# The FortiReckoning

## An Introduction

# ARF CI/CS Collaborators

- **CIWG** - Cyberinfrastructure Working Group
  - Operations Focus
  - Science Focus
- **HiSeasNet**
- **SatNAG** - Satellite Network Advisory Group
- **ARF NextGen Firewall Team**
- **OmniSOC**
- **Fortinet Application Engineering**

# Cyberinfrastructure

**Next Gen Firewall**

- Opt-In Service for ARF Vessels
- Engagement by multiple ARF institutions
- Supports both Operations and Science
- Testing phase started in early 2023. First deployment on Endeavor Aug. 23.
- Hardware Procurement in process by UCSD

**Provides**

- Seamless Internet access over Multiple SatComms
- Better Security Reporting for Cybersecurity Audits and Compliance

# Next Generation Firewall Project

This next generation firewall will provide many advanced capabilities including

- Automatically prefer Starlink/5G with VSAT as fallback
- Standardized WAN monitoring, troubleshooting, and traffic shaping
- US-based IP's (no more Norwegian google!)
- Remote access for tech support
- Standard hooks for OmniSOC Services
- Ability to shape and prioritize traffic tailored to specific cruise needs

With these new capabilities ARF vessels will be much better able to detect and respond to cyber security incidents, while also providing the ability to more granularly allocate network resources to prioritize projects for Science and Operations.

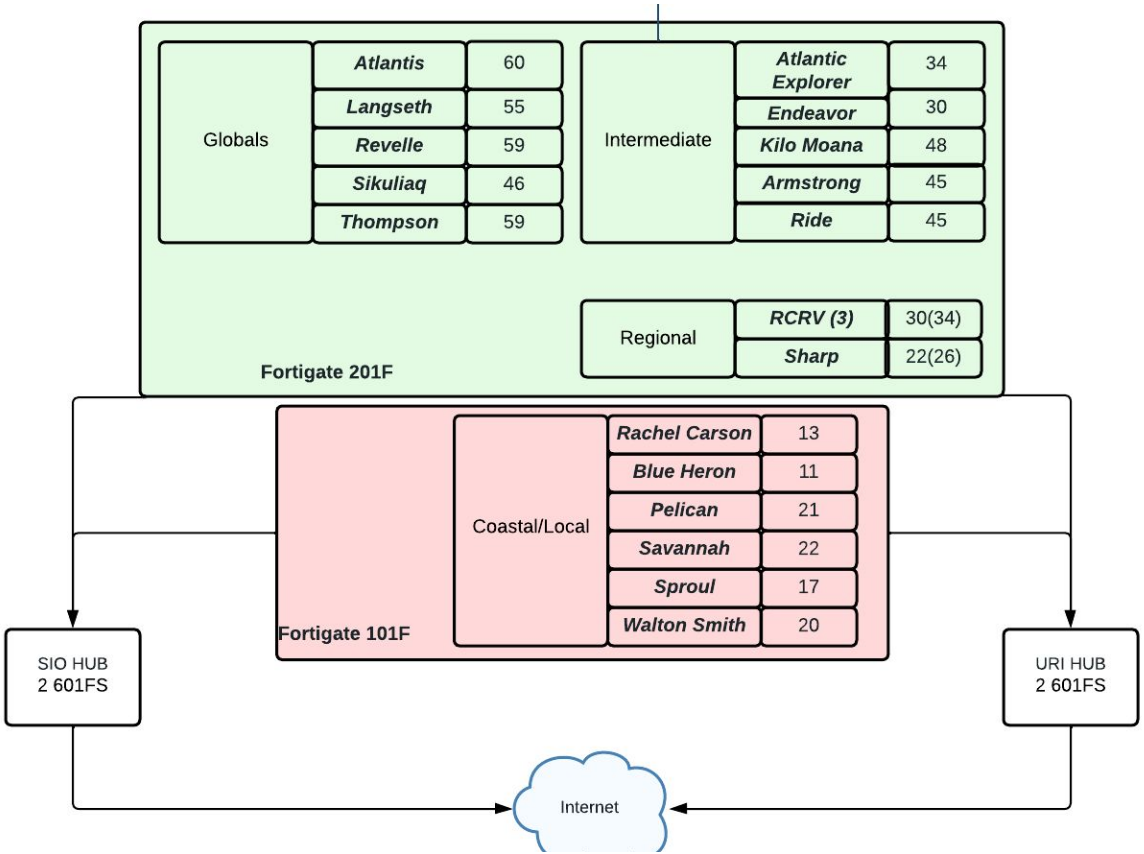
# NextGen Firewall - Why?

Cybersecurity is a core part of this project. However, we cannot continue to add compliance tasks until we simplify the existing infrastructure and tasks. If we streamline the basic infrastructure, eliminate day-to-day manual administration, and make sure our core cybersecurity objectives can run in the background, we stand the best chance of actually accomplishing these goals.

If you want to make it secure, then make security easy, and fix a couple other things while you're at it.

# NextGen Firewall -What?

- Fortigate firewalls on ship *(it slices! it dices!)*
  - Manages all WAN connections. Phones home to shore.
  - (Preferably) manages all onboard networks, although split installations with an existing router are possible.
- Fortigate firewalls at SIO/URI *(but wait, there's more!)*
  - Provides US-based IP address.
  - Can tunnel all traffic back to home institution, to provide campus addressing.
- FortiAnalyzer
  - Displays device inventory, and tracks data utilization by device
  - Handles traffic data distribution to OmniSOC (ResearchSOC)
- FortiManager
  - Handles configuration for shipboard and hub systems
  - Applies templates and manages data entry during commissioning
  - Configuration of all devices is backed up here



|  |  |  |
|---|---|---|
| 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) |
| Coastal/Local | ***Rachel Carson*** | 13 |
|  | ***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).

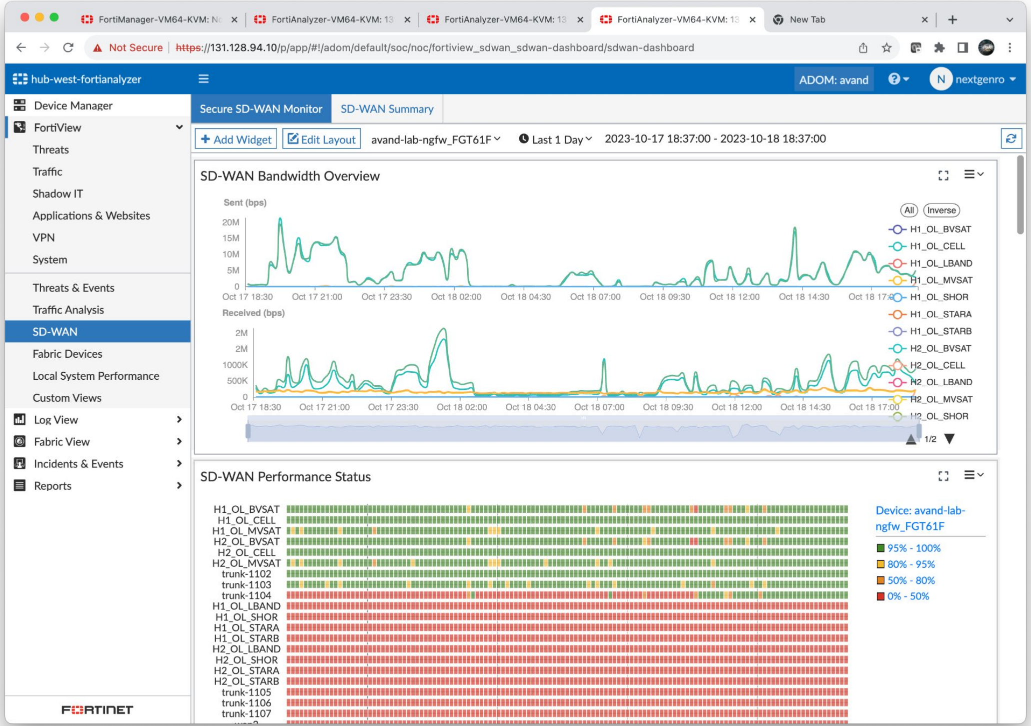
- Each vessel will have a US IP address and optionally tunnel back to home institution.

