Journal of Information and Technology

Implementation and Utilization of Software-Defined Wide Area Network (SD-WAN) Technology Within A Bank: A Case Study of Bank of Kigali

Richard Niyonkuru & Dr. Wilson Musoni

ISSN: 2617-3573

Stratford Peer Reviewed Journals and Book Publishing
Journal of Information and Technology
Volume 8||Issue 1||Page 133-159 ||October||2024|
Email: info@stratfordjournals.org ISSN: 2617-3573

Implementation and Utilization of Software-Defined Wide Area Network (SD-WAN) Technology Within A Bank: A Case Study of Bank of Kigali

Richard Niyonkuru[1] & Dr. Wilson Musoni[2]

[1]Master of Science in Information Technology, University of Kigali, Rwanda

[2]Senior Lecturer, University of Kigali, Rwanda

***How to cite this article*: Niyonkuru R. & Musoni W. (2024). Implementation and Utilization of Software-Defined Wide Area Network (SD-WAN) Technology Within A Bank: A Case Study of Bank of Kigali. *Journal of Information and Technology. Vol* 8(1) pp. 133-159.** https://doi.org/10.53819/81018102t2444

Abstract

The banking industry has undergone a significant transformation in recent years, driven by advancements in technology and the need to meet the evolving demands of customers. One of the key technological innovations in this sector is the adoption of Software-Defined Wide Area Network (SD-WAN) technology. A relatively new networking technique that is quickly gaining acceptance in the enterprise space is called software-defined wide area network, or SD-WAN. Compared to conventional WAN technology, SD-WAN has several benefits, such as increased security, flexibility, and performance. This research study presents a comprehensive case study that explores the implementation and utilization of SD-WAN technology within the Bank of Kigali. It investigates the motivations behind adopting SD-WAN, the benefits of emerging trends in communications and networking technology, such as software-defined wide area networks. The primary goal is to create a virtual environment that simulates both traditional and SDWAN (Software-Defined Wide Area Network) infrastructures in order to conduct a technical comparison at the design and configuration level. The findings confirm that the advantages of SDWAN preserve business continuity, foresee scenarios in which the infrastructure can respond appropriately, maximize connection while upholding security, and offer enhancements in the administration of the entire infrastructure. The researcher will employ a quantitative approach to assess to examines the implementation and utilization of SD-WAN technology within the Bank of Kigali. The case study discusses the bank's motivation for deploying SD-WAN, the specific challenges that it faced, and how SD-WAN has helped to improve its network performance, flexibility, and security. This research study concludes with a discussion of the future of SD-WAN technology and its potential impact on the banking industry.

Key words: *Implementation, Utilization, Software-Defined Wide Area Network Technology, Bank of Kigali, Rwanda*

1. Introduction

In the era of digital transformation, the banking sector has experienced a profound evolution characterized by increased customer expectations, operational complexities, and a heightened focus on data security. Financial institutions everywhere are forced to reassess their conventional infrastructure as a result of these difficulties, particularly with regard to networking technologies. The Software-Defined Wide Area Network is one such revolutionary technology that has attracted a lot of interest (SD-WAN).

The banking sector, which is sometimes referred to as the engine of the economy, is essential to the smooth operation of financial markets, the expansion of the economy, and the financial security of both people and companies. To fulfil this mandate efficiently, banks are continuously seeking ways to enhance their network capabilities, ensuring that they can deliver seamless services to customers, remain resilient to cyber threats, and stay agile in an ever-changing landscape.

SD-WAN technology, a groundbreaking development in networking, offers the potential to address these imperatives. By centralizing control of network functions, simplifying network management, and providing dynamic traffic routing capabilities, SD-WAN technology has emerged as a strategic tool for optimizing network performance, enhancing security, and reducing operational costs. In doing so, it empowers banks to innovate, scale their services, and better meet customer demands, all while maintaining the integrity and confidentiality of sensitive financial data.

Since traditional WAN, also known as Multiprotocol Label Switching (MPLS), has been used for WAN connectivity between several sites, the goal of this study work is to propose SDWAN as a new technological alternative. MPLS is known in the technological field as the most popular communication protocol and used by service providers to connect multiple locations of their customers. It is necessary to emphasize that in Rwanda there are many companies that do not dare to make technological changes or renovations due to a lack of knowledge or rejection of change. Therefore, The advantages of SDWAN technology are the main emphasis of this study. To that end, the deployment-level operational advantages of software-defined network solutions for WAN connectivity are examined.

1.1 Problem statement

Ensuring the security and resilience of networking infrastructure is a crucial aspect of digital transformation in the banking industry. Complex networks are necessary for banks to perform a variety of tasks, such as data management, ATM services, and internet banking. In addition to having to manage large amounts of transactions, these networks also need to be extremely safe in order to fend against increasingly potent cyberattacks. However, the higher security requirements of the digital age are frequently not met by conventional network topologies.

With the introduction of Software-Defined Wide Area Network (SD-WAN) technology, there is a great chance to improve infrastructure modernization and security while also strengthening network security. While SD-WAN provides network managers with flexibility, scalability, and efficiency, its most important benefit for the banking industry is that it may improve security. SD-WAN assists banks in reducing risks and safeguarding sensitive financial data by offering centralised control, encrypted data transmission, and dynamic traffic routing with integrated security policies.

Embracing the digital era head-on, the Bank of Kigali is one of the top financial institutions in Rwanda and has started incorporating SD-WAN technology into its network architecture. But there are difficulties with this project, especially in terms of security. In the banking industry, implementing SD-WAN necessitates making difficult choices about data protection, network architectural security, and regulatory compliance. Careful planning, execution, and ongoing assessment are necessary for this procedure in order to address any vulnerabilities and provide strong defence against cyber threats.

This study aims to tackle two issues, with a focus on security in particular. Its initial goal is to investigate the reasons and forces underlying the Bank of Kigali's use of SD-WAN technology, specifically with regard to security concerns, legal requirements, and consumer confidence. Its second goal is to comprehend the security issues and fixes that arose when SD-WAN technology was implemented in a banking setting. Although SD-WAN technology promises improved security and network optimization, a careful balance between technological innovation, thorough risk management, and preserving a seamless and secure client experience is necessary for its effective integration into a banking environment.

1.2 Research objectives

The goal of this study is to offer a thorough grasp of how Software-Defined Wide Area Network (SD-WAN) technology is implemented and used at the Bank of Kigali**.** Specifically, the study aimed to:

(i) Evaluate SD-WAN improvements in network reliability, resilience against cyber threats, and the overall security of data transmission.

(ii) Analyze how SD-WAN strengthens the bank's security measures, supports compliance with regulatory requirements, and reduces vulnerabilities in network traffic.

(iii) Prioritize the integration of advanced security protocols, threat detection, and response capabilities to safeguard the bank's network infrastructure.

2. Literature Review

An important aspect of SD-WAN is that it functions at three different levels, all of which add to a strong security structure. By creating a logical infrastructure that is layered atop the physical network, the data plane makes it easier to create secure communication across locations and allows for encrypted data transfers between origins. By controlling connected devices' configurations, including enforcing security policies, access controls, and routing information, the control plane plays a critical role in maintaining security. The orchestration plane, on the other hand, provides a framework for business policies and serves as the foundation for the security architecture, guaranteeing that all policies are implemented uniformly throughout the network (Duliński et al., 2020).

The inherent security benefits of SD-WAN become clear when one considers how simple it is to setup and manage connections across a company's branches. In addition to being adaptable and simple to manage, these connections have sophisticated security features like automated threat detection and end-to-end encryption, which help to lower operating risks and expenses over the medium and long terms. Some degree of traffic prioritisation and bandwidth control is provided by traditional WANs; however, SD-WAN improves upon these features by including security into the process, thereby addressing the vulnerabilities and difficulties that are sometimes associated with outdated networks (Troia et al., 2021).

The capacity to administer, control, and configure a company's networks from a single, centralised platform is a major security benefit of SD-WAN. The dangers associated with manual setups and delayed security patches are reduced by this centralisation, which makes it easier to provide security updates and alterations instantly throughout the network. Real-time

https://doi.org/10.53819/81018102t2444

security monitoring and response are made possible by the platform's unified view of crucial characteristics, which include interface data consumption, link latencies, IP bandwidth usage, and available bandwidth. On the other hand, manual device settings are usually necessary for traditional WANs, which can be time-consuming, prone to human mistake, and potentially expose the network during updates (Perez et al., 2021).

Additionally, based on pre-established security regulations, SD-WAN platforms have the ability to distinguish and prioritise different types of traffic, including voice, data, video, and management traffic. To protect the integrity of network management activities, for example, prioritising management traffic makes sure that communications relevant to security remain high on the list of priorities.

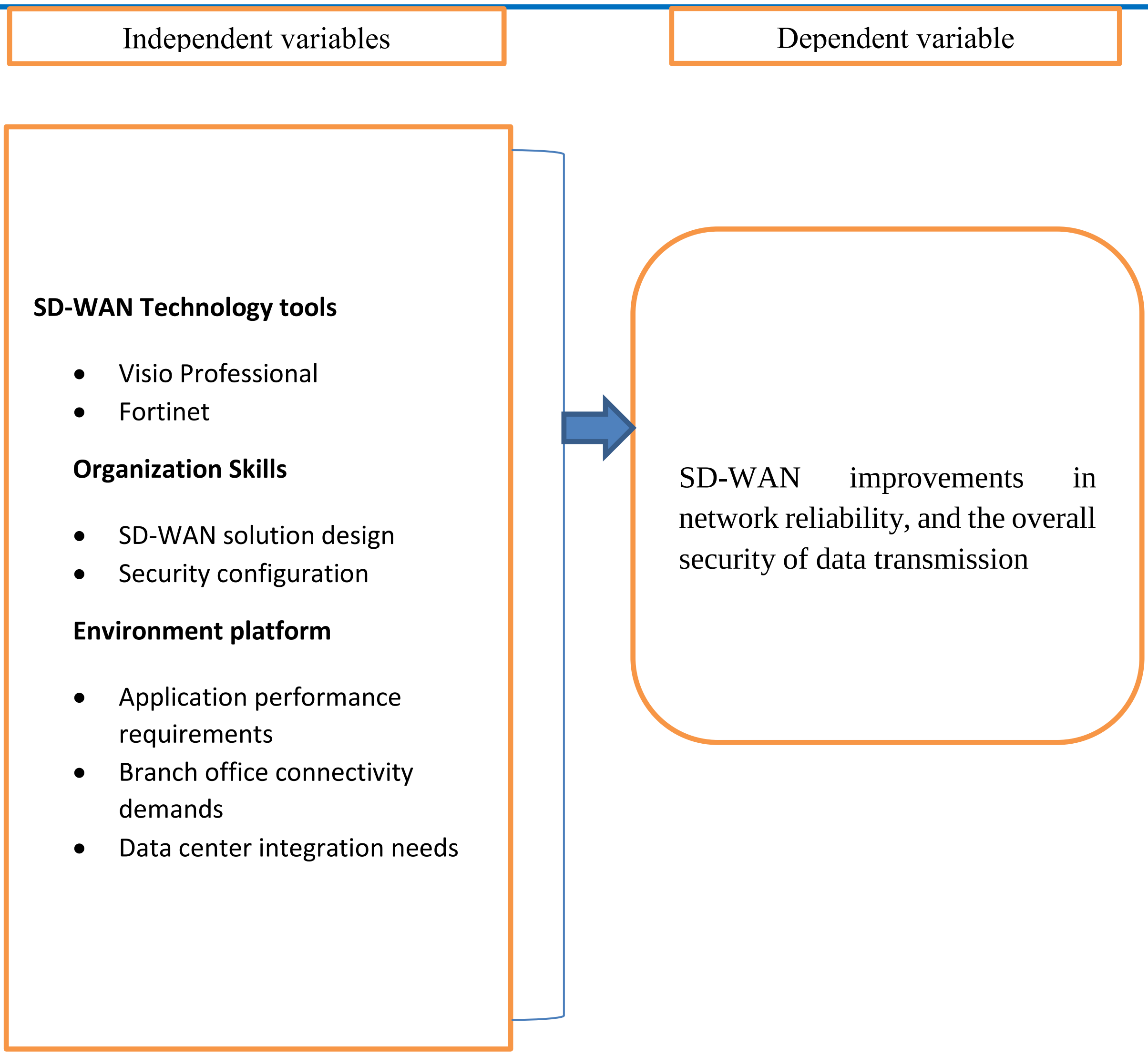
Empirical research has confirmed, via simulations and real-world deployments, the security advantages of SD-WAN. One study, for instance, deployed an SD-WAN network virtually in order to assess its efficacy in comparison to more conventional networks. The results showed that traffic prioritisation strategies for SD-WAN may be set up to provide high-quality service levels with little CPU load while improving security via dynamic routing and constant monitoring.

Two network scenarios—one utilising manual routing policies and standard IP/MPLS and the other utilising SD-WAN technology—were compared. The SD-WAN scenario demonstrated better security performance by dynamically routing traffic based on the state of the network and automatically modifying to ensure safe, low-latency communication. This was made possible by its centralised control and real-time topology awareness.

Another study looked at how to integrate more modules into the SD-WAN controller to optimise traffic routing while taking security concerns into account. Load balancing and improved security management over many links are made possible by SD-WAN's ability to function with numerous connection lines, guaranteeing that network traffic is handled effectively and safely (Ellawindy & Heydari, 2019).

2.1 Conceptual Framework

The main players, elements, deployment procedure, application, advantages, and difficulties related to deploying SD-WAN technology at Bank of Kigali are depicted graphically in this diagram.



Independent variables

Dependent variable

SD-WAN Technology tools

- Visio Professional
- Fortinet

Organization Skills

- SD-WAN solution design
- Security configuration

Environment platform

- Application performance requirements
- Branch office connectivity demands
- Data center integration needs

SD-WAN improvements in network reliability, and the overall security of data transmission

***Figure 1*: Conceptual framework**
Source: Researcher

3. Research methodology

The research design is a crucial component of this study as it outlines the structure, approach, and methodology used to investigate the implementation and utilization of Software-Defined Wide Area Network (SD-WAN) technology within the Bank of Kigali. To achieve the research objectives and answer the research questions effectively, a mixed-methods approach, combining both qualitative and quantitative research techniques, will be employed.

