The FortiReckoning

System Design (The Nitty Gritty)

Project-defining valuable insight from the Marine Tech Community

@MARTECH_MEMES
ME PRETENDING TO TROUBLESHOOT WHY YOU CAN'T INTERNET
*I know why, It's just not my job to fix your crusty lap
imgflip.com

The official Ivory Tower rebuttal

```
configure martech-memes-rebuttal
```

```
edit
"portlandia_references_hit_differ
ent_when_RVTEC_isnt_in_the_PNW"
```

DUNKING ON CYBERINFRASTRUCURE PRESENTATIONS AT RVTEC?
STRAIGHT TO 8KBPS BIDIRECTIONAL TRAFFIC SHAPER
imgflip.com

```
next
```

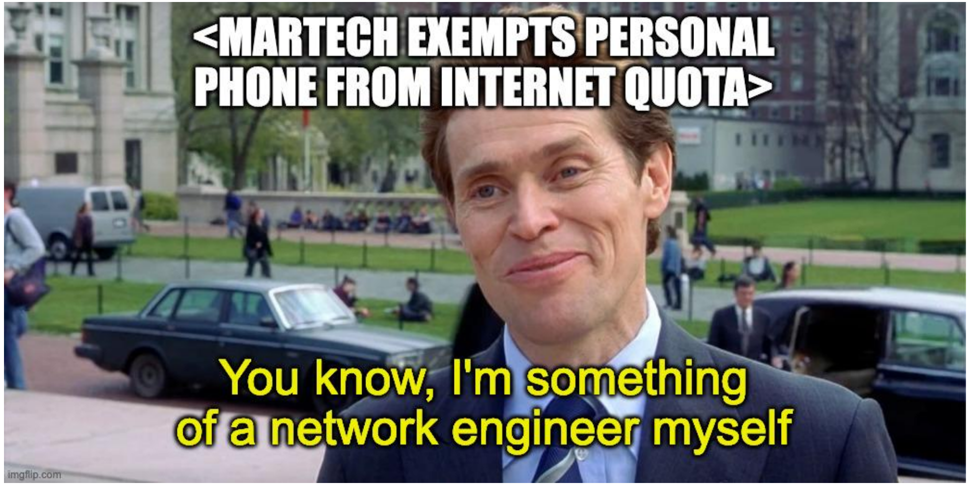
```
edit "ok-boomer-chiefsci"
```

ChiefSci Laptop
50 Tabs
The Official Cruise WhatsApp
The Cruise WhatsApp, but only cool people
Google Drive
GMRT but the entire known universe
Microsoft Teams

```
next
```

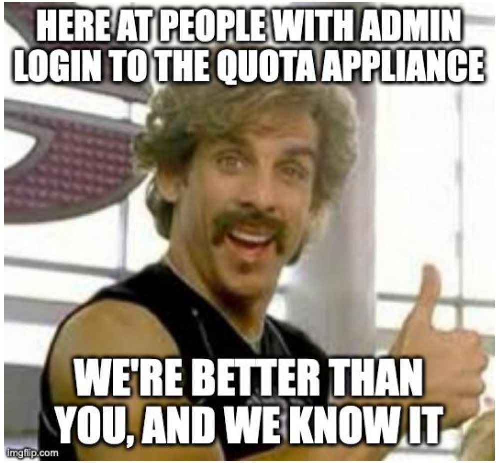
The official Ivory Tower rebuttal (that just finished buffering...)

edit "diss_track_line3_CORRECTED.all"


<MARTECH EXEMPTS PERSONAL PHONE FROM INTERNET QUOTA>
You know, I'm something of a network engineer myself
imgflip.com

next

edit "diss_track_line3_CORRECTED_FINAL.all"


HERE AT PEOPLE WITH ADMIN LOGIN TO THE QUOTA APPLIANCE
WE'RE BETTER THAN YOU, AND WE KNOW IT
imgflip.com

next
end

What, exactly, are we presenting?

- Reusable reference Fortigate-based network architecture for research vessels
  - Management of onboard networks
  - Management of different Internet connections (VSAT, Starlink, 5G modems, Shorelink, etc)
  - Connection back to the home institution
  - Hooks into big-picture cyberinfrastructure projects (OmniSOC)
- Installation process
  - Ability to install Fortigates without major changes onboard (no changing IP addresses…)
  - Data collection spreadsheets, installation scripts, procedures
  - Ability to install with minimal downtime, Endeavor cutover done with <15 mins of network downtime
- Support resources
  - Troubleshooting procedures
  - Cruise rollover procedures
  - New device procedures

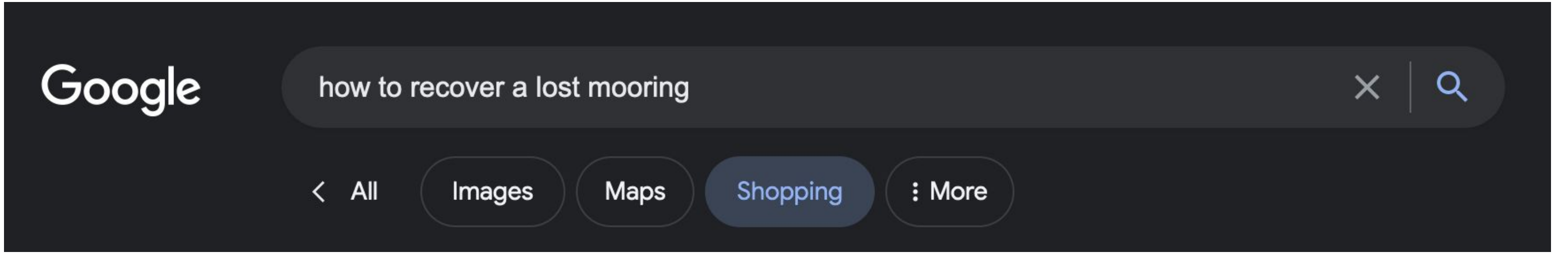
The FortiReckoning

System Design (The Nitty Gritty)

Chapter 1: The Nickel Tour

Internet

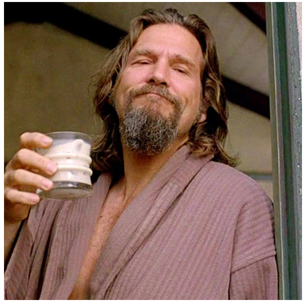
(Hub Forti,
Host Inst.)



how to recover a lost mooring

Ship->Hub

(Ship Forti,
Hub Forti)



< Pacific
(Preferred)

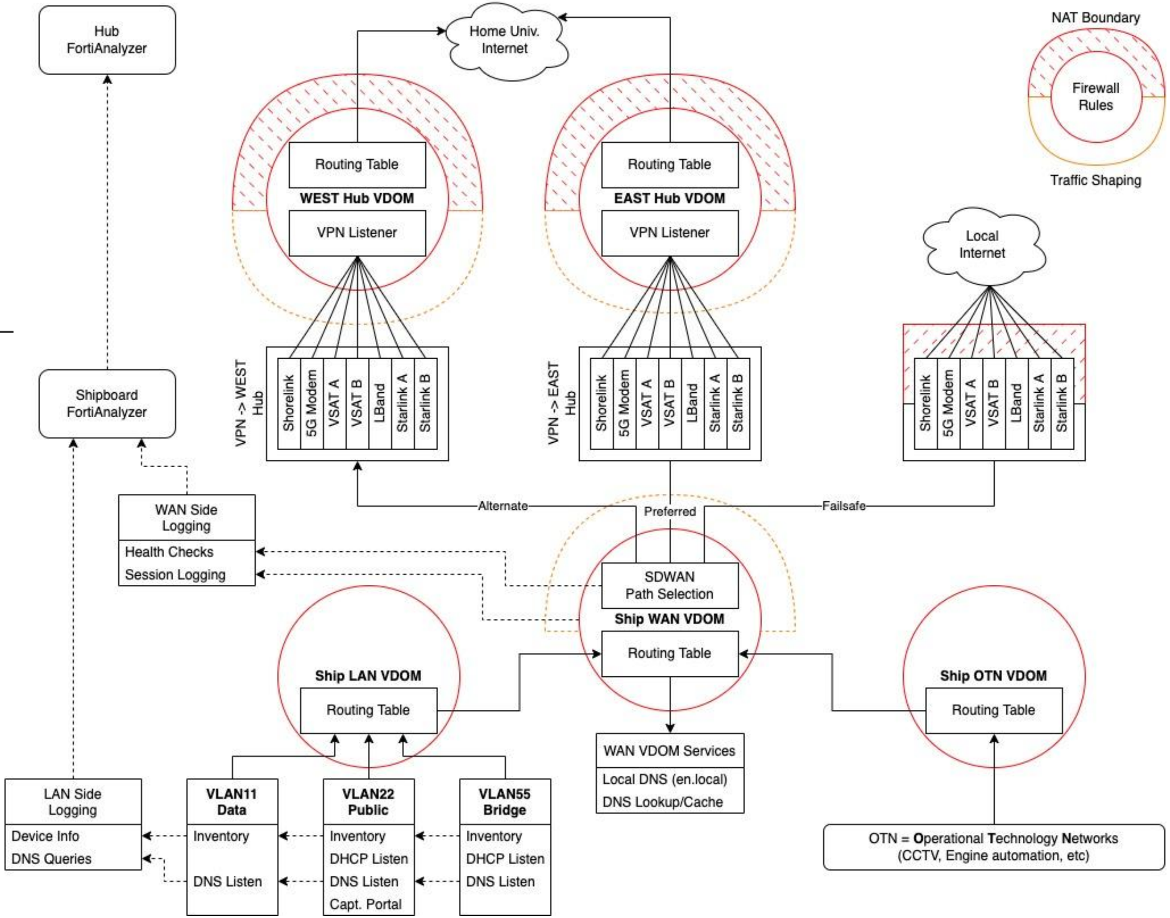
Atlantic >
(Preferred)

Onboard
Network

(Ship Forti)

^ VPN Tunnel to the Hubs ^

Fortigate VDOM's in the ship's traffic flow: GOTTA CATCH 'EM ALL!



Hub FortiAnalyzer

Home Univ. Internet

NAT Boundary

Firewall Rules

Traffic Shaping

Routing Table

WEST Hub VDOM

VPN Listener

Routing Table

EAST Hub VDOM

VPN Listener

Local Internet

VPN -> WEST Hub

Shorelink
5G Modem
VSAT A
VSAT B
LBand
Starlink A
Starlink B

VPN -> EAST Hub

Shorelink
5G Modem
VSAT A
VSAT B
LBand
Starlink A
Starlink B

Shorelink
5G Modem
VSAT A
VSAT B
LBand
Starlink A
Starlink B

Shipboard FortiAnalyzer

Alternate

Preferred

Failsafe

WAN Side Logging
Health Checks
Session Logging

SDWAN Path Selection

Ship WAN VDOM

Routing Table

Ship LAN VDOM

Routing Table

Ship OTN VDOM

Routing Table

WAN VDOM Services
Local DNS (en.local)
DNS Lookup/Cache

LAN Side Logging
Device Info
DNS Queries

VLAN11 Data
Inventory
DNS Listen

VLAN22 Public
Inventory
DHCP Listen
DNS Listen
Capt. Portal

VLAN55 Bridge
Inventory
DHCP Listen
DNS Listen

OTN = **O**perational **T**echnology **N**etworks
(CCTV, Engine automation, etc)

NSF, ONR, ARF CIWG, UNOLS, SatNAG, HiSeasNet, ResearchSOC

How do we build this: Device Config

- Onboard redundant systems
- Why Virtualization?
- Virtual LANs (VLANs) & Virtual Domains (VDOMs) & Virtual Private Networks (VPNs)
- Administrative Domains (ADOMs)
- How the virtualized layers fit together
- Basic Network Services (DHCP, DNS)
- Device Inventory & Username Capture
- Getting Online
  - SDWAN
  - "Local" Internet (directly on the ship)
  - Hub Internet and Tunneling
- Firewall Objects & Rules

How do we build this: Traffic Flow

- Device Config is what it is to get the ship's onboard networks and Internet connections up and running. However, the "policy" side of the house is more abstract, and is flexible enough so that rules can be written based upon usage.
- Policy statements are based upon objects and groups, and these can be set up to represent how the ship actually operates, not based upon config files.
- What are the tools available to direct traffic flow?
  - Firewall Rules
  - SDWAN
  - Traffic Shaping
- How can we solve some practical problems with these?