- Connection will be seamless as they switch connections.
    - FX and Sealink
    - Cell and Starlink

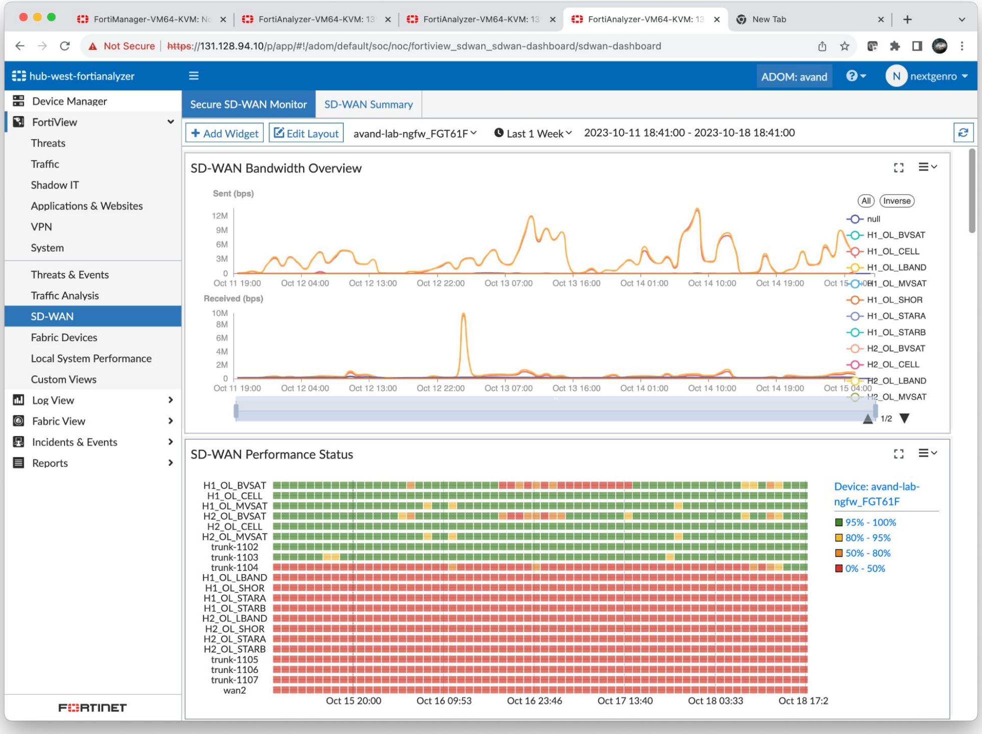
# NextGen Firewall - How?

- Endeavor had a very favorable schedule in Summer/Fall 2023
- Built mirror of Endeavor network with WAN emulation
  - 10 Test and refine in the lab
  - 20 Implement on Endeavor
  - 30 Training for MT's
  - 40 Debrief after operations
  - 50 GOTO 10
- Make design updates, template changes, and write scripts based upon most recent experience. Each installation should get progressively easier.
- **Commissioning should not be a root canal**.
  - Fortigates brought up in parallel with existing network and tested
  - Shipboard network flash-cut over so downtime was not noticeable
  - **Faster than EK80 install with only 10% of the profanity**

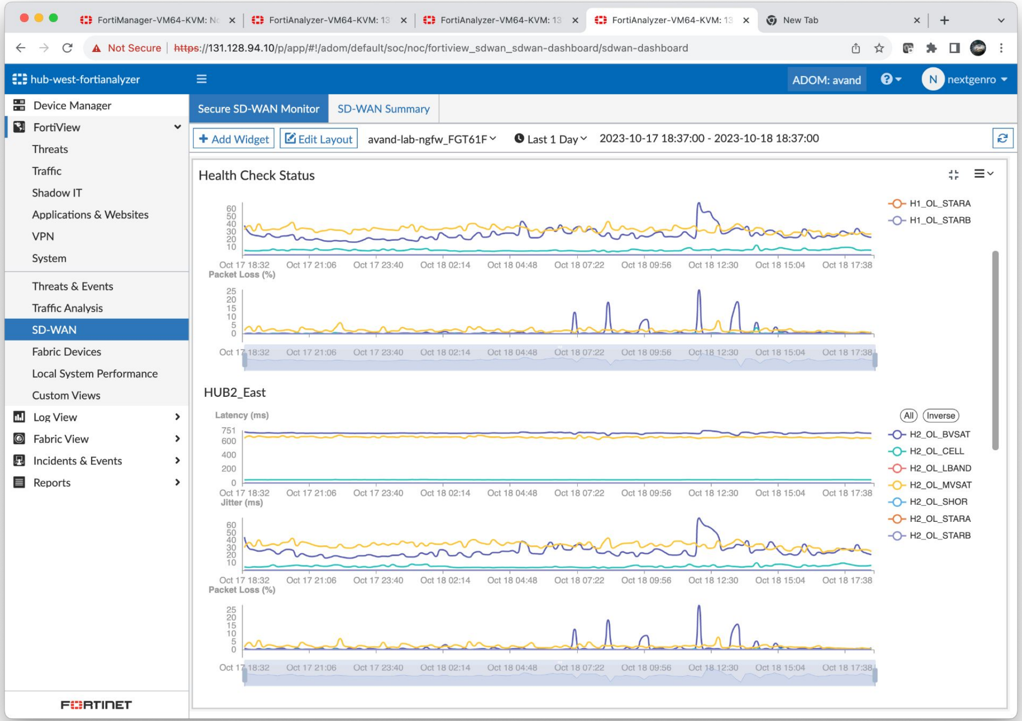
# WAN Usage and Connection Quality Last 24-hours



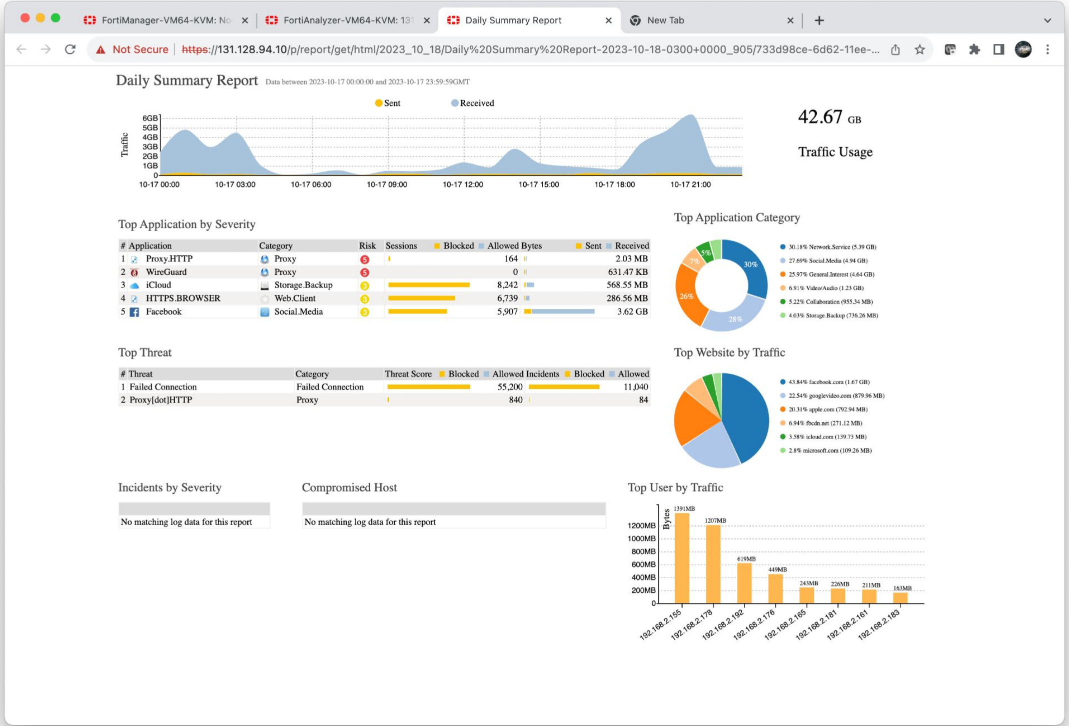
# WAN Usage and Connection Quality Last Week



