The FortiReckoning

Endeavor Trials +
Future Development

Erich Gruebel, Laura Stolp, Rachel Simon

Fortigate 61F Installed in August 2023

- Dove (dived) in with both feet. Fortigate is both the firewall and network core
- HA pair
- DNS relay + DHCP server

Favorable Schedule:

- 14 day inport followed by a few short duration local cruises

Favorable Location:

- Close to Laura, Rachel, Erich
- Beautiful scenic Narragansett RI
    - “The Gem of New England”

Low Risk:

- Relatively simple medium ship network
- Very little *Operational Technology* (OT)

2 Step Process

Phase I -

- Drop-in replacement for Peplink. *Barebones* firewall and basic services
- Done in Aug. 2023

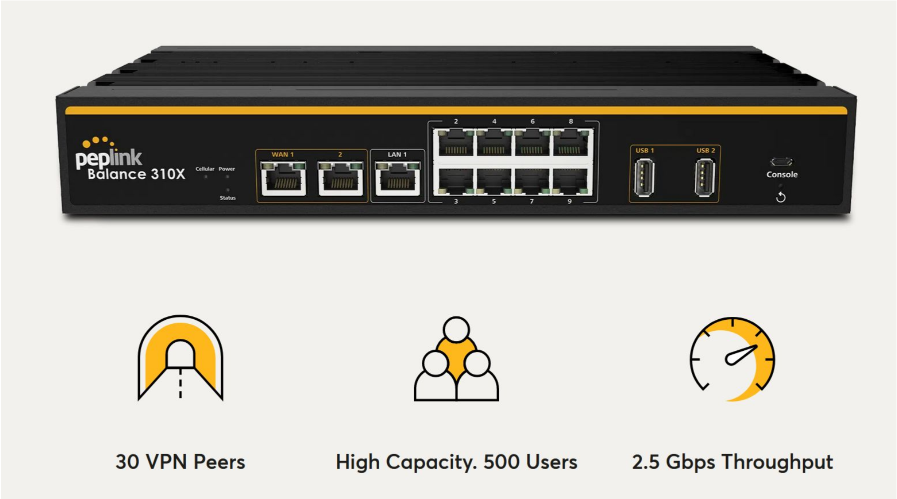
Phase II -

- Traffic routed through the HUB
- Management moved to FortiManager, ashore
- Done last week

Concerns

Replacing a Peplink Balance 310X HA pair

- Tried and true firewall
- Designed for Maritime
- PepVPN is amazing
- Captive portal was *usable*



Had high hopes for Sophos XG that never panned out

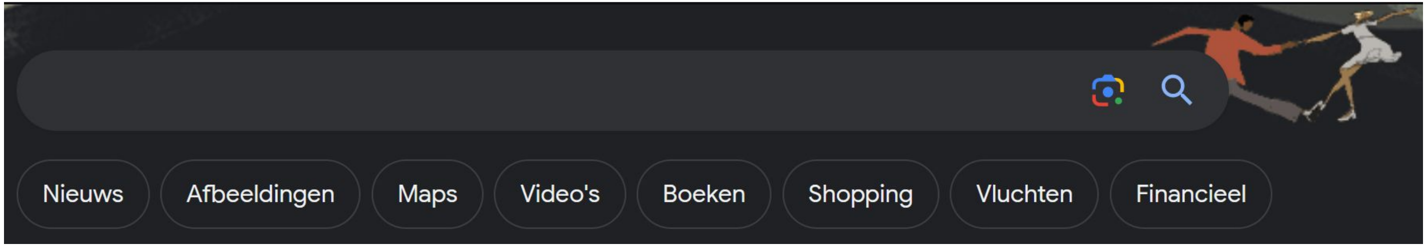
Concerns

Nagging Issues

- No solid fixed IP for remote access

- Foreign Public IP Addresses
    - Geofencing of services
    - Tailored search results for other countries

