MASTER'S IN INDUSTRIAL ENGINEERING

MASTER'S THESIS

SMART GRID SUPPORT NETWORK

Autor: Jordi Guasch Albareda

Director: Sarah Iddles

Co-Director: Vladimir Stankovic

Glasgow

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

Smart Grid Support Network

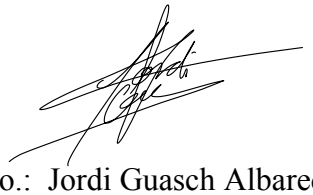
en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 2022/23 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido

tomada de otros documentos está debidamente referenciada.



Fdo.: Jordi Guasch Albareda Fecha: 15 / 08 / 23

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Sarah Iddles

Fdo.: Sarah Iddles Fecha: 15 / 08 / 23

Acknowledgements

I would like to use this section to express my sincere gratitude to all the people that contributed to the completion of this project. Firstly, I would like to extend my thanks to Sarah Iddles, my industrial advisor from Scottish Power, for the guidance and the contribution to any of the resources needed for the completion of the paper. Also, I am grateful to Vladimir Stankovic, my academic advisor from Strathclyde University, who also helped me to focus on the right path the practical parts of the project. Moreover, deep appreciation to Apostolos Vavouris, from Strathclyde University, who accompanied me with guidance in much of the project. I cannot forget to mention all my co-workers who helped me any issue or doubt during the realization of the project.

RED DE APOYO DE SMART GRID

Author: Guasch Albareda, Jordi
Director: Iddles, Sarah. Stankovic, Vladimir.
Entidad Colaboradora: Scottish Power

RESUMEN DEL PROYECTO

La arquitectura de los cortafuegos de cualquier infraestructura crítica, como la red eléctrica, es clave para proporcionar seguridad y fiabilidad a esos sistemas. Este proyecto trabajó con las diferentes tecnologías y configuraciones disponibles para actualizar la arquitectura actual de cortafuegos de Scottish Power. Una arquitectura unida y simétrica, compuesta por parejas de cortafuegos de nueva generación de alta disponibilidad de Palo Alto en configuración activo-activo fue el modelo final propuesto, debido a la mejora en sus resultados de rendimiento.

Palabras clave: cortafuegos, activo-activo, activo-pasivo, disponibilidad

1. Introducción

Hoy en día, en el contexto de un mundo interconectado, la gestión de infraestructuras críticas, como la red eléctrica, se ha vuelto vital. Las redes inteligentes han cambiado la visión de la generación, distribución y consumo de electricidad mediante la integración de nuevas y avanzadas tecnologías. Sin embargo, la dependencia de los sistemas digitales hace que la red eléctrica esté expuesta a ciber amenazas o ataques, poniendo en riesgo su rendimiento y fiabilidad. Para lograr el éxito en la implantación de la Smart Grid, es esencial contar con sólidas medidas de ciberseguridad. El componente clave para aportar esa seguridad son los cortafuegos, que protegen la red de telecomunicaciones de la red eléctrica procesando y filtrando el tráfico que pasa por esa red. Un buen diseño de la arquitectura de esos dispositivos evitará actividades maliciosas o cualquier acceso no autorizado.

2. Definición del proyecto

Scottish Power Energy Networks ha iniciado un programa de revisión y actualización de la infraestructura de redes IP que sustenta elementos clave de los entornos SPEN Telecomunicaciones y RTS. La Red de Apoyo a la Smart Grid se define como el trabajo funcional de los servidores y la infraestructura de interconexión para las plataformas de gestión de red que dan soporte a las redes RTS y de Telecomunicaciones. Los objetivos de este proyecto son los siguientes:

- Evaluar la viabilidad de la consolidación de la infraestructura actual de cortafuegos.
- Proponer el diseño de una arquitectura de cortafuegos centrada en la seguridad, alineada con el Modelo de Red Purdue.
- Evaluación de las tecnologías disponibles para facilitar una arquitectura de cortafuegos segura, incluida la gestión de la configuración.
- Comparación de los despliegues activo/activo y activo/pasivo.
- Evaluación de las tecnologías de red para optimizar el entorno de enrutamiento actual.

3. Selección tecnologías de cortafuegos

Una de las cuestiones principales del proyecto fue la selección de los cortafuegos más adecuados que pudieran proporcionar la redundancia y alta disponibilidad que la futura arquitectura requiere. Se realizó un análisis de las diferentes tecnologías disponibles en el mercado para conseguir una propuesta correcta y argumentada sobre la selección de la tecnología, la Tab. 1 muestra las capacidades de los diferentes firewalls estudiados, dos de Palo Alto y uno de Cisco [1][2][3]. Todos los cortafuegos tenían capacidades de alta disponibilidad (activo-activo y activo-pasivo) y funcionalidades similares, pero dado que los diseñados por Palo Alto tienen mejores características y todos ellos pueden trabajar bajo el mismo software de gestión y supervisión, Panorama, son los seleccionados para la arquitectura final.

Tab. 1: Comparativa capacidad de los FWs

FW Model	Cisco 2130	PA-3220	PA-3430
Flujo FW	5.4 Gbps	4.6/5 Gbps	25.5/20.5 Gbps
Sesiones máximas	2 M	2 M	2.5 M
Alta disponibilidad	A/A & A/P	A/A & A/P	A/A & A/P

4. Activo-activo vs. activo-pasivo

El análisis en las configuraciones disponibles en los firewalls de Palo Alto se llevó a cabo para estudiar cuál tendrá mejores resultados en términos de eficiencia y rendimiento. El análisis se realizó diseñando y creando un modelo Simulink en MATLAB R2022b con el uso de la librería SimEvents [4]. El modelo, que se muestra en la Figura 81 del Anexo III, está compuesto por dos pares diferentes de cortafuegos, uno activo-activo y otro activo-pasivo, en paralelo que recibirán paquetes a lo largo del tiempo y tendrán una probabilidad de fallar. En el caso de la configuración activo-activo los paquetes pasarán por ambos cortafuegos, alternándose uno con otro, si uno de los cortafuegos falla el otro seguirá filtrando los paquetes por sí mismo hasta que esté reparado y operativo. Por otro lado, en la configuración activo-pasivo, habrá un cortafuegos primario que procesará todos los paquetes hasta que se produzca un evento de fallo. En ese caso, el cortafuegos primario se desconectará y el otro, el cortafuegos de reserva, empezará a procesar los paquetes hasta que se repare.

El fallo de los cortafuegos se simula con un modelo para la configuración activo-activo y activo-pasivo, como se muestra en la Figura 30 y la Figura 31 respectivamente. Ese fallo depende de una probabilidad que, en realidad, es increíblemente alta. Se estudiaron diferentes distribuciones para ver cual se acercaba más a la forma en que fallan los cortafuegos y supervisar los resultados de rendimiento que obtenían las diferentes configuraciones, dichas distribuciones fueron las siguientes:

- Distribución Random: hay un 5% de probabilidad de fallo. El modelo generará números aleatorios entre 0 y 1 para cada cortafuegos; si alguno de esos números tiene un valor inferior a 0,05, se detecta un fallo y se desconecta el cortafuegos..
- Distribución Lognormal: hay un 95% de probabilidad de que el cortafuegos no experimente ningún fallo. El modelo generará un número aleatorio entre 0 y 100, siguiendo la distribución con una media de 5 y sigma de 0,5 y 1, si alguno de esos números tiene un valor superior a 95, se detecta un fallo, y se desconecta el cortafuegos.
- Distribución Extreme value: hay un 5% de probabilidad de fallo. El modelo generará un número aleatorio entre 0 y 100, siguiendo la distribución con una media de 95 y

sigma de 3 y 8, si alguno de esos números tiene un valor inferior a 5, se detecta un fallo, y se desconecta el cortafuegos.

Las diferentes distribuciones crearon diferentes escenarios en las simulaciones del rendimiento de las configuraciones. Al final, la empleada para la arquitectura final es la distribución de extreme value, ya que es la que más se aproxima a la realidad, al no experimentar fallos durante la simulación. En cuanto al rendimiento de las diferentes configuraciones, en todas las distribuciones la opción activo-activo mostró mejores resultados en términos de tráfico total de paquetes y su tiempo total de espera para ser completamente filtrado y transmitido, siendo la razón por la que la configuración se eligió para la arquitectura final. La Tab. 2 presenta este comportamiento, mostrando la comparación entre los resultados activo-activo y activo-pasivo en una simulación de 10.000 segundos utilizando la distribución lognormal como ejemplo.

Tab. 2: Activo-activo vs. active-pasivo, Distribución Lognormal (sigma 0.5)

Configuración	Activo-Activo	Activo-Passivo
Flujo total (paquetes)	6.532 e3	5.673 e3
Tiempo de espera máximo (segundos)	368	917

5. Arquitectura propuesta

La arquitectura propuesta, comparada con la que funciona actualmente en Scottish Power, presenta algunas actualizaciones que aumentarán la disponibilidad y redundancia de la red en general. Todos los cortafuegos del sistema procederán de Palo Alto, funcionarán por parejas en configuración activo-activo y se gestionarán con el software Panorama. Estas actualizaciones unificarán las dos redes originalmente separadas, la de RTS y la de Telecomunicaciones. La nueva arquitectura será simétrica, lo que significa que todas las redes que participan en Scottish Power tendrán las mismas características, reduciendo la complejidad en el funcionamiento del sistema.

Para probar la nueva arquitectura, se diseña otro modelo, descrito en el Anexo III, que representa todas las redes. Se realizaron otras simulaciones, en las que los fallos de los cortafuegos seguían una distribución de valores extremos, para ver los beneficios del cambio comparando los resultados de rendimiento en la arquitectura actual y en la propuesta. Las simulaciones mostraron una mejora en términos de congestión de la red, donde la propuesta tenía menores tasas de congestión, también, incluso sin eventos de fallo ocurridos durante la simulación, también mostró beneficios en el flujo total de los paquetes transmitidos. La creación de simulaciones que tendían más a tener escenarios en los que ocurrían fallos, donde el fallo de los cortafuegos seguía una distribución aleatoria, mostró el potencial real y los beneficios del cambio. En esa simulación de 100 segundos, se produjeron fallos en ambas arquitecturas. La Tab. 6 muestra cómo, incluso con un escenario en el que la arquitectura propuesta tuvo tres fallos más, su rendimiento total fue casi un 50% superior, en comparación con la arquitectura actual.

Tab. 3: Resultados de rendimiento de la arquitectura actual y propuesta en una de las redes

Architecturo	Actual	Propuesta
Flujo total (paquetes)	416	608
Número de fallos	1	3

6. Conclusiones

El proyecto tenía como objetivo estudiar y actualizar la arquitectura de cortafuegos de Scottish Power para conseguir una red caracterizada por una alta redundancia y disponibilidad. Tras investigar las diferentes tecnologías, el cambio a cortafuegos Palo Alto supervisados con Panorama sería la solución más beneficiosa. Se realizó un análisis de las configuraciones de alta disponibilidad, que condujo a la selección de la configuración activo-activo a pesar de ser una solución más compleja. Además, este proyecto también aporta algunas recomendaciones para optimizar el panorama de enrutamiento actual.

Se diseñó una nueva arquitectura simétrica que unía el conjunto de cortafuegos de infraestructura utilizando cortafuegos de Palo Alto en pares de alta disponibilidad. Las simulaciones demostraron cómo la arquitectura propuesta tenía una clara superioridad durante condiciones críticas, indicando una mejora en el rendimiento, la fiabilidad y la seguridad en general.

7. Referencias

[1] Cisco FirePower 2100 Series Data Sheet.
https://www.cisco.com/c/en/us/products/collateral/security/firepower-2100-series/datasheet-c78-742473.html

[2] Palo Alto 3200 Series Data Sheet.
https://www.paloaltonetworks.co.uk/resources/datasheets/pa-3200-series

[3] Palo Alto 3400 Series Data Sheet.
https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series

[4] SimEvents Library – Model and simulate message communication and discrete-event systems.
https://uk.mathworks.com/products/simevents.html

SMART GRID SUPPORT NETWORK

Author: Guasch Albareda, Jordi
Supervisor: Iddles, Sarah. Stankovic, Vladimir.
Collaborating Entity: Scottish Power

ABSTRACT

The architecture of the firewalls in any critical infrastructure, such as the electrical grid, is the key to provide the security and reliability to those systems. This project worked with the different technologies and configurations available to update the current architecture of firewalls from Scottish Power. A unite and symmetric architecture, composed with pairs of high availability new generation firewalls from Palo Alto in active-active configuration was the final model proposed, due to the improvement in its performance results compared to the ones obtained in the current architecture.

Keywords: firewalls, active-active, active-passive, availability.

1. Introduction

Nowadays, in an interconnected world context, the management of critical infrastructures, such as the electrical grid, has become vital. The Smart Grids have changed the view on electricity generation, distribution, and consumption by the integration of new and advanced technologies. Nevertheless, the reliance on digital systems makes the electrical grid to be exposed to cyber threats or attacks, risking its final performance and reliability. To achieve a successful Smart Grid implementation, robust cybersecurity measures are essential. The key component to bring that security are the firewalls, which protect the electrical grid's telecommunication network by processing and filtering the traffic going through that network. A good design of the architecture of those devices will prevent malicious activities or any unauthorized access.

2. Definition of the project

Scottish Power Energy Networks has started a programme to review and upgrade the IP Networking Infrastructure that underpins key elements of the SPEN Telecoms and RTS environments. The Smart Grid Support Network is defined as the functional working of servers and interconnecting infrastructure for the Network management platforms that support RTS and Telecoms networks. The objectives of this project are the following:

- Assessment of feasibility in consolidation of current Infrastructure Firewall Estate.
- Propose design of security focused firewall architecture, aligning with the Purdue Network Model.
- Assessment of available technologies to facilitate secure firewall architecture, including configuration management.
- Comparison of Active/Active and Active/Passive deployments.
- Assessment of networking technologies to optimize current routing landscape.

3. Firewalls technology selection

One of the main focuses of the project was to select the most suitable firewalls that could provide the redundancy and high availability that the future architecture requires. An

analysis of the different technologies available in the market was carried to achieve a correct and argued proposition on the technology's selection, Tab. 4 shows the capabilities of the different firewalls studied, two from Palo Alto and one from Cisco [1][2][3]. All the firewalls had high availability capabilities (active-active and active-passive) and similar functionalities, but since the ones designed by Palo Alto have better characteristics and all of them can work under the same management and supervision software, Panorama, they are selected for the final architecture.

Tab. 4: FW capabilities comparison

FW Model	Cisco 2130	PA-3220	PA-3430
FW throughput	5.4 Gbps	4.6/5 Gbps	25.5/20.5 Gbps
Max sessions	2 M	2 M	2.5 M
High Availability	A/A & A/P	A/A & A/P	A/A & A/P

4. Active-active vs. active-passive

The analysis in the configurations available in the firewalls from Palo Alto was carried to study which will have better results in terms of efficiency and performance. The analysis was made by designing and creating a Simulink model in MATLAB R2022b with the use of the SimEvents library [4]. The model, shown in Figure 81 from Annex III, is composed by two different pairs of firewalls, one active-active and the other active-passive, in parallel that will receive packets overtime and have a probability to fail. In the case of the active-active configuration the packets will go through both firewalls, alternating from one another, if one of the firewalls fails the other one will continue filtering the packets by itself until it is repaired and operational. On the other hand, in the active-passive configuration, there will be one primary firewall which will process all the packets until a failure event occurs. In that case, the primary firewall will be disconnected and the other one, the back-up firewall, will start processing the packets until it is repaired.

The failure of the firewalls is simulated with one model for active-active configuration and active-passive configuration, as shown in Figure 30 and Figure 31 respectively. That failure depends on a probability, which, in reality, is high. Different distributions were studied to see which was closer to the way in which the firewalls fail and to supervise the performance results that the different configurations obtained, those distributions were the following:

- Random distribution: there is a 5% of probability of failure. The model will generate random number between 0 and 1 for each firewall, if any of those numbers have a value below 0.05, a failure is detected, and the firewall is disconnected.
- Lognormal distribution: there is a 95% of probability that the firewall does not experience any failure. The model will generate a random number between 0 and 100, following the distribution with a mean of 5 and sigma of 0.5 and 1, if any of those numbers have a value above 95, a failure is detected, and the firewall is disconnected.
- Extreme value distribution: there is a 5% of probability of failure. The model will generate a random number between 0 and 100, following the distribution with a mean of 95 and sigma of 3 and 8, if any of those numbers have a value below 5, a failure is detected, and the firewall is disconnected.

The different distributions created different scenarios in the simulations of the performance of the configurations. At the end, the one used for the final architecture is the Extreme value distribution, since is the one closer to reality, experiencing no failures during the simulation. Regarding the performance of the different configurations, in all distributions the active-active options showed better results in terms of total throughput of packets and its total time waited to completely filtered and transmitted, being the reason why the configuration in chosen for the final architecture. Tab. 5 presents this behaviour, showing the comparison between active-active and active-passive results in a simulation of 10.000 seconds using the lognormal distribution as an example.

Tab. 5: Active-active vs. active-passive, Lognormal Distribution (sigma 0.5)

Configuration	Active-Active	Active-Passive
Total throughput (packets)	6.532 e3	5.673 e3
Wait time peak (seconds)	368	917

5. Proposed architecture

The proposed architecture, compared to the one which is currently operating in Scottish Power, have some updates that will increase the availability and redundancy of the network overall. All firewalls in the system will come from Palo Alto, will work in pairs in active-active configuration and will be managed with Panorama software. These updates will unify both networks originally separated, the RTS and Telecommunication networks. The new architecture will be symmetrical, meaning all networks taking part in Scottish Power will have the same characteristics, reducing the complexity on the operation of the system.

To test the new architecture, another model, described in Annex III, representing all networks is designed. Other simulations, where firewalls´ failure followed an Extreme value distribution, were made to see the benefits of the change comparing the performance results in the current and proposed architecture. The simulations showed an improvement in terms of congestion of the network, where the proposed one had lower congestion rates, also, even with no failure events occurred during the simulation, it also showed benefits in the total throughput of the packets. Creating simulations which tended more to have scenarios in which failures occur, where firewalls´ failure followed a random distribution, showed the real potential and benefits of the change. In that 100 second simulation, failures occurred in both architectures. Tab. 6 shows how, even with a scenario in which the proposed architecture had three more times failure, its total throughput was nearly a 50% higher, compared to the current architecture.

Tab. 6: Current and proposed architecture performance results in one of the networks

Architecture	Current	Proposed
Total throughput (packets)	416	608
Failure events	1	3

6. Conclusiones

The project was aimed to study and update the firewall architecture of Scottish Power in order to achieve a network characterised by high redundancy and availability. After researching the different technologies, a shift to Palo Alto firewalls monitored with

Panorama would be the most beneficial solution. An analysis on the high availability configurations was done, leading to the selection of active-active configuration despite being a more complex solution. Additionally, this project also brings some recommendations to optimize the current routing landscape.

A new symmetrical architecture uniting the Infrastructure Firewall Estate was designed using Palo Alto firewalls in a high availability pairs. Simulations demonstrated how the proposed architecture had a clear superiority during critical conditions, indicating an improvement in performance, reliability and security overall.

7. References

[1] Cisco FirePower 2100 Series Data Sheet.
https://www.cisco.com/c/en/us/products/collateral/security/firepower-2100-series/datasheet-c78-742473.html

[2] Palo Alto 3200 Series Data Sheet.
https://www.paloaltonetworks.co.uk/resources/datasheets/pa-3200-series

[3] Palo Alto 3400 Series Data Sheet.
https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series

[4] SimEvents Library – Model and simulate message communication and discrete-event systems.
https://uk.mathworks.com/products/simevents.html

Content's index

Figure's Index

Table's Index

Equation's Index

Capítulo 1. INTRODUCTION

Nowadays, in the context of a technology driven and interconnected world, the key to protect critical infrastructures, such as the electrical grid, is to design them to being able to be efficient and possess a secure management. The Smart Grids, which mixes information and communication technologies with the traditional electrical power systems, are changing the traditional perception of generating, distributing and consuming electricity. Nonetheless, with its increasing dependency in digital technologies, the possibility to suffer from cyber-attacks, being potential riskers to the security and reliability of those systems, has also increased.

A critical aspect to ensure the successful operation and implementation of Smart Grids is to integrate robust cybersecurity measures in its system. An essential asset for any secure information system is the firewall. They are fundamental components which take a key role in filtering and securing the communication in the Smart Grids' telecommunications network. Those barriers or gateways are the first line of defence, preventing malicious activity and undesired or unauthorised access.

The main focus of this project is to investigate and address the importance of a correct design in the firewall's architecture of the Scottish Power network. To do that a deep analysis on the different technologies, techniques and configurations will be carried.

1.1 PROJECT'S DEFINITION

The Smart Grid Operations LAN consist of the RTS and Telecoms network devices segregated by the policy from respective Firewalls. These domains are managed separately, however both domains can overlap in the LAN to communicate with specific end point devices.

The current separation of RTS and Telecoms LAN domains is a consequence of the evolution of SPEN as a business and has resulted in a complexity which is impacting network performance.

Each domain uses their own Switches and Firewalls that are used to perform traffic filtering, route filtering and NAT (network address translation) which aid in keeping the domains separate but is now limiting options for system integration.

Scottish Power Energy Networks has started a programme to review and upgrade the IP Networking Infrastructure that underpins key elements of the SPEN Telecoms and RTS environments. The Smart Grid Support Network is defined as the functional working of servers and interconnecting infrastructure for the Network management platforms that support RTS and Telecoms networks.

1.2 OBJECTIVES

The main objectives of this project are the following:

- Assessment of feasibility in consolidation of current Infrastructure Firewall Estate.
- Propose design of security focused firewall architecture, aligning with the Purdue Network Model.
- Assessment of available technologies to facilitate secure firewall architecture, including configuration management.
- Comparison of Active/Active and Active/Passive deployments.
- Assessment of networking technologies to optimize current routing landscape.

1.3 METHODOLOGY

An extensive analysis of the current firewall's infrastructure will be performed. The different issues of the present architecture will be identified and recommendations to have an update in the actual performance will be presented.

These recommendations will then be considered in the proposition on a new design of the firewall's architecture, which main goal is focusing on security and redundancy while aligning with the Perdue Network Model. This new design will consider configuration management, routing techniques and the different High Availability to create a resilient and feasible model.

To achieve the final goal of the project, the use of different reports and information regarding the technologies and the techniques used will be reviewed and analysed. Moreover, different models of Simulink will be designed to, first, understand the behaviour of the current architecture, to finally create and correctly argue the new architecture's proposal.

Capítulo 2. STATE OF THE ART

2.1 SMART GRIDS' REVIEW

The electrical power network has been key for the development of our industry and life. This infrastructure, even though it has been updating and developing for decades, it has many issues that need to be addressed. There has been more blackouts, overloads and other problematic scenarios, in the past decade than over the last forty years. Also, the constant increase in the capacity has increased the contribution that this infrastructure has in terms of carbon emission to the atmosphere. Moreover, this increase in capacity has also been inducted by the increase on the population, making some parts of the grid old and reducing its reliability. Furthermore, the new appliances added to buildings and residential areas in general have created more instability to the present power network. Currently, the electrical grid systems have four main elements. Firstly, electricity generators, followed by the transmission substations and then the distribution substations, finally, the end users or customers [1]. This is shown in Figure 1.

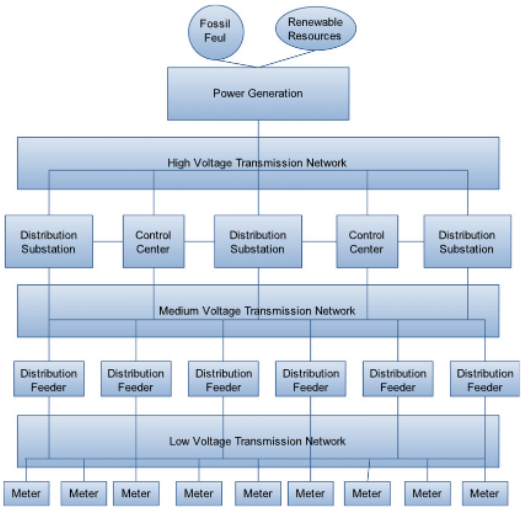


Figure 1: Traditional power system overview [1]

The demand on a system power system that increases its stability and efficiency is clear. This electric infrastructure needs to be not only reliable but also manageable and scalable, while also being secure and cost effective. Also, the constant advances of computation and telecommunications are encouraging the use of these technologies in many utility industries. Many of those industries have suffered from a great change due to the use of information and communication technologies (ICTs), the electrical power grid has been exposed to this tendency since the beginning of the 21st century. The use of these telecommunications networks inside the electrical power grid is what is known as a "Smart Grid" [2]. The term is an idealistic vision for the features needed to achieve a better electrical grid, some of those features are:

- General modernization of grid infrastructure.
- Higher number of controls and sensors which, managed by a central system, can help in the operation of the electricity power system.
- Ability to control all components, including critical, of the grid.
- DG resources combined with storage systems and bulk power generation.
- Reduce the impact of energy production and distribution on the environment.
- Automatic operations.
- Efficiency in all the energy chain, from production to consumption.
- Prevention of failures, providing resilience to the system.
- Power quality assurance.

That grid also needs to consider some technologies that have not been completely implemented in the actual electric power system [3]. Energy storage is one of them, the technology will be essential to mitigate the effects of the variability of power production coming from residential distributed generation and power load from electric vehicles. Power management from that storage system will be key to smooth the excess demand on the grid and to maximize the profitability coming from renewable energy units. It also provides redundancy, avoiding the collapse of the system in case of a quick drop on balance between generation and demand, and voltage and frequency control features. Another technology which will have a main role in the deployment of smart grids will be telecommunication

systems. These systems will provide the customers-DSO and DSO-TSO communications in a bidirectional flow in broadband access. The technologies used will go from xDSL or fiber optics, to wireless or PLC communications. Any technology used will transport and route the information coming from metering devices and digital communications to finally monitor its real-time state and control any distributed energy resource in a reliable way. Finally, that data will be part of an ICT infrastructure, such as a SCADA system, which will permit to know at any time at any place the status of the system [3]. A representation of a Smart Grids can be seen in Figure 2.

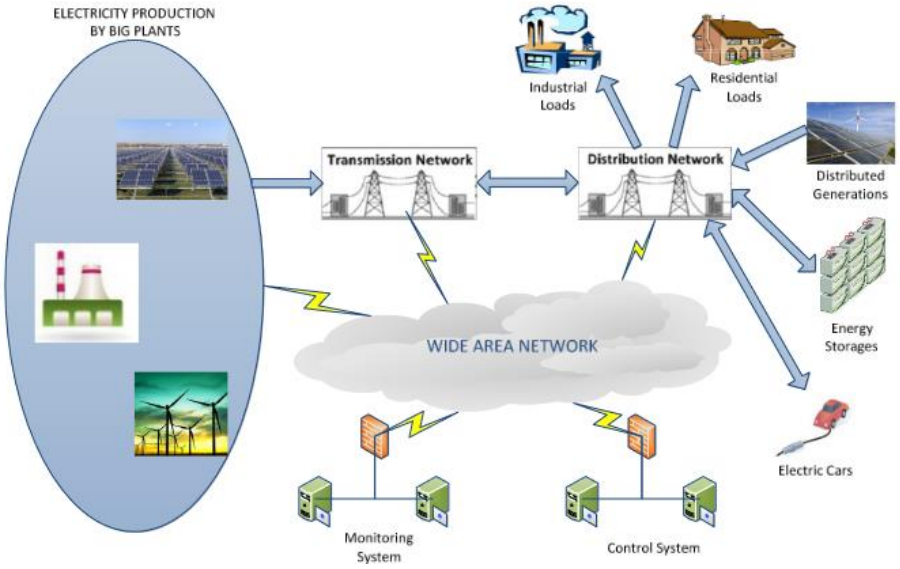


Figure 2: Smart grid network [3]

Smart grids implementation can be limited to different technical and economical constraints. The common aspects of the definitions given to ICTs In Smart Grids can go from the presence of ICT in all activities of the electricity system to the integration of those technologies in its infrastructure and applications. It also considers the deployment of not only hardware, but software dedicated to ICTs. Information and communication technologies are considered as the electronic or computing devices coupled with a telecom network and are the ones which integrates the physical layer of the grid to the algorithms and intelligence of the smart grid.

Furthermore, telecommunication technologies are expected to have a bigger role in the grid, Figure 3 shows the current and expected participation of telecommunications in the different parts of the electrical grid. It also needs to be said that not every telecommunications network will be suitable for the electrical grid, applications from that system can have different requirements that must be considered for the telecoms design. Ideally, telecommunication networks need to follow these features:

- Support bidirectional traffic and being wideband.
- Low latency communications.
- Support huge amount of real-time data from a massive number of end-points.
- High reliability.

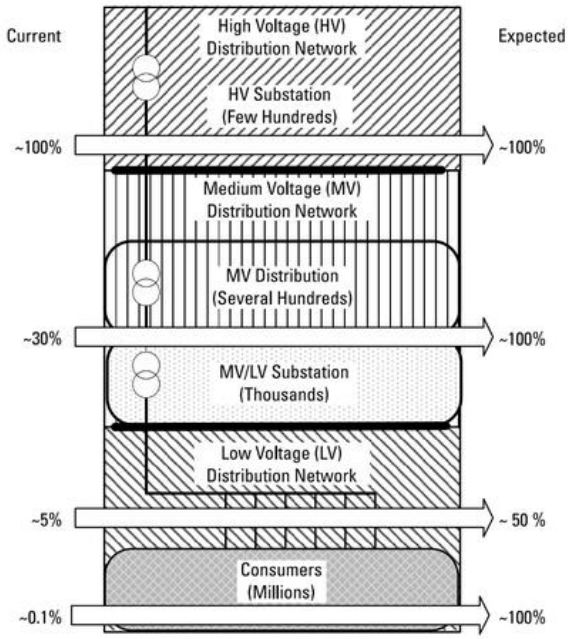


Figure 3: Telecommunications' evolution in electrical grid [2]

These necessary aspects from the telecoms network will need to be adjusted, depending on the applications or segment of the power grid that the network will support. The new changes that will take place in the following years, regarding electrical power systems, will come with new challenges. Information and communication technologies will have a key role in the correct integration of those new elements.

2.2 TELECOMUNICATIONS IN SMART GRIDS

As it was described in the last subsection, the assumption that power flows in the power grid are unidirectional or that simple time-graded methods of protection are enough are nor reliable anymore. Modern electrical grid's technologies, including DG, will lead to bidirectional power flows and to new necessities in terms of protection systems. All the new applications will need of a system capable of collecting real-time data from the network (telemetry), for its future operational instructions (telecontrol). Therefore, a telecommunications network is needed.

These applications will also include different technologies, such as synchrophasor measurements, wide area monitoring or sensors capable of diagnose, protect and control the network. Other applications will be the future use of smart metering, PHEVs, EVs, demand response management and the possibility to operate part of the grid as a microgrid.

The two fundamental metrics that telecommunications networks need to operate parallel to the power grid are the throughput of the channel and the latency/delay of that channel. The throughput of the channel depends on the amount of information that the network is capable of sending from point A to point B in a given time. In the case of power systems, their control and operation are time sensitive operations with low throughput. However, the increase of demand for real-time monitoring through all the energy chain will make the speed requirements increase over time [4]. The IEEE Power Engineering Society described the requirements, in terms of performance, that the substation must have depending on its application, that segmentation is described below:

- Very high speed/Very low latency (<2 ms) applications: stream CT and VT samples, and protection signals, to the switchgear.
- High speed/Low latency (2-10 ms) applications: event notifications for protection.
- Medium speed/Medium latency (10-100 ms) applications: non-critical data traffic between the protection units or other control functions, such as synchrophasors.

- Low speed/High latency (>100 ms) applications: Information exchange external to any substation, control centre or IEDs.

When creating a telecommunications network, other aspects must be considered for its correct deployment and future upgrades that might occur. Network scalability is an essential aspect to consider, its design should consider the performance of the services the system requires, even taking into consideration the evolution that might happen in the following years. Thus, a scalable design will guarantee that any new technologies or applications can be integrated, without needing from huge investment to adapt the system for their integration due to limited design.

Another important aspect to consider at the design of the telecommunications network, is its reliability, resiliency, dependability and availability. The resiliency depends on the network's capability to recover from a malfunction or a change as quick as possible. ITU-T Recommendation E.800 define the rest of the features [2], regarding service quality characteristics:

- Reliability is the probability that a device can perform its function in a given time interval and under given conditions.
- Dependability depends on the certainty with which the function is done, without considering performance metrics such as speed or accuracy.
- Availability is the ability to of a device to being able to perform a function at a given time or at any instant from a given time interval, assuming that the external resources required to perform the task are also given.

Finally, security of the network is another fundamental feature of a telecommunications network. Tools and recommendations are not enough to consider the infrastructure as secure; security needs to be progressively integrated in all the energy chain, including utilities and processes. Network security considers both, data traffic protection, access control, and the protection of the network itself. The cybersecurity of the Smart Grids makes its operation more complex and will be furtherly discussed in the following subsection.

2.3 CYBERSECURITY IN SMART GRIDS

Electrical power systems and telecommunications systems are critical infrastructures, and its large-scale architecture creates a complex scenario. Also, both were designed to be reliable, and that design is based on a huge pool of standards.

Even if both infrastructures have some similarities, they experience different type of problematics and uses. In the electrical power grid, incidents usually come from hardware errors or failures. They were also commonly perceived with a unidirectional behaviour, as a homogeneous service (coming from the central supply), and as an expensive and time-consuming architecture regarding its scalability. On the other hand, telecommunication networks, problems usually come from software failures. In the case of that market, is not monopolist as the power market, is more competitive. This type of market implies that the supply of service es distributed and heterogeneous. Moreover, this type of networks is bidirectional, since customers not only consume, but also produce data. Also, compared to the power systems, scaling these networks can be done in less time and resources [5].

Security, by definition, is the inability of the environment to affect, in an undesirable way, the system. The introduction of telecommunication networks, as a critical component of the Smart Grids, new security measures need to be considered. The concept of cybersecurity and information security relates to features such as confidentiality, integrity, availability, and network and IP security overall. When it comes to security requirements, power systems, or any process control system, have differences compared to IT systems:

- Security objectives: in telecommunications, integrity, availability and confidentiality are the objective. On the other hand, power grid focuses on continuous operation and protection of both, components and people.
- Security architecture: in telecommunications, the central centre is the part of the network which needs higher security, while in power systems, all parts need to be secured.

- Technological base: compared to telecoms, power systems use a vast number of different proprietary systems.
- QoS requirements: power systems, or any control system, disruption of operation can have critical financial consequences.

The Smart Grids make it possible to remote control and support the network. Although this seems beneficial in the first place, it also results in a higher networking between SCADA systems and ICT infrastructures, which means that both infrastructures will share requirements and vulnerabilities. These new networks make it possible for attackers to reach form anywhere.

When we talk about cybersecurity in smart grids, all components of the grid need to be considered, from the generation units to the loads, also considering DG. Everything that has been introduced in terms of Smart Grids security presents new challenges regarding cyber security in Smart Grids. Firstly, Smart Grids imply a transition to a more distributed environment where there will be many devices interconnected, increasing the connectivity of the network. This upgraded connectivity converts systems which used to be enough protected like SCADA, into systems reachable by new types of threats. Also, connectivity implies that those new attacks could potentially disable multiple devices at once. Moreover, the possibility that an attack on a system can propagate to another because of their connection must be considered.

Another point to cover is the necessity of new trust models, people are used to believe that electricity as a trustworthy environment. With the new model of Smart Grids, assuming all participants are trustful would be unsecure, therefore, new mechanisms should be integrated in the system to cover that new issue. Also, the increase in the amount of devices from a utility will pose challenges in terms of management, trust or monitoring for cyber-instructors. Key management could be a solution, but would imply an increase in resources, such as processing capacity, that might not be possible at the time of the deployment.

A challenge that is essential to cover is the software vulnerabilities, mainly due to malware attacks. General purpose technologies and solutions are used in Smart Grids which, even if

it brings advantages, it also risks the system to suffer from a malicious attack. The vulnerabilities of the system can be fixed, but patching can be very costly and time-consuming in critical infrastructures. Furthermore, when it comes to software design, security testing is not a priority, which makes it very common to have working solution networks with vulnerabilities and a general security shortage. Finally, consumers privacy is another challenge for the cyber security of the Smart Grids. Devices such as smart meters, creates a scenario in which private information about customers is being treated. The data from those devices needs to be correctly protected during storage and transfer to avoid extern agents from getting that private information.

2.4 NETWORK'S SECURITY

Network security has many definitions, but all have common aspects, those definitions include monitoring, traffic analysis or intrusion detection [6]. The security of a corporate's network can also be divided in three main parts: data, network business and network system security [7]. Transferring information securely, has been one of the biggest challenges that any industry integrating telecoms systems had to confront. This subsection will discuss the different aspects of how a corporate's network con be designed and maintained to be considered as secure and efficient.

Many security methods have been discussed and implemented, separately and together. The first is the use of cryptography in the data being transmitted through the network. This method is the most commonly used for securing the services and the information of the network. Firewalls are also a highly used device for the protection of any network, these devices form a wall between two networks and data will need their permission to pass form one to the other. There are different types of firewalls currently offered in the security market [8]:

- Application Gateways: this was the first operating type of firewall, commonly known as proxy firewall, are made up of bastion hosts to act as proxy server. It operates in the Application Layer from the ISO/OSI reference model. By categorizing the clients

to access the Internet services, these firewalls created a highly secure architecture, not allowing to access by default. An example is shown in Figure 4.

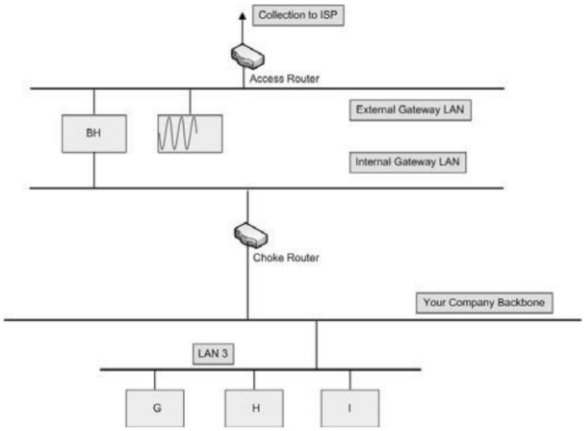


Figure 4: Application gateway network [8]

- Packet filtering: for this case, routers have ACL capabilities. The routers will pass all traffic sent to the device, ACL defines rules to allow traffic to access from the "outside world" to the corporate's network or the other way around. The control of the data's access is much simpler, compared to the type explained above, the access is control at a lower ISO/OSI layer's level. Also, this method is way faster, but it has a main disadvantage, the source address cannot be ensured, that's the reason why using layers of packet filters is essential to locate where the traffic is coming from. A packet filtering network is shown in Figure 5.

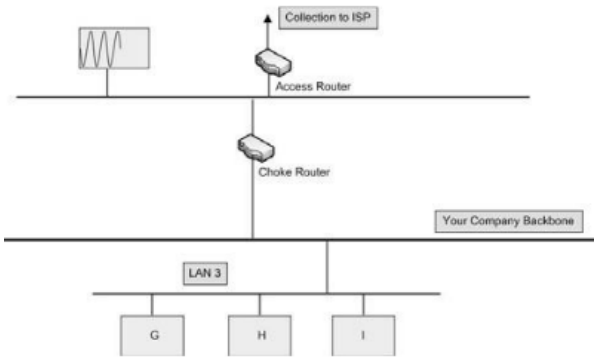


Figure 5: Packet filtering network [8]

Hybrid models can also be implemented, uniting both features, security from the application layer with speed from the second option, can create an architecture with great resilience and efficiency. Also, in the case of an attack, the threat must pass through not only the access router, but also the bastion host and the chock router. Different models' approaches are compared in terms of speed and security in Figure 9.