# Connection Health to the Shore HUBs



# Daily Summary Report


FortiManager-VM64-KVM: No
FortiAnalyzer-VM64-KVM: 13
Daily Summary Report
New Tab
Not Secure
https://131.128.94.10/p/report/get/html/2023_10_18/Daily%20Summary%20Report-2023-10-18-0300+0000_905/733d98ce-6d62-11ee-...

## Daily Summary Report

Data between 2023-10-17 00:00:00 and 2023-10-17 23:59:59GMT

● Sent
● Received
Traffic
6GB
5GB
4GB
3GB
2GB
1GB
0
10-17 00:00
10-17 03:00
10-17 06:00
10-17 09:00
10-17 12:00
10-17 15:00
10-17 18:00
10-17 21:00

42.67 GB

Traffic Usage

### Top Application by Severity

| # | Application | Category | Risk | Sessions ■ Blocked ■ Allowed | Bytes ■ Sent ■ Received |
|---|---|---|---|---|---|
| 1 | Proxy.HTTP | Proxy | 5 | 164 | 2.03 MB |
| 2 | WireGuard | Proxy | 5 | 0 | 631.47 KB |
| 3 | iCloud | Storage.Backup | 3 | 8,242 | 568.55 MB |
| 4 | HTTPS.BROWSER | Web.Client | 3 | 6,739 | 286.56 MB |
| 5 | Facebook | Social.Media | 3 | 5,907 | 3.62 GB |

### Top Application Category

- ● 30.18% Network.Service (5.39 GB)
- ● 27.69% Social.Media (4.94 GB)
- ● 25.97% General.Interest (4.64 GB)
- ● 6.91% Video/Audio (1.23 GB)
- ● 5.22% Collaboration (955.34 MB)
- ● 4.03% Storage.Backup (736.26 MB)

### Top Threat

| # | Threat | Category | Threat Score ■ Blocked ■ Allowed | Incidents ■ Blocked ■ Allowed |
|---|---|---|---|---|
| 1 | Failed Connection | Failed Connection | 55,200 | 11,040 |
| 2 | Proxy[dot]HTTP | Proxy | 840 | 84 |

### Top Website by Traffic

- ● 43.84% facebook.com (1.67 GB)
- ● 22.54% googlevideo.com (879.96 MB)
- ● 20.31% apple.com (792.94 MB)
- ● 6.94% fbcdn.net (271.12 MB)
- ● 3.58% icloud.com (139.73 MB)
- ● 2.8% microsoft.com (109.26 MB)

