Vera C. Rubin Observatory
Rubin Observatory Project Office

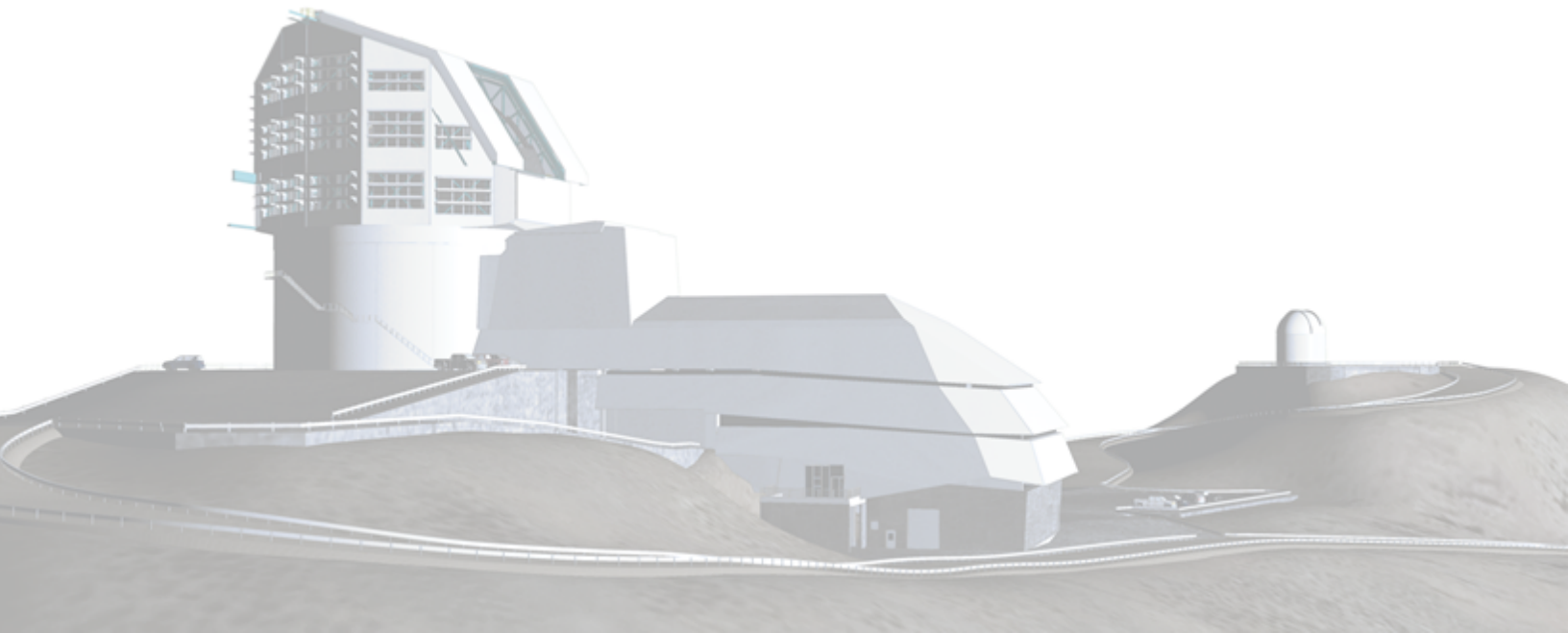
Internet Edge Firewall Design

Julio Constanzo

ITTN-049

Latest Revision: 2021-08-20

DRAFT



Abstract

This document describe the internet edge firewall design, actual setup migration and integration with Rubin's monitoring system.

Change Record

Version	Date	Description	Owner name
1	2021-08-18	Unreleased	Julio Constanzo

Document source location: `https://github.com/lsst-it/ittn-049`

Contents

Internet Edge Firewall Design

1 Scope

The scope of this document will concentrate on the hardware and software descriptions of the pfsense solution, alongside the proposed network design and integration into Rubin's network architecture. Be in mind that this document will also show images and information related to the "FY21 network re-design", so be aware that this firewall design is also part of that big picture. Migration will be also included but will not describe each activity in detail, since detailed information will be concentrated into JIRA tickets.