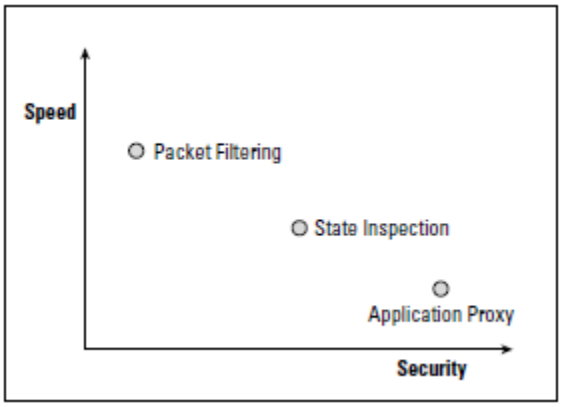


Figure 6: Network's speed/security capabilities [9]

The main issues, from network security perspective, are for example the incorrect implementation of security policies and procedures that end up not being accordingly used. The use of technology might help to impose those policies through users and processes. The architecture deployed must follow easy and cost-effective implementations, while enabling a system capable to scale up without compromising performance.

Different end-to-end solutions are also offered to secure every aspect of a corporate's telecoms network. These solutions are composed by the combination of software and hardware platforms, and a management solution which apply different functions to maintain a secure operation of the network. The different options can be defined in the following categories:

- ASIC based appliances: this service makes it possible to move from a software-based, open platform, solutions to purpose-build appliances.

- SSL-VPN: better encryption technology via SSL and IP-VPN. The necessity to reduce the risk of transmitting data via text created the opportunity for SSL-VPN technologies to offer a more secure end-to-end transmitting service.
- Instruction Detection Prevention System: this system provides a tool, using the best characteristics of firewalls and intrusion detection systems, able to configure network access control points in an environment where threat profiles change rapidly. The key from the technologies from this category is to, not only detect known threats, but also unknown ones in real time.

WAN security solutions can also be applied to networks with multiple satellite offices in different geographical zones. It enables the organizations with tools to automatically manage those separate assets safely. With the rapidly increase of different forms of cyberattacks, have created a necessity for corporations to be prepared in terms of proactive security, reactive security is not enough. A better understanding on how those attacks can evolve, with a scalable and correct architecture will be key for the security of the future organization's network.

2.5 FIREWALLS OVERVIEW

Firewalls were first created and developed by DEC in the 80s, they operated with a set of rules, filtering packets depending on the addresses and the ports number. The fast evolution of threats and attacks created a necessity to upgrade the traditional firewalls to make them more reliable and achieve a secure architecture. Every new design was created with the purpose to protect a specific type of attack, ending up with five main categories of firewalls: packet filtering firewall, application layer firewall, circuit-gateway firewall, stateful-firewall and next-generation firewall (NGFW) [10]. This evolution, including the new capabilities from the new designs, is presented in Figure 7.

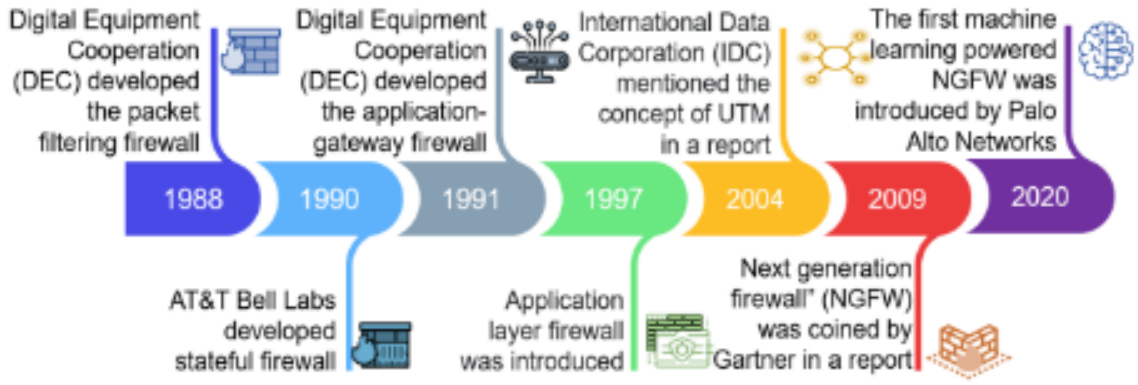


Figure 7: Evolution of the firewalls [10]

2.5.1 TRADITIONAL FIREWALLS REVIEW

The traditional firewalls were the first ones being deployed in networks. They had some simple security features that will be furtherly discussed here below. The firewalls discussed will be the packet filtering firewalls and the stateful-firewall.

Firstly, the packet filtering firewalls, Figure 8, were the first type of firewalls ever developed, filtering information packets by looking into the incoming and outgoing packets. That filter is created with a group of rules based on the IP, ports or protocols of the packets. The firewalls provide a simple configuration and a great efficiency in terms of filtering packets. Nonetheless, as the filtering does not occur on the application layer, it cannot check aspects such as payload or the authentication of the user, which end up with a vulnerable architecture.

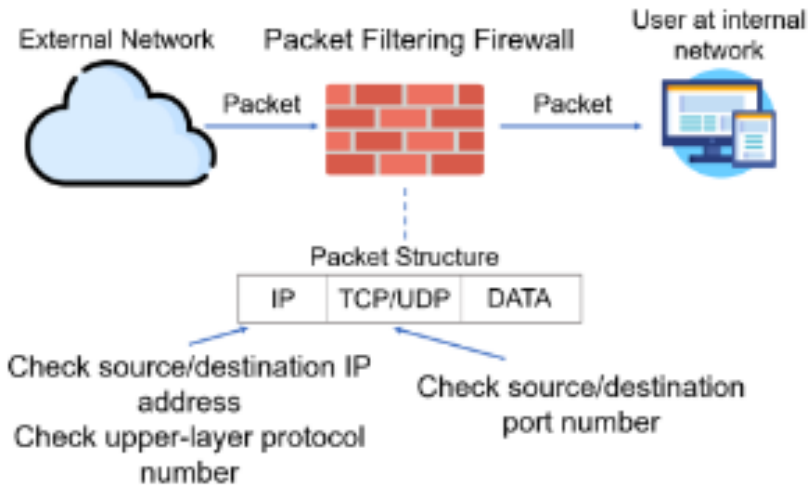


Figure 8: Packet filtering FW [10]

Secondly, stateful-firewalls can keep the track of specific flows, including the packets going from both directions of that flow. To have this ability, the firewall has installed a cache, which records the traffic flow going through the device. Basically, it works following the strategy below:

1. The packet matches an already existing stable route, it can continue.
2. The packet does not match an already existing stable route, the packet must go through the access policy requirements:
    a. It complies with the filtering rules, it can continue, and the route is stored.
    b. It does not comply with the filtering rules, access denied.

This type of firewall brings an upgrade to the type described above, it has more security and efficiency features. However, it requires more space mainly because of the cache installation and the cache can suffer from an overflowing scenario. Furthermore, this type nor does it have payload check or authentication of user. Figure 9 shows a schematic design of a stateful-firewall.

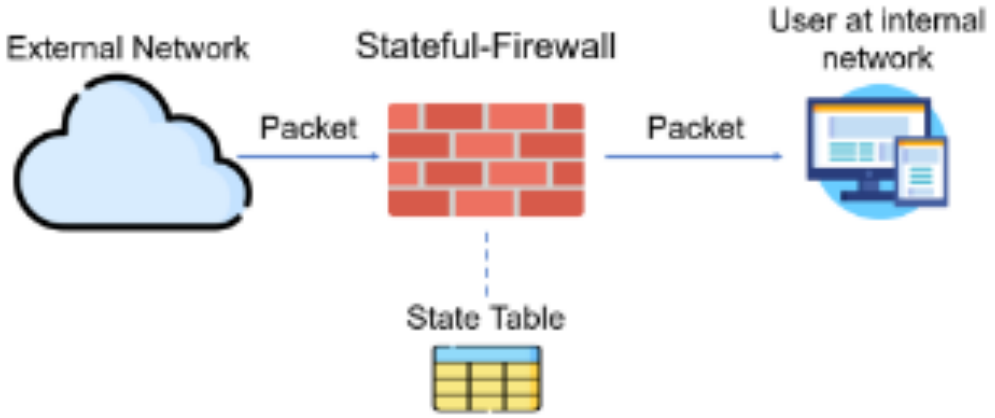


Figure 9: Stateful-FW [10]

2.5.2 APPLICATION-GATEWAY FIREWALLS

This type of firewalls brought for the first time the possibility to have a network control in the application level. The firewalls go from the concept of "wall" to a "gateway", it can examine the packets' flow at the application layer and with the use of proxies it can create new sessions with remote users. All the resources in flow will go to the gateway and then it will send it to the client, providing another protection layer, preventing the external client from having a direct contact with the corporate's server. The process is represented in Figure 10. The new procedure will increase the security of the system, while increasing the speed of the flow and the requests' responses.

Figure 10: Application-Gateway FW [10]

2.5.3 CIRCUIT-GATEWAY FIREWALL

This type of firewalls has some similarities compared to the one explained before, since it also works as a gateway. The main difference is that, instead of operating on the application layer, it works on the session one, it focuses on the connections between the server and the client, always ensuring that those connections are legitimate. Furthermore, apart from that it also supervises that the packets coming from the server are the ones requested by the client, denying the traffic if that does not comply. This type of firewall provides a faster response than the application-gateway firewall but has some decrease in terms of security quality, making common for architectures relying on this type of firewalls to have other types installed.

2.5.4 WEB-APPLICATION FIREWALL

This type of firewall is specific for web applications, it can protect from different types of threats the back-end web application. It supervises the HTTP/HTTPS request packets and other traffic patterns, denying requests and eliminating the session between server and client when malicious patterns are found. This technology has great performance with known attacks, on the other hand, unknown threats are difficult to detects because these firewalls depend on their pattern recognition.

2.5.5 UNIFIED THREAT MANAGEMENT

In the case of UFM firewalls, with just one hardware and software device, many functions are provided to the system. They can secure the system from many cyberattacks, providing with a set of mechanisms commented from the previous firewalls. Furthermore, UFMs also provide spamming and phishing defense techniques. This type of device achieves a lower complexity than the deployment of many firewalls of different types, while also having an easy deployment and installation. On the other hand, because of its multiple capabilities and the possibility to be installed alone, creates a single point of failure mainly because the failure of one of its functions will affect all the other services. Moreover, it will also decrease the performance of the network, reducing the average traffic speed due to the multiple inspections. A summarize of those function can be seen in Figure11.

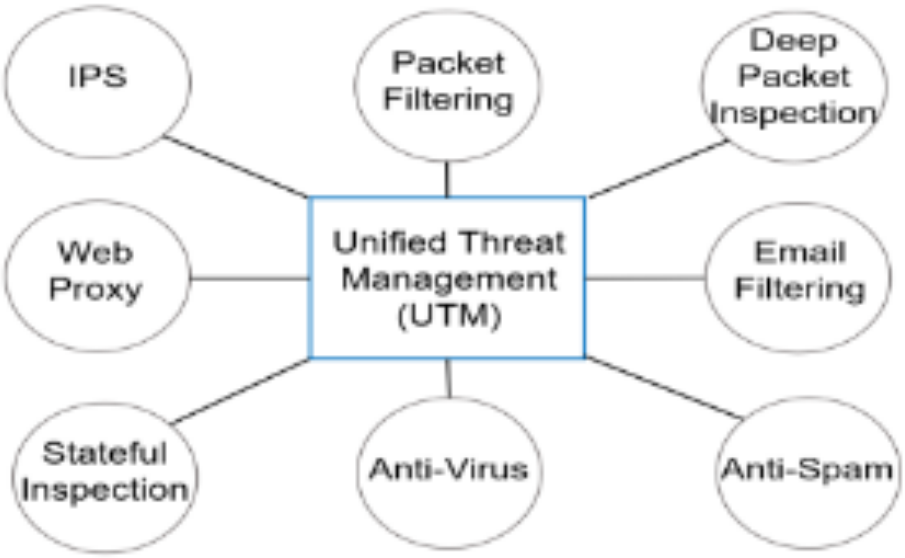


Figure 11: UTM's functions [11]

2.6 NEXT-GENERATION FIREWALLS

Next-Generation Firewalls (NGFW) have all the capabilities that the past types of firewalls had, such as packet filtering, NAT protocol, VPN or stateful inspection, and more advanced defence techniques like IPS. This new technology can identify applications regardless of port and protocol, it identifies the user, linking it to the packet, looking into the true intention of the payload [10]. Even if it could look like this technology does not have that much of a difference with other types explained above, that would not be the case. Although UTM also have a combination of functions, it would only efficiently work on small networks, whereas NGFW can cover and protect networks from enterprises and big corporations. Furthermore, even though WAF also deeply supervises the application layer of the packet, it does not have the capabilities of the NGFW to cover all OSI model's layers.

2.6.1 NGFW'S FEATURES

Firstly, NGFWs' application awareness makes it possible to look past the packet header, allowing the device to identify the real application of that packet. It also decrypts the application protocol from the payload's protection and re-encrypts it after analysing the

payload. Even more, most applications have a recognizable signature which is identifiable, in the case of suspicious signatures NGFW will block the application or analyse them furtherly, protecting the system from evasive tactics.

The dissection of the payload and the examination of the application signature will stop most of the known attacks, for the attacks that could not be blocked will go through a heuristic analysis as a backup plan. This new analysis can identify more complex applications, determining if it is harmful by looking into the behaviour of the program. To perform the analysis different components are used: data collector, interpreter and matcher [12]. Also, this technology is capable to perform file and URL filtering for a greater inspection of the packets.

User identification is also upgraded in NGFWs, after obtaining the basic information that any stateful firewall would get, the firewall communicates with the LDAP directories to gain clarity on who is the responsible of a packet from the traffic and being able to filter the packets, depending on the identity of the user.

2.6.2 NGFW'S BENEFITS

Performance is one of the key benefits of deploying NGFW in any corporate's architecture. To monitor traffic, it uses a stream-based packet scanning instead of the traditional file-based scanning. This method of scanning basically consists of scanning the traffic by packets, as soon as they start arriving, instead of waiting for the whole file [13]. This scanning method has great results increasing the throughput, while also decreasing the latency. Those improvements in the scanning process can be seen in Figure 12.

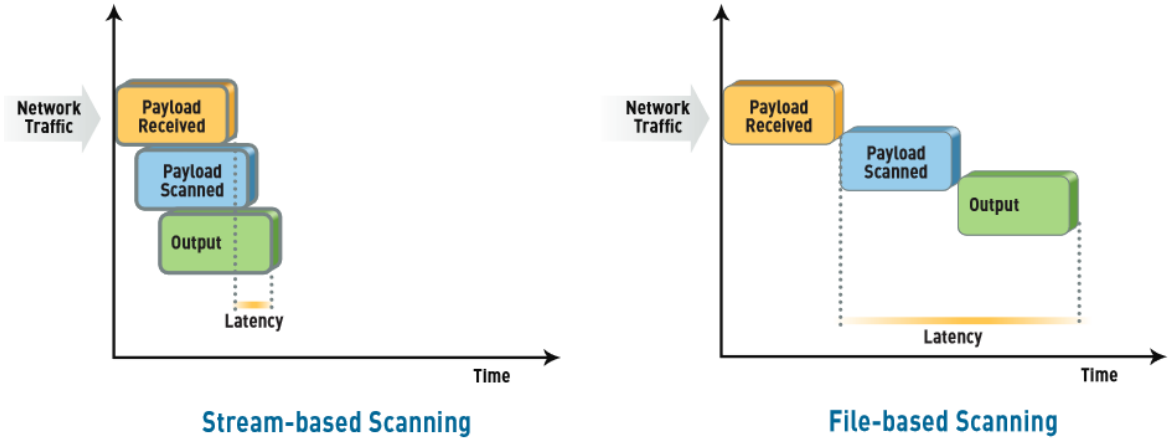


Figure 12: Stream-based scanning vs. File-based scanning performance [13]

Moreover, its uniform threat signature format makes it possible to detect different kind of threats by a single pass. Also, while firewalls with similar functions like UTMs work under multi-pass architectures, NGFWs are designed as a single-pass architecture, processing all the modules parallelly. This method achieves an operation which is not repetitive, minimizing processing time and maximizing performance overall. An example of that operation, from a Palo Alto NGFW, is shown in Figure 13.

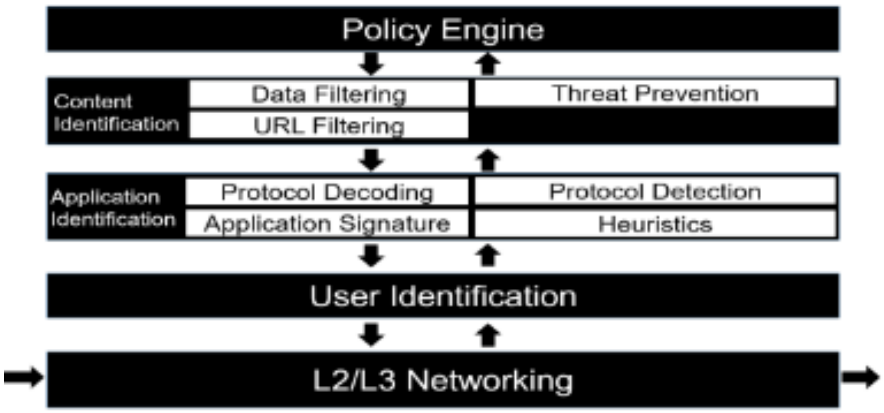


Figure 13: Palo Alto NGFW single-pass architecture [10]

Another important benefit of this type of technology, compared to the previous options, is that this firewall can protect and operate on layer 3, with traditional firewall techniques, layer 5, as a gateway, and layer 7, with different mechanisms to prevent and detect threats. Those

mechanisms can go from anomaly-based detection methods to statistical anomaly detection for DDoS attacks or Huestis analysis to prevent other more complex threats.

Finally, the simplicity of those devices is essential to benefit the architectures in which they are deployed. NGFWs provides the customer with a graphical user interface, which is used to monitor and control their networks. They also can help the user by reducing the complexity of the management of the firewalls.

2.6.3 NGFW'S VENDORS

NGFW are devices that can be developed and supported by different vendors in the market. The first ones come from Cisco, which is the company that leads the development of NGFWs. Cisco FirePower NGFW provides all the essential functions with its components, from IPS to DPI or sources regarding intelligent threat detection. Additionally, these firewalls can integrate perfectly with other tools coming from Cisco.

Another important NGFW vendor is Palo Alto Networks. This company is young and was fully created to develop NGFW, being its owner one of the people who worked in the early states of firewalls. Mainly because of being completely focused on the development and design of NGFW, Palo Alto was the first company to provide one of those firewalls with machine learning capabilities [14].

Finally, FortiGate, which is supported by Fortinet, is also a fast and secure responsive device applicable for enterprise-level and smaller networks. The device's SPU will also take the role of a CPU working on security functions, while the CPU takes part in other operations. The use of FortiGate, fully integrated with Fortinet, will provide the network with a robust software and hardware defence mechanisms. Apart from those vendors there are other suppliers that commercialize with NGFW, like Huawei or Forcepoint.

2.6.4 NGFW'S APPLICATIONS

Pattern recognition have been one of the best resources to detect, not only known, but also unknown threats, but these studies can be costly when done by a human. Machine learning

development is now key to produce new techniques that learn from the behaviours and different features of the wide types of malicious activity. Apart from that, many other components from the NGFWs could benefit from this new application, they could also be used to detect Advanced Evasion Techniques (AETs).

The use of NGFWs can also help with the security of IoT networks, since traditional firewalls are uncapable to protect the application layer of the network, being unable to protect the network from attacks in that layer. Traditional firewalls can protect IoT networks from layer 3 to 4, while NGFWs are able to protect it from layer 3 to 7, including the application layer.

Capítulo 3. ARCHITECTURE'S CURRENT STATE

As it was said in last section, currently RTS and Telecoms network devices work independently, each of the domains are managed separately. Even while being able to overlap themselves in the LAN to communicate with specific end point users, their firewalls are managed and designed completely different. This independency has caused at the end some inefficiencies in the performance of the network.

The system of study is conformed by 4 main networks. Those networks can be also divided in two sectors, the North Network is composed by the Kirkintilloch and Scottish Power House networks, while the South Network is composed by the Prenton and Wrexham network.

Apart from the differentiation between zones, the devices, specifically the firewalls used in the RTS, and Telecommunication network are completely different, even if their main goal is the same, filtering packets. The firewalls used in the Telecommunications network are the Cisco FirePower 2130 firewalls, those firewalls are configurated in a way that they create single points of failure, since if they fail the information cannot go through any other path.

On the other hand, the RTS network is designed we pair of high availability Palo Alto new-generation firewalls (NGFWs), which, at the moment, work in an active-passive configuration. This means that there is one firewall, the primary, which is constantly working until it fails. In the case of a failure, the backup firewall would start filtering, making possible to keep the filtering process and not stopping the flow of information.

Another aspect to take into consideration is how the system, comparing north and south, is not symmetric, which at the end makes it more difficult to operate, update or scale. In Figure 14, a high-level representation of the system which will be studies in this project is presented.

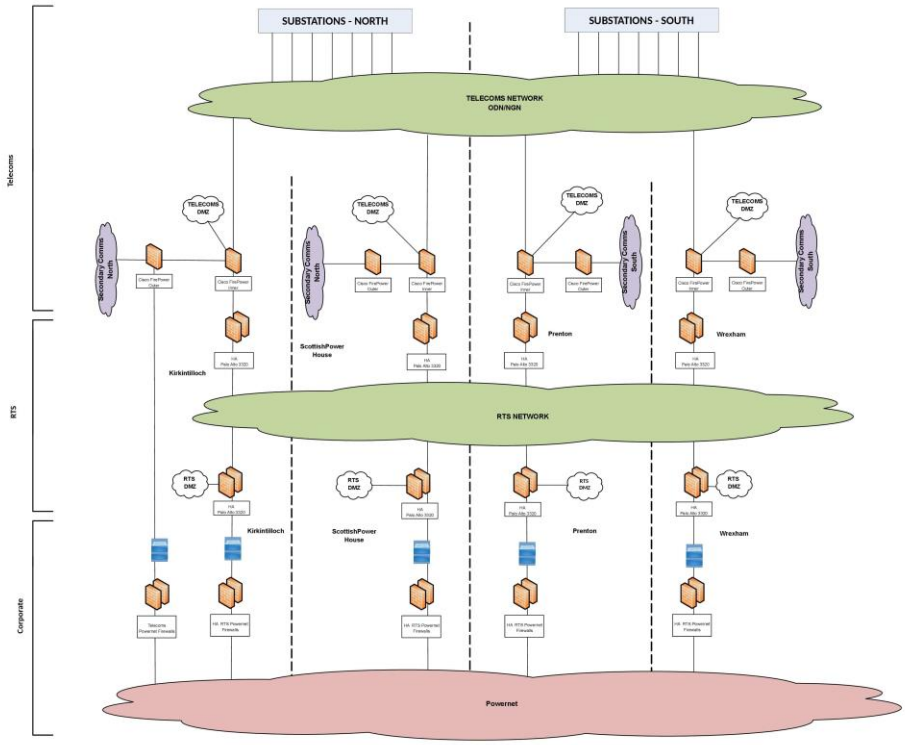


Figure 14: Architecture's current state

The new architecture will be intended to be designed in a way that the system achieves high redundancy with a high availability system. The final design must be capable to keep the information flowing, even in the case of a failure. In the following sections, a study of the actual and other firewalls technologies will be performed, considering its high availability configuration.

Capítulo 4. CISCO'S FIREWALLS REVIEW

4.1 ARCHITECTURE INTRODUCTION

The actual architecture of the firewalls inside the Telecommunications network is built with Cisco FirePower firewalls, from Cisco Advanced Services. A gap analysis was performed in order to provide a wide view of the current configuration, feature or functionality for Cisco FirePower in SPEN's network.

The review of the architecture will study the following devices:

- Cisco FirePower Management Center (FMC) for VMWare v6.6.4 (x1).
- Cisco FirePower Management Center (FMC) for VMWare v6.6.a (x3).
- Cisco FirePower 2130 FTD v6.6.4 (x2).
- Cisco FirePower 2130 FTD v6.6.1 (x6).

4.2 CUSTOMER ENVIRONMENT

4.2.1 BUSINESS OVERVIEW

Cisco FirePower firewalls can be found in different parts of the SPEN architecture, specifically in four: the Scottish Power House, Kirkintilloch, Prenton and Wrexham. The topologies of these zones will be covered in this project. The Scottish Power House (SPH) network, shown in Figure 15, is formed by two Cisco FirePower 2130 connected as inner and outer firewalls. Both firewalls are connected to the Cisco FirePower Management Center, which acts as the manager. Moreover, the outer firewall is the one connected to the demilitarized zone (DMZ), the Leidos management circuit and the Future P-Net services. In the case of the inner firewall, it will only be connected to the internal enterprise.

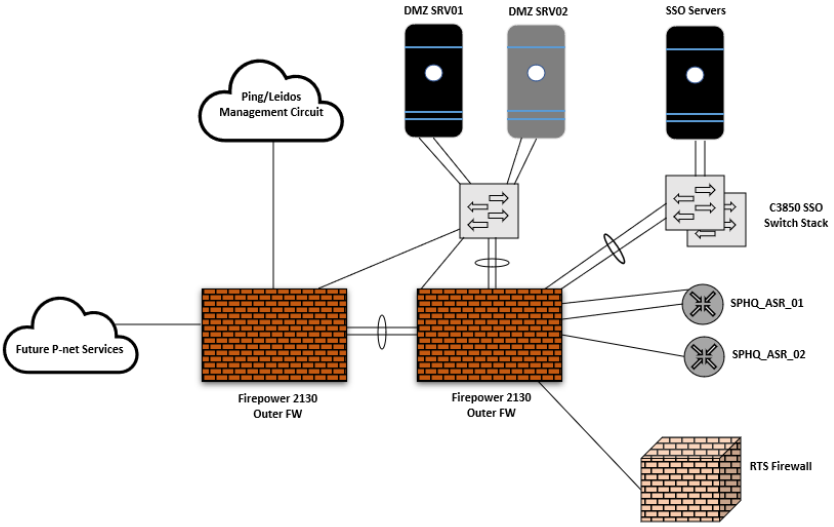


Figure 15: SPH Cisco FW architecture

Kirkintilloch (KRK) has a slightly different configuration than the SPH network, as seen in Figure 16. It also has two Cisco FirePower 2130 firewalls, acting as inner and outer firewalls. In this case, both devices are connected to the virtual machine which runs Firepower Management Center.

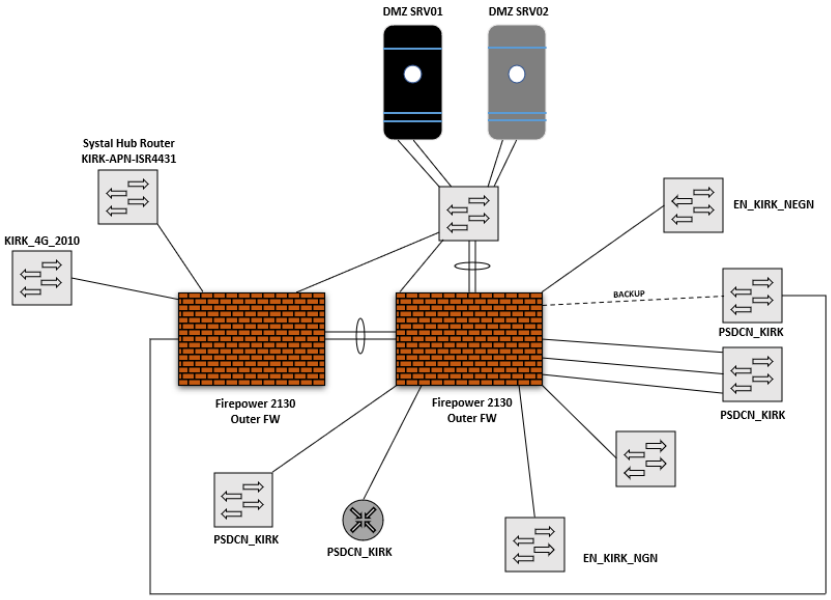


Figure 16: KRK Cisco FW architecture

The firewall's architecture from Prenton (PRN), Figure 17, has the same topology as the one from SPH. It has two, inner and outer, Cisco FirePower 2130 firewalls connected to a virtual FMC between the DMZs and the DMZs, the Leidos management circuit and the Future P-Net services.

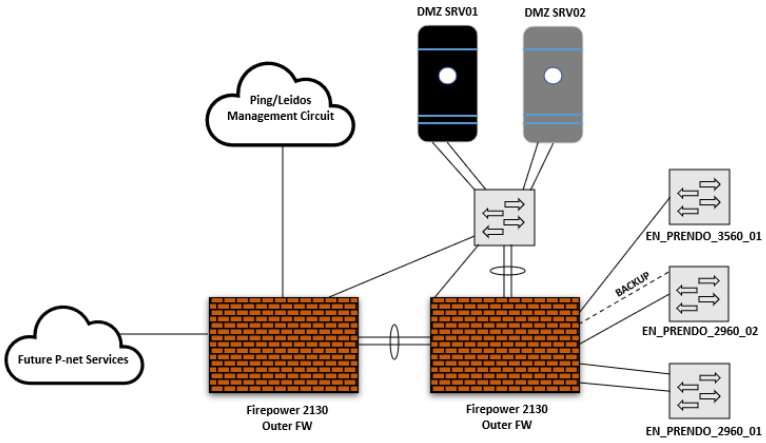


Figure 17: PRN Cisco FW architecture

Finally, the last headquarter, the Wrexham (WRX) network, Figure 18, also has two of the Cisco FirePower 2130 firewalls connected to a unique virtual FMC connecting to the Future P-Net services and the DMZs. For this last case, no Leidos management circuit was deployed.

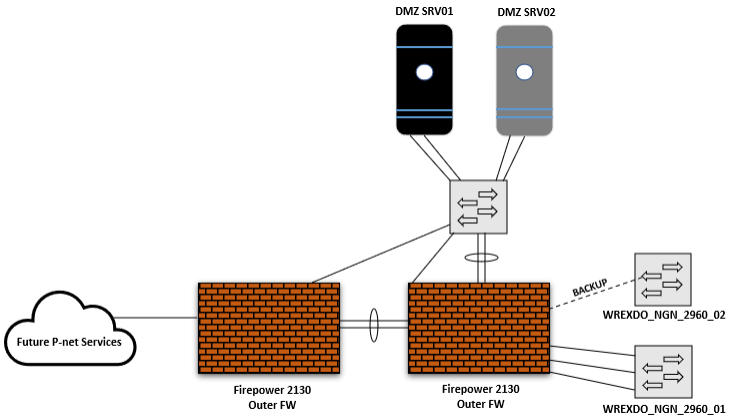


Figure 18: WRX Cisco FW architecture

4.2.2 LIFECYCLE OVERVIEW

As a way to have a better understanding of the deployed architecture, the lifecycle of its devices is something to take into consideration. There can be many reasons to consider than any device has reached the end of its lifecycle. Those causes can be technology innovation and development driving changes, or as simple as that the device mature over time and must be replaced by other functionality richer alternatives. The end-of-life milestones from the firewalls deployed can affect their performance on the network. The most common end-of-life milestones that need to be considered, when it comes to firewall's architecture design, are the following:

- End-of-Life Announcement Date: the user will be documented with the end-of-sale and end-of-life of life of the device.
- End-of-Sale Date: this date determines the last date to order the product from Cisco point-of-sale mechanisms. After that date, the product will not be for sale.
- Last Ship Date: last date in which a ship can be requested at Cisco or its contract manufacturers.
- End of Routine Failure Analysis Date: last date in which it can be determined the cause of a failure or defect in hardware through a routine failure analysis.
- End of New Service Attachment Date: this date is considered for equipment and software which was not included in service-and-support cover contract. It is the last date in which a new service-and-support contract can be requested, or an equipment or software can be added to an existing contract.
- End of Signature Release Date: date in which there will not be more signature update releases for Cisco FirePower devices going End-of-Life.
- End of Service Contract Renewable Date: last date to renew, or extend, a service contract for a product/device.
- Last Date of Support: last date to receive support or applicable service for the product acquired by active service contracts or any other warranty terms and conditions. Once the date passes, the support service becomes unavailable, and the products ends up becoming obsolete.

The Cisco's Next Generation Firewall (NGFW) Product Line Software Release Train provides, every year, two new features, usually every 6 months. There are different types of releases that Cisco deploys. The first one is the Long-Term Release (LTR), which is launched during the first half of the year. These releases are recommended for users interested in longer support durations. Another type of release is the Extra Long-Term Release (XLTR), which is the one chosen for government certifications, a year in which XLTR is shipped, LTR will not. These releases, as LTR, are launched during the first part of the year. Lastly, Short-Term Release (STR) are deployed during the second half of the year and is recommended to users who are looking for the latest set of feature release.

Cisco NGFW Software releases follow a numbering format W.X.Y.Z. The releases are notified with the change of one of the four numbers or digits. A change in W will imply a bigger change than a one in Z, following that logic with the rest of the digits. Changes in those digits can be caused by different reasons:

- Changes in W: significant infrastructure or architectural changes related to the software.
- Changes in X: introducing new enhancements, functions or any other feature.
- Changes in Y: bug/security fixes.
- Changes in Z: critical fixes based on the current demand.

Regarding the configuration of the Cisco FirePower firewalls across the network follow some common rules. In advanced setting of the policy the setting which are enabled are the following:

- Retry URL cache miss lookup.
- During policy apply, traffic will be inspected.
- Threat intelligence Director is enabled.

After the analysis of the current architecture of the Cisco FirePower 2130 firewalls some issues were assessed and recommendations for a possible update of the design in the architecture and firewalls were studied.

4.3 FOUND ISSUES AND RECOMMENDATIONS

4.3.1 GENERAL ARCHITECTURE

Regarding Firewall Threat Detection (FTD), the configuration is not High Availability (HA). A HA or failover setup joins two devices so that if the considered as primary have any kind of failure or error, the other one, the secondary, takes over. With that configuration the network can keep operating while the failure is being analysed and treated. The recommendation for this case is to configurate the architecture with two, identically configurated, FTDs connected through a failover or state link. These devices will have to communicate over that link to determine which unit would operate the network and to synchronize any changes in their configuration if the failover link is the one adopted. For the case of state link, the system would pass information to a standby device to maintain the connection inn the network in the case of a failover event.

Analysing the operation of the Firewall Management Center (FMC) it was also studied the benefits that its configuration in HA would benefit the architecture. HA feature allows the user to manage devices with a redundant FMC, which would ensure the continuity of the operations. FMC can work under Active/Standby HA configuration, being the active the one unit which would manage the devices, and the standby unit the one which would not actively manage them. Synchronization to share communication within the units is essential, this feature would permit the active unit to write configuration data into a data store, replicating data in both units. It should be noted that, as in the FTD case, if the active FMC fails, the one in standby mode would take over and continue the operation in the network, promoting it as the new active unit.

4.3.2 SCOTTISH POWER HOUSE

Focusing on Scottish Power House (SPH), three aspects have been studied: the Firewall Management Center (FMC) and the inner and outer firewall of its infrastructure. Regarding FMC several issues were analysed:

- Reporting missing: recommended to generate reports monthly for a better understanding of the operation of the unit.
- VDB automatic updates are missing: recommended to be daily checked to have an updated database, essential for the security from different vulnerabilities.
- Configure SNMP traps: no trap configured for the Access Control Policies, is a good practice to enable traps in the devices. It would save network resources and negatively impacting agent performances.
- Configure Change Reconciliation: recommended feature which is not currently implemented in the FMC configuration.

As regard to the firewalls other issues have been detected in the operation and configuration of these devices:

- CSS Styles loading issue in Chrome 85, IE and Edge browsers: the bug happening is the CSCvv5746 and is present on the latest version of Edge and Chrome browsers. This error occurs when the CSS is not getting applied when switching to a different theme. If the theme is not the default one and the browser is not the latest version, the issue appears. The recommendation of this issue is to set the device in unstable state when it occurs. Also, open the FDM UI in Firefox browser and switch to "Default Color Theme".
- Threat score disposition override setting decreased below default: the setting of the "Override AMP Cloud Disposition Based upon Threat Score" is established below 76 (Very High). To increase the security of the firewalls' operations, the value 76 is the setting recommended.
- Static route where the next-hop IP address is not the same IP subnet as the interface associated with the route: this feature can be critical since its used to determine the best path to efficiently send information and data to their final destination.

4.3.3 KIRKINTILLOCH

The Kirkintilloch network has also been deeply analysed. The study, as in the case of SPH network, is divided in two technologies: FMC and firewalls. In the case of the Firewall

Management Center, the founded issues had the same nature as the ones studied in SPH network. There are reporting and VDB automatic updates missing. Also, there are not traps configurated for Access Control Policies and no configuration for the change reconciliation.

Regarding firewalls, there's also loading problems from CSS Styles in browsers such as Chrome 85 or Edge and the threat score disposition setting is below the default one. In regard to firewalls there have been found new issues in the devices from this zone. There was a software crash detected in the last 30 days of the study because of a line crash and there was also a full usage of one of the firewalls, a review on the disk usage and the platform logs is recommended.

4.3.4 PRENTON

The Prenton network was also studied in the same way as the other environments. In the case of the Firewall Management Center, it was discovered that it had the same issues as the other zones, KRK and SPH. Reporting and VDB automatic updates missing and no configuration for SNMP traps. Focusing on firewalls, as it happened with the FMC, some issues of the same nature were found: CSS Style loading issue and threat score disposition override setting below the default configuration. A new and important problem found for one of this network's firewall is that the packet captures are configurated. This can potentially decrease performance and raise CPU from the device. Captures cause a CPU spike, this configuration should be used for troubleshooting traffic flow issues, and, after troubleshooting, the setting should be off.

4.3.5 WREXHAM

The analysis of Wrexham environment shown similar results, compared to the other networks already commented. Considering its FMC, reporting and VDB automatic updates are missing, and traps should be configurated for the Access Control Policy. For this specific environment only CSS Styles loading issues in browsers were contemplated in both firewalls. Table 1 shows a summary of those issues and their importance.

4.3.6 ISSUES' SUMMARY

Table 1: Issues analysis and their importance

Element	Issue	Importance
A1	FTD are not in HA configuration	High
A2	FMC in HA	High
SPH-FMC1	Reporting missing	Low
SPH-FMC2	VDB automatic updates missing	Low
SPH-FMC3	Configure SNMP traps	Medium
SPH-FMC4	Configure Change Reconciliation	Medium
SPH-FW1	CSS Styles loading issues in Chrome 85, IE and Edge browsers	Low
SPH-FW2	Threat score disposition override setting decreased below default	Medium
SPH-FW3	Static route where the next-hop address is not in the same IP subnet	High
KRK-FMC1	Reporting missing	Low
KRK-FMC2	VDB automatic updates missing	Low
KRK-FMC3	Configure SNMP traps	Medium
KRK-FMC4	Configure Change Reconciliation	Medium
KRK-FW1	CSS Styles loading issues in Chrome 85, IE and Edge browsers	Low
KRK-FW2	Threat score dispositions override setting decreased below default	Medium
KRK-FW3	Software crash detected 31 days ago	Low
KRK-FW4	100% disk usage and platform logs	Medium
PRN-FMC1	Reporting missing	Low
PRN-FMC2	VDB automatic updates missing	Low
PRN-FMC3	Configure SNMP traps	Medium
PRN-FW1	CSS Styles loading issues in Chrome 85, IE and Edge browsers	Low
PRN-FW2	Threat score disposition override setting decreased below default	Medium
PRN-FW3	Packet captures enabled	High
WXR-FMC1	Reporting missing	Low
WXR-FMC2	VDB automatic updates missing	Low
WXR-FMC3	Configure SNMP traps	Medium
WRX-FW1	CSS Styles loading issues in Chrome 85, IE and Edge browsers	Low

Capítulo 5. CURRENT ROUTING REVIEW

5.1 SPEN NETWORK HIGH-LEVEL OVERVIEW

The network connectivity from Scottish Power can be divided, from a high-level perspective, into five main networks domain:

- E-Terra.
- ICOND: used in both, North and South.
- NGN: used in both, North and South.
- Powernet.
- Telecoms.