### Incidents by Severity

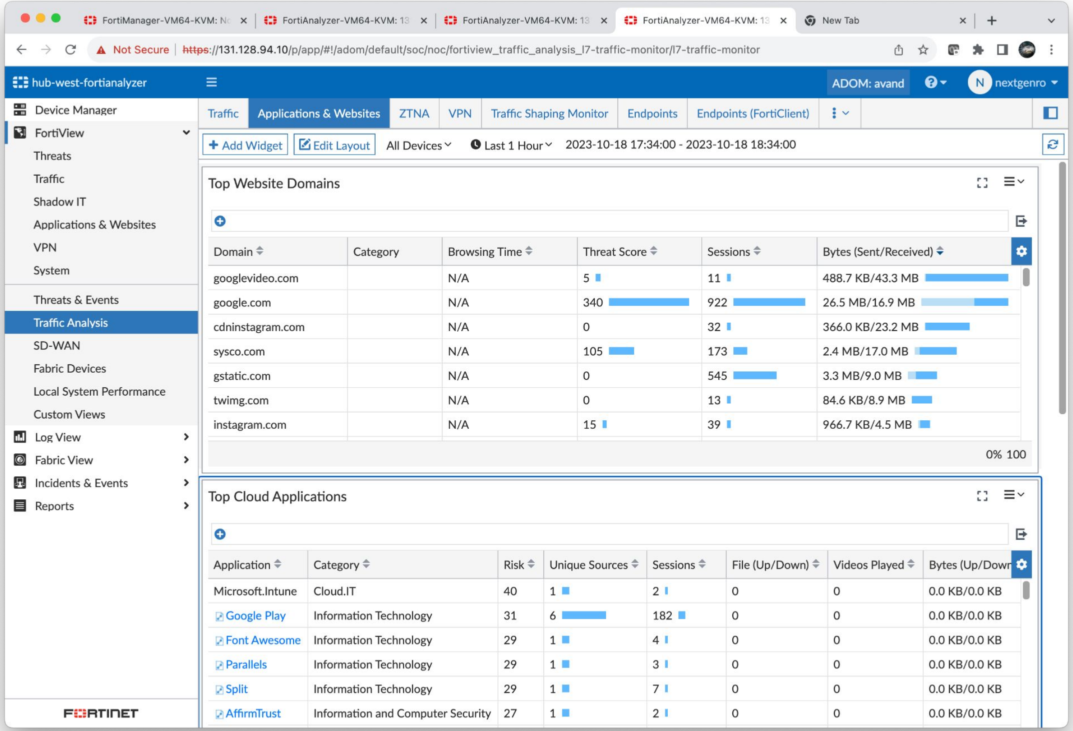
No matching log data for this report

### Compromised Host

No matching log data for this report

### Top User by Traffic

# Traffic Analysis Example



2023-10-18 17:34:00 - 2023-10-18 18:34:00

## Top Website Domains

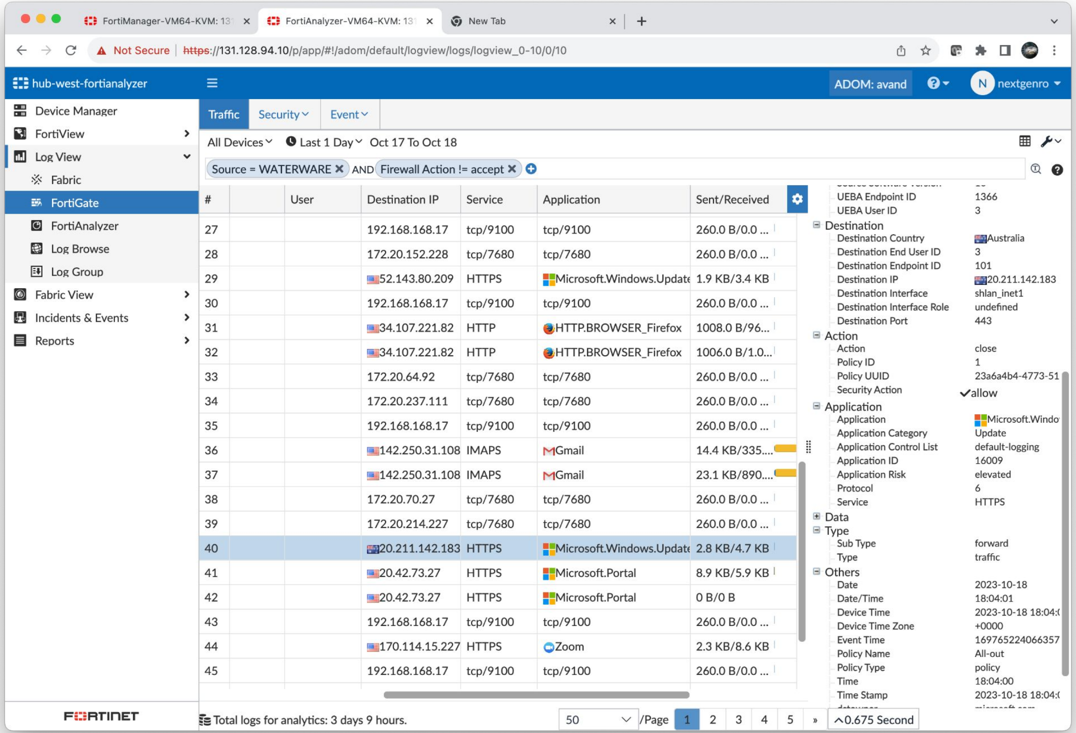
| Domain | Category | Browsing Time | Threat Score | Sessions | Bytes (Sent/Received) |
|---|---|---|---|---|---|
| googlevideo.com | | N/A | 5 | 11 | 488.7 KB/43.3 MB |
| google.com | | N/A | 340 | 922 | 26.5 MB/16.9 MB |
| cdninstagram.com | | N/A | 0 | 32 | 366.0 KB/23.2 MB |
| sysco.com | | N/A | 105 | 173 | 2.4 MB/17.0 MB |
| gstatic.com | | N/A | 0 | 545 | 3.3 MB/9.0 MB |
| twimg.com | | N/A | 0 | 13 | 84.6 KB/8.9 MB |
| instagram.com | | N/A | 15 | 39 | 966.7 KB/4.5 MB |

0% 100

## Top Cloud Applications

| Application | Category | Risk | Unique Sources | Sessions | File (Up/Down) | Videos Played | Bytes (Up/Down |
|---|---|---|---|---|---|---|---|
| Microsoft.Intune | Cloud.IT | 40 | 1 | 2 | 0 | 0 | 0.0 KB/0.0 KB |
| Google Play | Information Technology | 31 | 6 | 182 | 0 | 0 | 0.0 KB/0.0 KB |
| Font Awesome | Information Technology | 29 | 1 | 4 | 0 | 0 | 0.0 KB/0.0 KB |
| Parallels | Information Technology | 29 | 1 | 3 | 0 | 0 | 0.0 KB/0.0 KB |
| Split | Information Technology | 29 | 1 | 7 | 0 | 0 | 0.0 KB/0.0 KB |
| AffirmTrust | Information and Computer Security | 27 | 1 | 2 | 0 | 0 | 0.0 KB/0.0 KB |

# Traffic to/from a specific host



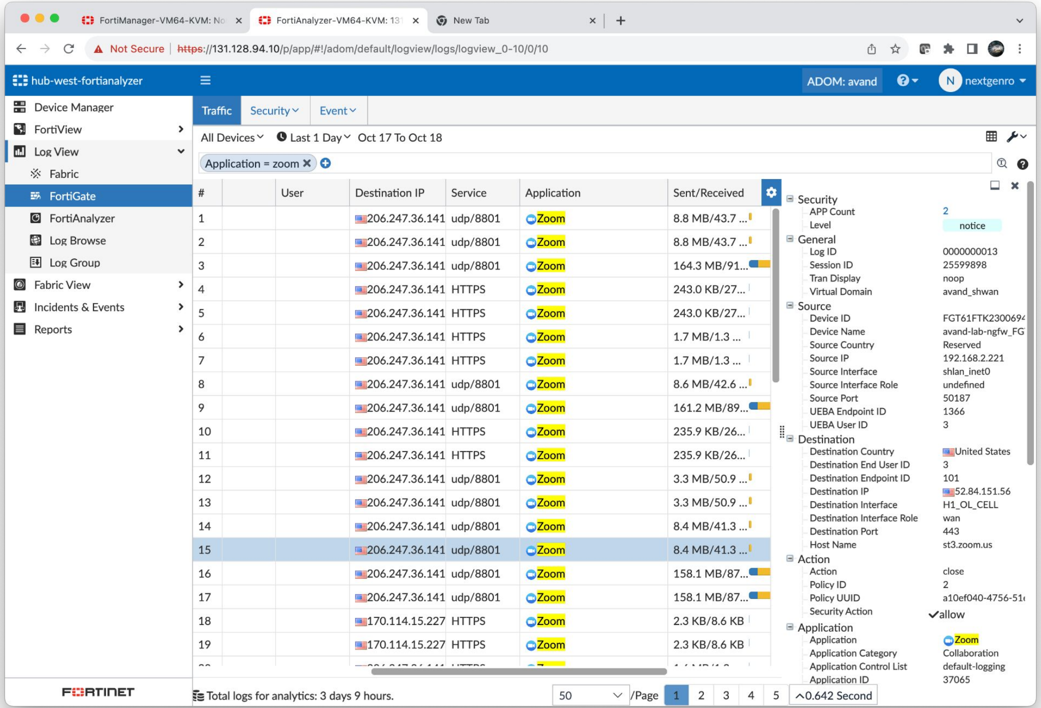
Source = WATERWARE ✕ AND Firewall Action != accept ✕

| # | | User | Destination IP | Service | Application | Sent/Received |
|---|---|---|---|---|---|---|
| 27 | | | 192.168.168.17 | tcp/9100 | tcp/9100 | 260.0 B/0.0 ... |
| 28 | | | 172.20.152.228 | tcp/7680 | tcp/7680 | 260.0 B/0.0 ... |
| 29 | | | 52.143.80.209 | HTTPS | Microsoft.Windows.Update | 1.9 KB/3.4 KB |
| 30 | | | 192.168.168.17 | tcp/9100 | tcp/9100 | 260.0 B/0.0 ... |
| 31 | | | 34.107.221.82 | HTTP | HTTP.BROWSER_Firefox | 1008.0 B/96... |
| 32 | | | 34.107.221.82 | HTTP | HTTP.BROWSER_Firefox | 1006.0 B/1.0... |
| 33 | | | 172.20.64.92 | tcp/7680 | tcp/7680 | 260.0 B/0.0 ... |
| 34 | | | 172.20.237.111 | tcp/7680 | tcp/7680 | 260.0 B/0.0 ... |
| 35 | | | 192.168.168.17 | tcp/9100 | tcp/9100 | 260.0 B/0.0 ... |
| 36 | | | 142.250.31.108 | IMAPS | Gmail | 14.4 KB/335.... |
| 37 | | | 142.250.31.108 | IMAPS | Gmail | 23.1 KB/890.... |
| 38 | | | 172.20.70.27 | tcp/7680 | tcp/7680 | 260.0 B/0.0 ... |
| 39 | | | 172.20.214.227 | tcp/7680 | tcp/7680 | 260.0 B/0.0 ... |
| 40 | | | 20.211.142.183 | HTTPS | Microsoft.Windows.Update | 2.8 KB/4.7 KB |
| 41 | | | 20.42.73.27 | HTTPS | Microsoft.Portal | 8.9 KB/5.9 KB |
| 42 | | | 20.42.73.27 | HTTPS | Microsoft.Portal | 0 B/0 B |
| 43 | | | 192.168.168.17 | tcp/9100 | tcp/9100 | 260.0 B/0.0 ... |
| 44 | | | 170.114.15.227 | HTTPS | Zoom | 2.3 KB/8.6 KB |
| 45 | | | 192.168.168.17 | tcp/9100 | tcp/9100 | 260.0 B/0.0 ... |