- Authentication for URI VPN was hit or miss



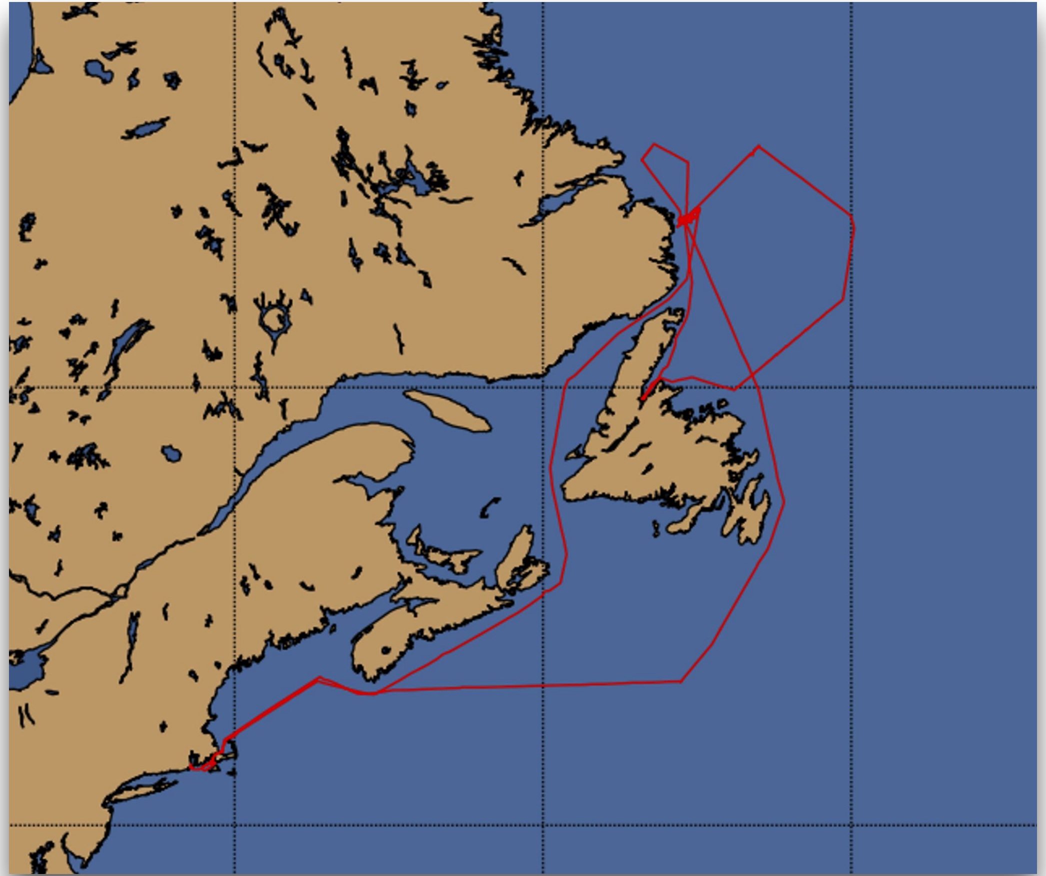
Phase I Results

Very Impressed!

- Fortigate handles WAN balancing *better* than Peplink
- Identification and blocking of problem users is manageable (not great)
- 28 day cruise from Woods Hole to Labrador Sea without a single connectivity issue

The result of two factors

- Adequate bandwidth and dual independent VSATs. Hiseasnet, NSF, & ONR
- Solid firewall, solid network engineering, and lots of homework