5.2 RTS CONNECTIVITY REVIEW

Figure 19 shows the full RTS connectivity, being divided into various networks and different domains. RTS DMZ are included in this diagram. The key domains considered for the RTS Managed Estate are the following: RTS E-Terra, ICOND North, ICOND South and RTS Development Network.

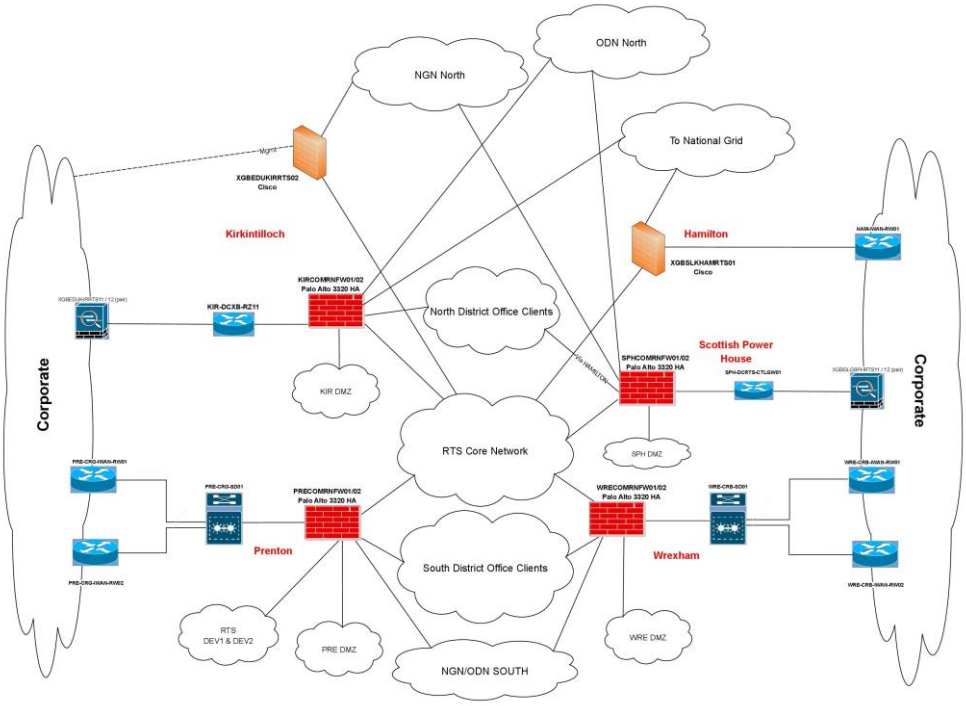


Figure 19: RTS connectivity overview

Every domain is deployed in a way that it's separated in their own OSPF instance. Those instances are designed in a way that will always create a dynamic routing, ensuring the best/shortest path. In case that any failure or error occurs at any path or any link, a dynamic rerouting would occur.

Looking into the details of the OSPF and routing for the High-Availability (HA) Palo Alto Firewalls (the firewalls in red in the diagram form above), some functionalities can be overviewed. Regarding OSPF areas, in the South of the SPEN network, Prenton and Wrexham, the pair of HA firewalls have two virtual routers configured, covering two different areas from the network. On the other hand, for the North part of the network, Kirkintilloch and SPHQ, there's only one area configurated. Furthermore, the NGN connection between RTS and Telecoms in Kirkintilloch is made with Cisco firewalls, whereas in the connection in SPH is with the combination of both, Cisco and Palo Alto firewalls.

When we look at the OSPF neighbours of the different parts of the network, in the South part of the network, the OSPF relationship between Telecoms and RTS proceed from the RTS HA firewalls pairs. RIP protocols are also being sued to redistribute between RTS and Telecoms OSPF protocols. In the case of the North lands, the OSPF relationship between RTS and Telecoms goes to the KIRLANSW03 switch, behind the RTS HA firewalls pairs. As in the case of OSPF areas, there is extra relationship with NGN in the South, compared to the North lands.

Other characteristics of the actual architecture and routing techniques shows that the South lands have 10 times a greater number of routes, using OSPF protocol, than North lands. Moreover, as described before, South lands' Palo Alto HA firewalls also use RIP protocol, which is not the case for the ones deployed on the North. Finally, North uses more static routes, with some dynamic OSPF routing techniques, while South relies more on dynamic routing, OSPF and RIP, with some static routes.

5.3 E-TERRA ANALYSIS

The connectivity between the primary sites of the E-Terra is shown Figure 20. The blue connections represent the RTS North EMSR Links. This network also uses OSPF routing protocol between the different sites as redundant circuits. The different areas of this specific schematic are the following:

- Area 0: Kirkintilloch; Hamilton; Scottish Power House (SPH); Prenton; Wrexham.
- Area 1: Kirkintilloch; Hamilton; Dewar Palace.

There are also different static routes set on the RTS devices from both, North and South lands, for E-Terra network.

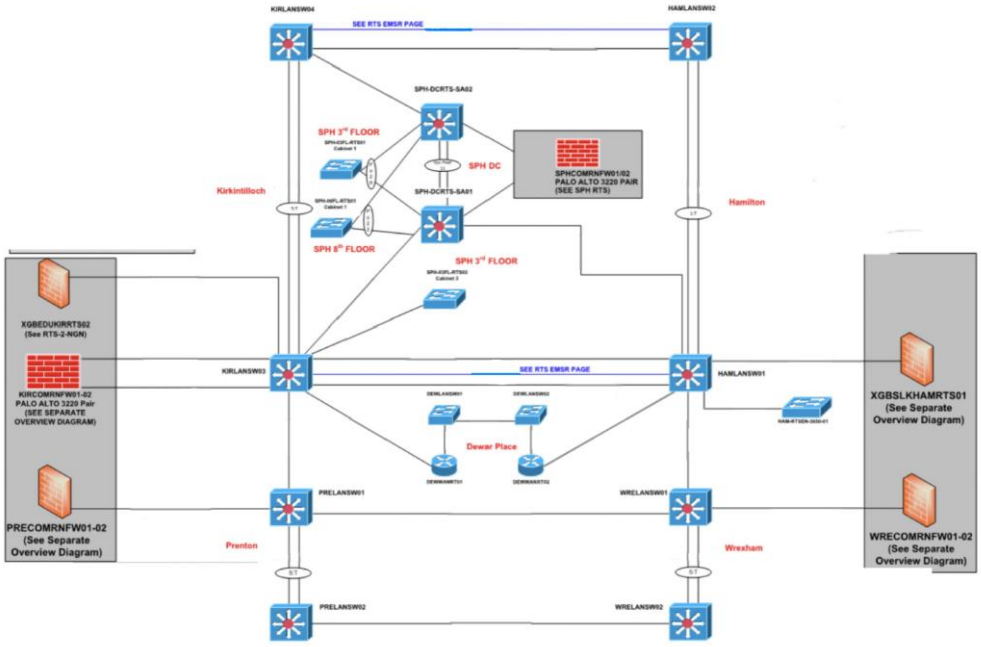


Figure 20: E-TERRA network overview

5.4 I-COND NORTH ANALYSIS

The ICOND North network include the respective district office/depot client sites within the network. This is shown in the Figure 21, in which it can be seen how SPHQ connectivity is performed via a switch in Hamilton, however Hamilton LAN has no direct connectivity to the ICOND. This network also uses dynamic routing (OSPF) between sites. The OSPF areas for this case are the following:

- Area 0: Kirkintilloch; Hamilton; Scottish Power House (SPH).
- Area 1: Kirkintilloch; Hamilton; Berwick; Galashiels; Kilmarnock; Dumfries; Telferton.
- Area 2: Kirkintilloch; Hamilton; Glenrothes; Cambuslang; St Vincent Crescent; Bonnybridge.

It also must be noted how at the end of the network the firewalls are connected. The devices will filter the traffic and decide if it can be allowed or denied inside the network. Those firewalls are the following: SPHCOMRNFW01/02 & KIRCOMRNFW01/02.

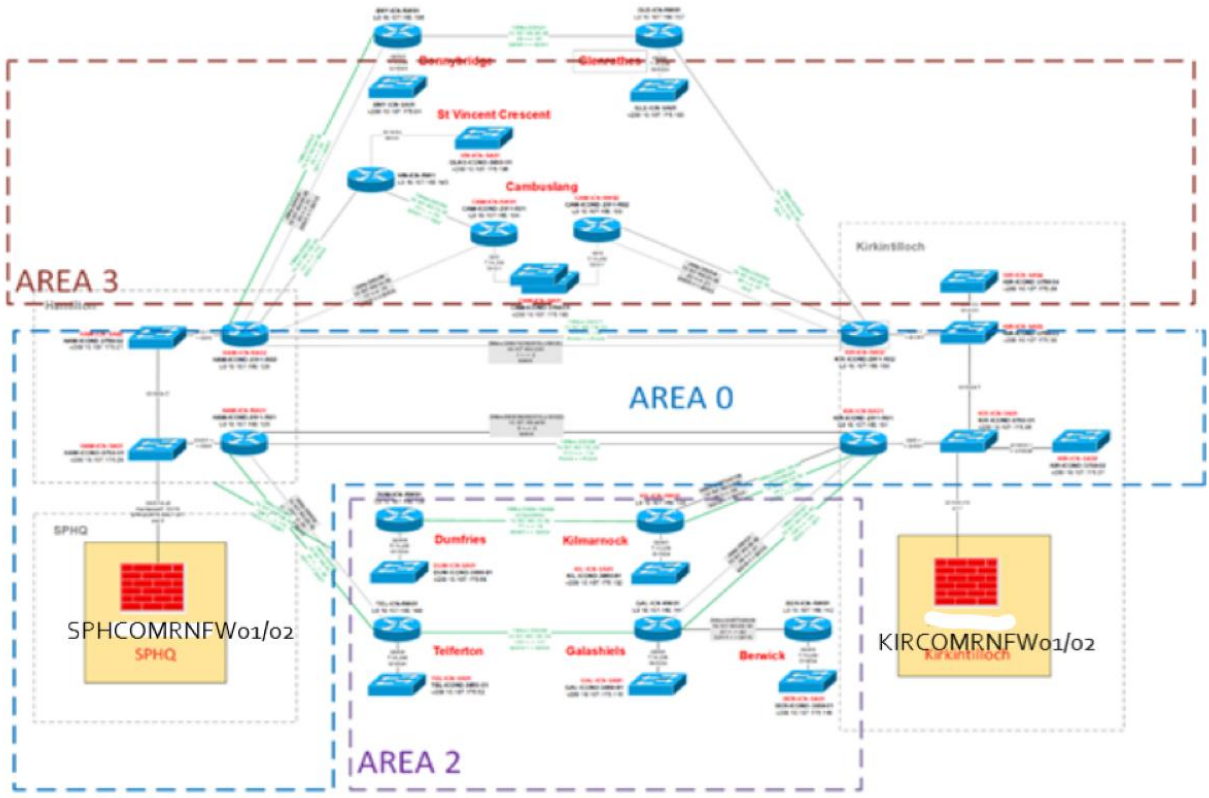


Figure 21: I-COND North network overview

5.5 I-COND SOUTH ANALYSIS

The ICOND South network is also known as the Power-on Depot Network. This network also uses OSPF as a dynamic routing technique. The area used for this network is Area 10 which is composed by the following zones: Prenton; Wrexham; Waunfawr; Middlewich; Warrington; Caernarfon; Rhyl; Llandudno Junction; Caernarfon; Aberystwyth; Chester; Oswestry; Queensferry; Lister Drive 'B'; Liverpool; Bootle; Crewe. As the case of the other networks, this one also has redundant circuits between sites, using OSPF routing to find the best path in case that there's any link failure. The OSPF instance is only using Area 10 for

this case, there can only be 1 single OSPF area for ICOND South network because, without an Area as the backbone, you cannot have multiple areas. Figue 22 shows the schematic of the network.

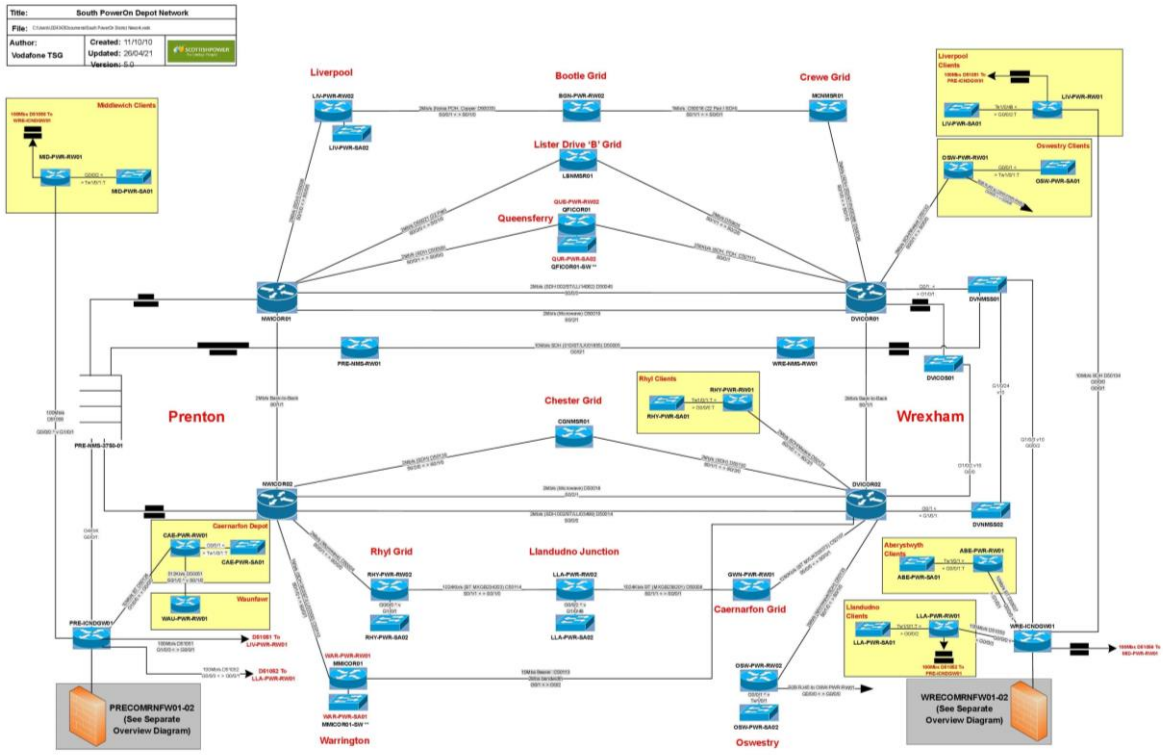


Figure 22: I-COND South network overview

5.6 RTS DEVELOPMENT ENVIRONMENT

This RTS environment uses virtual routing and forwarding (VRF) configuration for its development network. The environment uses different OSPF areas and routing and VLANS. This virtual network configuration is shared between Hamilton, Prenton, SPH and Kirkintilloch. This environment can be seen in Figure 23.

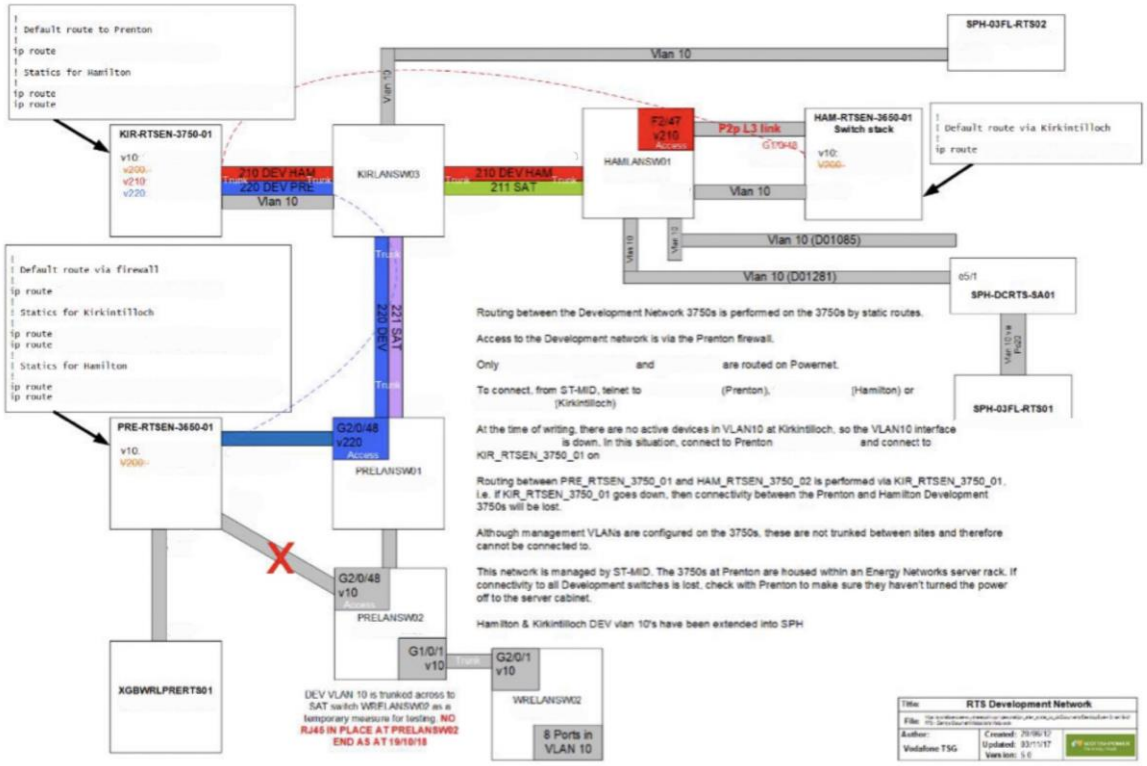


Figure 23: RTS Dev environment

5.7 NETWORK DYNAMIC ROUTING – DEFAULT ROUTE

The North E-Terra network, composed by Kirkintilloch, SPH and Hamilton, has a default route which is configured on the network switches statically. It directs traffic to Kirkintilloch firewall, KIRCOMRNFW01/02, as the primary route, then the traffic will be directed to the Powernet network. Scottish Power House and Hamilton also can distribute static default routes, known as floating static routes, allowing each site to populate the routing tables with their own route, if the primary route is removed. Many scenarios of different kind of failures would decide the next default route, those scenarios depend on where the breakdown of telecommunications occur. The standard priority if the default route is the following: first, Kirkintilloch, second SPH and Hamilton as the last one.

The South E-Terra network, composed by Prenton and Wrexham, has a default route configured on the firewalls as a static route which can direct traffic to Prenton as the primary.

For this network, the gateway device is the Prenton Control Gateway Router (PRE-CTRL-GW01). Moreover, Wrexham also distributes static default route, allowing the routing table to be updated from the site with its won default route if there is an event in which the primary default route must be removed. The priority for the default route for the South network is the following: the primary Prenton and the second Wrexham.

In all cases, failover of the default gateway device will need of a manual intervention mainly because it will not remove the static default route from the devices. The route will continue to be advertised. Default gateway is used for subnets which are not shared via OSPF within the RTS Managed Estate, such as traffic for Power-net or internet.

The service assurance agent IP SLA could be an option to monitor the failure of that default gateway, making it possible for the failover to go from a manual intervention to an automatic one. Furthermore, OSPF routing could be used instead of static routes, but this option needs to be examined to see what would be advertised form OSPF routing.

5.8 SECONDARY COMMS NORTH AND SOUTH

The Secondary Communications traffic in the North is used for remote substations, being in Kirkintilloch the primary route through the Scottish Power networks head end router. If the internal Telecom firewall suffers from a failure, the traffic from the RTS network in KRK will keep sending information to KRK Telecommunications for the Secondary Comms substation. SPH will continue sending to SPH Telecommunications. No failover occurs in RTS, like it would happen on the South lands, having a service loss until the internal Telecom firewalls regain activation. Figure 24 shows what would happen in a schematic way.

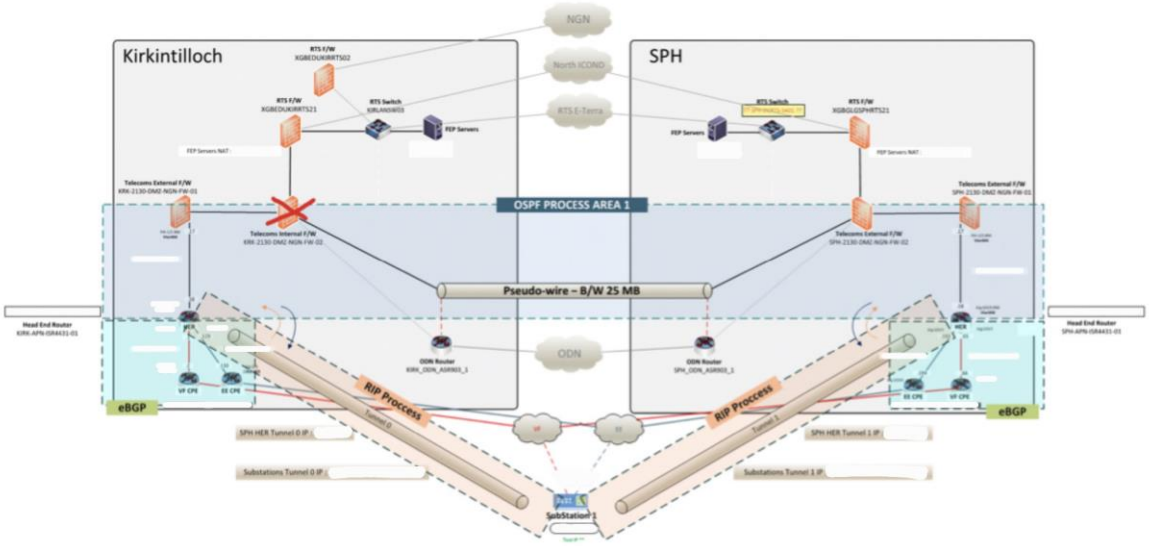


Figure 24: Secondary Comms N&S overview

In the case of the South lands' network, there's a OSPF end-to-end configuration. This means that in the scenario in which there's a failure in Telecoms, RTS can detect it and use an alternative RTS route to the other site, out to the Secondary Comms substations.

A recommendation for future configurations would be the use of dynamic routing for North's RTS and telecoms in the same way as in the South, achieving a redundant network. As a short-term solution, the inner FW could use a pseudo-wire between them to being able to achieve failover, this would cover many scenarios, but nothing close to a HA system. Since those inner FW are single points of failure (SPFs) a resilient configuration considered as HA could be designed with a pair of Palo Alto FW for the inner firewalls, and the 2 existing Cisco 2130 FW as the outer firewalls. Changing all Cisco and deploy a complete Palo Alto infrastructure could also be a reliable option. Figure 25 shows what the combination of both models would look like.

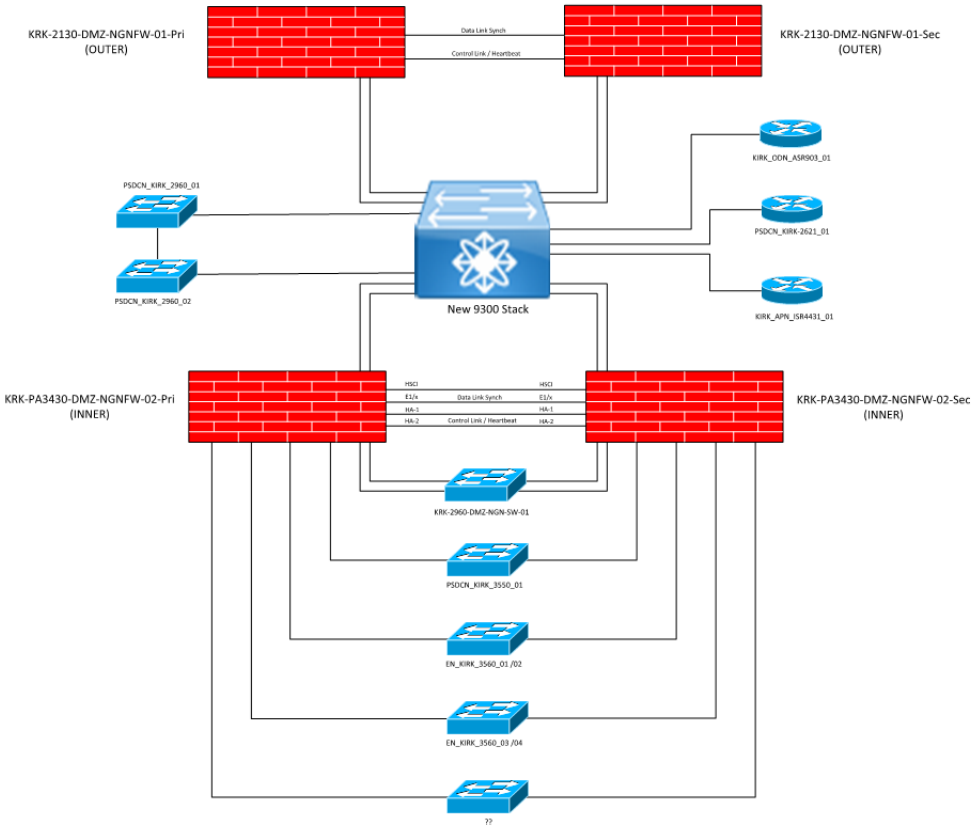


Figure 25: HA architecture Cisco

5.9 ROUTING SUMMARY

This section tried to describe, from a high-level perspective, the SPEN estate. This part of the section is dedicated to summarizing and describe some routing and administration practices that would help in the implementation of future implementations for new network designs. Firstly, it needs to be acknowledged that having a new routing design is a large fix and will need of a great amount of time and resources.

RTS and Telecoms networks are currently being managed and maintained by three different companies: Systal, Leidos and Magdalene. In the Telecoms network the firewalls are being managed by Leidos, but they will be changed by Systal in the future. This change will help with a quicker response in business-as-usual activities and any resolution regarding incidents, such as faults or malfunctions from assets managed by Systal.

As it was detailed during this section, there are two parts in the SPEN estate that differ not only in geographical terms, but also in some practices inside their networks. The North is characterized by the use of static routing to send traffic between devices or for default routes. On the other hand, the South networks use more dynamic routing protocols. This redundant method permits the change in the routing layout due to any failures of link or devices that might occur in the network, which make it a more advantageous option.

Another potential issue is the fact that in Telecoms network Cisco 2130 firewalls' setup is in such a way that creates a SPF, whereas in RTS network the Palo Alto FW are configurated as HA pairs, being more resilient to failures and permitting a more redundant architecture. For future network designs upgrades in the network regarding redundancy must be treated.

Finally, some OSPF practices that will need to be considered for future deployments or configuration of network are the following:

- Summarization Techniques: the summarization is essential for two main reasons, firstly, to limit the number of routes in an area, especially in the backbone. Secondly, it's important to minimise the impact of flapping links. These techniques can be really useful more intra-area routes. Also, in an area with multiple Area Border Routers (ABRs), which is also useful in terms of redundancy, summarization should be configurated in all ABRs. Even though it helps with redundancy, the number of ABRs needs to be reasonable, to limit the number of summary Link State Advertisements (LSAs) inside the domain.
- Router ID: use router-id command to configure a deterministic router ID for OSPF process. Choosing the router ID from the same OSPF area address space the router belongs to will be helpful for summarization for the cases in which the router IDs need to be routed.
- Process ID: it has local significance to the router, recommended to have the same for any router that works under the same OSPF domain. By making this, configuration consistency will be improved.

- Authentication: MD5 authentication between OSPF neighbors can be configured if security is a key feature of the network.
- Area Size: the routing table should not be big, not only in terms of possible routes, also routers.
- OSPF flood reduction: can be enabled on a router if it can be supported. This ability can minimize the LS aging process in a link device. This ability needs to be furtherly considered if neighboring router does not support DC bit mainly because it could be the case that it does not work.

Capítulo 6. ARCHITECTURE'S FIREWALLS REVIEW

This section will consist of a more technical review of, not only the firewalls that are being currently used, but also about the new model that is being considered for the future design of the infrastructure. After the study, a comparison between the different models will be performed.

6.1 CISCO FIREPOWER 2130

The Cisco Firepower 2100 Series is a four-threat-focused security platform family which have the ability to deliver a higher performance threat defense and resiliency to the business and telecommunications infrastructure. Exceptional sustained performance can be achieved while their advanced threat functions are being used. Cisco Firepower 2100 Series' platforms incorporate a dual multicore CPU architecture which provides the system with firewall, threat inspection and detection, and cryptographic functionalities. Network Equipment Building Standards (NEBS)-compliance is supported by the model used in the TELECOM SYSTEM, the Cisco Firepower 2130 platform. These devices can operate with the Secure Firewall ASA or Threat Defense software [15].

In the case of 2100 Series working with Cisco Threat Defense software, the total throughput that the Cisco Firepower 2130 is capable of is 5.4 Gbps with a maximum concurrent session, considering AVC, of 2 million, also the maximum new connections per second is of 30K. The Transport Layer Security have a capacity of 760 Mbps and its IPSec VPN throughput of 1.9 Gbps and maximum VPN Peers of 7500. Other characteristics of these model are the existence of a local management system, known as Cisco Firepower Device Manager or the capacity from the Application Visibility and Control (AVC) to support more than 4000 applications, including geolocations, users or websites. Moreover, the model's security intelligence is composed of IP, URL and DNS threat intelligence. Also, its NGIPS can passively detect endpoints for Indicators and Compromise intelligence and threat

correlation. Cisco's AMP for networks can detect, track, block, analyse and contain targeted malware, working on that attack not only during the event, but also after. Regarding URLs, the number of URL filtering categories are more than 80 and the number of the URLs categorized more than 280 million. Finally, other features are the automated threat feed and IPS signature updates, the third-party and open-source ecosystem, its capability to perform as a high availability and clustering node, in an active/standby configuration.

On the other hand, using ASA software, the stateful inspection firewall throughput is of 10 Gbps under ideal conditions, reduced to 5 Gbps when traffic consists mostly of TCP-based protocols, but applications like HTTP or SMTP are considered. For this configuration the concurrent firewall connections and the maximum VPN peers stay the same, but the new connections per seconds is increased to 40K and the IPSec VPN throughput is reduced to 1 Gbps. Using this software makes it possible to achieve high availability working under both, active/active mode and active/standby mode. Clustering and scalability, with VPN load balancing, are considered for this case. Also, with this software in can also be managed centralized by Cisco Security Manager or alternatively in the cloud with Cisco Defense Orchestrator.

6.2 PALO ALTO PA-3220 FW

Palo Alto Networks PA-3200 Series appliances secure traffic, including the encrypted traffic with the use of processing and memory for security, management, networking, and threat prevention. PAN-OS software is the controlling element of these devices. The software can classify all traffic, which includes threats, contents and other applications, in order to traffic it to the user at any location and device type. The application, content and user will then be used to create the security policies, which will reduce incident response time and improve the security posture of the system. The key characteristics of these devices can be classified in different features and are presented below [16].

1. Machine Learning Powered.

These new generation of firewalls uses machine learning (ML) to provide attack prevention for file-based attack all the while it can identify and stop at the moment phishing attempts never experienced by the system. It uses cloud-based ML processes which help to achieve a no-delay response to the NGFW. The device can also use behavioural analysis to detect IoT devices and automates policy recommendations to the operator, reducing chance of human errors and saving time.

2. Identifies and categorizes all applications and port constantly with full Layer 7 inspection.

The firewalls can detect any applications going through the network, regardless of encryption, port, or any evasive technique. It can automatically discover and control new applications and uses the applications as the core for any safe enablement policy decision, identifying all data within the application to block and report any malicious file. Creation of App-ID tags for proprietary applications are possible. Finally, it also offers safe migration of legacy Layer 4 rule sets to App-ID-based rules, creating a rule set which is not only easier to manage but also a rule set more secure.

3. Security is implemented for users regardless of device or location, while adapting policy based on user activity.

The devices can enable security policies, visibility or reporting based, not only on IP addresses, but also on users and groups. They can integrate in different repositories to leverage user information and even allow dynamic user group. The policies established are consistent and irrespective of devices or users' locations. The enforcement used in terms of security prevents the leak of credentials to third-party websites and enables multifactor authentication, preventing the reuse of credentials stolen. At the end the device provides dynamic security processes which constantly authenticates and authorizes the users, restricting suspicious users and activities, moving toward a Zero Trust security posture with Cloud Identity Engine.

4. Detect malicious activity concealed in encrypted traffic.

The technology applies policy to TLS/SSL-encrypted traffic, including traffic that uses other types of packets such as HTTP/2 and TLS 1.3. It has the capacity to visualize into TLS traffic without decrypting it. It also lets the user enable and disable decryption flexibly and permits decryption mirroring for historical purposes or data loss prevention. The Network Packet Broker feature makes it possible for the firewalls to forward all traffic to third-party security tools, improving performance and reducing costs.

5. Centralized management and visibility.

Panorama network security management is a one united user interface which permit a centralized visibility, management, and configuration of the various Palo Alto NGFWs in the network. The Application Command Centre (ACC) also provides the user with insights and deep visibility of the network's traffic and detected threats.

6. Use of AIOps to maximize security investment and prevent disruptions.

AIOps for firewalls delivers customized recommendations for every unique deployment, securing the investment. It also predicts the performance, health, and capacity problems that the firewalls might have with its ML capacities, giving insights on predicted disruptions.

7. Cloud-delivered security services have a role in advanced threats' detection and prevention.

Today's multiple threat vectors and advanced techniques to deliver cyberattacks makes the traditional strategy go obsolete, causing big challenges to the organizations in terms of cybersecurity, security gaps and inconsistencies in access and visibility of their network. Cloud-delivered security services for firewalls can instantly coordinate intelligence and protect the network across all vectors. The services include for this specific feature are the following:

- Advanced Threat Prevention: stop malware, spyware, or any command-and-command (C2) threats. It prevents 60% more unknown attacks and 48% more C2 threats than traditional solutions.

- Advanced WildFire: 60x faster process to ensure the safety of the network by preventing all kinds of threats, including unknown and C2 threats.
- Advanced URL Filtering: permits safe access to the internet reducing the risk on web-based attack by 40% and 88% of malicious URLs threats are detected 48 hours before other companies' models.
- DNS Security: no changes in the infrastructure are needed to gain a 40% more threat coverage and stop nearly 85% of the abuses that a DNS deployment may experience.
- Enterprise DLP: this service brings the risk of data breach to a low level, achieving a twice greater coverage than any other enterprise DLP.
- SaaS Security: enables the user to see and secure all apps across all protocols.
- IoT Security: implement Zero trust device security faster than any other model.

8. Packet processing with single-pass architecture.

A single device can perform multiple functions with a lower amount of processing with its single-pass architecture. Only a single pass is required to perform different tasks, such as policy lookup, decoding or networking, reducing latency on the system.

9. SD-WAN functionality.

It can adopt SD-WAN on already existing firewalls, with a safely implementation and minimizing latency and packet loss with an end-user service.

The performances and capacities of the PA-3200 firewalls' family have other quantitative capacities that need to be highlighted. The firewall throughput of the firewalls used in the Scottish Power network infrastructure, the PA-3220, has a value which goes from 3.7 to 4.2 Gbps. The Threat Prevention throughput has a lower value, going from 1.9 to 2.3 Gbps. In the case of the PA firewall the IPsec VPN throughput ends up with a value of 2.4 Gbps, max sessions of 1M, new sessions per second of 46k and maximum number of virtual systems of 6, being 1 the base case.

6.3 PALO ALTO PA-3430 FW

This new model has most of the capabilities and features that the past PA firewalls had. PAN-OS software is still the one used to classify traffic, threats, and any content regardless of the device or the location. PA-3400 Series includes the key security and connectivity features that the PA-3200 Series had. The new series are still a machine learning powered firewall, with the capacity to learn from error threats to automatically detect new ones. They also have the ability to identify and categorize, with full layer 7 inspection, any port or application at any time. The series adapt policy based on user activity while enforcing security for the user, regardless of device and location. PA-3400 series can also detect malicious activity inside encrypted traffic and offer centralized management and visibility. They also prevent business disruption with AIOps, and its cloud-delivered security devices can detect and prevent unknown threats. As the PA-3200, the new series enables SD-WAN functionality and provides the user with a single-pass architecture service for packet processing. The main feature that these new series bring is the native web proxy support. They can unite firewall and proxy in one platform while still being able to manage capabilities through the centralized management software [17].

The PA-3430 performance and capabilities are the following:

- Firewall throughput: 25.5/20.5 Gbps.
- Threat Prevention throughput: 9.2/10.5 Gbps.
- IPsec VPN throughput: 12.2 Gbps.
- Max concurrent sessions: 2.5M.
- New sessions per second: 240,000.
- Virtual systems (base/max): 1/11.

6.4 FIREWALLS COMPARISON

The firewalls described above are the ones considered for the new architecture of the RTS and Telecommunication's network. Table 2 presents the most important capabilities and

capacities which all the firewalls, already described, have. Annex I presents further information regarding the firewalls specifications.

Table 2: FW capabilities comparison

FW Model	Cisco 2130	PA-3220	PA-3430
FW throughput	5.4 Gbps	4.6/5 Gbps	25.5/20.5 Gbps
Ipsec VPN throughput	1.9 Gbps	2.6 Gbps	12.2 Gbps
Max sessions	2 M	2 M	2.5 M
New sessions/second	30 k	58 k	240 k
High Availability	A/A & A/P	A/A & A/P	A/A & A/P

The firewall throughput is the volume of traffic, in Gbps, that can pass through the firewall at any given time, this feature is a must since the network needs to have enough capacity to transport all the packets to have a complete view of the network. It can be seen how Cisco FirePower and PA-3220 firewalls have a similar capacity in terms of their throughput, but the PA-3430, as a new model have a capacity nearly 5 fives higher than the other models.

The IPsec VPN throughput is the measure that provides the amount of data that can be transported with IPsec VPN connection. High volume of data traffic needs to be possible to have remote accessible system which is reliable to the user. In the case of Cisco FirePower's firewalls, they are the models with the lower rate, which make them an unattractive option for future investments if remote control is a main part of the network operations.

The max sessions, as its name imply, are the maximum number of firewall sessions the device can support. On the other hand, the new sessions or connections per second are related to the pace in which the firewall can create and store new sessions. The total number of sessions that the different devices can manage are similar, with the PA-3430 model having the most, 2.5 million. The most distinctive feature is the new sessions per second, being the Palo Alto firewalls the one with better results. A network that is intended to transport, not only great amount of data, but also different data constantly, the new sessions per second feature is one that needs to be seriously considered.

In the case of their high availability configurations, all the models can work on active/active and active/passive configuration. This make it possible for the future architecture to have a flexible design, which could change in the future if there is any change regarding amount or typology of data and the size of the network.

Capítulo 7. HIGH AVAILABILITY PA FIREWALLS

7.1 HA CONCEPTS

Palo Alto Network firewalls can be configurated in groups of two up to 16 firewalls as a high availability (HA) cluster. The firewalls in the cluster can work as HA pairs or by their own, but HA configurations can bring to minimum levels the downtime by always having an alternate firewall, in the event that one of them fails. Data is synchronized and information of the state is always maintained with the help of HA ports, which used by the firewalls that work under an HA cluster. Other information about their configuration such as IP addresses, log data or Application Command Center (ACC) will not be shared with the rest of the firewalls. All applications or log view of the different HA pairs can be supervised by Panorama software, Palo Alto Networks' centralized management system.

When a firewall fails in an HA cluster/pair, the peer firewall takes the task of securing the traffic. In firewalls, the term used for this change in the event of a failure or error is failover, The main scenarios for an error, that would deploy a failover are the following:

- Monitored interfaces failure/Link monitoring.
- Destination specified on the firewall not reached/Path monitoring.
- Firewalls not responding to heartbeat polls/Heartbeat Polling.
- Component failure/packet path health monitoring.

7.2 HA MODES

The PA firewalls can work under two HA configurations:

- Active/passive: in this case, only one of the firewalls is working with the traffic of data, the other one is synchronized and, in the case of a failover event, will start working as the primary firewall. Both share the same configurations. In the case of a

shut-down of the primary firewall, the passive will work under the same policies to maintain the specified network security. This configuration supports virtual wire and Layer 2 and 3 deployments.