3.1 Qualitative research

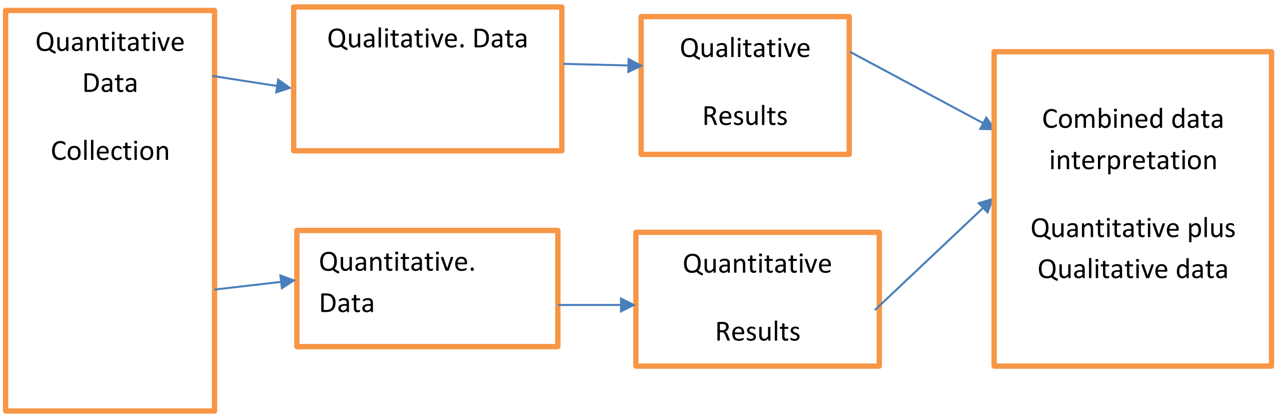
For a deeper comprehension of the reasons behind, difficulties encountered, advantages, and lessons discovered from the Bank of Kigali's SD-WAN adoption, qualitative research approaches are required. Qualitative study will be carried out using: Semi-structured Interviews: Key Bank of Kigali stakeholders will be the subject of in-depth interviews.

3.2 Quantitative Research

Quantitative measurements and evaluations will supplement the qualitative data obtained through quantitative research methodologies. Research with numbers will entail: Surveys: An organised questionnaire will be created and distributed to a subset of workers, comprising IT and network personnel. The purpose of the study is to measure the perceived advantages of using SD-WAN, such as enhanced network performance, cost effectiveness, and security.

3.3 Research Design

The Bank of Kigali's SD-WAN installation may be fully understood thanks to the integration of qualitative and quantitative research approaches. While the quantitative data will offer statistical insights and the capacity to generalise conclusions to a wider audience, the qualitative data will offer rich context and in-depth storytelling.


Quantitative Data Collection
Qualitative. Data
Qualitative Results
Quantitative. Data
Quantitative Results
Combined data interpretation
Quantitative plus Qualitative data

3.4 Study Population

The population, or 64 branches of Bank of Kigali, will serve as the basis for the study. Due to their crucial role in the deployment of SD-WAN, CIO/ICT Managers, Network Architects, Network & Support Engineers, and Security Engineers will be selected. The target demographic for this study consisted of decision-makers involved in the SD-WAN installation as well as network managers and administrators. These interviews will provide light on the reasons for the deployment of SD-WAN, the difficulties encountered, and the solutions used to overcome those difficulties.

3.5 Sample procedure and techniques

The population selected was 64 branches of Bank of Kigali was guided by the Krejcie and Morgan sample size formula since the population is known. The sample size was then multiplied with the selected decision makers from each organization of 5 individuals per organization.

https://doi.org/10.53819/81018102t2444

Population size known

$$SS = \frac{X^2NP(1-P)}{d^2(N-1) + X^2P\ (1-P)}$$

Figure 2: Sample Size Formulae (Krejcie and Morgan, 1970)
SS = required sample size.
X2 = the table value of chi-square for 1 degree of freedom at the desired confidence level (3.841).
N = the population size.
P = the population proportion (assumed to be .50 since this would provide the maximum sample size).
d = the degree of accuracy expressed as a proportion (.05). We therefore calculate the sample size of the known population; We therefore calculate the sample size of the known population;

$$SS = \frac{(3.841) * 69 * (0.5) * (1-0.5)}{0.0025 * (69-1) + (3.841) * 0.5\ (1-0.5)}$$

$$SS = 66.5 / (0.17 + 0.96025) = 58.8$$

Therefore, our sample size is at least 59 branches of Bank of Kigali will be used multiplying this number with the purposive sample population of 6 per Branch will provide us with at least 354 (59*6) responded required for the study.

Category	Target per Branch	Population	Sample Size
Network Manager	1	250	59
Network Administrators	2	500	118
Network Support	1	250	59
Security Engineers	2	500	118
Total	**6**	**1500**	**354**

Table 1: Respondents

3.6 Data Collection

Determining the adoption of SD-WAN was the study's goal. The following information is vital to the study. A questionnaire will be used to gather this data. Online survey technologies will be used to deliver these surveys. A few of the most important information to be gathered is how the organization's members view the adoption of SD-WAN, their level of familiarity with the technology, their role on the ICT team, any reservations they may have about it, and how they see the advantages of SD-WAN for the company. The questionnaire will consist of ranking and multiple choice questions arranged in the categories below.

Section 1: Software-defined wide area networks based on information.

Section 2: This section will provide participant characteristics, including demographics and the history of the company. The participants' understanding of software-defined wide area networks and its importance to their organisation will also be covered.

Section 3: This section will discuss how the participants see the adoption of software-defined wide area networks (SD-WAN) and what obstacles they anticipate.

3.7 Data Analysis

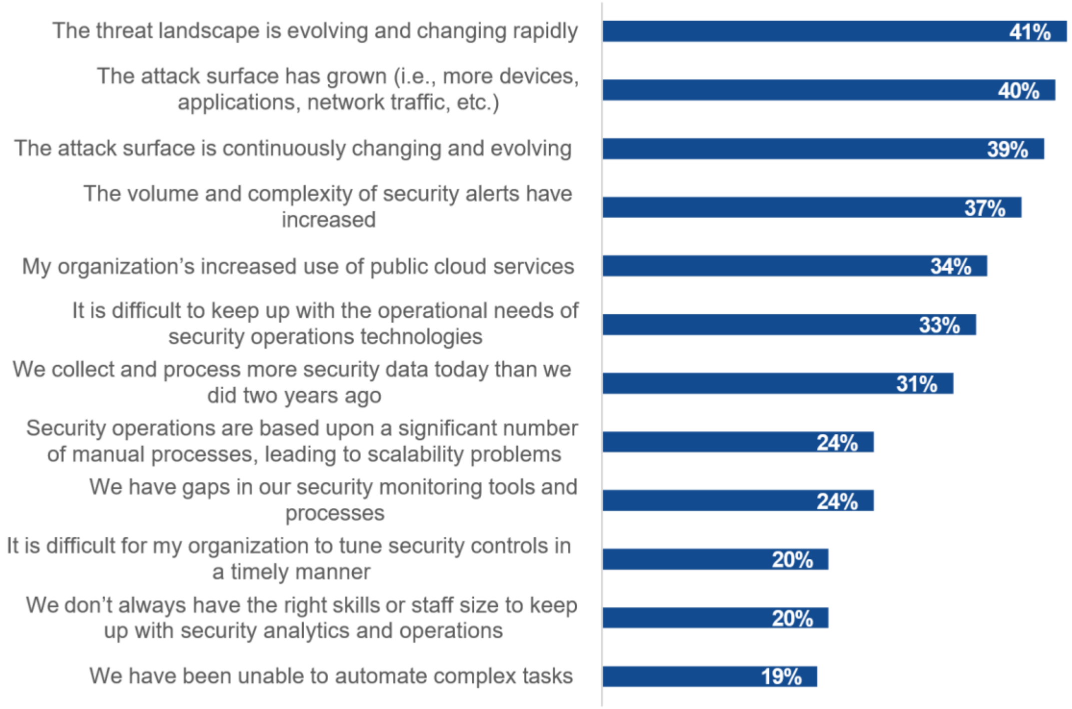
Data analysis will involve several stages. First, the data collected form the questionnaires were edited to make sure there is completeness and consistency in the data collected. The questioner was checked for clarity, how eligible they are, their relevance and how appropriate the feedback will be. The second phase was coding and processing of the data using excel and SPSS analysis software, then the output of the findings will be represented using graphs and charts.

4. Findings

4.1 Top Reasons Security Operations Are More Difficult Than They Were 2 Years Ago?

As Bank of Kigali grow and new technologies emerge, the result is a rapidly expanding attack surface, with more threats being created from more sources and across more devices than ever before. Employees are working from more places and using more devices, while companies are integrating IT services with customers and suppliers and shifting toward using more cloud technologies. This places even more pressure on security teams to keep up, and attackers are constantly evolving and trying to stay one step in front of existing security methods and tools.

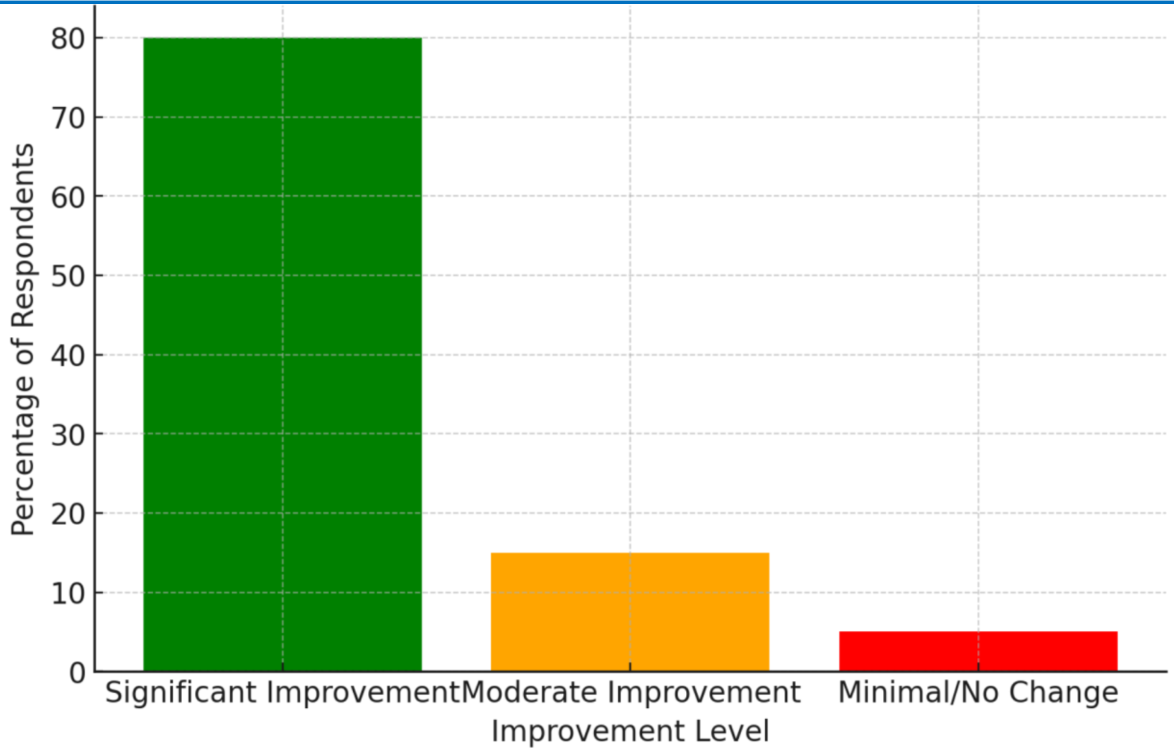
Attackers have access to their own supply chain of shared information and products and are made more effective by using services provided by more experienced cybercriminals such as malware-as-a-service (MaaS) and ransomware-as-a-service (RaaS). They also have access to distributed attacks (such as distributed denial of services or DDoS attacks) and are able to coordinate attacks with other individuals into campaigns that are much harder to detect and prevent against (it is not enough to simply block an IP or particular geography). This can lead to a steep learning curve for SOC teams and makes it difficult to stay ahead of the latest threats. The result is that Bank of Kigali without colossal budgets required to build and operate an effective SOC are slow to identify and remediate potential attacks.