2 Hardware Description

2.1 Minimum hardware requirements

The minimum hardware requirements for pfsense® 2.5.2-RELEASE on hardware not sold by Netgate are:

- 64-bit amd64 (x86-64) compatible CPU
- 1GB or more RAM
- 8 GB or larger disk drive (SSD, HDD, etc)
- One or more compatible network interface cards
- Bootable USB drive or high capacity optical drive (DVD or BD) for initial installation

2.2 Hardware to be used

The two boxes that we will be using have the following specifications:

CPU	Intel Xeon-DE D-1541 2.1 GHz FCBGA 1667 supported SoC
CPU Cores	Eight Cores, 45W
Networking	Dual LAN via Intel i350-AM2 1 Gigabit Ethernet Dual LAN via SoC 10GBase-T Virtual Machine Device Queues reduce I/O overhead Supports 10GBASE-T, 100BASE-TX, and 1000BASE-T, RJ45 output 1x Realtek RTL8201N PHY (dedicated IPMI)
Storage	132 GB Micron M.2 SSD
Memory	16 GB DDR4 UDIMM

Expansion	1x PCI-E 3.0 x 16 (in x4) AOC Slot 6x SATA3 ports
Other Ports	1x BMC integrated ASPEED AST2400 1x IPMI Port 1x VGA Port 1x Fast UART 16550 Serial Port (header)
USB Ports	2x USB 3.0 ports
LED	Power LED Hard drive activity LED 2x Network activity LEDs System Overheat LED Information LED (temp., status)
Enclosure	19” 1U Rack Mount - CSE-505-203B
Form Factor	1U 1.7”x17.2”x9.8”
Cooling	200W Low-noise PS with PFC: Active CPU fan, 40mm chassis fan
Power	1x SATA DOM power connector 100-240V, 50-60Hz, 2.6 Amp MAX AC Inlet: IEC320-C14 (3 PIN) Power Cord: NEMA 5-15P to IEC320-Cxx
Environmental	10°C to 35°C Operating Temp 8% to 90% Operating Relative Humidity (non-condensing)
Power Consumption	TBD W (idle)
Certifications	FCC, CE, RoHS, UL

3 Software Description

pfsense Plus software is a powerful firewall, router, and VPN solution that leverages a number of highly-regarded open-source projects. The software competes effectively with far more expensive, commercial alternatives and is used by hundreds of thousands of businesses, educational institutions, and government agencies all over the world. Leading secure-networking features and capabilities include:

- Ad blocker (pfBlockerNG)
- Captive Portal
- CARP / HA
- DNS Server
- DHCP Server
- HTTP transparent / web / reverse proxy (Squid)
- IP / Country block list (pfBlocker)
- IDS/IPS
- Packet capture / inspection
- Port forwarding
- QOS / rate limiters
- Software load balancer (HA Proxy)
- Traffic monitoring
- Traffic logging, statistics, and graphs
- Traffic shaping
- VLAN
- Wake-on-LAN
- Website blocker (pfBlocker)

3.1 Key features

3.1.1 Low total cost of ownership

- No artificial limits or add-ons are required to make your system fully functional.
- No additional usage or feature-based pricing. Enjoy unlimited users, unlimited firewall rules, unlimited IPsec tunnels, dual WAN, etc.
- Standard configuration with 16GB of RAM and 256GB Micron M.2 SSD*.
- Low power requirements to help save you money.
- This system is designed for a long deployment lifetime.

3.1.2 Growth

- From firewall to Unified Threat Management, get all the security features you need to protect your home or business.
- Flexible configuration and support for multi-WAN, high availability, VPN, load balancing, reporting, and monitoring, etc.
- Add optional packages such as Snort or Suricata for IDS/IPS and network security monitoring, Squid for optimized content delivery, and SquidGuard for
- anti-spam/anti-phishing and URL filtering. 1
- Maximum Active Connections: 16,000,000 (32,000,000 with 32 GB RAM)

3.1.3 GUI Management

- Manage pfsense Plus software settings through our web-based GUI.
- No fumbling with a command-line interface or typing arcane commands.

3.1.4 Secure Remote Access

- Connect via encrypted Virtual Private Networks (VPN) between your offices, let mobile workers connect securely, or connect to the Cloud.

- Use the built-in Amazon VPC Wizard to easily establish VPN connections with your Amazon EC2 cloud.

3.1.5 Best For

- Medium to Large Sized Networks with 1U rack mount cabinets
- Medium to Large Sized Branch Office with heavy loads
- Managed Service Providers (MSP) / Managed Security Service Provider (MSSP) On-Premises Appliance
- Enterprise
- Anyone with High-Speed 10 Gigabit and/or 1 Gigabit Connections
- Anyone with many VPN Connections
- Anyone with high-speed connections who wish to configure IDS/IPS features

4 Network Design

As explained in the scope of this document, the following network design is also related and tied to the FY21 network re-design which is also under development.

