People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

University A. Mira of Bejaia
Faculty of science and technology
ATE Department

THESIS

FOR THE OBTAINING OF THE MASTER DIPLOMA

Domain: Science and Technology **Speciality:** Telecommunications
Option: Network and Telecommunications

Presented by
Ms.Nessrine Kaouane

Supervised by
Mr.Abdelhani Diboune

Theme

Study and implementation of a SIEM (Security Information and Event Management) for the management and supervision of Information Systems (Sonelgaz)

Academic Year: 2022/2023

Acknowledgement

First and foremost, I would like to express my deepest appreciation to my supervisor, Mr. Abdelhanni Diboune, for accepting to supervise my work and providing me with proper guidance, expertise, and unwavering support. His insightful feedback and constructive criticism have significantly shaped the development of this thesis.

I would also like to extend my gratitude to the members of the jury for their dedicated effort in reviewing my thesis.

I would like to express my sincere appreciation to the ATE department.

Finally, I would like to express my deepest gratitude to the entire cohort. Your enriching exchanges throughout this academic journey have been essential. We have shared moments of joy, stress, and learning together. Thank you to every one of you for your friendship.

Dedications

To my beloved parents, sisters Sara, Roumaissa, Abir, and Maya,

This thesis is dedicated to everyone who has played a significant role in shaping my journey. Your unwavering support, love, and belief in me have been the driving force behind my accomplishments. Through your unique ways and individual impressions,

To everyone else who has been a part of my life's journey, if you were there, thank you.

This thesis is a testament to the love, support, and guidance I have received throughout my life. It stands as a tribute to each of you who have contributed to my academic and personal growth. I am forever grateful for the influence you have had on my life.

With heartfelt appreciation and love,

Kaouane Nessrine

Contents

Contents **I**

List of Figures **V**

List of Tables **VIII**

List of Abbreviations **IX**

General introduction **1**

1 Security of information systems **3**

1.1 Introduction 4

1.2 Information systems 4

1.2.1 Importance of IS security in organizations 5

1.2.2 The objective of the information systems security 5

1.2.3 Levels of Information System Security 6

1.2.3.1 Physical Security 6

1.2.3.2 Network security (Infrastructure) 6

1.2.3.3 Security of information systems 7

1.2.3.4 Human Security 7

1.2.3.5 Security of the organization 7

1.3 Information systems security paradigm 7

1.3.1 Vulnerabilities, threats, and attacks 7

1.3.2 Security attacks classification 8

1.3.2.1 General categories of attacks 8

1.3.3 The Evolving Landscape of Cyberattacks and Its Impact on Companies 11

1.3.3.1 Last five years 11

1.3.4 Solutions 12

1.3.4.1 Information systems security standards 12

1.3.4.2 Security policy 12

1.3.4.3 Defense mechanisms 12

1.4 Security Benefits and Monitoring Logs Activities 15

1.5 Security Monitoring Logs and SIEM Approach: 16

2 Security Information and Events Management 17

2.1 Introduction 18

2.2 SIEM Evolution 18

2.2.1 History 18

2.2.2 Security Information Management (SIM) 18

2.2.2.1 Definition 18

2.2.2.2 Log files 19

2.2.3 Security Event Management (SEM) 20

2.2.3.1 Definition 20

2.2.4 Security information and event managements(SIEM) 20

2.2.4.1 Definition 20

2.2.5 The architecture of SIEM 21

2.2.5.1 SIEM functions 22

2.2.6 Comparison of SIM, SEM, and SIEM 22

2.3 SIEM Benefits 23

2.4 Presentation of some SIEMs solutions 23

2.5 The choice of SIEM solution 24

2.6 Splunk 25

2.6.1 Definition 25

2.6.2 Splunk components 25

2.6.2.1 Splunk forwarder 26

2.6.2.2 Splunk Indexer 27

2.6.2.3 Splunk Search Head 27

2.6.3 Splunk Architecture 28

3 Internship Host Organization 29

3.1 Introduction 30

3.2 General presentation of Sonelgaz 30

3.2.1 History 30

3.2.2 Mission of Sonelgaz 30

3.3 Bejaia Distribution Concession (BDC) 31

3.3.1 General organizational chart for the Distribution Department of Electricity and Gas in Béjaïa 31
3.3.2 IT Systems Management Division (ISMD) 32
3.3.2.1 IT systems management division activities 32
3.3.3 Analyzing the deployment architecture 33
3.3.3.1 Analysis of computer park 34
3.3.4 Critics about the current deployment 36
3.3.5 Proposed Solution 37
3.3.5.1 Monitoring of modules 37

4 Implementation of the proposed solution 39
4.1 Introduction 40
4.2 New deployment 40
4.3 Development environment 41
4.4 Settings of monitoring environment 41
4.4.1 Forwarders Configuration 41
4.4.1.1 configuration of Syslog on a Router 41
4.4.1.2 configuration of Syslog on a FortiGate firewall 42
4.4.1.3 Windows forwarder 43
4.4.1.4 Linux forwarder 44
4.4.2 Splunk Installation and configuration 46
4.4.2.1 Splunk installation 47
4.4.2.2 Splunk configuration 49
4.4.3 Creating and configuring visualization tools 52
4.4.3.1 Creation and Configuration of Dashboards 52
4.4.3.2 Alert Configuration 62
4.4.3.3 Simulation of an attack scenario 64

General Conclusion and Future Perspectives 66

A 67
A.1 Graphical Network Simulator-3 (GNS3) Installation steps 67
A.2 VMware Workstation Installation Steps 68
A.3 Import network simulation devices 69
A.3.1 Installation of virtual machines 70

B 73
B.1 Configuration of a basic network topology 73

B.1.1 Configuration of trunk ports 73
B.1.2 Configuration of VTP protocol 73
B.1.3 VLAN port assignment 74
B.1.4 FortiGate firewall configuration 75
B.1.4.1 Configuring the IP address of port 3 on the FortiGate VM 75
B.1.4.2 Log in to the FortiGate web manager 75
B.1.4.3 Configurations of ports 76
B.1.4.4 VLAN configuration 76
B.1.4.5 Inter-VLAN routing 77
B.1.4.6 Static route configuration 77
B.1.4.7 Configuring policies in Fortigate 78

C **79**
C.1 SPL Language 79
C.2 Components of SPL 79
C.2.1 Syntax 79

List of Figures

1.1 Dimensions of IS [1]. 4
1.2 The Security triad [3]. 5
1.3 IS Security levels. 6
1.4 Interruption attack [8]. 8
1.5 Interception attack [8]. 9
1.6 Modification attack [8]. 10
1.7 Fabrication attack [8]. 10
1.8 Complaints and losses over the last five years [9]. 11
1.9 Intrusion Detection System [12]. 13
1.10 Intrusion Prevention System [15]. 14
1.11 Firewall [16]. 14
1.12 Virtual Private Network [50]. 15

2.1 SIEM basics components [26]. 21
2.2 Splunk Logo. 25
2.3 Splunk components [32]. 26
2.4 Splunk heavy forwarder [33]. 27
2.5 Splunk Architecture [33]. 28

3.1 Logo of Sonelgaz [34]. 30
3.2 Organization chart. 32
3.3 BCD LAN Architecture. 33

4.1 Deployment architecture 40
4.2 Syslog on Cisco Router. 42
4.3 Syslog on Fortigate firewall. 42
4.4 Settings events monitoring. 43
4.5 Universal forwarder Installation. 43
4.6 Configuring Splunk Deployment Server. 44

4.7 Universal forwarder installed. 44
4.8 Install Nginx. 44
4.9 Splunk forwarder installation. 45
4.10 Accept the Splunk Universal Forwarder license. 45
4.11 Set a username and password for the Splunk Universal Forwarder. . . 45
4.12 Add the Splunk server for log forwarding. 46
4.13 Add Nginx monitoring. 46
4.14 Nginx server web page. 46
4.15 Splunk download. 47
4.16 Splunk installation. 47
4.17 Creating an administrator account. 48
4.18 Installation steps. 48
4.19 User interface of Splunk. 49
4.20 Add Splunk listening port. 49
4.21 Add Data. 50
4.22 Index creation steps. 50
4.23 Windows logs. 51
4.24 Linux index creation. 51
4.25 Syslog Index Creation. 52
4.26 File importation. 53
4.27 Data added review. 53
4.28 PortCible Query. 54
4.29 IP addresses count. 54
4.30 Top IP addresses. 55
4.31 Total number of unique source IP. 55
4.32 Visualization type. 56
4.33 Add panel. 56
4.34 Dashboard Screen. 57
4.35 Fortinet Add-on download. 57
4.36 Fortinet App for Splunk download. 58
4.37 Install Fortinet app and addon for splunk. 58
4.38 Research query on Fortinet app. 59
4.39 Network Security Dashboard. 59
4.40 Navigate to the dashboard. 60
4.41 change constraints. 60
4.42 Enable configuration. 61

4.43 Change macros. 61
4.44 Traffic dashboard. 62
4.45 Audit index search. 62
4.46 Server login attempts. 63
4.47 Alert created. 63
4.48 Alerts. 63
4.49 Ports Scanning Attack. 64
4.50 Syslog logs. 65

A.1 GNS3 Installations steps. 67
A.2 GNS3 interface. 68
A.3 VMware workstation installation. 68
A.4 Link VM to GNS3. 69
A.5 Import Switch. 69
A.6 Import Router. 70
A.7 Import Fortigate firewall. 70
A.8 Ubuntu desktop installation. 71
A.9 Windows server installation. 71
A.10 Windows 10 installation. 72
A.11 Kali Linux installation. 72

B.1 Trunk configuration. 73
B.2 VTP server mode. 74
B.3 VTP Client mode. 74
B.4 Port assignment. 75
B.5 Fortigate firewall Configuration in CLI mode. 75
B.6 FortiGate web manager. 76
B.7 Ports configurations. 76
B.8 Vlan configuration. 77
B.9 Inter-VLAN. 77
B.10 Static route. 78
B.11 Firewall policies. 78

List of Tables

2.1 Comparison of different SIEM solutions 24

3.1 Table of DELL N3024 switch types [35]. 35

List of Abbreviations

IS	Information System
IT	Information Technology
CIA	Confidentiality,Integrity,Availability
DOS	Denial of Service
MITM	Men In The Middle
XSS	Cross-site scripting
SQL	Structured Query Language
IC3	Internet and Computing Core Certification
ITSEC	Information Technology Security Evaluation Criteria
TCSEC	Trusted Computer System Evaluation Criteria
ISO	International Organization for Standardization
ISMS	Information security management System
IDS	Intrusion detection System
NIDS	Network Intrusion Detection System
HIDS	Host Intrusion Detection System
IPS	Intrusion prevention System
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual Private Network
SIEM	Security information and event management
SIM	Security information management
SEM	Security event management
IP	Internet Protocol

HTTP	Hypertext Transfer Protocol
SNMP	Simple Network Management Protocol
OSSIM	Open Source Security Information Management
GUI	Graphical User Interface
BDC	Bejaia Distribution Concession
EGA	Electricité Gaz Algerie
ISMD	IT Systems Management Division
SPL	Search processing language

General introduction

The security of information systems is a pressing concern in today's digital landscape due to the escalating incidents of computer abuse and cyber threats. As organizations increasingly rely on technology to store, process, and transmit sensitive data, ensuring the security and integrity of information systems has become paramount. Systems analysts and designers play a crucial role in this endeavor by developing expertise in methods for specifying information systems security.
Effective specification of information systems security requires a comprehensive understanding of potential vulnerabilities, threat vectors, and security controls. Systems analysts and designers must possess the expertise to assess risks, identify potential security gaps, and develop strategies to mitigate these risks effectively. This involves a systematic approach to incorporating security requirements, selecting appropriate security technologies and protocols, and integrating security features into the overall system design.
One approach that has gained significant attention in recent years is Security Information and Event Management (SIEM). SIEM combines real-time monitoring, log management, and advanced analytics to provide organizations with a comprehensive view of their security posture. By correlating and analyzing security event data from various sources, SIEM enables the identification of potential security incidents and facilitates prompt response actions.
In this thesis and internship, we have analyzed and criticized the current deployment of Sonelgaz Bejaia and its services and applications, to propose a new deployment using SIEM solution with Splunk tool, focusing on its benefits, challenges, and potential impact on cybersecurity.

This thesis is divided into four main chapters.

Chapter 1 provides an overview of the security of information systems, highlights the importance of protecting sensitive data, and mitigates cyber threats.

Chapter 2 delves into the concept of SIEM and its significance in enhancing information system security. It explores SIEM solutions' features and capabilities, emphasizing the advantages of real-time monitoring, log management, and advanced analytics. Additionally, the chapter focuses on the selection and justification of Splunk as the SIEM tool for this implementation, considering its suitability for the organization's requirements.

Chapter 3 critically analyzes the organization's information system's current deployment and identifies existing vulnerabilities and weaknesses.

Chapter 4 proposes the implementation of SIEM with Splunk as a solution to enhance the supervision and security of the organization's information system. It outlines a detailed plan for implementing, configuring, and integrating SIEM into the existing infrastructure.

Chapter 1

Security of information systems

1.1 Introduction

As computers and other digital devices become more integral to business and commerce, they are increasingly targeted by attacks. Before businesses and individuals can confidently use their computing devices, they must ensure that the device has not been compromised and that all communications are secure. Information systems store, process, and transmit sensitive information, such as personal, financial, and business data. However, these systems are exposed to various threats, such as cyber-attacks, data theft, computer viruses, hacking, and malware. To effectively respond to these threats, it is important to understand various aspects of information system security. This chapter provides an overview of the basic concepts of information system security. It discusses various vulnerabilities in information systems and examines regulatory aspects and security standards that apply to information systems, such as ISO 27001. Finally, we will review some measures that can be taken to mitigate security threats [41].

1.2 Information systems

Information systems (IS), considered to be the heart of a company, is the set of organizational, human, and technological means implemented to manage information Figure 1.1. It must be free of any security flaw that could compromise the information that circulates within it regarding confidentiality, integrity, or availability. Thus, security standards have been defined, giving the rules to respect and maintain the security of the company's information systems. At the same time, given the complexity of implementing these standards, several risk analysis methods have been developed to facilitate and guide their use. However, most of these methods are only partially compatible, as it takes into account only a part of the rules stated in these standards [1].

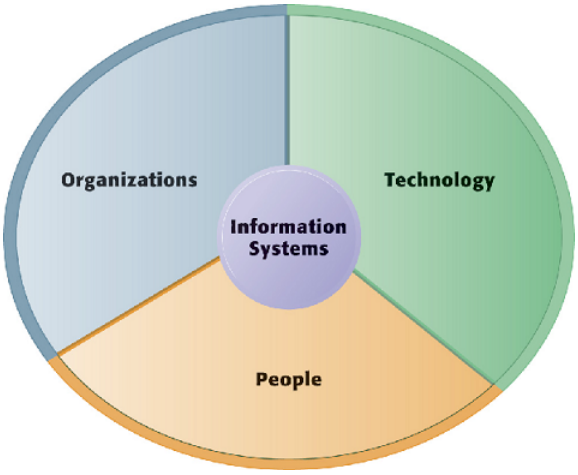


Figure 1.1: Dimensions of IS [1].

1.2.1 Importance of IS security in organizations

Information system security refers to the measures individuals and organizations take to safeguard information and ensure its safety for themselves, their company, and their clients. The protection of business integrity and client privacy are crucial considerations, and information security is a top priority for organizations due to its value and importance. All organizations require protection against Cyber-attacks and security threats, and investing in such safeguards is imperative. Data breaches can be detrimental, resulting in costly and time-consuming consequences. By implementing strong information system security measures, a company can reduce the risk of both internal and external attacks on its IT systems [52, 2, 40].

1.2.2 The objective of the information systems security

The major reason for providing security to the information systems is not just one fold but three folds as shown in Figure 1.2:

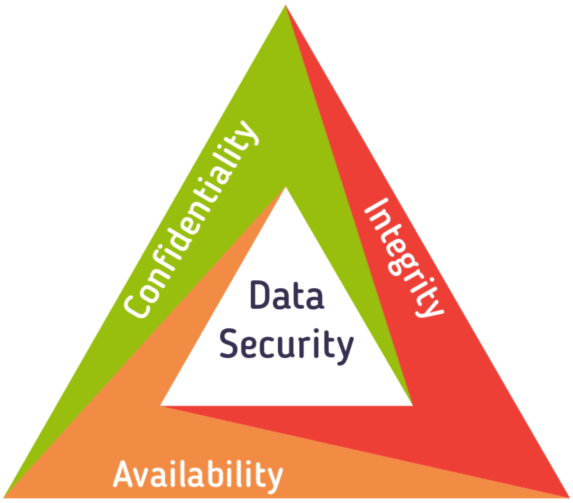


Figure 1.2: The Security triad [3].

The three letters in the "CIA triad" stand for Confidentiality, Integrity, and Availability. The CIA triad is a common model that forms the basis for the development of security systems. They are used for finding vulnerabilities and methods for creating solutions [4, 43].

- Confidentiality: helps to protect sensitive information from unauthorized access attempts. It is common to categorize data based on the amount and type of damage that can occur if the data falls into the wrong hands. Depending on the category, more or less strict measures can be implemented.
- Integrity: includes maintaining data consistency, accuracy, and reliability throughout the data lifecycle. Data must not be modified in transit, and steps must be taken to prevent unauthorized persons from modifying the data.

- Availability: means that information is consistent and easily accessible by authorized parties. This includes proper maintenance of the hardware and technical infrastructure and systems that store and display information [4].

Additionally, the CIA triad can be enhanced with additional factors such as reliability, non-repudiation, and accountability, depending on the specific needs of a particular system or environment [5].

- Reliability: Assurance that data is genuine, accurate, and reliable. This includes preventing unauthorized access, modification, or deletion of data.
- Non-repudiation: The origin and authenticity of data can be verified, ensuring that the sender cannot refuse to send the data

1.2.3 Levels of Information System Security

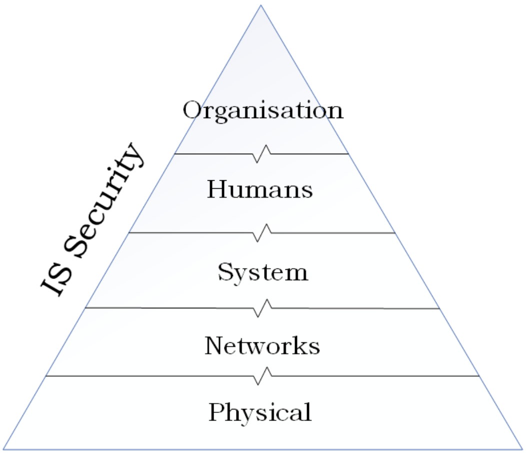


Figure 1.3: IS Security levels.

Information System security can be organized into several tiers Figure 1.3, depending on the different layers of security put in place to protect IS systems and the data they contain.

1.2.3.1 Physical Security

This level focuses on protecting computer equipment from physical risks such as theft or damage. It involves measures like limiting access to buildings and rooms using locks, key cards, or biometric authentication, as well as installing security cameras and alarms to monitor and detect unauthorized access or suspicious activity [6].

1.2.3.2 Network security (Infrastructure)

Once the physical security of devices is ensured, the next level is to protect them from virtual threats when connected to a network. Network administrators and security specialists are responsible for configuring and maintaining the organization's network infrastructure and implementing measures to prevent unauthorized access to the network, such as using software or hardware tools for detection and prevention [6].

1.2.3.3 Security of information systems

This level focuses on securing the computer systems themselves, including the operating systems, software, and data they contain. It involves implementing measures to protect the confidentiality, integrity, and availability of information. System administrators and security specialists are responsible for managing access to sensitive data by assigning specific privileges to users and ensuring the overall security of the computer systems [6].

1.2.3.4 Human Security

This level addresses the behavioral security of individuals using computer systems. It recognizes that human factors can be unpredictable and introduces potential risks. Human security measures involve implementing policies and procedures related to employee security, such as Security Awareness Training, Background Checks, and Identity and Access Management. The Human resources team typically takes responsibility for implementing these measures [6].

1.2.3.5 Security of the organization

To maintain security even during staff turnover, it is crucial to establish documented procedures. Security should be deeply ingrained in the company's culture and treated as a serious matter. Implementing a staff training plan is essential to ensure that all employees, especially new hires, embrace a safety culture.

To enforce security procedures effectively, the Information technology and Human resources departments need to collaborate. This collaboration involves implementing various measures, such as developing a comprehensive plan to respond to security incidents and minimizing potential damage and downtime.

Achieving strong enterprise security requires a systematic approach involving multiple steps. Adopting a bottom-up strategy is recognized as the most effective method. Although it does not provide complete assurance of absolute security, it offers valuable benefits [6].

1.3 Information systems security paradigm

1.3.1 Vulnerabilities, threats, and attacks

In the context of IS security, vulnerabilities, threats, and attacks are three key concepts that are closely related to each other.

1. Vulnerability is a weakness, a design problem, or an implementation error in a system that can lead to an unexpected and undesirable event regarding the

security system. It can exist almost anywhere, from hardware devices and infrastructure to operating systems, firmware, applications, modules, drivers, and application programming interfaces.

2. Threat refers to a potential danger or harm that can exploit a vulnerability in a system. Threats can come from different sources, such as hackers, malware, natural disasters, or human mistakes.

3. Attack is an assault on system security that is delivered by a person or a machine to a system, it violates security.

The relationship between these three concepts is that a vulnerability lead to a threat, and a threat can lead to an attack, In other words, a vulnerability creates an opportunity for a threat actor to exploit it and launch an attack [7].

1.3.2 Security attacks classification

One of the more exciting and dynamic aspects of network security relates to attacks. Our goals of security – Confidentiality, Integrity, Authentication, and Availability – can be threatened by security attacks. These attacks on information system security can be classified according to the objectives of the attacker.

1.3.2.1 General categories of attacks

1. **Interruption**
   A system asset is destroyed, becomes unavailable, or is rendered unusable. This is an attack on availability, see Figure 1.4.

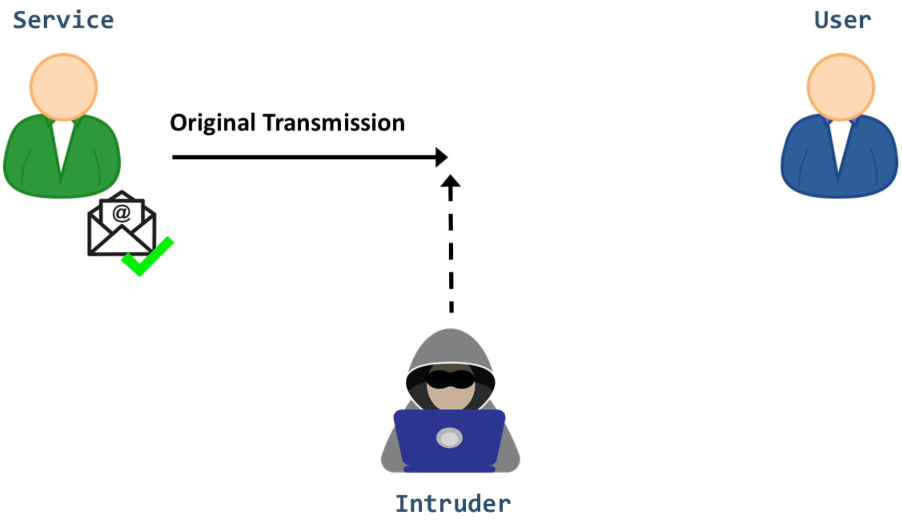


Figure 1.4: Interruption attack [8].