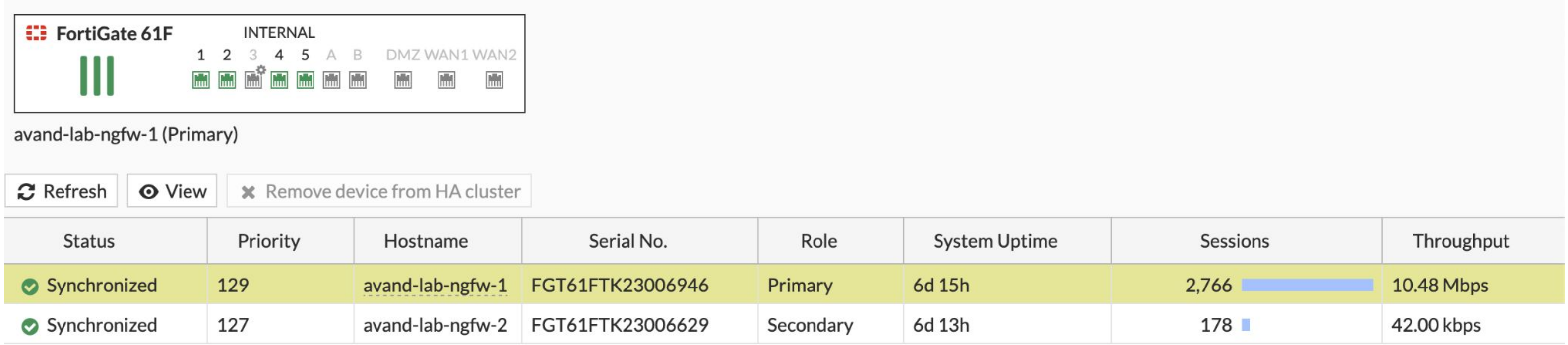
The FortiReckoning

System Design (The Nitty Gritty)

Chapter 2: Configuration

2.1: Onboard HA

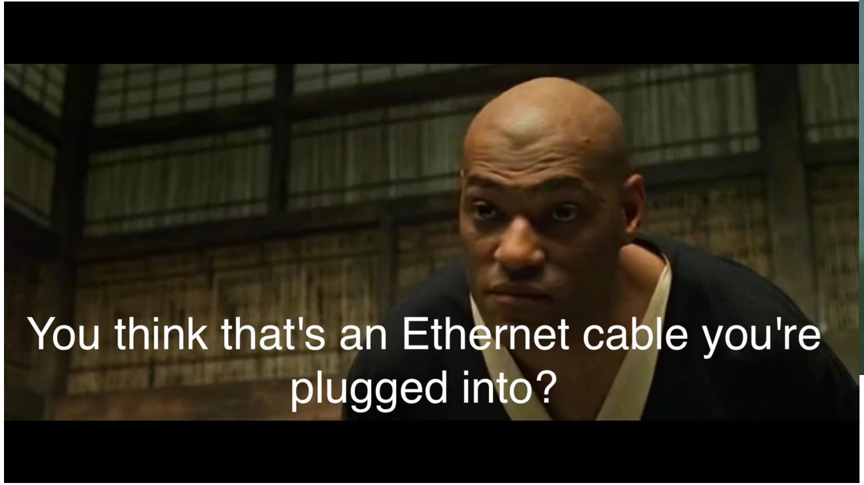
- Ship Fortigate pair operates as a HA cluster
  - Both units online at the same time and linked together. Config auto-synced.
  - **Active-Passive mode**: One unit carries all traffic flow until failure, then secondary unit takes over
  - Active-Active mode: Both units carry half the traffic in normal operation. In the event of a failure, one unit will carry all traffic



avand-lab-ngfw-1 (Primary)

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
✓ Synchronized	129	avand-lab-ngfw-1	FGT61FTK23006946	Primary	6d 15h	2,766	10.48 Mbps
✓ Synchronized	127	avand-lab-ngfw-2	FGT61FTK23006629	Secondary	6d 13h	178	42.00 kbps

2.2: Virtualization



2.2: Virtualization - VLAN/VDOM/VPN

- VLANs & VDOMs
  - Both of these are key components of the reference implementation
  - Requires some setup during commissioning but makes long-term operation and changes simpler.
- VLANs - separate a physical ethernet switch into isolated, logical segments
  - VLAN-enabled switches & wifi access points (and other network/IT devices) are connected together with trunk ports
  - Separates a switch layout into different onboard (data, public, etc) and WAN (vsat, starlink, cell) networks.
- VDOMs - separate a router into isolated, logical segments
  - LAN side of router = basic services to run network (DHCP, DNS), onboard net rules, get Internet from WAN Side
  - WAN side of router = Different internet connections, rules to select conn, "clean copy" of Internet traffic

2.2: Virtualization - VLAN/VDOM/VPN, cont'd.

- VPN's
  - Traffic across "normal" Internet (not leased-lines) requires routable IP addresses (to go between ISP's)
  - The private IP ranges we use onboard (10.x.x.x, 172.16-32.x.x, 192.168.x.x) are by definition not routable. VPN's create a tunnel that can bring non-publicly-routable IP's across the Internet, without requiring leased lines (MPLS, Metro Ethernet and their country-club friends)
- Why are we doing all of this?
  - The big picture for this project is the Fortigate traffic flow rules. However, to get the point where we can write really simple, reality-based rules for the Fortigate, we need to set up some "baffles" so that traffic flows in the best way possible.
  - Just as one wouldn't direct-drive a dentist's drill with a large-bore EMD diesel, some of these config items are necessary adaptations for templating purposes, and to simplify writing rules later on.

2.2.1 Core Switches & VLANs 101

- Physical only switching
  - Each separate network = separate (chain) of switches
  - Ever expanding daisy chains of switches
  - Easy to initially install
  - Lots of cabling required
  - Vulnerable to loops + UDP broadcast storms
- VLAN Based, Core + Access switches
  - Initial config needed
  - Can reuse cabling as new networks are added (VLAN trunk ports)
  - Protection against loops + UDP storms (spanning-tree)
- Note that core + access layer switching is not unique to the Fortigate project…

2.2.2 VDOM 101

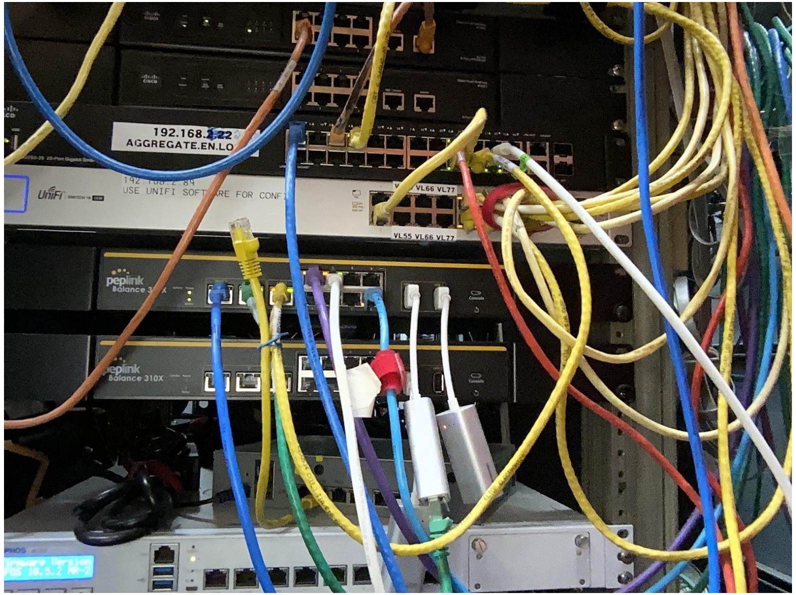
LAN VDOM

- **Focused on keeping onboard networks running (IP's, DHCP, DNS)**
- Has mix of onboard + Internet traffic
- Sees single Internet connection from WAN VDOM
- Different ships have different number of onboard networks
- Not concerned with traffic shaping onboard. Allow/deny rules only.
- **Largely unique to each ship.**

WAN VDOM

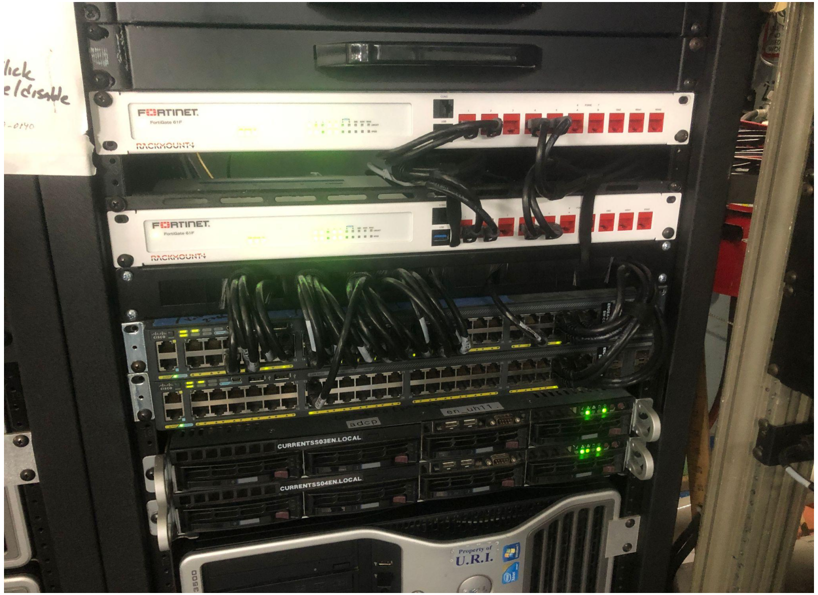
- **Focused on providing best-possible Internet to arbitrary number of onboard networks**
- "Clean Copy" of only Internet traffic. Logical place to track device usage.
- Sees single connection to arbitrary number of onboard networks.
- Can allow/block/prioritize/throttle Internet to device regardless of what network it's only
- **Many similarities across ships.**

- *Although lan/wan VDOMs are focused on different tasks, they are able to share the same physical hw.*
- *LAN VDOM is largely ship-specific*
- *WAN VDOM is largely reusable*



Purely physical network

- Less up-front config
- More complexity long-term



VDOM & VLAN-based network

- More config up-front
- Less complexity long-term

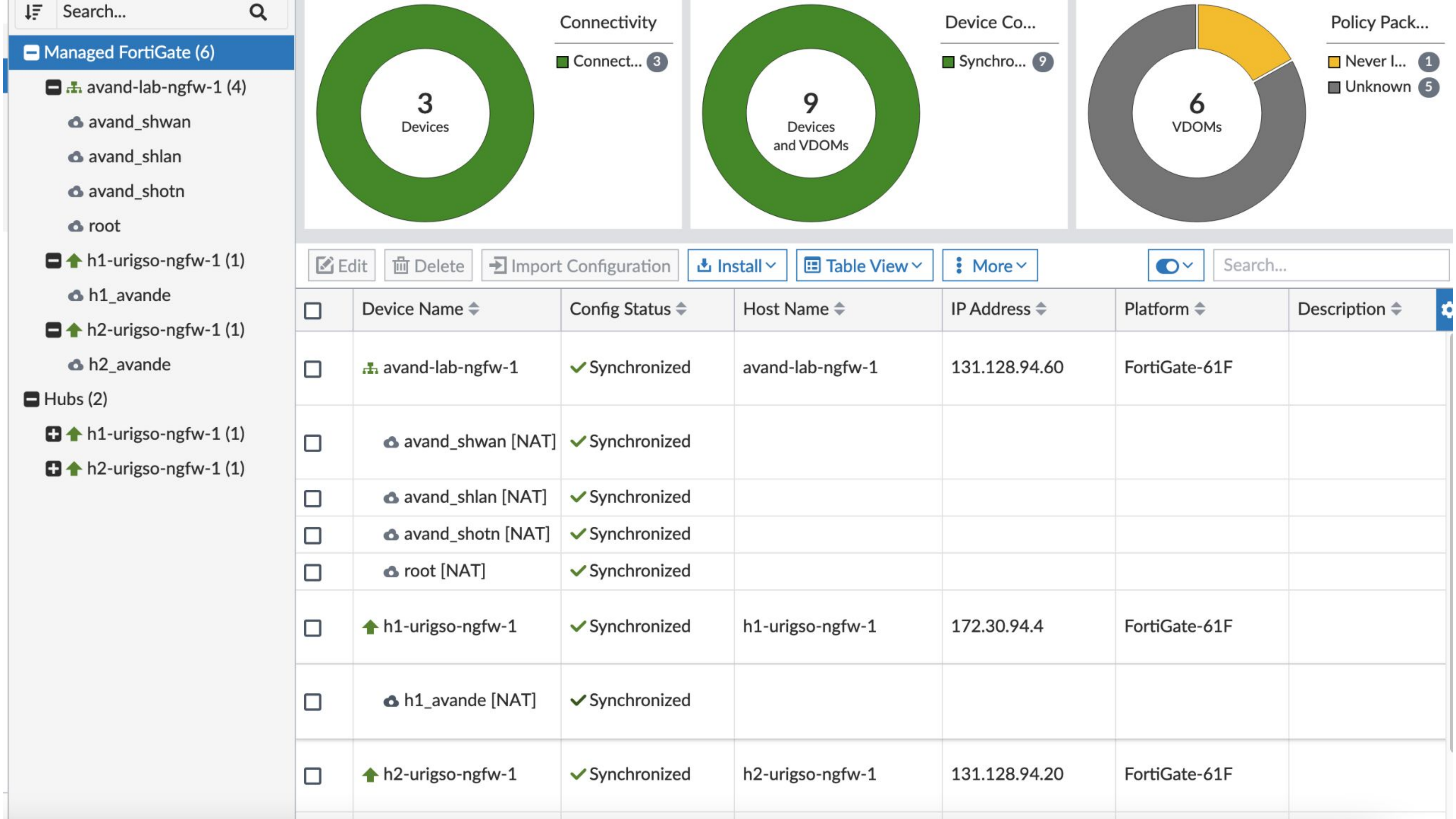
Endeavor network core, before and after core switch/Fortigate install. Note that both iterations have the same core capabilities. "Before" pic delivered many successful cruises but expansion was a struggle - especially W/R/T Internet connections. "After" pic has expansion slots for Starlink + eliminates addt'l routers.