- Active/active: both firewalls in the HA pair process traffic and work as active synchronously. The firewalls maintain sessions and routing operations while staying synchronized. In the case of this configuration, active/active HA clusters only support Level 3 and virtual wire deployments. Furthermore, the firewalls cannot support Dynamic Host Configuration Protocol (DCHP), only active-primary firewall can function as a DCHP Relay.

Regarding the configuration of HA clusters, it also needs to be noticed that active-active firewalls cannot balance load-traffic by themselves. A load-balancer will also be considered for the design of the architecture to have the ability to balance the load as the user considers to a achieve an even more flexible and reliable network.

In terms of which configuration use for the architecture of the network's firewalls, some other aspect needs to be taken into consideration:

1. If the final goal of the architecture is the simplicity of the network, active/passive would be the most reliable option. Routing and traffic flows are way easier to manage in that configuration. Also, active/passive configuration supports Level 2 deployments, while active/active configuration do not.
2. If the complexity of the network is not the main issue of the deployment of the new architecture, active/active configuration may be a reliable option. This configuration needs of a more advanced design, sometimes requiring the need of additional configurations on the firewalls. Those configurations would include the activation of networking protocols on all the firewalls or installing floating IP addresses to deliver the proper actions in the case of the failure of one of the firewalls. Since the two firewalls are actively trafficking data, they need to use more concepts to perform Layer 7 content inspections. This mode is recommended for architectures in which both firewalls need their own routing instances and if Scottish Power will require a

real-time redundancy from both firewalls at any time needed. One noticeable benefit of this configuration is its quick failover and its capacity to handle better peak traffic flows, compared to active/passive configurations. Moreover, this mode could temporarily manage more traffic than what one firewall could do by itself, but this is not recommended as the usual operation since if one fails the other firewall would not support all the traffic, resulting in high latency and/or application failure.

7.3 HA LINKS AND BACKUP LINKS

The firewalls set up as HA pair use links, known as HA links, which permits the pair to maintain information and share and synchronize data between them. Some of the firewalls' models have dedicated high availability ports, HA1, as Control links, and HA2, as Data links. The rest require in-band ports to be used as HA links. For the models with HA ports, these will be used, on the other hand, the recommendation is to use the management port for HA1 port, and dataplane for HA1 backup.

Looking into the different type of links, and their backups a deeper description of those utilities can be presented:

- Control link: HA1 link is commonly used to exchange HA state information, this includes hellos, heartbeats, synchronization management or any information regarding User-ID. Changes in any of the peer's configuration is also synchronized through this channel. Since it is a Layer 3 link, IP address is required.
- Data link: in the case of this link, its role is mainly to synchronize sessions, IPSec security configurations or ARP tables between the firewalls that form the HA pair. The data which goes through the link is unidirectional, it goes from the active-primary firewall, to the passive or active-secondary one. Data link is a Layer 2, using ether by default.
- Backup links (HA1 and HA2): these links are used to provide redundancy to the control and data links. In-band ports can be used as backup links for the control

(HA1) and data (HA2) connections. In order to configure correctly the backup HA links, some guidelines must be followed:

  - Prevent at all costs that the IP addresses of both, primary and backup, HA links overlap.
  - Primary and backup HA links must not share the same subnet.
  - Backup ports from HA1 and HA2 must also be configurated on different physical ports.
  - PA-3200 Series, one of the used for the actual and future architecture, cannot support IPv6 addresses for HA1 backup link. The address used is an IPv4.

- Packet-forwarding link: this link, known as HA3 link, is only required in HA active/active configurations. The link is used to forward packets to the peer when asymmetric traffic flow is occurring. It does not support Layer 3 addressing or encryption, being considered as a Layer 2 link. The firewall's Series used in the architecture can configure aggregate interfaces to work as a packet-forwarding link, adding redundancy to the link.
- HA4 link/HA4 backup link: those links are used for session cache synchronization between all HA cluster firewalls sharing cluster ID. The links also detect failures in the connectivity between different peers, using Layer 2 as the pathway.

7.4 HA PORTS

To achieve a successful connection between to PA firewalls, achieving a HA configuration, the use of HA ports, links and backup links is highly recommended. In the case of the ports, they include HA1 ports (HA1-A and HA1-B) to control and synchronize the traffic going through the HA pair, and HA2 and HSCI (High Speed Chassis Interconnect) ports for HA session setup traffic. HSCI port can also be configured to be use for HA3 traffic.

In the case of PA-3200 Series firewalls, HA1 ports are used for HA1 traffic in active/active and active/passive HA modes. HA1-A port from primary and secondary firewalls must be connected directly or through a router. HA1-B ports will be connected in the same way and will be used as a backup connection. This configuration on the ports connection will give

redundancy to the system, avoiding split brain issues in the case of device failure. HSCI ports is considered as a Layer 1 SPF+ interface, which enable HA2 and HA3 connections between a pair of firewalls.

7.5 DEVICE PRIORITY AND PREEMPTION

The priority between HA pairs of firewalls works different depending on the configuration in which they will work at the end. Firewalls in an active/passive HA configuration, will have the option to assign a device priority value, indicating which of the firewalls will take the active role. The firewall with the lower value will be considered as having higher priority, becoming the one which will be actively securing traffic.

For the active/active HA configuration, it has a similar behaviour. The device ID is used as a priority value, the firewall with a lower value in device ID will be considered as higher priority and will work as an active-primary. The other firewall will work as an active-secondary firewall.

Preemption in the devices is disabled by the default. Its activation enables the higher priority firewall to continue as active (or primary-active) after it recovers from an error.

7.6 FAILOVER EVENT

As explained above, this event occurs when one firewall suffers from a failure and its pair starts securing traffic. This event can be triggered by many scenarios, a common one is with the failure of a monitoring metric. Those metrics, used for firewall failure detection, are the following:

- Hello messages/heartbeat polling: these actions are commonly used to verify that the peer firewall is operational and responsive. These messages and pings are sent between intervals and are sent through the control link. If they are sent and the peer does not respond to three consecutive heartbeats, the connection is considered to be lost and a failure occurs.

- Link monitoring: the firewall can monitor specified link groups, monitoring each of the links' state. The user can create the failure condition. For example, if all links from a group fails, the group fails, or if just one of the links fails, the monitoring can be configured in order to consider that as a group failure. Multiple link groups conditions can also be determined, for example, if one of the link group fails, all the groups do.
- Path monitoring: it is also possible for the user to specify which destination IP addresses the firewall will monitor. It will monitor the path through the network, using ICMP pings to verify the reachability of the IP address. After ten consecutive pings, with no answer, it will be considered as unreachable. In the same way as the link monitoring, the user can specify the failure conditions, even global failure conditions. Moreover, a failover will occur when a firewall is suspended or there's an event of preemption.

Capítulo 8. ACTIVE-ACTIVE VS. ACTIVE-PASSIVE

A model in Simulink is created in order to understand in a clearer way how the different Palo Alto configuration would behave in the different studied scenarios. The engine and component library SimEvents [18] is the one chosen to perform these simulations. A model recreating an event-system system with discrete simulations will be designed, for its further use and analysis. All the models and simulations were created with MATLAB R2022b.

The first subsection will consist in an explanation of the different components of the model, its different parameters, functions, and main characteristics. It will be followed by different scenarios, the first one will consist of a case in which the failure of the firewalls participant of the architecture follows a random criterion. The rest of the subsections regarding this theme will consist of cases in which the probability of failure is not completely random but following different distributions. The first case will analyse how the system would act under a failure probability which follows an Extreme Value Distribution, being also studied different parameters for this specific distribution. The second, and last distribution studied, will be the Lognormal Distribution, also studying different parameters for this case. The different simulations will be performed to show how Active-Active and Active-Passive configurations work, comparing different parameters on the performance of each of the architecture options.

8.1 MODEL DESCRIPTION

The model created for the analysis of the different configurations consists of different parts that will be explained below. The different parameters and configurations of each of the components will be explained. The complete model can be seen on Annex II.

8.1.1 ENTITY GENERATOR

The entity generators are the blocks used to create the entities for the simulations. These entities are discrete items which represent the packages sent through the network, which will

be processed by the firewalls in the future. In this specific cases, different entity generators are displayed in the model, recreating different points of the network that send information through the system.

In Figure 26, an entity input switch can also be seen. The switch works in a way that permits the information from the different points to go through the network. The switching criterion chosen for this switch is the round robin criterion, which basically consists of letting pass the packages on a on a time, changing the input once it has sent its package. In the studied case, the criterion will follow an up-to-down criterion.

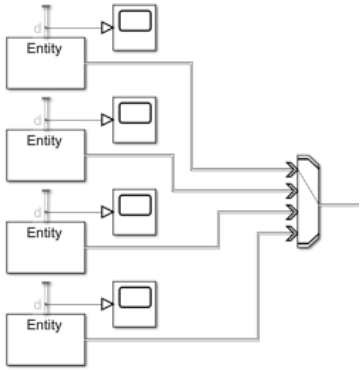


Figure 26: Entity generator diagram

Moreover, regarding the entity generators, they create packages following an exponential distribution, with a mean of one second. Equation 1 shows that distribution, being rand(1,1) a function which generates a random number between 0 and 1.

Equation 1: Entity generator intergeneration time action

$$dt = 1 \cdot \log\left(1 - rand(1,1)\right)$$

Also, it must be commented that those entities or packages of information will carry two attributes or characteristics. The first one is the size of those packages, 4 Mbps, and the other is the start time of that package, which is used in the simulation to get the time that the packages last to arrive to the final destination.

8.1.2 NETWORK DESIGN

To recreate the delay caused by the network to send the packages from the firewalls, a pair of an entity queue and an entity server was designed. The queue represents the place in which the packages are waiting in the network and the server, the time that it lasts to go from the network to the different firewalls. The cables considered for the network are the cat6, which have a capacity range from 100 Mbps to 1 Gbps, way higher than the expected throughput coming from the generators. That capacity is represented in the entity queue capacity. Figure 27 shows the diagram representing the network.

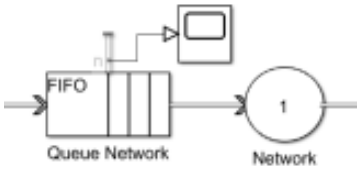


Figure 27: Network diagram

8.1.3 ACTIVE-ACTIVE FIREWALLS

The part of model design to follow how the active-active configuration works will be explained in this subsection. The active-active part of model is composed by an entity queue and a pair of entity servers in parallel, which represent the pair of Palo Alto NGFWs. They are separated by an entity gate, which closes the flow of information in the case that both firewalls fail and the routing of the packages between both firewalls is performed by an entity output switch. That switch behaviour depends on the situation in which the system is:

- No failure in any of the firewalls: the switch will send packages to both firewalls switching between one and the other.
- Firewall 1 fails: all flow goes through Firewall 2 (FW2 A-A).
- Firewall 2 fails: all flow goes through Firewall 1 (FW1 A-A).

The entity input switch at the end permits all packages to go through the entity terminator. The schematic design of this is presented in Figure 28.

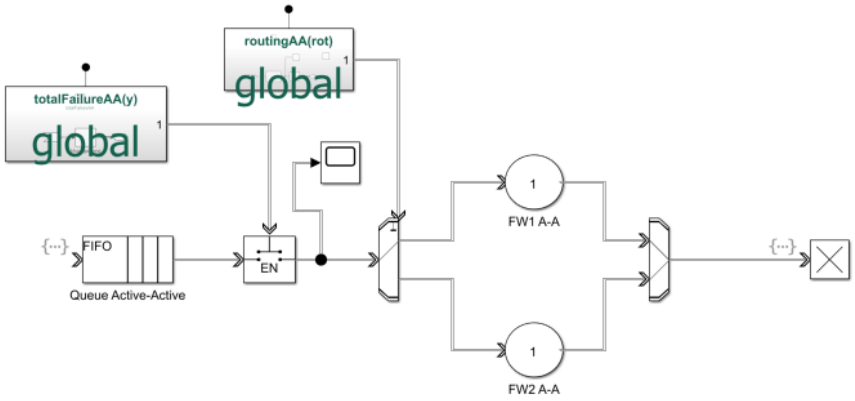


Figure 28: Active-active firewalls diagram

8.1.4 ACTIVE-PASSIVE FIREWALLS

The part of model design to follow how the active-passive configuration works will be explained in this subsection. The active-passive part of model is composed by an entity queue and a pair of entity servers in parallel, which represent the pair of Palo Alto NGFWs, the primary and the backup firewalls. They are separated by an entity gate, which closes the flow of information in the case that both firewalls fail and the routing of the packages between both firewalls is performed by an entity output switch. There is also another entity gate in the backup firewall path, used to simulate the delay caused by the change of the switching routing. The entity output switch behaviour depends on the situation in which the system is:

- No failure in Primary Firewall: all flow goes through the Primary Firewall.
- Primary Firewall fails: all flow goes through Backup Firewall.

Once the primary firewall is repaired, the flow goes back to the primary firewall with no delay. The entity input switch at the end permits all packages to go through the entity terminator. The schematic design of this is presented in Figure 29.

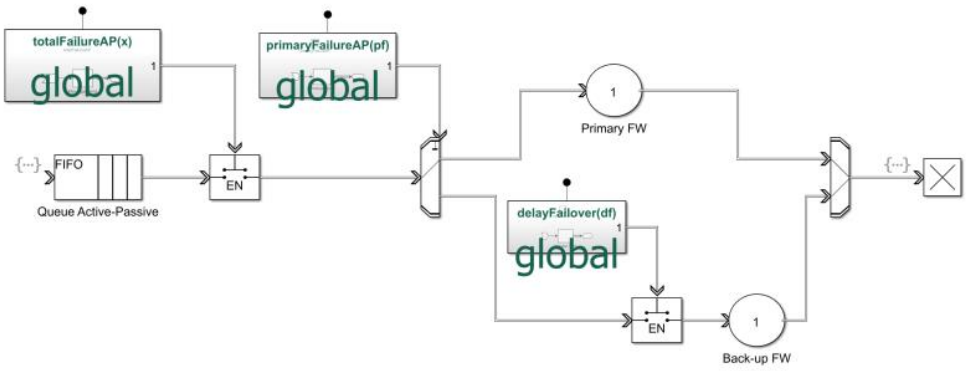


Figure 29: Active-passive firewalls diagram

8.1.5 ACTIVE-ACTIVE FAILURE DESIGN

The part of model design to follow how the active-active firewalls´ failure works will be explained in this subsection. To simulate that, an entity generator was designed to create messages periodically to observe the state of the firewalls. An attribute was created to communicate the state of the firewalls, taking different values depending on the situation. The servers used for this model create a random value, which can follow specific distributions. Depending on the numbers created in the servers, the value of the entity´s attribute change and different scenarios can occur:

- No firewalls fail: the flow of the data will continue as normal.
- Firewall 1 fails: disconnection of Firewall 1.
- Firewall 2 fails: disconnection of Firewall 2.
- Both firewalls fail: disconnection of all firewalls.

The attribute resulting from the simulation will be used by the active-active switch to operate in the correct path. The entity gates in this case are used to being able to maintain the state of the firewall for the amount of time considered as disconnected. The schematic design of this is presented in Figure 30.

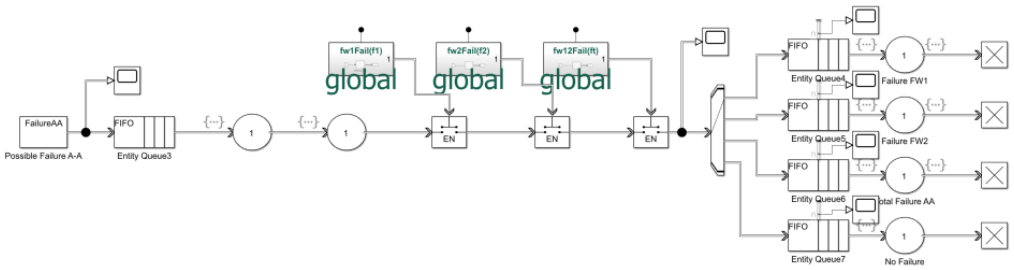


Figure 30: Active-active failure diagram

8.1.6 ACTIVE-PASSIVE FAILURE DESIGN

The part of model design to follow how the active-passive firewalls´ failure works will be explained in this subsection. To simulate that, an entity generator was designed to create messages periodically to observe the state of the firewalls. An attribute was created to communicate the state of the firewalls, taking different values depending on the situation. The servers used for this model create a random value, which can follow specific distributions. Depending on the numbers created in the servers, the value of the entity´s attribute change and different scenarios can occur:

- Primary Firewall does not fail: the flow of the data will continue as normal.
- Primary Firewall fails: disconnection of Primary Firewall and connection of Backup Firewall with a delay.
- Both firewalls fail: disconnection of all firewalls.

The attribute resulting from the simulation will be used by the active-passive switch to operate in the correct path. The entity gates in this case are used to being able to maintain the state of the firewall for the amount of time considered as disconnected. Once the failure is corrected, and maintenance is over, primary firewall will start taking the packets again with no delay considered, The schematic design of this is presented in Figure 31.

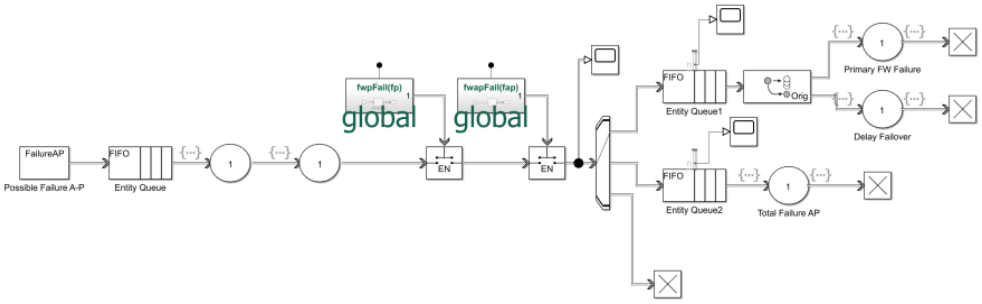


Figure 31: Active-passive failure diagram

8.1.7 SIMULINK FUNCTIONS

The functions used in the model are used for many reasons. Those functions and their characteristics will be explained in this subsection. All of them are global and they are the following:

- **totalFailureAA(y)/totalFailureAP(x):** this Simulink function is used to activate the entity gate that blocks the flow of packages to the firewalls. It is only activated when both firewalls fail, sending an entity message to the gate, as shown in Figure 32.

Figure 32: totalFailureAA(y)/totalFailureAP(x) diagram

- **routingAA(rot):** this Simulink function is used to perform the routing from the switch of the active-active model. The input of the function depends on the result on the active-active failure model. As said previously, if there is no failure, the switch will alternate the path of the packages, and if one of them fails, the other firewall would analyse all the traffic. For this case, a global variable had to be created and stored in a data store memory to record the previous path in the case of both firewalls working. The model used in this function can be seen in Figure 33.

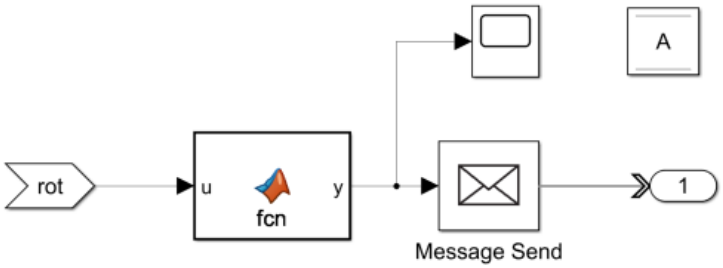


Figure 33: routingAA(rot) diagram

- **primaryFailureAP(pf):** this Simulink function is used to perform the routing from the switch of the active-passive model. The input of the function depends on the result on the active-passive failure model. As said previously, if there is no failure, the switch sends all packages to the primary wall, and if it suffers from a failure, the backup firewall would analyse all the traffic. These orders are sent via entity message.
- **delayFailover(df):** this Simulink function is used to perform the delay that occurs during the failover event in the active-passive configuration. It helps to activate the entity gate the time specified as the delay time, after that time is completed, the gate starts permitting data traffic.
- **fw1Fail(f1)/fw2Fail(f2)/fw12Fail(ft)/fwpFail(fp)/fwapFail(fap):** this Simulink function is used to activate the different entity gates from the active-active and active-passive firewalls´ failure models. They maintain the data contained if any of the failures occur until the maintenance is finished.
- **getCurrentTimeAA()/getCurrentTimeAP():** this Simulink function is used to capture the time in which a package arrives to the firewalls queue, it will also be used with the function used below to get the time that a package spends to go through the firewalls. To get that time, a digital clock block is used.

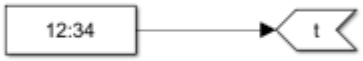


Figure 34: getCurrentTimeAA()/getCurrentTimeAP() diagram

- **recordAAWaitTimes()/recordAPWaitTimes():** this Simulink function is used to record the time that a package had to wait from arriving to the firewalls, to being completely processed. Figure 35 shows the schematic of that function.

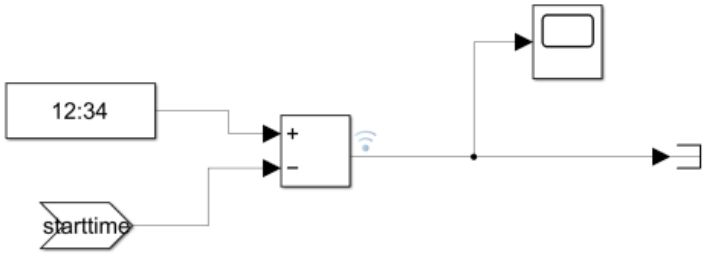


Figure 35: recordAAWaitTimes()/recordAPWaitTimes() diagram

8.2 SIMULATION RANDOM FAILURE

This part of the project will show the different results of the simulations when the probability of failure of the firewalls is completely random. To do that, the servers used in the active-active and active-passive firewalls´ failure models produce a number between 0 and 1, for each of the firewalls, with Equation 2:

Equation 2: Random number generator between 0 and 1

$$coder.extrinsic('rand')$$

In the case of active-active, if any of the firewalls´ numbers are below 0.05, that firewall is considered to have suffered from a failure and it will be disconnected. If both experience a failure at the same time, both will be disconnected. On the other hand, in active-passive, if the primary firewall´s number is below 0.5, the backup firewall will take its place. If both experience a failure at the same time, both will be disconnected.

8.2.1 ACTIVE-ACTIVE RESULTS

During the 100 seconds simulation, different failures of the firewalls were noticed. In Figure 36 it can be seen two variables, one is the Entity Gate5.FailureFW_AA, which depending on its value represents a scenario, no failure (4), total failure (3), FW2 failure (2) and FW1 failure (1), and Entity Gate5.AuxiliarAA, which is the random number created for Firewall 1.

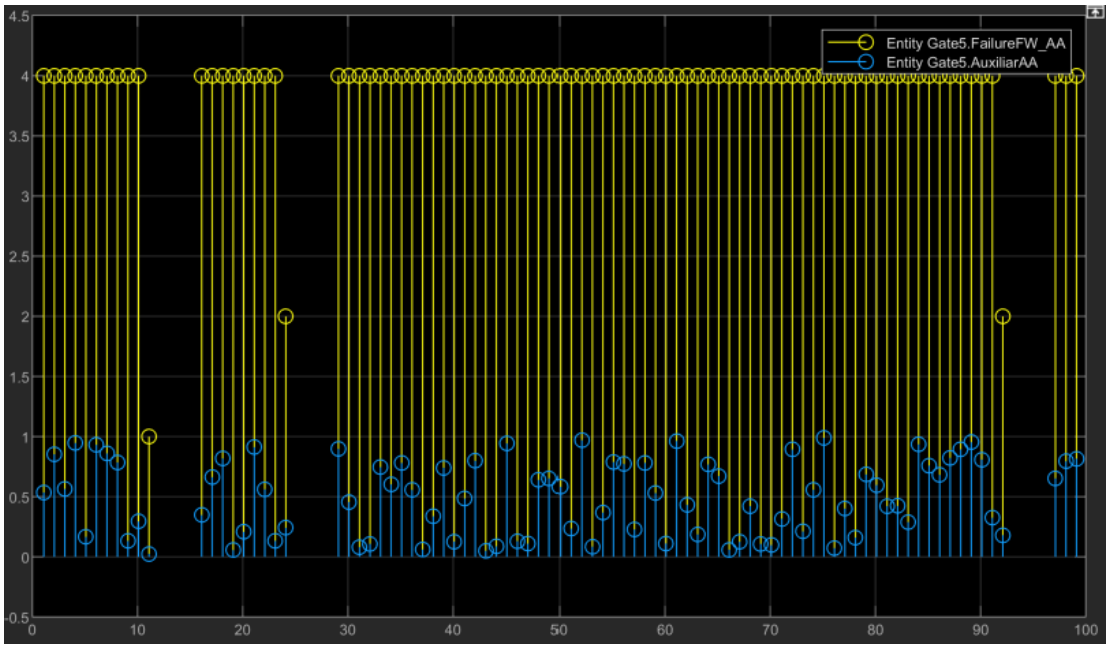


Figure 36: Random failure, active-active failure results

It can be seen how, for example, after failure of Firewall 1 at second 12, the state of the routing makes all the traffic go to Firewall 2 until the firewall is repaired. After that moment the system starts working with both firewalls again until a failure in Firewall 2 occurs.

The main results analysed were the total packets processed by the system and the time that the packets waited from arriving to the firewalls, to being processed. The process time of the firewalls used for this case was constant, 1 second. Firstly, the total packets processed by the pair of active-active firewalls depended on the firewalls available to operate. It can be seen how during the failures, the number of packets processed in time decreases compared to the times in which both are available. Figure 37 represents these results.

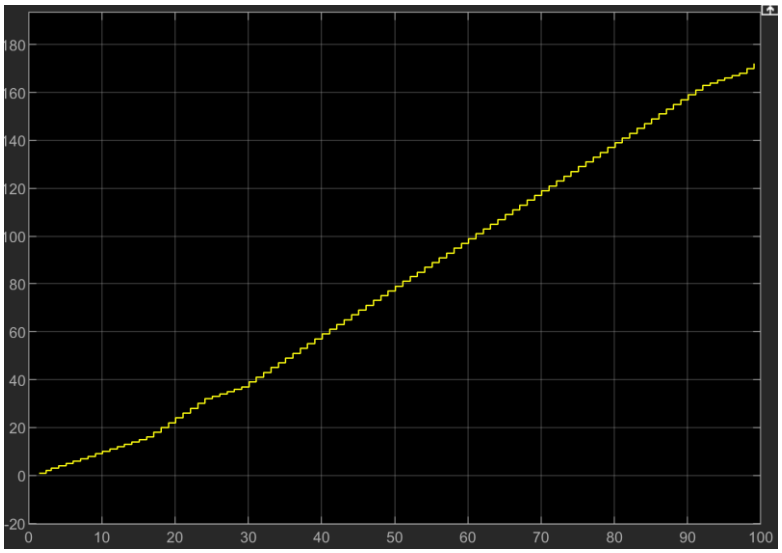


Figure 37: Random failure, total packets processed (active-active)

The time waited by the packets from arriving to the pair of firewalls to being processed keeps increasing with the pass of time. This may be because of the incapacity of the firewalls to process the packets at the same pace that the generating points send information. Figure 38 shows this increase, which could not be stabilized, at least, with the time simulated.

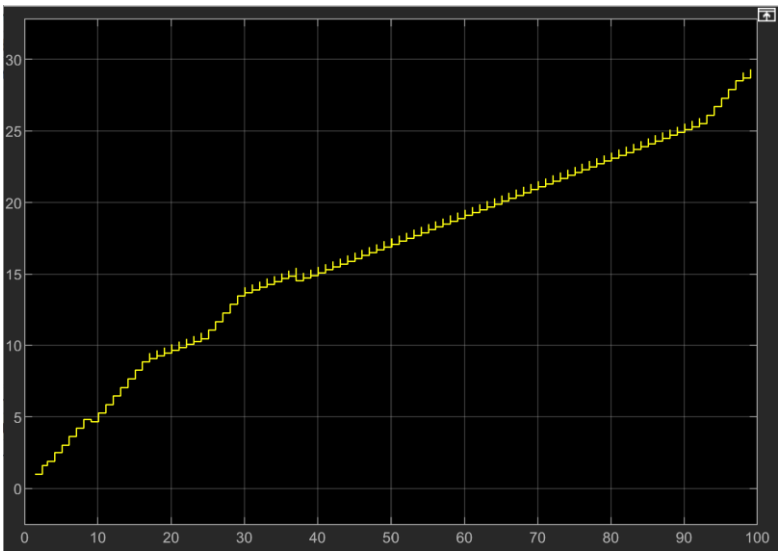


Figure 38: Random failure, total time to process a packet (active-active)

8.2.2 ACTIVE-PASSIVE RESULTS

During the 100 seconds simulation, a failure of the primary firewall occurred. In Figure 39 it can be seen two variables, one is the Entity Gate6.FailureFW_AP, which depending on its value represents a scenario, no failure (3), total failure (2) and primary firewall failure (1), and Entity Gate6.AuxiliarAP, which is the random number created for the primary firewall.

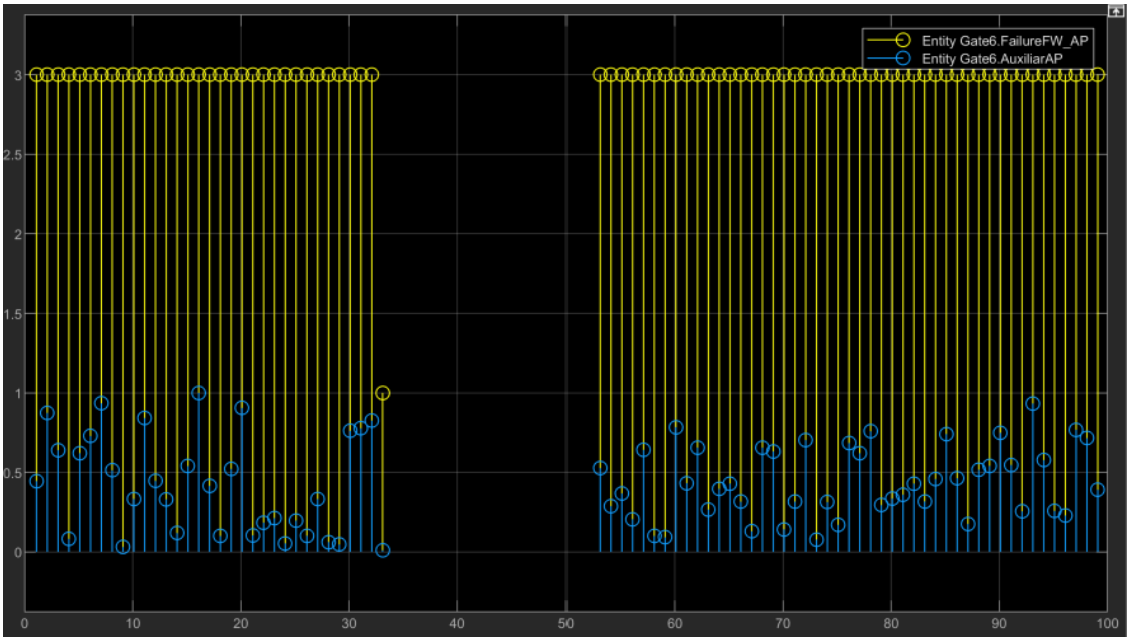


Figure 39: Random failure, active-passive failure results

It can be seen how after failure of the primary firewall at second 33, the state of the routing makes all the traffic go to secondary firewall, with a delay considered with a value of 5 seconds, until the firewall is repaired after 20 seconds. After that moment the system starts working again with the primary firewall until the end of the simulation.

The main results analysed were the total packets processed by the system and the time that the packets waited from arriving to the firewalls, to being processed. The process time of the firewalls used for this case was constant, 1 second. Firstly, the total packets processed by the pair of active-passive firewalls had an established rhythm, which only changed in second 33, when primary firewall failed, creating a delay until the backup firewall was able to be connected. Figure 40 represents these results.

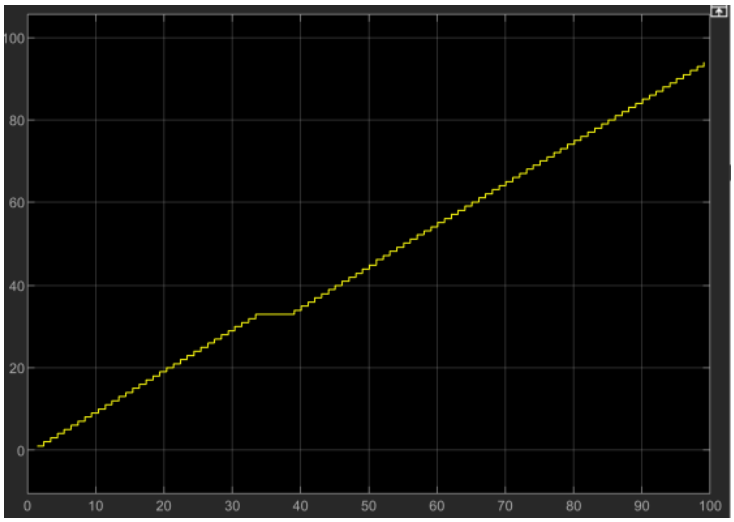


Figure 40: Random failure, total packets processed (active-passive)

The time waited by the packets from arriving to the pair of firewalls to being processed keeps increasing with the pass of time, only stopping for the delay, while no packets are being processed. The waited time keeps increasing, not being able to decrease it with the simulated time, as seen in Figure 41.

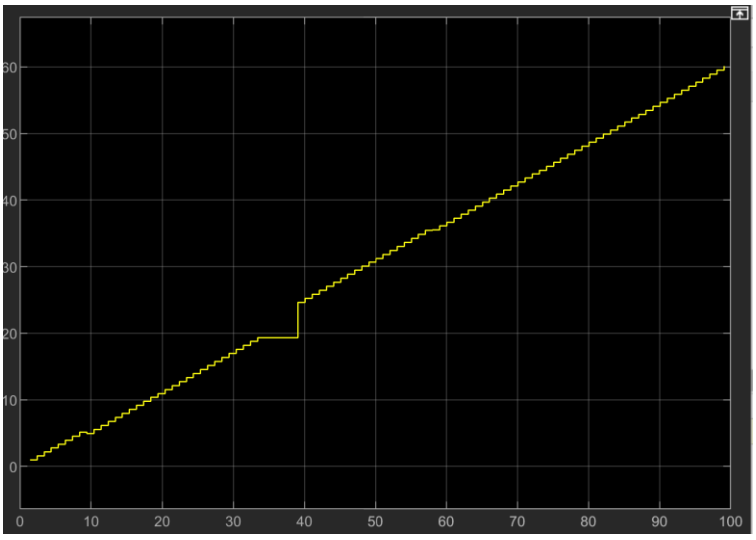


Figure 41: Random failure, total time to process a packet (active-passive)

8.2.3 COMPARISON ACTIVE-ACTIVE/ACTIVE-PASSIVE

It has been seen how, even though the active-active configuration experienced 3 failures, compared to the 1 failure from the active-passive pair, the active-active configuration was able to process nearly twice the amount the other configuration was able for the simulated time. Furthermore, data packets experienced a higher waited time, nearly twice as much, in the active-passive configuration, compared to the other option. The performance results can be seen in Table 3.

Table 3: Random failure, active-active vs active-passive

Configuration	Active-Active	Active-Passive
Total throughput (packets)	171	93
Wait time behaviour	Constant increase	Constant increase
Wait time peak (seconds)	29	60

8.3 SIMULATION LOGNORMAL DISTRIBUTION FAILURE

This part of the project will show the different results of the simulations when the probability of failure follows the Lognormal Distribution. To do that, the servers used in the active-active and active-passive firewalls´ failure models produce a number between 0 and 100, with the following equation, where sigma will take the values 0.5 and 1:

Equation 3: Lognormal distribution number creator between 0 and 100

$$lognrnd(\log(5), sigma)$$

The probability function of the Lognormal Distribution experiences huge peaks in a value close to the mean, the sigma value increases the variability, also placing the peak further from the mean value. The probability function of the different sigma, and same mean, is presented in Figure 42.

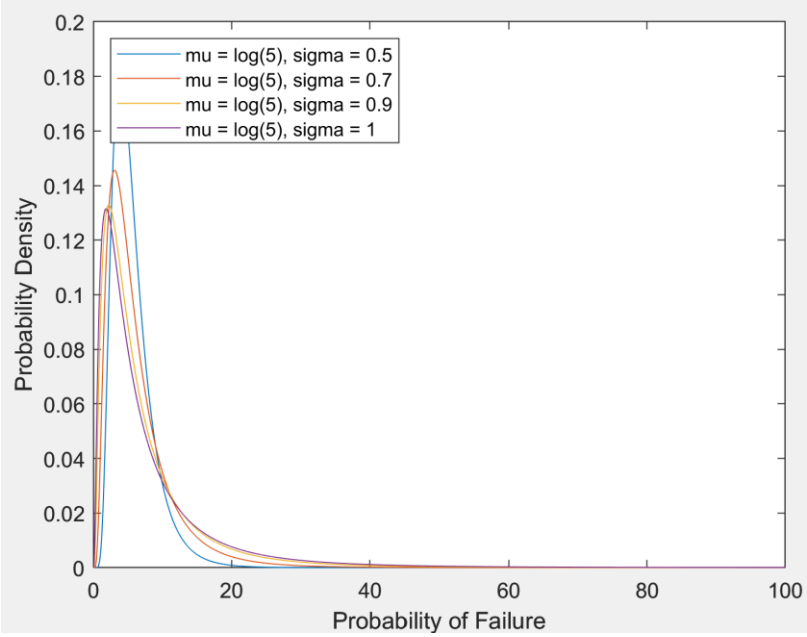


Figure 42: Lognormal distribution probability function

In the case of active-active, if any of the firewalls´ numbers are above 95, that firewall is considered to have suffered from a failure and it will be disconnected. If both experience a failure at the same time, both will be disconnected. On the other hand, in active-passive, if the primary firewall´s number is above 95, the backup firewall will take its place. If both experience a failure at the same time, both will be disconnected.

8.3.1 LOGNORMAL DISTRIBUTION SIGMA 0.5

This subsection of the project will furtherly analyse the results of both, active-active and active-passive configurations, regarding the performance of the pair of firewalls with a Lognormal Distribution which sigma´s value is 0.5.

- **Active-Active Results**

For this case, the time for this simulation was 5000 seconds. This new results from the active-active configuration are closer to reality, no errors were detected. In Figure 43 it can be seen the values of the number generated for Firewall 1. The distribution selected, with a sigma

with a value of 0.5, did not provide any failures, value above 95, being the peak of approximately 30.

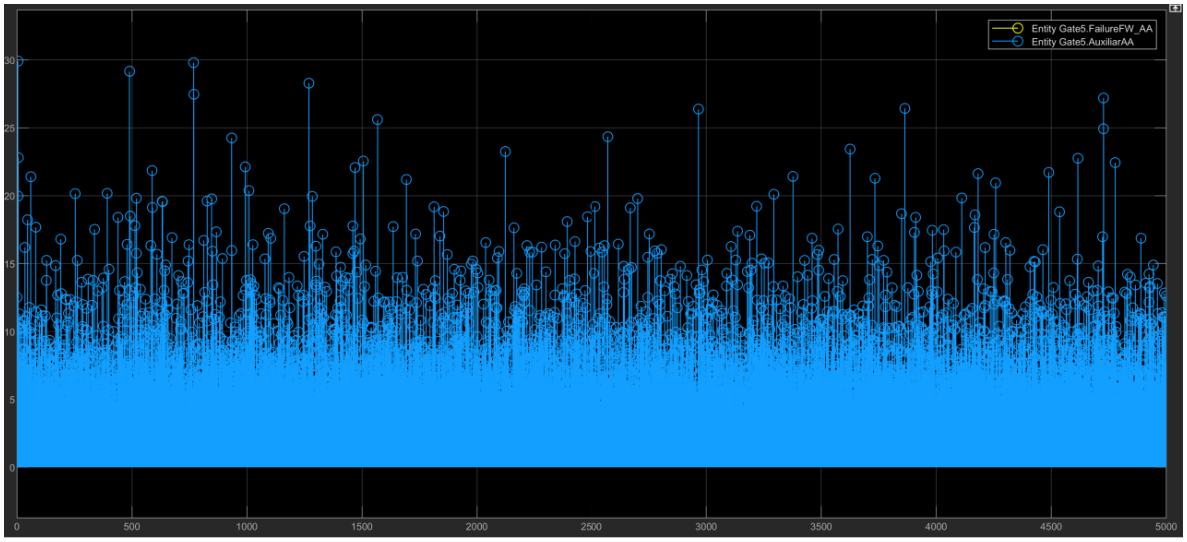


Figure 43: Lognormal distribution failure (sigma 0.5), active-active failure results

The main results analysed were the total packets processed by the system and the time that the packets waited from arriving to the firewalls, to being processed. The process time of the firewalls used for this case is variable, it follows two variables, a random value and a value which depends on the size of the packets:

Equation 4: Firewalls' service time in lognormal distribution simulation

$$dt = entity.Mbps \cdot 0.1 + rand(1,1)$$

Firstly, the total packets processed by the pair of active-active firewalls depended on the firewalls available to operate, in this case both were available during all the simulation. Figure 44 represents these results.