For example: due to various malicious actions, genuine users may experience difficulty accessing the system, either on a temporary or permanent basis.

A potential attacker can achieve this by stealing or damaging hardware or software components, or by launching a DoS (Denial of Service) attack on the server host, resulting in an overload of requests that prevents it from responding. Malware, such as viruses or Trojans, can also be used to erase data or disable a system's functionality, leading to legitimate users being unable to access [8, 55].

2. **Interception**
   Unauthorized access is gained to an asset. This is a violation of confidentiality. A human, a program, or a computer could be an unauthorized party, see Figure 1.5.

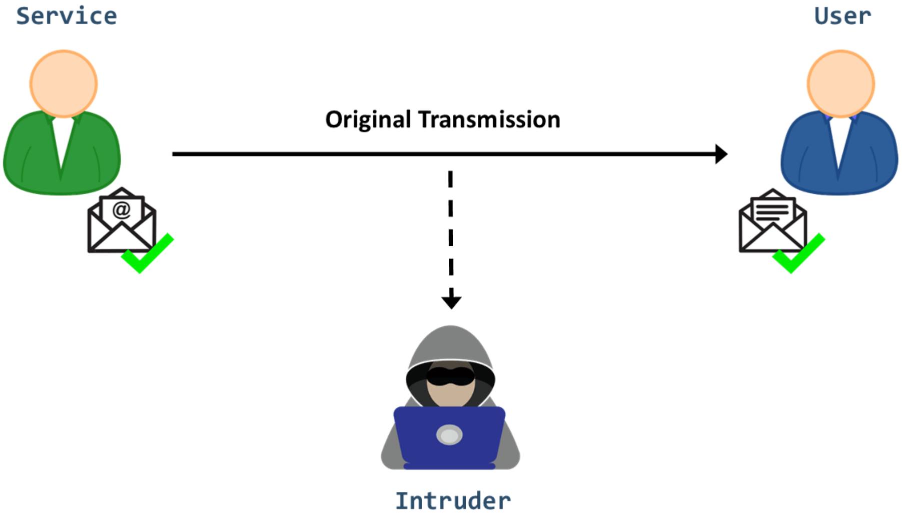


Figure 1.5: Interception attack [8].

Examples of such attacks include eavesdropping, which involves techniques like packet sniffing and man-in-the-middle (MITM). The main objective of an intruder in this type of attack is to obtain critical information such as passwords and credit card numbers or to disrupt data exchanges on the network. These attacks can be difficult to detect when executed successfully, as there may be little or no traces of the attack [8, 55].

3. **Modification**
   Modification is an attack against the integrity of the information. There are three types of modifications, see Figure 1.6.

   - Change: changing existing information that may already be present but inaccurate, to target either sensitive or public information.
   - Insertion: an insertion attack adds information that was not previously present, and can target historical data or information that has yet to be acted upon.
   - Deletion: deletion is the elimination of existing information.

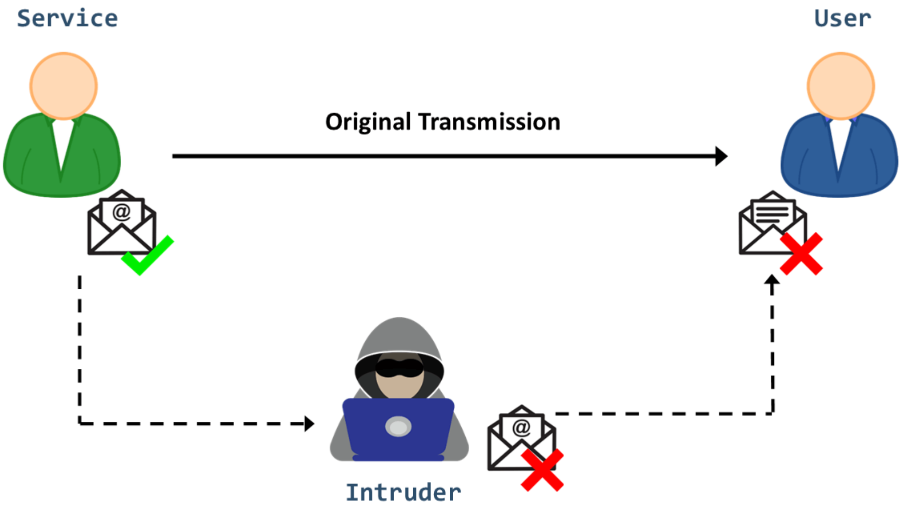


Figure 1.6: Modification attack [8].

For example, the man-in-the-middle attack (MITM) and Cross-Site Scripting (XSS) attack are two well-known methods of cyber attacks. In a MITM attack, the attacker can manipulate the system hardware, delete network messages or alter their content after intercepting data. Meanwhile, in an XSS attack, the hacker injects malicious scripts into a web application to modify its content or steal sensitive data [8, 55].

4. **Fabrication**
   When someone not authorized to access a system introduces fake items into it, it is an attack on the system's authenticity, see Figure 1.7.

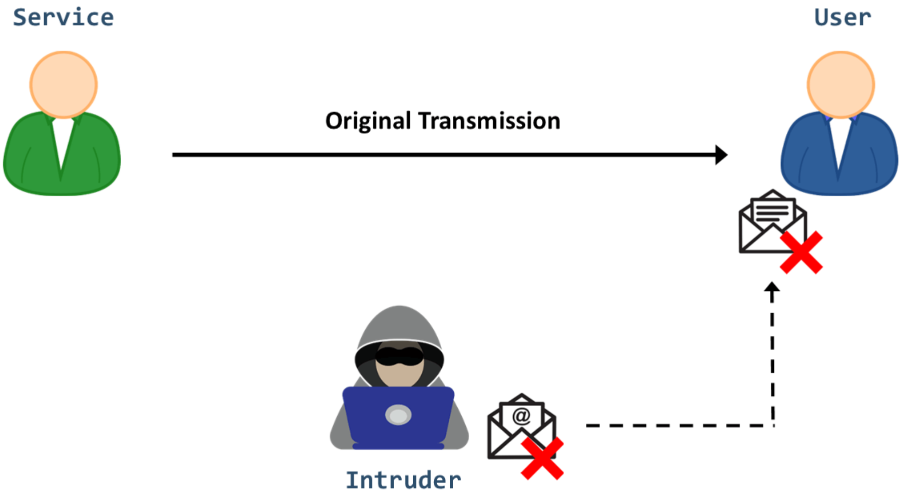


Figure 1.7: Fabrication attack [8].

For example, the act of fabrication occurs when an outsider introduces fraudulent information or misleading clues into a system. One example of this is when a hacker utilizes identity deception to create a fake version of a valid user, enabling them to engage in fraudulent activity or gain control of a bank account. Additionally, fabrication attacks can be executed using other methods, such as SQL injection and phishing [8, 55].

1.3.3 The Evolving Landscape of Cyberattacks and Its Impact on Companies

The environment of cyberattacks is evolving, getting more complicated and diverse. Attackers use a variety of strategies and approaches to achieve their objectives, and each form of assault provides its own set of obstacles for cybersecurity preventive measures. Cyberattacks can cause a variety of problems, including financial losses, reputational harm, and legal ramifications. These losses can be especially devastating for companies that rely significantly on digital infrastructure and customer data.

To deal with this growing threat, it is crucial to put strong security measures and prevention protocols in place.

1.3.3.1 Last five years

The chart in Figure 1.8 includes yearly and aggregated data for complaints and losses over the years 2018 to 2022. Over this time, the IC3 received a total of 3.26 million complaints, reporting a loss of $27.6 billion [9].

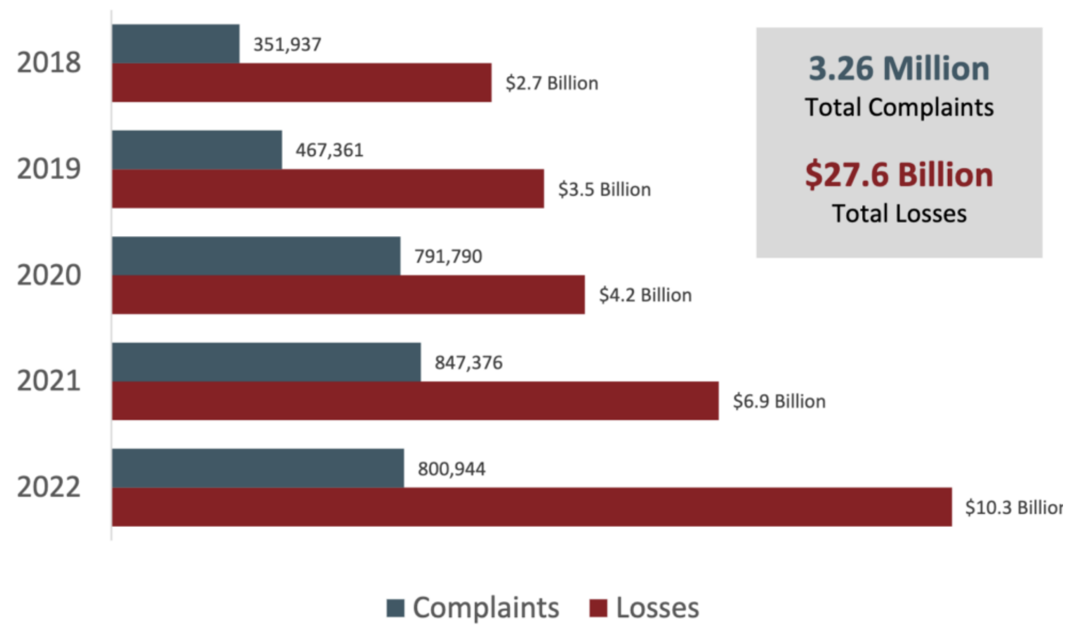


Figure 1.8: Complaints and losses over the last five years [9].

1.3.4 Solutions

1.3.4.1 Information systems security standards

- ITSEC (Information Technology Security Evaluation Criteria): was proposed by the French government in 1991. ITSEC is a European standard that aims to assess the security of computer systems in terms of functionality, integrity, confidentiality, and availability [46].
- TCSEC (Trusted Computer System Evaluation Criteria): was proposed by the US government in 1983. TCSEC is an American standard for evaluating the security of computer systems in terms of confidentiality, integrity, availability, and authentication [56, 44].
- ISO (International Organization for Standardization): is an independent international organization that sets standards for various industries, including IT security. The ISO/IEC 27001:2013 standard establishes an information security framework for organizations and defines the requirements for the establishment, implementation, maintenance, and continual improvement of an information security management system (ISMS) [10].

The ITSEC, TCSEC, and ISO provide a framework for defining security requirements and measuring compliance with those requirements. These standards also allow organizations to establish a consistent security policy tailored to their specific needs.

1.3.4.2 Security policy

IT Security Policy is a type of security policy that identifies the rules and procedures for all individuals who access and use an organization's IT assets and resources. This policy provides clear guidelines and protocols to ensure that all individuals comply with security best practices and follow established procedures to safeguard sensitive information [11].

1.3.4.3 Defense mechanisms

A) **Intrusion Detection System (IDS) :** Is a monitoring tool, whether in the form of a software application or a device, it monitors the system or activities of the network for policy violations or malicious activities and generates reports to the management system, Figure 1.9.

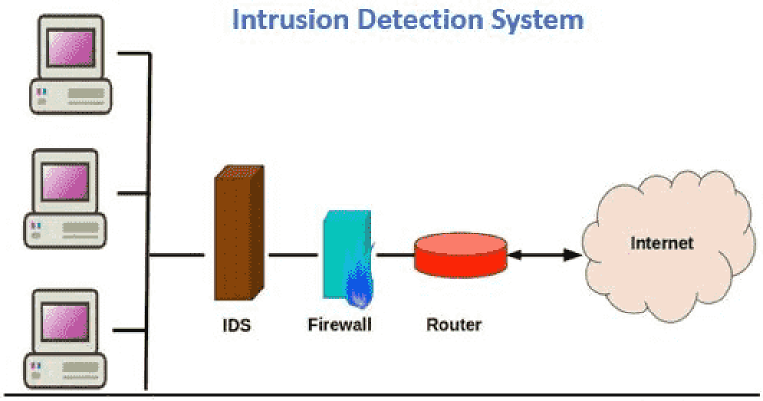


Figure 1.9: Intrusion Detection System [12].

Here are the two types of IDS technologies:

- Network Based: A network intrusion detection system (NIDS) is a type of IDS that operates by examining network traffic at all levels of the OSI model, it can analyze and make decisions about the nature of traffic, including identifying potentially suspicious activity that could indicate an attempted intrusion or attack.
- Host based: Host intrusion detection system (HIDS) is an intrusion detection system that monitors and analyzes the internals of a computer system, not just network packets on external interfaces. HIDS analyzes system-specific settings such as software calls, local security policies, and local log checks to detect potential security threats [53].

B) **Network Antivirus:** A network antivirus operates through a single dedicated network appliance, which is a hardware device that can protect any device that accesses your network. This means that instead of installing antivirus software on every individual device, you only need to install and maintain the antivirus on the network appliance [13].

C) **Antivirus:** An antivirus is a software that protects workstations or computer systems from computer infections. This software regularly monitors and analyzes all files and filters suspicious contents. If anomalies are detected, they will be notified and rejected. Most antivirus programs also include spam protection and can scan all incoming messages before they are delivered to their recipients [14].

D) **Intrusion Prevention System (IPS):** An IPS, Figure 1.10 is a system that automatically detects and thwarts computer attacks against protected resources. It examines communications in real time for attack patterns or signatures and blocks attacks once they have been detected. Unlike a traditional IDS, which focuses on reporting anomalies to the administrator, an IPS strives to automatically defend the target without direct administrator intervention. This protection can involve using signature-based or behavioral techniques to identify an attack and then block the malicious traffic or system call before it causes damage. In this regard, an IPS combines the functionality of a firewall and an IDS to provide a solution that automatically blocks offensive actions as soon as it detects an attack [15].

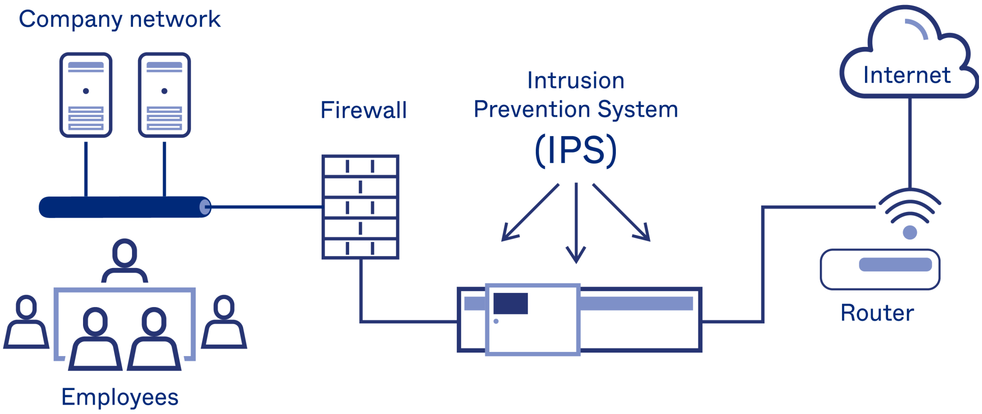


Figure 1.10: Intrusion Prevention System [15].

E) **Firewall:** A firewall, Figure 1.11 is a security system that can be either hardware or software or both. It acts as the first line of defense for a computer or application by preventing unauthorized access from hackers who may try to reach the computer through network traffic on the Internet or through other networks. The firewall also filters out viruses, worms, and other forms of malware. By creating a barrier between the computer and all its external communication channels, including both trusted and untrusted networks, the firewall helps to ensure that the computer remains secure and protected [16].

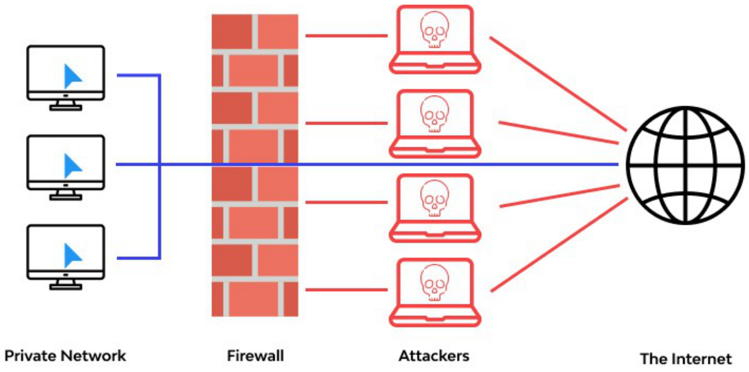


Figure 1.11: Firewall [16].

F) **Cryptography:** Is a security mechanism that involves transforming plain text data into an unreadable form, known as ciphertext, using mathematical algorithms and keys. Cryptography provides confidentiality, integrity, and authenticity of data. Cryptography can be used in two ways: symmetric key cryptography (the same key is used for both encryption and decryption) and asymmetric key cryptography (the public key is used to encrypt data, and a private key is used to decrypt the data) [17].

- SSL and TLS : SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols that provide a secure connection between a client and a server. They use a combination of symmetric and asymmetric cryptography to encrypt and authenticate data that is transmitted over the internet. This means that any information sent between the client and the server is kept private and secure, and can only be accessed by the intended recipient [54].

SSL and TLS are commonly used to protect web traffic, email, instant messaging, and other types of network communications.

G) **Virtual Private Network (VPN):** VPN, Figure 1.12 is a security mechanism that provides secure remote access to computer networks over the public Internet. The data transmitted through a Virtual Private Network (VPN) is encrypted using "tunnel" technology, making it inaccessible to other internet users. This encryption is facilitated by digital certificates which work like passports and must be present on both the remote computer and the server side. All certificates have a public and private key, and when a remote computer attempts to access the file, its public key is sent to the server, which also sends its public key, and a VPN connection is established, creating a tunnel where data is encrypted and decrypted through the certificate [45, 47].

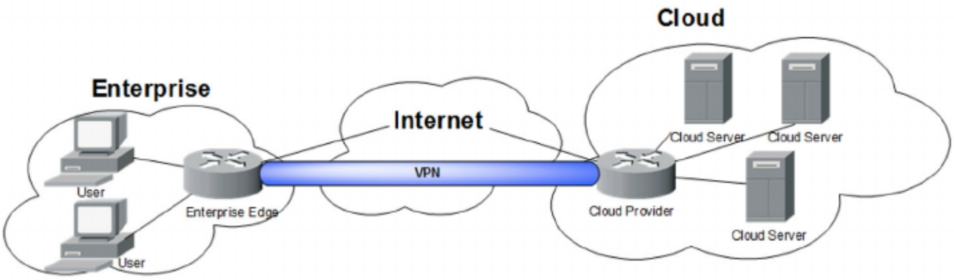


Figure 1.12: Virtual Private Network [50].

1.4 Security Benefits and Monitoring Logs Activities

Log files serve as the main source of data for network observability. They are computer-generated files that provide details about usage patterns, activities, and operations within various devices such as operating systems, applications, servers, and more.

Effective monitoring of event logs plays a critical role in safeguarding the security of computer systems, networks, and applications. Not only does it provide valuable insights into the system's overall functionality, but it also sheds light on the system's health. Analyzing event logs enables organizations to promptly identify potential security breaches, pinpoint any weaknesses or vulnerabilities, ensure adherence to relevant regulations and standards, conduct forensic investigations, and keep audit trails up-to-date. Overall, monitoring event logs is a crucial practice for maintaining the security and integrity of computer systems [18, 51].

1.5 Security Monitoring Logs and SIEM Approach:

There are multiple methods for monitoring data and mitigating security threats, but one particularly robust approach is Security Information and Events Management (SIEM). This solution is highly comprehensive and effective, making it an ideal tool for achieving the ultimate goal of security monitoring. By delivering real-time updates on system and network activity, SIEM equips IT teams with valuable insights that can aid in safeguarding against potential risks. Given the focus of this thesis, SIEM is of particular interest as a solution worth exploring [42].

Conclusion

Safeguarding information systems and protecting organizational data requires a comprehensive and proactive approach. By understanding the key concepts and implementing robust security measures discussed in this chapter, organizations can strengthen their security posture and mitigate risks effectively.

Chapter 2

Security Information and Events Management

2.1 Introduction

The SIEM (Security Information and Event Management) is critically important in a security of information systems context because the SIEM system is responsible for collecting and analyzing security-related data from various sources across an organization's Information technology infrastructure.
A SIEM system's ability to provide an accurate and complete picture of an organization's security posture relies on the security of the underlying information systems.

This chapter explores the evolution of computer-based security management, focusing on the major advances of SIM (Security Information Management) and SEM (Security Event Management). We will see how these tools have evolved into the SIEM (Security Information and Event Management) we know today. We will discuss the main features of SIEM, such as log management, event correlation, security analysis, and reporting. In addition, we will also provide an overview of some SIEM solutions currently available on the market. We will explore the strengths and weaknesses of each solution, and guide how to select the best SIEM solution for the organization's specific needs.

2.2 SIEM Evolution

2.2.1 History

The evolution of SIM, SEM, and SIEM reflects the increasing complexity and variety of security threats, the growing volume and variety of security data, and the need for more advanced analytics and automation capabilities to support them effectively. Incident response has been a key factor in the evolution of these solutions. In chronological order, first SIM appeared in the 1990s then after a decade SEM emerged in the 2000s [19].

SIEM (Security Information and Event Management) solutions have been around for over 15 years, but today's modern SIEMs have evolved from their predecessors. The term "SIEM" was coined in 2005 by Mark Nicolett and Amrit Williams in a Gartner research report entitled "Improving IT Security with Vulnerability Management". Today's SIEMs are an evolution of SIM and SEM that have integrated their capabilities while adding more advanced analysis and automation features [13].

2.2.2 Security Information Management (SIM)

2.2.2.1 Definition

SIM, or Security Information Management, is a set of automated tools for the collection and long-term storage of log files, as well as for the analysis and reporting of log data. SIM is often associated with log file management, as it allows log files to be collected from various sources and stored in a centralized location. SIM solutions are usually based on agents that run on the servers and computers being monitored. These agents relay security information and log files to a centralized SIM server, where system administrators can log in and run real-time security reports in graphical and tabular form. Some SIM solutions incorporate local filters to normalize, query, and clean up log files before they are transmitted to the centralized SIM server. This reduces the amount of data sent over the network, which can cause bandwidth congestion, and the amount of data stored on the SIM server, which can quickly consume disk space. However, these filters must be applied in a way that does not impede the ability to reconstruct the state of the system that triggered a security incident [20].

2.2.2.2 Log files

1. **Definition**
   Log files are records of activities, messages, and events taken by programs, operating systems, and other applications. They are employed to monitor and examine system activity, discover issues, and do troubleshoot. It enables analysis of a process's internal activity hour by hour or minute by minute. Errors, status updates, and other information regarding system activities can all be found in logs. The most recent occurrences are typically found near the end of text files that are stored in chronological order [21].