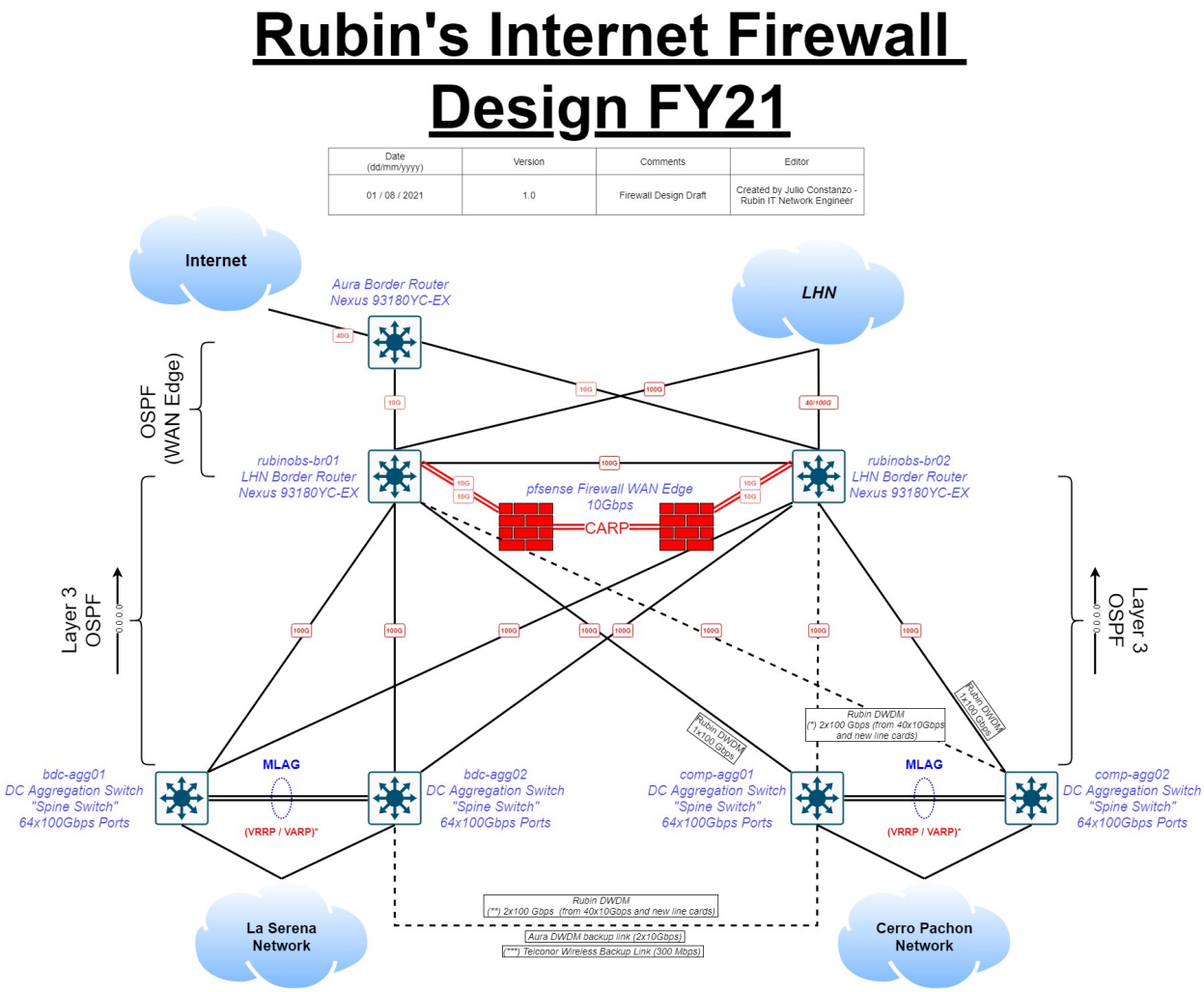


FIGURE 1: Internet Edge Firewall Network Design

5 Migration

The two Super Micro XG-1541 chassis were already racked and mounted inside our base data center during the beginning of 2021, and are running the latest and most updated version of pfsense (2.5.2-RELEASE built on Fri Jul 02 15:33:00 EDT 2021). The two boxes have a clean installation and can be moved at will since they are inside a development environment directly connected to AURA border router for WAN access. Meanwhile, out-of-band access is made through BMC interfaces.

5.1 Location inside Data Center

If physical movement is required, the two boxes will be moved to rack A4 near Rubin's and AURA border routers. 10Gbps interfaces are using LC multimode fiber and FS SFP+ modules. Gigabit ethernet connections are using CAT6/CAT6a cables. Their actual location is on rack B9.

5.2 Firewall Configurations

pfsense has a ”backup and restore” wizard which is pretty useful since also has the ability to perform area backups, meaning that can export and import specific code from/into the configuration file. Be aware that not all features are listed on the ”backup area” list. Meanwhile, the ”restore area” has a bigger option list.

Bear in mind that the actual 1Gbps firewall installed and in use in La Serena will be decommissioned once the new setup enters production. All configurations will be saved and used for the new 10Gbps firewall setup.