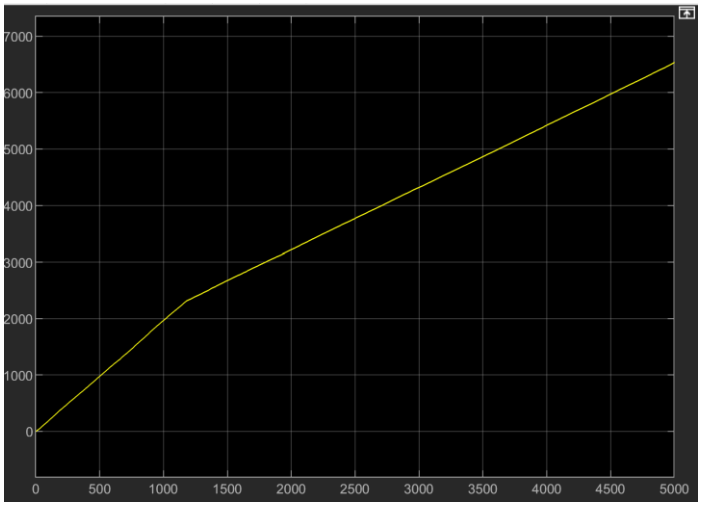


Figure 44: Lognormal distribution failure (sigma 0.5), total packets processed (active-active)

It can be seen how at the approximate time of 1200 seconds the rhythm in which the pair processes the packets gets slower. This is mainly because the fast process of both firewalls, Figure 45 shows the number of packets waiting to be processed by the pair of firewalls. It can be seen how that number increases and has a peak at the approximate time 350 seconds, with more than 700 packets, and it then decreases to nearly zero while the number or packets processed rhythm slows down.

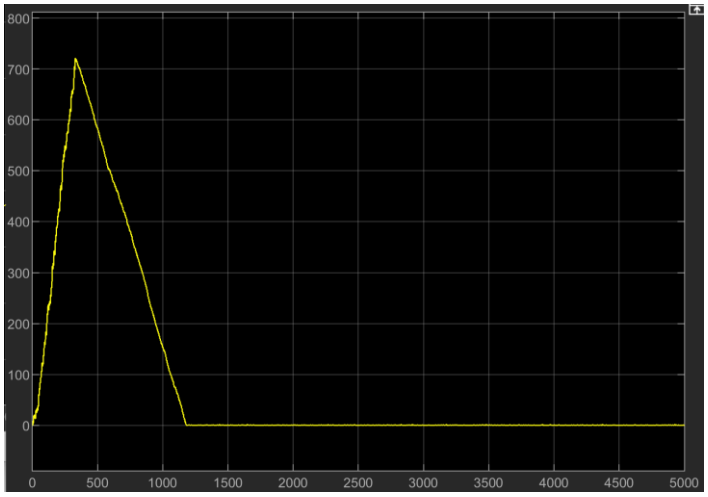


Figure 45: Lognormal distribution failure (sigma 0.5), number of packets waiting to be processed, active-active

The time waited by the packets from arriving to the pair of firewalls to being processed has the same behaviour as the last illustration. It experiences a peak value, and then it reduces the whole process. This may be because of the great capacity from the firewalls to process the packets at the same pace that the generating points send information. Figure 46 shows this event.

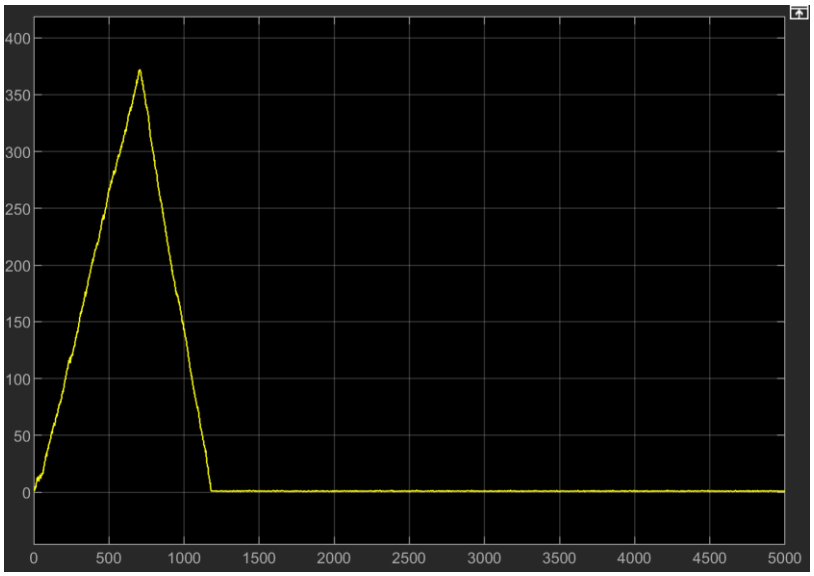


Figure 46: Lognormal distribution failure (sigma 0.5), total time to process a packet (active-active)

- **Active-Passive Results**

As in the last simulation, the time for this one was 5000 seconds. In the same way than in the active-active configuration, these results are way closer to reality, not finding any failure during the simulation. In Figure 47 it can be seen the values of the number generated for Firewall 1. The distribution selected, with a sigma with a value of 0.5, did not provide any failures, value above 95, being the peak of approximately 30.

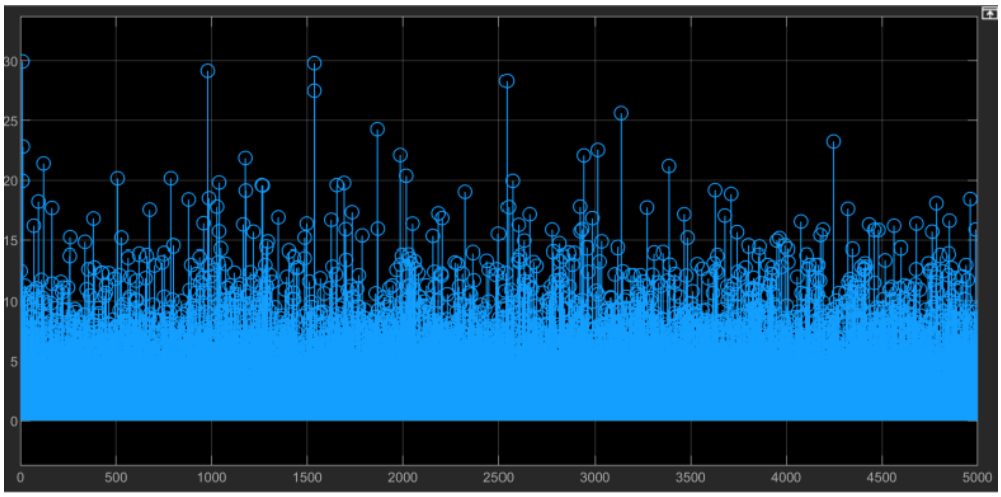


Figure 47: Lognormal distribution failure (sigma 0.5), active-passive failure results

The main results analysed were the total packets processed by the system and the time that the packets waited from arriving to the firewalls, to being processed. The process time of the firewalls used for this case follows the same function as in the active-active configuration.

The total packets processed by the pair of active-passive firewalls was constant, since the primary firewall was active during all the simulation. Figure 48 represents these results.

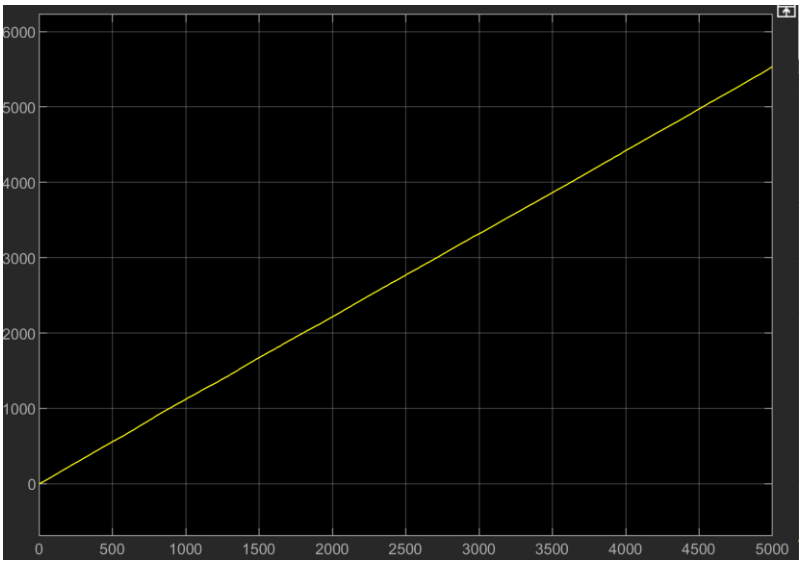


Figure 48: Lognormal distribution failure (sigma 0.5), total packets processed (active-passive)

Looking at how the packets were processed in can be seen how, unlike the active-active configuration, in this case the firewall arrived at its final capacity, which provoke losses on data information which could be key for the operation of the electrical grid. This limit is reached at approximately 300 seconds and could not be solved.

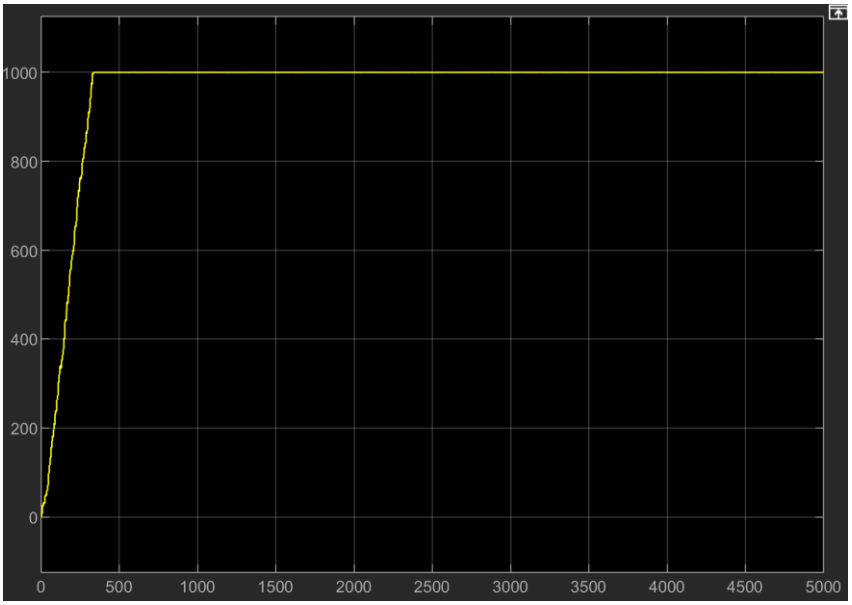


Figure 49: Lognormal distribution failure (sigma 0.5), number of packets waiting to be processed, active-passive

The time waited by the packets from arriving to the pair of firewalls to being processed had a similar behaviour seen in Figure 49. It experiences a cap at a certain point of time, which does not coincide with the number of packets waiting to be processed function. This cap is reached because the capacity of the firewall is reached, if the capacity of the primary firewall was bigger and it was reached, the cap of the function below would have a bigger value. This results are shown in Figure 50.

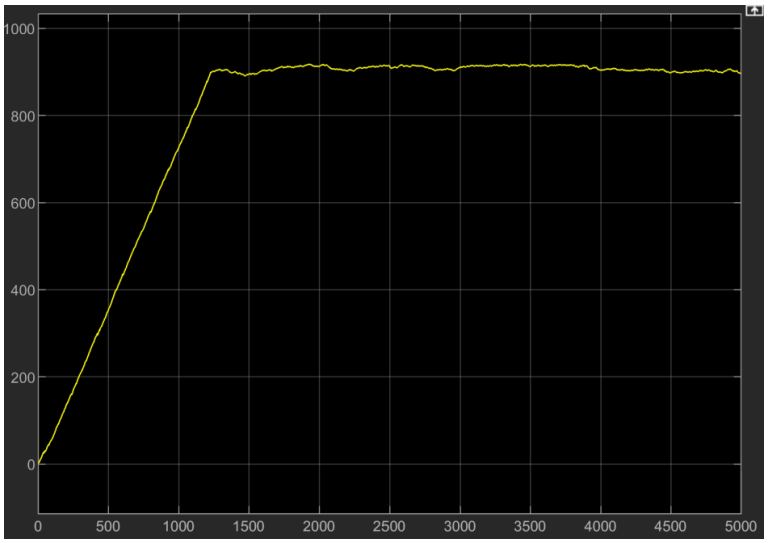


Figure 50: Lognormal distribution failure (sigma 0.5), total time to process a packet (active-passive)

- **Comparison Active-Active/Active-Passive**

As it was analysed above, there are clear differences between the use of active-active and active-passive configuration. The only aspect in which both configurations could seem similar is the total throughput, in which the difference is just an increase of 18% in favor of the active-active configuration. The reason was later explained, being the lack of packets to process the main reason why that upgrade is not nearly the 100%.

On the other hand, it was also noticed how in the case of active-passive, the pair of firewalls did not have the capacity to treat with all data, reaching full capacity rapidly. For the case of active-active, although the available also decreased rapidly, it was also recovered efficiently. The performance results can be seen in Table 4.

Table 4: Lognormal distribution failure (sigma 0.5), active-active vs active-passive

Configuration	Active-Active	Active-Passive
Total throughput (packets)	6.532 e3	5.673 e3
Wait time behaviour	Stable	Maximum limit reached
Wait time peak (seconds)	368	917

8.3.2 LOGNORMAL DISTRIBUTION SIGMA 1

This subsection of the project will furtherly analyse the results of both, active-active and active-passive configurations, regarding the performance of the pair of firewalls with a Lognormal Distribution which sigma´s value is 1.

- **Active-Active Results**

Again, the time for this simulation was 5000 seconds. The increase in the variability of the distribution, doubling sigma, has created a scenario in which failures occur. For this case of study, Figure 51 shows how there are several points in which the value from Firewall 1 exceeds the value 95, generating a failure in Firewall 1. Furthermore, even though that firewall experience various failure events and both firewalls follow the same distribution, Firewall 2 is always available.

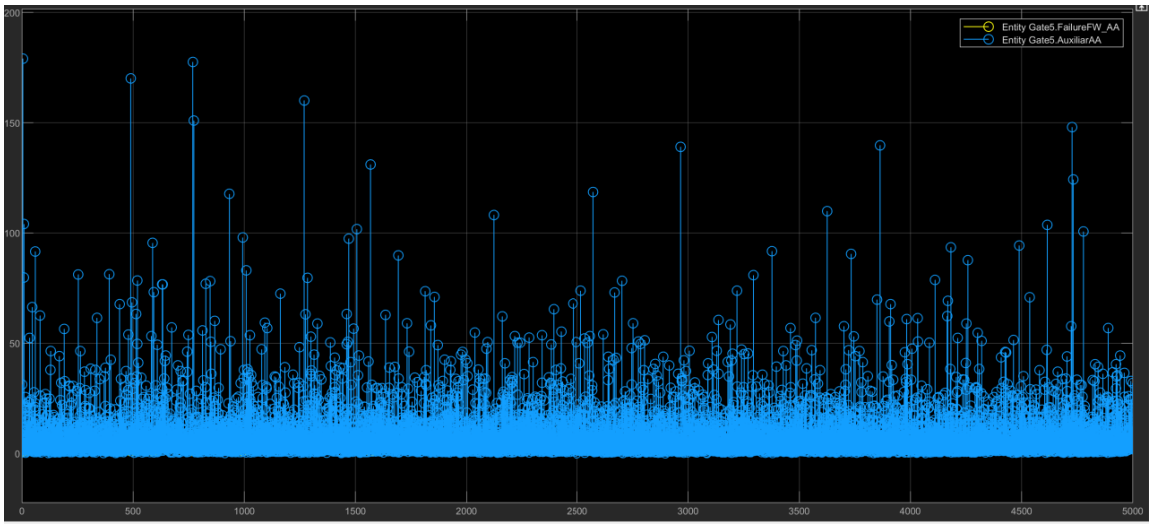


Figure 51: Lognormal distribution failure (sigma 1), active-active failure results

The main results analysed were the total packets processed by the system and the time that the packets waited from arriving to the firewalls, to being processed. The process time of the firewalls used for this case is the same as in the one with sigma 0.5, Equation 4.

Although this simulation worked under a higher sigma, the system experiences a very similar behaviour. There is a constant increase in the number of total packets processed as it can be

seen in Figure 52, the constant variability of the functions slope is related to the randomness of the firewall process time and the different failures suffered by Firewall 1.

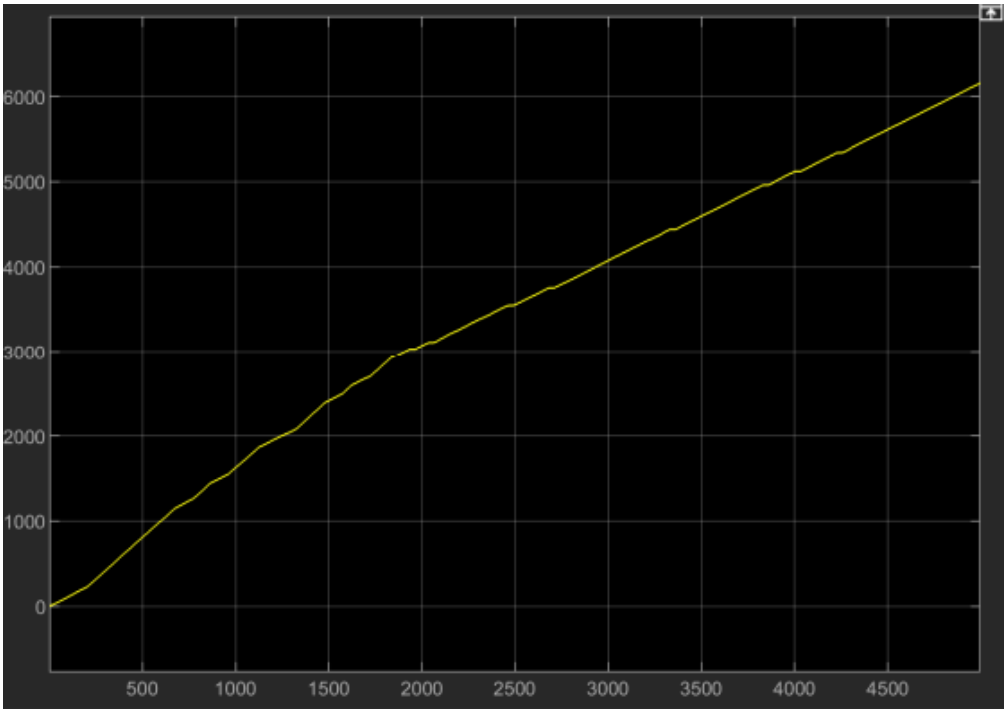


Figure 52: Lognormal distribution failure (sigma 1), total packets processed (active-active)

The change on the packet processing´s rhythm is also due to the same reason found in the sigma 0.5 simulation. The number of packets in the queue to be processed arrive to a peak and experiences a decrease which suffers from light increases due to the different failure the Firewall 1 experiences, but at the end it also ends with a constant value of nearly zero. At that instant is when, again, the total throughput reduces its increase. These events can be seen in Figure 53.

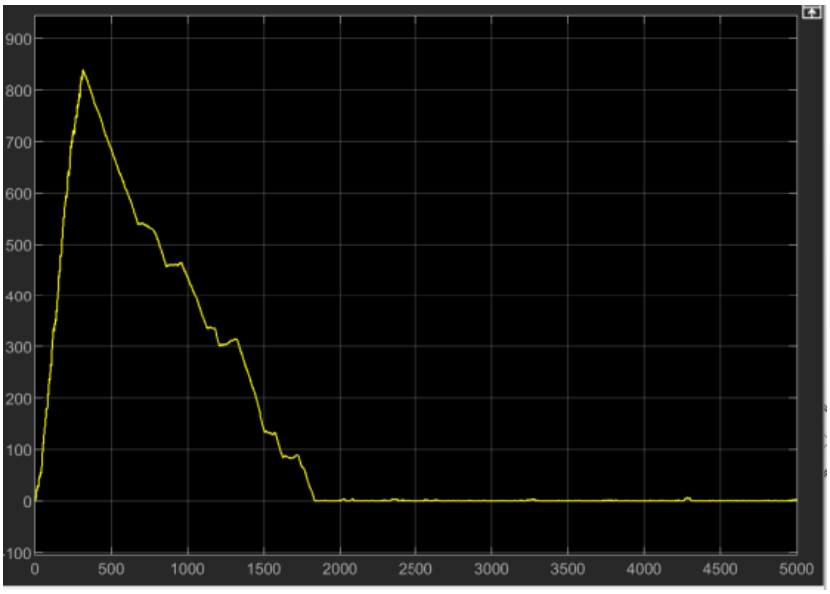


Figure 53: Lognormal distribution failure (sigma 1), number of packets waiting to be processed, active-active

The same happens with the time that packets had to experience between its arrival to the firewall to being processed. This behaviour follows the one than the queue is experiencing, in the same way as with sigma equal to 0.5, as it is shown in Figure 54.

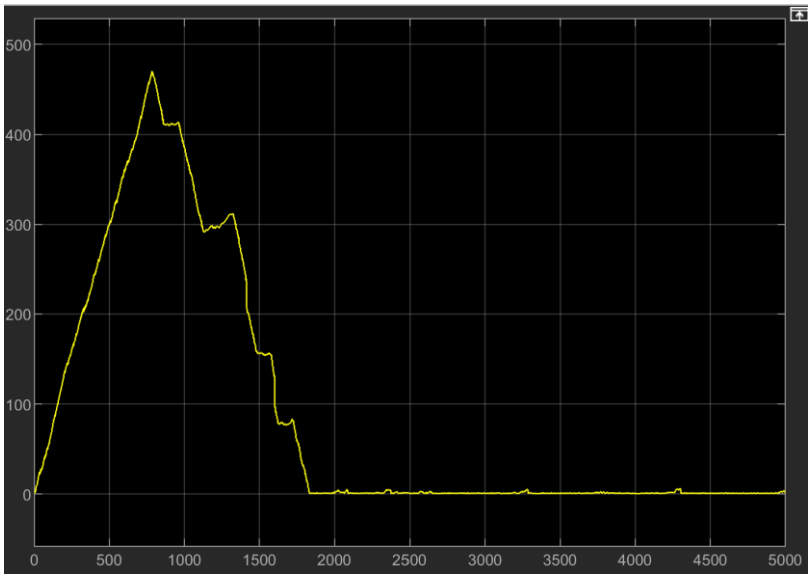


Figure 54: Lognormal distribution failure (sigma 1), total time to process a packet (active-active)

➢ Active-Passive Results

Following the parameters from the active-active scenario, the time for this simulation is 5000 seconds. In the same way than in the active-active configuration, the increase in the variability of the failure probability distribution created a scenario with several failures from the primary firewall. No total failures were experienced during the simulation. Those events are represented in Figure 55.

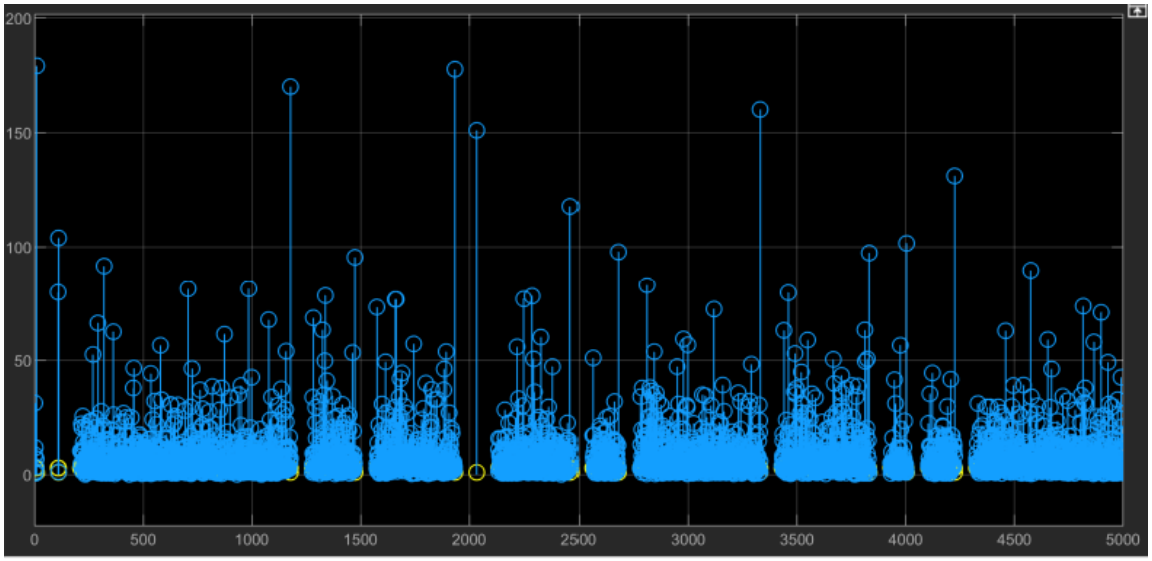


Figure 55: Illustration 30: Lognormal distribution failure (sigma 1), active-passive failure results

The main results analysed were the total packets processed by the system and the time that the packets waited from arriving to the firewalls, to being processed. The process time of the firewalls used for this case follows the same function as in the active-active configuration, Equation 4, a function with a variable and a random component

The total packets processed by the pair of active-passive firewalls followed a nearly a perfect line. The failures suffered by the primary firewall can be seen, leaving periods of time in which no packets were processed. Figure 56 represents these results.

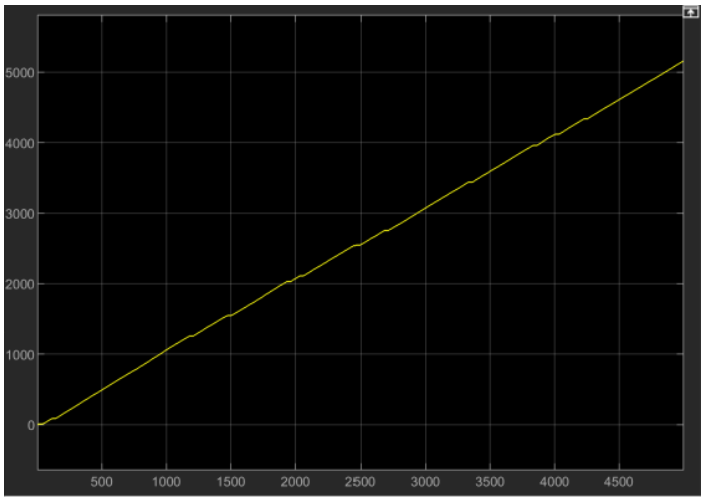


Figure 56: Lognormal distribution failure (sigma 1), total packets processed (active-passive)

This simulation had the same results, in terms of behaviour, not values, that the active-passive configuration with sigma 0.5 had. The wait time for the packets creates a function which increases rapidly until the capacity of the firewalls queue arrives to its limit. Once the limit is reached, the wait time stabilises, and the wait time stays in huge values, oscillating without many changes.

- **Comparison Active-Active/Active-Passive**

The results from the case of sigma 1 follows the same characteristics as the one from sigma 0.5. The results regarding total throughput don´t have a huge difference, mainly because the pair of active-active firewalls working under their full capacity. Moreover, it happens the same events as is sigma 0.5, active-passive configuration arrives to its processing limits, making the wait time oscillates in higher values, whereas in active-active it ends-up in values near 0. The performance results can be seen in Table 5.

Table 5: Lognormal distribution failure (sigma 1), active-active vs active-passive

Configuration	Active-Active	Active-Passive
Total throughput (packets)	6.159 e3	5.161 e3
Wait time behaviour	Stable	Maximum limit reached
Wait time peak (seconds)	470	1053

8.3.3 COMPARISON LOGNORMAL DISTRIBUTION SIGMA 0.5/SIGMA 1

The increase in variability of the probability distribution function created different scenarios. The most noticeable event was that the increase created failures in the sigma 1 simulation, while sigma 0.5 simulation experienced none.

Furthermore, the variability provoked changes in the performance of the system. The existence of failures in the simulation made the sigma 1 case to have a decrease in its performance. In active-active configuration, total throughput was 6% lower, and the wait time peak was 21% higher. On the other hand, in the case of active-passive configuration the total throughput was 9% lower, while the wait time peak increased a 14.8%. This results are presented in Table 6.

Table 6: Sigma 1 performance, compared to sigma 0.5

Configuration	Active-Active	Active-Passive
Total throughput	-6%	-9%
Wait time peak	21%	14.8%

8.4 SIMULATION EXTREME VALUE DISTRIBUTION FAILURE

This part of the project will show the different results of the simulations when the probability of failure follows the Extreme Value Distribution. To do that, the servers used in the active-active and active-passive firewalls´ failure models produce a number between 0 and 100, with Equation 5, where mean (mu) will have a value of 95 and sigma will take the values 3 and 8:

Equation 5: Extreme value distribution number creator between 0 and 100

$$random('ev', mu, sigma)$$

The probability function of the Extreme Value Distribution experiences the peak in the value of the mean, the sigma value increases the variability. In this case, compared to Lognormal Distribution, this distribution has the peak at the same value, only changing the variability

of the function. The probability function of the different sigma, and same mean (mu), is presented in Figure 57.

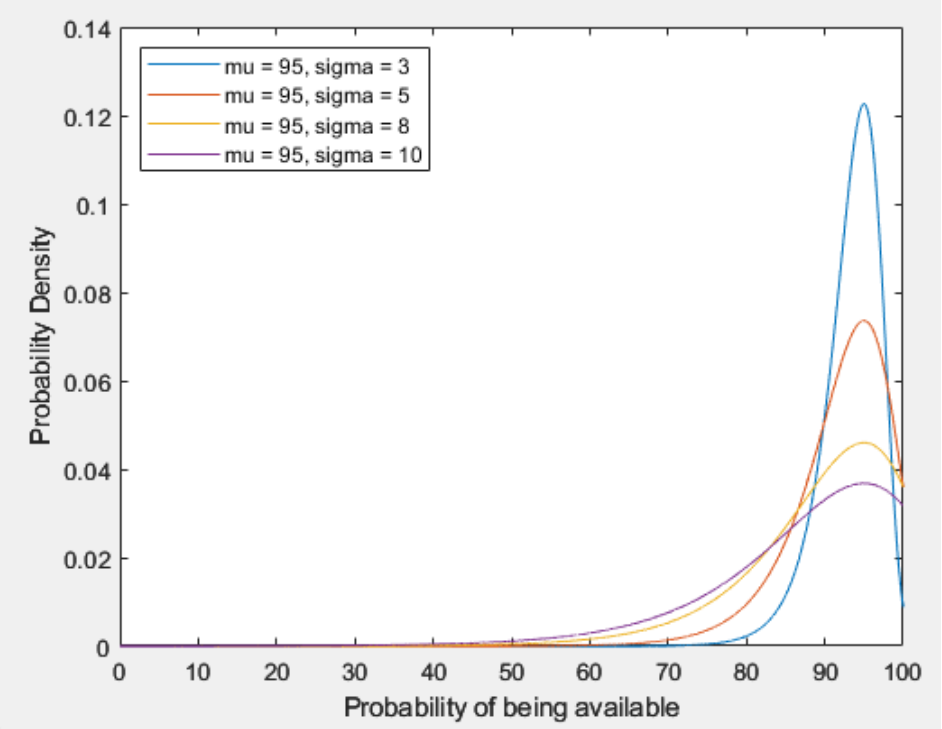


Figure 57: Extreme value distribution distribution probability function

In the case of active-active, if any of the firewalls´ numbers are below 5, that firewall is considered to have suffered from a failure and it will be disconnected. If both experience a failure at the same time, both will be disconnected. On the other hand, in active-passive, if the primary firewall´s number is below 5, the backup firewall will take its place. If both experience a failure at the same time, both will be disconnected.

8.4.1 Extreme Value Distribution Sigma 3

This subsection of the project will furtherly analyse the results of both, active-active and active-passive configurations, regarding the performance of the pair of firewalls with an Extreme Value Distribution which sigma´s value is 3.

- **Active-Active Results**

For this case, the simulation lasted 2500 seconds. In the same way as in the Lognormal Distribution simulation, the results are similar on what it is expected for this kind of architectures. No failures were detected during all the simulation. Figure 58 will show the values generated for Firewall1, from the span of time between 0 and 500 seconds. It can be seen how most of the values generated stay really close to the 95, being 76 the lowest found in that range of time.

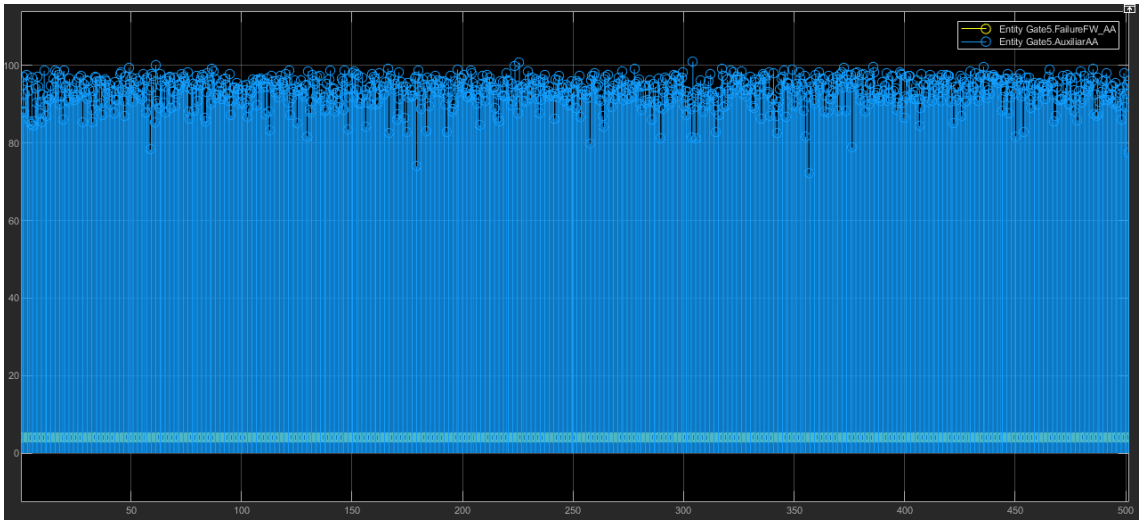


Figure 58: Extreme value distribution failure (sigma 3), active-active failure results (0-500 seconds)

The main results analysed were the total packets processed by the system and the time that the packets waited from arriving to the firewalls, to being processed. The process time of the firewalls used for this case is variable, as in the Lognormal Distribution (Equation 4), it follows two variables, a random value and a value which depends on the size of the packets.

Firstly, the total packets processed by the pair of active-active firewalls depended on the firewalls available to operate, in this case both were available during all the simulation. Figure 59 represents these results.

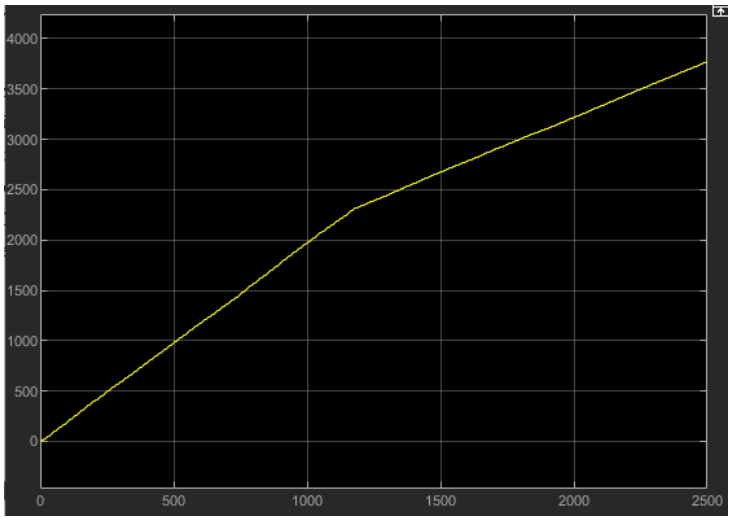


Figure 59: Extreme value distribution failure (sigma 3), total packets processed (active-active)

In the same way as in the Lognormal Distribution, around 1200 seconds the speed in which packets are processed slow down. Again, looking into the packets waiting to be processed by the firewalls, Figure 60, it can be seen how there is a peak of that number, which is reduces to a value close to zero at that time. That makes the pair of firewalls work under lower pressure, reducing the rhythm of processing.

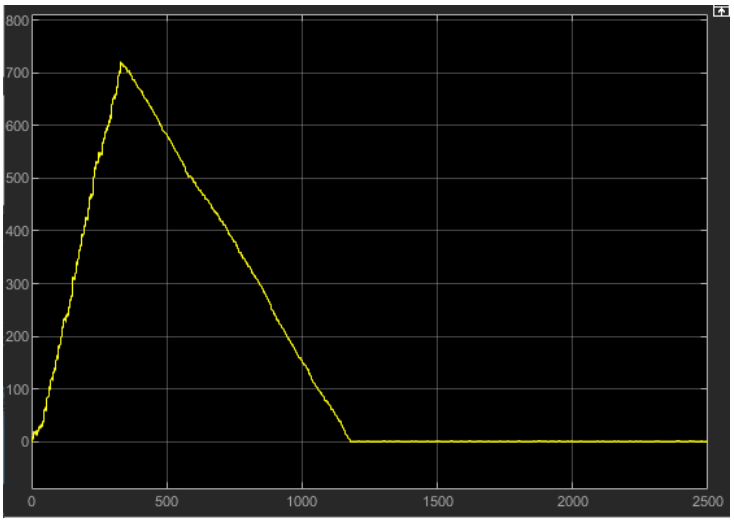


Figure 60: Extreme value distribution failure (sigma 3), number of packets waiting to be processed, active-active

The time waited by the packets from arriving to the pair of firewalls to being processed has the same behaviour as the last illustration. It experiences a peak value, and then it reduces the whole waiting process to nearly zero. As in last case, the assumption is that it may be because of the great capacity from the firewalls to process the packets, being able to complete their operation at the same pace that the generating points send information. Figure 61 shows this event.