| | |
|---|---|
| UEBA Endpoint ID | 1366 |
| UEBA User ID | 3 |
| **Destination** | |
| Destination Country | Australia |
| Destination End User ID | 3 |
| Destination Endpoint ID | 101 |
| Destination IP | 20.211.142.183 |
| Destination Interface | shlan_inet1 |
| Destination Interface Role | undefined |
| Destination Port | 443 |
| **Action** | |
| Action | close |
| Policy ID | 1 |
| Policy UUID | 23a6a4b4-4773-51 |
| Security Action | ✓allow |
| **Application** | |
| Application | Microsoft.Windo |
| Application Category | Update |
| Application Control List | default-logging |
| Application ID | 16009 |
| Application Risk | elevated |
| Protocol | 6 |
| Service | HTTPS |
| **Data** | |
| **Type** | |
| Sub Type | forward |
| Type | traffic |
| **Others** | |
| Date | 2023-10-18 |
| Date/Time | 18:04:01 |
| Device Time | 2023-10-18 18:04:( |
| Device Time Zone | +0000 |
| Event Time | 169765224066357 |
| Policy Name | All-out |
| Policy Type | policy |
| Time | 18:04:00 |
| Time Stamp | 2023-10-18 18:04:( |

Total logs for analytics: 3 days 9 hours.

# Traffic for a Specific Application



Application = zoom

| # | | User | Destination IP | Service | Application | Sent/Received |
|---|---|---|---|---|---|---|
| 1 | | | 206.247.36.141 | udp/8801 | Zoom | 8.8 MB/43.7 ... |
| 2 | | | 206.247.36.141 | udp/8801 | Zoom | 8.8 MB/43.7 ... |
| 3 | | | 206.247.36.141 | udp/8801 | Zoom | 164.3 MB/91... |
| 4 | | | 206.247.36.141 | HTTPS | Zoom | 243.0 KB/27... |
| 5 | | | 206.247.36.141 | HTTPS | Zoom | 243.0 KB/27... |
| 6 | | | 206.247.36.141 | HTTPS | Zoom | 1.7 MB/1.3 ... |
| 7 | | | 206.247.36.141 | HTTPS | Zoom | 1.7 MB/1.3 ... |
| 8 | | | 206.247.36.141 | udp/8801 | Zoom | 8.6 MB/42.6 ... |
| 9 | | | 206.247.36.141 | udp/8801 | Zoom | 161.2 MB/89... |
| 10 | | | 206.247.36.141 | HTTPS | Zoom | 235.9 KB/26... |
| 11 | | | 206.247.36.141 | HTTPS | Zoom | 235.9 KB/26... |
| 12 | | | 206.247.36.141 | udp/8801 | Zoom | 3.3 MB/50.9 ... |
| 13 | | | 206.247.36.141 | udp/8801 | Zoom | 3.3 MB/50.9 ... |
| 14 | | | 206.247.36.141 | udp/8801 | Zoom | 8.4 MB/41.3 ... |
| 15 | | | 206.247.36.141 | udp/8801 | Zoom | 8.4 MB/41.3 ... |
| 16 | | | 206.247.36.141 | udp/8801 | Zoom | 158.1 MB/87... |
| 17 | | | 206.247.36.141 | udp/8801 | Zoom | 158.1 MB/87... |
| 18 | | | 170.114.15.227 | HTTPS | Zoom | 2.3 KB/8.6 KB |
| 19 | | | 170.114.15.227 | HTTPS | Zoom | 2.3 KB/8.6 KB |

Total logs for analytics: 3 days 9 hours.

50 /Page 1 2 3 4 5 ^0.642 Second

Security

| | |
|---|---|
| APP Count | 2 |
| Level | notice |

General

| | |
|---|---|
| Log ID | 0000000013 |
| Session ID | 25599898 |
| Tran Display | noop |
| Virtual Domain | avand_shwan |

Source

| | |
|---|---|
| Device ID | FGT61FTK230069 |
| Device Name | avand-lab-ngfw_FG |
| Source Country | Reserved |
| Source IP | 192.168.2.221 |
| Source Interface | shlan_inet0 |
| Source Interface Role | undefined |
| Source Port | 50187 |
| UEBA Endpoint ID | 1366 |
| UEBA User ID | 3 |

Destination

| | |
|---|---|
| Destination Country | United States |
| Destination End User ID | 3 |
| Destination Endpoint ID | 101 |
| Destination IP | 52.84.151.56 |
| Destination Interface | H1_OL_CELL |
| Destination Interface Role | wan |
| Destination Port | 443 |
| Host Name | st3.zoom.us |

Action

| | |
|---|---|
| Action | close |
| Policy ID | 2 |
| Policy UUID | a10ef040-4756-51 |
| Security Action | ✓allow |

Application

| | |
|---|---|
| Application | Zoom |
| Application Category | Collaboration |
| Application Control List | default-logging |
| Application ID | 37065 |

# In the Process for Support

- Community Feedback
  - What are the biggest networking related things you are frustrated with?
  - What are the biggest day-to-day frustrations you have?
  - What would make it easier to get through the field season?
- Wiki/YouTube/Training Resources
  - What are the key items to be familiar with?
  - Previous FortiTraining Reference slides will be available.
  - What pre-cruise cyberinfrastructure questions are typically asked before mobilization?
  - What issues have come up at sea?
- Feature Requests - what are we missing?
- Installation + Technical Support
  - Procedures, scripts, troubleshooting guides