4.2 To what extent has SD-WAN improved network performance across branches?

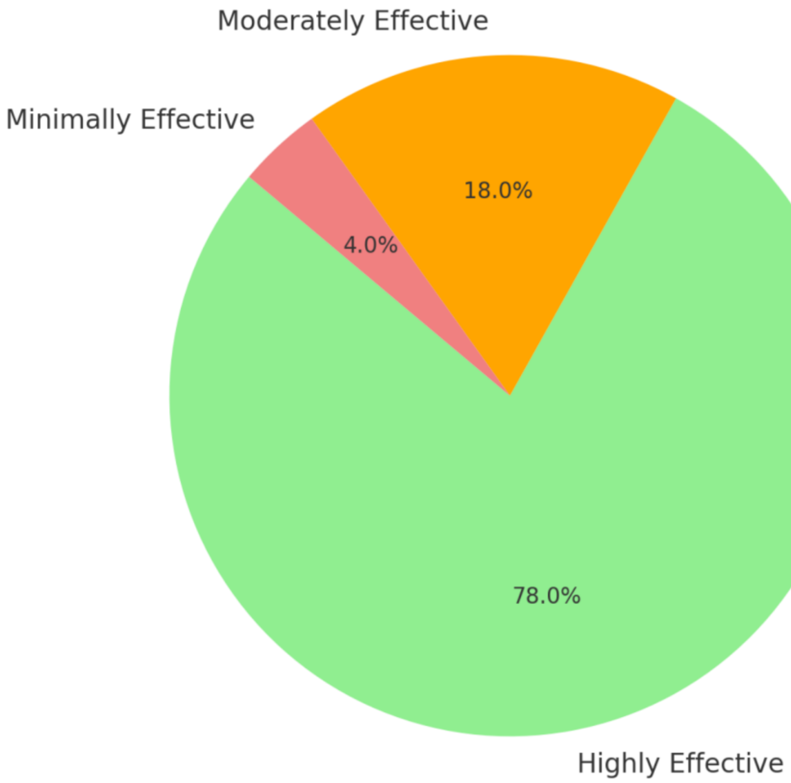
The adoption of Fortinet's SD-WAN at Bank of Kigali resulted in significant improvements in network agility and performance. Fortinet's Secure SD-WAN enabled faster deployment of networking solutions across multiple branches of Bank of Kigali. The use of FortiGate devices in each branch allowed seamless control of network traffic and reduced operational complexity. Fortinet's SD-WAN dynamically adjusted bandwidth allocation based on real-time traffic demand. The bank reported enhanced application performance, particularly for mission-critical services such as core banking and transaction processing. The implementation of FortiGate appliances also reduced latency across the bank's branches by optimizing traffic routing between headquarters and branch offices, ensuring a consistent and efficient experience for both employees and customers. 80% of respondents indicated significant improvement in network agility and performance. 15% reported moderate improvements. 5% saw minimal or no changes.

https://doi.org/10.53819/81018102t2444



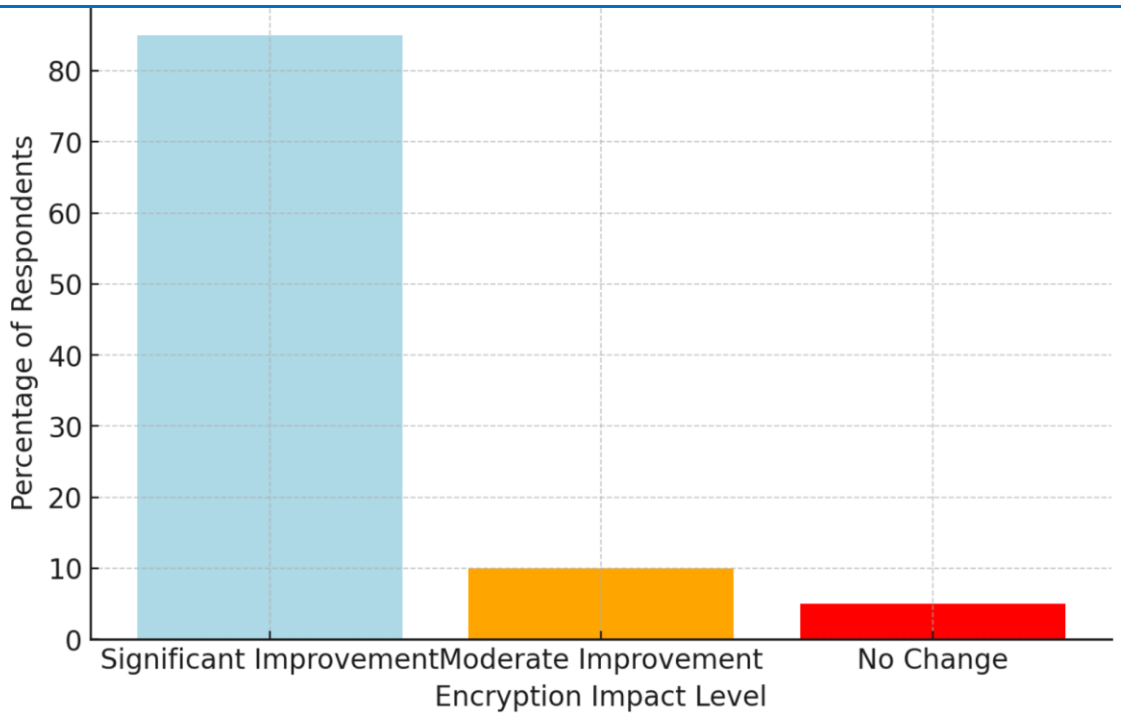
4.3 How effective is the centralized security management provided by Fortinet SD-WAN?

One of the major advantages Bank of Kigali experienced with Fortinet's SD-WAN was improved centralization of security policies. The use of FortiManager allowed Bank of Kigali's IT team to manage security policies from a single, centralized platform. This simplified the process of enforcing security rules and configurations across all branches. Through FortiAnalyzer, the bank monitored network traffic and security incidents in real-time. This centralized log management provided detailed visibility into network activities, enabling the bank to detect anomalies and take corrective measures. According to the respondents, 78% found it highly effective, 18% considered it moderately effective, while 4% rated it minimally effective



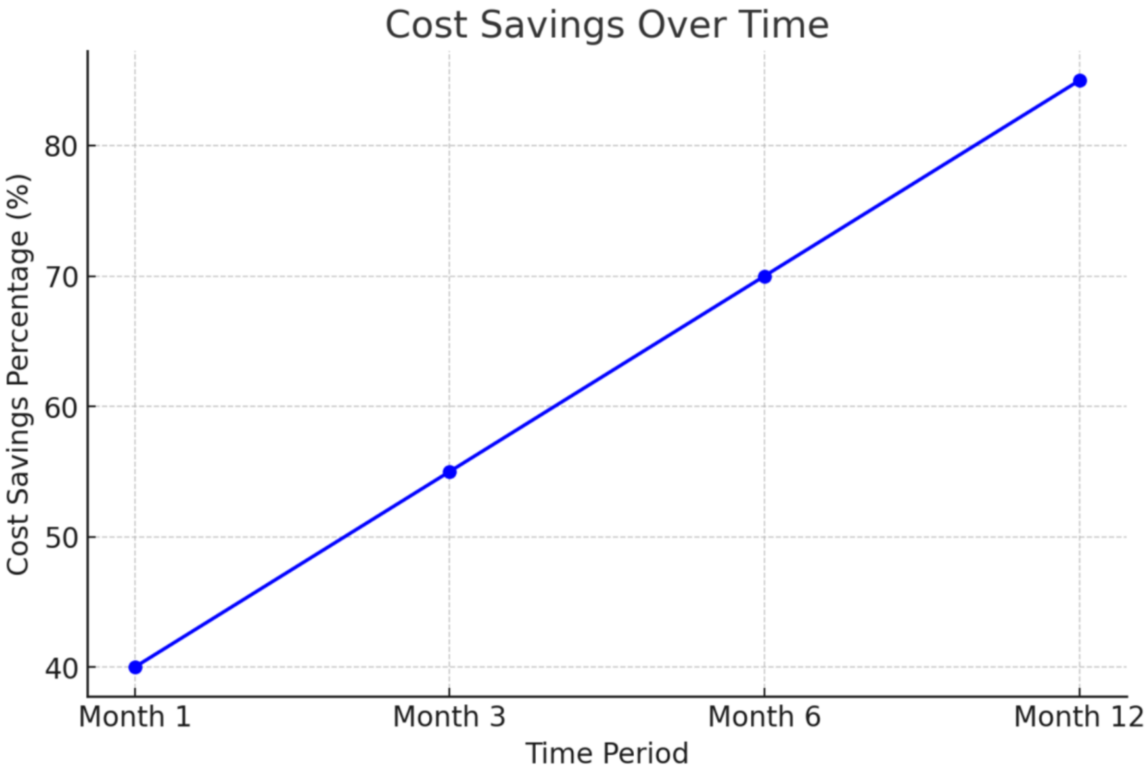
4.4 What impact has end-to-end encryption had on data security?

Data security was a key concern for Bank of Kigali, and Fortinet's SD-WAN solution provided robust encryption mechanisms. All data transferred across Bank of Kigali's network was encrypted using IPsec VPN tunnels provided by FortiGate devices. This ensured secure communication between branches and the central data center, protecting sensitive customer and financial data from interception. The bank segmented its network to isolate critical systems such as core banking and payment gateways from less critical operations. This segmentation was supported by Fortinet's built-in security features, which reduced the attack surface for cyber threats. According to the respondents, 85% reported significant improvements, 10% noticed moderate improvements, and 5% saw no change after implementing encryption with Fortinet's SD-WAN solution.



4.5 Has the implementation of Fortinet SD-WAN led to cost savings in IT infrastructure?

Cost savings were a significant finding of this case study, as Bank of Kigali managed to optimize its operational expenses through the Fortinet SD-WAN solution. One of the biggest cost-saving measures was reducing reliance on expensive MPLS circuits by leveraging broadband connections for non-critical traffic. Fortinet’s SD-WAN allowed the bank to create a hybrid model, where critical banking transactions continued over MPLS, and less-sensitive data was routed over broadband. By consolidating security and networking functions within FortiGate appliances, Bank of Kigali reduced the need for multiple hardware solutions, thereby decreasing both operational and hardware expenses. 70% of respondents reported substantial cost savings, 25% noticed moderate cost savings, 5% indicated minimal or no cost savings.



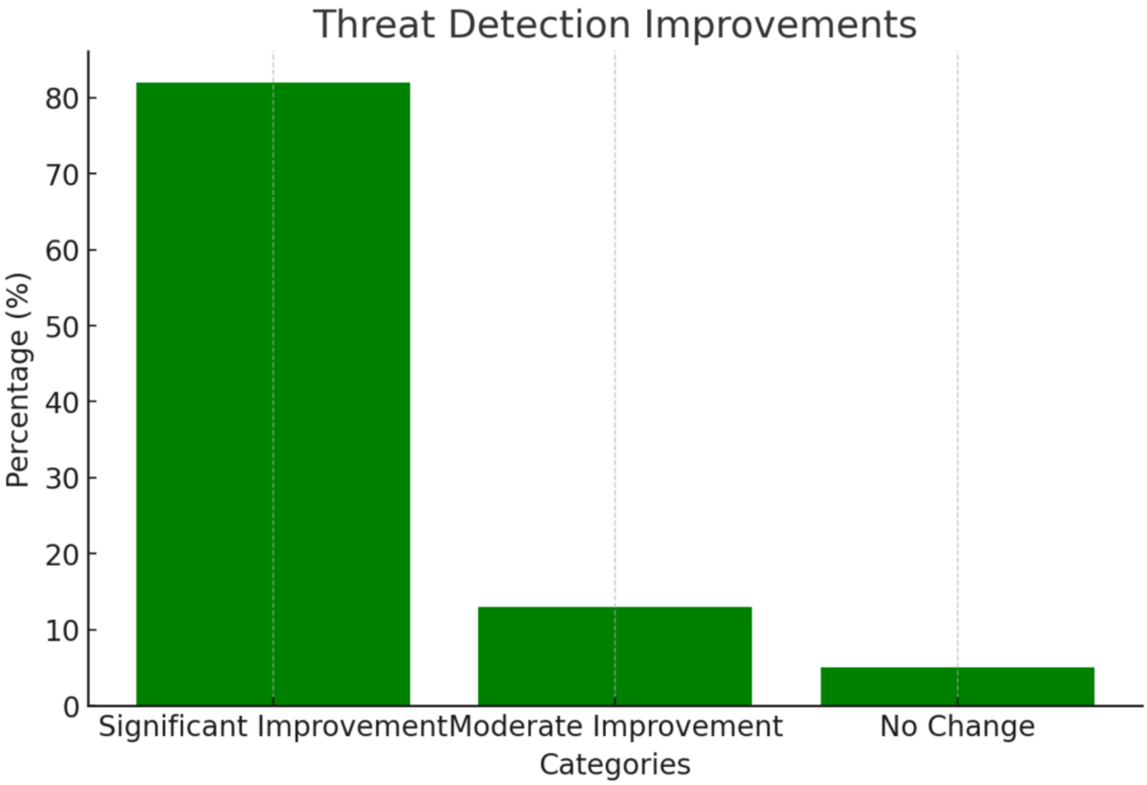
4.6 How has SD-WAN improved the bank's ability to detect and respond to threats?

Fortinet's SD-WAN integrated threat detection and response features significantly strengthened the bank's cybersecurity posture.

Fortinet's solution allowed seamless integration with the bank's Security Information and Event Management (SIEM) systems. This enabled comprehensive threat monitoring across all branches. Bank of Kigali leveraged FortiAnalyzer for real-time threat detection, which helped identify and mitigate security incidents before they could escalate.

The bank benefitted from Fortinet's automated threat response capabilities, which included the ability of FortiGate devices to block malicious traffic and update security policies automatically when threats were detected. 82% of respondents reported significant improvements in threat detection capabilities, 13% observed moderate improvements, 5% saw no significant change.

https://doi.org/10.53819/81018102t2444

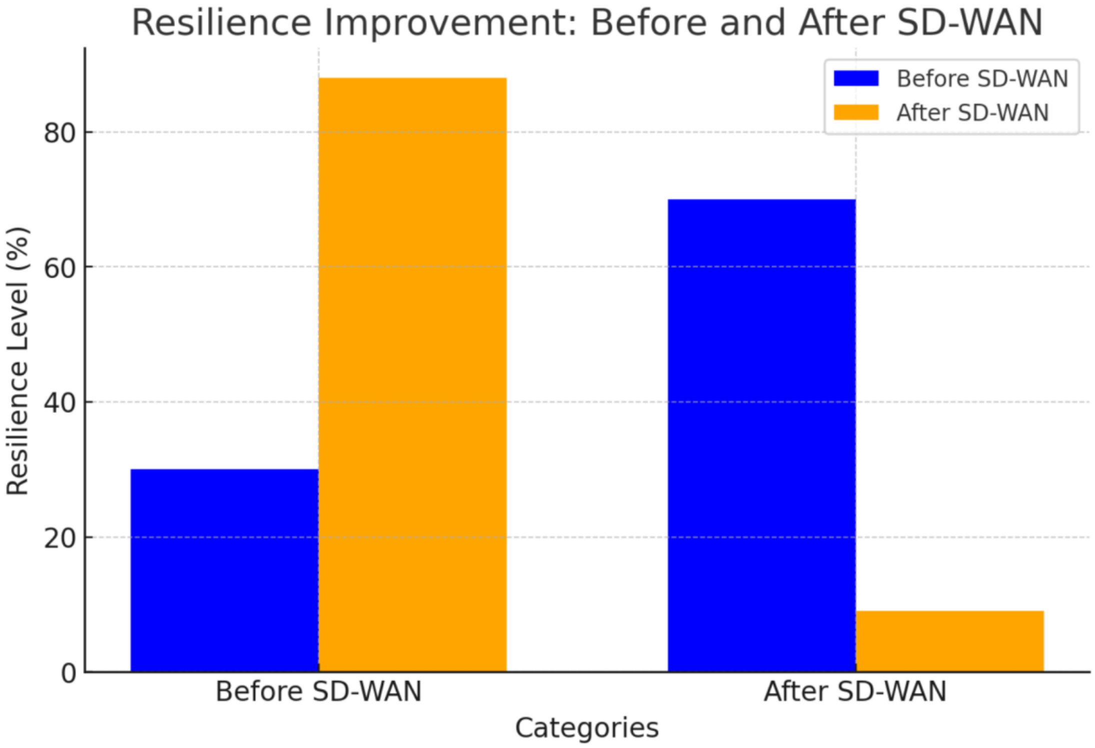


4.7 Has SD-WAN increased the resilience of the bank's network during outages?

Another critical finding was the increased network resilience and business continuity achieved through Fortinet's SD-WAN.