2.2.3 Disadvantages of VDOMs

- VDOM's give us a way to "baffle" traffic so that it flows optimally through the Fortigate, however, introducing this option into a config has some major side effects.
  - While standard IP "data" will easily flow between VDOMs, the Fortigate's added "metadata" annotations will NOT flow between VDOMs (without external assistance)
  - The Fortigate needs to have VDOM-Links (virtual network interfaces that bind VDOMs together) added so that VDOMs can talk to each other. These need to have IP addresses and routing configs set.
  - Each VDOM has its own firewall instance - so a traffic flow that crosses VDOMs will need VDOM Links, Routes, and firewall rules on both sides.
- VDOM layout is a fine balance between making traffic flows very simple and intuitive, or creating a massive duplication of configuration statements.
- If only there was some higher-order configuration-level virtualization layer…

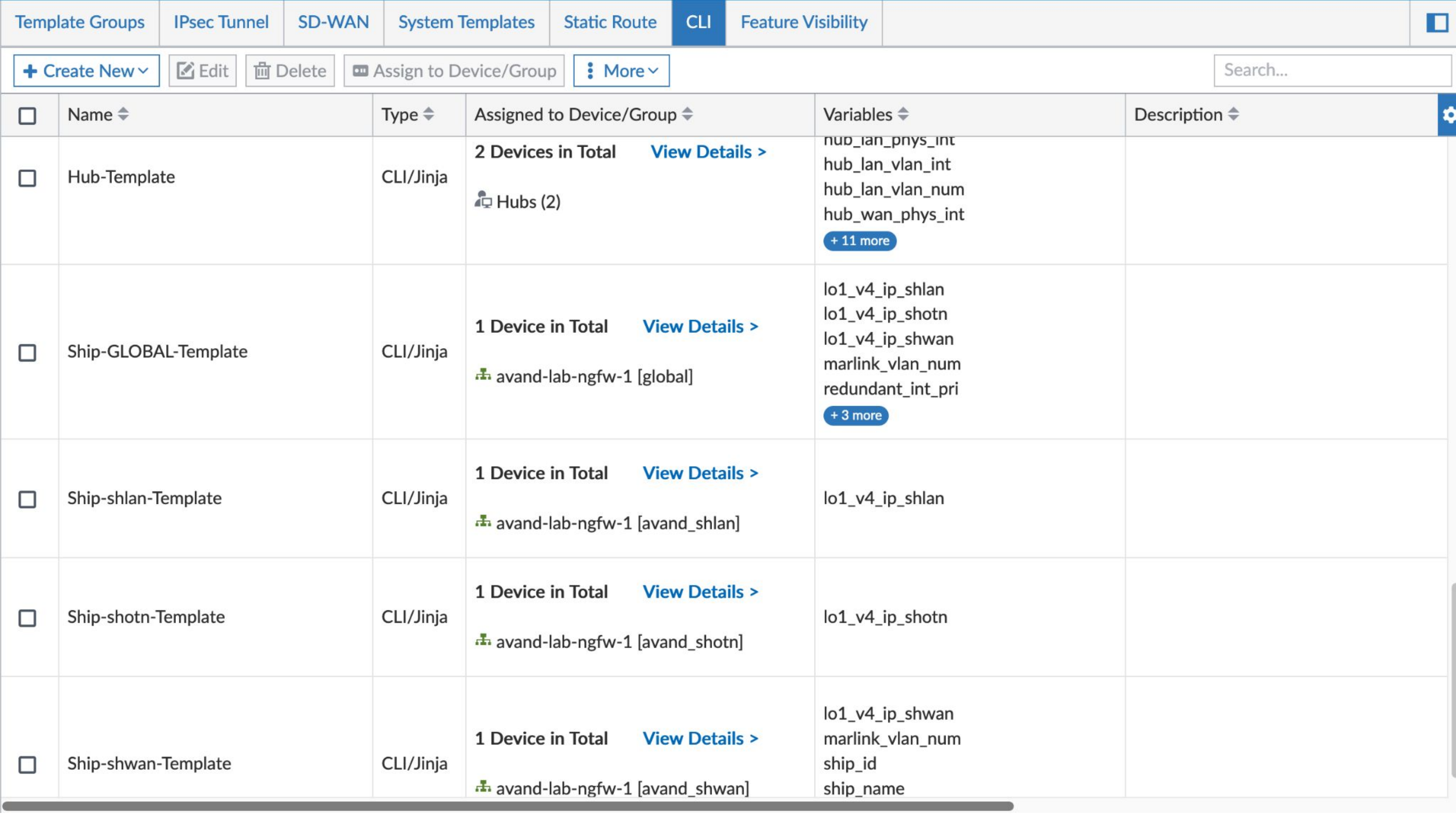
2.3: Administrative Domains (ADOM)

- So far, the layers of virtualization that we have discussed have all been directly related to traffic flow.
  - VLANs allow isolated networks to share a given network switch
  - VDOMs allow different pools of isolated networks to share a given router
  - VPNs allow non-routable networks to pass over the Internet without requiring private lines
- In the pokeball diagram, our reference architecture has:
  - An arbitrary number of VLANs based upon the ship in question
  - Five VDOMs, spread across three locations
  - 14 VPN tunnels, to two sites, across (up to) seven different Internet connections
- ADOM's exist in the config world, rather than the traffic flow world.
  - Back before LinkedIn "software defined innovation" vernacular took over, we would define this as a control-plane versus data-plane function
  - ADOM's pull all of these different items into a single location where config file variables and templates can be reused.



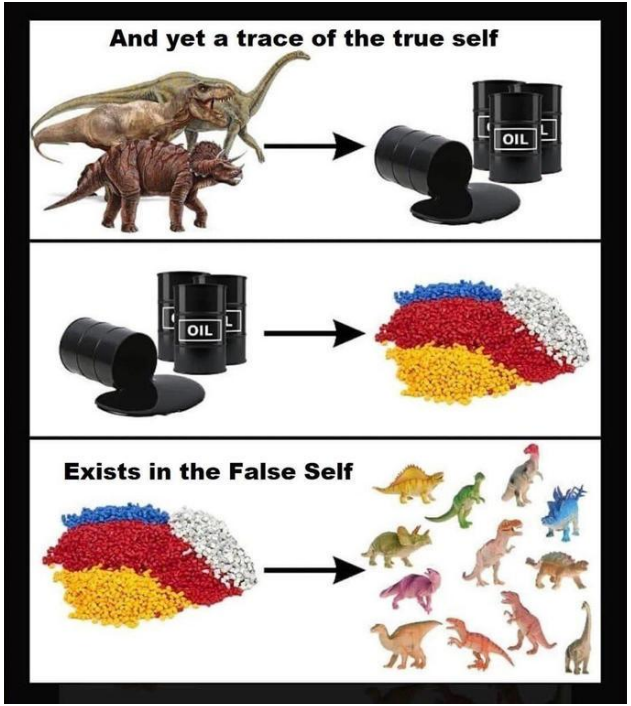
- Managed FortiGate (6)
  - avand-lab-ngfw-1 (4)
    - avand_shwan
    - avand_shlan
    - avand_shotn
    - root
  - h1-urigso-ngfw-1 (1)
    - h1_avande
  - h2-urigso-ngfw-1 (1)
    - h2_avande
- Hubs (2)
  - h1-urigso-ngfw-1 (1)
  - h2-urigso-ngfw-1 (1)

□	Device Name	Config Status	Host Name	IP Address	Platform	Description
□	avand-lab-ngfw-1	✓ Synchronized	avand-lab-ngfw-1	131.128.94.60	FortiGate-61F	
□	avand_shwan [NAT]	✓ Synchronized				
□	avand_shlan [NAT]	✓ Synchronized				
□	avand_shotn [NAT]	✓ Synchronized				
□	root [NAT]	✓ Synchronized				
□	h1-urigso-ngfw-1	✓ Synchronized	h1-urigso-ngfw-1	172.30.94.4	FortiGate-61F	
□	h1_avande [NAT]	✓ Synchronized				
□	h2-urigso-ngfw-1	✓ Synchronized	h2-urigso-ngfw-1	131.128.94.20	FortiGate-61F	



□	Name	Type	Assigned to Device/Group	Variables	Description
□	Hub-Template	CLI/Jinja	2 Devices in Total View Details > Hubs (2)	hub_lan_phys_int hub_lan_vlan_int hub_lan_vlan_num hub_wan_phys_int + 11 more	
□	Ship-GLOBAL-Template	CLI/Jinja	1 Device in Total View Details > avand-lab-ngfw-1 [global]	lo1_v4_ip_shlan lo1_v4_ip_shotn lo1_v4_ip_shwan marlink_vlan_num redundant_int_pri + 3 more	
□	Ship-shlan-Template	CLI/Jinja	1 Device in Total View Details > avand-lab-ngfw-1 [avand_shlan]	lo1_v4_ip_shlan	
□	Ship-shotn-Template	CLI/Jinja	1 Device in Total View Details > avand-lab-ngfw-1 [avand_shotn]	lo1_v4_ip_shotn	
□	Ship-shwan-Template	CLI/Jinja	1 Device in Total View Details > avand-lab-ngfw-1 [avand_shwan]	lo1_v4_ip_shwan marlink_vlan_num ship_id ship_name	

YOU GET A NESTED ABSTRACTION LAYER
YOU GET A NESTED ABSTRACTION LAYER
YOU GET A NESTED ABSTRACTION LAYER
EVERYONE GETS A NESTED ABSTRACTION LAYER
imgflip.com



2.4: How the virtualized layers fit together

Reality. No virtualization.
> "You are on a ship. There is a Fortigate here, with two cables connected"

```
print(f'{i}.{j}: Abstracted virtualization layer
for {virtualization-slide-joke}')
>NameError: name 'i' is not defined
```

Reality - 1. Interface level virtualization (VLAN, VPN)
> "There are ten handwaveable things in-between, but this is basically how the ADCP works"

Reality - 2. Routing-table level virtualization (VDOM)
> "We budgeted for three routers, but only one showed up to the vessel! However can we balance our yearly budget with NSF?"

Reality - 3. "Device-manifest" level virtualization (ADOM)
> "Here is the CAD model of our ship, and the locations of everything in the shipyard. This is a ship"

Reality - ∞. Terminal virtualization (???)
> *"You are on a ship. There is an unruly Fortigate here, with twenty-one virtual WAN interfaces. You try and ping google.com without specifying a source-ip for the ping. The ping fails. Somewhere on the backside of this ping test and twenty-one hours of airline travel you have a family. After so many miles in the seated marathon you've run, their names are as meaningless as the words on the safety placard contractually posted on the wall in front of you. If you squint your eyes, you can still read the text."*

2.5: Basic Network Services (DNS, DHCP)

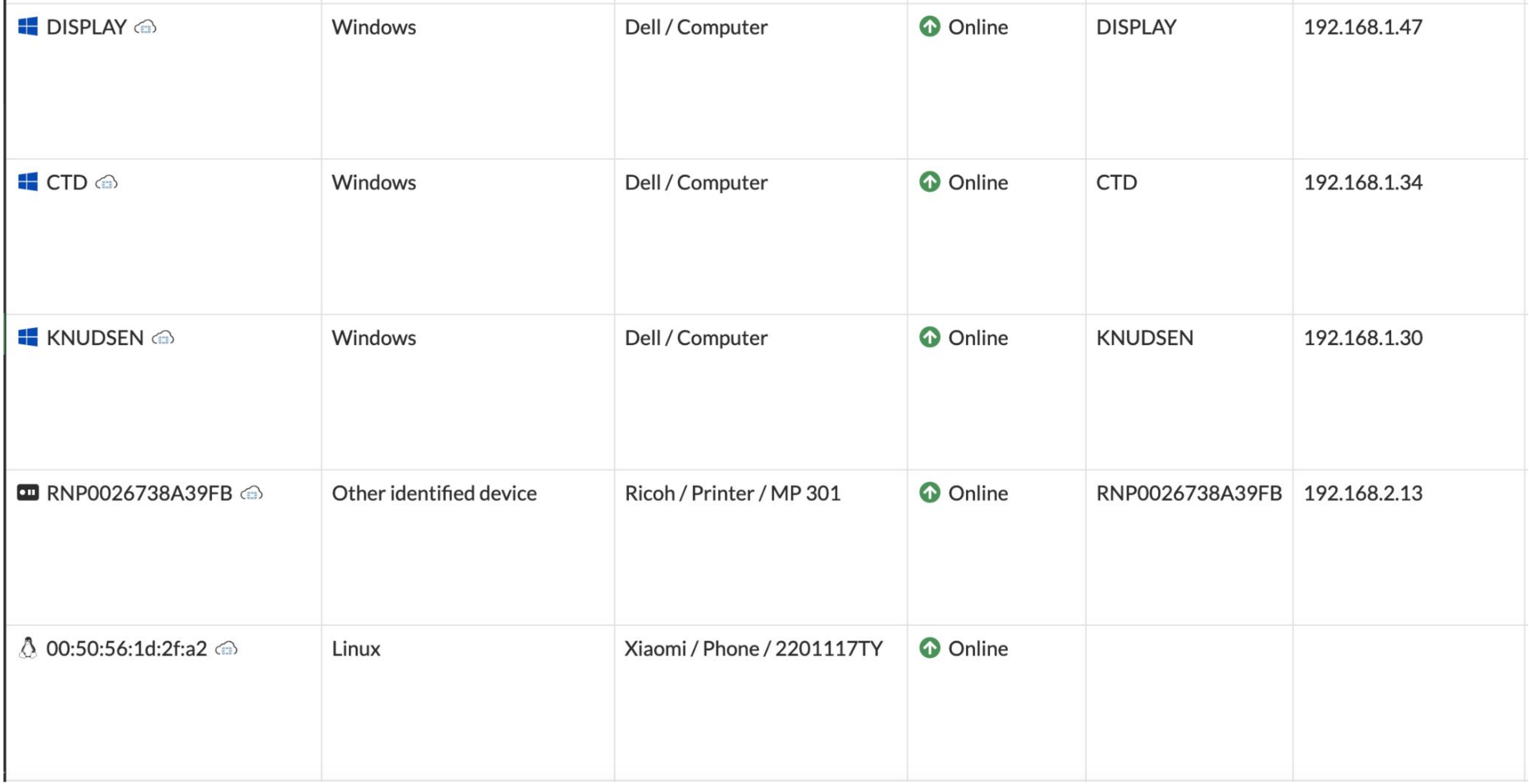
- Outside of the reality-bending nested virtualization features, the Fortigate can also serve as a DHCP listener, and it can help you get online!
  - It makes toast just as well as it provides an abstract interface to heating bread-like objects.
  - If DHCP is enabled on an interface, it can volunteer as tribute for DNS/NTP requests, or it can direct clients towards a more qualified DNS (Active Directory) or NTP (Hardware GPS clock) server.
- Default reference architecture behavior
  - DNS "listeners" are available on the default gateway of each shipboard LAN interface. (LAN, OTN VDOMs).
  - DNS requests are forwarded to the WAN VDOM.
  - The WAN VDOM caches DNS requests (HUGE latency improvement) or alternatively serves up a local DNS entry.
- DNS lookups are one of the hooks into the "logging-by-default" OmniSOC data delivery package.