2. **Log Format**
   A log format refers to a set of rules that dictate how log file content should be interpreted. These guidelines determine the record structure, encoding, and delimitation. Depending on the system or application for which it is used, the format may differ but generally conforms to a standardized format for easy user analysis. It may define various aspects, such as whether the content is structured or unstructured, whether the data is binary or plain text, and the type of encoding applied. Additionally, the format may specify record delimitation methods used to separate individual records in the log file. A log file typically includes a timestamp, user information, and event information. The timestamp allows for chronological sorting of log entries, while the user information includes the user identifier, the IP address, or the device type of the user who triggered the event. The event information provides details of the action performed, such as a login attempt, an error message, or a transaction request. It may also include additional information, such as the HTTP status code, bytes served, user agent, web page referenced, or other relevant data points, useful for troubleshooting and identifying the root cause of problems [22].

3. **Utility of log files**
   Log files are an important tool for monitoring and analyzing the behavior of applications and systems, it helps to ensure their reliability, security, and performance [57].

4. **Type of log files**
   A variety of log files are used in computer systems and applications, each serving a specific purpose. Some of the most common types include [21]:

   - Event logs: These high-level logs track network usage and traffic statistics, such as login attempts, unsuccessful password attempts, and application events.

- Server logs: These text files keep track of all activity involving a specific server over a given period.
- System logs (Syslogs): These logs record occurrences in the operating system, including starting messages, system modifications, unforeseen shutdowns, errors, and warnings. They are produced by Windows, Linux, and macOS systems.
- Access logs and authorization logs: These logs include a list of users and bots who have accessed particular programs or files.
- Change logs: These logs provide a timeline of modifications made to a program or file. Availability logs: These logs monitor system availability, uptime, and performance.
- Resource logs: These logs reveal details about connection problems and capacity restrictions.
- Threat logs: These logs are records of system, file, or application traffic that a firewall detects as matching a specified security profile. They help to identify potential security threats to the system.

2.2.3 Security Event Management (SEM)

2.2.3.1 Definition

Security Event Management (SEM) quickly identifies potential security breaches and alerts responsible parties. it's a technology used for real-time monitoring and correlation of system events and alerts, to identify threats, vulnerabilities, and risks. SEM improves upon Security Information Management (SIM). Typically, data is relayed from host computers to a central repository using protocols like SNMP and Syslog, where events and alerts are stored securely. Security algorithms and statistical calculations are used to analyze the information and identify significant entries that warrant attention, such as administrator logins outside of working hours. SEM allows for centralized monitoring, making it easier to detect events that impact multiple systems [23].

2.2.4 Security information and event managements(SIEM)

2.2.4.1 Definition

Security Information and Event Management (SIEM) software works by collecting log and event data from applications, devices, networks, infrastructure, and systems to provide a comprehensive view of an organization's information technology (IT). These solutions can be deployed on-premise or in the cloud. By analyzing all data in real time, SIEM solutions use statistical rules and correlations to provide actionable information for forensic investigations. SIEM technology examines all data, sorting threat activity according to its level of risk to help security teams quickly identify malicious actors and mitigate cyber-attacks. By using SIEM technology to gain visibility into network activity, organizations can address issues before they become a significant risk [24, 25].

2.2.5 The architecture of SIEM

A SIEM, or Security Information and Event Management, is a system consisting of interconnected steps that operate sequentially, with each step relying on the successful completion of the preceding step. Consequently, any failure in a step will fail in all subsequent steps.
A SIEM is divided into six fundamental steps as displayed in Figure 2.1.

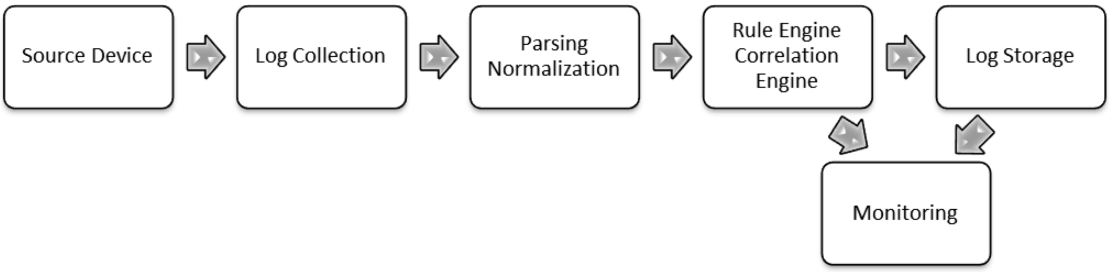


Figure 2.1: SIEM basics components [26].

1. **Source device:** The "source device" is the initial component in a SIEM framework that can be a device, an application, or any data that is storable and processable by a SIEM. Typically, source devices provide various logs, such as operating systems logs that document system interactions, appliance logs for routers and switches, and application logs that detail interactions within the application [26, 48].

2. **Log collection:** The Log Collection stage involves extracting logs from source devices, which can be accomplished through two distinct methods. The Push Method involves sending logs from the source device to a receptor on the SIEM side, often by redirecting the Syslog from the machine to the SIEM receptor. In contrast, the Pull Method requires the SIEM to initiate a connection to the source device to retrieve the logs from a network pathway. This method has a drawback, as logs must be obtained periodically instead of real time, as in the Push Method [26, 48].

3. **Parsing normalization:** During the Parsing Normalization phase, the obtained logs undergo standardization to enable the SIEM to understand and analyze the log entries. This process also enhances human comprehension of the log contents [26, 48].

4. **Rule/Correlation Engine:** During the Rule Engine sub-phase, rules are established and applied to the normalized logs, which influence the SIEM alerts. For instance, if a user authenticates to a machine with "root" access, a rule can be created to detect this event and generate an alert [26, 48].

5. **Log Storage:** The Log Storage phase involves retaining all SIEM-processed logs for future access if necessary. The processed logs can be stored in three ways: database, text file, or binary file. Storing logs in databases, like Oracle

or MySQL, is the most common method, but it requires additional administration. Text file storage has the benefit of being human-readable, but it necessitates a delimiter between log parameters and is not scalable. Binary files, which are only accessible within the SIEM, are advantageous for scalability because they enable fast read/write operations and efficient memory usage [26, 48].

6. **Monitoring:** The final phase of a SIEM architecture is monitoring, where the SIEM interacts with stored logs and presents the obtained information in an interface. The interface may be web or application-based and is used to manage the SIEM, providing a unified view of the environment [26, 48].

This cyclical process continues as long as the SIEM system is in use, helping to continuously monitor and improve the organization's security posture.

2.2.5.1 SIEM functions

SIEM, or Security Information and Event Management, has been around for over a decade. Previously, SIEMs required meticulous management throughout the entire data pipeline, including data ingestion, policy implementation, alert review, and anomaly analysis.

SIEM functions by gathering log and event data from various sources such as host systems, networks, security devices, and applications. Agents are deployed across the organization's technology infrastructure to collect all the data and centralize it on a single platform. SIEM software identifies network anomalies, antivirus events, security incidents, and firewall logs and sorts them into categories, such as successful and failed logins, malware activity, and other potential threats. When the software detects events that may pose a risk to the organization, it generates alerts to signal a possible security problem. Alerts can be configured with different levels of priority based on predefined rules. Administrators can set rules and thresholds to define what type of anomaly is considered as a security incident [24].

2.2.6 Comparison of SIM, SEM, and SIEM

SIM, SEM, and SIEM are all related to security event management, but they differ in their focus and capabilities.

The main difference is that in SIM, the device only collects data from a log, which can include different forms of data. Technologies are increasingly focusing on particular types of events in SEM. It is possible to imagine systems created specifically to monitor high-level management access, suspicious authentications, and account logins at specific times.

Technologies that combine SIM and SEM are called SIEM. Here we have to distinguish between general information monitoring and event monitoring. Another important approach to differentiate the two is to consider SIM as a longer or broader process that allows for the methodical analysis of larger and more varied data. In contrast, SEM again focuses on individual user event types that can serve as warning signals or provide managers with specific information about network activities [27].

2.3 SIEM Benefits

SIEM solutions provide a powerful method of threat detection, real-time reporting, and long-term analytics of security logs and events. This tool can be incredibly useful for safeguarding organizations of all sizes.

Here are some benefits of SIEM [24]:

- Increased security: SIEM solutions help organizations to detect and respond to security threats in real time. By monitoring security events across the organization, SIEM can identify potential threats and provide actionable insights to security teams to respond to them.
- Improved compliance: Many organizations are required to comply with regulations. SIEM can help organizations to meet compliance requirements by providing audit trails and logs of security events.
- Centralized monitoring: SIEM provides a centralized view of security events across the organization. This enables security teams to identify patterns and trends in security events that may not be apparent when viewing individual events in isolation.
- Faster incident response: SIEM can automate the incident response process by providing alerts to security teams in real time. This enables security teams to respond to incidents faster and reduce the time it takes to mitigate the impact of a security breach.
- Cost savings: By automating many security-related tasks, SIEM can reduce the cost of managing security operations. It can also help organizations identify and prioritize security-related risks, enabling them to allocate resources more effectively.

2.4 Presentation of some SIEMs solutions

Many SIEM solutions are available on the market today, each with unique features and functionality, to make it easier to compare these solutions, Table 2.1 summarizes the most promising SIEMs to date.

SIEM Solution	**Operating System**	**Advantages**	**Disadvantages**
		paid solutions	
Splunk Enterprise Security [28, 29]	Windows, Linux, Unix, macOS	Highly customizable, easy integration with other tools, user-friendly interface, powerful data analytics, excellent dashboard, effective large data analysis	Expensive, designed for large companies
IBM QRadar [28, 29]	Linux	Advanced analytics and threat detection, excellent scalability, comprehensive reporting	High initial cost, steep learning curve
LogRhythm [28, 29]	Windows, Linux	Advanced threat detection, automated response, easy-to-use interface	Expensive, limited scalability
		free solutions	
Elastic Stack (ELK Stack) [28]	Windows, Linux, macOS	Highly customizable, flexible, excellent visualization capabilities	Requires significant technical expertise to set up and maintain
OSSIM [49]	Linux	Comprehensive security features, easy-to-use interface, customizable dashboards	Limited scalability, less support compared to paid solutions
Graylog [28]	Linux	Easy to use interface, high customizability, strong community support	Limited scalability, less advanced features compared to paid solutions

Table 2.1: Comparison of different SIEM solutions

2.5 The choice of SIEM solution

Each SIEM solution has its unique set of pros and cons. Ultimately, the selection of a SIEM solution depends on individual requirements and budgetary constraints. After evaluating and comparing multiple SIEM solutions, in this project for the implementation of a SIEM solution for the supervision of the IS, we have chosen Splunk, which is a well-established and highly-regarded SIEM solution that offers numerous benefits.

And here are some of its advantages over other solutions [30] :

- Scalability and Ease of Implementation: Splunk can handle large volumes of data and process it quickly, making it highly scalable. Additionally, it is easy to implement and can be deployed quickly and easily.
- Interactive Analytics Reporting: Splunk enables users to explore data easily and find trends and patterns using interactive charts, graphs, and tables. Users can also create custom dashboards to visualize their data.
- Automatic User Information Discovery: Splunk can quickly identify user information and extract useful information from different data sources.
- Search Saving and Sharing: Splunk allows users to save customized searches for future use and share them with other users, making it easy to find and analyze the data they need.

2.6 Splunk

2.6.1 Definition

Splunk, (Splunk Logo, Figure 2.2) is a software application that helps organizations to search, monitor, and analyze data from any source. It is an exceptional tool for big data analysis, especially where there is a lot of machine data to be analyzed. Splunk collects machine data from various sources and enhances its searchability through intelligent search capabilities. It can be used for tasks such as data visualization, report generation, and data analysis, enabling IT teams to improve overall efficiency based on insights obtained from the data [31, 30].

Figure 2.2: Splunk Logo.

2.6.2 Splunk components

Splunk is made up of three major components, Figure 2.3:

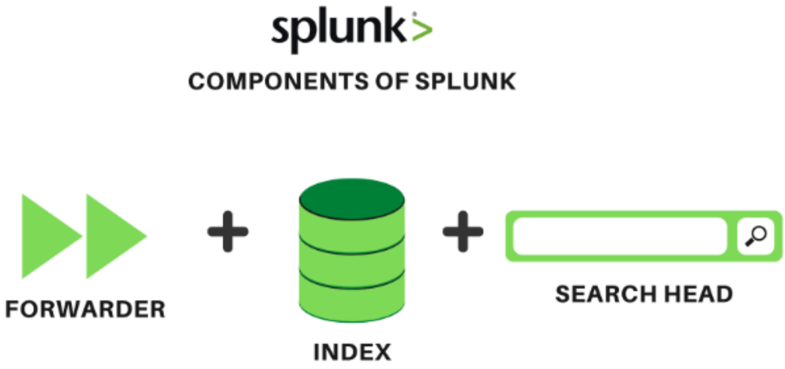


Figure 2.3: Splunk components [32].

1. Splunk Forwarder is a data forwarding tool.
2. Splunk Indexer, which is used for data parsing and indexing.
3. Search Head is a graphical user interface (GUI) for searching, analyzing, and reporting.

2.6.2.1 Splunk forwarder

Splunk forwarder is a tool that allows for real-time data collection from various sources, including remote systems. It can be configured to send this data in real time to a Splunk indexer, enabling users to analyze the data in real time using Splunk. The Splunk forwarder is also efficient in terms of processing power and can be easily scaled to meet increased data collection needs.

There are two types of forwarders:

- Splunk Universal Forwarder: The universal forwarder is a simple Splunk component designed to send raw data collected at the source to an indexer with minimal processing. It allows straightforward data transfer and can help avoid performance overheads caused by the forwarding of unnecessary data. Unlike some other tools on the market, the universal forwarder does not process incoming data streams extensively, making it an efficient solution for forwarding data [33, 31].
- Splunk Heavy Forwarder : The heavy forwarder, Figure 2.4 is a Splunk component that can solve data processing challenges by performing some data processing at the source before forwarding it to the indexer. Typically, a heavy forwarder will parse and index data at the source, which helps reduce the amount of unnecessary data that is forwarded and ultimately saves bandwidth and storage space. By parsing the data before forwarding, the heavy forwarder ensures that the indexer only has to deal with the indexing segment of the data, making it an efficient tool for handling large volumes of data [33, 31].

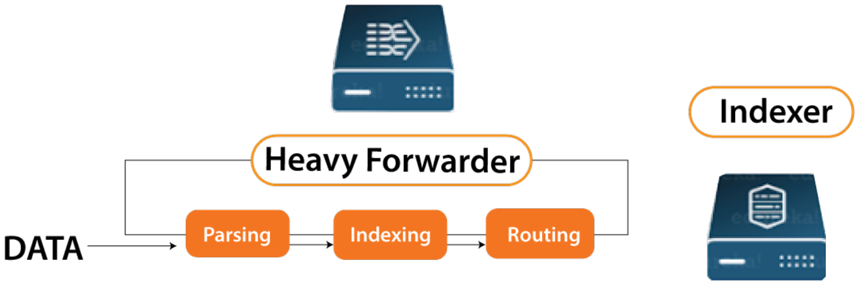


Figure 2.4: Splunk heavy forwarder [33].

2.6.2.2 Splunk Indexer

The Splunk indexer is a tool used for indexing and storing data that is fed from forwarders. Its primary purpose is to convert data into events and index it for efficient search operations. When data is received through the Universal Forwarder, the Splunk indexer first parses the data to eliminate unwanted data before indexing it. When data is received through the Heavy Forwarder, the Splunk indexer only indexes the data. The Splunk indexer stores data in compressed raw data, indexes pointing to raw data, and metadata files, which are stored in buckets - collections of directories. One of the benefits of using Splunk indexer is data replication, which ensures that multiple copies of indexed data are stored to prevent data loss. This process is referred to as indexer clustering or index replication [31].

2.6.2.3 Splunk Search Head

The Splunk Search Head, Figure 2.5 is a component that provides users with a graphical user interface for interacting with Splunk. Users can enter search terms to search and query data indexed by the Splunk Indexer, and receive the expected results. The search head can be installed on the same server as other Splunk components or on a separate server, and enabling it involves enabling the Splunk web service on the Splunk server. Within a Splunk instance, a search head can send search requests to a group of indexers, or search peers, who perform searches on their indexes. The search head combines the results and returns them to the user, using a distributed searching technique that provides faster data search. Search head clusters are groups of search heads that work together to coordinate search operations. The cluster assigns jobs based on current loads and ensures that all search heads have direct access to the same collection of objects [31].

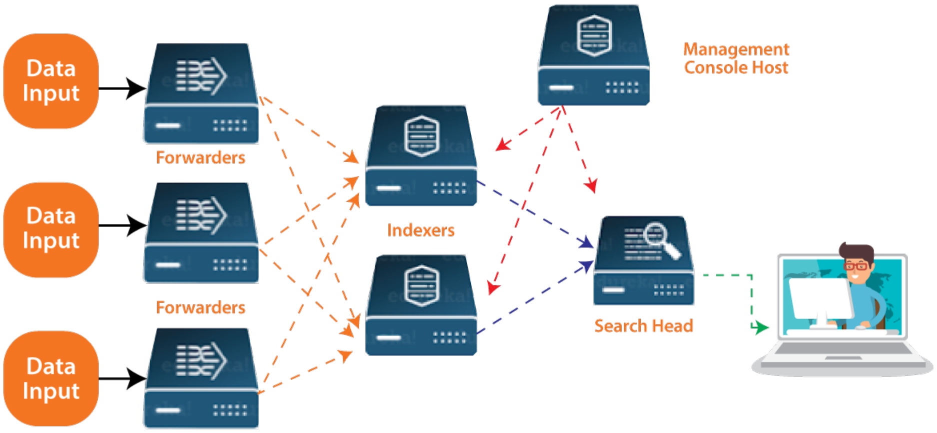


Figure 2.5: Splunk Architecture [33].

2.6.3 Splunk Architecture

The architecture of Splunk in Figure 2.5 shows how Splunk works from beginning to end. The diagram show cases of multiple remote Forwarders that send data to the Indexers.

The Search Head provides various functionalities such as searching, analyzing, visualizing, and generating knowledge objects for Operational Intelligence based on the data in the Indexer. The Management Console Host acts as a centralized configuration manager, distributing configurations, app updates, and content updates to Deployment Clients. Forwarders, Indexers, and Search Heads are all Deployment Clients in this architecture [33].

Conclusion

This chapter explored the various facets of Security Information and Event Management highlighting its importance as a critical component of contemporary cybersecurity practices. It discussed the obstacles that organizations face when deploying and administering their systems and their vital role in protecting an organization's assets, data, and reputation from ever-increasing cyber threats. Ultimately, it is clear that SIEM is an indispensable tool in mitigating the risks posed by cybercrime in today's digital landscape.

Chapter 3

Internship Host Organization

3.1 Introduction

After presenting the concepts related to our thesis in the previous parts, we dedicate this chapter to introduce the host organization, SONELGAZ, specifically Bejaia distribution concession BDC. We will also discuss the role of the IT Systems Management Division in this process and then analyze its deployment such as handling tasks related to system administration, monitoring, and change management. Then we will identify the limits and issues with the current deployment which will help us to come up with an approach to realize our migration.

3.2 General presentation of Sonelgaz

SONELGAZ (acronym of Société Nationale de l'Électricité et du Gaz), is an Algerian industrial energy group, specializing in the production, transport, and distribution of electricity, as well as the purchase, transport, and distribution of natural gas. Its head office is located in Algiers [34].

Figure 3.1: Logo of Sonelgaz [34].

3.2.1 History

Sonelgaz was created in 1969 to replace EGA, a company created in 1947 to monopolize these activities. Since its creation, Sonelgaz has expanded its activities to include the installation and maintenance of electrical and gas appliances, as well as the promotion of the use of these energies in the industrial, craft, and domestic sectors. In 1995, the company became a public enterprise of an industrial and commercial nature, before becoming a joint stock company in 2001 to allow for an expansion of its activities. Since then, it has become a major national investor and a group of industrial subsidiaries, with 39 subsidiaries and 5 joint ventures. The main subsidiaries are responsible for the generation, transmission, and distribution of electricity and the transmission and distribution of gas through pipelines [34].

3.2.2 Mission of Sonelgaz

Sonelgaz's mission is to distribute electricity and gas by pipeline, and to operate, maintain and develop the electricity and gas distribution networks while respecting the required safety standards. It must also connect and manage new customers promptly, ensure continuity and quality of service, and comply with environmental protection legislation. In addition, Sonelgaz must take into account the strategic orientations and policies defined, ensure that the public service missions are in line with the commitments made with the public authorities, and meet customer satisfaction and environmental protection requirements. It must market electricity and gas under the best conditions of quality, safety, and at the lowest cost, develop and offer energy services in the fields of electricity and gas, and achieve economic objectives by improving management, seeking greater synergy, and controlling costs [34].

As part of my end-of-study internship, I had the opportunity to work for Sonelgaz, a company based in [Bejaia/Algeria], which will be further presented in the following section.

3.3 Bejaia Distribution Concession (BDC)

The Bejaia Distribution Concession (BDC), is responsible for distributing electricity and gas to customers and ensuring the quality and continuity of service. The concession is located in the city of TOBAL and plays a crucial role in the efficient supply of electricity and gas to customers.
The distribution department of BDC is responsible for various functions, including operating, maintaining, and developing the electricity and gas distribution networks. The department also handles marketing activities related to electricity and gas, ensuring quality and continuity of service throughout the concession area, and ensuring the safety of the installations.
In addition, the department is responsible for handling customers' connection requests in the most cost-effective and timely manner possible, with the ultimate goal of satisfying their needs and ensuring their satisfaction.

3.3.1 General organizational chart for the Distribution Department of Electricity and Gas in Béjaïa

The organization chart illustrated in Figure 3.2 summarises the general organization of the Bejaia Electricity and Gas Distribution directorate.

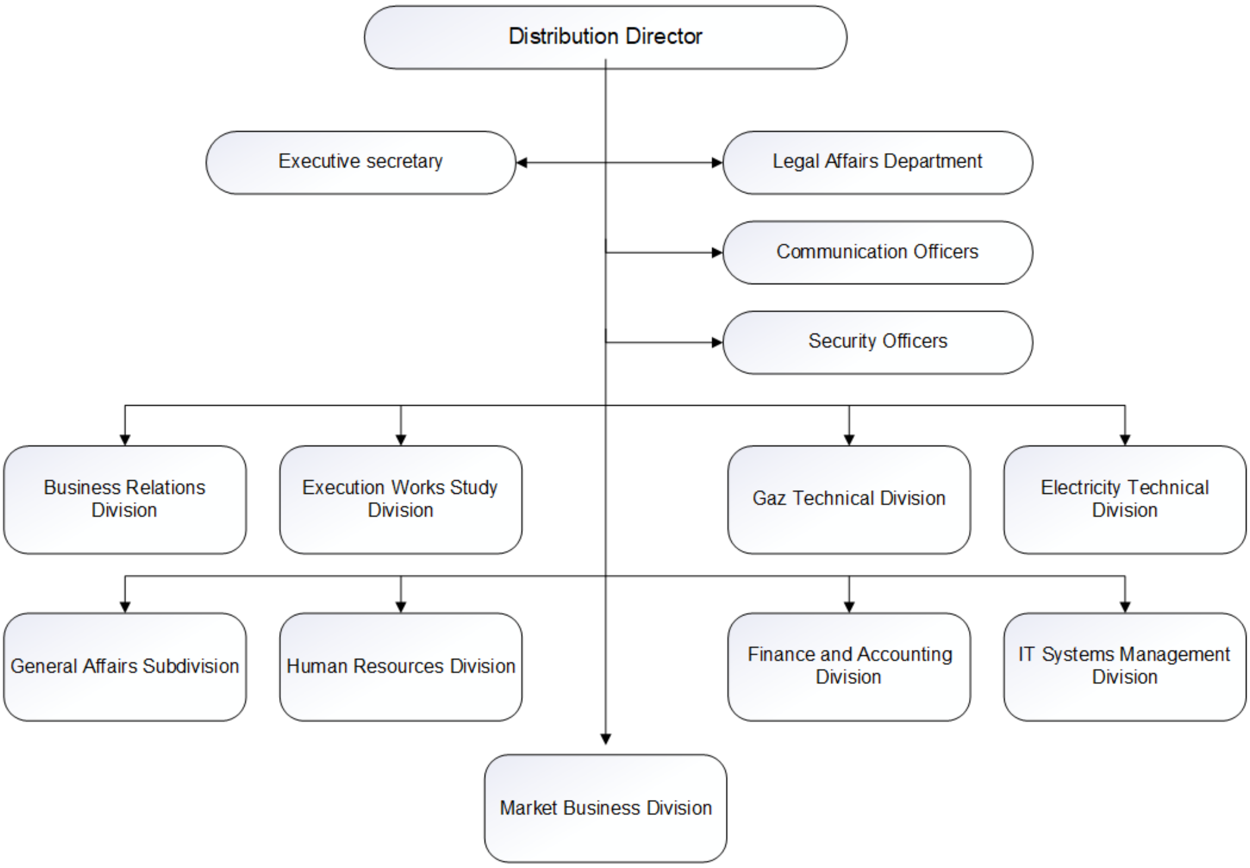

Distribution Director
Executive secretary
Legal Affairs Department
Communication Officers
Security Officers
Business Relations Division
Execution Works Study Division
Gaz Technical Division
Electricity Technical Division
General Affairs Subdivision
Human Resources Division
Finance and Accounting Division
IT Systems Management Division
Market Business Division

Figure 3.2: Organization chart.