Bank of Kigali implemented multiple failover paths using Fortinet's SD-WAN, ensuring that the network remained operational even during outages or link failures. FortiGate devices automatically rerouted traffic when primary links were unavailable, minimizing disruptions to banking services.

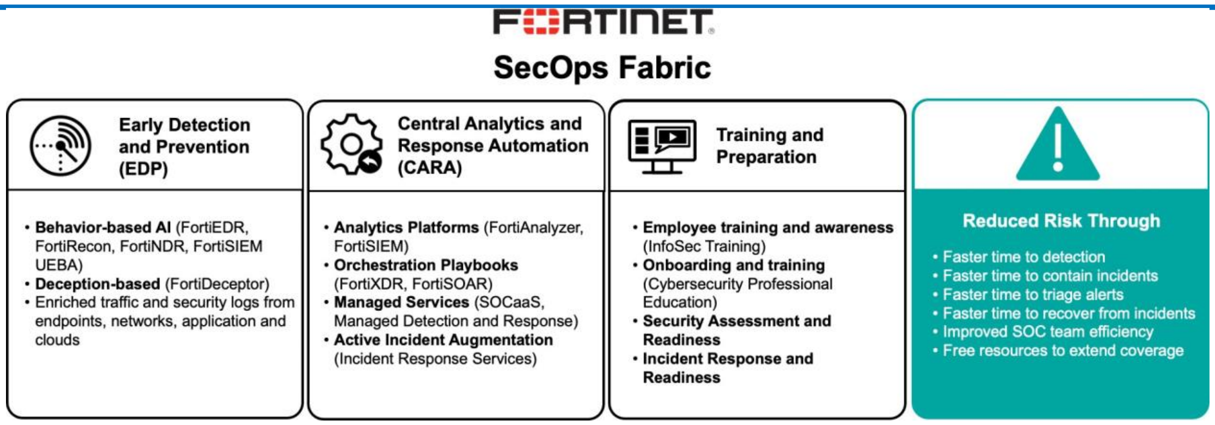
Fortinet's solution also improved Bank of Kigali's disaster recovery capabilities. With centralized control and automated network reconfiguration, the bank could recover more quickly in case of a network failure or breach 88% of respondents agreed that SD-WAN improved resilience, 9% indicated moderate improvements, 3% did not observe significant changes.



4.8 Fortinet Security Operations Solutions

Fortinet Security Operations solutions provide real-time threat detection and response capabilities to protect Bank of Kigali against cyberattacks. They are delivered by an integrated SecOps Fabric made up of components that combine threat intelligence, advanced analytics, and automation to help security teams quickly identify and respond to threats. The SecOps Fabric uses machine learning and artificial intelligence (AI) algorithms to analyze massive amounts of data from multiple sources, including network traffic, endpoints, applications, and more. It also leverages threat intelligence from the global network of Fortinet sensors and security operations centers to stay up to date on the latest threats, as well as active threats, and provides security teams with a single pane of glass for visibility and management of security incidents. It uses a closed-loop approach to automate the incident response process, from detection to containment and remediation. This enables security teams to respond quickly and efficiently to threats, reducing the time it takes to detect and mitigate attacks.

Fortinet offers expert security services to support in-house security resources and integrates with the broader Fortinet security portfolio, including firewalls, intrusion prevention systems, and additional endpoint protection solutions. This enables Bank of Kigali to provide effective and comprehensive protection across the entire attack surface and helps them stay ahead of today's advanced threats and protect their sensitive data and digital assets.



FORTINET

SecOps Fabric

Early Detection and Prevention (EDP)

- **Behavior-based AI** (FortiEDR, FortiRecon, FortiNDR, FortiSIEM UEBA)
- **Deception-based** (FortiDeceptor)
- Enriched traffic and security logs from endpoints, networks, application and clouds

Central Analytics and Response Automation (CARA)

- **Analytics Platforms** (FortiAnalyzer, FortiSIEM)
- **Orchestration Playbooks** (FortiXDR, FortiSOAR)
- **Managed Services** (SOCaaS, Managed Detection and Response)
- **Active Incident Augmentation** (Incident Response Services)

Training and Preparation

- **Employee training and awareness** (InfoSec Training)
- **Onboarding and training** (Cybersecurity Professional Education)
- **Security Assessment and Readiness**
- **Incident Response and Readiness**

Reduced Risk Through

- Faster time to detection
- Faster time to contain incidents
- Faster time to triage alerts
- Faster time to recover from incidents
- Improved SOC team efficiency
- Free resources to extend coverage

Figure 8. Fortinet Security Operations Solutions

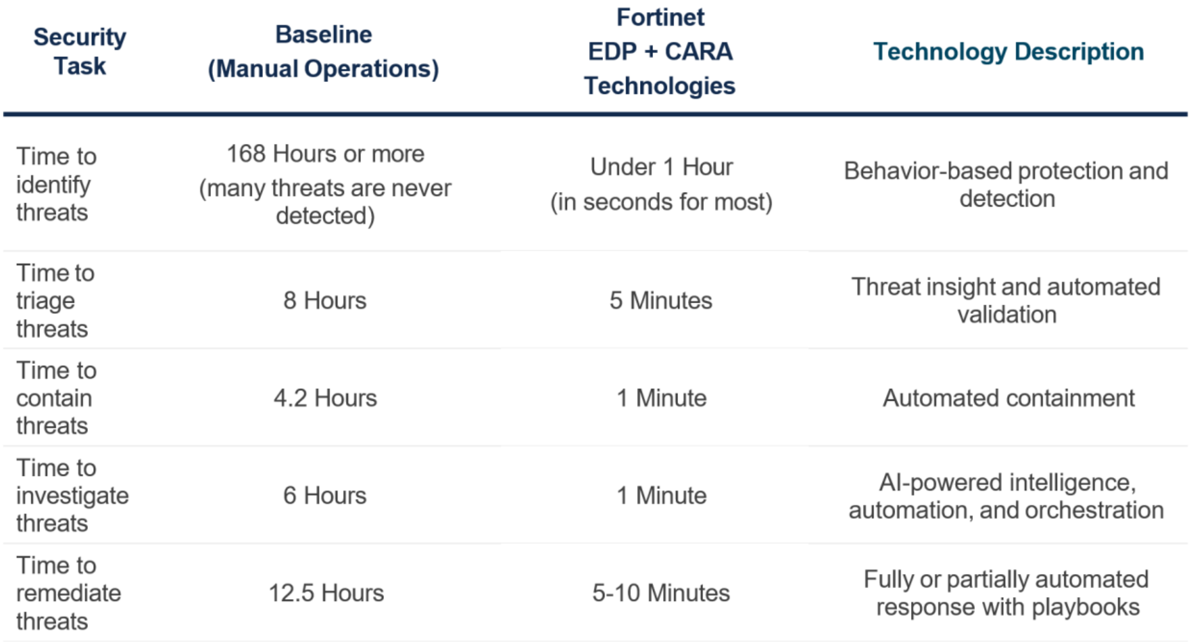
The SecOps Fabric provides the people, technology, and proven processes to reduce cyber-risk for Bank of Kigali across three pillars:

Early Detection Prevention (EDR) – Fortinet provides effective detection and prevention by deploying technologies such as endpoint detection and response (EDR), network detection and response (NDR), user and entity behavior analytics, digital risk protection service, Sandbox, and deception networks. These technologies monitor real-time behaviors and activity, detect anomalies (often using AI), and alert on automated/human attacks as well as external threats, creating an active defense layer. They also integrate with other security tools to automate an effective response, helping to minimize mean time to detection (MTTD) and mean time to response (MTTR).

Central analytics and response automation (CARA) – FortiSIEM provides a comprehensive multivendor visibility, analytics, and incident management solution, while FortiAnalyzer provides a visibility, analytics, and incident response component dedicated to the Fortinet Security Fabric. FortiXDR provides a number of security tools that help small and growing security teams detect and automate response to threats, and

FortiSOAR provides flexible and powerful orchestration and automation for established SOC teams. In addition, Fortinet Managed Detection and Response (MDR) and SOCaaS can offload security team functions, helping Bank of Kigali with limited resources deliver higher levels of security and offload resources from established SOC teams to focus on other tasks.

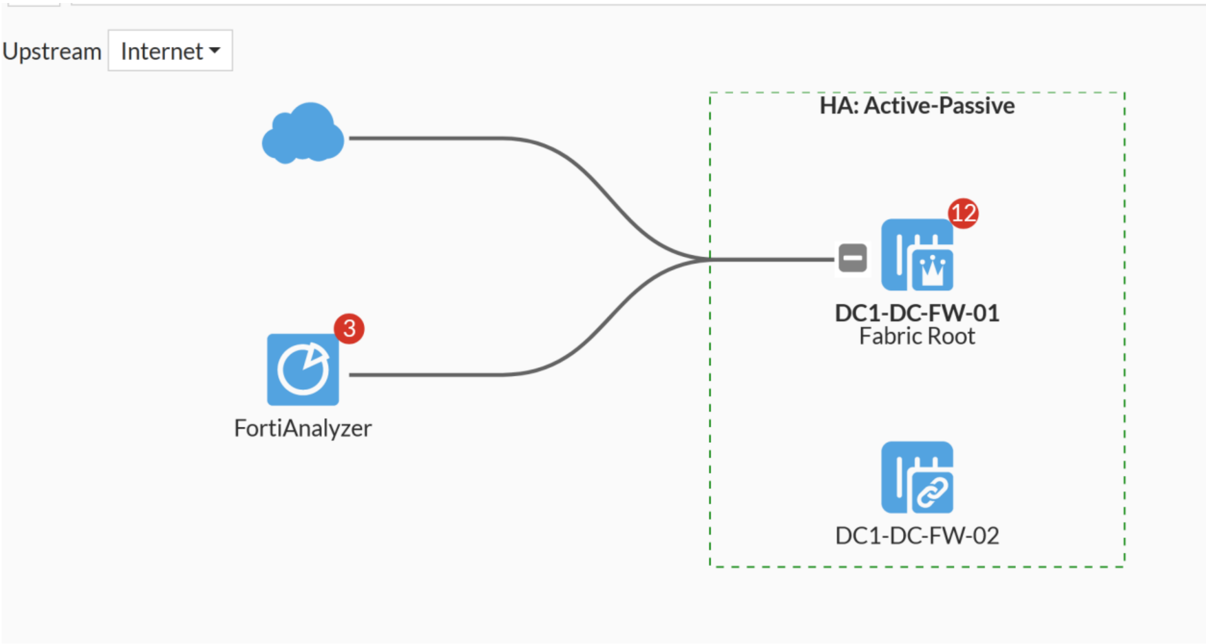
Training and preparation – Providing assessments, training, and visibility helps make Bank of Kigali’ employees and business units more aware of potential cyber threats, with actionable readiness plans that help guarantee immediate and effective responses to contain or prevent potential damage when needed. Technical training helps accelerate onboarding and ramping up of expertise for all security resources.



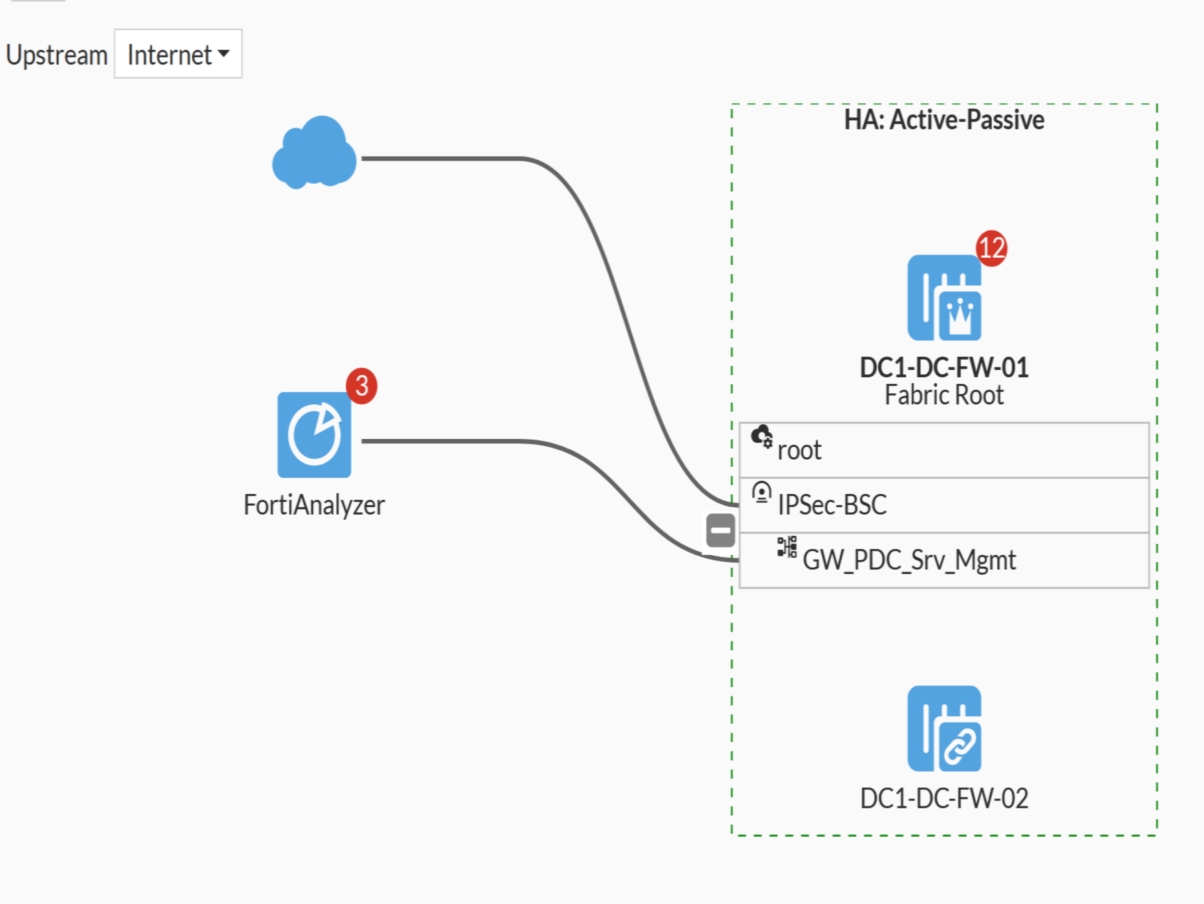
Security Task	Baseline (Manual Operations)	Fortinet EDP + CARA Technologies	Technology Description
Time to identify threats	168 Hours or more (many threats are never detected)	Under 1 Hour (in seconds for most)	Behavior-based protection and detection
Time to triage threats	8 Hours	5 Minutes	Threat insight and automated validation
Time to contain threats	4.2 Hours	1 Minute	Automated containment
Time to investigate threats	6 Hours	1 Minute	AI-powered intelligence, automation, and orchestration
Time to remediate threats	12.5 Hours	5-10 Minutes	Fully or partially automated response with playbooks

Table 5 Combined improvements of using both Fortinet EDP and CARA technologies.