Still To-Do for Phase II

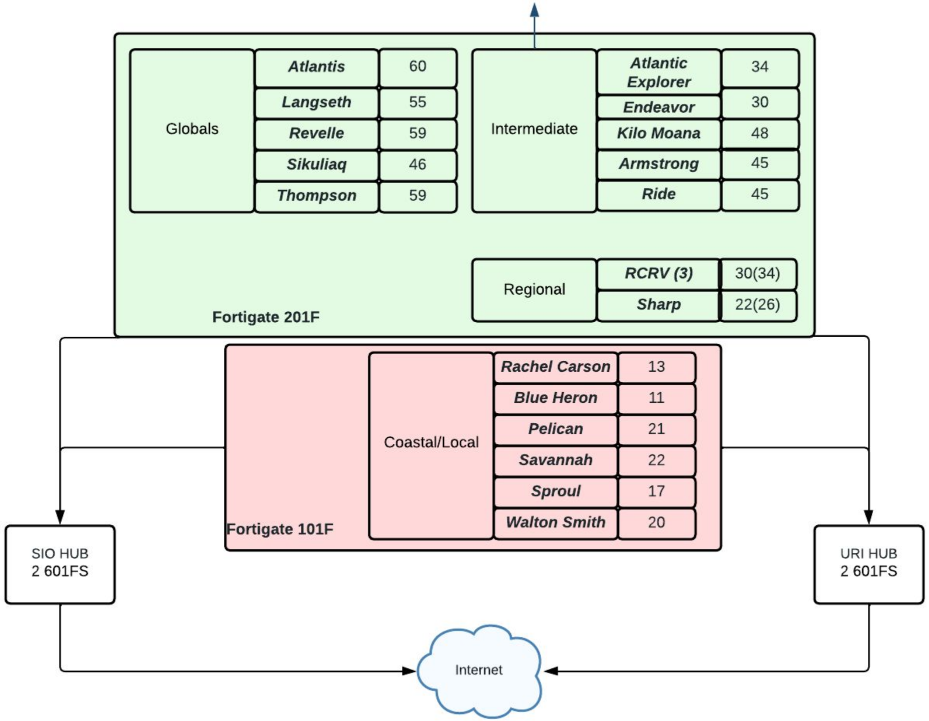
Sea Trials for Hub Architecture

- Nov. 2nd, 5 days after RVTEC
- Our main POC will be out to sea

Get Log Data Flowing to OmniSOC

Trials for shore based Fortimanager

- There’s going to be some pain but the positives outweigh the negatives



Fortigate 201F

Globals		
	Atlantis	60
	Langseth	55
	Revelle	59
	Sikuliaq	46
	Thompson	59

Intermediate		
	Atlantic Explorer	34
	Endeavor	30
	Kilo Moana	48
	Armstrong	45
	Ride	45

Regional		
	RCRV (3)	30(34)
	Sharp	22(26)

Fortigate 101F

Coastal/Local		
	Rachel Carson	13
	Blue Heron	11
	Pelican	21
	Savannah	22
	Sproul	17
	Walton Smith	20

Looking for Early Adopters

- Shore HUBS are on order - hope to be up and running by the end of 2023
- Ship Fortigates have been ordered for the early buy-inners
- Come talk to SatNAG or Hiseasnet people if you are interested in getting involved.

Future Development

Long-Term Support

This is a complex system and there’s a lot of room for growth

There’s routine and corrective maintenance that needs to be addressed

Great topic to approach as a fleet

Still a lot of discussion about what support would and should look like

Future Development

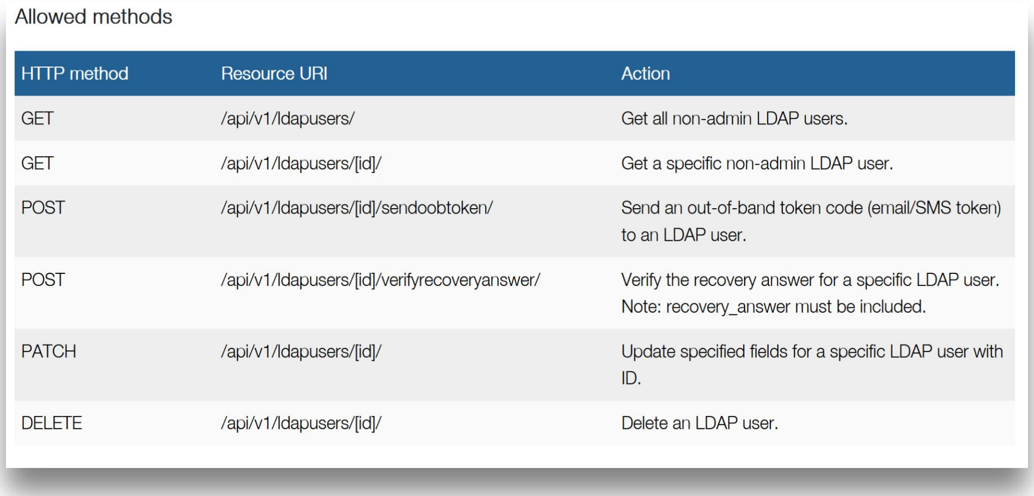
FortiOS REST API Tools

Robust user base and libraries

Quickly identify problem users

Block and unblock with ease

Custom dashboards and displays for self-monitoring



Allowed methods

HTTP method	Resource URI	Action
GET	/api/v1/ldapusers/	Get all non-admin LDAP users.
GET	/api/v1/ldapusers/[id]/	Get a specific non-admin LDAP user.
POST	/api/v1/ldapusers/[id]/sendoobtoken/	Send an out-of-band token code (email/SMS token) to an LDAP user.
POST	/api/v1/ldapusers/[id]/verifyrecoveryanswer/	Verify the recovery answer for a specific LDAP user. Note: recovery_answer must be included.
PATCH	/api/v1/ldapusers/[id]/	Update specified fields for a specific LDAP user with ID.
DELETE	/api/v1/ldapusers/[id]/	Delete an LDAP user.