2.6: Device Inventory & Username Capture

- Once a device has an IP address, default gateway, and DNS servers, it's online.
- The "data" (device IP and MAC address) is not particularly helpful without *metadata*: device OS info (marginally helpful), hostname (often not helpful) and associated username (by far the most useful field, also the hardest to get)
- Metadata
    - MAC address can sometimes (but not always) tell you what company made the device. This can easily be a red herring (IE, Broadcom/Intel/etc network interface). MAC addresses are randomized on most iOS/android tablets, which makes life harder.
    - OS fingerprinting techniques can sometimes, but not always, tell you what OS the thing is running (Windows, MacOS, iOS, Android)
    - Device hostname can sometimes, but not always, be captured. However, this is often not useful, since many devices have non-indicative hostnames (burgermeister, moonfish)

2.6: Device Inventory & Username Capture, cont'd.

- Username capture, two approaches
  - Captive Portal (hotel-style)
  - 802.1X
- Captive Portal
  - Relies on browser and/or OS to detect the redirect
  - Will almost certainly trip a SSL/TLS certificate "Insecure Site" warning
- 802.1X
  - Alongside VDOMs, this can be a genie or a Balrog.
  - Works exceptionally well (has network-level username capture) until it doesn't. Keep in mind that most universities run 802.1X on their home network, and often install clients on their employee's work laptops to facilitate this. So even a setup that _should_ work according to the standards may fail because of a 3rd party client installation.
- Option C: Just ban the device hogging the Internet beans, and see who complains



DISPLAY	Windows	Dell / Computer	Online	DISPLAY	192.168.1.47
CTD	Windows	Dell / Computer	Online	CTD	192.168.1.34
KNUDSEN	Windows	Dell / Computer	Online	KNUDSEN	192.168.1.30
RNP0026738A39FB	Other identified device	Ricoh / Printer / MP 301	Online	RNP0026738A39FB	192.168.2.13
00:50:56:1d:2f:a2	Linux	Xiaomi / Phone / 2201117TY	Online		

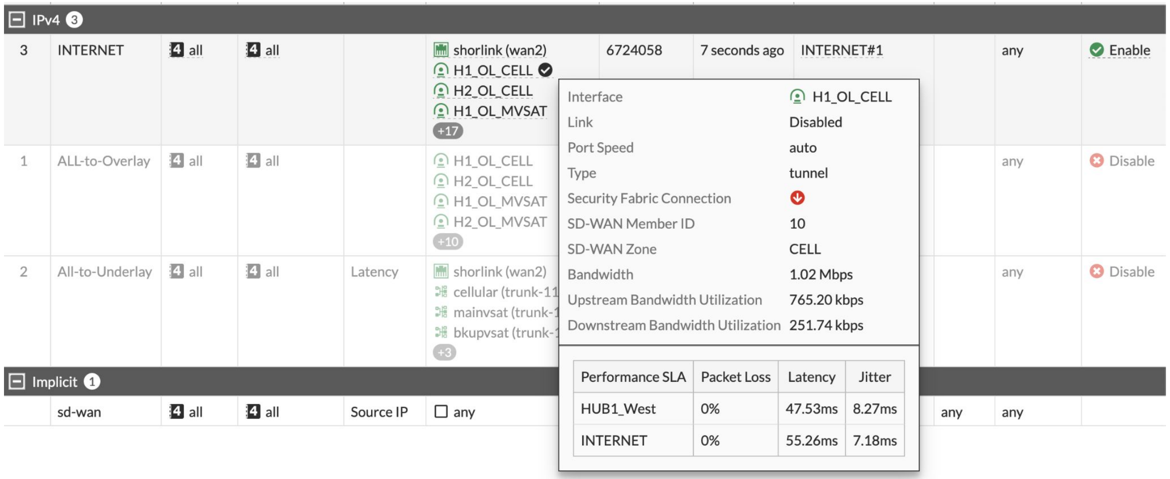
2.7: Getting Online

- SDWAN (software defined WAN)
  - Assume Peplink is the closest thing to a fleetwide standard - Fortigate SDWAN is a mixture of Peplink's health-checks on WANs, as well as the ability to use VPN connections for Internet access
  - Default SDWAN behavior - list of interfaces by admin-defined preference. Use the best-performing interface, so long as it meets a given performance characteristic (packet loss)
- SDWAN -> automatic path selection from predefined list of paths
- Tools that provide paths
  - "Local" internet - no Hub
  - Hub Internet and Tunneling

2.7: Getting Online, cont'd.

Path Type	Requires an available Hub site?	Control upload bandwidth?	Control download bandwidth?	Ship has static IP?
"Underlay" (local Internet, no tunnel to Hub)	NO	YES	NO	NO
"Overlay" (tunnel to Hub that provides Internet)	YES	YES	YES	YES

2.7.1: SDWAN



IPv4 3

3	INTERNET	all	all		shorlink (wan2) H1_OL_CELL ✓ H2_OL_CELL H1_OL_MVSAT +17	6724058	7 seconds ago	INTERNET#1		any	✓ Enable
1	ALL-to-Overlay	all	all		H1_OL_CELL H2_OL_CELL H1_OL_MVSAT H2_OL_MVSAT +10					any	☒ Disable
2	All-to-Underlay	all	all	Latency	shorlink (wan2) cellular (trunk-11 mainvsat (trunk-1 bkupvsat (trunk-1 +3					any	☒ Disable

Implicit 1

	sd-wan	all	all	Source IP	□ any				any	any

Interface	H1_OL_CELL
Link	Disabled
Port Speed	auto
Type	tunnel
Security Fabric Connection	↓
SD-WAN Member ID	10
SD-WAN Zone	CELL
Bandwidth	1.02 Mbps
Upstream Bandwidth Utilization	765.20 kbps
Downstream Bandwidth Utilization	251.74 kbps

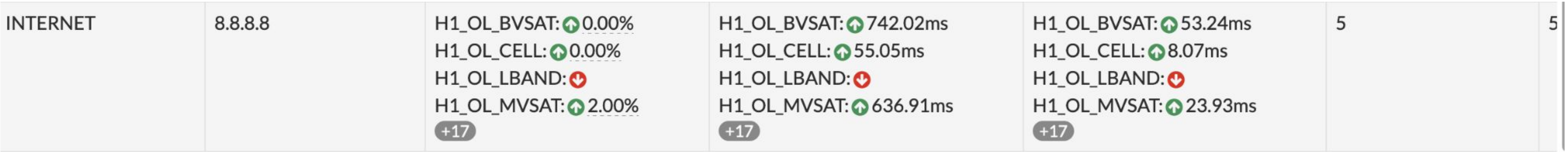
Performance SLA	Packet Loss	Latency	Jitter
HUB1_West	0%	47.53ms	8.27ms
INTERNET	0%	55.26ms	7.18ms

H1_OL_CELL

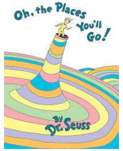
- OL (Overlay) = tunnel to hub
- H1 (Hub1)
- CELL = 5G Modem

Selected based upon:

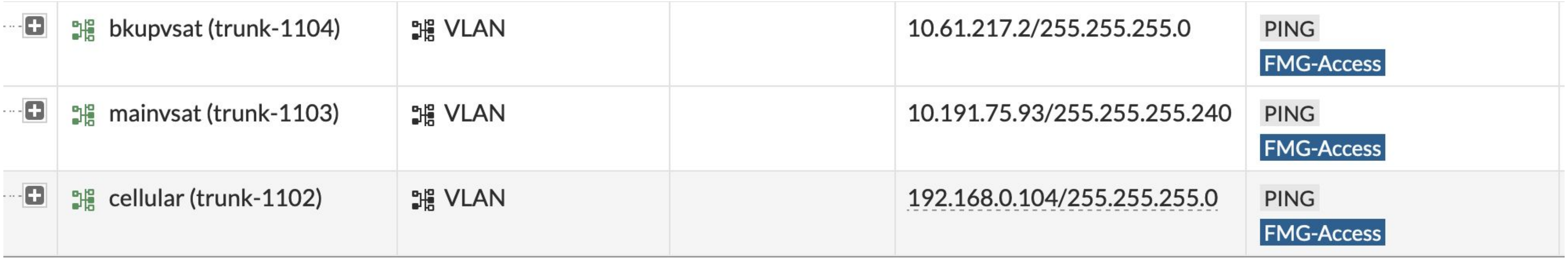
- Admin's priority list
- Realtime interface performance within admin's edict



INTERNET	8.8.8.8	H1_OL_BVSAT: ↑ 0.00% H1_OL_CELL: ↑ 0.00% H1_OL_LBAND: ↓ H1_OL_MVSAT: ↑ 2.00% +17	H1_OL_BVSAT: ↑ 742.02ms H1_OL_CELL: ↑ 55.05ms H1_OL_LBAND: ↓ H1_OL_MVSAT: ↑ 636.91ms +17	H1_OL_BVSAT: ↑ 53.24ms H1_OL_CELL: ↑ 8.07ms H1_OL_LBAND: ↓ H1_OL_MVSAT: ↑ 23.93ms +17	5	5



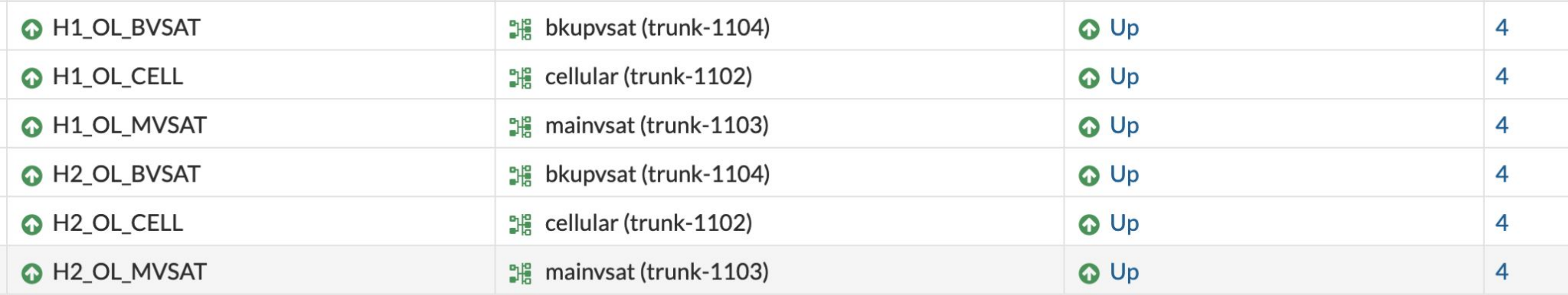
2.7.2: Getting Online: Local Internet



⊞	bkupvsat (trunk-1104)	VLAN		10.61.217.2/255.255.255.0	PING FMG-Access
⊞	mainvsat (trunk-1103)	VLAN		10.191.75.93/255.255.255.240	PING FMG-Access
⊞	cellular (trunk-1102)	VLAN		192.168.0.104/255.255.255.0	PING FMG-Access

Local Internet has minimal config dependencies. Most modems will give you a usable IP via DHCP and so there's really not much that needs to happen here.