5.3 Authentication

Authentication will be made through IPA services. IT administrators should not use a local account unless explicitly is required (i.e during an IPA outage). The local account is only for the mandatory admin user and IT admin user. AD account only if needed.

5.4 Interfaces

Interfaces will require to be modified since the WAN and LAN connections will change. This will not affect CARP or BMC interfaces.

5.5 Firewall Aliases

Firewall Aliases can be exported and copy directly into new boxes. Aliases can be " only-restore" on pfsense web-based GUI wizard.

5.6 NAT Rules

NAT rules will require to be modified since the WAN and LAN interfaces will change. NAT rules can be "backup and restore" on pfsense web-based GUI wizard.

5.7 Firewall Rules

Firewall rules will require to be modified since the WAN and LAN interfaces will change. Firewall rules can be "backup and restore" on pfsense web-based GUI wizard.

5.8 CARP

CARP interfaces are belonging to a private range that is not in use in another segment of the network which made high availability possible, so no action is required.

5.9 Routing

Static routes will require to be modified since the WAN and LAN interfaces will change. Static rules can be "backup and restore" on pfsense web-based GUI wizard.

5.10 IPSec

IPSec will require to be modified since the WAN and LAN interfaces will change. This activity will require coordination with Steward and Rubin's Tucson IT departments. IPSec can be

"backup and restore" on pfsense web-based GUI wizard.

Note: Policy-Based or VTI modes are available. See availability on end-points for both solutions.

5.11 OpenVPN

OpenVPN will require to be modified since the WAN and LAN interfaces will change, alongside the certificates. OpenVPN configuration can be "backup and restore" on pfsense web-based GUI wizard.

Note: WireGuard has been removed from the base system in releases after pfSense Plus 21.02-p1 and pfSense CE 2.5.0 when it was removed from FreeBSD. If upgrading from a version that has WireGuard active, the upgrade will abort until all WireGuard tunnels are removed. WireGuard is available as an experimental add-on package on pfSense Plus 21.05, pfSense CE 2.5.2, and later versions. The settings for the WireGuard add-on package are not compatible with the older base system configuration.

5.12 Snort

Snort policies will require to be carefully applied to the correct interfaces using the correct "Pass-Lists" and "Aliases". Snort rules can NOT be "backup and restore" on pfsense web-based GUI wizard, is preferred to do it manually and proceed with caution since it's going to block Interface traffic if it's not correctly applied.

6 Integration

6.1 Integration with Rubin Observatory network

Both boxes have the possibility to be monitored by IT monitoring services such as:

- Graylog: Syslog monitoring system
- Icinga: Heartbeat and services monitoring system
- Grafana: Graphic telemetry monitoring system

Note: The actual setup is integrated with Graylog and Icinga monitoring services. Grafana hasn't been used in the past, but it's good to have in our monitoring system.

6.2 Integration with third-party services

There is coordination to be made and emails to be sent in order to inform third-party services about our firewall changes, in order to avoid cloud or third-party services outages.

7 Conclusion

This firewall proposal is based on the well-known pfsense solution that is already in use on the Vera C. Rubin Observatory network, but with the benefits of 10Gbps interfaces for WAN and LAN, alongside a more well-suitable network design for base and summit facilities.

There are no hardware or software costs involved since all the materials were already under the control of the IT La Serena department, and the software is open-source based.

The activities required to perform a successful migration are less complicated than if we decided to go with another firewall solution different from pfsense. Also notice that the two new boxes are already running the latest software and are under development which is a plus in time, cost, and planning.

Again, be aware that this design is very tied to the FY21 network re-design, so most of the actual routing will change in the future to accommodate the design explained in this document, mainly on how both sites are going to reach Internet access.

A References

B Acronyms

Acronym	Description
AC	Alternating Current
AD	Associate Director
AOC	AURA Oversight Council
AURA	Association of Universities for Research in Astronomy
CE	Communications Engagement
CPU	Central Processing Unit
DE	dark energy
DNS	Domain Name Service
DOM	Document Object Model
FS	File System
FY21	Financial Year 21
GB	Gigabyte
GUI	Graphical User Interface
HDD	Hard Disk Drive
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
IPS	Integrated Project Schedule
IPsec	Internet Protocol Security
IT	Information Technology
LAN	Local Area Network
LED	Light-Emitting Diode
NAT	Network Address Translation
PCI	Peripheral Component Interconnect
PMO	Project Management Office
PS	Project Scientist
RAM	Random Access Memory
SATA	Serial Advanced Technology Attachment

SSD	Solid-State Disk
TBD	To Be Defined (Determined)
URL	Universal Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPC	Virtual Private Cloud
VPN	virtual private network
WAN	Wide Area Network