3.3.2 IT Systems Management Division (ISMD)

ISMD is a key service within the BCD, responsible for overseeing the movement of IT equipment and ensuring effective and efficient allocation to the various services. Its role is crucial in ensuring that all departments in the BCD have the equipment they need to perform their functions effectively, while at the same time ensuring that the movement of IT equipment is managed optimally.

3.3.2.1 IT systems management division activities

Sonelgaz Bejaia's IT systems management division is in charge of various activities that aim to ensure the smooth running of the company's IT systems. First of all, it manages the BT/BP billing groups, closely following the billing and collection schedule designed for this purpose. This task is crucial to ensure the satisfaction of Sonelgaz customers by providing them with accurate and timely invoices.

In addition, this division is responsible for maintaining Sonelgaz's IT networks, ensuring they are functional and accessible at any time. It also ensures the maintenance of systems, including databases, to ensure the continuity of the company's activities.

Finally, the division is responsible for managing Sonelgaz Bejaia's computer center and promoting the systems to distribution management. Working closely with the company's other departments contributes to the optimization activities and the improvement of the quality of services offered to Sonelgaz customers.

3.3.3 Analyzing the deployment architecture

Figure 3.3 shows the network infrastructure of Bejaia Distribution:

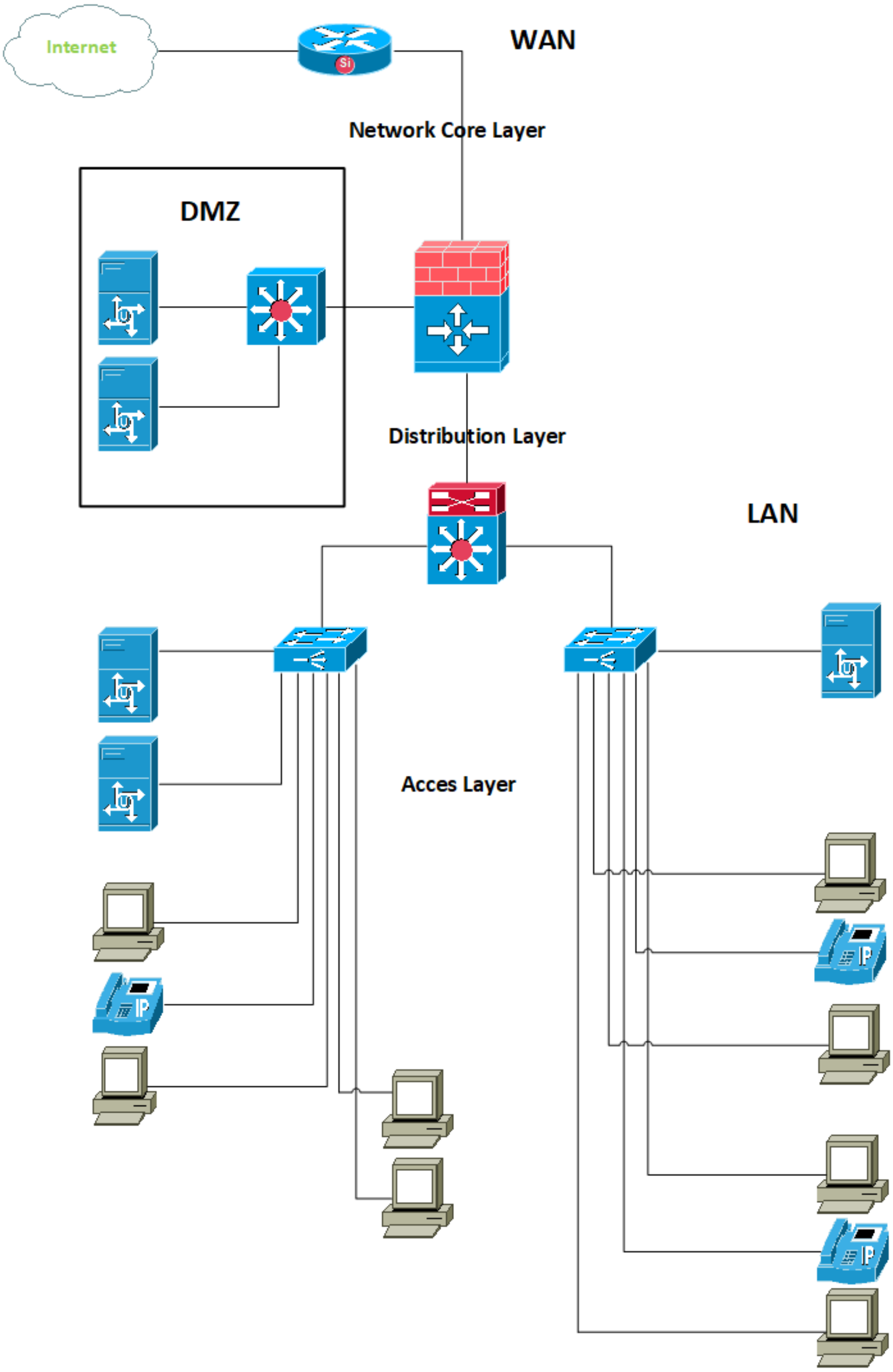


Figure 3.3: BCD LAN Architecture.

This network is designed in a hierarchical model, i.e. it is divided into 3 layers as follows:

1. **Access layer**
    - Serves as an interface for end devices.
    - Controls which devices are allowed to communicate on the network.
    - Includes switches, bridges.
2. **Distribution layer**
    - Aggregates data received from access layer switches for routing to the final destination.
    - Manages the flow of network traffic using policies.
    - Delimits broadcast domains via routing functions between defined VLANs at the access layer.
3. **Network Core Layer**
    - Constitutes the high-speed backbone of the inter-network.
    - Essential for interconnectivity between distribution layer devices.
    - Aggregates traffic from all distribution layer devices,
    - Capable of rapidly forwarding large amounts of data.

3.3.3.1 Analysis of computer park

I. **Hardwar analysis**

The local computer network of the Bejaia distribution department is composed of:

(a) Two network racks

- Ground floor rack, containing 3 stacked switches that have been illustrated by a single switch. It covers the IT, commercial and electrical divisions.
- The first-floor rack contains 5 stacked switches covering the second and third-floor offices.

They contain the types of switches defined in Table 3.1:

Switch type	**Description**
DELL N3024P	24-port Gigabit Ethernet switch that provides Power over Ethernet (PoE) capabilities to power devices such as wireless access points, IP phones, and cameras
DELL N3024F	24-port Gigabit Ethernet switch that is non-PoE, meaning it does not provide Power over Ethernet capabilities for powering devices such as wireless access points or IP phones

Table 3.1: Table of DELL N3024 switch types [35].

DELL EMC NETWORKING N3000 SERIES SWITCHES
The N3000 switch series offers a power-efficient and resilient Gigabit Ethernet (GbE) switching solution with integrated 10GbE uplinks for advanced Layer 3 distribution for offices and campus networks. The series has high-performance capabilities and wire-speed performance utilizing a non-blocking architecture to easily handle unexpected traffic loads [35].

(b) Cisco 2600 Router: The Cisco 2600/2600XM series family of modular multiservice access routers provides flexible LAN and WAN configurations, multiple security options, voice/data integration, and a range of high-performance processors. This range of features makes the Cisco 2600/2600XM family the ideal branch-office router for today's and tomorrow's customer requirements [36].

(c) IP telephony: Avaya IP500 V2 is a popular IP telephone system used in many organizations for managing their voice communication needs. It is a highly scalable and flexible system that can support up to 384 telephones and 8 T1/E1 trunks [37].

II. **Software analysis**

(a) Servers: In the computer network of Sonelgaz, the distribution concession of Béjaïa, several types of servers are present, including:

i. **Database server:** It is responsible for storing, managing, and providing secure access to data. Database servers enable efficient data management and manipulation, as well as the execution of queries and transactions.

ii. **Application server:** provides a runtime environment for software applications. It hosts and executes applications, offering services such as session management, access to databases, query processing, and communication with other systems.

iii. **Communication server:** manages communications between different devices or systems. It handles routing, transmission, and exchange of data between users or machines. Communication servers can support functionalities such as telephone calls, email, video conferencing, chat services, etc.)

iv. **File server:** A file server is a system that stores and shares files with other computers or users within a network. It facilitates centralized storage of files and enables secure and controlled access to these files. File servers provide features such as access rights management, data backup, version control, and file collaboration.

III. **Security analysis**
"Sonelgaz" regards security as a major privilege and employs advanced security techniques such as:

(a) Firewall: Fortinet's FortiGate is equipped with a Firewall-FortiOS module, which is an essential component of the FortiOS suite for strengthening the security of corporate IT networks. Firewall-FortiOS plays a critical role in blocking unauthorized access, but it also faces growing challenges such as the emergence of new threats and evasion techniques, as well as diversification of access methods and increased data volume. Fortinet is the pioneer in securing networked IT systems, providing the perfect convergence to make your system fit any location: remote office, branch office, campus, data center, and cloud. FortiGate is at the heart of FortiOS everywhere and provides deep visibility and security in a range of formats, including container firewalls, virtual firewalls, and security appliances [38].

(b) Anti-virus: Anti-virus Symantec endpoint Security is installed at SONELGAZ. Symantec is renowned for its flagship product, Symantec Endpoint Protection. This leading security suite offers comprehensive protection against all kinds of online threats such as viruses, malware, spyware, phishing attacks, and more. Symantec uses innovative technologies to reduce the attack surface, prevent attacks, breaches, and detect intrusions, all powered by one of the world's largest intelligence networks. This all-in-one solution from Symantec offers flexible management and deployment, including a fully cloud-based, on-premise, or hybrid solution, for maximum protection of traditional and mobile enterprise devices [39].

3.3.4 Critics about the current deployment

In the context of our study, it was identified that Sonelgaz faces several criticisms and challenges:

1. Limited Visibility: The organization lacks centralized visibility into security events, making it difficult to monitor and detect threats in real time, leaving the organization vulnerable to undetected attacks or breaches.

2. Manual Log Analysis: Manual log analysis is necessary, leading to time-consuming and inefficient processes. It becomes challenging to identify patterns or anomalies promptly, increasing the risk of delayed or missed detection of security incidents.

3. Compliance and Regulatory Challenges: Industry regulations require proper log management and incident response capabilities. meeting these requirements becomes difficult, resulting in potential non-compliance penalties and legal consequences.

3.3.5 Proposed Solution

To address the challenges and issues in the current deployment, it is crucial to implement a Security Information and Event Management (SIEM) system using the Splunk tool. Splunk is a powerful and widely used SIEM solution that can help in centralizing and analyzing security events and logs from various sources.

Implementing such a system would enhance the security of Sonelgaz's networks and data by enabling real-time threat detection and efficient incident response to various types of intrusions, cyber threats, and misfunctions. Splunk would allow for the consolidation of information from diverse sources to gain an overall view of the situation, facilitating the identification and resolution of security issues.

3.3.5.1 Monitoring of modules

To test our solution, we will select a few specific equipments on which we will conduct our tests and configurations. The selected types of equipment will serve as representative samples for validating the effectiveness and functionality of the implemented SIEM system using Splunk. These tests will help us ensure that the system performs as expected and meets the desired security objectives.

1. **Firewall**
   For testing purposes, we will choose a specific FortiGate firewall. This firewall will be closely monitored to gain real-time insights into network traffic, identify rule violations, detect intrusion attempts, and observe other critical security events.

2. **Cisco Router**
   Supervising the Cisco router to evaluate its performance in effectively routing data packets between networks and enforcing access control policies. Our focus will be on closely monitoring network traffic, and identifying any abnormal behavior.

3. **Windows machine**
   This machine will be closely monitored to ensure its system logs are actively tracked, suspicious activities are detected, and adherence to security policies is maintained.

4. **Ubuntu machine**
   By configuring our SIEM system to monitor Nginx logs, we can effectively supervise and monitor the logs, enabling us to track and analyze system events and user activity.

Conclusion

After having completed our study and analysis of the current deployment, we have identified the conditions to be met. We have also described some of the issues that should be fixed in the new deployment.

Chapter 4

Implementation of the proposed solution

4.1 Introduction

In the previous chapter, we analyzed and studied the current deployment, and defined the conditions we will consider in the new deployment. This chapter provides an overview of the implementation of a SIEM solution using Splunk Enterprise. It covers the planning, installation, configuration, data collection, search, and analysis.

4.2 New deployment

This architecture referred to as 4.1, is designed to leverage various virtual machines and server technologies to enhance the capabilities of our SIEM system.

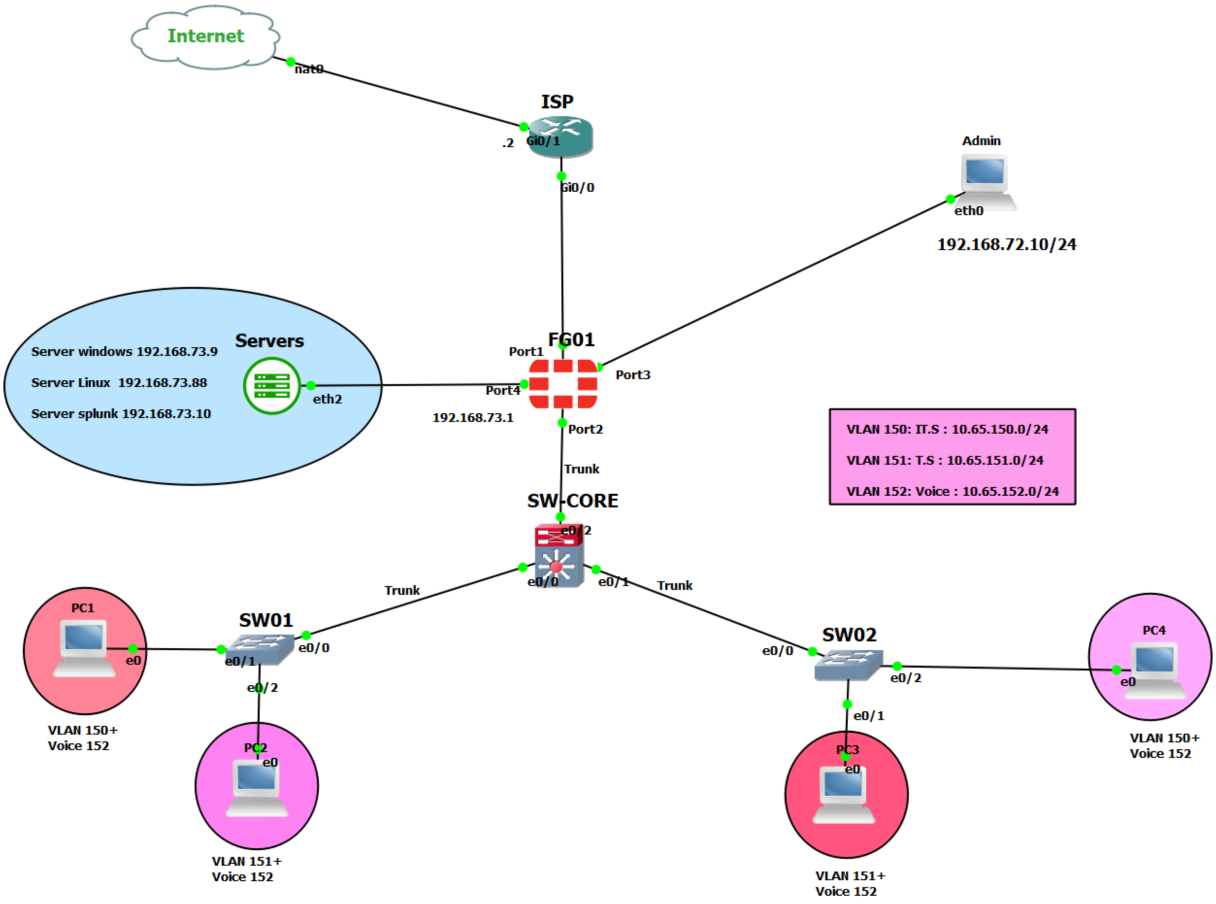


Figure 4.1: Deployment architecture

To support this architecture, we have carefully selected hardware specifications for our PC. It features an Intel Core i5-6300U CPU with a clock speed of 2.40GHz, providing ample processing power for handling the SIEM workload. With 12.00 GB of RAM and a 64-bit operating system, we can ensure efficient memory utilization and compatibility with the chosen components.

4.3 Development environment

In our SIEM solution implementation project, we established a development environment using various software and platforms. We relied on GNS3, a network virtualization software to simulate the network infrastructure.

GNS3 enabled us to import and utilize IOU images for different network devices. Specifically, we employed the following IOU images:

- FortiGate: FGT_VM64_KVM-v7.0.6.F-build0366-FORTINET.out.kvm
- Router: i86bilinuxl3-adventerprisek9-ms.155-2.T.bin
- Switch: i86bilinuxl2-adventerprisek9-15.2d.bin

For hosting the necessary virtual machines for our SIEM solution, we opted for VMware Workstation. This platform facilitated the creation and management of virtual machines running various operating systems. The virtual machine images used for our development environment included:

- Ubuntu machine: ubuntu-20.04.6-desktop-amd64
- Windows 10: Windows10-64bit
- Windows Server: SERVER 2022
- Kali Linux: kali-linux-2021.4a-installer-amd64

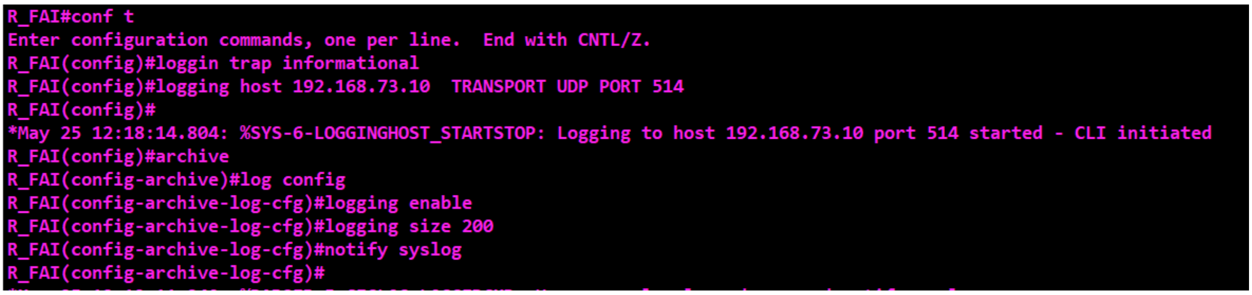
4.4 Settings of monitoring environment

In our monitoring environment, we have installed Splunk on a Windows Server machine, which serves as the central platform for log management and analysis. To efficiently collect logs from various sources, we have deployed universal forwarders on Windows 10 and Ubuntu machine. These lightweight Splunk agents ensure that logs generated by these systems are forwarded to the central Splunk instance. Additionally, we have configured the Syslog protocol on the Cisco router and FortiGate firewall, allowing us to capture and ingest their logs into Splunk for analysis.

4.4.1 Forwarders Configuration

4.4.1.1 configuration of Syslog on a Router

To configure Syslog on a Cisco router, we need to access the router's console and execute a series of commands. These commands enable the router to receive logs via the UDP protocol on port 514 and send them to the Splunk server for further analysis.



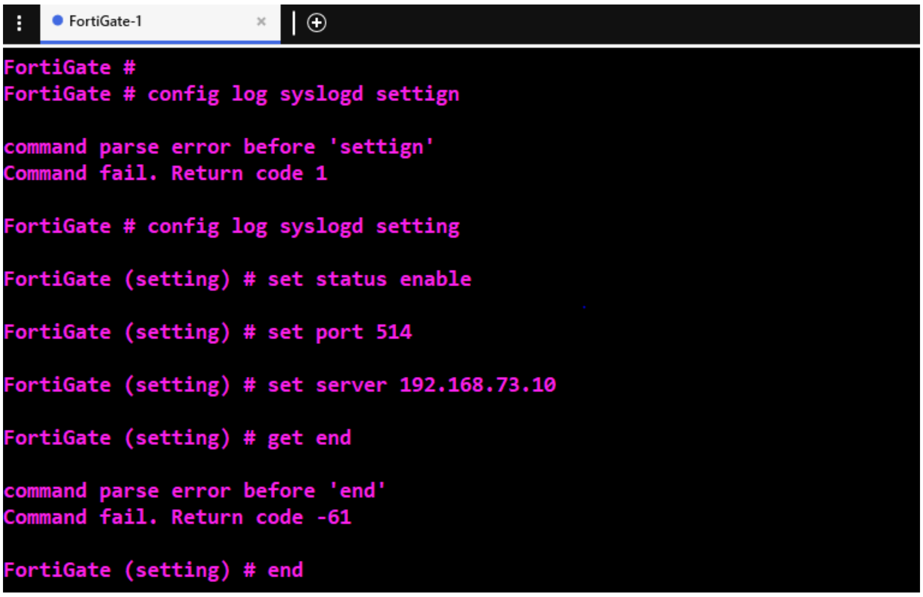
```
R_FAI#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R_FAI(config)#loggin trap informational
R_FAI(config)#logging host 192.168.73.10  TRANSPORT UDP PORT 514
R_FAI(config)#
*May 25 12:18:14.804: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.73.10 port 514 started - CLI initiated
R_FAI(config)#archive
R_FAI(config-archive)#log config
R_FAI(config-archive-log-cfg)#logging enable
R_FAI(config-archive-log-cfg)#logging size 200
R_FAI(config-archive-log-cfg)#notify syslog
R_FAI(config-archive-log-cfg)#
```

Figure 4.2: Syslog on Cisco Router.

4.4.1.2 configuration of Syslog on a FortiGate firewall

To enable the sending of Syslog, we access the FortiGate firewall's command-line interface (CLI) to configure log forwarding to the Splunk server. Afterward, we proceed to the FortiGate user interface and navigate to the "Log Setting" tab to enable the sending of logs for Syslog.