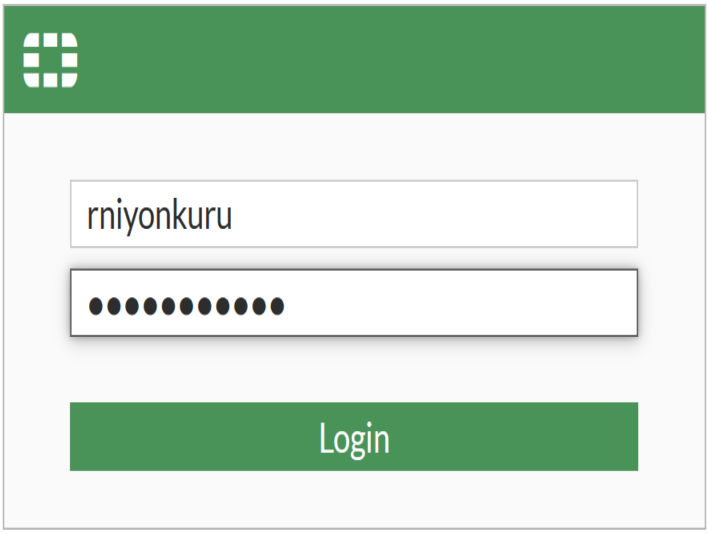
4.9 Physical Topology



4.10 Physical Topology



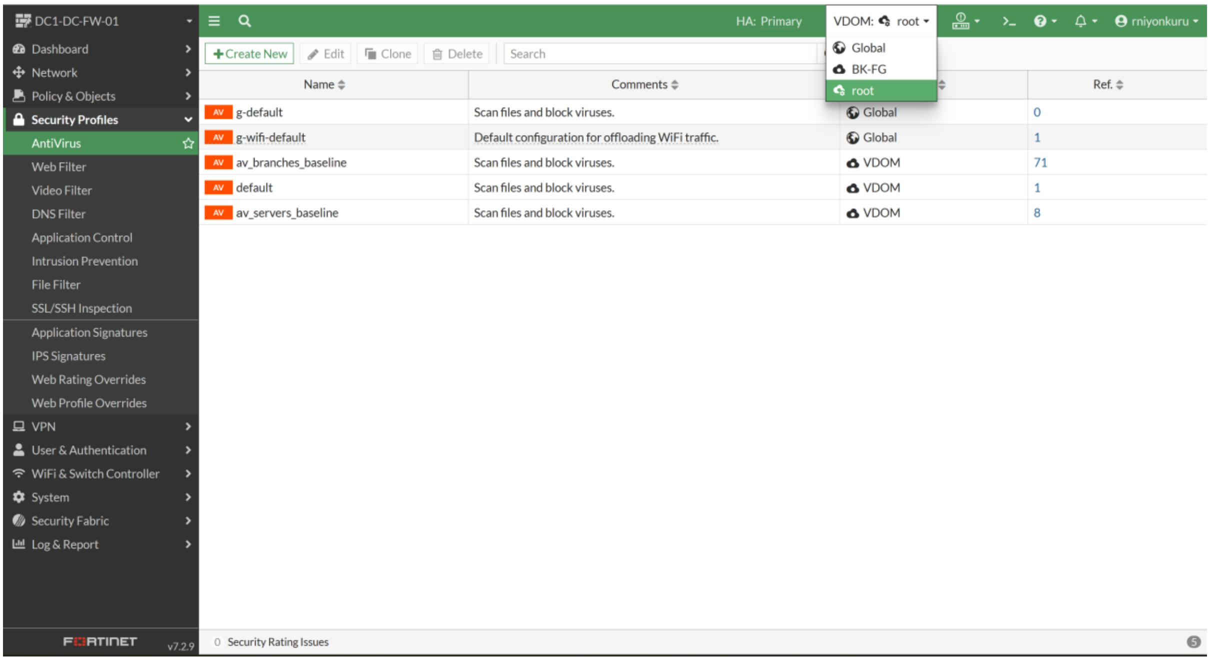
4.11 Fortinet Administration Login



rniyonkuru

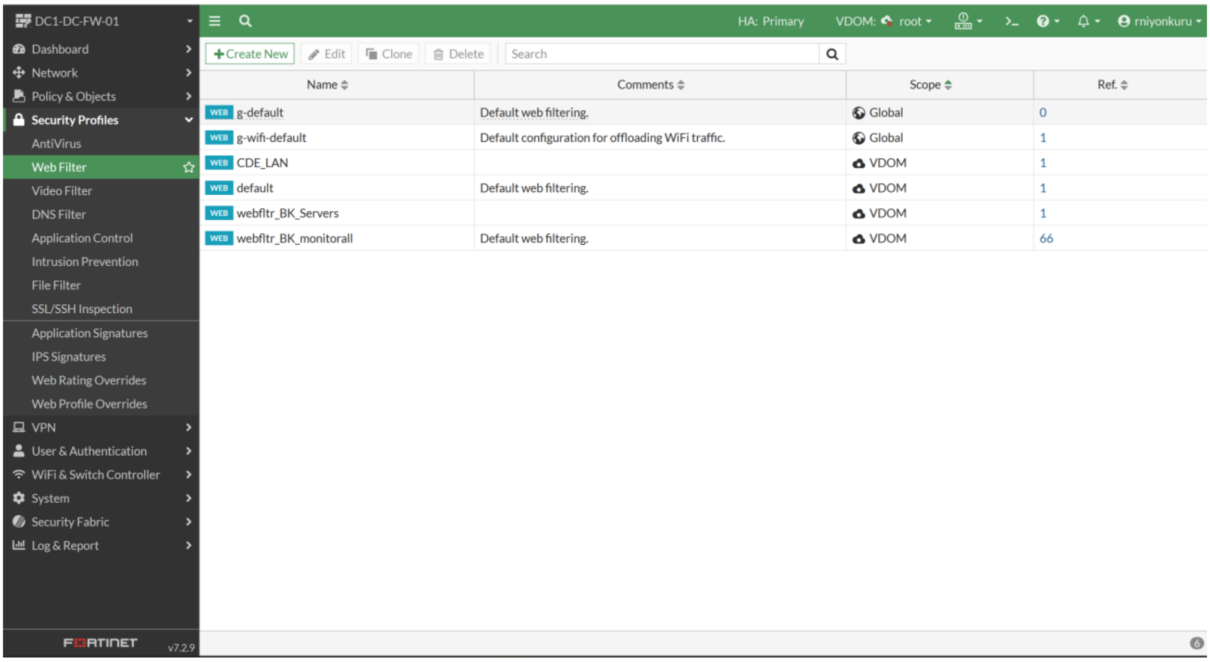
●●●●●●●●●●●

4.12 Fortinet Security Profiles



Name	Comments		Ref.
AV g-default	Scan files and block viruses.	Global	0
AV g-wifi-default	Default configuration for offloading WiFi traffic.	Global	1
AV av_branches_baseline	Scan files and block viruses.	VDOM	71
AV default	Scan files and block viruses.	VDOM	1
AV av_servers_baseline	Scan files and block viruses.	VDOM	8

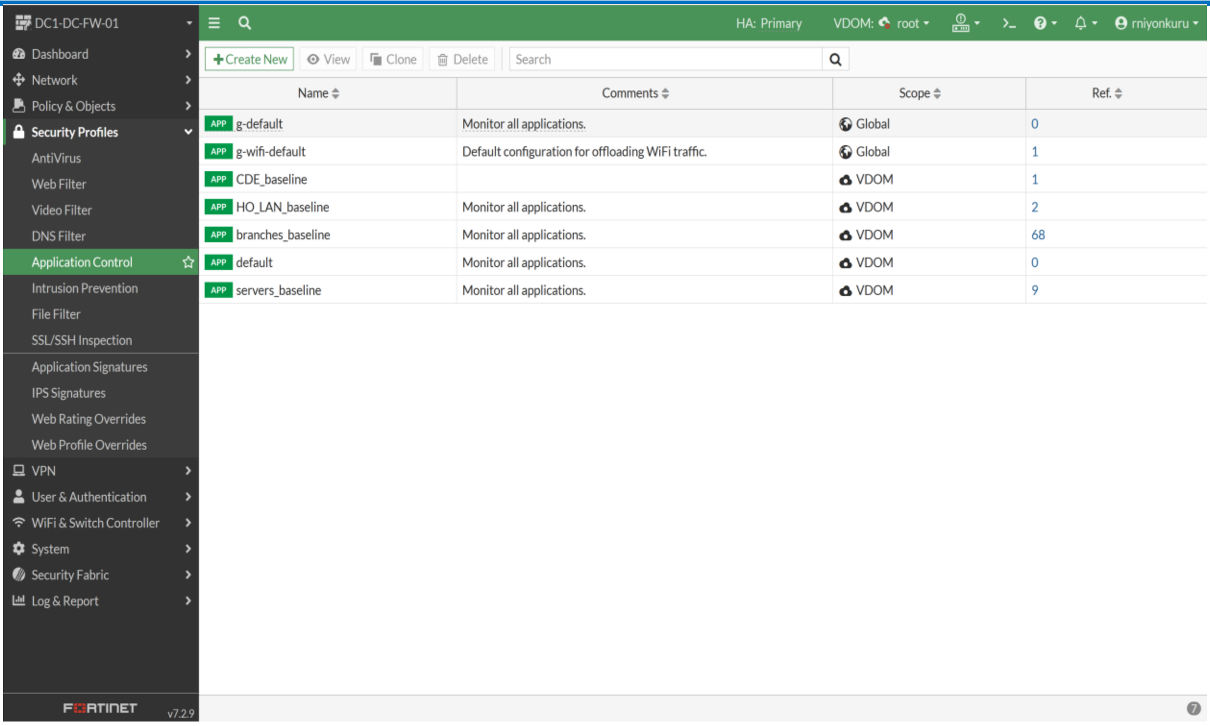
Antivirus Profile scans network traffic for viruses and malware and profiles can be configured for different levels of protection (e.g., to block, quarantine, or log threats).



Name	Comments	Scope	Ref.
WEB g-default	Default web filtering.	Global	0
WEB g-wifi-default	Default configuration for offloading WiFi traffic.	Global	1
WEB CDE_LAN		VDOM	1
WEB default	Default web filtering.	VDOM	1
WEB webfltr_BK_Servers		VDOM	1
WEB webfltr_BK_monitorall	Default web filtering.	VDOM	66

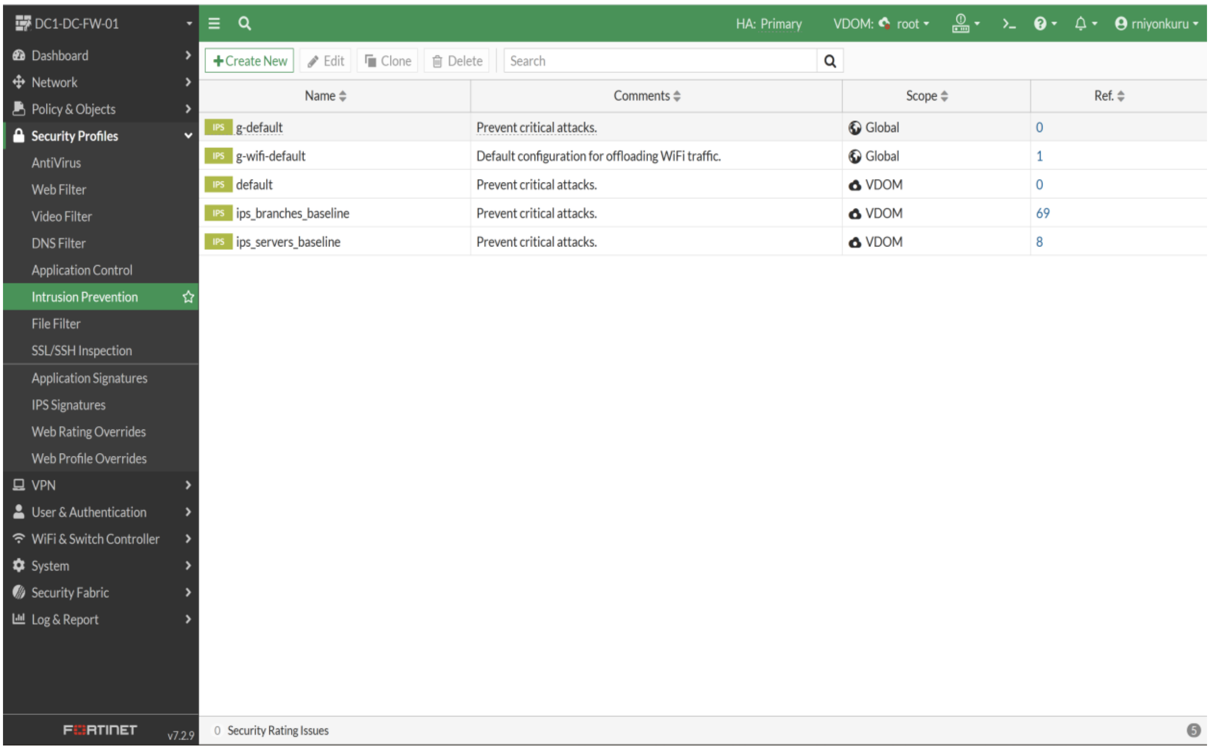
Web Filter Profile provides URL filtering to control access to websites based on categories (such as social media, gambling, or adult content). Helps enforce security policies, reduce bandwidth consumption, and protect users from malicious or inappropriate content.

