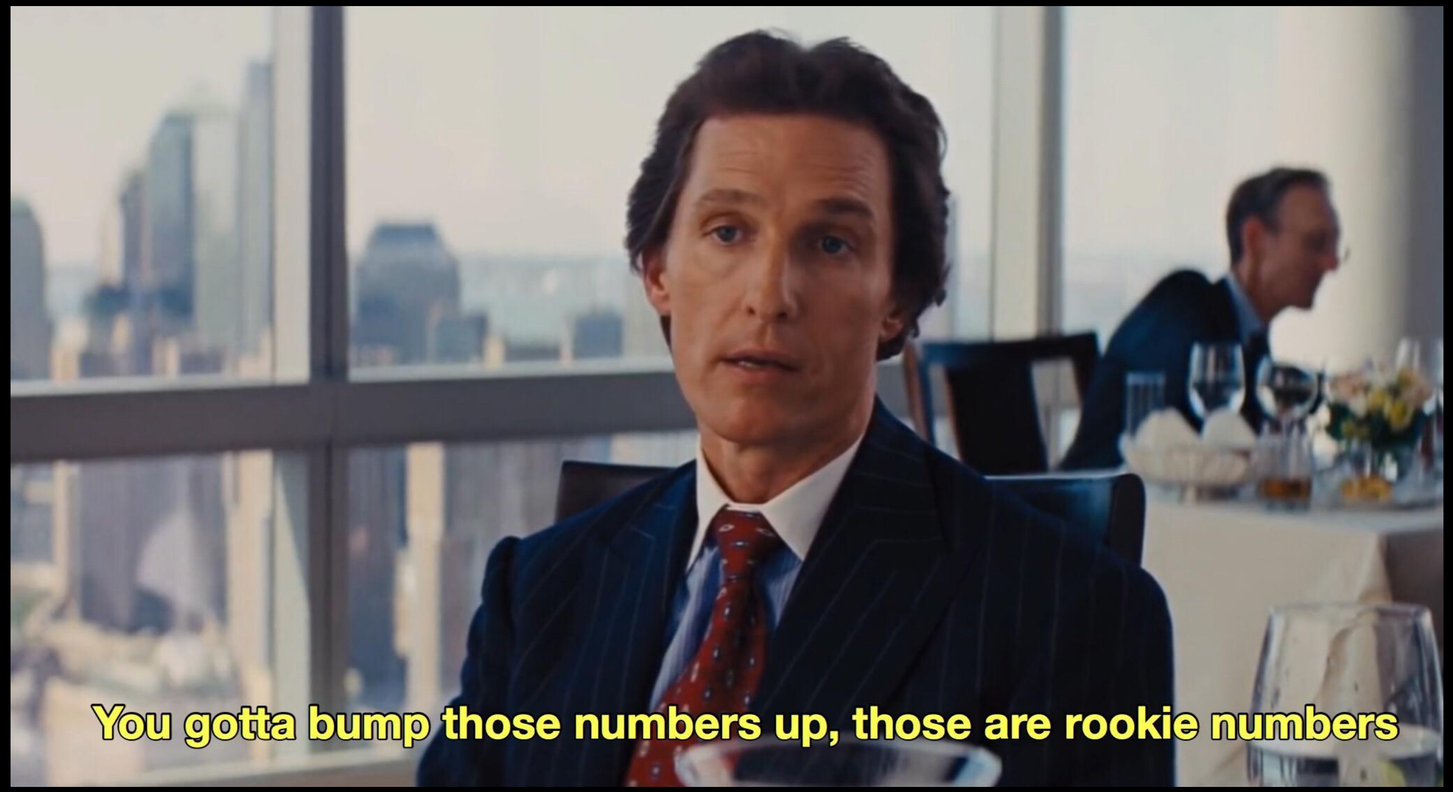
'24 To Date

- Shipboard installations
  - 1 (2023) -> 7 (2024, including 2 non-ARF vessels - Nautilus & Western Flyer)
  - Phone/WhatsApp/Zoom support as needed
- East Coast, West Coast Hub installations
  - East Coast (URI/Kingston Campus)
  - West Coast (SIO/San Diego Supercomputing Center)

'24 To Date, cont'd.