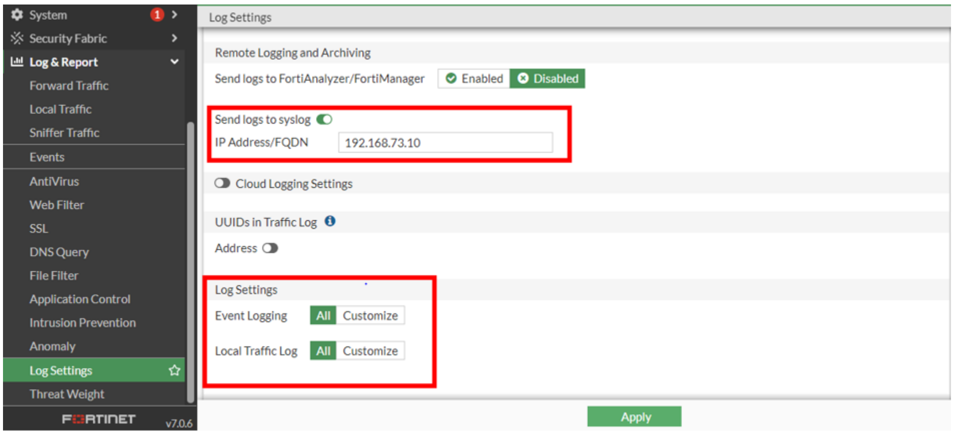
1. Activation of port Syslog:



```
FortiGate #
FortiGate # config log syslogd settign

command parse error before 'settign'
Command fail. Return code 1

FortiGate # config log syslogd setting

FortiGate (setting) # set status enable

FortiGate (setting) # set port 514

FortiGate (setting) # set server 192.168.73.10

FortiGate (setting) # get end

command parse error before 'end'
Command fail. Return code -61

FortiGate (setting) # end
```

Figure 4.3: Syslog on Fortigate firewall.

2. Settings events monitoring On the FortiGate web interface:



Log Settings

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager: Enabled | Disabled

Send logs to syslog: on

IP Address/FQDN: 192.168.73.10

Cloud Logging Settings: off

UUIDs in Traffic Log

Address: off

Log Settings

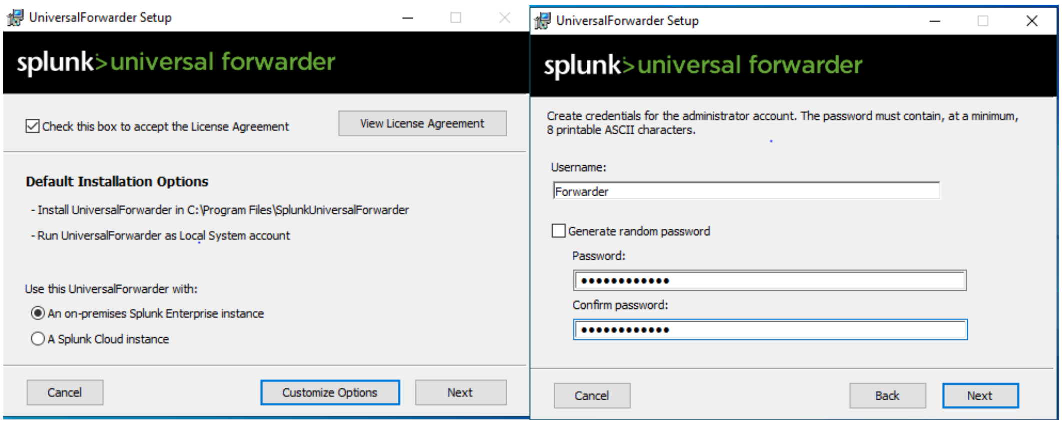
Event Logging: All | Customize

Local Traffic Log: All | Customize

Figure 4.4: Settings events monitoring.

4.4.1.3 Windows forwarder

To install a Universal Forwarder on Windows 10, first, we download the forwarder image (MSI file). Then, we proceed by accepting the license agreement and clicking ’Next’. After that, we enter the required information to create an administrator account.



☑ Check this box to accept the License Agreement

Default Installation Options

- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder
- Run UniversalForwarder as Local System account

Use this UniversalForwarder with:

● An on-premises Splunk Enterprise instance

○ A Splunk Cloud instance

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username: Forwarder

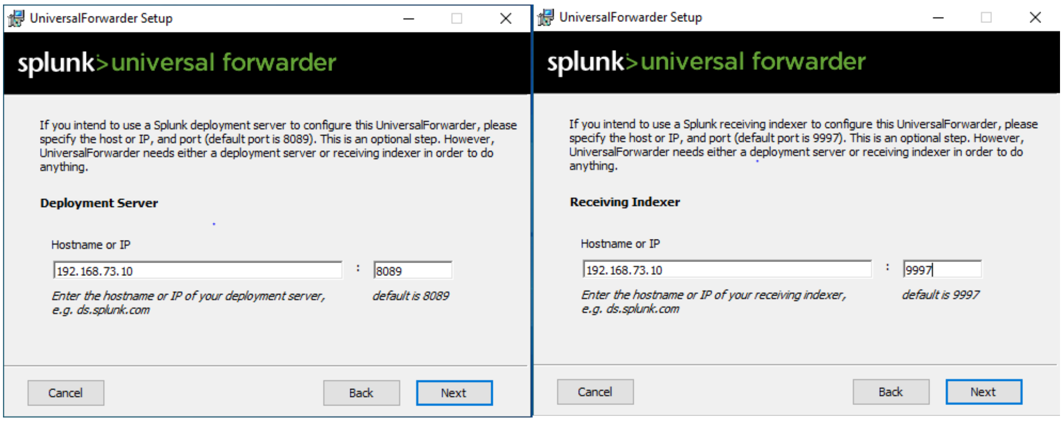
□ Generate random password

Password: ••••••••••••

Confirm password: ••••••••••••

Figure 4.5: Universal forwarder Installation.

Next, we need to specify the deployment server and indexer by providing the name or IP address of the Splunk server. We leave the ports at their default value.



UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Deployment Server

Hostname or IP: 192.168.73.10 : 8089

Enter the hostname or IP of your deployment server, e.g. ds.splunk.com — *default is 8089*

UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

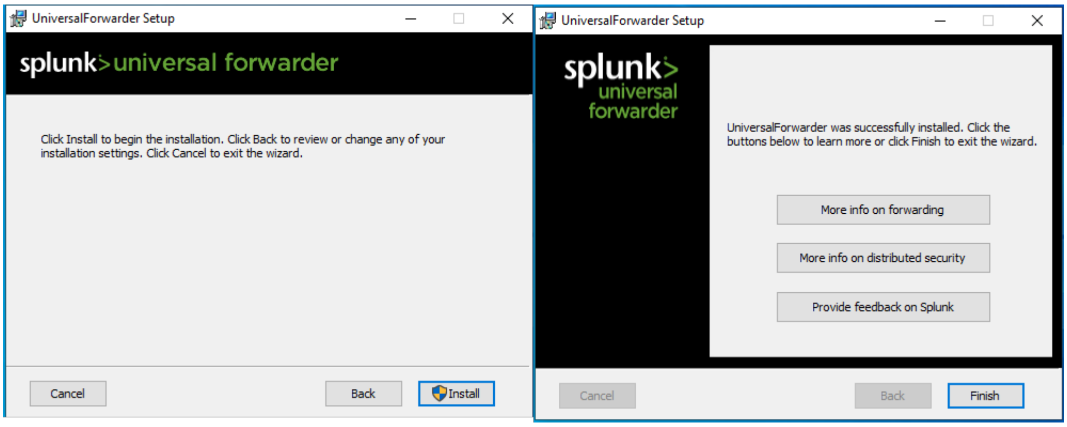
Receiving Indexer

Hostname or IP: 192.168.73.10 : 9997

Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com — *default is 9997*

Figure 4.6: Configuring Splunk Deployment Server.

Finally, We complete the installation of Splunk Universal Forwarder by clicking on 'Finish'.



UniversalForwarder Setup

splunk>universal forwarder

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

UniversalForwarder Setup

splunk> universal forwarder

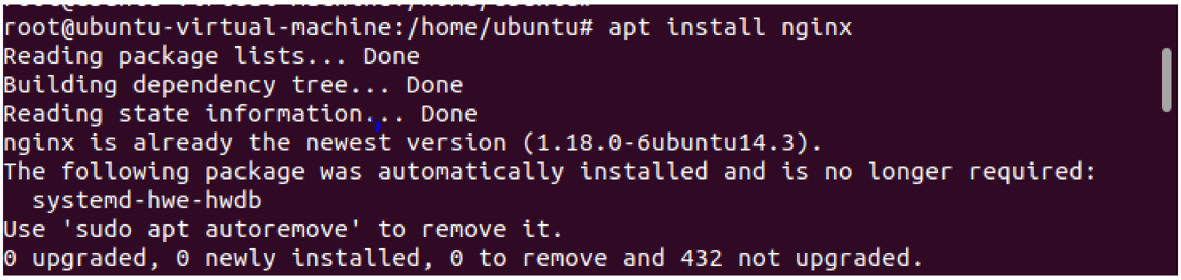
UniversalForwarder was successfully installed. Click the buttons below to learn more or click Finish to exit the wizard.

Figure 4.7: Universal forwarder installed.

4.4.1.4 Linux forwarder

To install the Splunk Universal Forwarder on Linux, we first need to download the Splunk Universal Forwarder package for Ubuntu from the Splunk website, then execute the following commands on the terminal:

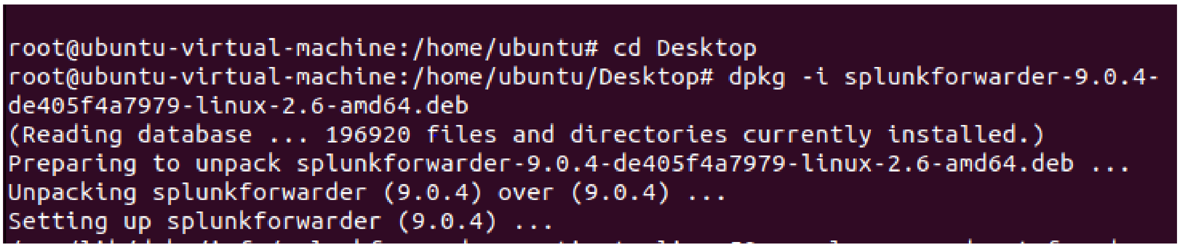
– Nginx web server Installation



```
root@ubuntu-virtual-machine:/home/ubuntu# apt install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nginx is already the newest version (1.18.0-6ubuntu14.3).
The following package was automatically installed and is no longer required:
  systemd-hwe-hwdb
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 432 not upgraded.
```

Figure 4.8: Install Nginx.

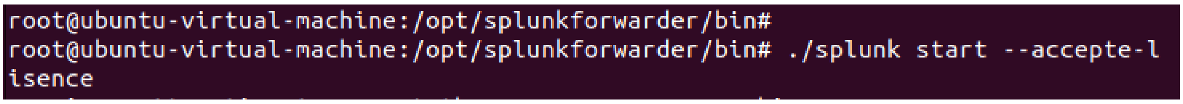
– Configure the Splunk Universal Forwarder



```
root@ubuntu-virtual-machine:/home/ubuntu# cd Desktop
root@ubuntu-virtual-machine:/home/ubuntu/Desktop# dpkg -i splunkforwarder-9.0.4-
de405f4a7979-linux-2.6-amd64.deb
(Reading database ... 196920 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb ...
Unpacking splunkforwarder (9.0.4) over (9.0.4) ...
Setting up splunkforwarder (9.0.4) ...
```

Figure 4.9: Splunk forwarder installation.

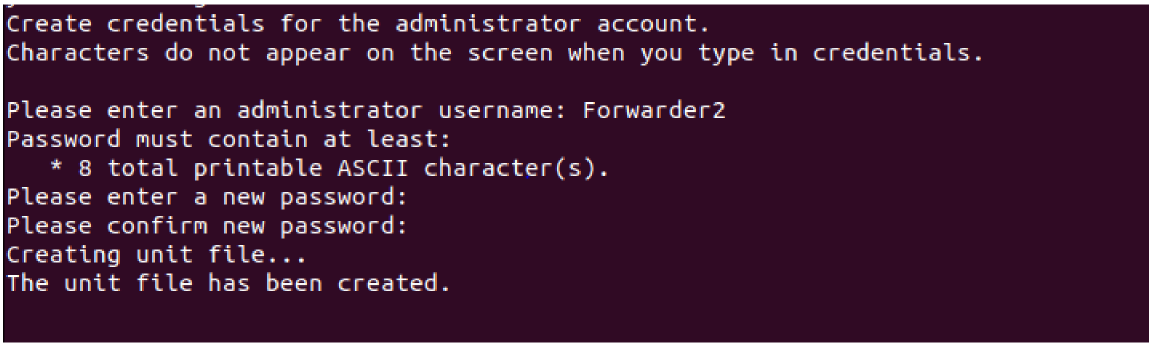
– Accept the Splunk Universal Forwarder license, This command starts the Splunk Universal Forwarder and accepts the license



```
root@ubuntu-virtual-machine:/opt/splunkforwarder/bin#
root@ubuntu-virtual-machine:/opt/splunkforwarder/bin# ./splunk start --accepte-l
isence
```

Figure 4.10: Accept the Splunk Universal Forwarder license.

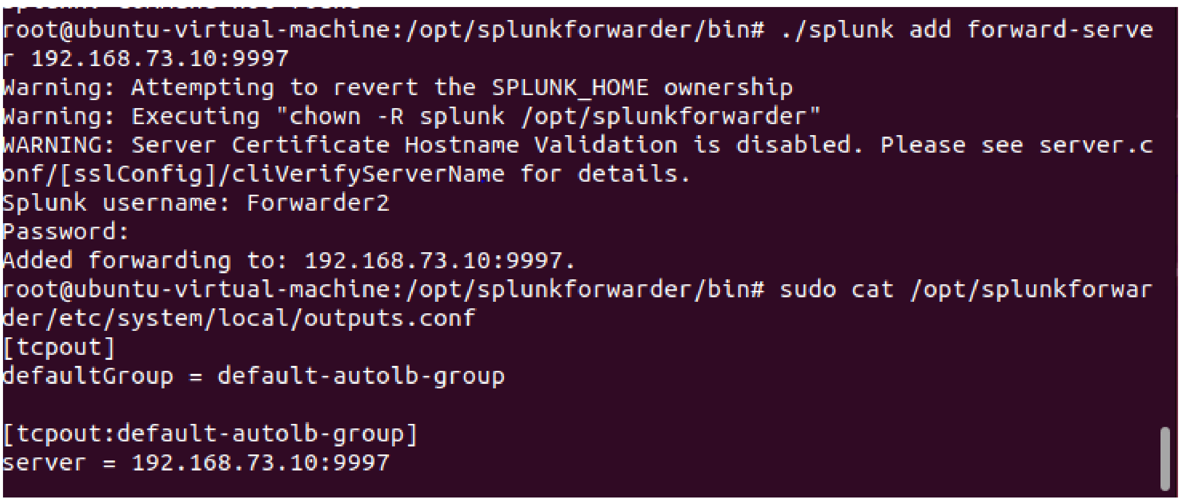
– Set a username and password for the Splunk Universal Forwarder



```
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: Forwarder2
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
The unit file has been created.
```

Figure 4.11: Set a username and password for the Splunk Universal Forwarder.

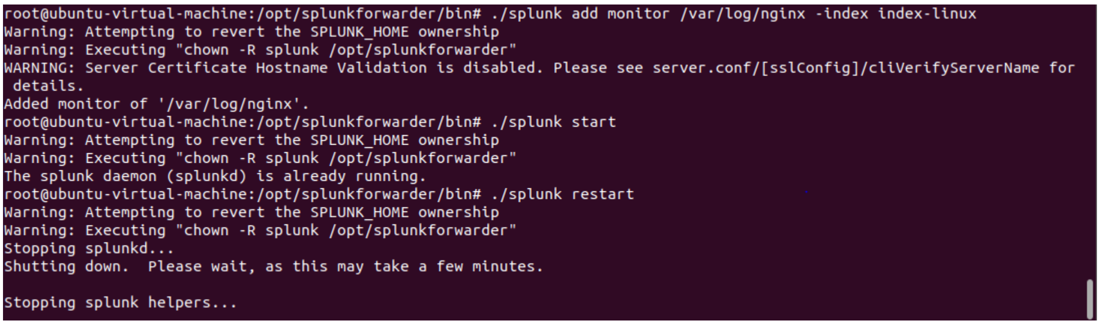
– Add the Splunk server for log forwarding, This command configures the Splunk Universal Forwarder to send logs to the specified Splunk server with server IP.



```
root@ubuntu-virtual-machine:/opt/splunkforwarder/bin# ./splunk add forward-serve
r 192.168.73.10:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk /opt/splunkforwarder"
WARNING: Server Certificate Hostname Validation is disabled. Please see server.c
onf/[sslConfig]/cliVerifyServerName for details.
Splunk username: Forwarder2
Password:
Added forwarding to: 192.168.73.10:9997.
root@ubuntu-virtual-machine:/opt/splunkforwarder/bin# sudo cat /opt/splunkforwar
der/etc/system/local/outputs.conf
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 192.168.73.10:9997
```

Figure 4.12: Add the Splunk server for log forwarding.

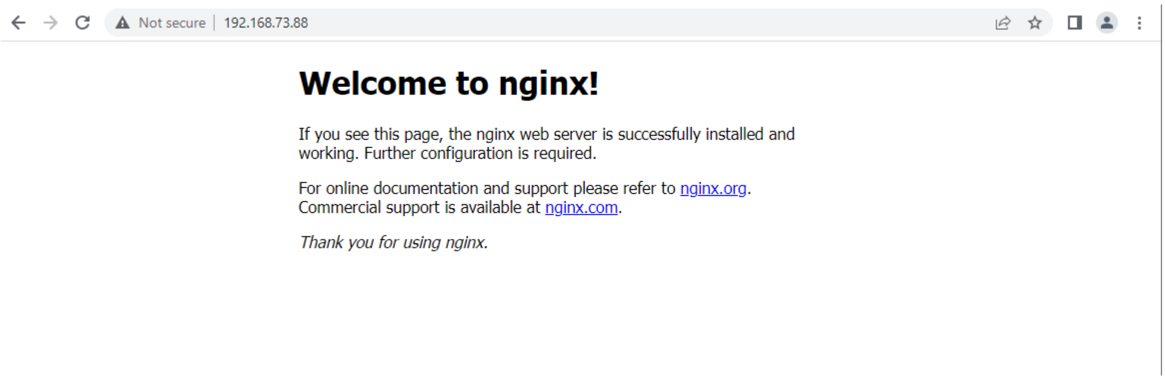
- Add Nginx monitoring, This command configures the Splunk Universal Forwarder to monitor the Nginx access log file and send it to the Splunk server



```
root@ubuntu-virtual-machine:/opt/splunkforwarder/bin# ./splunk add monitor /var/log/nginx -index index-linux
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk /opt/splunkforwarder"
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for
 details.
Added monitor of '/var/log/nginx'.
root@ubuntu-virtual-machine:/opt/splunkforwarder/bin# ./splunk start
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk /opt/splunkforwarder"
The splunk daemon (splunkd) is already running.
root@ubuntu-virtual-machine:/opt/splunkforwarder/bin# ./splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk /opt/splunkforwarder"
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.

Stopping splunk helpers...
```

Figure 4.13: Add Nginx monitoring.

- Finally, we Access the Nginx server using a web browser as illustrated below.



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

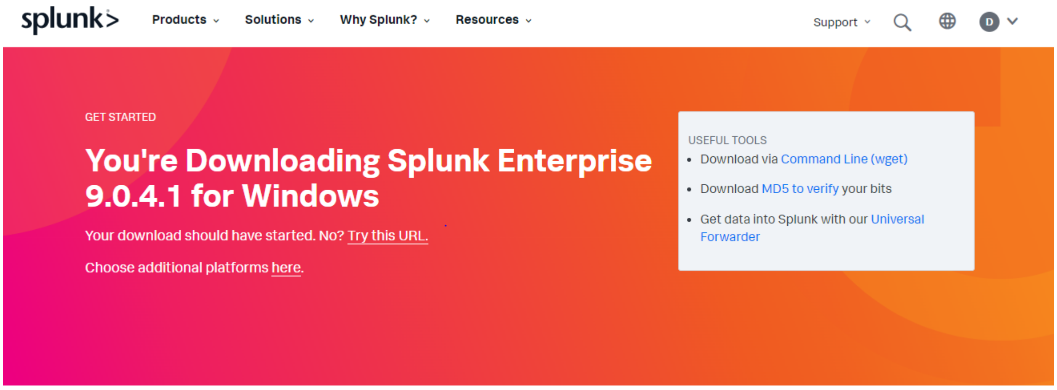
Figure 4.14: Nginx server web page.

4.4.2 Splunk Installation and configuration

In this section, we will illustrate and explain the process of installing and configuring Splunk on a Windows 10 server, and by the end, we will have a working Splunk instance ready to collect and analyze your log data.

4.4.2.1 Splunk installation

1. To begin the installation of Splunk on a Windows 10 server, first, we download the Splunk software from the official website.



GET STARTED

You're Downloading Splunk Enterprise 9.0.4.1 for Windows

Your download should have started. No? Try this URL.

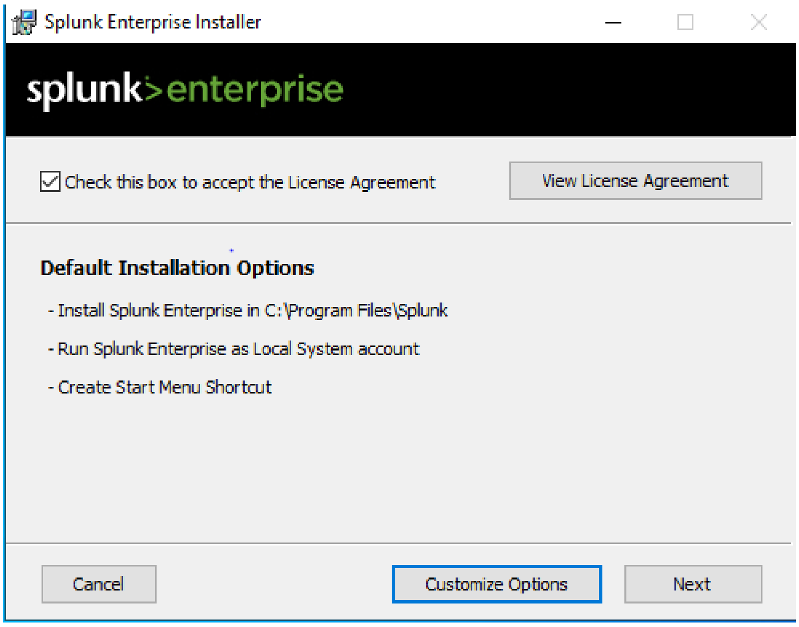
Choose additional platforms here.

USEFUL TOOLS

- Download via Command Line (wget)
- Download MD5 to verify your bits
- Get data into Splunk with our Universal Forwarder

Figure 4.15: Splunk download.

2. We will proceed with the installation of Splunk on the Windows 10 server. Begin by locating the downloaded Splunk installer (.msi file) and double-clicking it. Follow the on-screen prompts to accept the license agreement and select the installation directory. Finally, click "Next" to continue the installation process.