https://doi.org/10.53819/81018102t2444



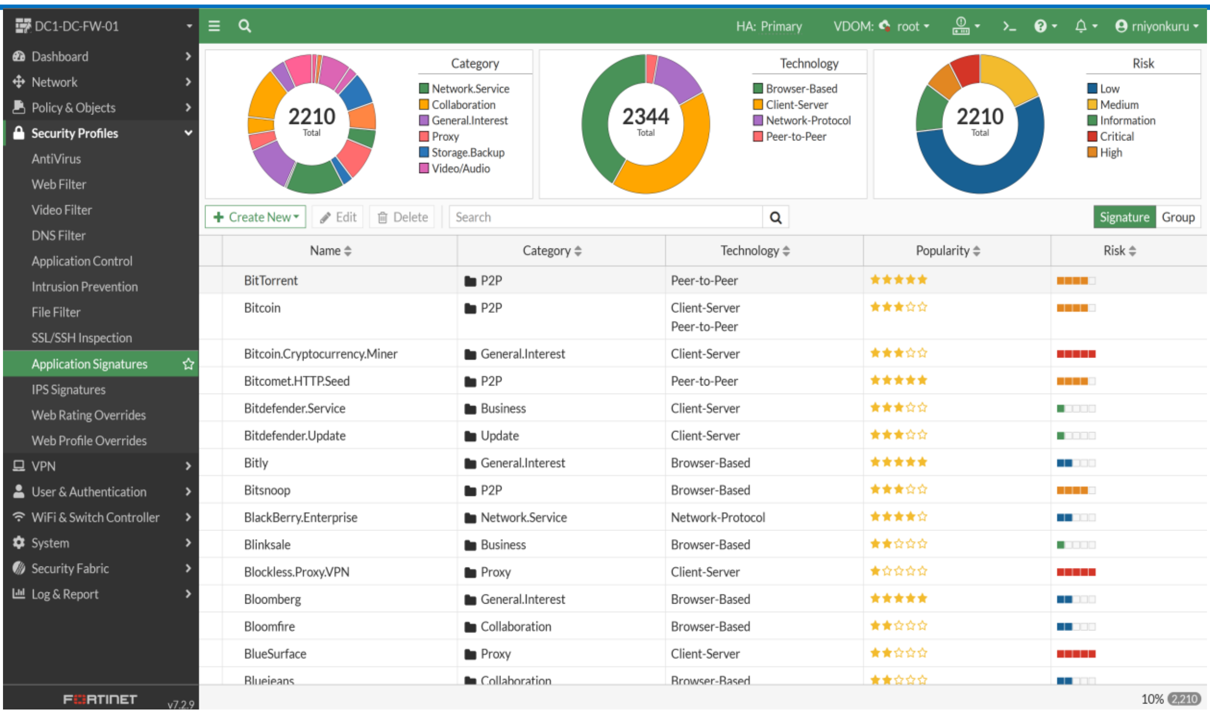
Name	Comments	Scope	Ref.
APP g-default	Monitor all applications.	Global	0
APP g-wifi-default	Default configuration for offloading WiFi traffic.	Global	1
APP CDE_baseline		VDOM	1
APP HO_LAN_baseline	Monitor all applications.	VDOM	2
APP branches_baseline	Monitor all applications.	VDOM	68
APP default	Monitor all applications.	VDOM	0
APP servers_baseline	Monitor all applications.	VDOM	9

Application Control Profile monitors and controls applications based on predefined categories or custom rules, can allow, block, or restrict applications to manage bandwidth usage and prevent risky apps from being used on the network. It detects thousands of applications, even those using non-standard ports or encryption to bypass detection.



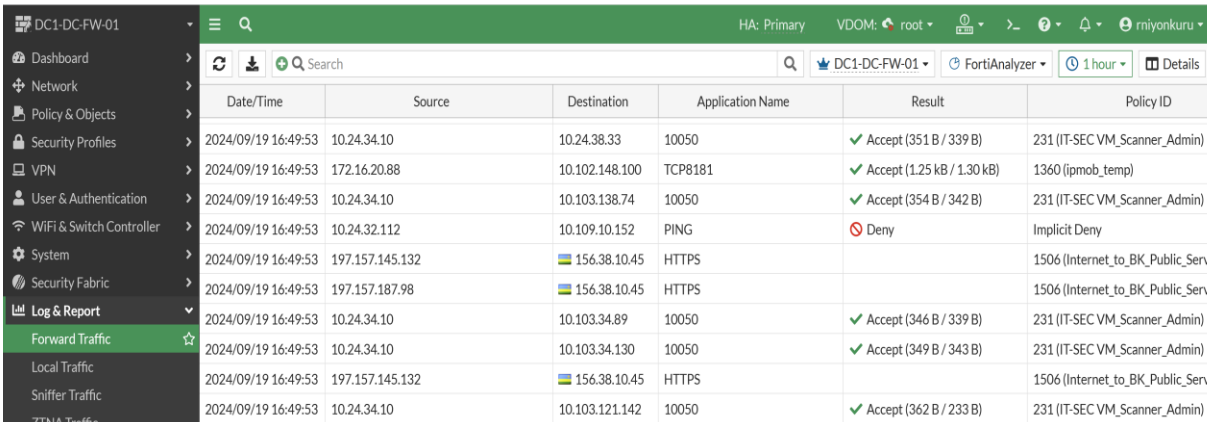
Name	Comments	Scope	Ref.
IPS g-default	Prevent critical attacks.	Global	0
IPS g-wifi-default	Default configuration for offloading WiFi traffic.	Global	1
IPS default	Prevent critical attacks.	VDOM	0
IPS ips_branches_baseline	Prevent critical attacks.	VDOM	69
IPS ips_servers_baseline	Prevent critical attacks.	VDOM	8

Intrusion Prevention System (IPS) Profile protects networks from known and zero-day vulnerabilities by detecting and blocking suspicious network activities. Protects against exploits, malware, and other attacks at the network level.



Name	Category	Technology	Popularity	Risk
BitTorrent	P2P	Peer-to-Peer	★★★★★	■■■■□
Bitcoin	P2P	Client-Server Peer-to-Peer	★★★☆☆	■■■■□
Bitcoin.Cryptocurrency.Miner	General.Interest	Client-Server	★★★☆☆	■■■■■
Bitcomet.HTTP.Seed	P2P	Peer-to-Peer	★★★★★	■■■■□
Bitdefender.Service	Business	Client-Server	★★★☆☆	■□□□□
Bitdefender.Update	Update	Client-Server	★★★☆☆	■□□□□
Bitly	General.Interest	Browser-Based	★★★★★	■■□□□
Bitsnoop	P2P	Browser-Based	★★★☆☆	■■■■□
BlackBerry.Enterprise	Network.Service	Network-Protocol	★★★★☆	■■□□□
Blinksale	Business	Browser-Based	★★☆☆☆	■□□□□
Blockless.Proxy.VPN	Proxy	Client-Server	★☆☆☆☆	■■■■■
Bloomberg	General.Interest	Browser-Based	★★★★★	■■□□□
Bloomfire	Collaboration	Browser-Based	★★☆☆☆	■■□□□
BlueSurface	Proxy	Client-Server	★★☆☆☆	■■■■■
Bluejeans	Collaboration	Browser-Based	★★☆☆☆	■■□□□

Application Control Profile monitors and controls applications based on predefined categories or custom rules. Can allow, block, or restrict applications to manage bandwidth usage and prevent risky apps from being used on the network. Detects thousands of applications, even those using non-standard ports or encryption to bypass detection.



Date/Time	Source	Destination	Application Name	Result	Policy ID
2024/09/19 16:49:53	10.24.34.10	10.24.38.33	10050	✓ Accept (351 B / 339 B)	231 (IT-SEC VM_Scanner_Admin)
2024/09/19 16:49:53	172.16.20.88	10.102.148.100	TCP8181	✓ Accept (1.25 kB / 1.30 kB)	1360 (ipmob_temp)
2024/09/19 16:49:53	10.24.34.10	10.103.138.74	10050	✓ Accept (354 B / 342 B)	231 (IT-SEC VM_Scanner_Admin)
2024/09/19 16:49:53	10.24.32.112	10.109.10.152	PING	⊘ Deny	Implicit Deny
2024/09/19 16:49:53	197.157.145.132	156.38.10.45	HTTPS		1506 (Internet_to_BK_Public_Serv
2024/09/19 16:49:53	197.157.187.98	156.38.10.45	HTTPS		1506 (Internet_to_BK_Public_Serv
2024/09/19 16:49:53	10.24.34.10	10.103.34.89	10050	✓ Accept (346 B / 339 B)	231 (IT-SEC VM_Scanner_Admin)
2024/09/19 16:49:53	10.24.34.10	10.103.34.130	10050	✓ Accept (349 B / 343 B)	231 (IT-SEC VM_Scanner_Admin)
2024/09/19 16:49:53	197.157.145.132	156.38.10.45	HTTPS		1506 (Internet_to_BK_Public_Serv
2024/09/19 16:49:53	10.24.34.10	10.103.121.142	10050	✓ Accept (362 B / 233 B)	231 (IT-SEC VM_Scanner_Admin)

Fortinet provides robust logging and reporting features, allowing administrators to monitor and analyze security events in detail. It has the capabilities to provide deep insight into network activities and security events, helping organizations maintain a strong security posture and ensure compliance with regulations.

4.13 The Importance of Network Visibility and Analytics

As organizations build out a distributed IT infrastructure, applications, and user environments, it is critical that they have end-to-end visibility of the IT environment and eliminate any blind spots, as it is impossible to manage something that you cannot "see." Enterprise Strategy Group research validates this and demonstrates the importance of network visibility, as 81% of organizations stated that end-to-end network visibility is either critical or very important, and only one percent stated it wasn't important at all

https://doi.org/10.53819/81018102t2444

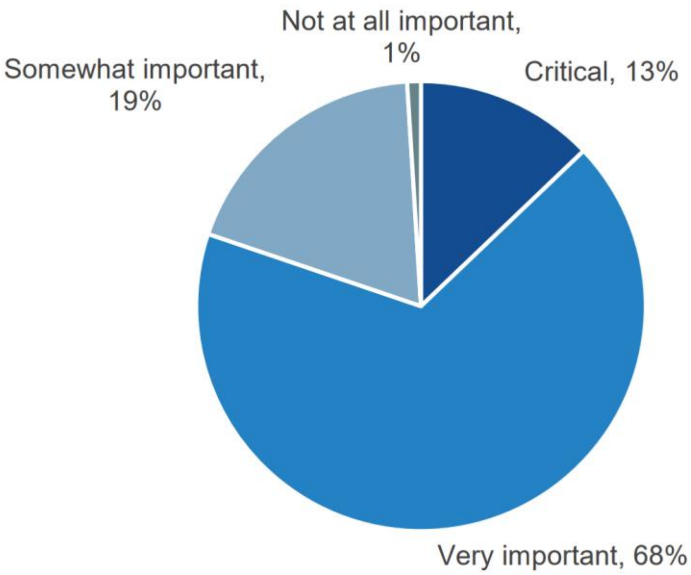
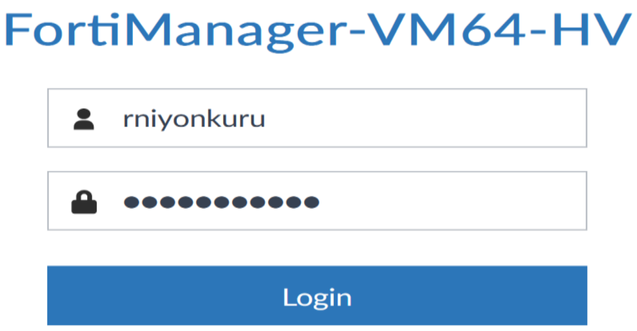


Figure 9. Importance of End-to-end Visibility

4.14 The Importance of Network Visibility and Analytics

Fortinet understands the challenges associated with implementing a zero trust architecture and has developed solutions to enable organizations to jumpstart their zero trust journey. It starts with Fortinet's Secure SD-WAN, which provides organizations with a foundation to provide the visibility, analytics, and automation capabilities that drive operational efficiencies and enhance security postures. For example, the visibility, analytics and automation are extended across the entire network (LAN, WLAN and WAN [including 4G/5G]) to enhance zero trust initiatives. Furthermore, organizations are able to segment and prioritize application traffic to reduce attack surface and ensure performance. With the purpose-built ASIC, scale and power efficiency are optimized as well. Additional operational efficiencies are achieved using zero-touch provisioning and centralized management combined that enables network, application, and security configurations and policies to be distributed to all sites and hybrid workers correctly and consistently. FortiManager and FortiAnalyzer to deliver the end-to-end visibility, analytics, and reporting across the Fortinet Security Fabric to ensure end-to-end visibility across the WAN, LAN, and WLAN. This unified visibility enables operations teams to drive operational efficiency even though the network and security environment is becoming more distributed and complex. The use of out-of-the-box templates to follow best practices and device blueprints drives additional efficiencies. Having a centralized management platform that provides deep visibility of systems, applications, and interfaces that include items such as network segmentation, performance SLAs, IoT device ID, route tables, IPS templates, and top talkers.