2.7.2: Getting Online: Hub Internet

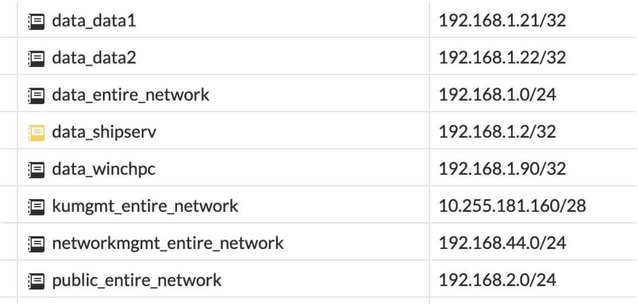


H1_OL_BVSAT	bkupvsat (trunk-1104)	Up	4
H1_OL_CELL	cellular (trunk-1102)	Up	4
H1_OL_MVSAT	mainvsat (trunk-1103)	Up	4
H2_OL_BVSAT	bkupvsat (trunk-1104)	Up	4
H2_OL_CELL	cellular (trunk-1102)	Up	4
H2_OL_MVSAT	mainvsat (trunk-1103)	Up	4

Working "local" internet is actually a prerequisite for Hub-based Internet. Once a given WAN connection has working Internet, outside of being available for local Internet access, the WAN connection will also launch a VPN client process. In this case, rather that directly hitting the modem, traffic flow via this path goes inside a VPN client session. This allows for bidirectional traffic flow (remote access to the ship, as well as the ship's static IP and download-side shaping)

2.8: Firewall Objects & Rules

- In the Fortigate, firewall policies (and other things that control traffic flow) are not bound directly to IP addresses (or interfaces for that matter)
- IP addresses are wrapped into objects, and N number of objects can be set as the source or destination addresses ('any' also exists within the system). Ability to "bundle" flows together into small number of policies is one of the most powerful parts of this system.

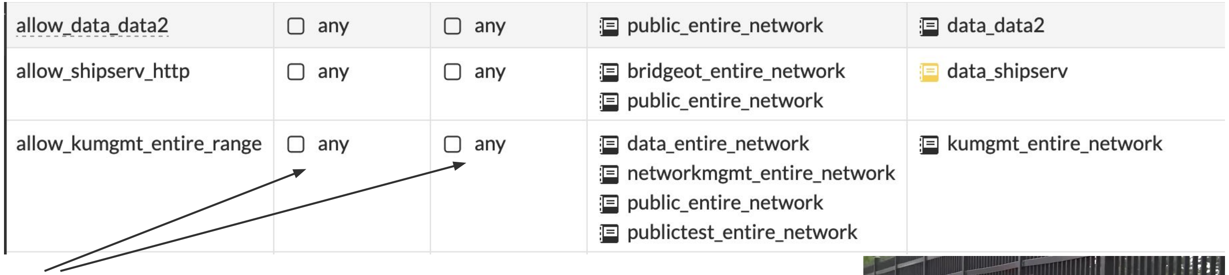


data_data1	192.168.1.21/32
data_data2	192.168.1.22/32
data_entire_network	192.168.1.0/24
data_shipserv	192.168.1.2/32
data_winchpc	192.168.1.90/32
kumgmt_entire_network	10.255.181.160/28
networkmgmt_entire_network	192.168.44.0/24
public_entire_network	192.168.2.0/24

Address objects can be a single host (w.x.y.z/32), or a network (192.168.2.0/24), or a range of IP's
A firewall policy can reference more than one source or destination address objects.

2.8: Firewall Objects & Rules

- "Public" devices (printers, onboard webpage, data share) will have many source objects accessing a specific destination
- "Restricted" devices (MOXA WebUI, etc) will have some source objects accessing a specific service on a specifc device.
- Default block = allow NO communication. Have to have more specific rules to allow anything to get through.



allow_data_data2	□ any	□ any	public_entire_network	data_data2
allow_shipserv_http	□ any	□ any	bridgeot_entire_network public_entire_network	data_shipserv
allow_kumgmt_entire_range	□ any	□ any	data_entire_network networkmgmt_entire_network public_entire_network publictest_entire_network	kumgmt_entire_network

Rule not bound to any "section" of fence (IE, source/dest interface)
Makes writing broad strokes policy MUCH easier

The FortiReckoning

System Design (The Nitty Gritty)

Chapter 3: The Traffic Flow

MOXA with
$GPGGA

yahoo.com

Shiptracker
Webpage

"Let's just add one more rule…"

SCS/
OpenRVDAS

On behalf of **NSF, ONR, ARF CIWG, UNOLS, SatNAG, HiSeasNet, ResearchSOC** please do not build this

3.1: Parts of the Traffic Flow

Onboard (LAN, East-West)

- Fairly definite list of things onboard
- Changes as instruments, etc installed
- Bandwidth onboard is (generally) not an immediate concern
- Paths are generally reliable
- Very vessel-specific

Internet (WAN, North-South)

- Arbitrary cloud services, shoreside, etc
- Bandwidth is easier (Starlink, expanded VSAT) but still a fraction of LAN bandwidth
- Have to assume paths will go down
- Easier to template

WAN is basically an extension of what we start to build on ship.

Implementation of the Traffic Flow

Onboard =	Firewall Rules		
Internet =	Firewall Rules	SDWAN	Traffic Shaping

Firewall Rules	Can it get there at all?	
SDWAN	How should it get there?	Paths do not have equal performance, and can fail…
Traffic Shaping	How important is it?	Prioritizing limited bandwidth

Firewall Rules example

- Firewall Rules are absolute, and are used on both LAN and WAN sides.
- Generally based upon source IP's and destination IP's
  - Forti can detect cloud applications / services like Windows Update
  - These definitions are maintained as part of the support package
- Firewall rules sources + destinations can be bundled.
- LAN side
  - Block Public -> Data network by default
  - Allow VERY specific Public -> Data access to certain services
- **WAN side**
  - Payoff of the device setup process is that we can write very effective bundles of rules.
  - Example - in the event of an emergency, keep Internet access for the bridge, otherwise, drop Internet.

SDWAN Example

- This is where we're focusing on what pathway should traffic go down. Really only used on the WAN side of the equation.
- Endeavor example - we have 5G, Sealink, and FleetXpress as Internet connections.
  - 5G is great coastally, but will drop out (slowly) as we go further out
  - Sealink + FX -> high latency
- For each of these connections, we can either get Internet via Hub1, Hub2, or fallback to local Internet if both Hub sites are down.
  - Prefer Hub1
  - Accept Hub2
  - Local Internet if absolutely necessary (non-US IP addresses)
- Define a list of connections, tell the Fortigate the priority we generally want to see, and then the Forti will select the best available option.

Traffic Shaping

- A given WAN interface only has so much bandwidth available
  - Historically, implemented quotas
  - Looking forward, allow bandwidth hogging (but entertaining) services to run in background and use available bandwidth
  - On the other side, really important services get the ability to preempt non-critical traffic
- Where are these applied?
  - Upload applied onboard
  - Download applied at the hub
- Ship and Hub parts of the config coordinated in FortiManager

Traffic Shaping (Tiers)

Name	Relative Priority	Behavior	Example Traffic Flow
TOP	+3	Preempt everything	Telemedicine, Bridge, Phones
CRITICAL	+2	Preempt H/M/L	
HIGH	+1	Preempt M/L	Zoom
MEDIUM	(Default)	Preempt L	(everything else)
LOW	-1	Background Traffic	iCloud, YouTube…

In Review

- Everything
    - Rules can be applied to bundles of devices, not just one at a time.
    - Fortigate has definitions for cloud applications which are maintained
- Firewall rules - absolute
    - Block sources (allow bridge, block general Internet)
    - Block destinations/services.
- SDWAN - relative to configured list, and then actual moment-to-moment performance
- Traffic Shaping - amount of bandwidth available depends on what higher priority flows are using

The FortiReckoning

System Design (The Nitty Gritty)

Chapter 4: Implementation & Lessons Learned

Recent Experience

- Received testing hardware ~June
- Endeavor ship-only installation August '23
  - Move all ship networking to the Fortigate
  - Internet directly via the ISP
  - Install with device CLI
  - Maintain with device GUI
- Endeavor hub installation October '23
  - Internet via the hub
  - Install via FortiManager and reusable templates
  - Maintain with FortiManager + local device console (if needed)

Current Work

- Install Scripting
    - Current templates work but need to be refactored so it's easier to match them to a installation punchlist
    - Continue developing the data collection spreadsheet, and present it with filled-in examples
- OmniSOC Integration
    - OmniSOC "client" vessel config being built inside FortiManager
    - Build reusable process so that this standup is just a checkbox
- Traffic Shaping
    - Rachel working on this onboard Nautilus (current cruise is very data intensive)
    - Goal #1 on making background updates less of an issue
    - Goal #2 is realtime/near-real-time video & data

Thank You!

v OLD STUFF v

Firewall Rules 101

- What are firewall rules?
- Firewall rules best practices
  - E.g. allow UDP across VLANs before deny rules
- How do Fortigate rules differ from SophosXG?
- How/Where to implement in FortiWorld
  - Include diagram of FortiWorld here

Configuration Best Practices

-

Troubleshooting Best Practices

Cybersecurity Logging/Analysis

- Cybersecurity Logger
- FortiAnalyzer
    - On ship
    - Shore Aggregation
- What do you need to pay attention to on a daily basis?

ResearchSOC Monitoring

- Where do they get data?
- What are they monitoring/looking for?
- What can you expect to receive from their monitoring?

FortiManager

- What is the FortiManager?
- What are the advantages?
- What are templates?
  - why should we use them?

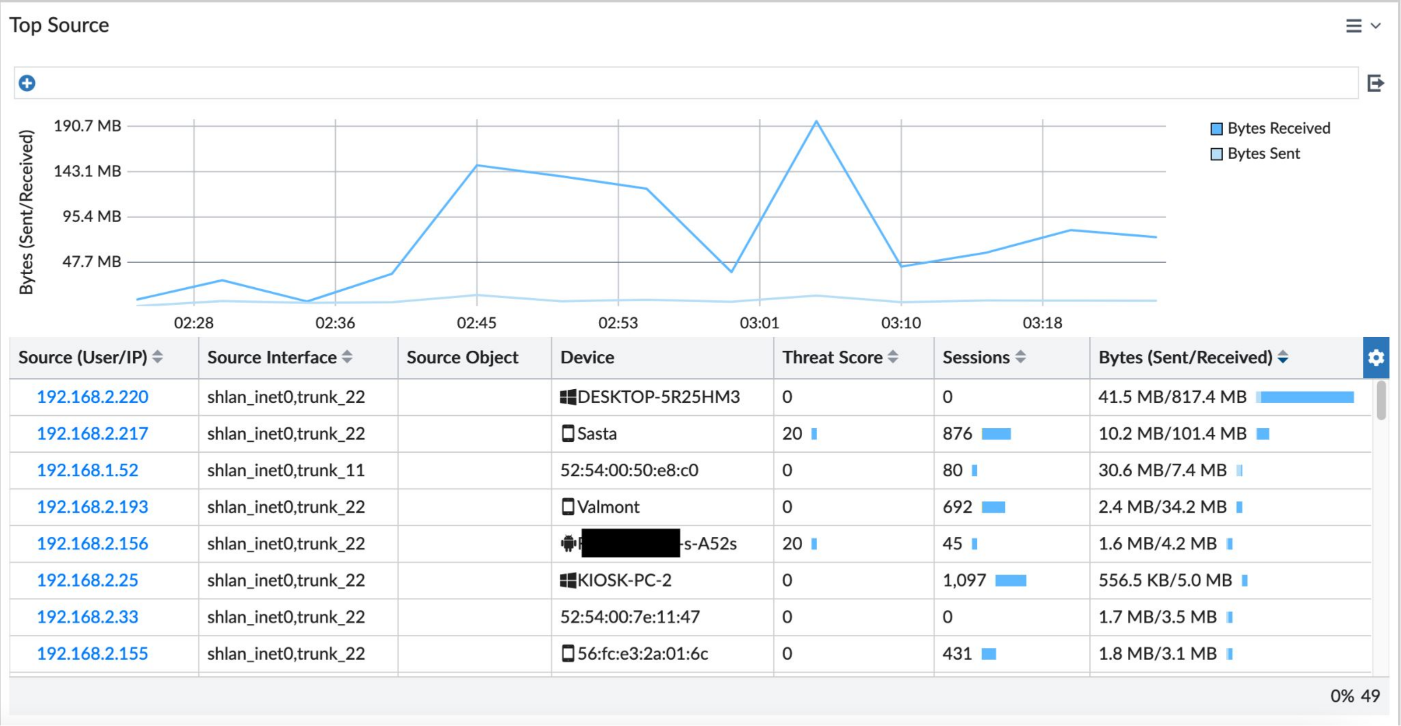
Overview of Shore Hubs

- How is the specific hub chosen?
- What are the advantages?
  - US IP address / opt tunnel to home inst
  - WAN aggregation for seamless connectivity
- Role of the FortiManager
- What can you expect as a tech responsible for ship comms?