☑ Check this box to accept the License Agreement

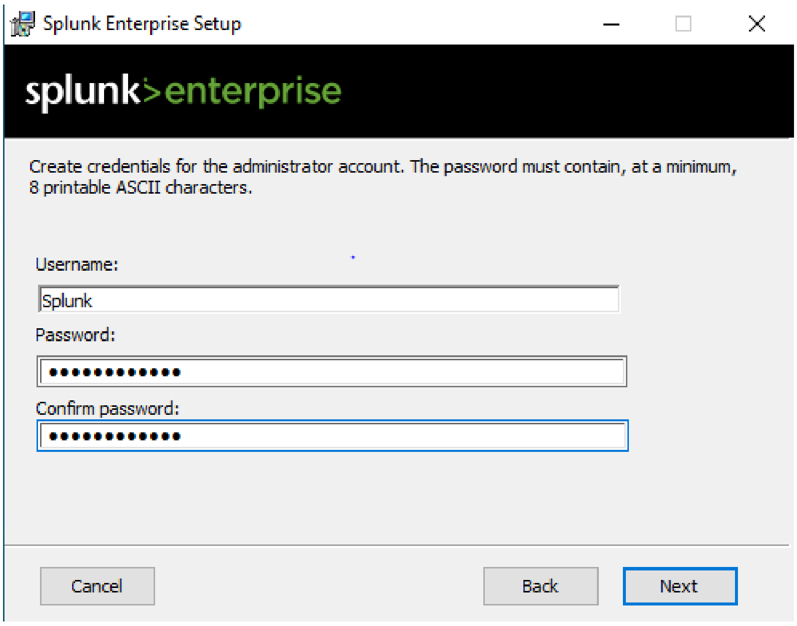
Default Installation Options

- Install Splunk Enterprise in C:\Program Files\Splunk
- Run Splunk Enterprise as Local System account
- Create Start Menu Shortcut

Figure 4.16: Splunk installation.

3. After clicking "Next," the installation program will display the "Connection Information" panel. In this panel, we will specify a username and password for Splunk. We should enter the desired username and password, then click

"Next" to proceed with the installation. This step ensures secure access to your Splunk instance.



Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

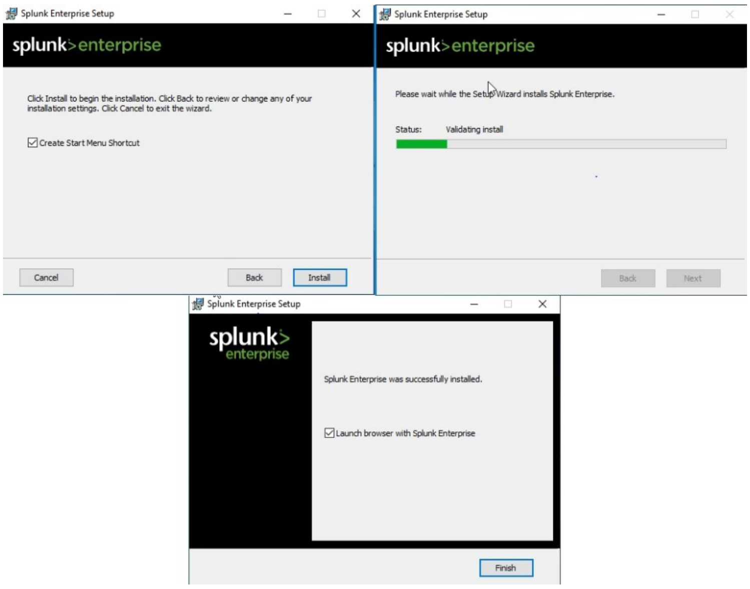
Username: Splunk

Password: ••••••••••••

Confirm password: ••••••••••••

Figure 4.17: Creating an administrator account.

4. Next, we should click on the "Install" button to initiate the installation process. The program will then begin running and proceed to install the Splunk software on the Windows 10 server. After the installation is finished, a window labeled "Installation Complete" will appear. Finally, we can click on the "Finish" button.



Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

☑ Create Start Menu Shortcut

Please wait while the Setup Wizard installs Splunk Enterprise.

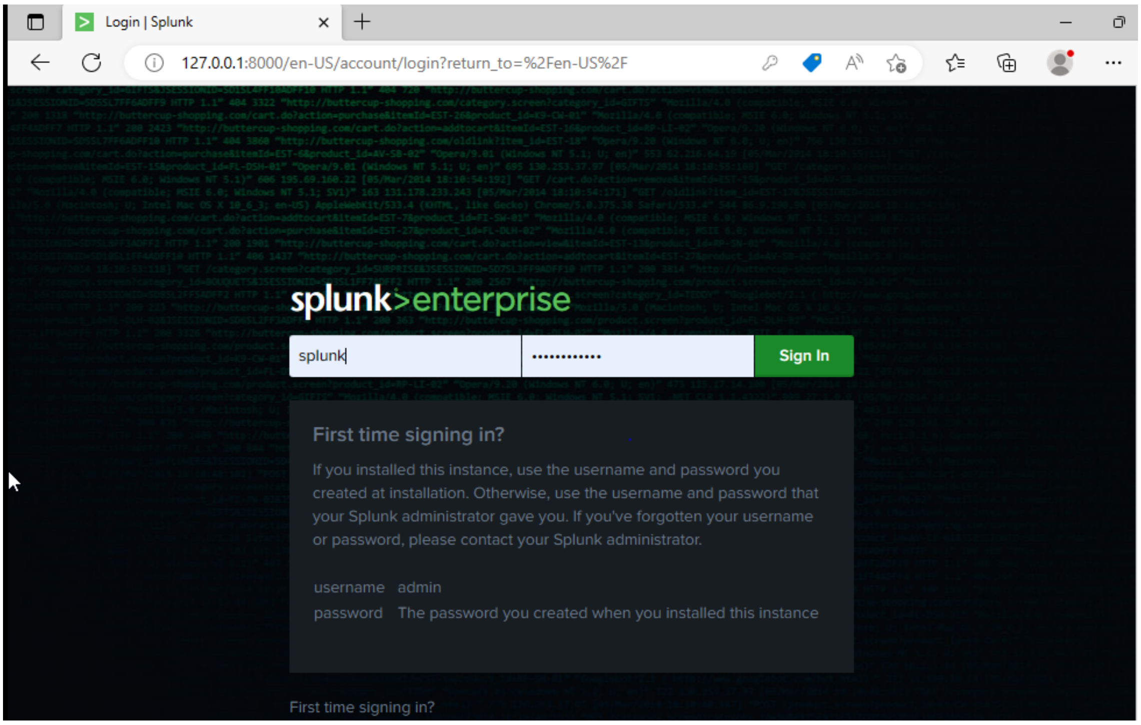
Status: Validating install

Splunk Enterprise was successfully installed.

☑ Launch browser with Splunk Enterprise

Figure 4.18: Installation steps.

5. A username and password are required to access the Splunk interface. Screenshot 4.19 shows the home page of Splunk Enterprise.



splunk

••••••••••••

First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin

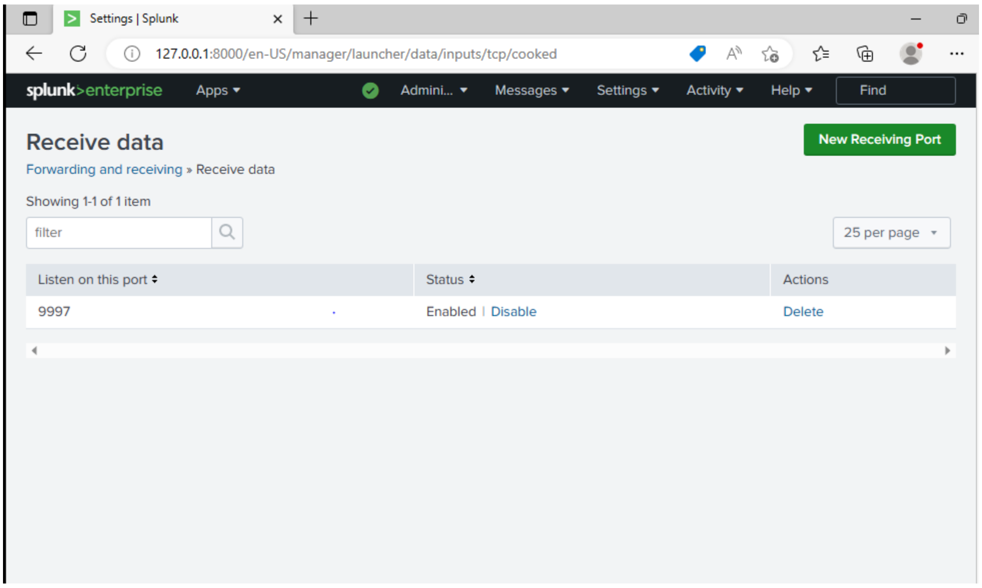
password The password you created when you installed this instance

First time signing in?

Figure 4.19: User interface of Splunk.

4.4.2.2 Splunk configuration

1. **Allowing Reception**
   To enable log reception and collection on our Splunk server, we need to configure the listening port to be 9997. To do this, we can access the Splunk web interface, go to "Settings," and select "Forwarding and Receiving." Then, choose "Configure Receiving" and click on "Add New." Finally, enter the port number 9997 in the "Listen on this port" field.



Receive data

Forwarding and receiving » Receive data

Showing 1-1 of 1 item

Listen on this port	Status	Actions
9997	Enabled | Disable	Delete

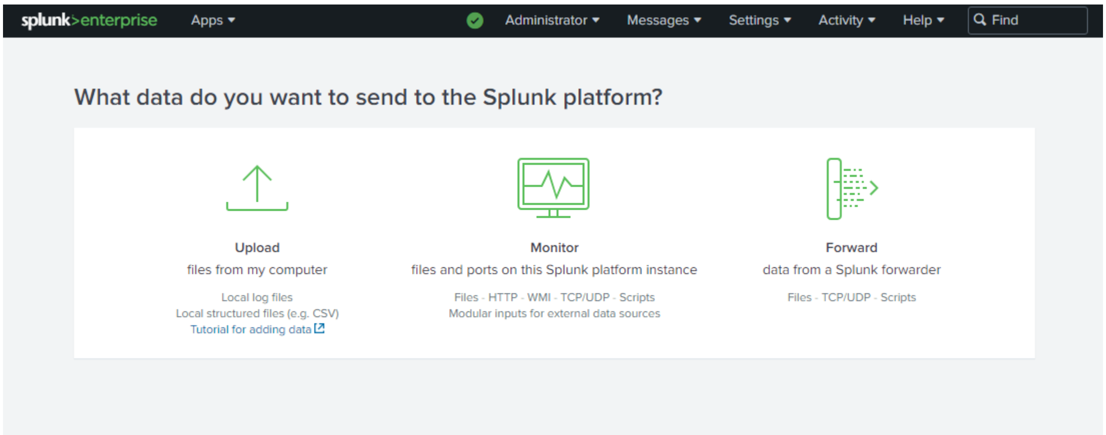
Figure 4.20: Add Splunk listening port.

2. **Indexes Creation**

   In order to effectively receive and manage logs from each configured module, we create indexes for Windows, Linux, FortiGate, and Cisco modules.

   - Creating Index for Windows

     We start by accessing the homepage of the Splunk server. From there, we click on the "Add Data" option located in the top navigation bar. This action directs us to the "Add Data" page. On this page, we specifically select the "Forward" option to proceed with the data integration process.



What data do you want to send to the Splunk platform?

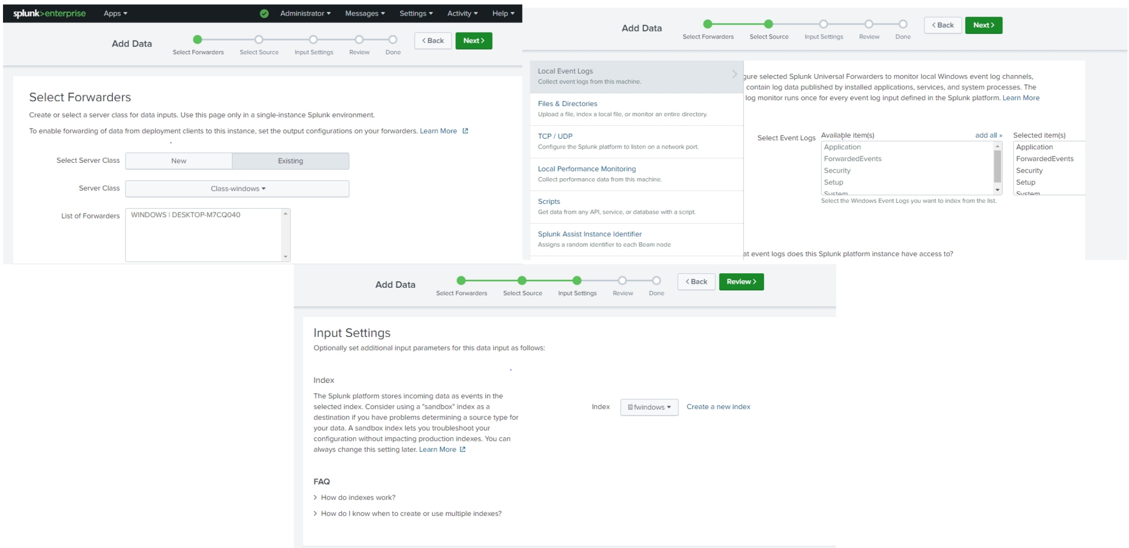
Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

Monitor
files and ports on this Splunk platform instance
Files · HTTP · WMI · TCP/UDP · Scripts
Modular inputs for external data sources

Forward
data from a Splunk forwarder
Files · TCP/UDP · Scripts

Figure 4.21: Add Data.

After selecting a list of machines and a class for data inputs on the "Add Data" page, we click on "Next". Then, we choose the Windows Event Logs we want to index from the provided list. Finally, we create an index specifically for storing the indexed Windows Event Logs.



Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. Learn More

Select Server Class: New | Existing

Server Class: Class-windows

List of Forwarders: WINDOWS | DESKTOP-M7CQ040

Local Event Logs
Collect event logs from this machine.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Scripts
Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier
Assigns a random identifier to each Beam node

gure selected Splunk Universal Forwarders to monitor local Windows event log channels, contain log data published by installed applications, services, and system processes. The log monitor runs once for every event log input defined in the Splunk platform. Learn More

Select Event Logs
Available item(s) — add all »
Application
ForwardedEvents
Security
Setup
System
Selected item(s)
Application
ForwardedEvents
Security
Setup
System
Select the Windows Event Logs you want to index from the list.

at event logs does this Splunk platform instance have access to?

Input Settings

Optionally set additional input parameters for this data input as follows:

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: fwindows — Create a new index

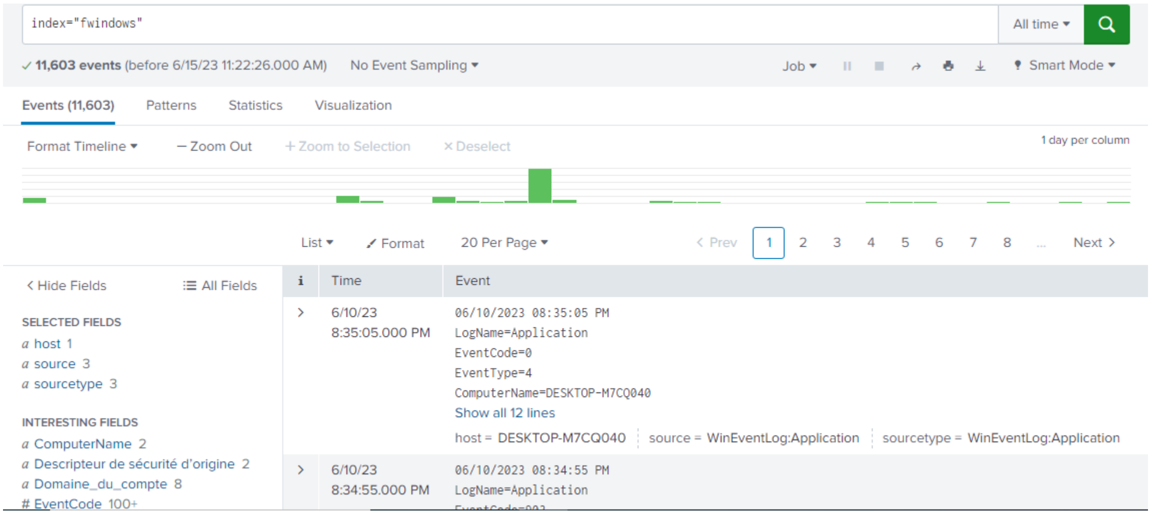
FAQ

> How do indexes work?

> How do I know when to create or use multiple indexes?

Figure 4.22: Index creation steps.

And here are the results of the search index of Windows logs.



```
index="fwindows"
```

✓ 11,603 events (before 6/15/23 11:22:26.000 AM) No Event Sampling ▾

SELECTED FIELDS
- a host 1
- a source 3
- a sourcetype 3

INTERESTING FIELDS
- a ComputerName 2
- a Descripteur de sécurité d'origine 2
- a Domaine_du_compte 8
- # EventCode 100+

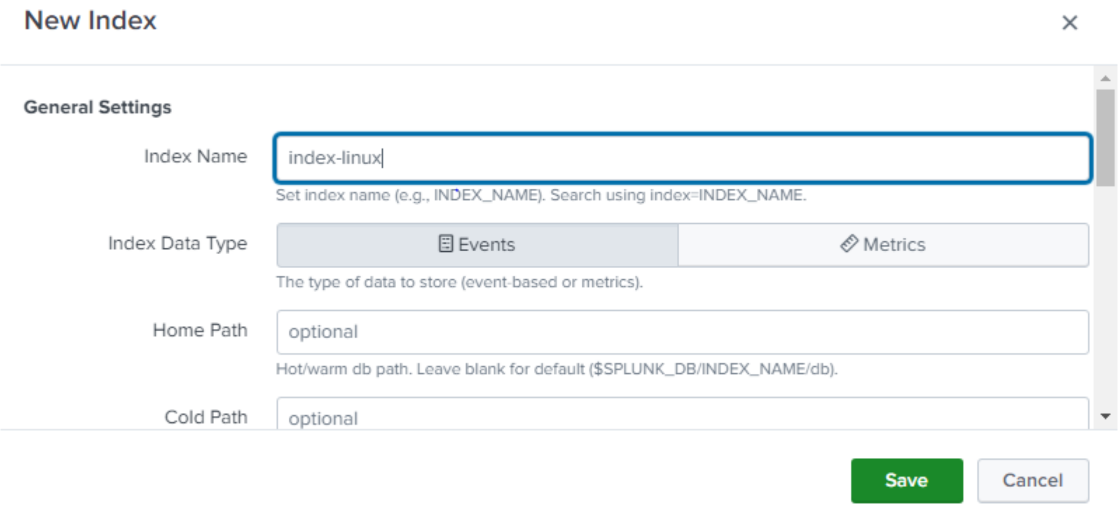
i	Time	Event

›	6/10/23
	8:35:05.000 PM
		06/10/2023 08:35:05 PM
		LogName=Application
		EventCode=0
		EventType=4
		ComputerName=DESKTOP-M7CQ040
		Show all 12 lines
		host = DESKTOP-M7CQ040 source = WinEventLog:Application sourcetype = WinEventLog:Application

›	6/10/23 8:34:55.000 PM	06/10/2023 08:34:55 PM LogName=Application

Figure 4.23: Windows logs.

- creating index for Linux
  We access the web interface of Splunk. From there, we navigate to the Settings section and select Indexes. Next, we click on the option to create a new index. We provide a name for the index and configure the necessary settings. Finally, we save the index.



New Index

General Settings

Index Name: index-linux
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events | Metrics
The type of data to store (event-based or metrics).

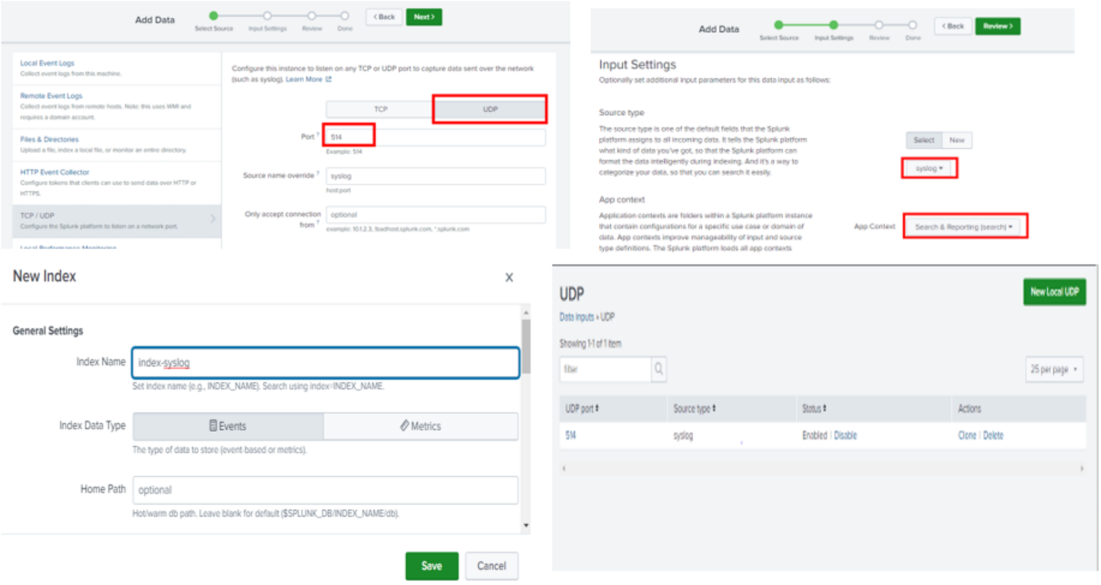
Home Path: optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional

Figure 4.24: Linux index creation.

- creating index for FortiGate's firewall and Cisco router:
  The default Syslog listens on port 514, so we configure Splunk to retrieve logs from both FortiGate and Cisco routers using a single index.

  To accomplish this, we first log into the Splunk web interface. Then, we navigate to "Settings" > "Data Inputs" and add a new UDP input with port 514. We select "Syslog UDP" as the source type and create a new index called "index_syslog." Finally, we submit the configuration to start ingesting and storing the combined Syslog data from both devices in the designated index.



Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More

Port ? 514
Example: 514

Source name override ? syslog
host:port

Only accept connection from ? optional
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

Input Settings
Optionally set additional input parameters for this data input as follows:

Source type
The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

syslog ▾

App context
Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts

App Context Search & Reporting (search) ▾

New Index

General Settings

Index Name index-syslog
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type Events Metrics
The type of data to store (event-based or metrics).

Home Path optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

UDP
Data inputs » UDP
Showing 1-1 of 1 item

UDP port	Source type	Status	Actions
514	syslog	Enabled | Disable	Clone | Delete

Figure 4.25: Syslog Index Creation.