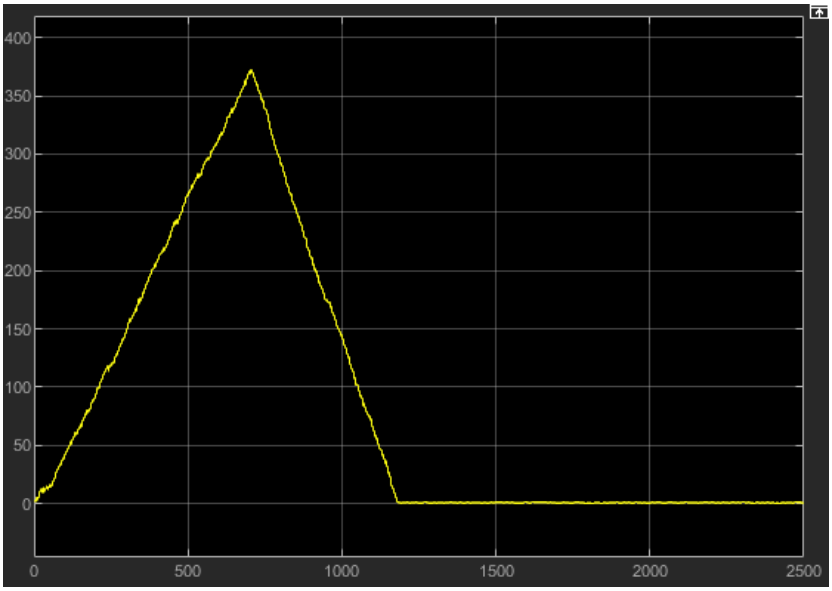


Figure 61: Extreme value distribution failure (sigma 3), total time to process a packet (active-active)

- **Active-Passive Results**

In the same way as in the active-active configuration simulation, a 2500 second simulation was made. The results were the ones expected, the distribution made the values not go below the value 5, creating no failures during the time of the simulation. Figure 62 shows a snapshot of the values from Firewall 1, where it can be seen how the values never go below 70.

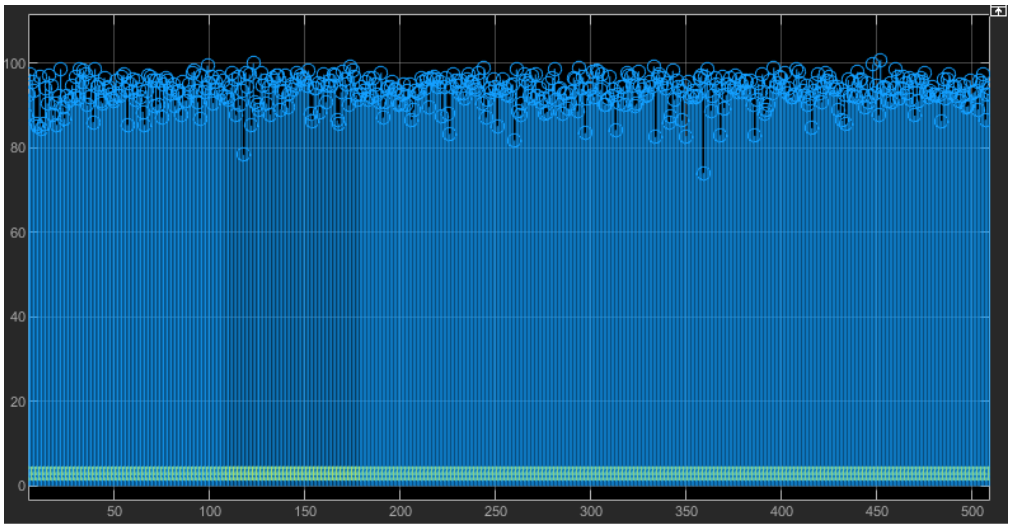


Figure 62: Extreme value distribution failure (sigma 3), active-passive failure results (0-500 seconds)

The main results analysed were the total packets processed by the system and the time that the packets waited from arriving to the firewalls, to being processed. The process time of the firewalls used for this case follows the same function as in the active-active configuration. The total packets processed by the pair of active-passive firewalls was constant, as in the Lognormal distribution (sigma 0.5) since the primary firewall was active during all the simulation. Figure 63 represents these results.

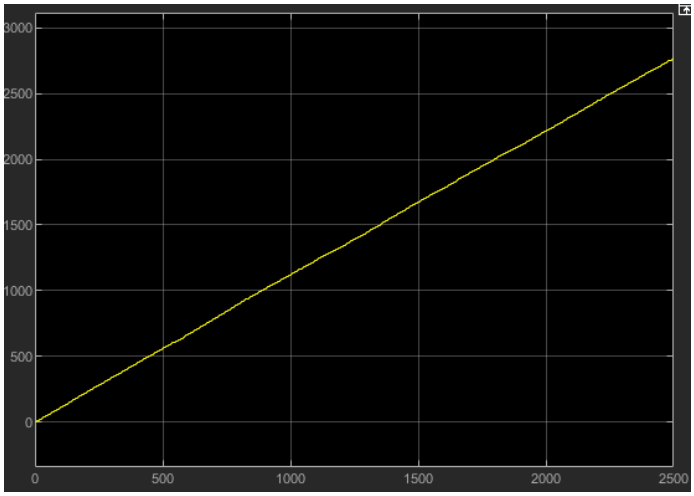


Figure 63: Extreme value distribution failure (sigma 3), total packets processed (active-passive)

Looking at how the packets were processed in can be seen how, unlike the active-active configuration, in this case the firewall arrived at its final capacity, which provoke losses on data information which could be key for the operation of the electrical grid. This limit is reached at approximately 300 seconds, as seen in Figure 64, and could not be solved with the parameters established for the simulation.

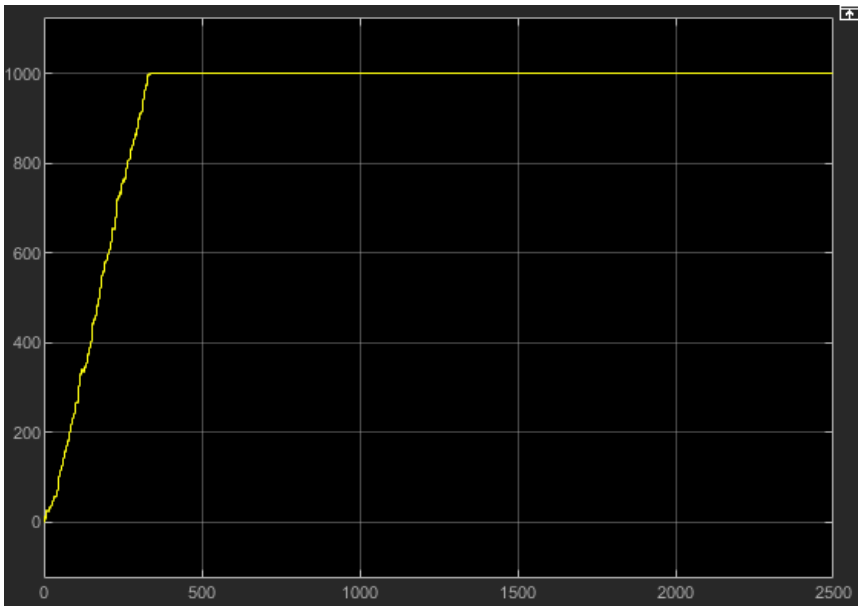


Figure 64: Extreme value distribution failure (sigma 3), number of packets waiting to be processed, active-passive

As it was expected considering other simulations, the time waited by the packets from arriving to the pair of firewalls to being processed had a similar behaviour seen Figure 64. It experiences a cap at a certain point of time, which does not coincide with the number of packets waiting to be processed function. This cap is reached because the capacity of the firewall is reached, like the other cases analysed. The results can be seen in Figure 65.

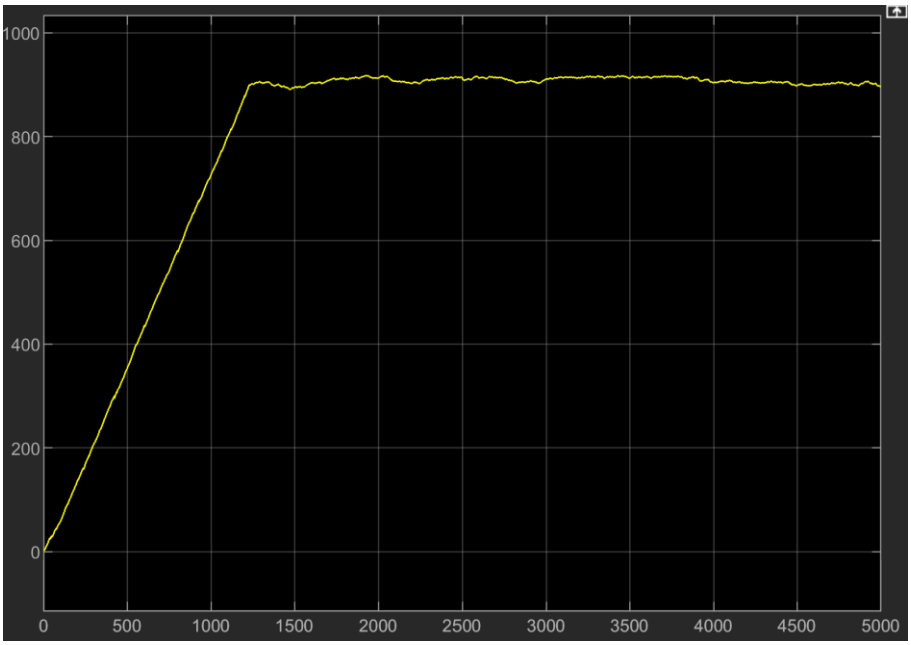


Figure 65: Extreme value distribution failure (sigma 3), total time to process a packet (active-passive)

➢ **Comparison Active-Active/Active-Passive**

As it was analysed above, there are clear differences between the use of active-active and active-passive configuration. The only aspect in which both configurations could seem similar is the total throughput, in which the difference is just an increase of 18% in favor of the active-active configuration. The reason was later explained, being the lack of packets to process the main reason why that upgrade is not nearly the 100%.

On the other hand, it was also noticed how in the case of active-passive, the pair of firewalls did not have the capacity to treat with all data, reaching full capacity rapidly. For the case of active-active, although the available also decreased rapidly, it was also recovered efficiently. Results can be seen in Table 7.

Table 7: Extreme value distribution failure (sigma 3), active-active vs active-passive

Configuration	Active-Active	Active-Passive
Total throughput (packets)	3.764 e3	2.740 e3
Wait time behaviour	Stable	Maximum limit reached
Wait time peak (seconds)	368	917

8.4.2 EXTREME VALUE DISTRIBUTION SIGMA 8

This subsection of the project will furtherly analyse the results of both, active-active and active-passive configurations, regarding the performance of the pair of firewalls with a Extreme Value Distribution which sigma´s value is 8.

- **Active-Active Results**

Again, the time for this simulation was 2500 seconds. The increase in the variability of the distribution, changing from the value 3 to 8, did not affect the availability of any of the firewalls. The variability of the function created numbers below 40, but nothing close to the value 5 limit. Figure 66 shows a snapshot until the second 500.

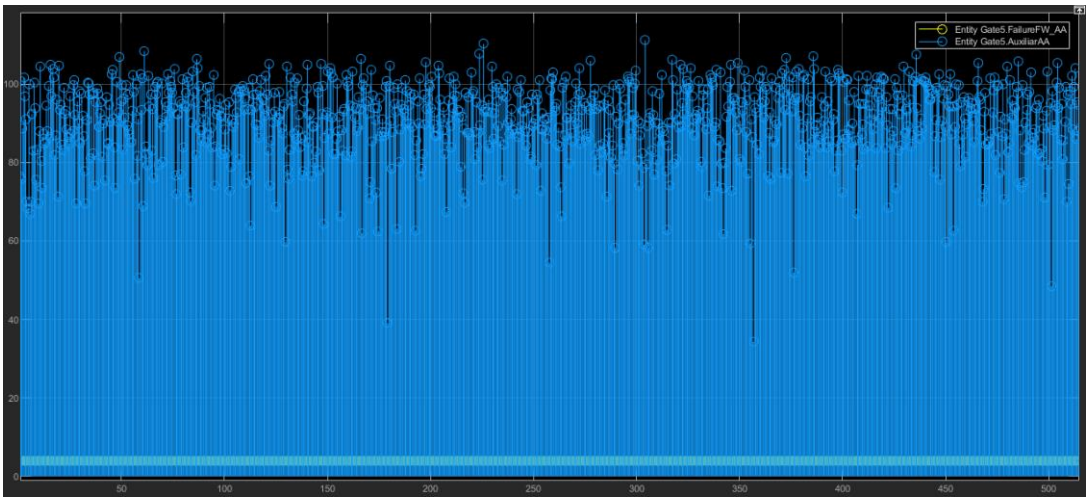


Figure 66: Extreme value distribution failure (sigma 8), active-active failure results (0-500 seconds)

Mainly because the variability did not change the availability of any of the firewalls the performance results are exactly the same. Knowing the function that simulates the processing operation of the firewall keeps being the same as the last simulation, the total throughput is presented in Figure 67.

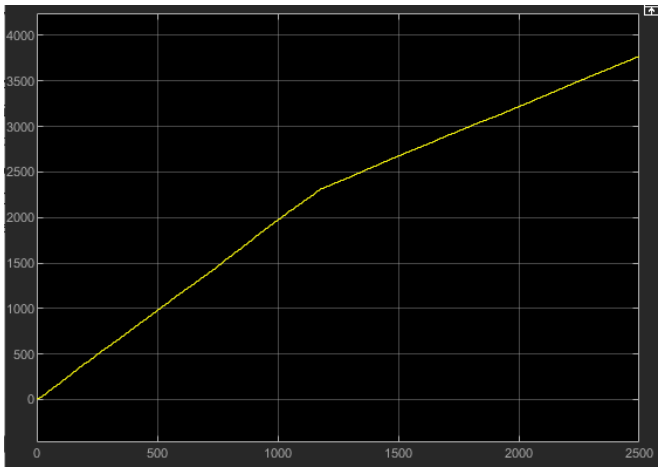


Figure 67: Extreme value distribution failure (sigma 8), total packets processed (active-active)

The same happens with the time that packets had to experience between its arrival to the firewall to being processed. The results are the same as the ones from the lower variability, as seen in Figure 68.

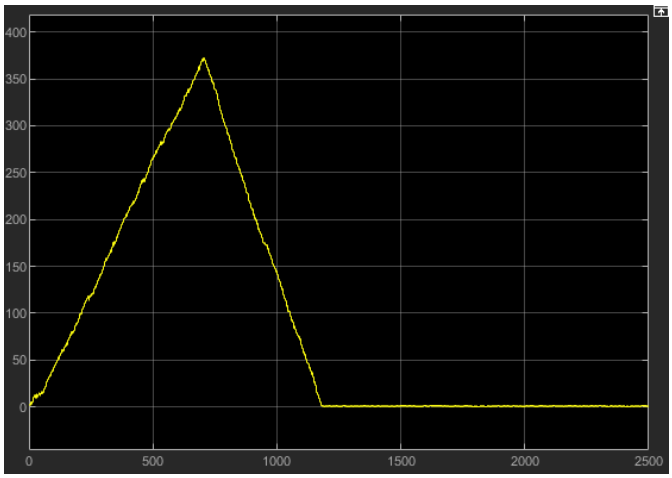


Figure 68: Extreme value distribution failure (sigma 8), total time to process a packet (active-active)

- **Active-Passive Results**

Following the parameters from the active-active scenario, the time for this simulation is 2500 seconds. In the same way than in the active-active configuration, the change in the availability of the failure function did not affect the performance of any of the firewalls. In

snapshot from 0 to 500 seconds in the following illustration shows how the values hardly go below 40. That snapshot is presented in Figure 69.

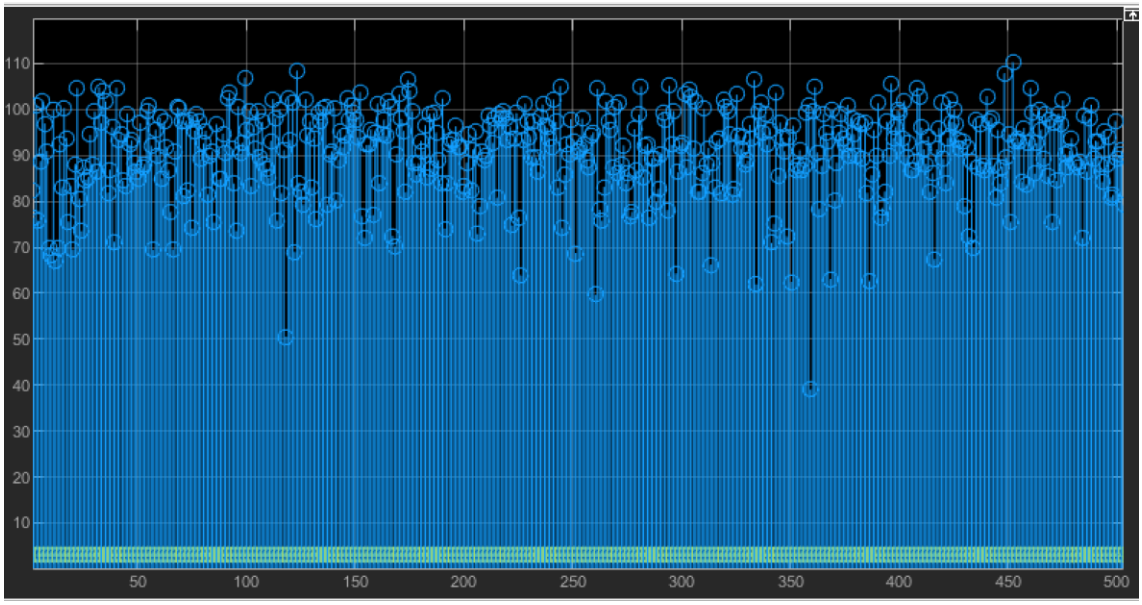


Figure 69: Extreme value distribution failure (sigma 1), active-passive failure results (0-500 seconds)

In the same way than the active-active configuration, with no changes in the failure events compared to the simulation with a sigma with the value of 3, the performance results stay the same. This similarity not only considers the behaviour of the function, but also the values.

- **Comparison Active-Active/Active-Passive**

The results from the case of sigma 8 are the same that the ones from sigma 3. Table 8 shows a summary of the performance results explained in the sections above.

Table 8: Extreme value distribution failure (sigma 8), active-active vs active-passive

Configuration	Active-Active	Active-Passive
Total throughput (packets)	3.764 e3	2.740 e3
Wait time behaviour	Stable	Maximum limit reached
Wait time peak (seconds)	368	917

8.4.3 COMPARISON SIGMA 3/SIGMA 8

The increase in variability of the probability distribution function could not change the behaviour and values of the performance. Active-active and active-passive configurations worked under perfect conditions, with no failure events, regardless the variabilities considered in the simulations. This also made a situation in which neither the total throughput or the wait time peak changed between configurations, as seen in Table 9.

Table 9: Sigma 8 performance, compared to sigma 3

Configuration	Active-Active	Active-Passive
Total throughput	0%	0%
Wait time peak	0%	0%

Capítulo 9. PROPOSED ARCHITECTURE

This section will analyse the changes recommended for the new architecture of firewalls of all Scottish Power's networks. Some of the most applicable technologies have been already studied in last sections.

Cisco FirePower NGFWs in the Telecommunications networks originated a vast list of problems, being the single point of failure (SPF) the critical of all. This problem created scenarios in which, in case of a failure of one of those firewalls, the network was uncapable of transmitting information. Furthermore, it also was commented, how a transition to Palo Alto NGFWs would be the most reliable option at the moment, not only for their better capabilities, but also that, since all Palo Alto firewalls from the system can be managed and supervised through the Panorama software, their integration would reduce the complexity of operating them.

Moreover, it was also studied how, in a scenario were all firewalls used were from Palo Alto, the network will have high availability capabilities, uniting both, RTS and Telecommunications network. The two configurations available for this technology were active-active and active-passive, and both configurations would be beneficial and possible to implement in the new architecture. Since both had advantages and difficulties in its operation, last Capítulo helped to decide which would be optimal at the end. With the help of the different models and simulations used, implementing a pair of Palo Alto NGFWs in active-active configuration would have better results in term of performance, even if it also increases the complexity of the operation of those assets.

Finally, having updated the different networks, changing all firewalls or pair of firewalls, to an active-active pair of Palo Alto firewalls, another aspect commented in the beginning is also addressed for the final proposal. A symmetric system, between north and south, was also considered. That makes the hole system of networks look similar, reducing

complications during the management of the different firewalls and the operation of transmitting information overall.

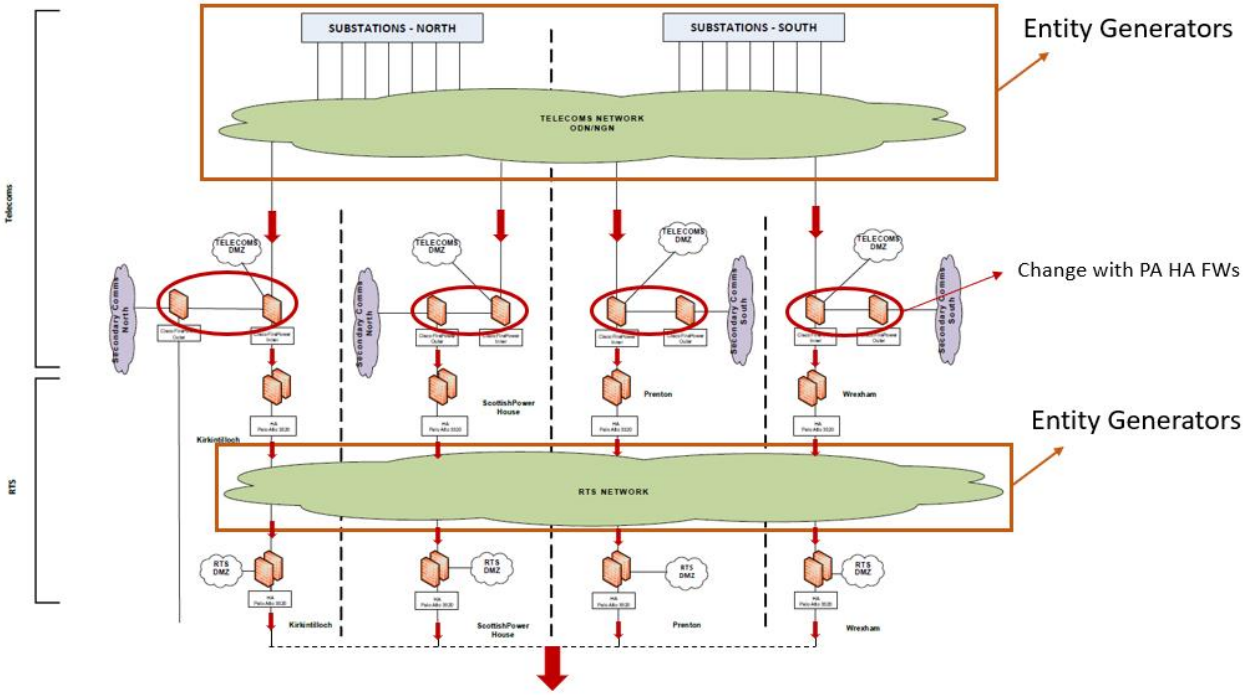


Figure 70: Proposed architecture

With that being said, Figure 70 shows the changes proposed for the new architecture of firewalls. The next subsection from this part of the project will analyse through other Simulink models the performance of the new architecture, compared to the current one which possesses SPFs.

Firstly, a definition of some technical specifications used for the design of the model will be presented with the presentation of the model itself. Then the next subsection will analyse both results, considering normal conditions, in which a failure of a firewall is nearly impossible using the Extreme Value Distribution used in last section. Finally, the last one will increase the probability of failure, using the constant scenario from last section, to see how the two systems behave and perform during failure scenarios.

9.1 TECHNICAL SPECIFICATIONS AND MODEL

This part of the project will cover the different technical specifications taken into account during the design of the Simulink's model traying to recreate both, the current and the proposed architecture.

The model is divided in two parts, the recreation of every network, and the model simulating the possible failure of every firewall of those networks. The networks are divided in two different areas:

- North Network: this area is composed by the Kirkintilloch network and the Scottish Power House network.
- South Network: this area is composed by the Prenton network and the Wrexham network.

As it was presented before, symmetry is one of the focuses, so networks are the same, in terms of features, technologies and behaviour. This condition will create scenarios in which all networks share similar performance results. All those networks have a similar architecture as the model used for the active-active vs. active-passive models. The main differences are, as seen in Figure 70, there will be 3 clusters of firewalls and two parts where entities are generated, the ones coming from the telecommunication network and the ones coming from the RTS network. The entity generators will follow the same behaviour as the ones used in the last simulations, both are composed by group of four generators, generating packets with a size of 4 Mbps with an intergeneration time action following Equation 1.

In the same way as in last simulation, network itself is considered, using cat6 with a capacity that goes between 100 Mbps and 1 Gbps, more than sufficient for the packets being transmitted. That capacity is correctly represented in the capacity of the entity queue dedicated to the network.

For the firewalls, the ones chosen are the Palo Alto Serie 3200 and 3400, being the Series 3200 the more restrictive one. They have a throughput capacity that can reach 5 Gbps, again,

more than enough for the inputs considered. That capacity is also represented in the queue capacity representing the firewalls. Regarding the processing time of the firewalls, there will be two options. During the first set of simulations, the one closer to reality, the processing time will follow Equation 4. On the other hand, on the critical conditions simulation the processing time will be considered fast (0.01 seconds), that fastness is also programmed in the server's, used to represent the firewalls, process time.

Moreover, the model used to simulate the failure of any of the firewalls from the network follows the same structure and behaviour as the one used in the active-active configuration from last section. The main difference is that in the current architecture's case, if the SPF fails, all the information that needs to go through the device is blocked until repaired. But, besides that aspect, the coding and conditions remain the same.

The different models used for the study coming from this section are presented in Annex III. Those diagrams are from the North and South Network and from the different failure models.

9.2 NORMAL CONDITIONS ANALYSIS

This subsection will analyse the different performance results coming from the current and proposed architecture models. The probability of failure from the models will follow an Extreme Value Distribution with a sigma of 3. These results will have the results more similar to reality, since the probability of failure is really low. Lastly, the simulation will last 100 seconds.

9.2.1 CURRENT ARCHITECTURE SIMULATION

During the 100 seconds simulation, as expected, no failures occurred in any of the firewalls from the different networks, since the probability is really low. Figure 71 shows how the failure parameter never came near the value 5 in one of the pair of firewalls from the system's model.

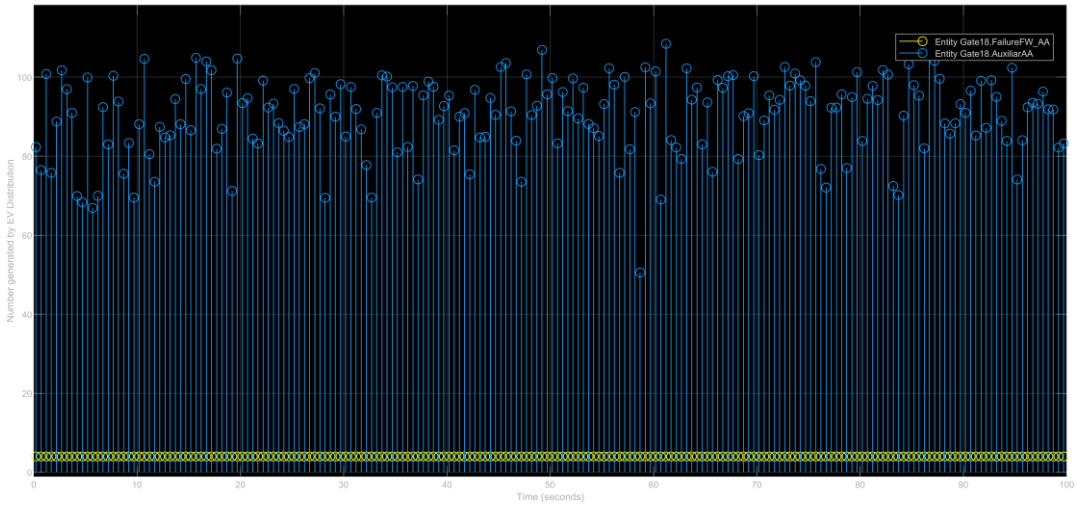


Figure 71: Current architecture, failure results under normal conditions SPF firewall (SPH)

The pace in which the system overall was capable of finishing the transmission of the different packets from the generators to the receivers was nearly constant. This makes sense since the firewalls always worked without arriving to capacity limits. The total throughput of one of the networks is shown in Figure 72.

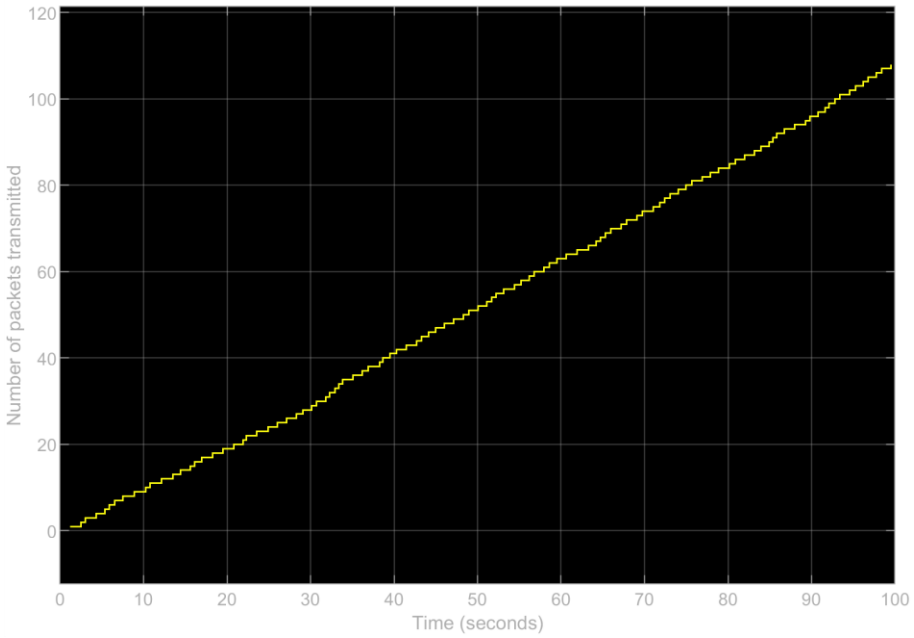


Figure 72: Current architecture, total throughput under normal conditions (SPH)

Another important aspect to take into account is the identification of the bottle neck from the system. In this case, the part of the network which has a lower processing rate is the SPF, since there is only one operating firewall. The number of packets waiting to be processed keeps increasing and are shown in Figure 73.

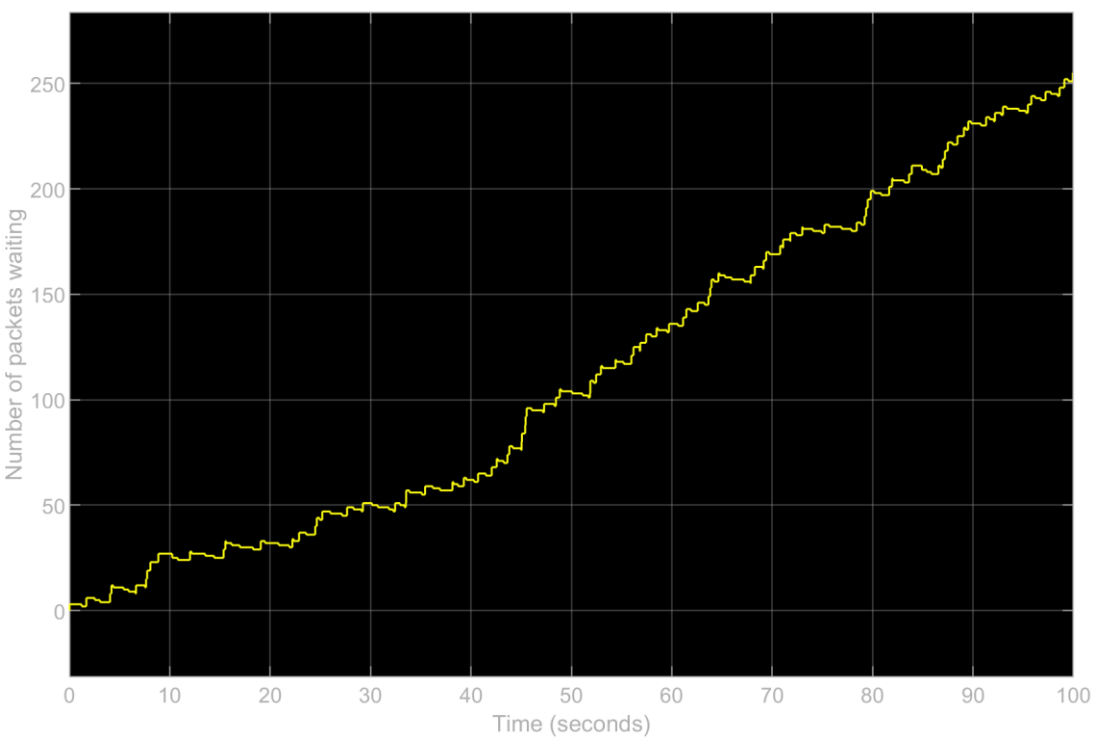


Figure 73: Current architecture, waiting time from one firewall under normal conditions (SPH)

9.2.2 PROPOSED ARCHITECTURE SIMULATION

In the case of the proposed architecture, there were not any failures in any of the firewalls during the 100 seconds simulation. In the same way as in the current architecture, the failure values did not get to any value near the limit to be considered as a failure. Figure 74 shows the different values during the 100 seconds simulation.

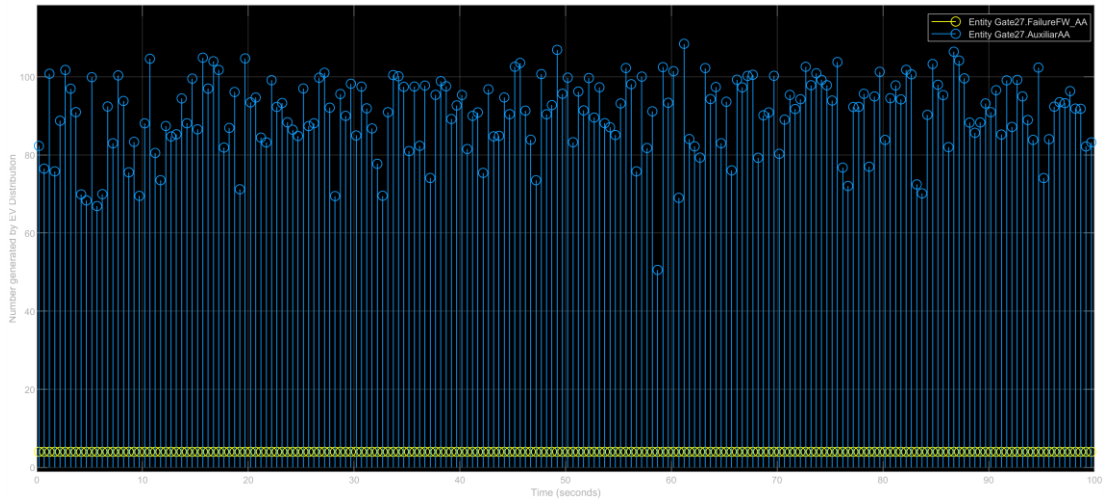


Figure 74: Proposed architecture, failure results under normal conditions pair of firewalls (SPH)

Again, the total throughput is similar, for not saying the same, as in the current architecture. Since the capacity of the firewalls is bigger than the information being transmitted this is an event that makes sense, since no increase in the number of firewalls working is needed in the system modelled to operate all the input. The throughput from one of the networks, at the end point, is shown in Figure 75.

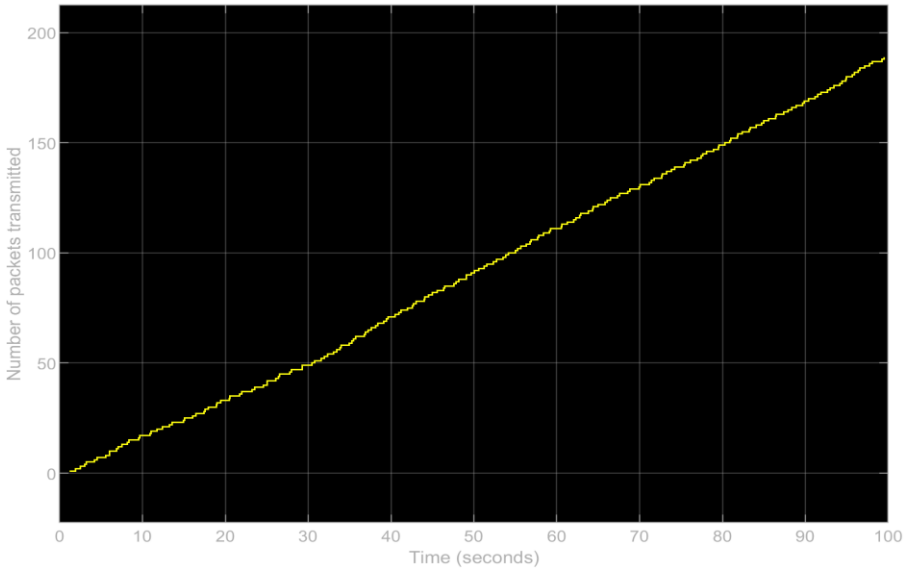


Figure 75: Proposed architecture, total throughput under normal conditions (SPH)

The bottle neck from this system is the first pair of firewalls, the ones that used to be from the Telecommunication network. In that point the number of packets waiting to be processed lightly increases without reaching worrying limits, as shown in Figure 76.

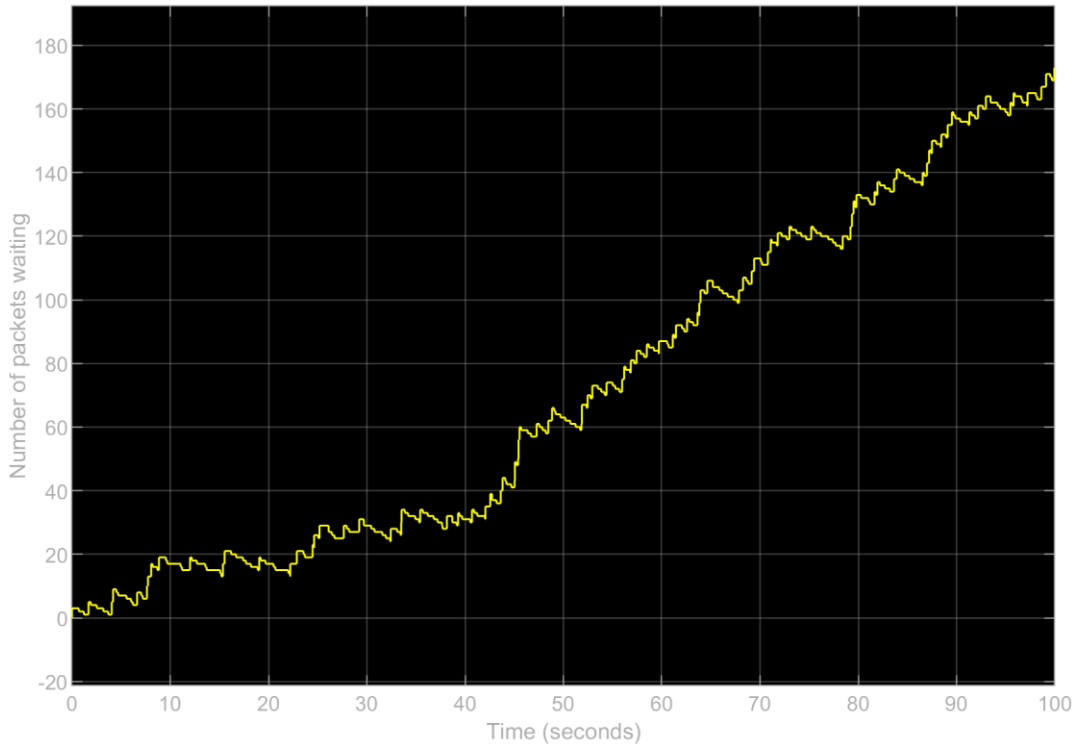


Figure 76: Proposed architecture, waiting time from one firewall under normal conditions (SPH)

9.2.3 COMPARISON BETWEEN CURRENT AND PROPOSED ARCHITECTURE

In normal conditions, there is no failure expected from any of the firewalls since the technologies are recognized to be hugely reliable. The total throughput from both architectures studied change, for this case the new architecture is capable of filtering and transmitting more pockets.

Furthermore, something noticeable is how the limit capacity of the firewalls will be reached slower with the proposed architecture, compared to the current one. This can be clearly seen comparing Figure 73 and Figure 76.