Simplicity of Daily operations

- The components described above seem complex, but there will be little that needs to change or be monitored by techs on a regular basis.
- Role of FortiManager

FortiAnalyzer / Device Inventory

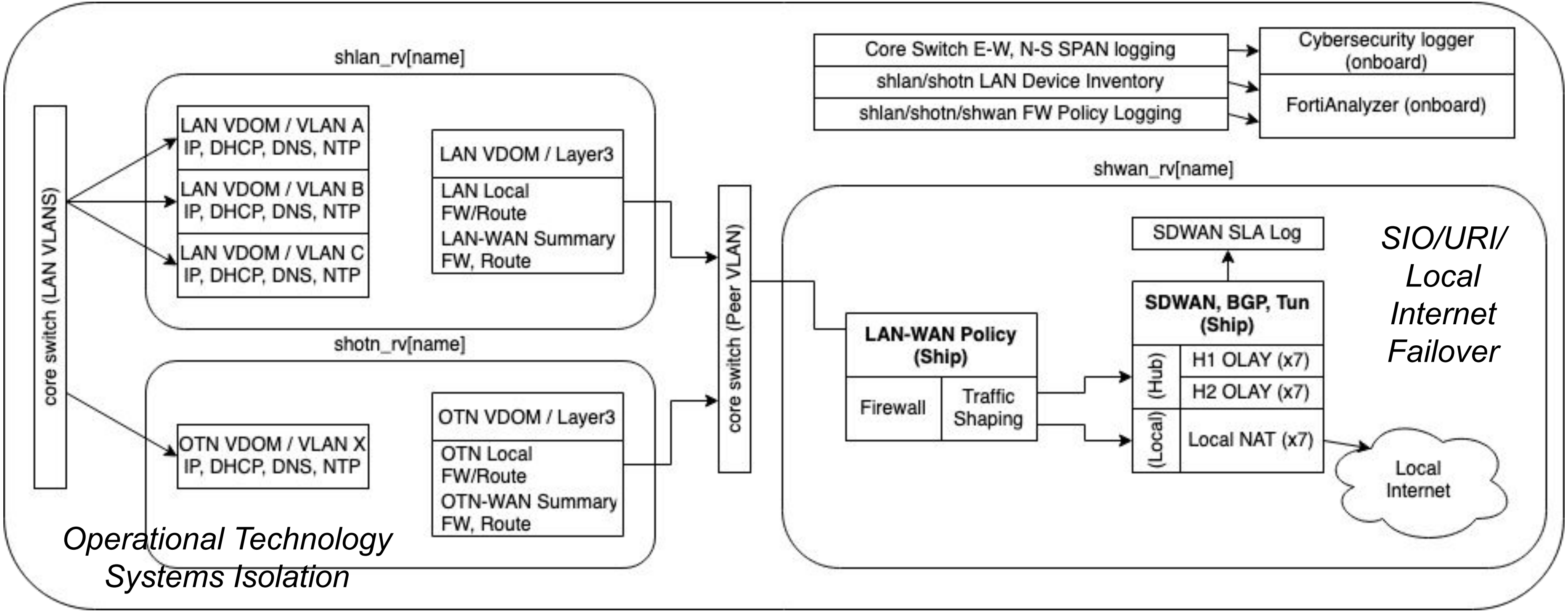


Source (User/IP)	Source Interface	Source Object	Device	Threat Score	Sessions	Bytes (Sent/Received)
192.168.2.220	shlan_inet0,trunk_22		DESKTOP-5R25HM3	0	0	41.5 MB/817.4 MB
192.168.2.217	shlan_inet0,trunk_22		Sasta	20	876	10.2 MB/101.4 MB
192.168.1.52	shlan_inet0,trunk_11		52:54:00:50:e8:c0	0	80	30.6 MB/7.4 MB
192.168.2.193	shlan_inet0,trunk_22		Valmont	0	692	2.4 MB/34.2 MB
192.168.2.156	shlan_inet0,trunk_22		[redacted]-s-A52s	20	45	1.6 MB/4.2 MB
192.168.2.25	shlan_inet0,trunk_22		KIOSK-PC-2	0	1,097	556.5 KB/5.0 MB
192.168.2.33	shlan_inet0,trunk_22		52:54:00:7e:11:47	0	0	1.7 MB/3.5 MB
192.168.2.155	shlan_inet0,trunk_22		56:fc:e3:2a:01:6c	0	431	1.8 MB/3.1 MB

0% 49

Example Network Architecture (Shipboard)

Traffic analysis and Device Inventory



core switch (LAN VLANS)

shlan_rv[name]

LAN VDOM / VLAN A
IP, DHCP, DNS, NTP

LAN VDOM / VLAN B
IP, DHCP, DNS, NTP

LAN VDOM / VLAN C
IP, DHCP, DNS, NTP

LAN VDOM / Layer3

LAN Local
FW/Route
LAN-WAN Summary
FW, Route

shotn_rv[name]

OTN VDOM / VLAN X
IP, DHCP, DNS, NTP

OTN VDOM / Layer3

OTN Local
FW/Route
OTN-WAN Summary
FW, Route

core switch (Peer VLAN)

Core Switch E-W, N-S SPAN logging

shlan/shotn LAN Device Inventory

shlan/shotn/shwan FW Policy Logging

Cybersecurity logger (onboard)

FortiAnalyzer (onboard)

shwan_rv[name]

SDWAN SLA Log

SDWAN, BGP, Tun (Ship)

(Hub)

H1 OLAY (x7)

H2 OLAY (x7)

(Local)

Local NAT (x7)

LAN-WAN Policy (Ship)

Firewall

Traffic Shaping

Local Internet

SIO/URI/ Local Internet Failover

Operational Technology Systems Isolation

Implementation Process

- Various resources are available to help.
  - Wiki coming soon!
  - Send email to arf-firewall-team@unols.org
- The next presentation will go into detail about how this was implemented on Endeavor.

Questions?

Thoughts?

Suggestions?

Additional Reference Slides

What problems are we trying to solve?

Big Picture

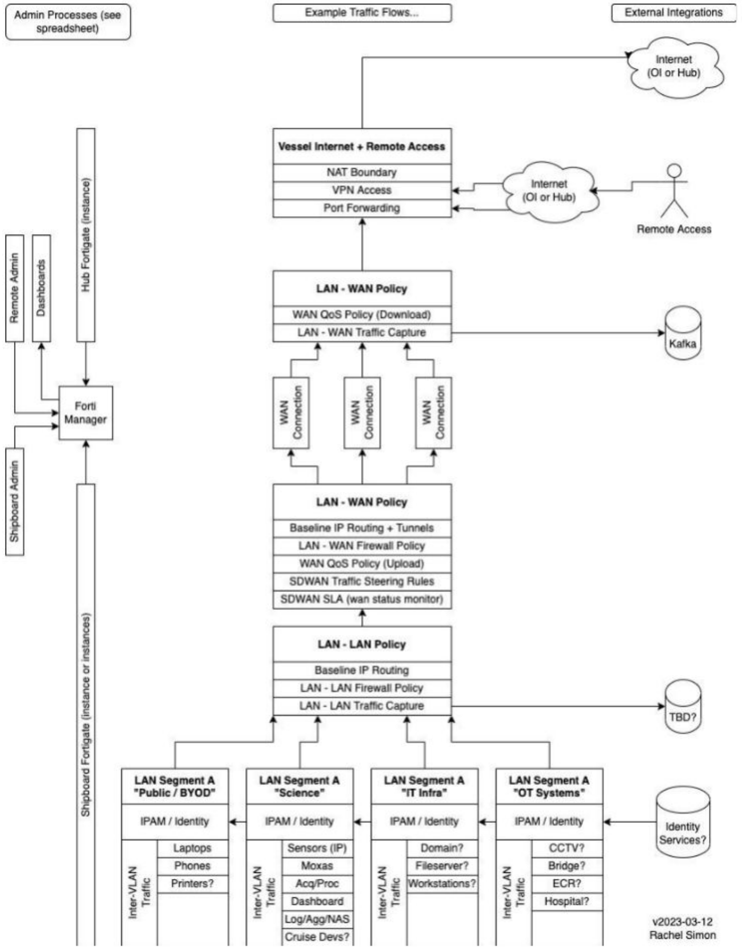
- Cybersecurity goals
  - OmniSOC hooks built-in by default
  - Monitoring tools should "just work"
- Simplify maintenance
  - Templates + procedures can be reused between ships
  - All networking tasks can be done in one system (config + hardware)
- Make it easy to implement big-picture fleet cyberinfrastructure objects

Day to Day

- **Ship's IP address**
  - No Norwegian/Dutch Google!
  - Access to host university systems...
- Key information on a single screen
- Inventory of who's on the network
  - Device + user information
  - Internet usage (and why…)
- Usage
  - Auto prefer lowest latency
  - +Zoom et al, -iCloud et al.

What components? Where are they located?

- Core Switches (ship)
  - Note, these do not have to be Fortinet switches!
  - Pair of VLAN-capable switches at the core, feeds out to Wifi AP's + switches around the vessel
- Fortigate Hardware Appliances (ship + hub)
  - Network traffic passes through these devices
  - Ship Fortigate can manage all onboard networks (DNS, DHCP, etc) and do inventory (Win PC/Mac/iPhone/Android etc, get hostnames)
  - Hooks for OmniSOC data collection
- FortiAnalyzer (ship + hub)
  - Organizes inventory + traffic logs into reports (usage, security logs -> OmniSOC)
  - Day to day status dashboard (WAN status, device usage, etc)
- FortiManager (hub)
  - Configuration, templates, backups of all parts of the system.



Admin Processes (see spreadsheet)

Example Traffic Flows...

External Integrations

Internet (OI or Hub)

Vessel Internet + Remote Access

NAT Boundary

VPN Access

Port Forwarding

Internet (OI or Hub)

Remote Access

Hub Fortigate (instance)

Remote Admin

Dashboards

Forti Manager

Shipboard Admin

Shipboard Fortigate (instance or instances)

LAN - WAN Policy

WAN QoS Policy (Download)

LAN - WAN Traffic Capture

Kafka

WAN Connection

WAN Connection

WAN Connection

LAN - WAN Policy

Baseline IP Routing + Tunnels

LAN - WAN Firewall Policy

WAN QoS Policy (Upload)

SDWAN Traffic Steering Rules

SDWAN SLA (wan status monitor)

LAN - LAN Policy

Baseline IP Routing

LAN - LAN Firewall Policy

LAN - LAN Traffic Capture

TBD?

LAN Segment A "Public / BYOD"

IPAM / Identity

Inter-VLAN Traffic

Laptops

Phones

Printers?

LAN Segment A "Science"

IPAM / Identity

Inter-VLAN Traffic

Sensors (IP)

Moxas

Acq/Proc

Dashboard

Log/Agg/NAS

Cruise Devs?

LAN Segment A "IT Infra"

IPAM / Identity

Inter-VLAN Traffic

Domain?

Fileserver?

Workstations?

LAN Segment A "OT Systems"

IPAM / Identity

Inter-VLAN Traffic

CCTV?

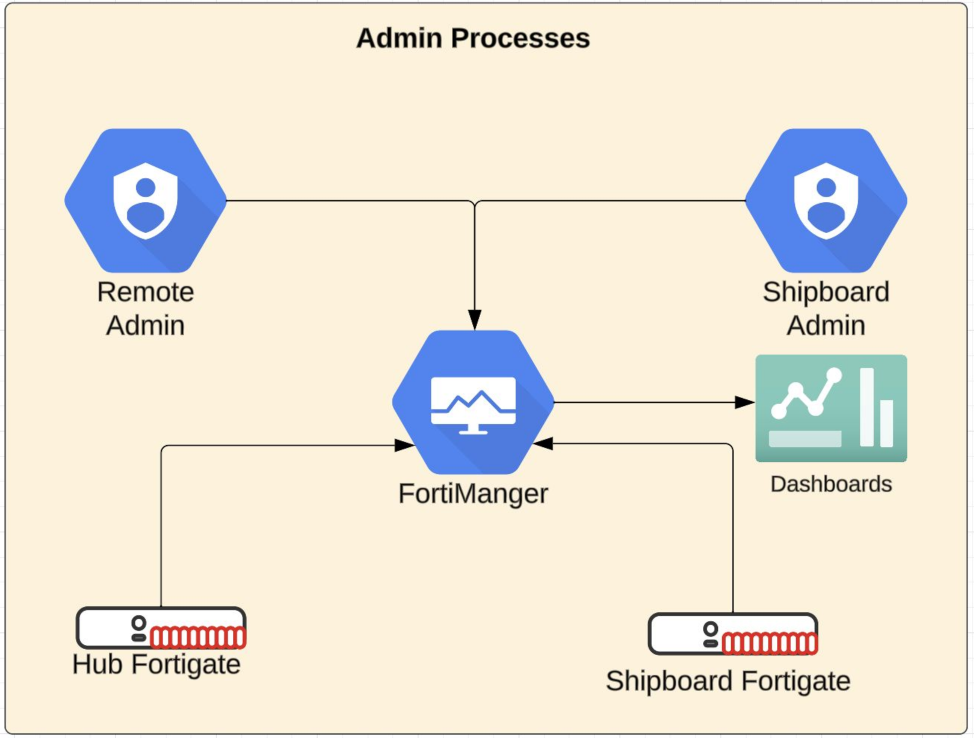
Bridge?

ECR?

Hospital?