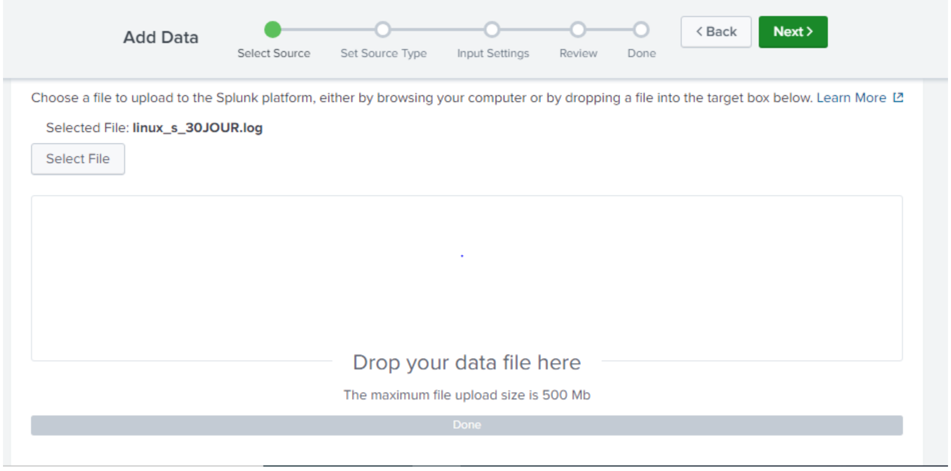
4.4.3 Creating and configuring visualization tools

Splunk provides powerful features for data visualization and the creation of customized dashboards. In this section, we will present how to create and configure dashboards and alerts using Splunk.

4.4.3.1 Creation and Configuration of Dashboards

1. **Manual Dashboard:** Realistic Representation of SSH Connection Logs
   To create a manual dashboard that closely reflects real-world scenarios, we import a 30-day log file containing security logs from a Linux server. Specifically, these logs capture SSH connection activities.

   - Log File Import
     To import data via file upload in Splunk, we access the Splunk Web interface and log in with our credentials. Then, we go to the "Add Data" section. There, we choose the option that allows us to upload data from files. We select the file we want to upload by clicking on the "Choose File" button.



Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

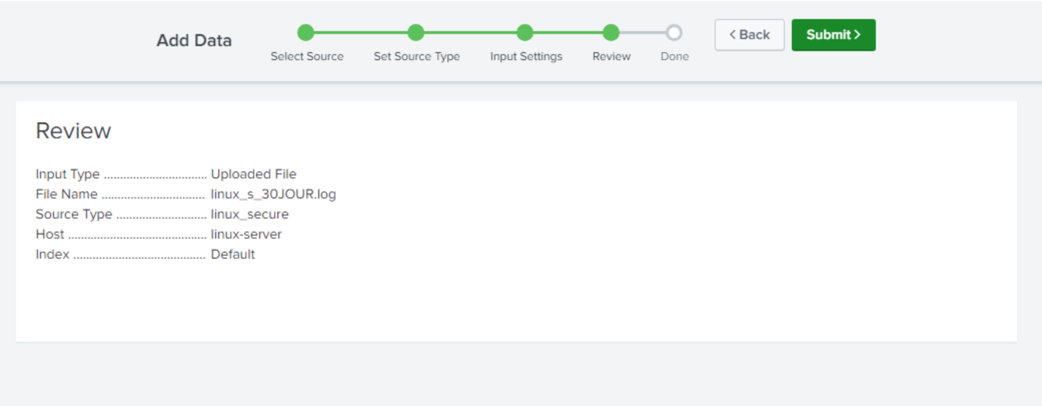
Selected File: **linux_s_30JOUR.log**

Drop your data file here

The maximum file upload size is 500 Mb

Figure 4.26: File importation.

We specify the source type for the downloaded file as "Linux-secure" since these are security-related logs. We continue with the subsequent steps, and then we submit the configuration. The summary of the upload is displayed on the screen.



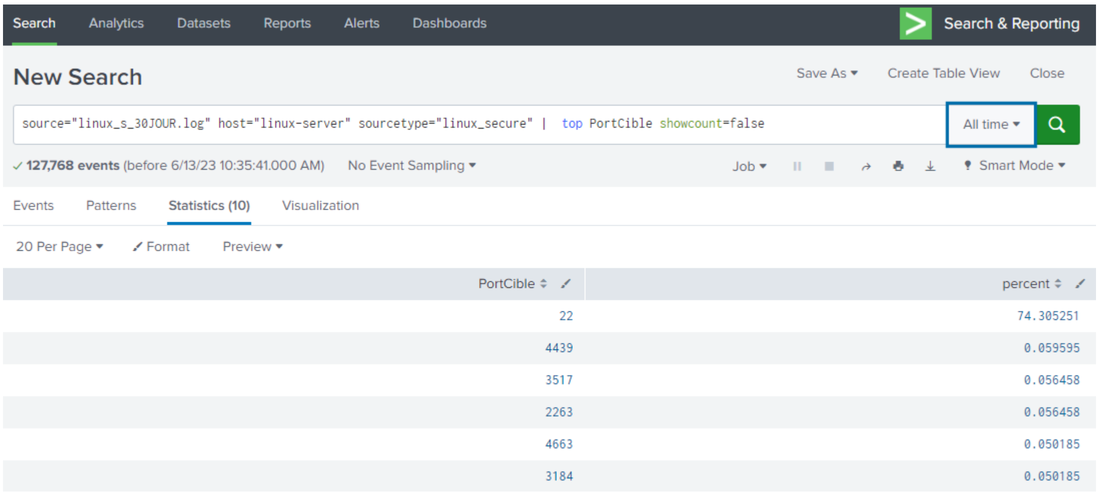
Review

Input Type .... Uploaded File
File Name .... linux_s_30JOUR.log
Source Type .... linux_secure
Host .... linux-server
Index .... Default

Figure 4.27: Data added review.

- Searching with SPL(Search Processing Language):
  Splunk provides a powerful query language called SPL that allows us to search and analyze the data. In our case, we have chosen four SPL queries to extract the desired information from the log file. To do this, we need to navigate to the "Search & Reporting" application. Then, in the search bar, we enter the following SPL queries:

  1. Query 1 - List of the most frequent target ports:



```
source="linux_s_30JOUR.log" host="linux-server" sourcetype="linux_secure" |  top PortCible showcount=false
```

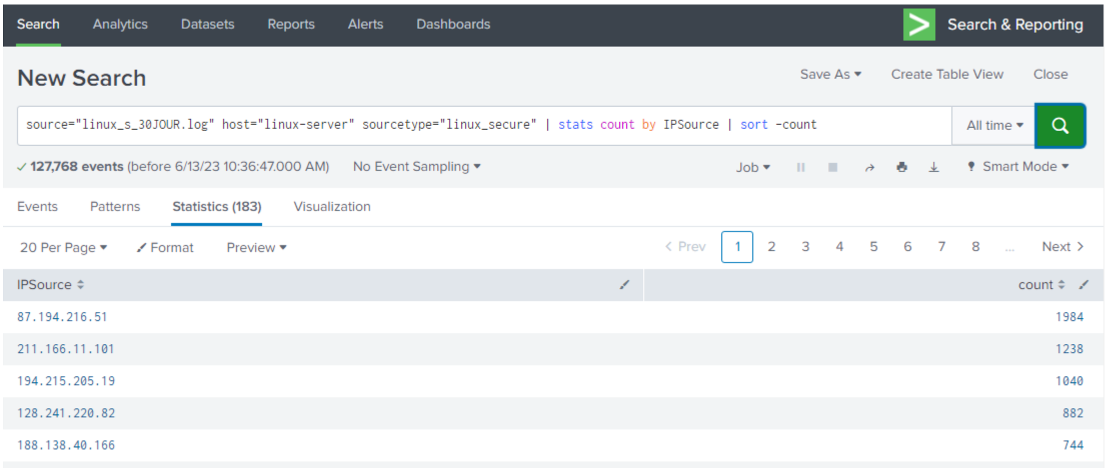
✓ 127,768 events (before 6/13/23 10:35:41.000 AM) No Event Sampling ▾

PortCible	percent
22	74.305251
4439	0.059595
3517	0.056458
2263	0.056458
4663	0.050185
3184	0.050185

Figure 4.28: PortCible Query.

This query searches for SSH connection events in the logs with the source type "Linux_secure" from the host "Linux-server." It displays a list of the most frequent target ports, excluding the count for each port (showcount=false).

2. Query 2 - Number of unique source IP addresses and their count:



```
source="linux_s_30JOUR.log" host="linux-server" sourcetype="linux_secure" | stats count by IPSource | sort -count
```

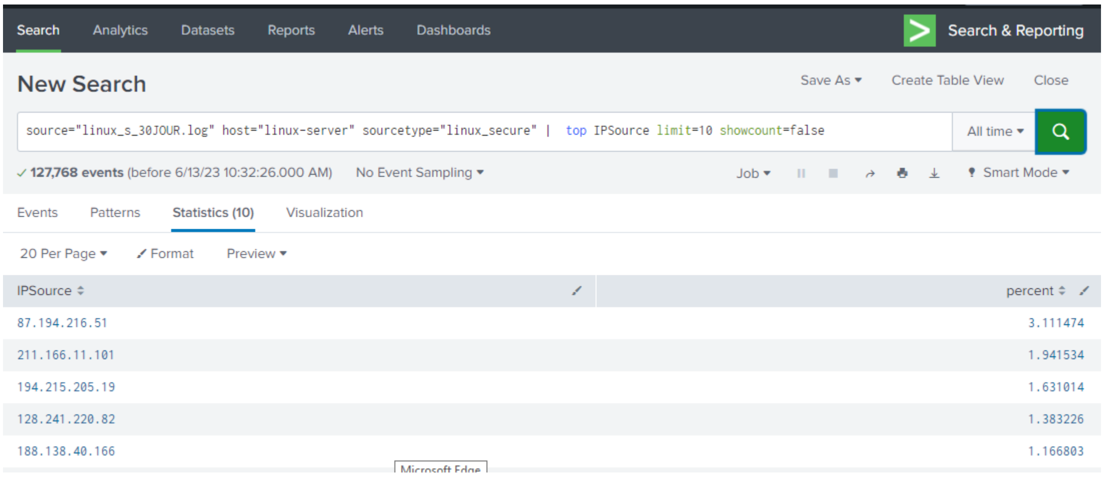
✓ 127,768 events (before 6/13/23 10:36:47.000 AM) No Event Sampling ▾

IPSource	count
87.194.216.51	1984
211.166.11.101	1238
194.215.205.19	1040
128.241.220.82	882
188.138.40.166	744

Figure 4.29: IP addresses count.

This query performs a statistical calculation to count the number of unique source IP addresses and sorts them in descending order by count.

3. Query 3 - Percentage of the most frequent source IP addresses:



```
source="linux_s_30JOUR.log" host="linux-server" sourcetype="linux_secure" |  top IPSource limit=10 showcount=false
```

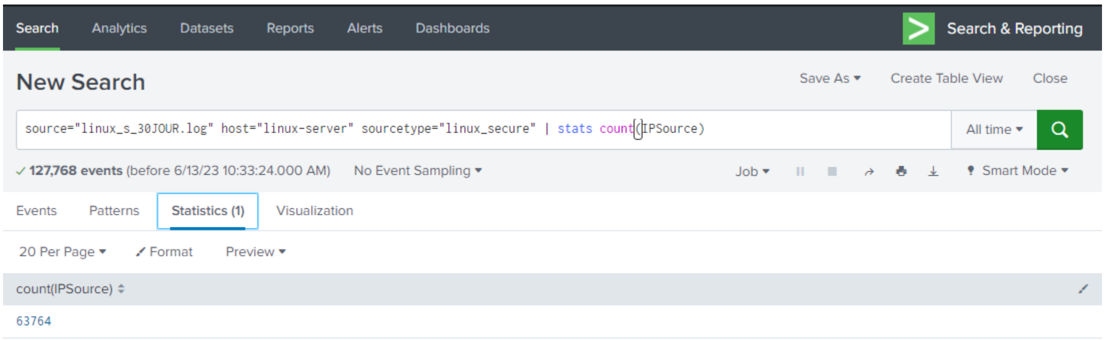
✓ 127,768 events (before 6/13/23 10:32:26.000 AM) No Event Sampling ▾

IPSource	percent
87.194.216.51	3.111474
211.166.11.101	1.941534
194.215.205.19	1.631014
128.241.220.82	1.383226
188.138.40.166	1.166803

Figure 4.30: Top IP addresses.

This query displays the percentage of the top 10 most frequent source IP addresses, excluding the count for each address (showcount=false).

4. Query 4 - Total count of unique IP addresses:



```
source="linux_s_30JOUR.log" host="linux-server" sourcetype="linux_secure" | stats count(IPSource)
```

✓ 127,768 events (before 6/13/23 10:33:24.000 AM) No Event Sampling ▾

count(IPSource)
63764

Figure 4.31: Total number of unique source IP.

This query performs a statistical calculation to count the total number of unique source IP addresses.

- Creation of a dashboard:

  First, we have to build a visualization, Splunk offers a range of visualization options to present the data effectively as illustrated in Figure 4.32:

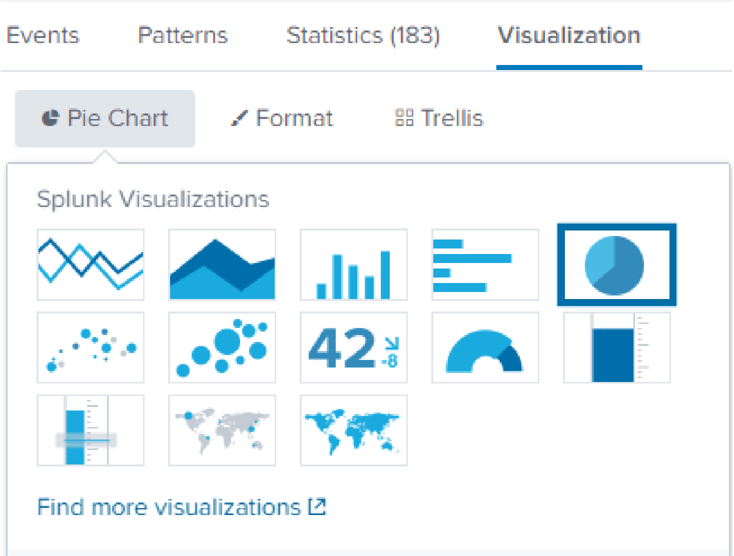
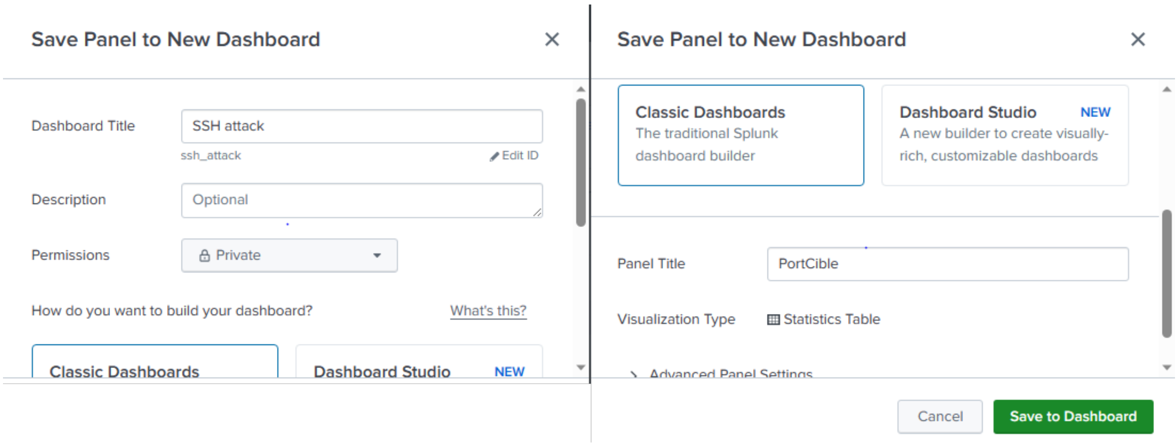


Figure 4.32: Visualization type.

Then, we choose the appropriate visualization type for each query and add a panel:



Save Panel to New Dashboard

Dashboard Title: SSH attack
ssh_attack
Description: Optional
Permissions: Private
How do you want to build your dashboard?

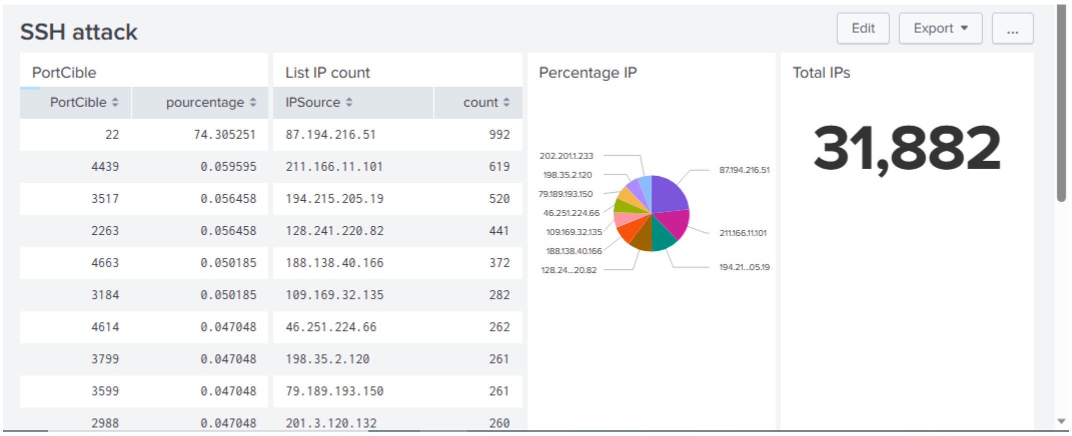
Save Panel to New Dashboard

Classic Dashboards
The traditional Splunk dashboard builder
Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards

Panel Title: PortCible
Visualization Type: Statistics Table

Figure 4.33: Add panel.

After adding all the panels to the existing dashboard, here is the final screen that shows the dashboard of different metrics and insights in a visually appealing and informative manner.



SSH attack

PortCible

PortCible	pourcentage
22	74.305251
4439	0.059595
3517	0.056458
2263	0.056458
4663	0.050185
3184	0.050185
4614	0.047048
3799	0.047048
3599	0.047048
2988	0.047048

List IP count

IPSource	count
87.194.216.51	992
211.166.11.101	619
194.215.205.19	520
128.241.220.82	441
188.138.40.166	372
109.169.32.135	282
46.251.224.66	262
198.35.2.120	261
79.189.193.150	261
201.3.120.132	260

Percentage IP

Total IPs

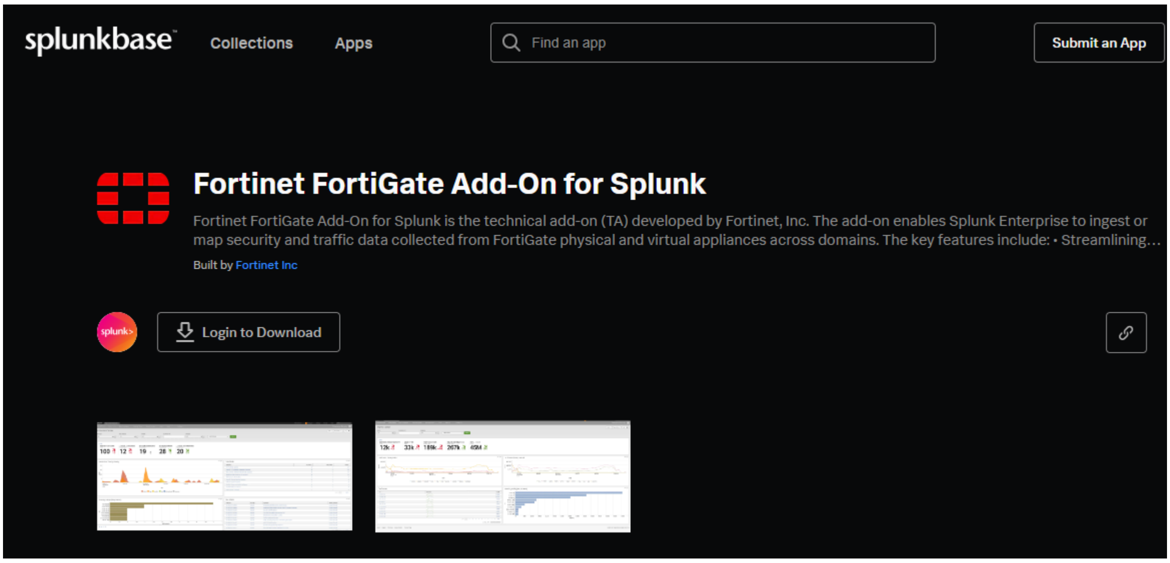
31,882

Figure 4.34: Dashboard Screen.

2. **Default Dashboard:** Fortinet network security and Traffic,
   In addition to the manual dashboard, we also created default dashboards that provide real-time monitoring and analysis of network traffic using the FortiGate app.

   Before starting to configure the dashboard, we install the Splunk Fortinet App and Add-on. Here are the steps explained:

   - Install Splunk Fortinet App and Add-on: Apps and add-ons in Splunk streamline tasks, simplify operations, and extend capabilities. They offer pre-built content and configurations, empowering users to effectively analyze data, monitor systems, and make informed decisions

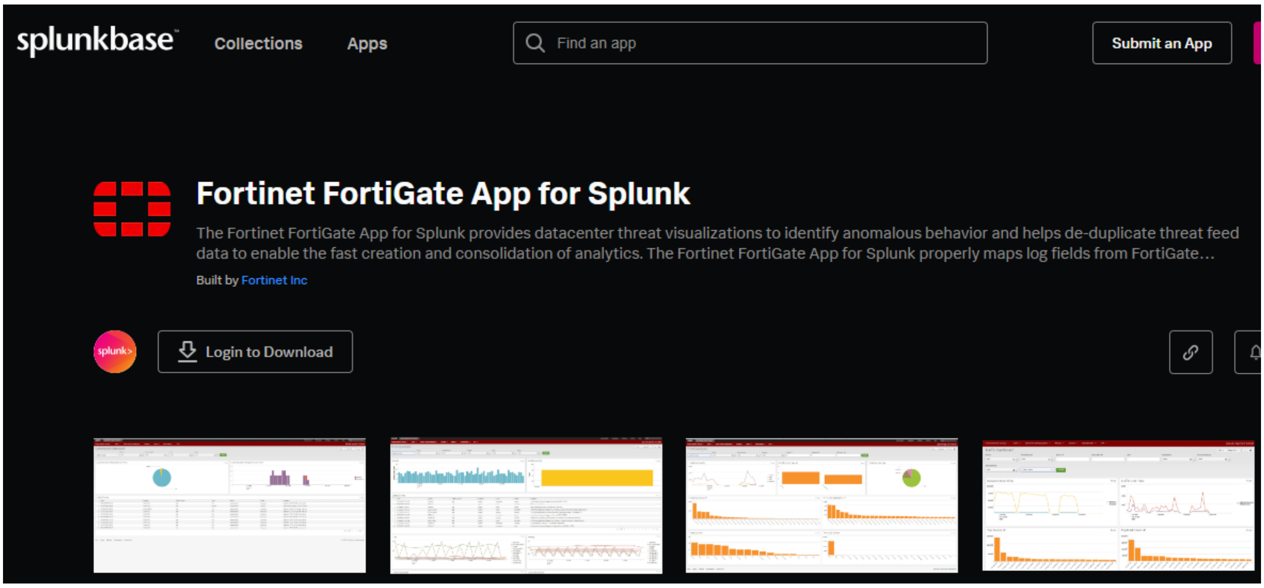


Fortinet FortiGate Add-On for Splunk

Fortinet FortiGate Add-On for Splunk is the technical add-on (TA) developed by Fortinet, Inc. The add-on enables Splunk Enterprise to ingest or map security and traffic data collected from FortiGate physical and virtual appliances across domains. The key features include: • Streamlining...