- Training Cruises & Meetings
  - April 2024 - Sikuliaq/SKQ202406T - Fortigate admin training
  - October 2024 - OmniSOC @ URI - Installation process review
  - December 2024 - Endeavor/EN727 - Network training cruise
- Policy & Procedure Development
  - Compromised Device Alerts & Response - Started Dec. 2023
  - Change Management @ The Hubs

'25 style goals



Installation Details

Vessel	Ship LAN?	Ship WAN?	Hub WAN?	Hub FAZ?	Hub FMG?
Endeavor	Yes	Yes	Yes	Yes	Yes
Atlantic Explorer	Yes	Yes	No	Yes	No
Kilo Moana	No	Yes	No	No	No
Thomas G. Thompson	No	Yes	No	No	No
Sikuliaq	Yes	No	No	No	No
(Nautilus)	No	Yes	Yes	No	No
(Western Flyer)	Yes	Yes	No	No	No
TOTAL	4	6	2	2	1

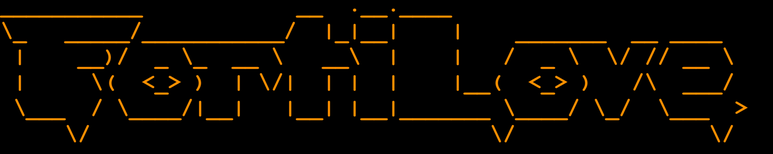
2023
How it started

2024
How it's going

Installation Details, cont'd.

- Peplink replacement (Shipboard WAN) role is common
  - At a minimum, we must duplicate this functionality for local Internet usage
  - On the WAN side, extend this functionality w/ Hub tunnels, application control & SDWAN, and the logging/IDS functionality
- LAN role is less common, but is doable.
  - LAN changes have more ripple effects on servers, etc than WAN
  - Splitting LAN routing/firewall from DHCP/DNS can be a challenge
- Shipboard adoption is moving along, looking for greater usage of hub resources in 2025

Installation Logistics



- Shipboard installation has taken ~1week overall on average
  - Fortigate setup (from factory defaults) takes a few days
  - Cutover takes ~15mins
- Most installations have taken place during port calls
  - 1week out of multi-week port call, not during science mob
  - KM was done offshore, during a STEMSEAS cruise
- These will continue to get easier and easier as the project moves on.
- Staging hardware in advance is helpful, but oftentimes new details come to light when we actually arrive on site.

'24 Technical Items

Core Design

- Hub & Local SDWAN & IPSec tunneling
  - Plenty of troubleshooting here...
  - Endeavor -> Hub is easy, Nautilus -> Hub less so (lots of lessons learned)
- Hub & Local Traffic shaping
  - Upload always on ship
  - Download usually at hub, with failsafe local policies.
- Logging Setup -> OmniSOC
- Remote access & campus routing via the Hub (working on IPSec auth options for remote access VPN)

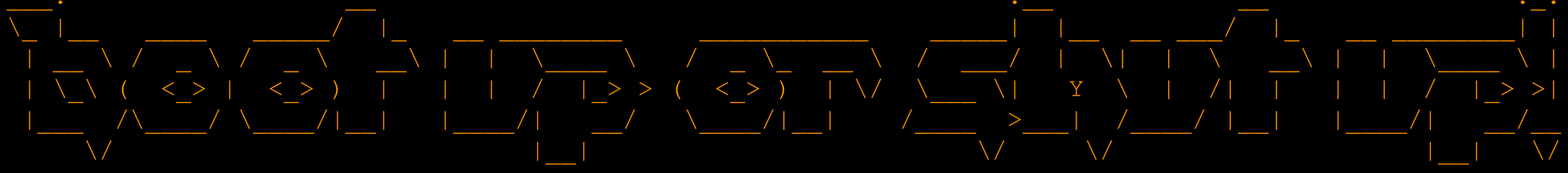
"Cookbook"

- Quota (fourdquota)
  - Hard cutoff - IP bans
  - Soft cutoff - throttle
- Address Object Management
  - fourdaddress
  - dnsmasq, csv, ip ranges as sources
- Captive Portal
  - LDAP
  - Sikuliaq MFP->AD import

Goals for '25

- Continue lighting up new vessels
- Greater usage of hub resources
  - Tunneled Internet access (traffic shaping, remote access options)
  - Hub log managment -> OmniSOC pipeline
  - Hub config management
- Fortigate vessel user community, mailing list updates, knowledgebase
- More training cruises
- Keeping this project in the news - this project moves fast and many things will change between RVTECs.

What's next?



arf-firewall-team@unols.org