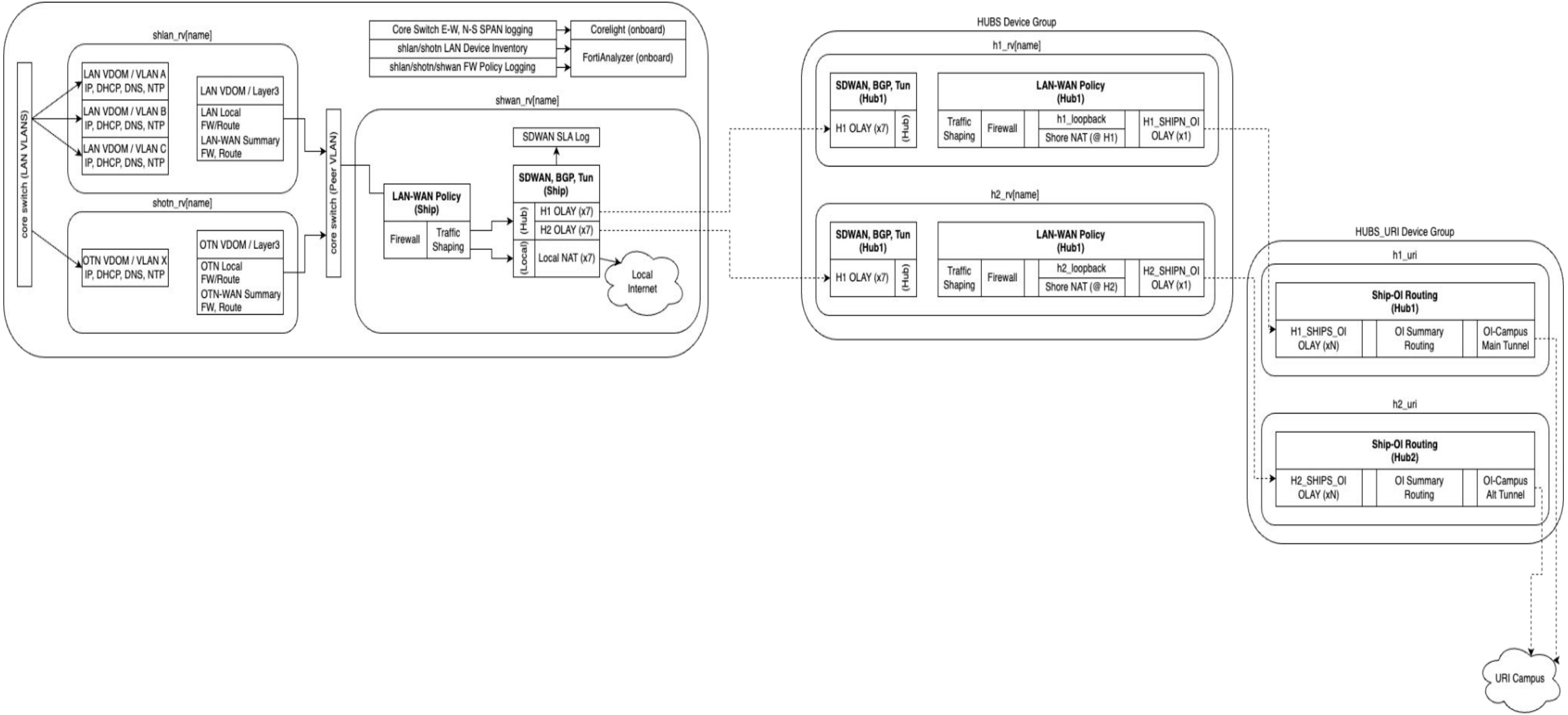
# Thank You!

## Questions?

## Thoughts?

## Suggestions?

# Additional Reference Slides



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

Corelight (onboard)

FortiAnalyzer (onboard)

shwan_rv[name]

LAN-WAN Policy
(Ship)

Firewall

Traffic Shaping

SDWAN SLA Log

SDWAN, BGP, Tun
(Ship)

(Hub)

H1 OLAY (x7)

H2 OLAY (x7)

(Local)

Local NAT (x7)

Local Internet

HUBS Device Group

h1_rv[name]

SDWAN, BGP, Tun
(Hub1)

H1 OLAY (x7)

(Hub)

LAN-WAN Policy
(Hub1)

Traffic Shaping

Firewall

h1_loopback

Shore NAT (@ H1)

H1_SHIPN_OI OLAY (x1)

h2_rv[name]

SDWAN, BGP, Tun
(Hub1)

H1 OLAY (x7)

(Hub)

LAN-WAN Policy
(Hub1)

Traffic Shaping

Firewall

h2_loopback

Shore NAT (@ H2)

H2_SHIPN_OI OLAY (x1)

HUBS_URI Device Group

h1_uri

Ship-OI Routing
(Hub1)

H1_SHIPS_OI OLAY (xN)

OI Summary Routing

OI-Campus Main Tunnel

h2_uri

Ship-OI Routing
(Hub2)

H2_SHIPS_OI OLAY (xN)

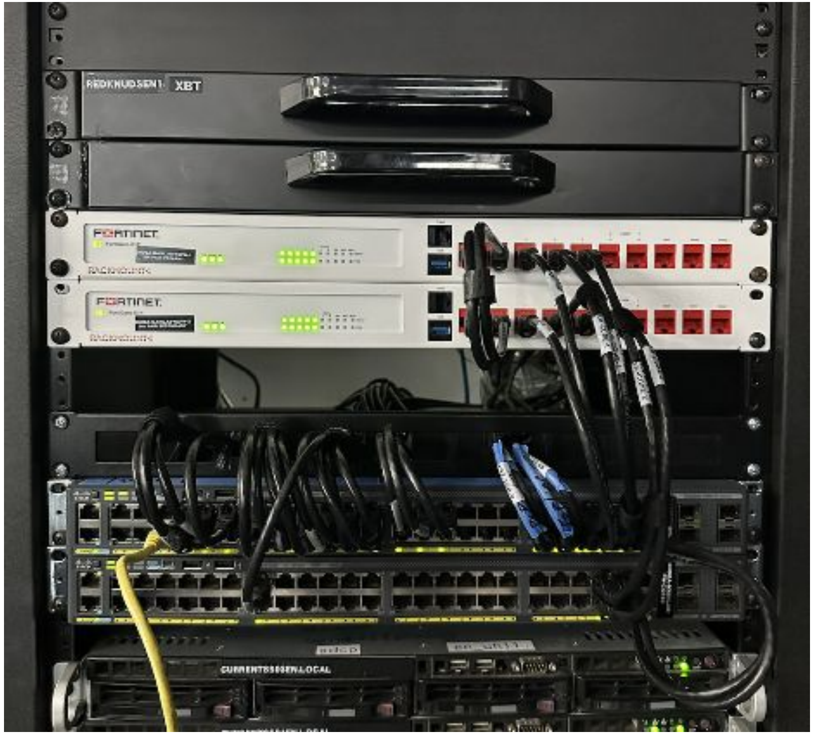
OI Summary Routing

OI-Campus Alt Tunnel

URI Campus

# R/V Endeavor Install

- Fortigate 61F HA Pair
  - Local SSD used for logging/analysis
  - DHCP, DNS
- Forti manages all WAN connections
- Forti manages the LAN
  - DHCP + Device Inventory
  - Local DNS
- Works with non-Fortinet hardware
  - Cisco switches
  - Ubiquiti Wifi AP's
  - (Adding) Active Directory



# RVTEC Cyber Monday

During the afternoon of Cyber Monday

- discuss the goals of the next generation firewall project
- reference architecture,
- day to day tasks,
- WAN management,
- tracking connection,  and
- lessons learned from the Endeavor install.

In the second session we will delve into

- firewall rules, configuration best practices,
- VLAN and VDOM creation, rationale for VLANs and VDOMs,
- troubleshooting WAN connections.

# FortiTraining References

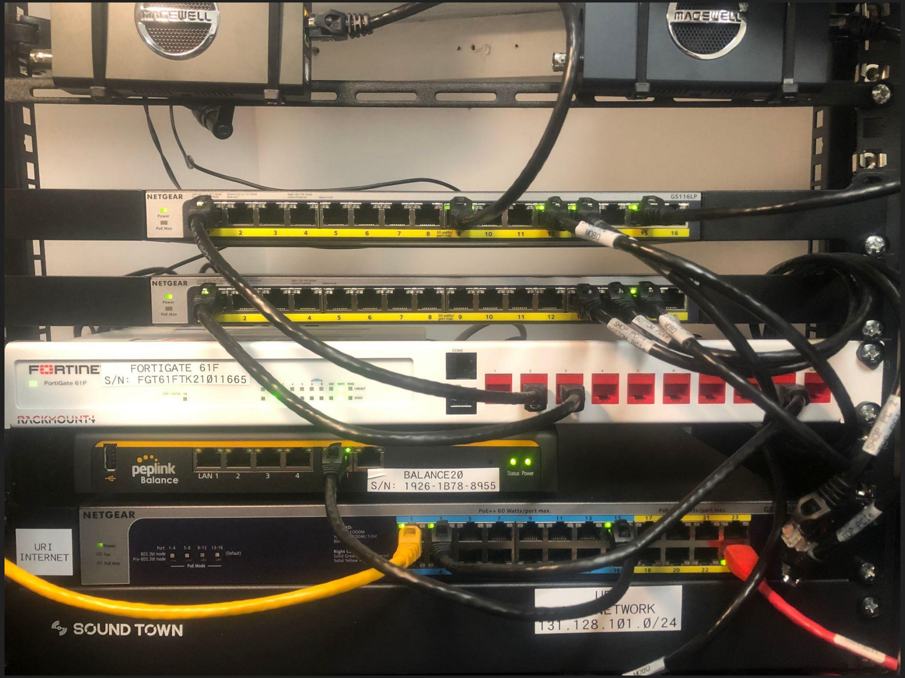
- WAN usage and status (current upload/download, historical, WAN quality)
- Temp-banning devices using excessive amounts of internet beans
- Inventory - DHCP tracking - hostname associated with a given IP
- LAN side firewall rules
- LAN versus WAN VDOMs
- Manually enabling/disabling WAN connections