Identity Services?

v2023-03-12
Rachel Simon



Admin Processes

Remote Admin

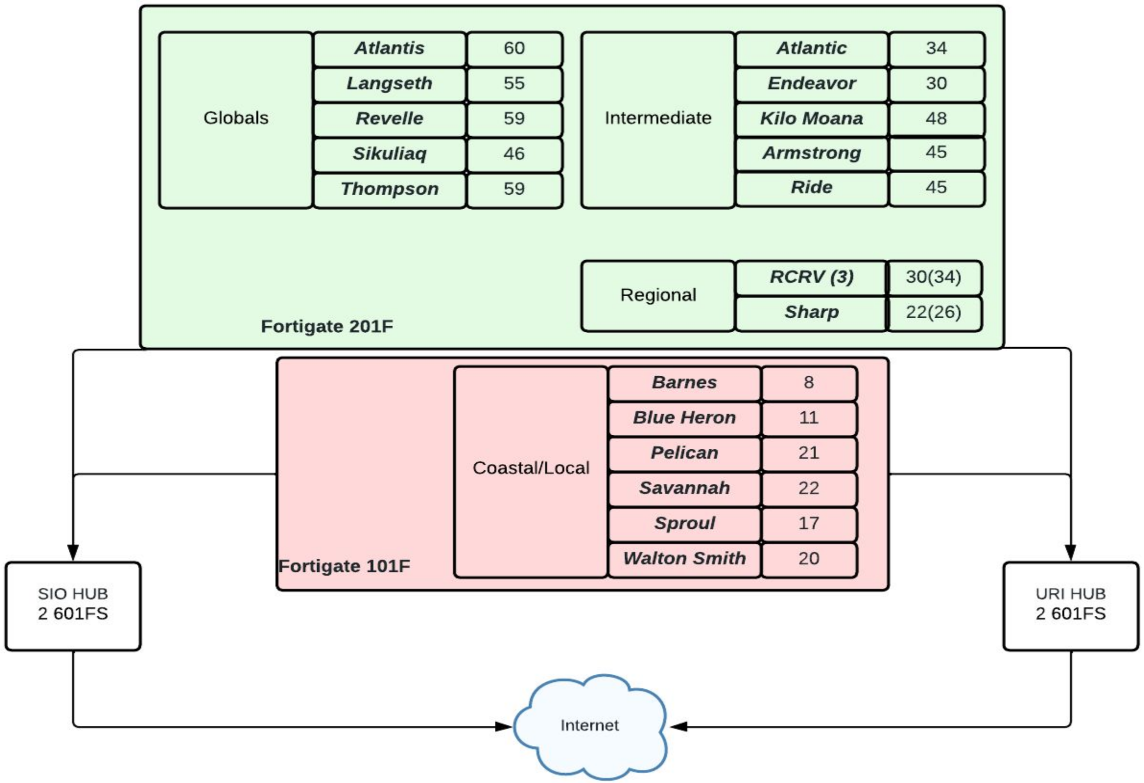
Shipboard Admin

FortiManger

Dashboards

Hub Fortigate

Shipboard Fortigate



Fortigate 201F

Globals		
	Atlantis	60
	Langseth	55
	Revelle	59
	Sikuliaq	46
	Thompson	59

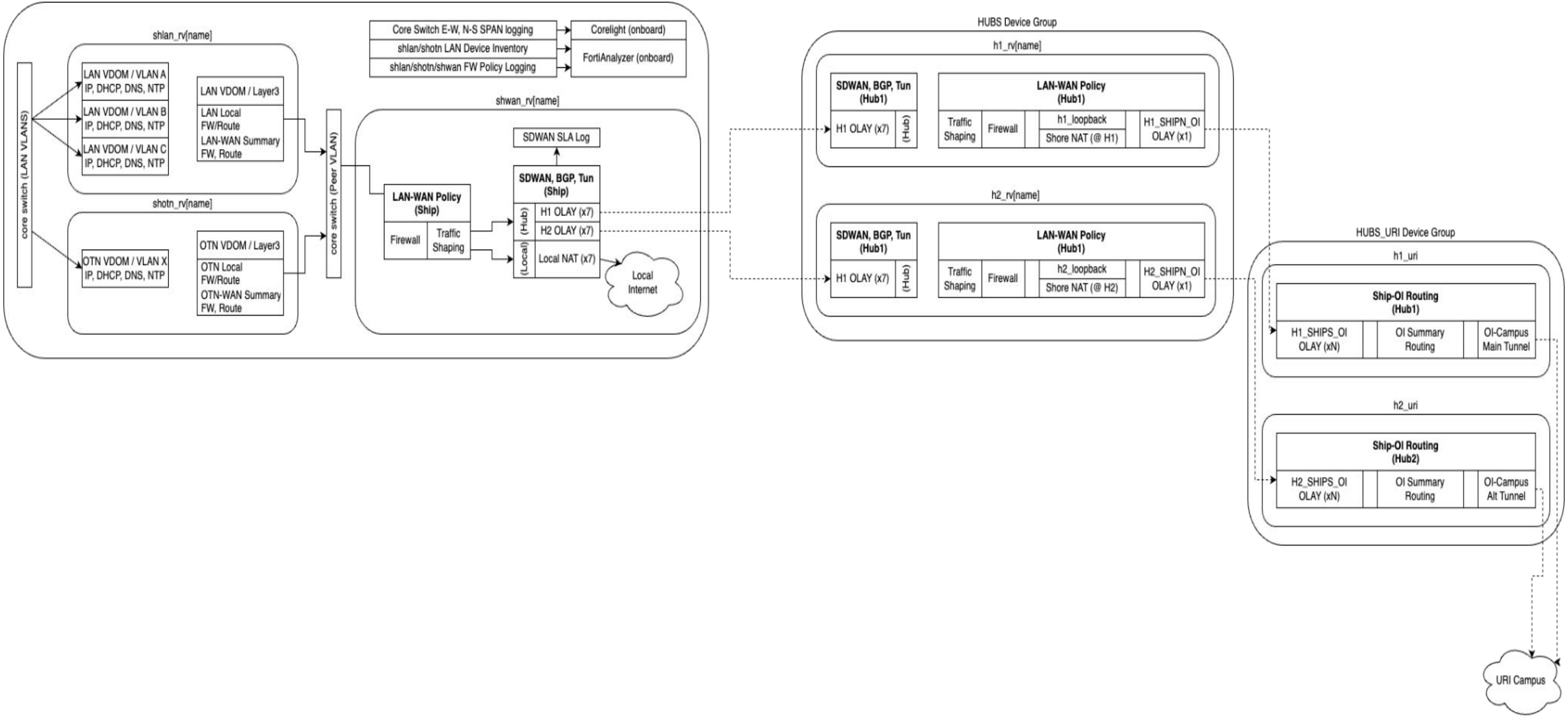
Intermediate		
	Atlantic	34
	Endeavor	30
	Kilo Moana	48
	Armstrong	45
	Ride	45

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

Fortigate 101F

Coastal/Local		
	Barnes	8
	Blue Heron	11
	Pelican	21
	Savannah	22
	Sproul	17
	Walton Smith	20

- Ships will connect to redundant hubs (SIO + URI)
- Ships retain the "failsafe" local Internet
- Each vessel will have dual devices for High Availability (HA).
- Each vessel will have a US IP address and optionally tunnel back to home institution.
- Connection will be seamless as they switch connections.
    - FX and Sealink
    - Cell and Starlink



Shoreside lab

Fortigate 61F

- Objective is to replicate specific issues that happened on Nautilus
- Prototype workflows for device management and NAC
- ISC facility has a Starlink (terrestrial) terminal for testing
- Ability to spin up Ku GEO VSAT system for testing

Complications - LAN Side

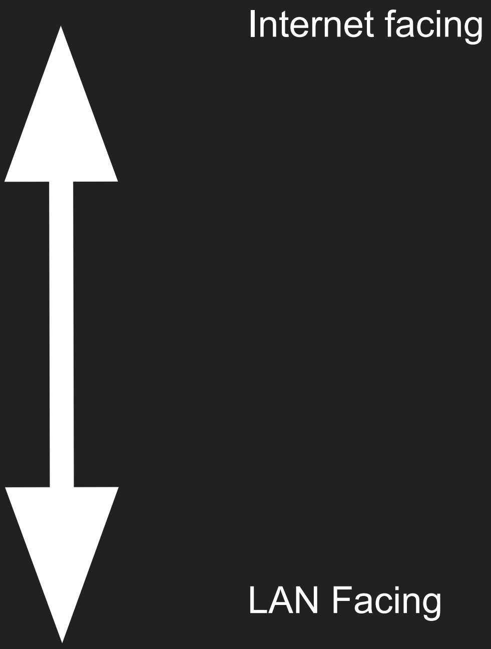
- Host institution cybersecurity/device management efforts
  - More and more institutions are rolling out client security applications and tightening policies on work laptops
  - Can cause considerable headaches when 802.1X comes into play
  - Examples that ISC has seen - UNH managed Win10 laptops
- Apple/Microsoft MAC randomization “privacy theatre”
  - “This is totally going to help keep your stuff private from Big Tech, there are no other ways to do device fingerprinting LOL” - Gus Fring Pollos Hermanos business model
- Uncrewed Systems
  - Lots of physical systems to mobilize, deck units for vessel communication take up mob time
  - Not fully operational yet - need to upload telemetry to shore office for tech support
  - Tend to create de-facto BYOD vlans outside of the ship’s normal architecture
- Device-to-device mDNS model
  - mDNS-based casting is replacing USB/HDMI cameras + displays
  - Laptop + Wifi Cam has replaced traditional rack + SDI streaming
- Active Directory
  - Comes to a question of what system provides DHCP

Hardware/Licensed components of the Fortigate system

- Hardware or VM NGFW appliance
  - Network traffic flows through here, desired policies are applied
  - Some capability for local traffic analysis
- Security Fabric
  - Single management interface for multiple NGFW appliances
  - Example - ship and shore NGFW pair, managed as one Security Fabric
    - Ship to shore policy/object/etc sync
    - Provides dashboard level overview of what's happening
  - NOTE - security fabric usage conflicts with VDOM (N virtual instances on top of 1 physical firewall) - blocks you from multi-VDOM operating mode
- FortiAnalyzer
  - Collects traffic logged by HW/VM Fortigates and runs in depth analysis
  - Needed to really use Security Fabric component
- Fortigate hardware switches and wifi AP's
  - Supports Forti's in-house 802.1X environment, ties in with FortiClient device policy enforcement
  - Consider WAN complication #1 - conflicting home institution apps…

Key components of a specific Forti NGFW instance

- Internet
  - Interface Config (Role: WAN)
  - SD-WAN member config
  - SD-WAN Rule config
  - Traffic Shaping config
  - SD-WAN Zone config
  - **Firewall policy**
  - Interface Config (Role : LAN)
- LAN
- FortiView - traffic analysis via onboard logs or FortiAnalyzer



Internet facing

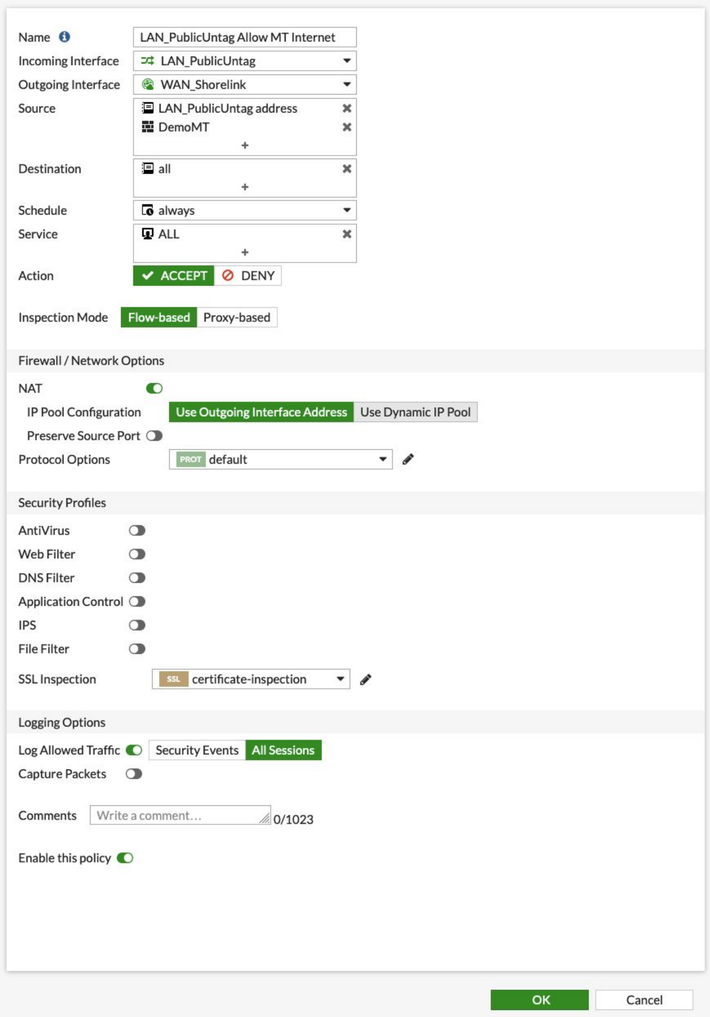
LAN Facing

Step 1: LAN interfaces / NAC

Device Management Method	Usage for BYOD	Usage for ship’s owned computers	Usage for ship’s “devices” (Apple TV, Moxa, etc)
802.1X	Home institution cybersec can cause problems	Works well	Very device-specific
Captive Portal	Works well	Can be a pain with shared accounts	No
VLAN+DHCP Reservation	Not a good option- MAC randomization	Works well for servers/workstations (marginal for desktops)	Good option