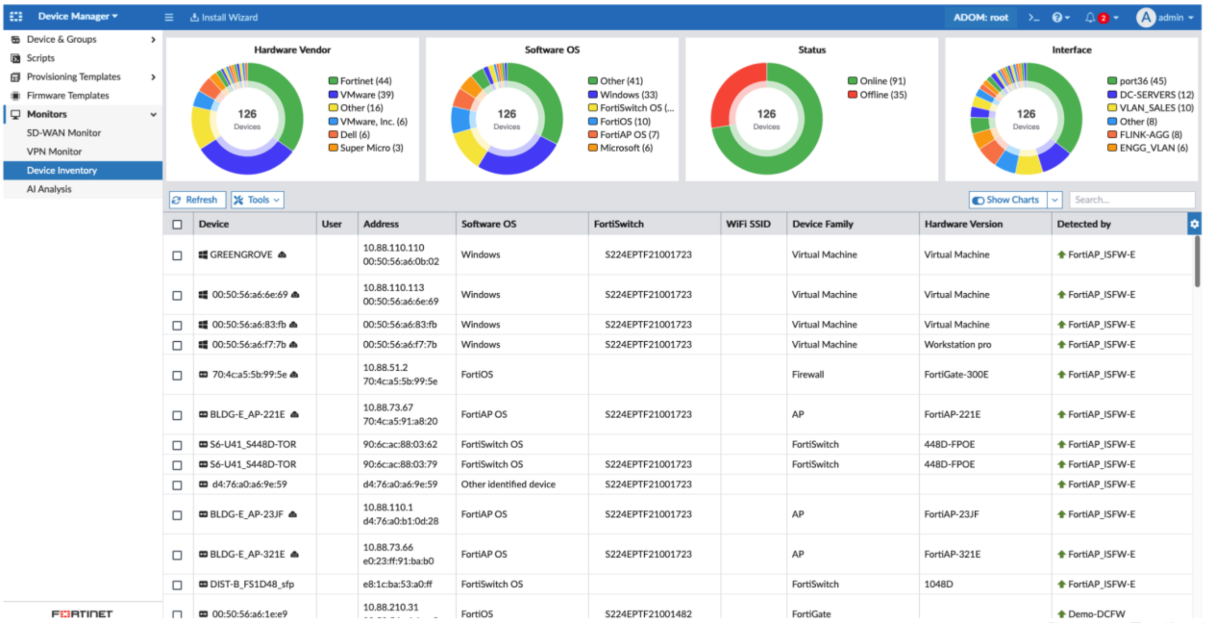
4.15 FortiManager Administration Login


FortiManager-VM64-HV

rniyonkuru

●●●●●●●●●●●

4.16 Centralized Management and Visibility



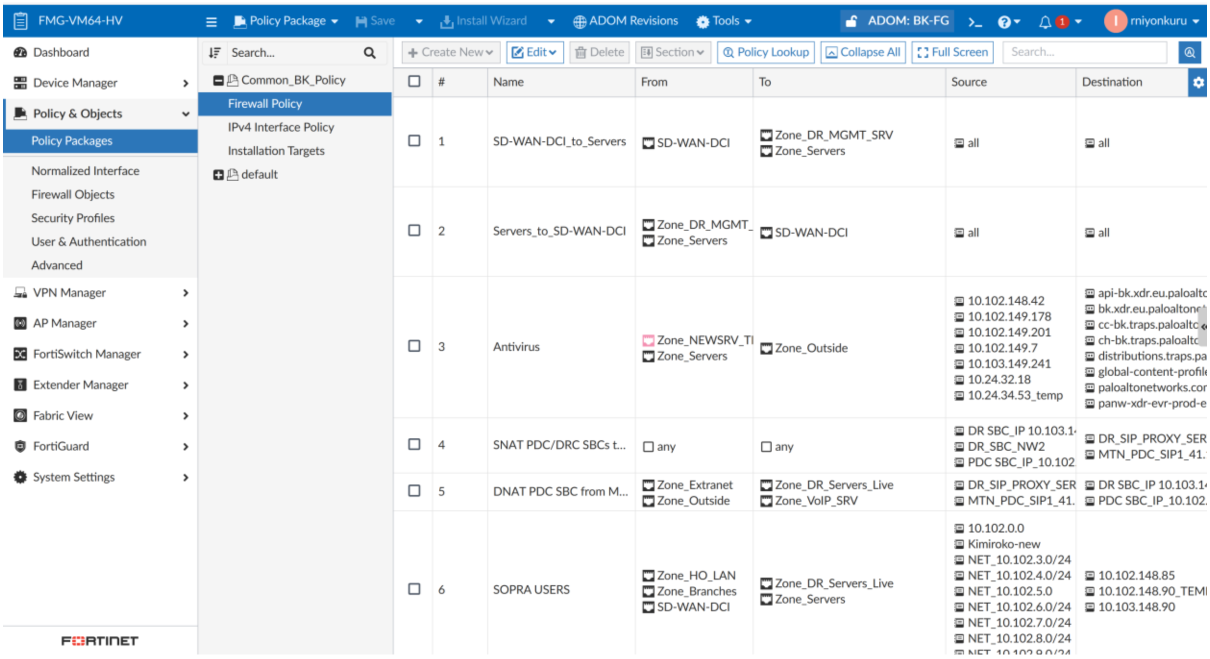
☐	Device	User	Address	Software OS	FortiSwitch	WiFi SSID	Device Family	Hardware Version	Detected by
☐	GREENGROVE		10.88.110.110 00:50:56:a6:0b:02	Windows	S224EPTF21001723		Virtual Machine	Virtual Machine	FortiAP_ISFW-E
☐	00:50:56:a6:6e:69		10.88.110.113 00:50:56:a6:6e:69	Windows	S224EPTF21001723		Virtual Machine	Virtual Machine	FortiAP_ISFW-E
☐	00:50:56:a6:83:fb		00:50:56:a6:83:fb	Windows	S224EPTF21001723		Virtual Machine	Virtual Machine	FortiAP_ISFW-E
☐	00:50:56:a6:f7:7b		00:50:56:a6:f7:7b	Windows	S224EPTF21001723		Virtual Machine	Workstation pro	FortiAP_ISFW-E
☐	70:4c:a5:5b:99:5e		10.88.51.2 70:4c:a5:5b:99:5e	FortiOS			Firewall	FortiGate-300E	FortiAP_ISFW-E
☐	BLDG-E_AP-221E		10.88.73.67 70:4c:a5:91:a8:20	FortiAP OS	S224EPTF21001723		AP	FortiAP-221E	FortiAP_ISFW-E
☐	S6-U41_S448D-TOR		90:6c:ac:88:03:62	FortiSwitch OS			FortiSwitch	448D-FPOE	FortiAP_ISFW-E
☐	S6-U41_S448D-TOR		90:6c:ac:88:03:79	FortiSwitch OS	S224EPTF21001723		FortiSwitch	448D-FPOE	FortiAP_ISFW-E
☐	d4:76:a0:a6:9e:59		d4:76:a0:a6:9e:59	Other identified device	S224EPTF21001723				FortiAP_ISFW-E
☐	BLDG-E_AP-23JF		10.88.110.1 d4:76:a0:b1:0d:28	FortiAP OS	S224EPTF21001723		AP	FortiAP-23JF	FortiAP_ISFW-E
☐	BLDG-E_AP-321E		10.88.73.66 e0:23:ff:91:ba:b0	FortiAP OS	S224EPTF21001723		AP	FortiAP-321E	FortiAP_ISFW-E
☐	DIST-B_FS1D48_sfp		e8:1c:ba:53:a0:ff	FortiSwitch OS			FortiSwitch	1048D	FortiAP_ISFW-E
☐	00:50:56:a6:1e:e9		10.88.210.31	FortiOS	S224EPTF21001482		FortiGate		Demo-DCFW

Figure 10. Centralized Management and Visibility

This visibility enables organizations to mitigate risk and deliver enhanced experiences. Leveraging automation-driven network configuration, visibility, and policy management will enable organizations to be more agile and turn up new locations quickly, while operations teams can spend more time on strategic initiatives and less time performing repetitive manual tasks. To drive additional efficiencies, FortiManager has streamlined workflows that are integrated with almost 500 ecosystem partners.

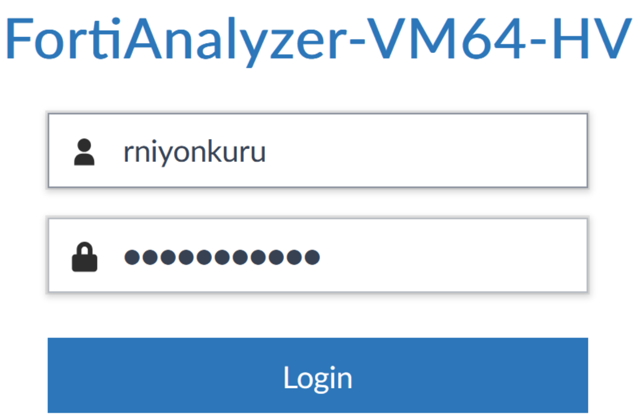
4.14 Policy Packages and Firewall Policy Management

Fortinet FortiManager is a centralized management solution that allows organizations to manage Fortinet devices (primarily FortiGate firewalls) from a single interface. It's designed for enterprises, Managed Security Service Providers (MSSPs), and large network environments to simplify the deployment and management of security policies across multiple devices.



☐	#	Name	From	To	Source	Destination
☐	1	SD-WAN-DCI_to_Servers	SD-WAN-DCI	Zone_DR_MGMT_SRV Zone_Servers	all	all
☐	2	Servers_to_SD-WAN-DCI	Zone_DR_MGMT_ Zone_Servers	SD-WAN-DCI	all	all
☐	3	Antivirus	Zone_NEWSRV_TI Zone_Servers	Zone_Outside	10.102.148.42 10.102.149.178 10.102.149.201 10.102.149.7 10.103.149.241 10.24.32.18 10.24.34.53_temp	api-bk.xdr.eu.paloaltc bk.xdr.eu.paloaltonc cc-bk.traps.paloaltc ch-bk.traps.paloaltc distributions.traps.pa global-content-profile paloaltonetworks.cor panw-xdr-evr-prod-e
☐	4	SNAT PDC/DRC SBCs t...	any	any	DR SBC_IP 10.103.1 DR_SBC_NW2 PDC SBC_IP_10.102	DR_SIP_PROXY_SER MTN_PDC_SIP1_41.
☐	5	DNAT PDC SBC from M...	Zone_Extranet Zone_Outside	Zone_DR_Servers_Live Zone_VoIP_SRV	DR_SIP_PROXY_SER MTN_PDC_SIP1_41.	DR SBC_IP 10.103.1 PDC SBC_IP_10.102
☐	6	SOPRA USERS	Zone_HO_LAN Zone_Branches SD-WAN-DCI	Zone_DR_Servers_Live Zone_Servers	10.102.0.0 Kimiroko-new NET_10.102.3.0/24 NET_10.102.4.0/24 NET_10.102.5.0 NET_10.102.6.0/24 NET_10.102.7.0/24 NET_10.102.8.0/24 NET_10.102.9.0/24	10.102.148.85 10.102.148.90_TEMI 10.103.148.90