Future Development

Directory Service

Regarding Common Vulnerabilities:
“The use of default administrator accounts and passwords”

Procedural Protective Measures 7.3:
“User accounts should not be passed on from one user to the next using generic usernames”

This is a challenging problem with consideration of all of the edge cases of RV operations

- Permanent crew, visiting scientists, vendors, guests
- IT and OT in the same environment
- Multi-institution machines and users
- On and on and on….very challenging environment

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

Produced and supported by

BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC)

Future Development

Directory Service…the Dream

Holistic User Management

Pre-Cruise

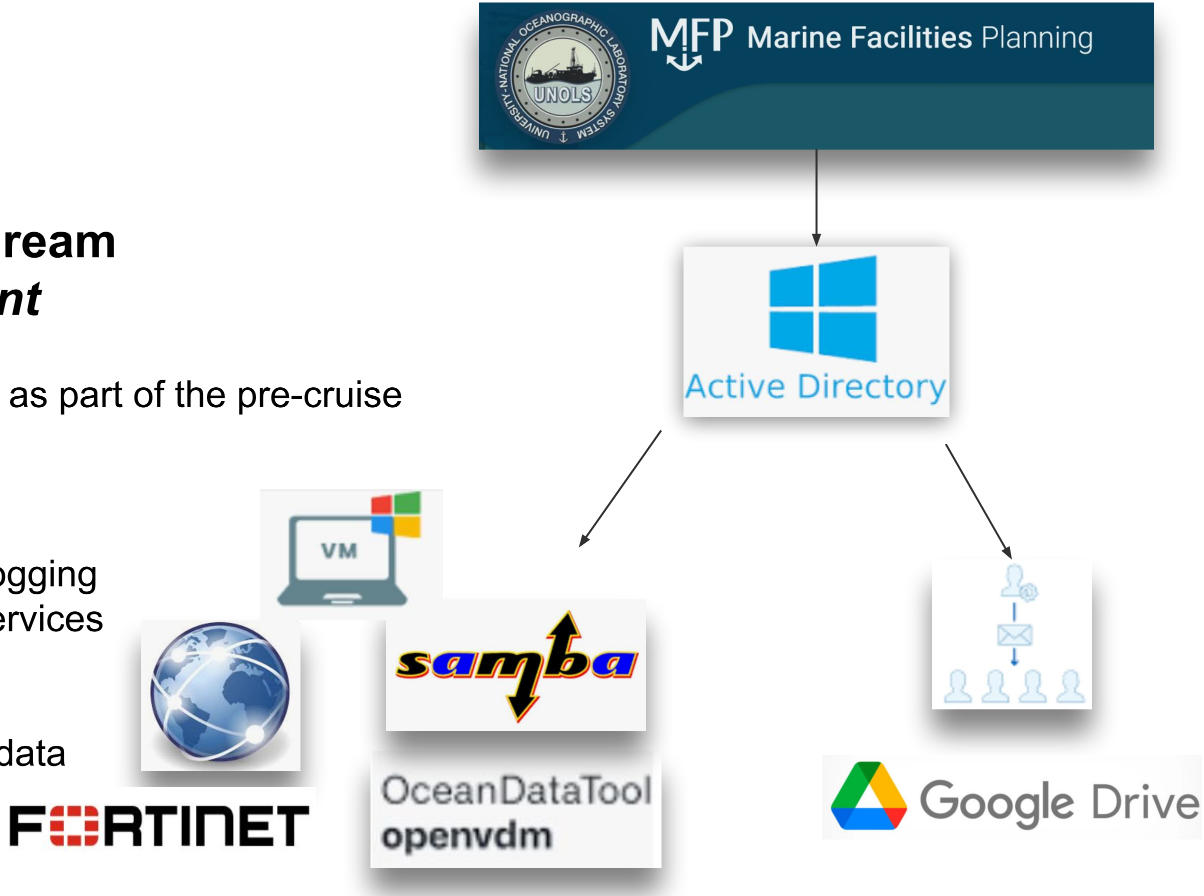
- User onboarding automated as part of the pre-cruise planning

During Cruise

- Reliable user tracking and logging
- SSO access to shipboard services

Post-Cruise

- Controlled access to cruise data
- Long-term communication



Questions?

Thoughts?

Suggestions?