9.3 CRITICAL CONDITIONS ANALYSIS

This subsection will analyse the different performance results coming from the current and proposed architecture models when the conditions of failure are more possible. The probability of failure from the models will follow a complete random distribution, meaning the real probability of failure is 5%. These results try to show the real difference in terms of availability and operation in critical scenarios between both architectures. The simulation will last 100 seconds and if a SPF firewall fails, this firewall will take 80 seconds to be operational again, creating a context which represents the real problematic that one of those events could have in the system. On the other hand, failures from one of the firewalls from a HA pair will take 30 seconds to recover, existing a 5 second delay for the active-passive configurations to change from primary to back-up, to clearly show how that system will work, alternating the flow depending on the availability of the firewalls.

9.3.1 CURRENT ARCHITECTURE SIMULATION

The current architecture suffered from failures in some of the firewalls, being the more critical the one happening in the firewall with no pair, the SPF. This is due the fact that all communication going through that point is blocked in the event of a failure.

In Figure 77 it can be seen how at 22 seconds a failure occurs, the state from the firewall goes from 2 to 1, meaning the generated number by the failure module reaches a value below or equal to 0.05. The failure then is maintained until the end of the simulation since it will take 80 seconds to be repaired. The system will suffer that event since all information going through that firewall will not be able to arrive to the end point.

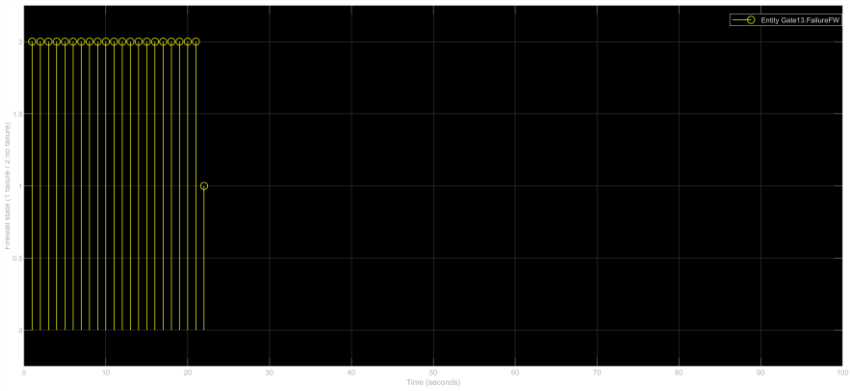


Figure 77: Current architecture, failure results under critical conditions SPF firewall (KRK)

Analysing the total throughput of one of the networks, this failure is reflected. The pace in which the packets are being processed and transmitted to the end point slows down from the seconds 22. Until that time, the information coming from the RTS and Telecommunication services were being transmitted, but since the firewall blocks all information coming from the Telecommunications packets, the only information transmitted from the time of the failure are RTS generated packets. That total throughput from one of the networks is shown in Figure 78.

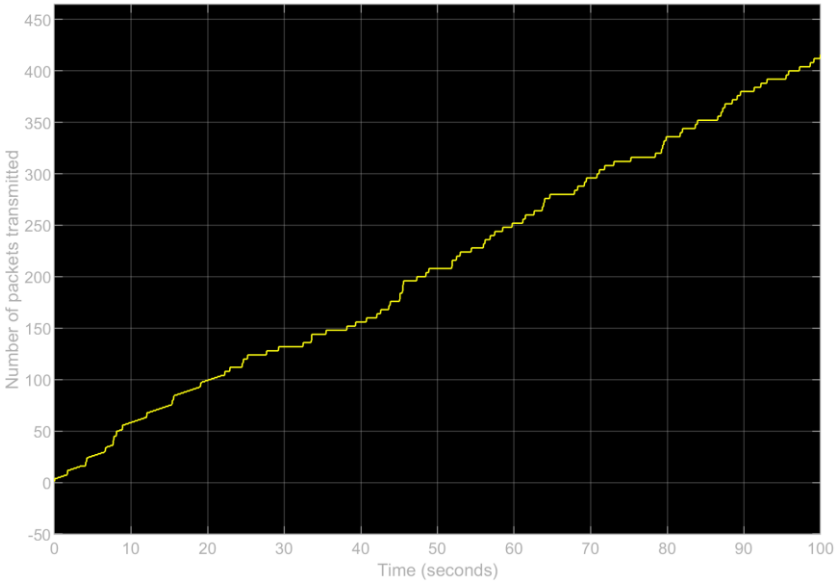


Figure 78: Current architecture, total throughput under critical conditions (KRK)

9.3.2 PROPOSED ARCHITECTURE SIMULATION

In the same way as in the current architecture's simulation, failures occurred during the simulation of this model. Figure 79 shows the different failure event that occurred in one of the pair of the firewalls. It can be seen how during the 100 seconds simulation, 3 failure events happened. During the times that one of the firewalls was not operational, the operational one kept transmitting, processing, and filtering information.

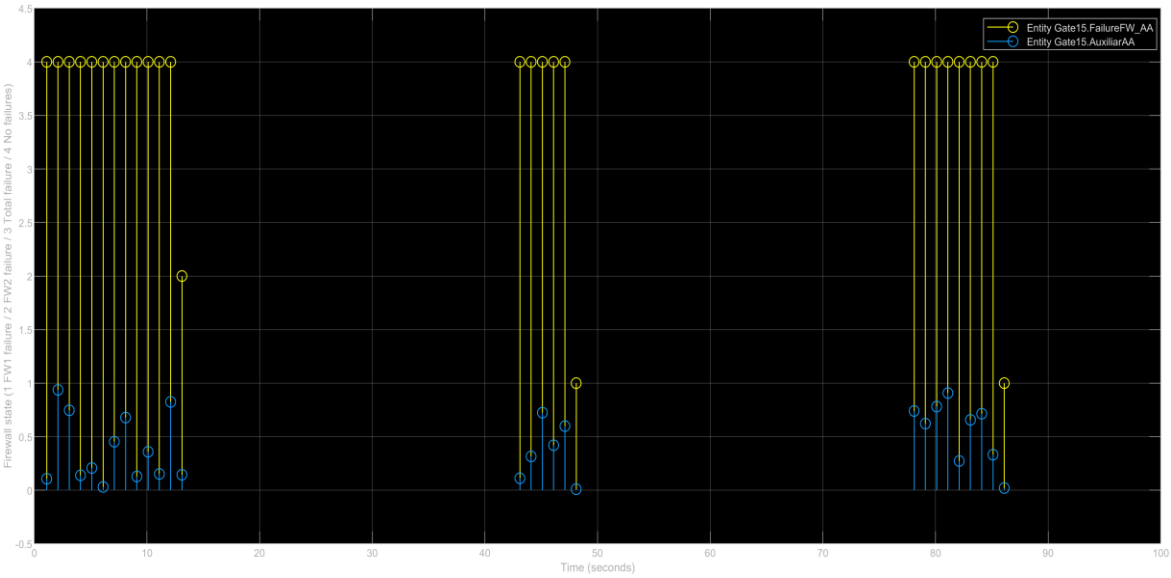


Figure 79: Proposed architecture, failure results under critical conditions pair of firewalls (KRK)

During those failures, the pair of firewalls kept transmitting packets, this made possible to achieve a pace in the total throughput that relatively did not change during the test time. The high availability of the pair of firewalls let the information coming from the RTS and Telecommunication services to be transmitted to the end point. This can be seen in Figure 80, which shows the total throughput of one of the networks.

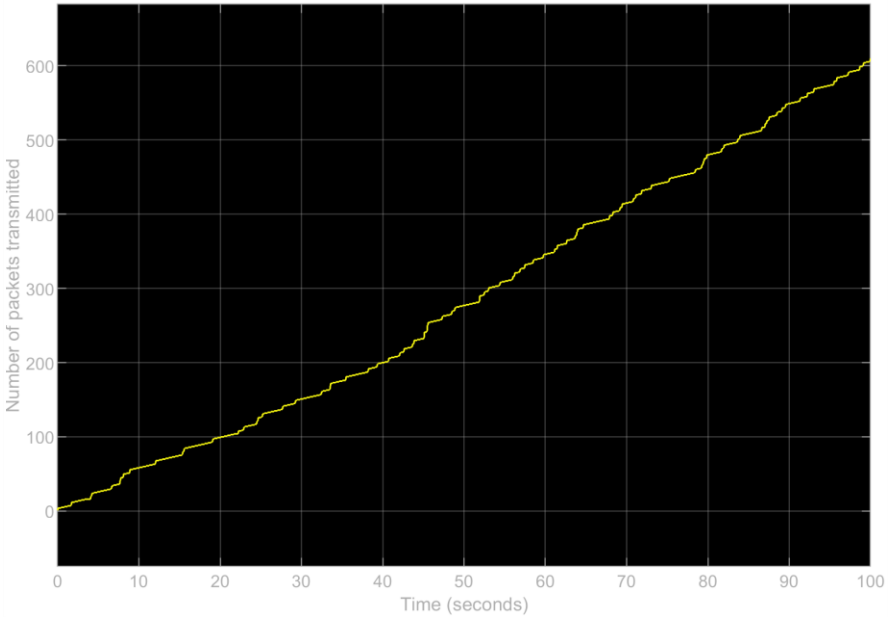


Figure 80: Proposed architecture, total throughput under critical conditions (KRK)

9.3.3 COMPARISON BETWEEN CURRENT AND PROPOSED ARCHITECTURE

In critical conditions, failures have occurred in both architectures. The current architecture was incapable of transmitting information from one of the packets generating points (Telecom network), while the proposed one kept transmitting thanks to the availability from the other firewall of the pair. This created a scenario in which, even when the proposed architecture suffered from three times more failure events, the proposed architecture was capable to transmit nearly 50% more packets than the current architecture. Table 10 shows a summarize of the performance results of one the networks (KRK) from both systems.

Table 10: Current and proposed performance results under critical conditions (KRK)

Architecture	Current	Proposed
Total throughput (packets)	416	608
Failure events	1	3

Capítulo 10. SDGs PERSPECTIVE

This chapter will comment the importance of this project to contribute to some of the goals from the Sustainable Development Goals (SDGs).

Firstly, goal 9 talks about the importance to create resilient infrastructure, promoting industrialization and technological innovation. The development and improvement of the communication systems performance from the electrical grid, the project can contribute to, overall, a better and more reliable infrastructure.

Furthermore, the project can also be considered to contribute to goal 7, regarding clean and affordable energy, and goal 11, which tries to achieve more sustainable communities and cities. Updating the telecommunications and RTS systems from the electrical grid will, at the end, contribute to ensure affordable and reliable energy supply, benefiting consumers, cities, and society.

Capítulo 11. CONCLUSIONS & FUTURE WORKS

This project intention was to analyse the different technologies, techniques and configurations that could be helpful in Scottish Power firewalls architecture to achieve a high redundancy and availability network. To achieve that end goal, a study on the different technologies available in the market was carried, concluding that a complete change to Palo Alto new generation firewalls (NGFWs) was the most beneficial due to, not only the updated capabilities, but also because of the possibility to manage and supervise all assets by one only software, Panorama. Most of the firewalls connected to the architecture will operate in Level 3 of the Purdue Model, the control level, the exceptions will be the firewalls connected to the corporate/enterprise network, which will be in Level 3.5 as DMZ, and the firewalls connected to the devices from Level 2, which will be part of Level 2.5.

Once the technologies for the future architecture were chosen, a first study of the operation of those technologies was done. Their high availability (HA) configurations were analysed, from a technical view, looking into the characteristics of those configurations to look which would be more reliable in the desired future system. That analysis was then followed by a practical analysis, in which simulations were performed and the performance results of the different configurations available on Palo Alto's NGFWs were revised. That technical and practical analysis helped to come with the conclusion that active-active configuration was the one which would provide with most benefits, even if this choice carried an increase in the complexity of the operation of the architecture.

Moreover, a high-level analysis on the routing landscape was performed. The routing techniques used in the different networks from Scottish Power were studied, concluding that North and South use different strategies. The North network relied more in static routing techniques, while the use of dynamic routing techniques was more usual in the South Network. The list of recommendations to update and optimize the current routing landscape are the following: summarization techniques to limit routes and complexity on the routing, the use of router ID and process ID to improve consistency and summarization, the

authentication between OSPF neighbours to achieve higher security, and finally, reducing the routing area and the OSPF flood, reducing complexity overall.

Finally, a new architecture consoling the management and supervision of the Infrastructure Firewall Estate, uniting RTS and Telecommunications networks, was proposed. This new architecture was composed in a whole by pair of firewalls from Palo Alto NGFWs, creating HA clusters of firewalls, all operated with the help of Panorama software. Also, the proposed architecture will be symmetric between North and South network, reducing complexity in its operation and management. Once al technical specifications from this proposed architecture were stablished, other simulations were performed to see the behaviour of both, the current and the proposed architecture. Those simulations showed how in normal conditions, were the firewalls have a low probability to fail, the performance of the proposed systems was more beneficial in terms of efficiency and total throughput. The main change from both architectures is that, in normal conditions, in systems with a firewalls cluster where there is only one single firewall, the system will be more congested at that point, which at the end could cause problematics in terms of processing capacity. Moreover, in critical conditions, were failures occurred more often, the proposed architecture showed a great superiority in terms of total throughput performance compared to the current architecture. All those updates showed how there would be an improvement in the performance on the network, which at the end it means that the proposed architecture will be more secure and reliable, and with high availability and redundancy capabilities.

Future works, related to this project could discuss the real problematics that an active-active configuration of the architecture's firewalls could generate. Problems such as asymmetric routing or an undesired and uncontrolled increase in the complexity of the operation and management of the system and its firewalls would need to be covered to have a clear view on how those changes will really affect the architecture at the end.

Capítulo 12. BIBLIOGRAPHY

[1] Jingcheng Gao, Yang Xiao, Jing Liu, Wei Liang, C.L. Philip Chen, "A survey of communication/networking in Smart Grids", Future Generation Computer Systems, Volume 28, Issue 2, 2012, Pages 391-404.

[2] Alberto Sendin, Miguel A. Sanchez-Fornie, Inigo Berganza, Javier Simon, Iker Urrutia, "Telecommunication Networks for the Smart Grid", Artech House, 2016.

[3] M. C. Falvo, L. Martirano, D. Sbordone and E. Bocci, "Technologies for smart grids: A brief review," *2013 12th International Conference on Environment and Electrical Engineering*, Wroclaw, Poland, 2013, pp. 369-375, doi: 10.1109/EEEIC.2013.6549544.

[4] D. M. Laverty, D. J. Morrow, R. Best and P. A. Crossley, "Telecommunications for Smart Grid: Backhaul solutions for the distribution network," IEEE PES General Meeting, Minneapolis, MN, USA, 2010, pp. 1-6, doi: 10.1109/PES.2010.5589563.

[5] M. B. Line, I. A. Tøndel and M. G. Jaatun, "Cyber security challenges in Smart Grids," 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, Manchester, UK, 2011, pp. 1-8, doi: 10.1109/ISGTEurope.2011.6162695.

[6] G. A. Marin, "Network security basics," in IEEE Security & Privacy, vol. 3, no. 6, pp. 68-72, Nov.-Dec. 2005, doi: 10.1109/MSP.2005.153.

[7] Wu Kehe, Zhang Tong, Li Wei, Ma Gang, "Security Model Based on Network Business Security", In Proc. of Int. Conf. on Computer Technology and Development, 2009.

[8] Shailja Pandey, Mr Reza Beshghi, "Modern network security: issues and challenges", Technology, BBDNITM, Iran, Vol. 3 No. 5, May 2011.

[9] Eric Cole, Ronald Krutz, James W. Conley, "Network Security Bible", 20 December 2004.

[10] J. Liang and Y. Kim, "Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall," *2022 IEEE 12th Annual Computing and*

Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2022, pp. 0752-0759, doi: 10.1109/CCWC54503.2022.9720435.

[11] Cruz, Luis. "What Is Unified Threat Management (UTM)?" Study.com. https://study.com/academy/lesson/what-is-unified-threat-management-utm.html.

[12] Bazrafshan, Zahra, Hashem Hashemi, Seyed Mehdi Hazrati Fard, and Ali Hamzeh. "A survey on heuristic malware detection techniques." In The 5th Conference on Information and Knowledge Technology, pp.113-120. IEEE, 2013, pp. 2

[13] "Integrated Threat Prevention - Paloguard." https://www.paloguard.com/datasheets/Threat_Prevention_ds-new.pdf.

[14] Palo Alto Networks Santa Clara, CA Jun 17. "Palo Alto Networks Launches World's First ML-Powered NGFW." Palo Alto Networks. https://www.paloaltonetworks.com/company/press/2020/palo-alto-networks-launches-worlds-first-ml-powered-ngfw

[15] Cisco FirePower 2100 Series Data Sheet. https://www.cisco.com/c/en/us/products/collateral/security/firepower-2100-series/datasheet-c78-742473.html

[16] Palo Alto 3200 Series Data Sheet. https://www.paloaltonetworks.co.uk/resources/datasheets/pa-3200-series

[17] Palo Alto 3400 Series Data Sheet. https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series

[18] SimEvents Library – Model and simulate message communication and discrete-event systems. https://uk.mathworks.com/products/simevents.html

ANNEX I: DATASHEET TABLES

CISCO FIREPOWER 2100 SERIES

Table 11: Cisco FirePower 2100 Series hardware specifications, part 1 [15]

Features	Cisco Firepower Model			
	2110	2120	2130	2140
Dimensions (H x W x D)	1.73 x 16.90 x 19.76 in. (4.4 x 42.9 x 50.2cm)	1.73 x 16.90 x 19.76 in. (4.4 x 42.9 x 50.2 cm	1.73 x 16.90 x 19.76 in. (4.4 x 42.9 x 50.2 cm)	1.73 x 16.90 x 19.76 in. (4.4 x 42.9 x 50.2 cm)
Form factor (rack units)	1RU	1RU	1RU	1RU
Integrated I/O	12 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45), 4 x 1 Gigabit (SFP) Ethernet interfaces	12 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45), 4 x 1 Gigabit (SFP) Ethernet interfaces	12 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45), 4 x 10 Gigabit (SFP+) Ethernet interfaces	12 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45), 4 x 10 Gigabit (SFP+) Ethernet interfaces
Network modules	None	None	10G SFP+, 1/10G FTW Options	10G SFP+, 1/10G FTW Options
Note: The 2100 Series appliances may also be deployed as dedicated threat sensors with fail-to-wire network modules. Please contact your Cisco representative for details.				
Maximum number of interfaces	Up to 16 total Ethernet ports, (12x1G RJ-45, 4x1G SFP)	Up to 16 total Ethernet ports, (12x1G RJ-45, 4x1G SFP)	Up to 24 total Ethernet ports (12x1G RJ-45, 4x10G SFP+, and network module	Up to 24 total Ethernet ports (12x1G RJ-45, 4x10G SFP+, and network module
Integrated network management ports	1 x 10M/100M/ 1GBASE-T Ethernet port (RJ-45)	1 x 10M/100M/ 1GBASE-T Ethernet port (RJ-45)	1 x 10M/100M/ 1GBASE-T Ethernet port (RJ-45)	1 x 10M/100M/ 1GBASE-T Ethernet port (RJ-45)

Table 12: Cisco FirePower 2100 Series hardware specifications, part 2 [15]

Features	Cisco Firepower Model			
Serial port	1 x RJ-45 console	1 x RJ-45 console	1 x RJ-45 console	1 x RJ-45 console
USB	1 x USB 2.0 Type-A (500mA)	1 x USB 2.0 Type-A (500mA)	1 x USB 2.0 Type-A (500mA)	1 x USB 2.0 Type-A (500mA)
Storage	1x 100 GB, 1x spare slot (for MSP)	1x 100 GB, 1x spare slot (for MSP)	1x 200 GB, 1x spare slot (for MSP)	1x 200 GB, 1x spare slot (for MSP)
Power supply configuration	Single integrated 250W AC power supply.	Single integrated 250W AC power supply.	Single 400W AC, Dual 400W AC optional. Single/Dual 350W DC optional1	Dual 400W AC. Single/dual 350W DC optional1
AC input voltage	100 to 240V AC	100 to 240V AC	100 to 240V AC	100 to 240V AC
AC maximum input current	< 2.7A at 100V	< 2.7A at 100V	< 6A at 100V	< 6A at 100V
AC maximum output power	250W	250W	400W	400W
AC frequency	50 to 60 Hz	50 to 60 Hz	50 to 60 Hz	50 to 60 Hz
AC efficiency	>88% at 50% load	>88% at 50% load	>89% at 50% load	>89% at 50% load
DC input voltage	-	-	-48V to -60VDC	-48V to -60VDC
DC maximum input current	-	-	< 12.5A at -48V	< 12.5A at -48V
DC maximum output power	-	-	350W	350W
DC efficiency			>88% at 50% load	>88% at 50% load
Redundancy	None	None	1+1 AC or DC with dual supplies	1+1 AC or DC with dual supplies
Fans	4 integrated (2 internal, 2 exhaust) fans2	4 integrated (2 internal, 2 exhaust) fans2	1 hot-swappable fan module (with 4 fans)2	1 hot-swappable fan module (with 4 fans)2
Noise	56 dBA @ 25C 74 dBA at highest system performance.	56 dBA @ 25C 74 dBA at highest system performance.	56 dBA @ 25C 77 dBA at highest system performance.	56 dBA @ 25C 77 dBA at highest system performance.

Table 13: Cisco FirePower 2100 Series hardware specifications, part 3 [15]

Features	Cisco Firepower Model			
Rack mountable	Yes. Fixed mount brackets included. (2-post). Mount rails optional (4-post EIA-310-D rack)	Yes. Fixed mount brackets included. (2- post). Mount rails optional (4-post EIA-310-D rack)	Yes. Mount rails included (4-post EIA- 310-D rack)	Yes. Mount rails included (4-post EIA- 310-D rack)
Weight	16.1 lb (7.3 kg): with 2x SSDs	16.1 lb (7.3 kg): with 2x SSDs	19.4 lb (8.8 kg) 1 x power supplies, 1 x NM, 1 x fan module, 2x SSDs	21 lb (9.53 kg) 2 x power supplies, 1 x NM, 1 x fan module, 2x SSDs
Temperature: operating	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C) or NEBS operation (see below)3	32 to 104°F (0 to 40°C)
Temperature: nonoperating	-4 to 149°F (-20 to 65°C)	-4 to 149°F (-20 to 65°C)	-4 to 149°F (-20 to 65°C)	-4 to 149°F (-20 to 65°C)
Humidity: operating	10 to 85% noncondensing	10 to 85% noncondensing	10 to 85% noncondensing	10 to 85% noncondensing
Humidity: nonoperating	5 to 95% noncondensing	5 to 95% noncondensing	5 to 95% noncondensing	5 to 95% noncondensing
Altitude: operating	10,000 ft (max)	10,000 ft (max)	10,000 ft (max) or NEBS operation (see below)3	10,000 ft (max)
Altitude: nonoperating	40,000 ft (max)	40,000 ft (max)	40,000 ft (max)	40,000 ft (max)
NEBS operation (FPR- 2130 Only)3			Operating altitude: 0 to 13,000 ft (3962 m) Operating temperature: Long term: 0 to 45°C, up to 6,000 ft (1829 m) Long term: 0 to 35°C, 6,000 to 13,000 ft (1829 to 3964 m) Short term: -5 to 55°C, up to 6,000 ft (1829 m)	

[1] Dual power supplies are hot-swappable.

[2] Fans operate in a 3+1 redundant configuration where the system will continue to function with only 3 operational fans. The 3 remaining fans will run at full speed.

[3] FPR-2130 platform is designed to be NEBS ready. The availability of NEBS certification is pending.

Table 14: Cisco FirePower 2100 Series NEBS, Regulatory, Safety and EMC Compliance [15]

Specification	Description
Regulatory compliance	Products comply with CE markings per directives 2004/108/EC and 2006/108/EC
Safety	• UL 60950-1 • CAN/CSA-C22.2 No. 60950-1 • EN 60950-1 • IEC 60950-1 • AS/NZS 60950-1 • GB4943
EMC: emissions	• 47CFR Part 15 (CFR 47) Class A (FCC Class A) • AS/NZS CISPR22 Class A • CISPR22 CLASS A • EN55022 Class A • ICES003 Class A • VCCI Class A • EN61000-3-2 • EN61000-3-3 • KN22 Class A • CNS13438 Class A • EN300386 • TCVN7189
EMC: Immunity	• EN55024 • CISPR24 • EN300386 • KN24 • TVCN 7317 • EN-61000-4-2, EN-61000-4-3, EN-61000-4-4, EN-61000-4-5, EN-61000-4-6, EN-61000-4-8, EN61000-4-11

PALO ALTO 3200 SERIES

Table 15: Palo Alto 3200 Series networking features, part 1 [16]

Interface Modes
L2, L3, tap, virtual wire (transparent mode)
Routing
OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing
Policy-based forwarding
Point-to-Point Protocol over Ethernet (PPPoE)
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
SD-WAN
Path quality measurement (jitter, packet loss, latency)
Initial path selection (PBF)
Dynamic path change
IPv6
L2, L3, tap, virtual wire (transparent mode)
Features: App-ID, User-ID, Content-ID, WildFire, and SSL Decryption
SLAAC

Table 16: Palo Alto 3200 Series networking features, part 2 [16]

IPsec VPN
Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication)
Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
VLANs
802.1Q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), LACP
Network Address Translation
NAT modes (IPv4): static IP, dynamic IP, dynamic IP and port (port address translation)
NAT64, NPTv6
Additional NAT features: dynamic IP reservation, tunable dynamic IP and port oversubscription
High Availability
Modes: active/active, active/passive, HA clustering
Failure detection: path monitoring, interface monitoring
Zero Touch Provisioning (ZTP)
Available with -ZTP SKUs (PA-3260-ZTP, PA-3250-ZTP, PA-3220-ZTP). Requires Panorama 9.1.3 or higher

Table 17: Palo Alto 3200 Series hardware specifications, part 1 [16]

I/O
PA-3220: 10/100/1000 (12), 1G SFP (4), 1G/10G SFP/SFP+ (4)
PA-3250: 10/100/1000 (12), 1G/10G SFP/SFP+ (8)
PA-3260: 10/100/1000 (12), 1G/10G SFP/SFP+ (8), 40G QSFP+ (4)
Management I/O
10/100/1000 out-of-band management port (1), 10/100/1000 high availability (2), 10G SFP+ high availability (1), RJ-45 console port (1), Micro USB (1)
Storage Capacity
240 GB SSD
Power Supply (Avg/Max Power Consumption)
Redundant 650-watt AC or DC (195/240)
Max BTU/hr
819
Input Voltage (Input Frequency)
AC: 100–240 VAC (50–60Hz)
DC: -48V to -60V
Max Current Consumption
AC: 2.3 A @ 100 VAC, 1.0 A @ 240 VAC
DC: -48 V @ 4.7 A, -60 V @ 3.8 A
Mean Time Between Failure (MTBF)
14 years
Rack Mount Dimensions
2U, 19" standard rack (3.5" H x 20.53" D x 17.34" W)
Weight (Standalone Device/As Shipped)
29 lbs / 41.5 lbs
Safety
cTUVus, CB
EMI
FCC Class A, CE Class A, VCCI Class A

Table 18: Palo Alto 3200 Series hardware specifications, part 2 [16]

Table 3: PA-3200 Series Hardware Specifications (continued)
Certifications
See paloaltonetworks.com/company/certifications.html
Environment
Operating temperature: 32°F to 122°F, 0°C to 50°C
Non-operating temperature: -4°F to 158°F, -20°C to 70°C
Humidity tolerance: 10% to 90%
Maximum altitude: 10,000 ft / 3,048 m
Airflow: front to back

PALO ALTO 3400 SERIES

Table 19: Palo Alto 3400 Series networking features [17]

Interface Modes
L2, L3, tap, virtual wire (transparent mode)
Routing
OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing
Policy-based forwarding
Point-to-Point Protocol over Ethernet (PPPoE)
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
Bidirectional Forwarding Detection (BFD)
IPsec and SSL VPN
Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication)
Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
GlobalProtect large-scale VPN for simplified configuration and management*
Secure access over IPsec and SSL VPN tunnels using GlobalProtect Gateway and Portals*
VLANs
802.1Q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), LACP
Network Address Translation
NAT modes (IPv4): static IP, dynamic IP, dynamic IP and port (port address translation)
NAT64, NPTv6
Additional NAT features: dynamic IP reservation, tunable dynamic IP and port oversubscription
High Availability
Modes: active/active, active/passive, HA clustering
Failure detection: path monitoring, interface monitoring
Mobile Network Infrastructure† (PA-3440 and PA-3430)
5G Security
GTP Security
SCTP Security

* Requires GlobalProtect License.
† For additional information, refer to our ML-Powered NGFWs for 5G datasheet.

Table 20: Palo Alto 3400 Series hardware specifications, part 1 [17]

I/O
PA-3410: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)
PA-3420: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)
PA-3430: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4), 40G/100G QSFP/QSFP28 (2)
PA-3440: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4), 40G/100G QSFP/QSFP28 (2)
Management I/O
100/1000 out-of-band management port (1) 100/1000 high availability (2), 10G SFP+ high availability (1) RJ-45 console port (1), Micro USB (1)
Storage Capacity
480 GB SSD

Table 21: Palo Alto 3400 Series hardware specifications, part 2 [17]

Table 3: PA-3400 Series Hardware Specifications (continued)
Power Supply (Avg/Max Power Consumption)
Redundant 450-watt AC (133W/190W)
Max BTU/hr
650
Input Voltage Frequency
AC: 100–240 VAC (50–60Hz)
Max Current Consumption
AC: 1.9 A @ 100 VAC, 0.8 A @ 240 VAC
Mean Time Between Failure (MTBF)
22 years
Rack Mount Dimensions
1U, 19" standard rack 14.15" x 17.15" x 1.70"
Weight (Standalone Device/As Shipped)
15.5 lbs / 25 lbs
Safety
cTUVus, CB
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
See paloaltonetworks.com/company/certifications.html
Environment
Operating temperature: 32°F to 104°F, 0°C to 40°C
Nonoperating temperature: -4°F to 158°F, -20°C to 70°C
Humidity tolerance: 10% to 90%
Maximum altitude: 10,000 ft/3,048 m
Airflow: front to back

ANNEX II: MATLAB CODE

PROBABILITY FUNCTION: EV & LOGNORMAL DISTRIBUTION

```
clear;
clc;

%Extreme value distribution
x=[0:0.01:100];
y1=evpdf(x,95,3);
y2=evpdf(x,95,5);
y3=evpdf(x,95,8);
y4=evpdf(x,95,10);
figure('Name','Extreme Value Distribution');
plot(x,y1)
hold on
plot(x,y2)
plot(x,y3)
plot(x,y4)
hold off
xlabel('Probability of being available')
ylabel('Probability Density')
legend('mu = 95, sigma = 3','mu = 95, sigma = 5','mu = 95, sigma = 8','mu = 95, sigma =
10','Location','northwest')

%Log-normal distribution
x=(0:0.01:100)';
pd1=makedist('Lognormal','mu',log(5),'sigma',0.5);
pd2=makedist('Lognormal','mu',log(5),'sigma',0.7);
pd3=makedist('Lognormal','mu',log(5),'sigma',0.9);
pd4=makedist('Lognormal','mu',log(5),'sigma',1);
y1=pdf(pd1,x);
y2=pdf(pd2,x);
y3=pdf(pd3,x);
y4=pdf(pd4,x);
figure('Name','Log-Normal Distribution');
plot(x,y1)
hold on
plot(x,y2)
plot(x,y3)
plot(x,y4)
hold off
xlabel('Probability of Failure')
ylabel('Probability Density')
legend('mu = log(5), sigma = 0.5','mu = log(5), sigma = 0.7','mu = log(5), sigma = 0.9','mu
= log(5), sigma = 1','Location','northwest')
```

PROBABILITY OF FAILURE IN ACTIVE-ACTIVE

```
%Random number
coder.extrinsic('rand');
entity.AuxiliarAA = rand;
probability1 = entity.AuxiliarAA;
probability2 = 1;

coder.extrinsic('rand');
probability2 = rand;

if probability1 <= 0.03
    entity.FailureFW_AA = 1;

elseif probability2 <= 0.03
    entity.FailureFW_AA = 2;

elseif probability2 <= 0.03 && probability1 <=0.03
        entity.FailureFW_AA = 3;

else
    entity.FailureFW_AA = 4;
end

%Log-normal distribution
entity.AuxiliarAA = lognrnd(log(5),1);
probability1 = entity.AuxiliarAA;
probability2 = 1;

probability2 = lognrnd(log(5),1);

if probability1 >= 95
    entity.FailureFW_AA = 1;

elseif probability2 >= 95
    entity.FailureFW_AA = 2;

elseif probability2 >= 95 && probability1 >= 95
        entity.FailureFW_AA = 3;

else
    entity.FailureFW_AA = 4;
end

%Extreme value distribution
entity.AuxiliarAA = random('ev',95,8);
probability1 = entity.AuxiliarAA;
probability2 = 1;

probability2 =random('ev',95,8);

if probability1 <= 5
    entity.FailureFW_AA = 1;

elseif probability2 <= 5
    entity.FailureFW_AA = 2;

elseif probability2 <= 5 && probability1 <= 5
        entity.FailureFW_AA = 3;

else
    entity.FailureFW_AA = 4;
end
```

PROBABILITY OF FAILURE IN ACTIVE-PASSIVE

```
%Random number
coder.extrinsic('rand');
entity.AuxiliarAP = rand;
probability1 = entity.AuxiliarAP;
probability2 = 1;

coder.extrinsic('rand');
probability2 = rand;

if probability1 <= 0.03
    entity.FailureFW_AP = 1;

elseif probability2 <= 0.03 && probability1 <=0.03
        entity.FailureFW_AP = 2;

else
    entity.FailureFW_AP = 3;

end

%Log-normal distribution
entity.AuxiliarAP = lognrnd(log(5),1);
probability1 = entity.AuxiliarAP;
probability2 = 1;

probability2 = lognrnd(log(5),1);

if probability1 >= 95
    entity.FailureFW_AP = 1;

elseif probability2 >= 95 && probability1 >=95
        entity.FailureFW_AP = 2;

else
    entity.FailureFW_AP = 3;

end

%Extreme value distribution
entity.AuxiliarAP = random('ev',95,8);
probability1 = entity.AuxiliarAP;
probability2 = 1;

probability2 = random('ev',95,8);

if probability1 <= 5
    entity.FailureFW_AP = 1;

elseif probability2 <= 5 && probability1 <=5
        entity.FailureFW_AP = 2;

else
    entity.FailureFW_AP = 3;

end
```

FUNCTION IN ROUTINGAA(ROT) SIMULINK FUNCTION BLOCK

```
function y = fcn(u)

% u=1, normal case, both FW working
% u=2, FW1 fails
% u=3, FW2 fails

global A;

if u == 2
    y = 2;
elseif u == 3
        y = 1;
elseif u ==1
        if A == 1
            y = 1;
            A = 2;
        elseif A ==2
           y = 2;
            A = 1;
        else
            y = 1;
            A = 1;
        end
else
    y = 1;

end
```