4.15 FortiAnalyzer Administration Login

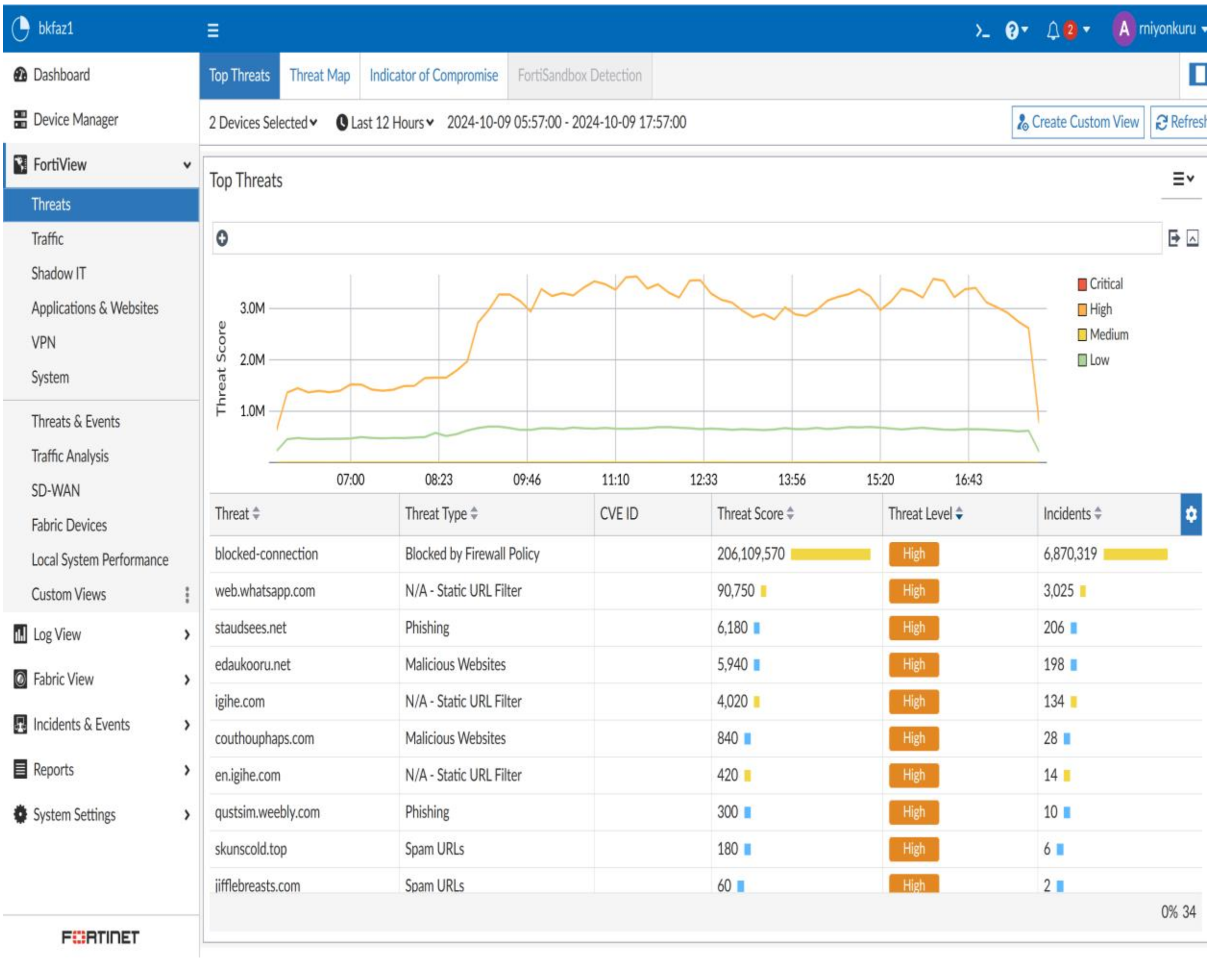


FortiAnalyzer-VM64-HV

rniyonkuru

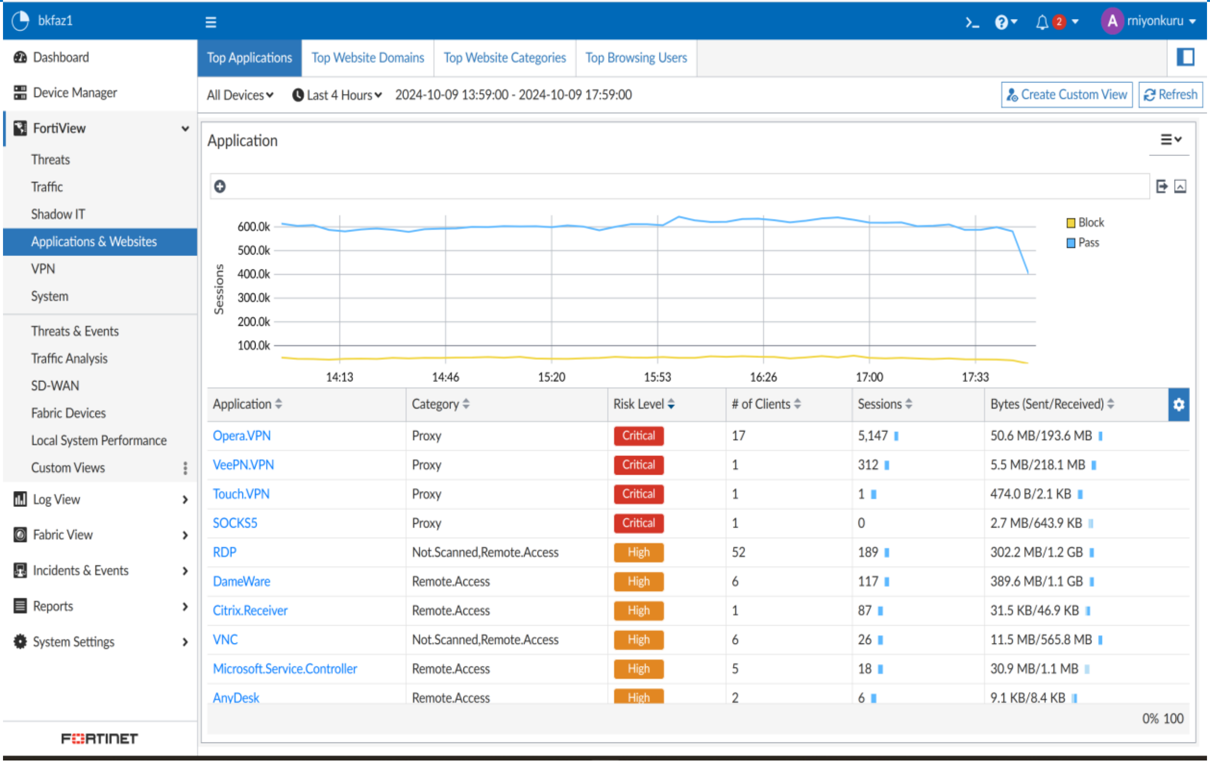
●●●●●●●●●●●●

Login



Threat	Threat Type	CVE ID	Threat Score	Threat Level	Incidents
blocked-connection	Blocked by Firewall Policy		206,109,570	High	6,870,319
web.whatsapp.com	N/A - Static URL Filter		90,750	High	3,025
staudsees.net	Phishing		6,180	High	206
edaukooru.net	Malicious Websites		5,940	High	198
igihe.com	N/A - Static URL Filter		4,020	High	134
couthouphaps.com	Malicious Websites		840	High	28
en.igihe.com	N/A - Static URL Filter		420	High	14
qustsim.weebly.com	Phishing		300	High	10
skunscold.top	Spam URLs		180	High	6
jifflebreasts.com	Spam URLs		60	High	2

0% 34



All Devices · Last 4 Hours · 2024-10-09 13:59:00 - 2024-10-09 17:59:00

Application	Category	Risk Level	# of Clients	Sessions	Bytes (Sent/Received)
Opera.VPN	Proxy	Critical	17	5,147	50.6 MB/193.6 MB
VeePN.VPN	Proxy	Critical	1	312	5.5 MB/218.1 MB
Touch.VPN	Proxy	Critical	1	1	474.0 B/2.1 KB
SOCKS5	Proxy	Critical	1	0	2.7 MB/643.9 KB
RDP	Not.Scanned,Remote.Access	High	52	189	302.2 MB/1.2 GB
DameWare	Remote.Access	High	6	117	389.6 MB/1.1 GB
Citrix.Receiver	Remote.Access	High	1	87	31.5 KB/46.9 KB
VNC	Not.Scanned,Remote.Access	High	6	26	11.5 MB/565.8 MB
Microsoft.Service.Controller	Remote.Access	High	5	18	30.9 MB/1.1 MB
AnyDesk	Remote.Access	High	2	6	9.1 KB/8.4 KB

The implementation of Fortinet's SD-WAN at Bank of Kigali provided multiple benefits. The findings revealed that the bank achieved significant improvements in network performance, IT security, cost efficiency, and regulatory compliance. The use of centralized management and advanced security features, combined with Fortinet's ability to integrate with the bank's existing systems, made it possible to maintain secure, efficient, and resilient banking operations.

5. Conclusion and Recommendations

The Bank of Kigali's successful deployment of SD-WAN emphasises the necessity of ongoing IT personnel training. The bank ought to make investments to upskill its employees, especially in SD-WAN system configuration, security protocols, and network management. By doing this, the bank will be able to take full use of SD-WAN's capabilities and remain ahead of evolving security threats.

It is advised that SD-WAN be installed throughout the Bank of Kigali's whole network architecture as it expands. By doing this, the bank will be able to keep all of its branches operating at the same level of security and network performance. Additionally, expanding the use of SD-WAN to farther-flung areas may improve connection and save operating expenses.

The Bank of Kigali should think about incorporating automation and artificial intelligence (AI) into its SD-WAN system to improve network administration and security. Further enhancing overall efficiency and security, these technologies can automate repetitive jobs, expedite response times to network anomalies, and improve decision-making processes.

To make sure that SD-WAN rules are in line with the latest technical developments and operational requirements, the bank should institute a regular review process. This entails revising traffic management guidelines and security protocols in response to evolving threats and network conditions.

Future researchers may examine the end-user experience following the implementation of SD-WAN. This could include surveys and interviews with IT staff, network managers, and general employees to assess the perceived benefits and challenges from a user perspective, especially regarding usability, network performance, and security.

A deeper examination of the economic impact of SD-WAN in developing regions like Africa, Asia, and South America could be useful. Researchers could analyze how SD-WAN enables digital transformation in emerging economies and how it supports growth in sectors like banking, healthcare, and education in these markets.

With the growing use of AI and automation in network management, further research could explore how AI-driven SD-WAN solutions can enhance network performance, streamline operations, and improve security responses. Investigating the role of machine learning and automation in optimizing SD-WAN capabilities could be a future area of study. Compliance with regulations like GDPR, PCI DSS, and other data protection laws can influence how SD-WAN is implemented, especially in highly regulated sectors. Further research could explore how SD-WAN helps organizations meet regulatory requirements and manage compliance across different jurisdictions.

Acknowledgements

First and foremost I would like to express my deepest gratitude to my dissertation supervisor, **Dr. MUSONI Wilson**, for the invaluable guidance and support throughout this research journey. The completion of this work was made possible by the perceptive criticism and resolute support.

I would like to express my gratitude to the faculty members of Information Technology who have offered valuable feedback and recommendations during my research. To my beloved family and friends, for your unwavering love, support, and encouragement and patience during challenging times kept me motivated and allowed me to focus on my research.

References

Ali, E. K., Manel, M., & Habib, Y. (2017). An efficient MPLS-based source routing scheme in software-defined wide area networks (SD-WAN). In *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1205-1211). IEEE. https://doi.org/10.1109/AICCSA.2017.165

Andromeda, S., & Gunawan, D. (2020). Techno-economic analysis from implementing SD-WAN with 4G/LTE: A case study in XYZ Company. In *2020 International Seminar on Intelligent Technology and Its Applications (ISITIA)* (pp. 345-351). IEEE.

Arias-Marreros, R., Nalvarte-Dionisio, K., & Andrade-Arenas, L. (2020). Design of a mobile application for the learning of people with Down syndrome through interactive games. *International Journal of Advanced Computer Science and Applications, 11*(11). http://dx.doi.org/10.14569/IJACSA.2020.0111187

Badotra, S., & Panda, S. N. et al. (2020). A survey on software-defined wide area network. *International Journal of Applied Science and Engineering, 17*(1), 59-73.

Carrion-Silva, A., Diaz-Nunez, C., & Andrade-Arenas, L. (2020). Admission exam web application prototype for blind people at the University of Sciences and Humanities. *International Journal of Advanced Computer Science and Applications, 11*(12). http://dx.doi.org/10.14569/IJACSA.2020.0111246

Duliński, Z., Stankiewicz, R., Rzym, G., & Wydrych, P. (2020). Dynamic traffic management for SD-WAN inter-cloud communication. *IEEE Journal on Selected Areas in Communications, 38*(7), 1335-1351. https://doi.org/10.1109/JSAC.2020.2986957

Ellawindy, I., & Heydari, S. S. (2019). QoE-aware real-time multimedia streaming in SD-WANs. In *2019 IEEE Conference on Network Softwarization (NetSoft)* (pp. 66-71). IEEE. https://doi.org/10.1109/NETSOFT.2019.8806622

Gomero-Fanny, V., Bengy, A. R., & Andrade-Arenas, L. (2021). Prototype of web system for organizations dedicated to e-commerce under the scrum methodology. *International Journal of Advanced Computer Science and Applications, 12*(1). http://dx.doi.org/10.14569/IJACSA.2021.0120152

Hosseini, A., Dolati, M., & Ghaderi, M. (2021). Bulk transfer scheduling with deadline in best-effort SD-WANs. In *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)* (pp. 313-321). IEEE.

Houle, A. C., Boulianne, L., & Dupras, L. (2008). SD-WAN: A technology for the efficient use of bandwidth in multi-wavelength networks. In *OFC/NFOEC 2008 - 2008 Conference on Optical Fiber Communication/National Fiber Optic Engineers Conference* (pp. 1-10). IEEE. https://doi.org/10.1109/OFC.2008.4528303

Mohammad, S., Ramesh, D., Pasha, S., & Shankar, K. et al. (2019). Research on new network architecture through SD-WAN. *International Journal of Innovative Technology and Exploring Engineering, 8*(6 Special Issue 4), 483-490.

Mora-Huiracocha, R. E., Gallegos-Segovia, P. L., Vintimilla-Tapia, P. E., Bravo-Torres, J. F., Cedillo-Elias, E. J., & Larios-Rosillo, V. M. (2019). Implementation of an SD-WAN for the interconnection of two software-defined data centers. In *2019 IEEE Colombian Conference on Communications and Computing (COLCOM)* (pp. 1-6). IEEE.

Perez, R., Zabala, A., & Banchs, A. (2021). Alviu: An intent-based SD-WAN orchestrator of network slices for enterprise networks. In *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)* (pp. 211-215). IEEE. https://doi.org/10.1109/NetSoft51509.2021.9492534

Pratiwi, W., & Gunawan, D. (2021). Design and strategy deployment of SD-WAN technology: In Indonesia (Case Study: PT. XYZ). In *2021 International Conference on Green Energy, Computing and Sustainable Technology (GECOST)* (pp. 1-6). IEEE. https://doi.org/10.1109/GECOST52368.2021.9538796

Rajagopalan, S. (2020). An overview of SD-WAN load balancing for WAN connections. In *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1-4). IEEE.

Subramanian, R., & Puthenparambil, J. (2020). Shared memory enabled service plane optimization. In *2020 International Conference on Communication Systems & Networks (COMSNETS)* (pp. 683-684). IEEE. https://doi.org/10.1109/COMSNETS48256.2020.9027436

Troia, L. M. M., Zorello, A. J., Maralit, A. J., & Maier, G. (2020). SD-WAN: An open-source implementation for enterprise networking services. In *2020 22nd International Conference on Transparent Optical Networks (ICTON)* (pp. 1-4). IEEE.

Troia, S., Sapienza, F., Varé, L., & Maier, G. (2021). On deep reinforcement learning for traffic engineering in SD-WAN. *IEEE Journal on Selected Areas in Communications, 39*(7), 2198-2212. https://doi.org/10.1109/JSAC.2020.3041385

Tupia-Astoray, A., & Andrade-Arenas, L. (2021). Implementation of an e-commerce system for the automation and improvement of commercial management at a business level. *International Journal of Advanced Computer Science and Applications, 12*(1). http://dx.doi.org/10.14569/IJACSA.2021.0120177

Wu, X., Lu, K., & Zhu, G. (2018). A survey on software-defined wide area networks. *Journal of Communications, 13*(5), 253-258.

Yang, Z., Cui, Y., Li, B., Liu, Y., & Xu, Y. (2019). Software-defined wide area network (SD-WAN): Architecture, advances and opportunities. In *2019 28th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-9). IEEE.

Zhang, H., Wang, Y., Qi, X., Xu, W., Peng, T., & Liu, S. (2017). Demo abstract: An intent solver for enabling intent-based SDN. In *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 968-969). IEEE.