Firewall Policy

- This is VERY heavily used to configure core parts of the Forti
- Source + Destination -> can insert Address Groups, Firewall User groups here, helps to avoid tons of duplicate config
- SSL inspection configured here
- App Control/AntiVirus/IPS enabled here
- Log Allowed Traffic -> All Sessions
  - Prerequisite for WAN usage monitoring via FortiView
- Provides accounting of usage for “groups” of traffic flow



Name	LAN_PublicUntag Allow MT Internet
Incoming Interface	LAN_PublicUntag
Outgoing Interface	WAN_Shorelink
Source	LAN_PublicUntag address DemoMT
Destination	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY
Inspection Mode	[✓ Flow-based] Proxy-based

Firewall / Network Options

NAT	●
IP Pool Configuration	[✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port	○
Protocol Options	PROT default

Security Profiles

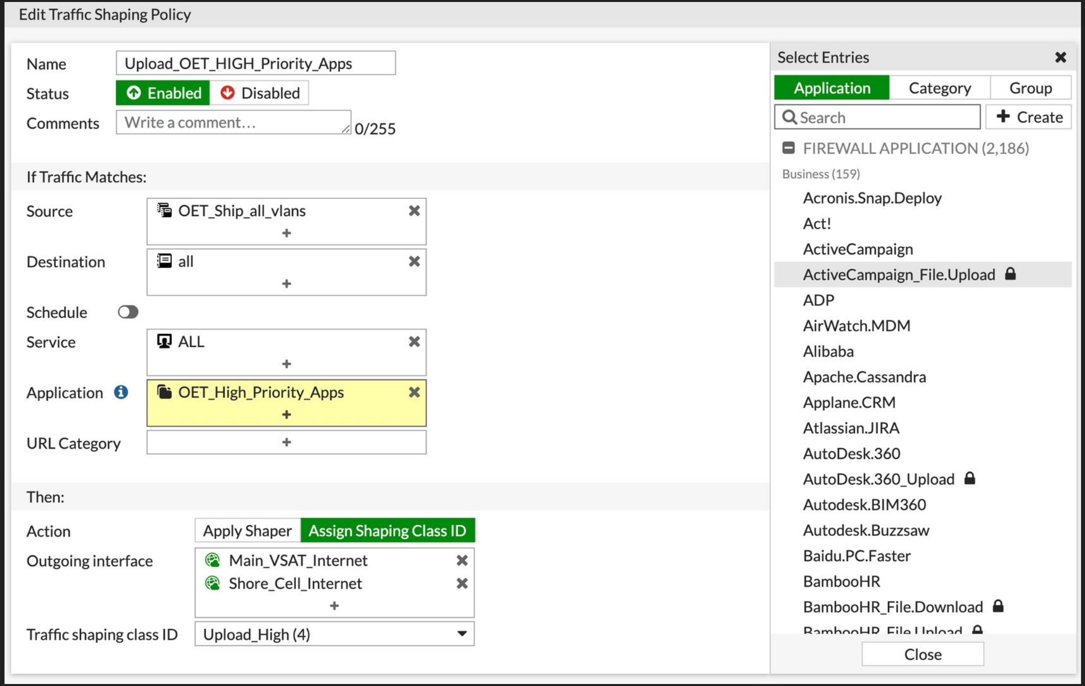
AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	○
IPS	○
File Filter	○
SSL Inspection	SSL certificate-inspection

Logging Options

Log Allowed Traffic	● Security Events [✓ All Sessions]
Capture Packets	○
Comments	Write a comment... 0/1023
Enable this policy	●

Traffic Shaping

- This particular segment was taken by one of the data engineers adding a temp policy to prioritize ASV uploads
- Uploads -> Traffic Shaping Policy, tied to interface
- Downloads -> Shared reverse shapers (limitation of ship-only topology)



Edit Traffic Shaping Policy

Name: Upload_OET_HIGH_Priority_Apps

Status: Enabled | Disabled

Comments: Write a comment... 0/255

If Traffic Matches:

Source: OET_Ship_all_vlans

Destination: all

Schedule

Service: ALL

Application: OET_High_Priority_Apps

URL Category

Then:

Action: Apply Shaper | Assign Shaping Class ID

Outgoing interface: Main_VSAT_Internet, Shore_Cell_Internet

Traffic shaping class ID: Upload_High (4)

Select Entries

Application | Category | Group

Search | Create

FIREWALL APPLICATION (2,186)

Business (159)

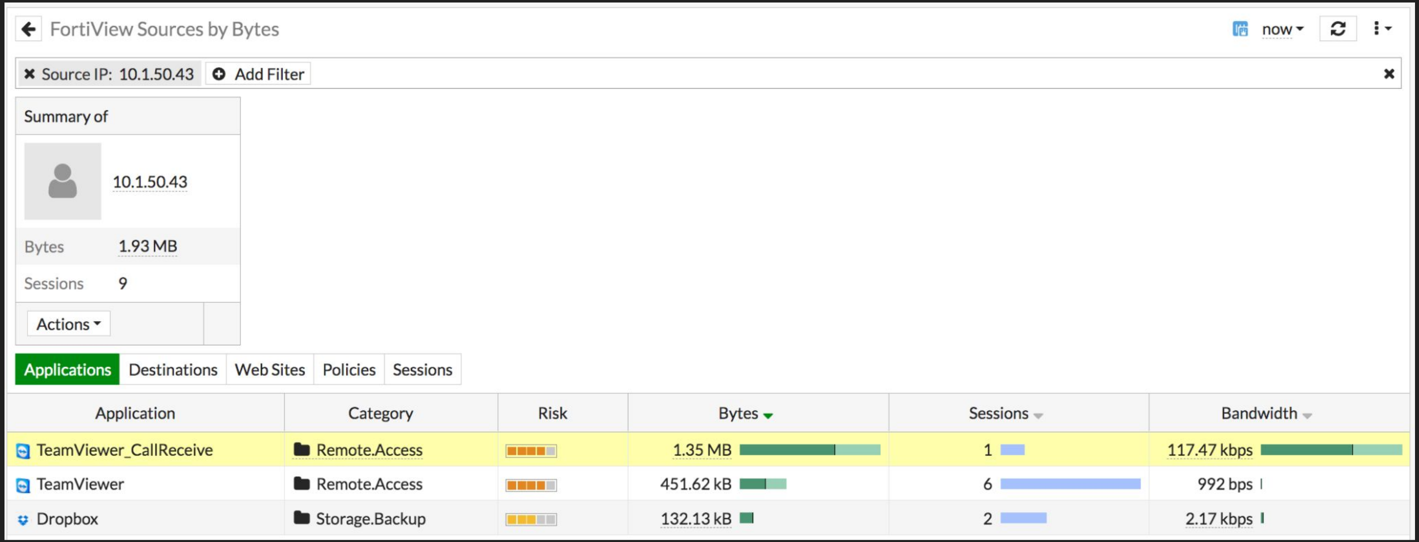
- Acronis.Snap.Deploy
- Act!
- ActiveCampaign
- ActiveCampaign_File.Upload
- ADP
- AirWatch.MDM
- Alibaba
- Apache.Cassandra
- Applane.CRM
- Atlassian.JIRA
- AutoDesk.360
- AutoDesk.360_Upload
- Autodesk.BIM360
- Autodesk.Buzzsaw
- Baidu.PC.Faster
- BambooHR
- BambooHR_File.Download
- BambooHR_File.Upload

Close

FortiView

Really needs to have BYOD devices auth through FW

Theoretically supports hostname lookup - this doesn't work well



FortiView Sources by Bytes

Source IP: 10.1.50.43 | Add Filter

Summary of

10.1.50.43

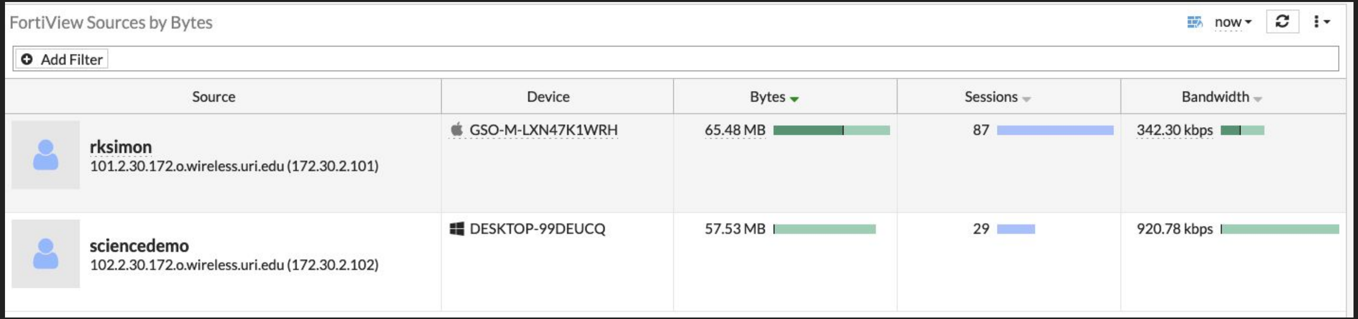
Bytes	1.93 MB
Sessions	9

Actions

Applications | Destinations | Web Sites | Policies | Sessions

Application	Category	Risk	Bytes	Sessions	Bandwidth
TeamViewer_CallReceive	Remote.Access		1.35 MB	1	117.47 kbps
TeamViewer	Remote.Access		451.62 kB	6	992 bps
Dropbox	Storage.Backup		132.13 kB	2	2.17 kbps

Hostname resolution rarely resolves in real time

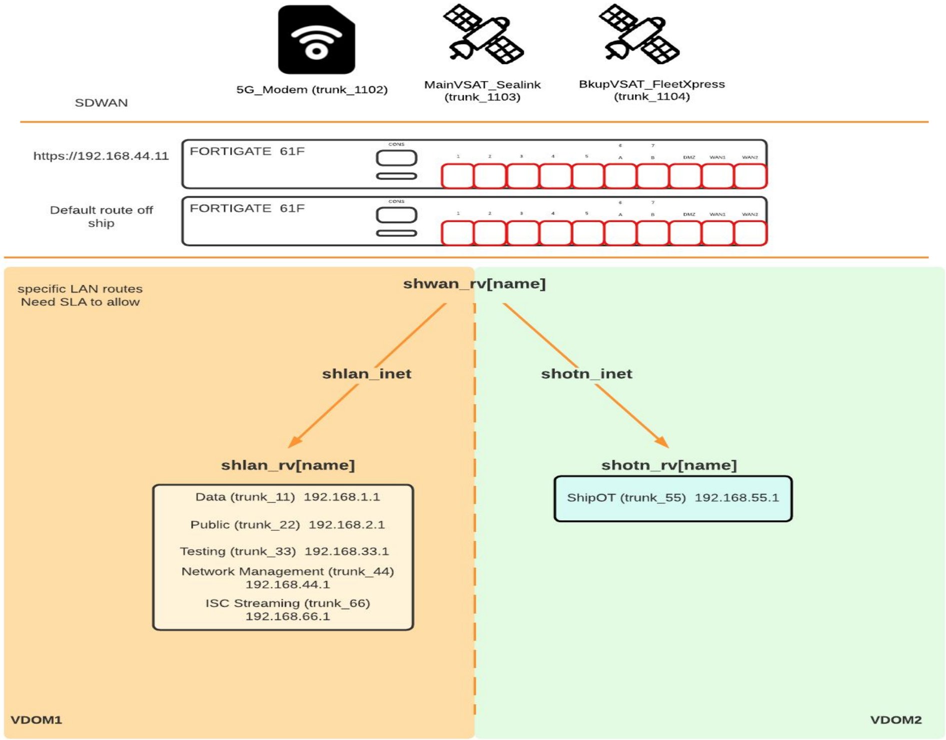


FortiView Sources by Bytes

Add Filter

Source	Device	Bytes	Sessions	Bandwidth
rksimon 101.2.30.172.o.wireless.uri.edu (172.30.2.101)	GSO-M-LXN47K1WRH	65.48 MB	87	342.30 kbps
sciencedemo 102.2.30.172.o.wireless.uri.edu (172.30.2.102)	DESKTOP-99DEUCQ	57.53 MB	29	920.78 kbps

Example - device has L2 connection/DHCP/Captive Portal through Forti



SDWAN

5G_Modem (trunk_1102)

MainVSAT_Sealink
(trunk_1103)

BkupVSAT_FleetXpress
(trunk_1104)

https://192.168.44.11

FORTIGATE 61F

Default route off
ship

FORTIGATE 61F

specific LAN routes
Need SLA to allow

shwan_rv[name]

shlan_inet

shotn_inet

shlan_rv[name]

Data (trunk_11) 192.168.1.1

Public (trunk_22) 192.168.2.1

Testing (trunk_33) 192.168.33.1

Network Management (trunk_44)
192.168.44.1

ISC Streaming (trunk_66)
192.168.66.1

shotn_rv[name]

ShipOT (trunk_55) 192.168.55.1

VDOM1

VDOM2