ANNEX III: SCHEMATICS

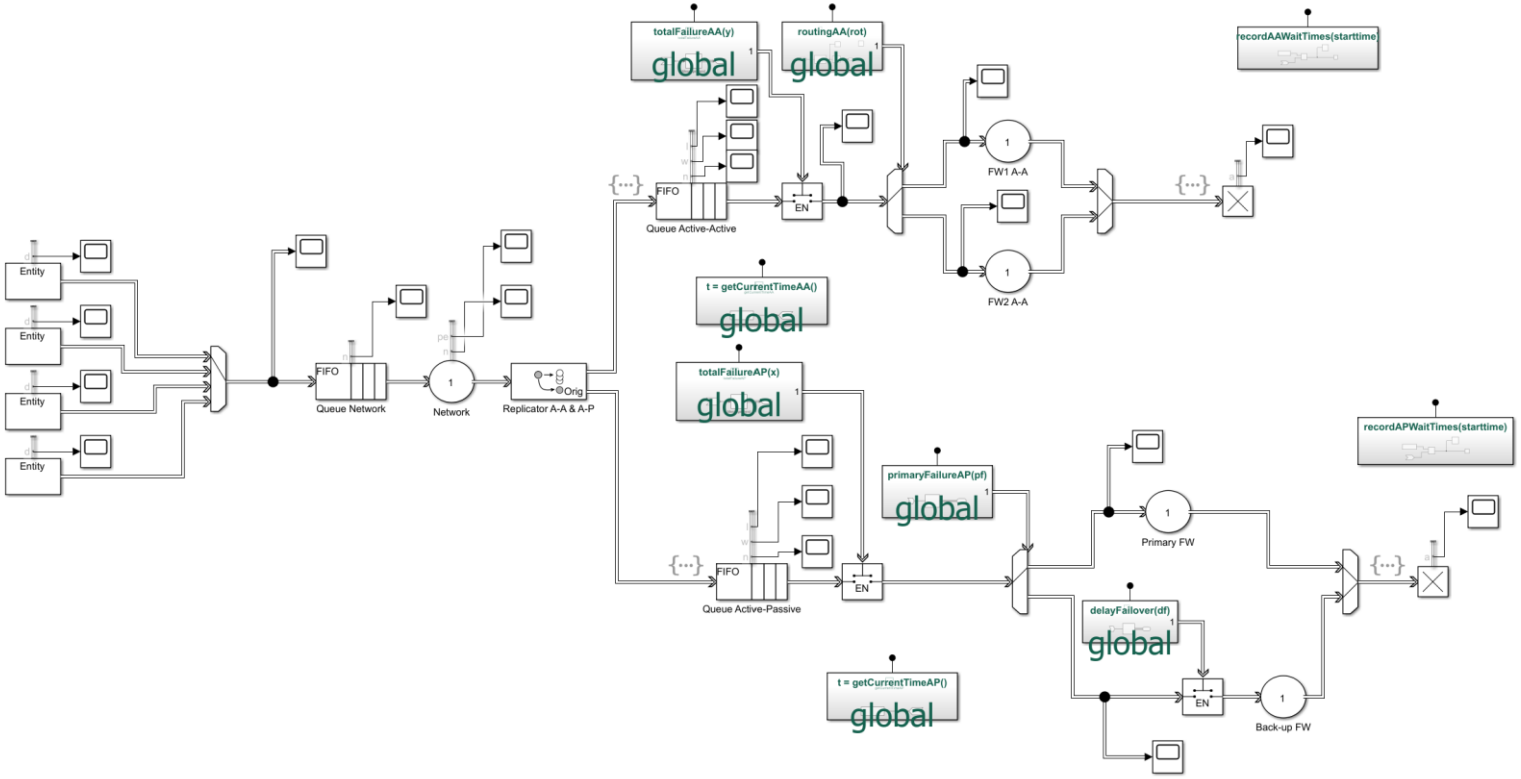


Figure 81: Simulink HA FW model

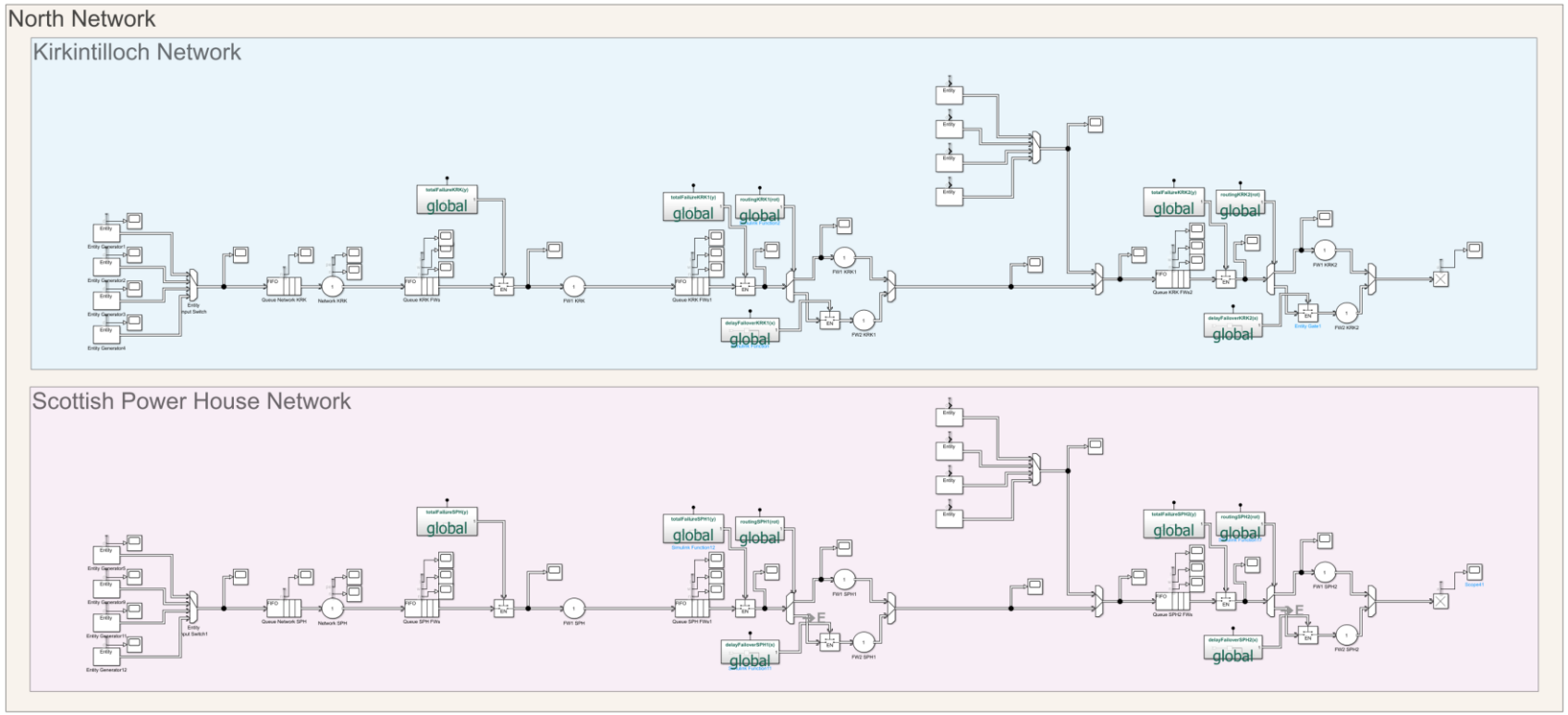


Figure 82: Current architecture North Network

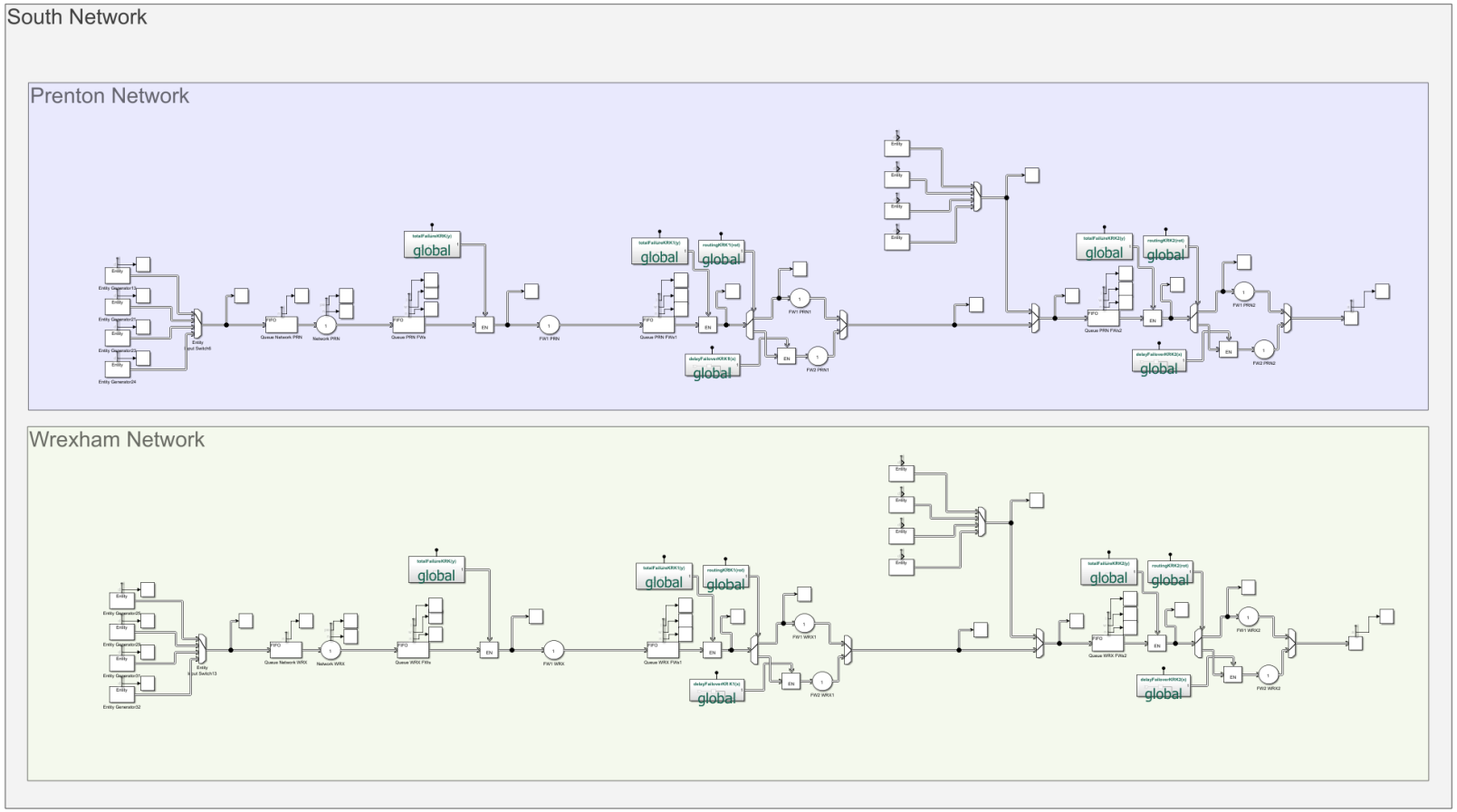


Figure 83: Current architecture South Network

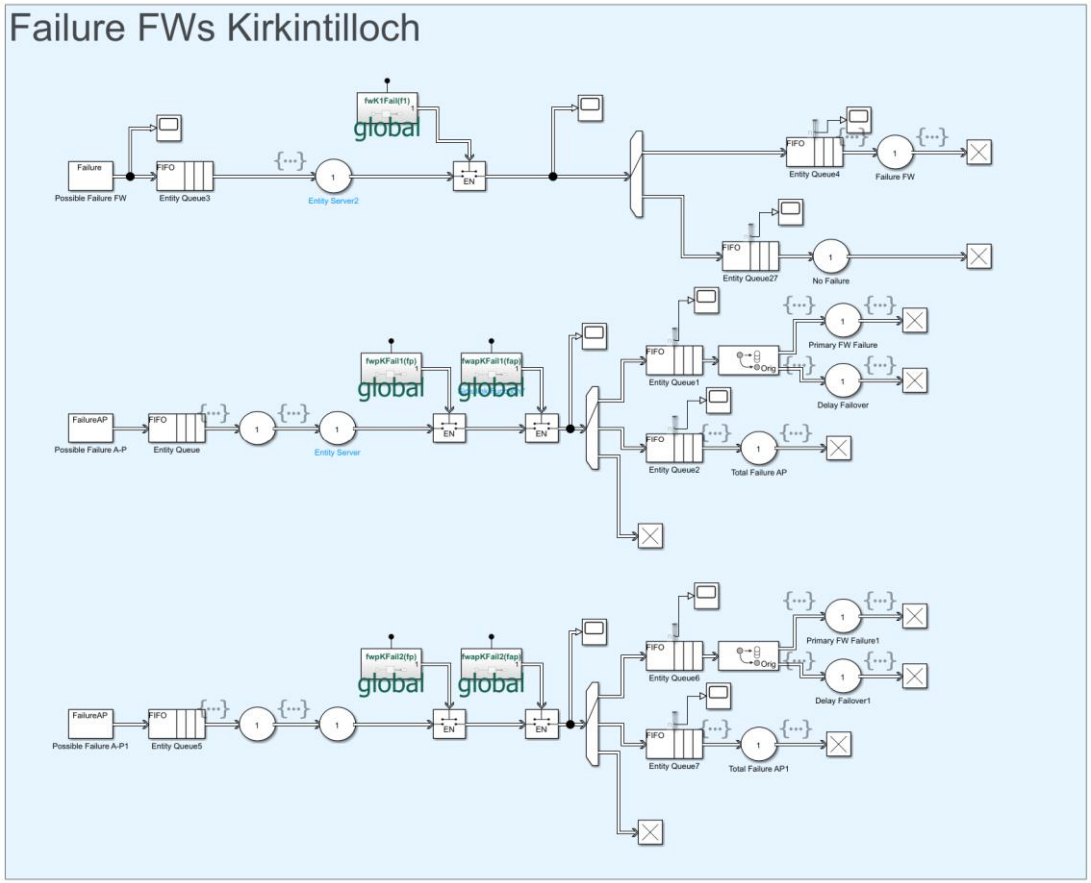


Figure 84: Current architecture failure model KRK

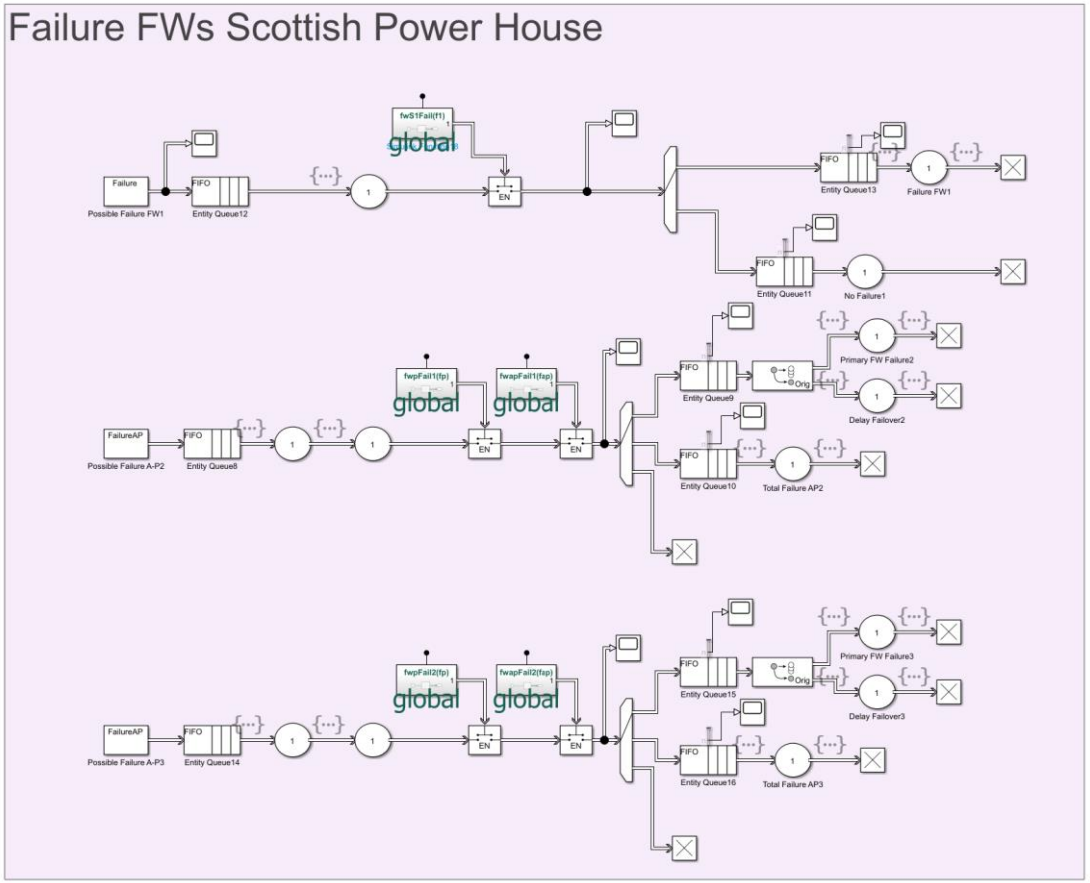


Figure 85: Current architecture failure model SPH

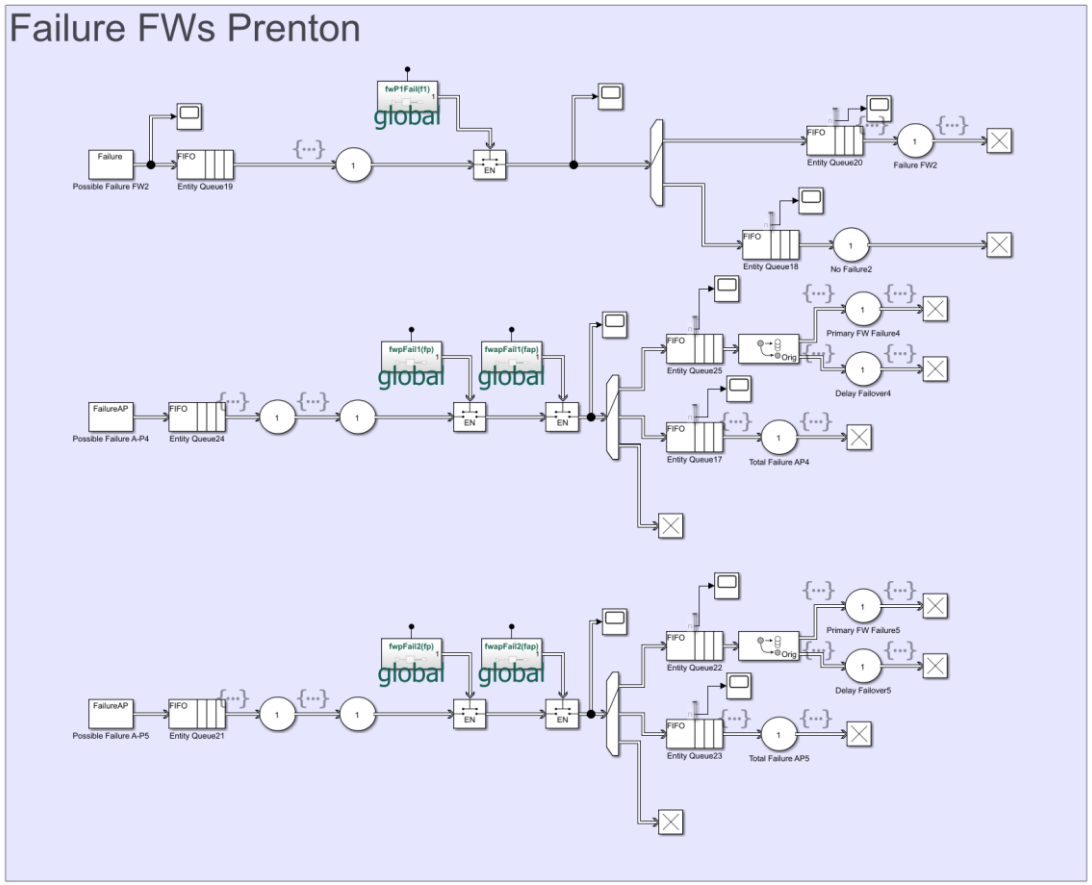


Figure 86: Current architecture failure model PRN

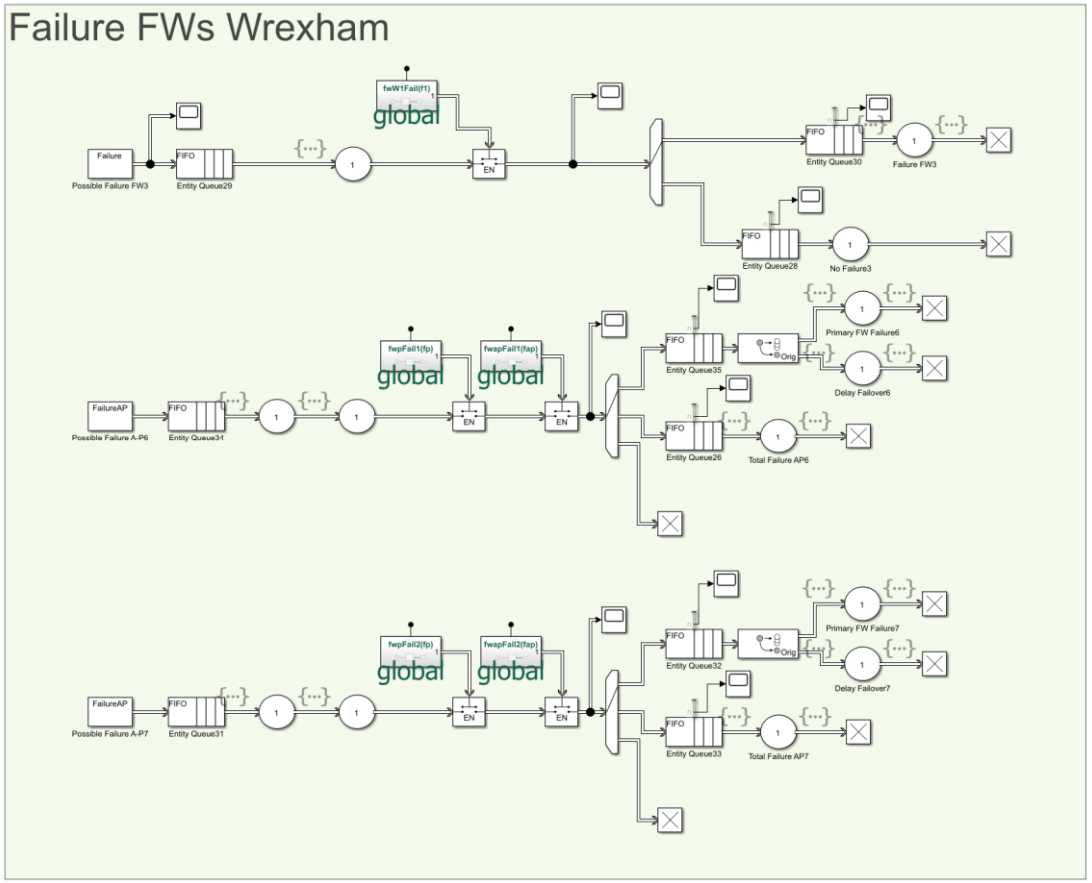


Figure 87: Current architecture failure model WRX

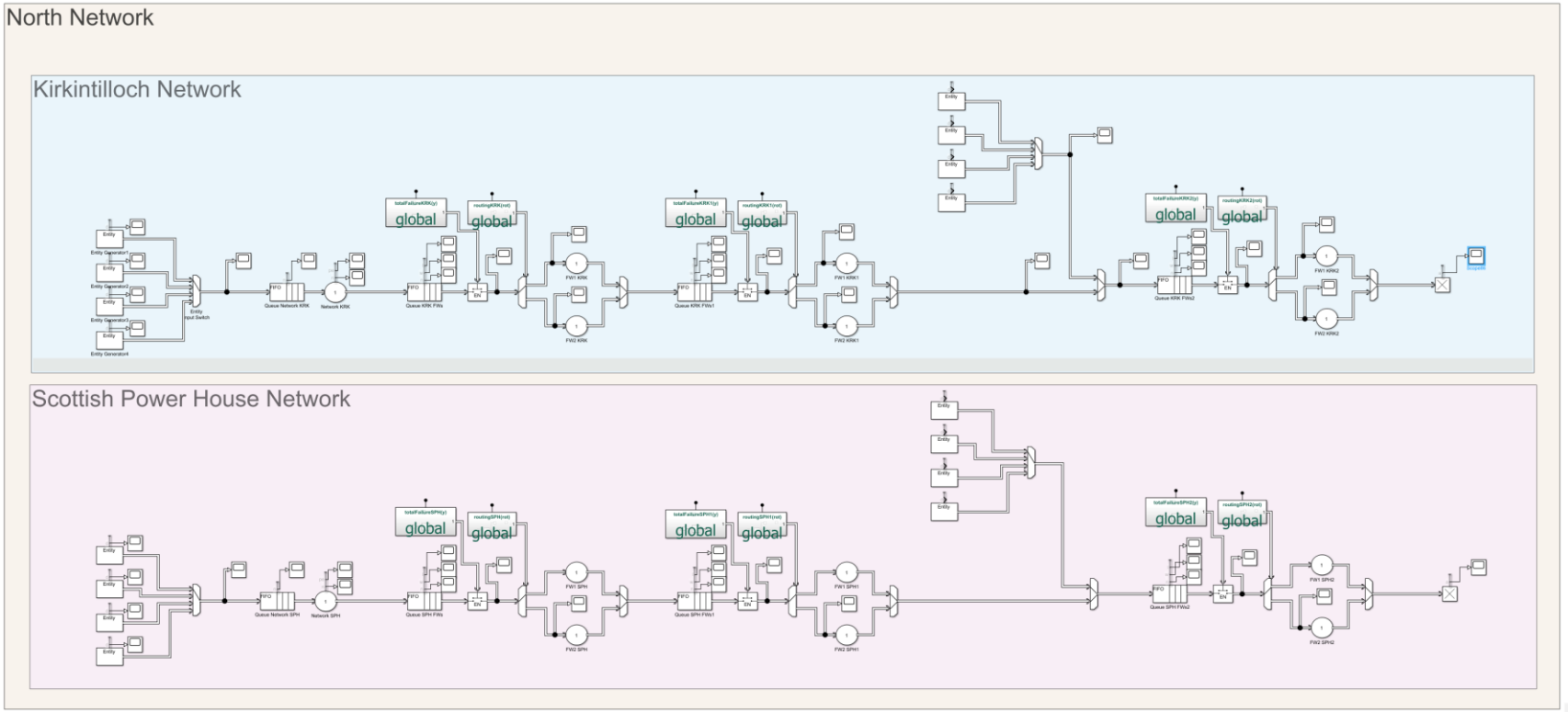


Figure 88: Proposed architecture North Network

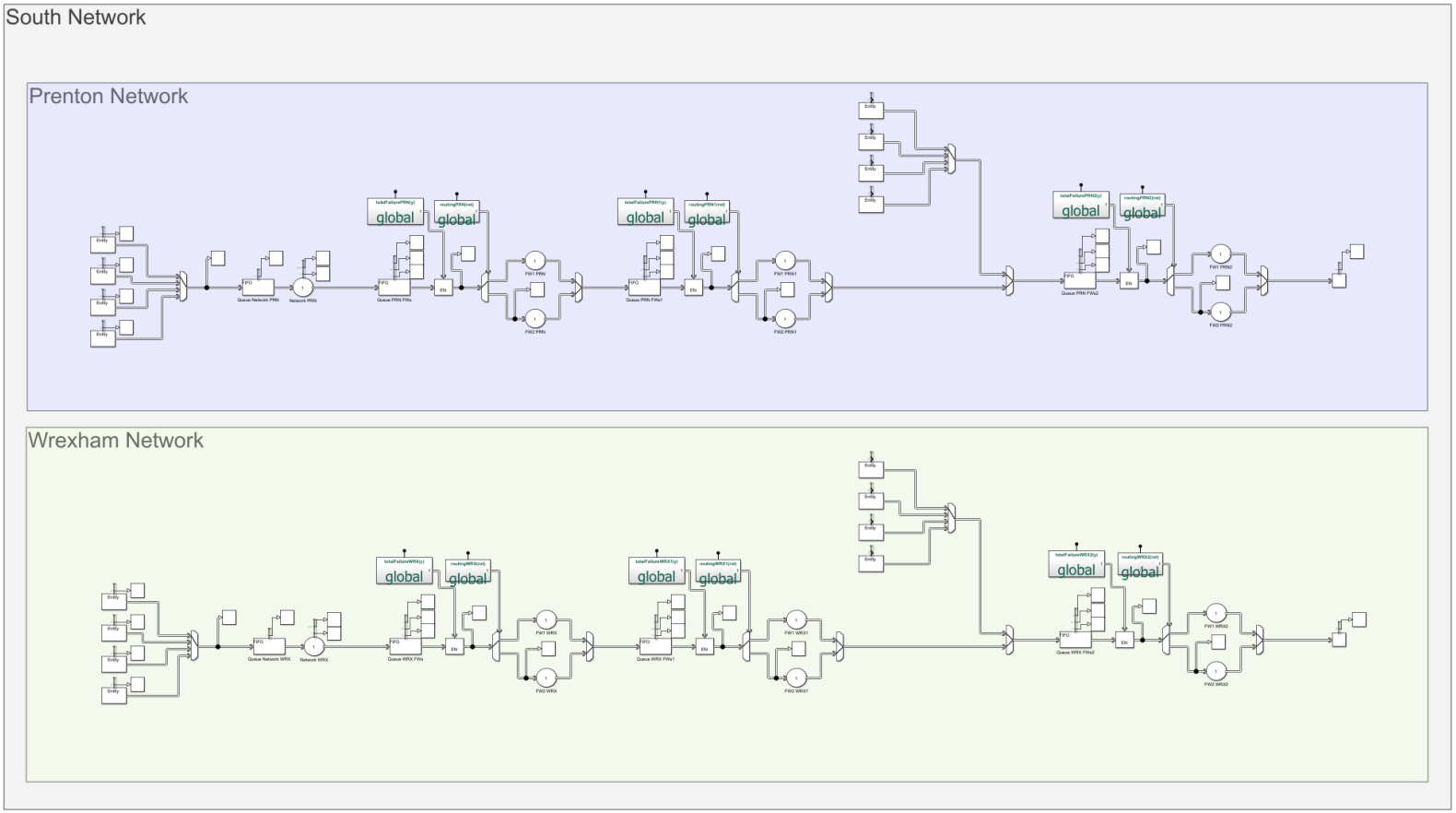


Figure 89: Proposed architecture South Network

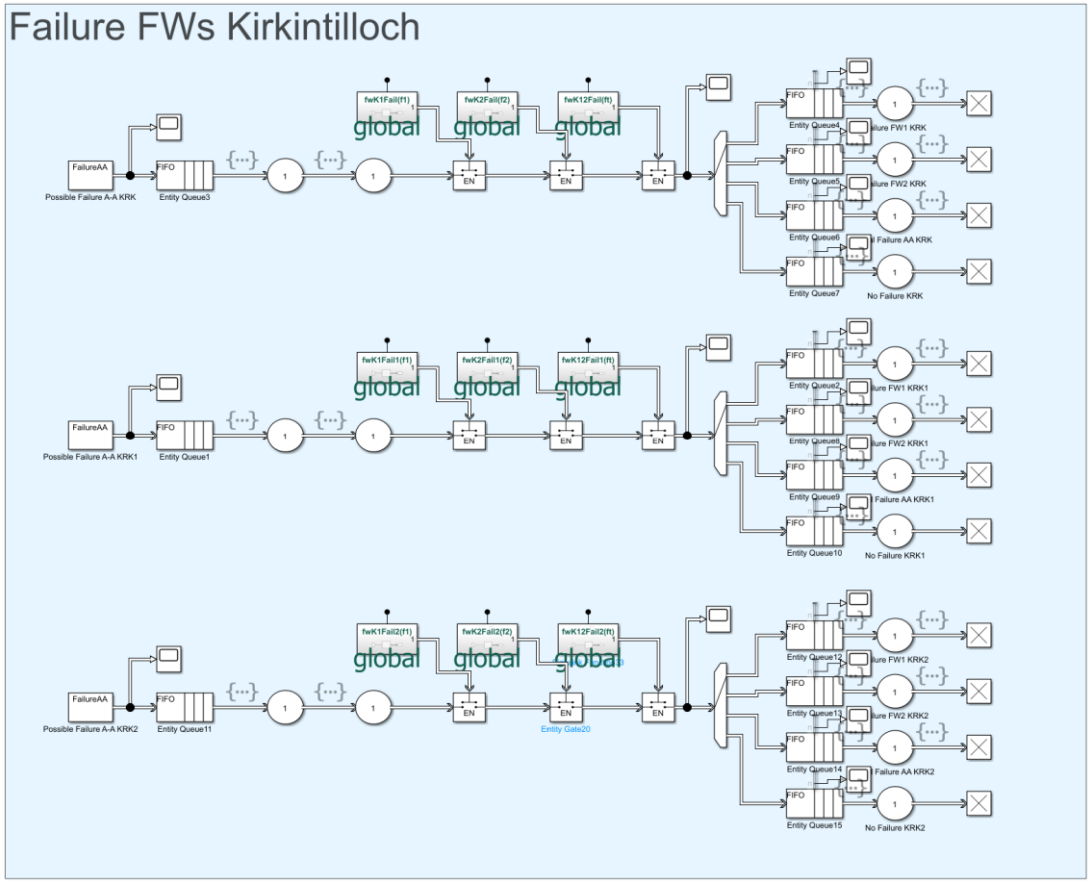


Figure 90: Proposed architecture failure model KRK

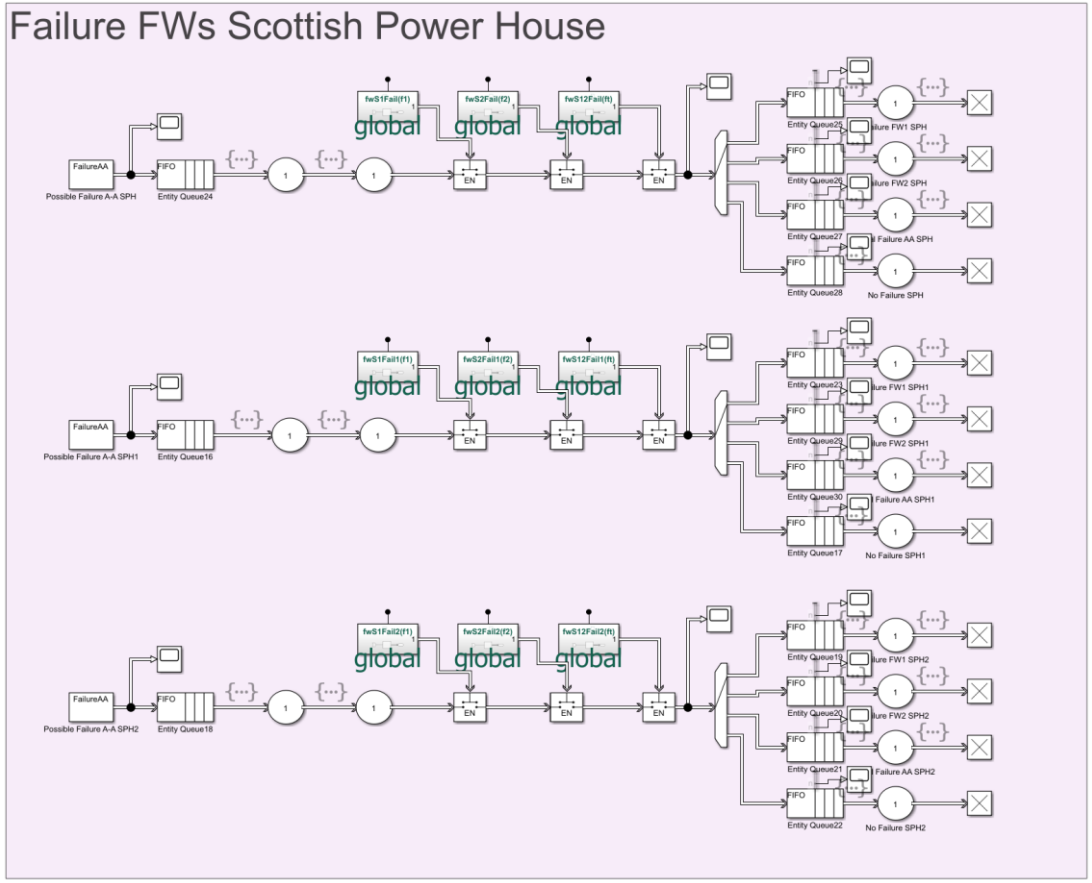


Figure 91: Proposed architecture failure model SPH

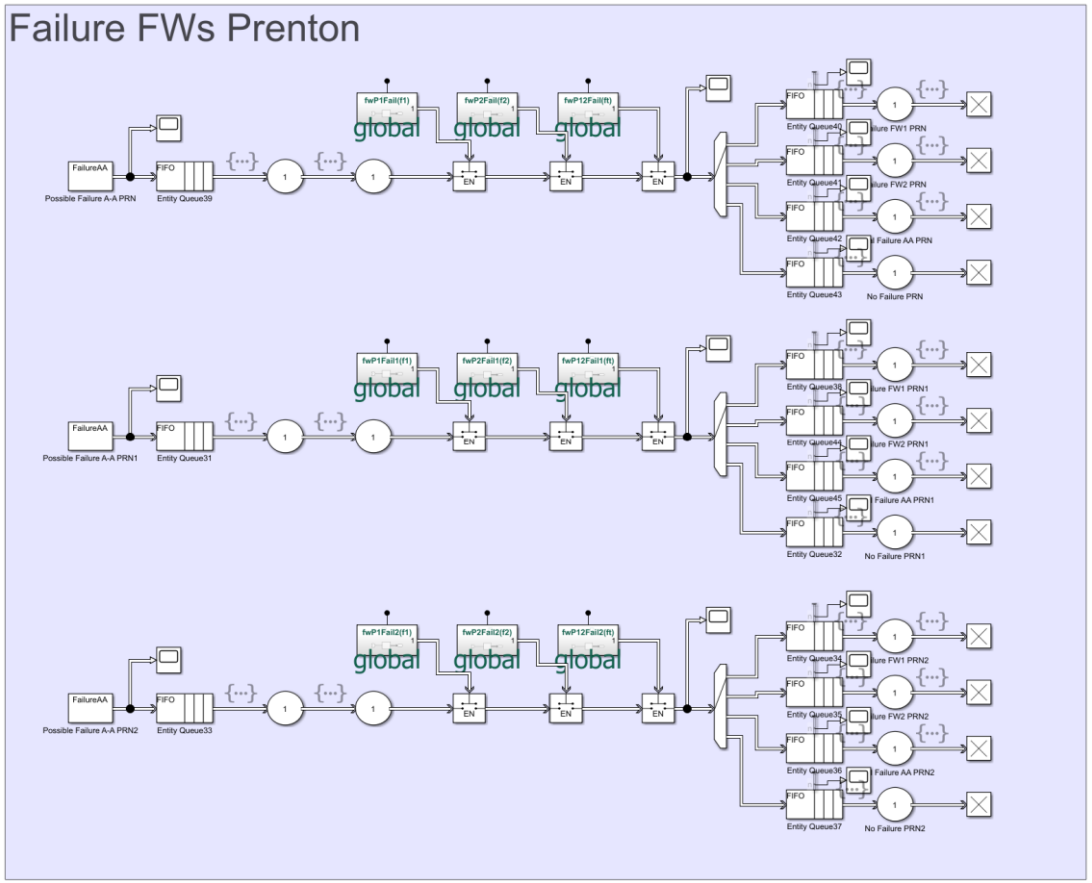


Figure 92: Proposed architecture failure model PRN

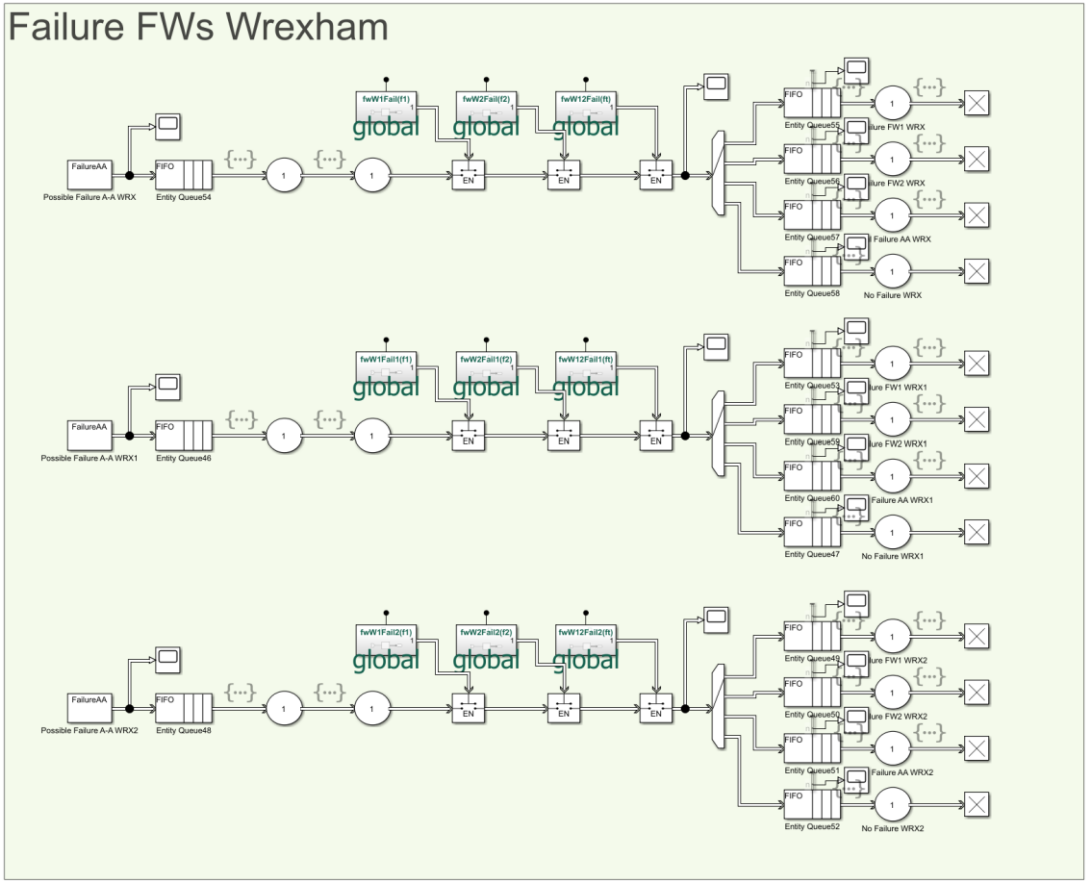


Figure 93: Proposed architecture failure model WRX

ANNEX IV: ACRONYM´S TABLE

Table 22: Meaning of acronyms

Acronym	Meaning
AA	Active-Active
ABR	Area Border Router
ACC	Application Command Centre
ACL	Access Control List
AETs	Advanced Evasion Techniques
AIOps	Artificial Intelligence for IT Operations
AMP	Accelerated Mobile Pages
AP	Active-Passive
ASA	Adaptive Security Appliances
ASIC	Application-Specific Integrated Circuit
AVC	Application Visibility and Control
C2	Command-to-Command
CPU	Central Processing Unit
CSS	Cascading Style Sheets
CT	Current Transformer
DCHP	Dynamic Host Configuration Protocol
DDoS	Distributed Denial-of-Service
DEC	Digital Equipement Corporation
DG	Distributed Generation
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
DPI	Deep packet inspection
DSO	Distribution System Operator
EV	Electric Vehicles
FMC	Firewall Management Center
FTD	Firewall Threat Detection
FW	Firewall
HA	High Availability
HSCI	High Speed Chassis Interconnect
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	The Internet Control Message Protocol

ICT	Information and Communication Technologies
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
IT	Information Technology
KRK	Kirkintilloch
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LSA	Link State Advertisement
LTR	Long-Term Release
ML	Machine Learning
NAT	Network Address Translation
NEBS	Network Equipment Building Standards
NGFW	Next-Generation Firewall
NGIPS	Next Generation Intrusion Prevention System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PA	Palo Alto
PHEV	Plug-in Hybrid Electric Vehicles
PLC	Power-Line Communication
PRN	Prenton
RIP	Routing Information Protocol
RTS	Real Time Systems
SaaS	Software as a Service
SCADA	Supervisory Control And Data Acquisition
SD-WAN	Software-Defined Wide Area Network
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPEN	Scottish Power Energy Networks
SPF	Single Point of Failure
SPH	Scottish Power House
SPU	Standard Product Unit
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSO	Transmission System Operator

UFM	United Threat Management
URL	Uniform Resource Locator
VDB	Virtual Database
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VT	Voltage Transformer
WAF	Web Application Firewall
WAN	Wide Area Network
WRX	Wrexham
xDSL	x Digital Subscriber Line
XLTR	Extra Long-Term Release