Questions and asks from Techs on Endeavor, will delve into more detail during Cyber Monday of RVTEC

# 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

# Endeavor Architecture and Testing

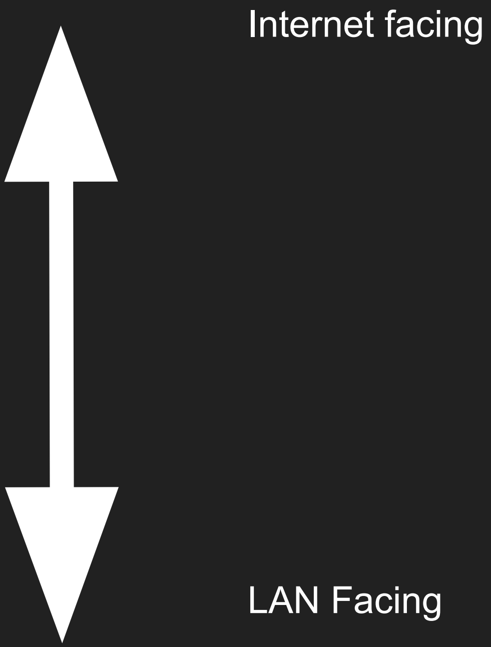
- Endeavor "ship-only" install done in August, successful cruises Aug/Sept
  - EN710 - NRT CTD data to shore for QA
  - Moved all LAN/WAN functions into Fortigates
  - Local Internet access (no hub just yet)
  - Began to test over-the-air log workflows for OmniSOC integration
  - Developed install scripts to automate data entry
- Ship + Hub bench testing late Aug - September
  - Set up shoreside copy of Endeavor infrastructure
  - Simulated latency + bandwidth limits to work out performance issues before install on ship
  - Test failover between hub sites, and failure of both hubs
- Endeavor hub install October 1st - 12th
  - Apply templates refined during bench testing
  - Will route all traffic via hub w/ US IP address
- To RVTEC and Beyond!
  - EN711 short (outreach)  cruise - David Smith/RI Teachers At Sea - October 13th through 18th.
  - Next science cruise w/ the hub would be EN712 Nov ~1st through 8th

# 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

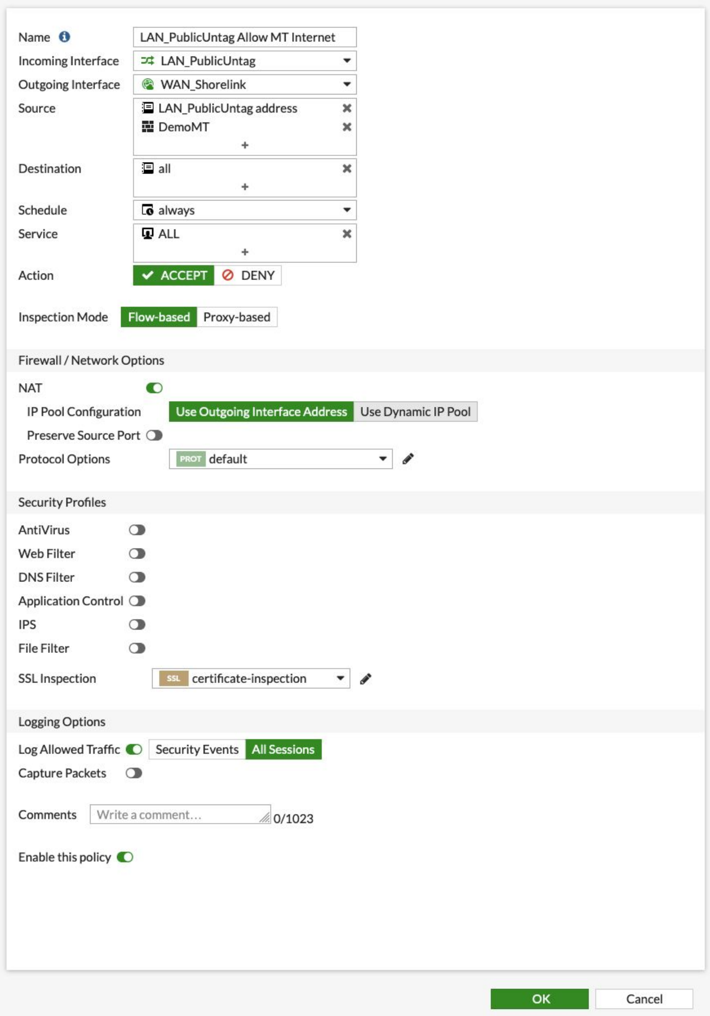
LAN Facing

# 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<br>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

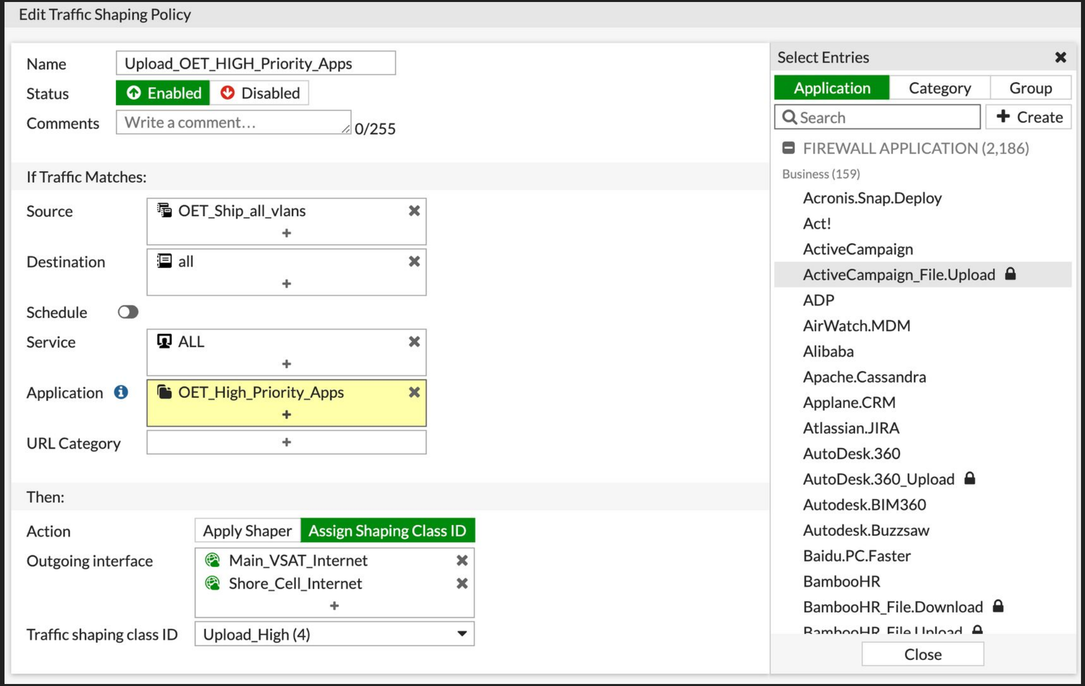
| | |
|---|---|
| AntiVirus | ○ |
| Web Filter | ○ |
| DNS Filter | ○ |
| Application Control | ○ |
| IPS | ○ |
| File Filter | ○ |
| SSL Inspection | SSL certificate-inspection |

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

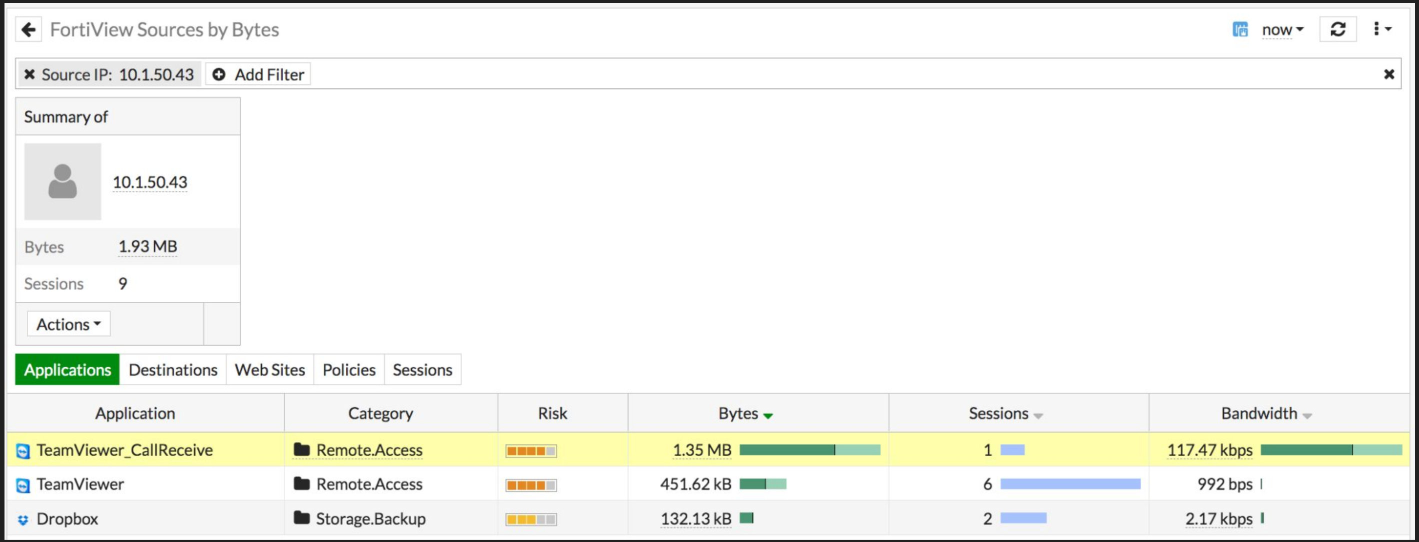
Outgoing interface: Main_VSAT_Internet, Shore_Cell_Internet

Traffic shaping class ID: Upload_High (4)

# 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

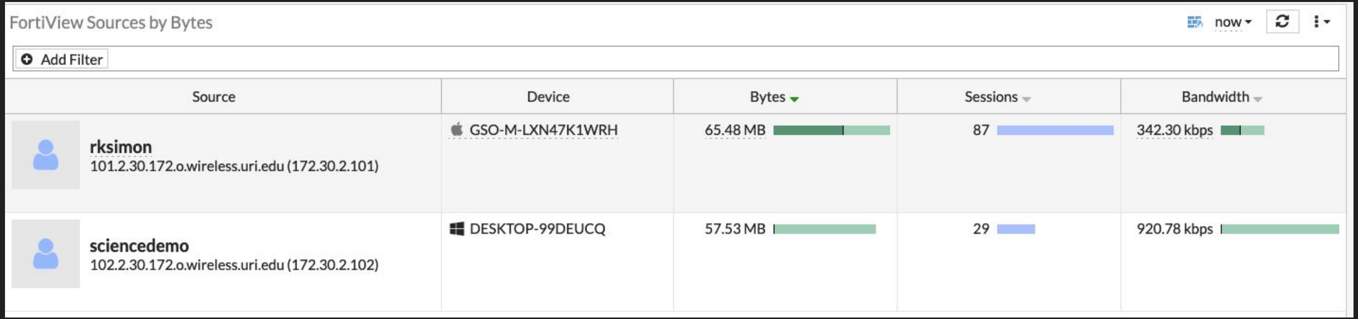
| | |
|---|---|
| Bytes | 1.93 MB |
| Sessions | 9 |

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

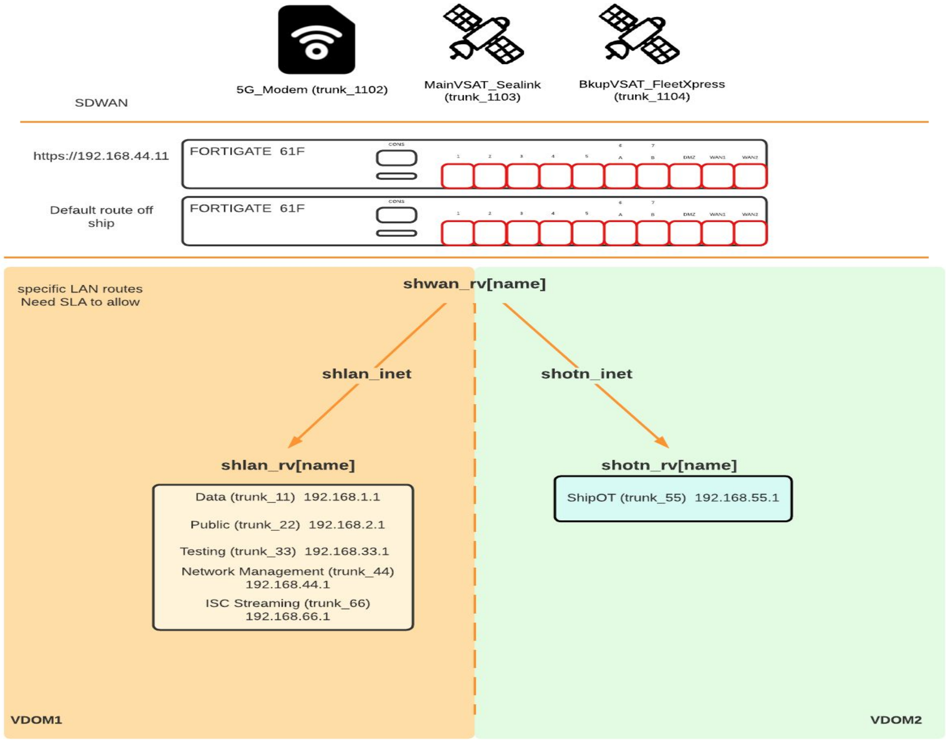


FortiView Sources by Bytes

Add Filter

| Source | Device | Bytes | Sessions | Bandwidth |
|---|---|---|---|---|
| rksimon<br>101.2.30.172.o.wireless.uri.edu (172.30.2.101) | GSO-M-LXN47K1WRH | 65.48 MB | 87 | 342.30 kbps |
| sciencedemo<br>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