Built by Fortinet Inc

Figure 4.35: Fortinet Add-on download.



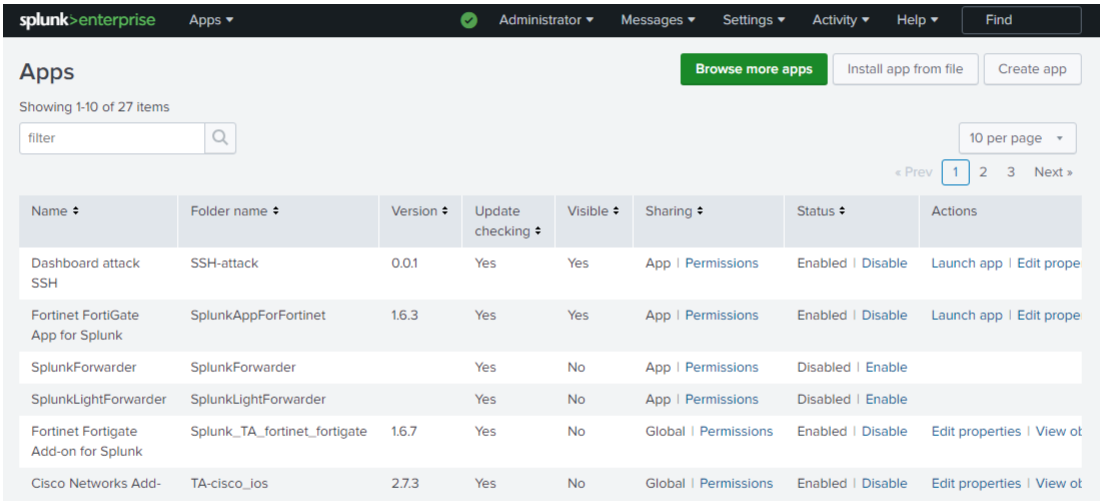
Fortinet FortiGate App for Splunk

The Fortinet FortiGate App for Splunk provides datacenter threat visualizations to identify anomalous behavior and helps de-duplicate threat feed data to enable the fast creation and consolidation of analytics. The Fortinet FortiGate App for Splunk properly maps log fields from FortiGate...

Built by Fortinet Inc

Figure 4.36: Fortinet App for Splunk download.

In the top navigation bar, we click on the "Apps" icon to access the applications section. Then, we select "Install the app from file" and follow the instructions to select the downloaded files and complete the installation process.



Apps

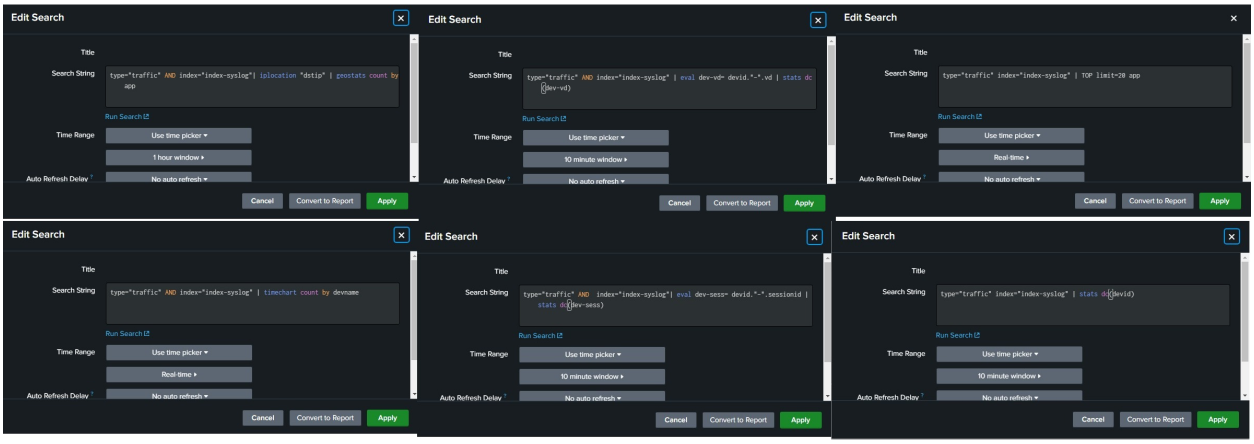
Showing 1-10 of 27 items

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Dashboard attack SSH	SSH-attack	0.0.1	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit prope
Fortinet FortiGate App for Splunk	SplunkAppForFortinet	1.6.3	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit prope
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
Fortinet Fortigate Add-on for Splunk	Splunk_TA_fortinet_fortigate	1.6.7	Yes	No	Global | Permissions	Enabled | Disable	Edit properties | View ot
Cisco Networks Add-	TA-cisco_ios	2.7.3	Yes	No	Global | Permissions	Enabled | Disable	Edit properties | View ot

Figure 4.37: Install Fortinet app and addon for splunk.

- Configure Fortinet App to analyze all logs in the default dashboard: To ensure that the Fortinet App can search and generate reports for all logs, we have followed these steps to adjust the research query: we will have to use type="traffic" AND index="index-syslog" to replace "fgt_traffic" For session numbers in 10 minutes, we will have to use sessionid to replace session_id We will use type="utm" to replace "fgt_utm", and use apprisk to replace severity.

– Fortinet Network Security tab



Title

Search String
```
type="traffic" AND index="index-syslog"| iplocation "dstip" | geostats count by
    app
```
Time Range: Use time picker ▾ / 1 hour window ▸

Auto Refresh Delay: No auto refresh ▾

Title

Search String
```
type="traffic" AND index="index-syslog" | eval dev-vd= devid."-".vd | stats dc
    (dev-vd)
```
Time Range: Use time picker ▾ / 10 minute window ▸

Auto Refresh Delay: No auto refresh ▾

Title

Search String
```
type="traffic" index="index-syslog" | TOP limit=20 app
```
Time Range: Use time picker ▾ / Real-time ▸

Auto Refresh Delay: No auto refresh ▾

Title

Search String
```
type="traffic" AND index="index-syslog" | timechart count by devname
```
Time Range: Use time picker ▾ / Real-time ▸

Auto Refresh Delay: No auto refresh ▾

Title

Search String
```
type="traffic" AND  index="index-syslog"| eval dev-sess= devid."-".sessionid |
    stats dc(dev-sess)
```
Time Range: Use time picker ▾ / 10 minute window ▸

Auto Refresh Delay: No auto refresh ▾

Title

Search String
```
type="traffic" index="index-syslog" | stats dc(devid)
```
Time Range: Use time picker ▾ / 10 minute window ▸

Auto Refresh Delay: No auto refresh ▾

Figure 4.38: Research query on Fortinet app.

Then we will have this dashboard as the final result.

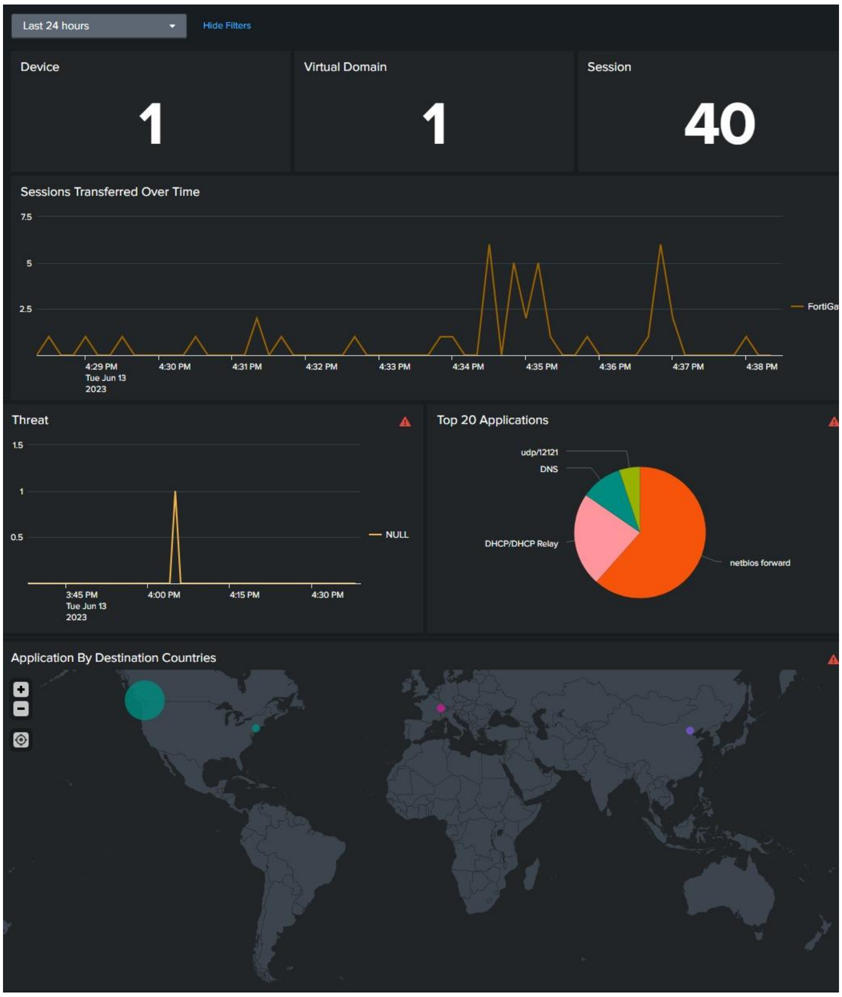


Figure 4.39: Network Security Dashboard.

- Traffic Dashboard:
  The Traffic Dashboard in the Fortinet Network Security system introduces a new approach compared to the previous dashboard. It incorporates a data model and a custom macro called "ftnt_dropdown" to enhance the search functionality and data population within the dashboard.

In order to configure the Traffic Dashboard, we followed these steps:

(a) we have to navigate to the traffic dashboard as illustrated in Figure 4.38.

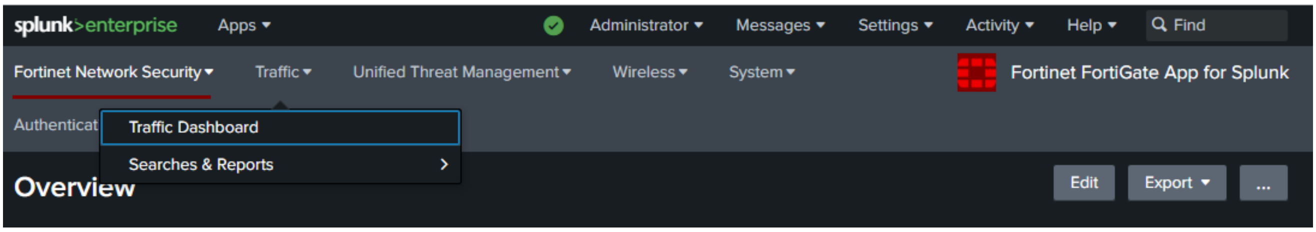
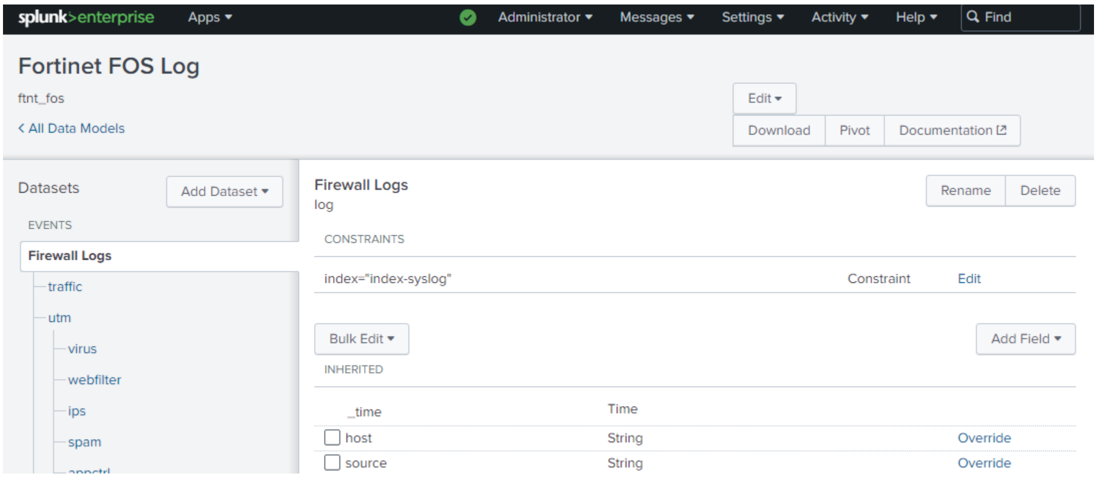


Figure 4.40: Navigate to the dashboard.

(b) Then We click on data models in the settings section to change Constraints from fgt_logs to index="index-syslog".

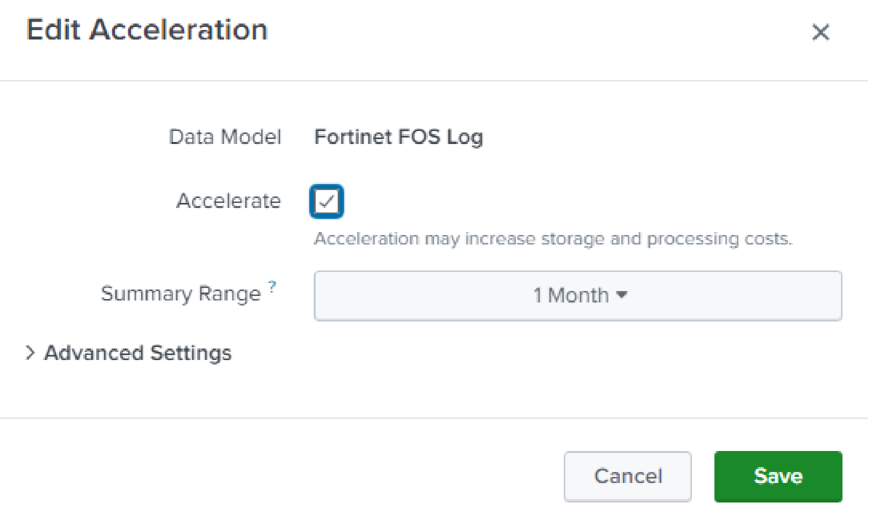


index="index-syslog"	Constraint	Edit

_time	Time	
□ host	String	Override
□ source	String	Override

Figure 4.41: change constraints.

(c) Finally we enable the acceleration to improve performance and enhanced data analysis.



Data Model: Fortinet FOS Log

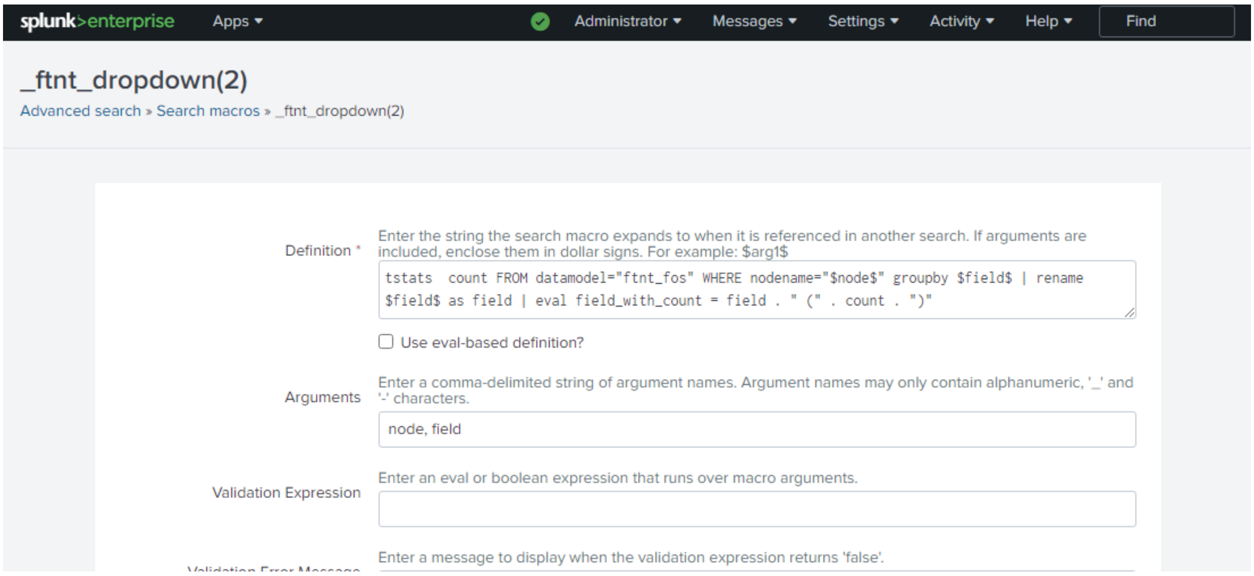
Accelerate: ☑

Acceleration may increase storage and processing costs.

Summary Range ?: 1 Month ▾

Figure 4.42: Enable configuration.

(d) To enhance search capabilities, we modified macros by removing summariesonly=true which is commonly used to retrieve only summary data instead of the full details of search results.



_ftnt_dropdown(2)

Advanced search » Search macros » _ftnt_dropdown(2)

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: $arg1$

```
tstats  count FROM datamodel="ftnt_fos" WHERE nodename="$node$" groupby $field$ | rename
$field$ as field | eval field_with_count = field . " (" . count . ")"
```

□ Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

node, field

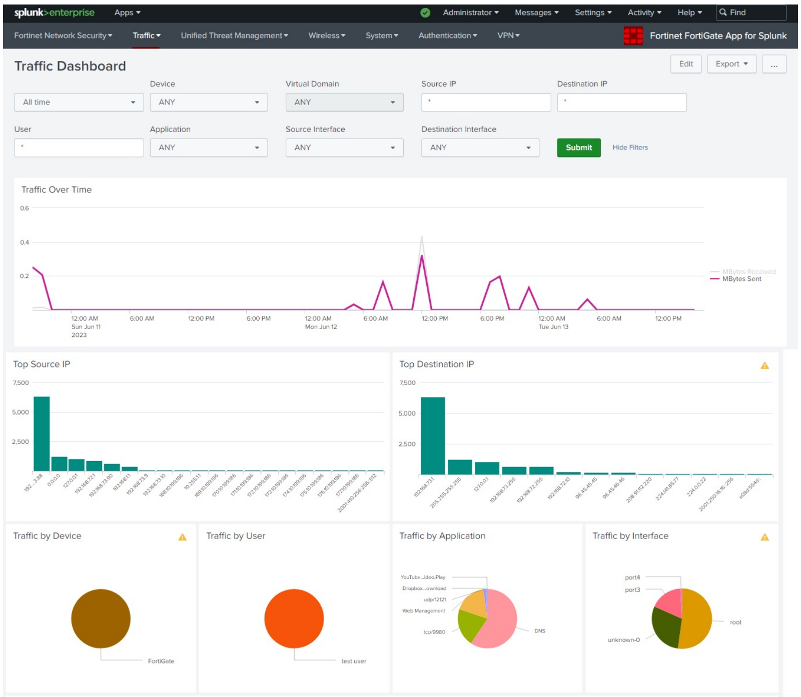
Validation Expression

Enter an eval or boolean expression that runs over macro arguments.

Enter a message to display when the validation expression returns 'false'.

Figure 4.43: Change macros.

(e) Finally we will have this dashboard as the final result.



Traffic Dashboard

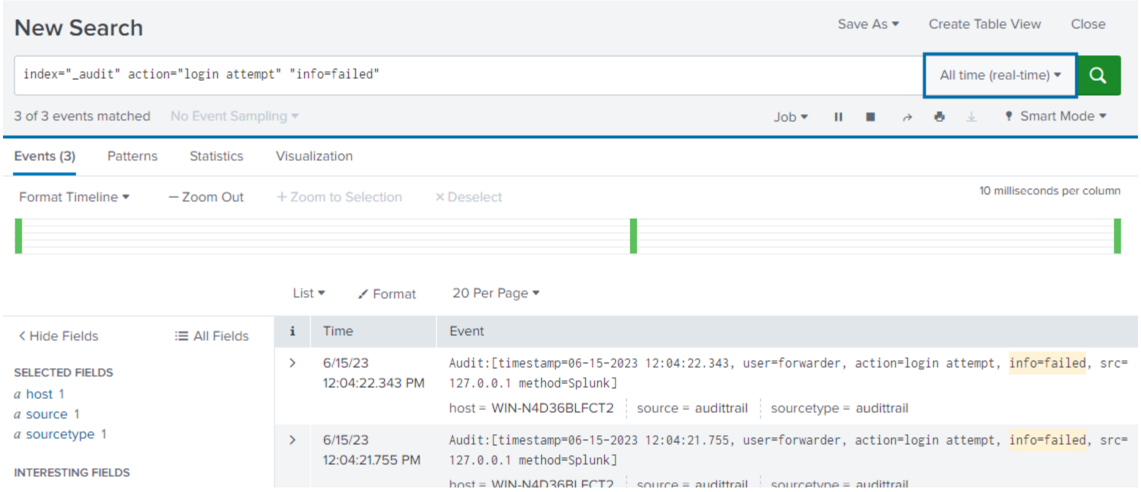
All time
Device: ANY
Virtual Domain: ANY
Source IP: *
Destination IP: *
User: *
Application: ANY
Source Interface: ANY
Destination Interface: ANY

Figure 4.44: Traffic dashboard.

4.4.3.2 Alert Configuration

Splunk uses alerts to proactively monitor machine data in real time, enabling the identification of issues, errors, or attacks before they impact customers and services. In this section, we will provide an example of monitoring failed login attempts.

- First, we run a search on our audit index for all events containing failed login attempts.



```
index="_audit" action="login attempt" "info=failed"
```

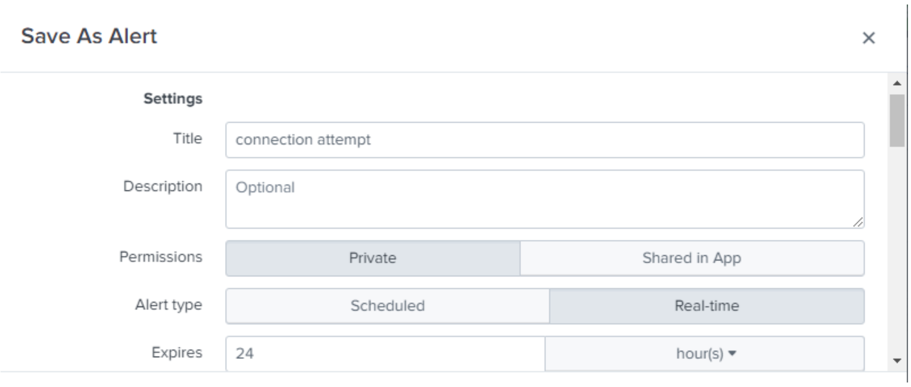
All time (real-time)

3 of 3 events matched   No Event Sampling

i	Time	Event
>	6/15/23 12:04:22.343 PM	Audit:[timestamp=06-15-2023 12:04:22.343, user=forwarder, action=login attempt, info=failed, src=127.0.0.1 method=Splunk] host = WIN-N4D36BLFCT2 source = audittrail sourcetype = audittrail
>	6/15/23 12:04:21.755 PM	Audit:[timestamp=06-15-2023 12:04:21.755, user=forwarder, action=login attempt, info=failed, src=127.0.0.1 method=Splunk] host = WIN-N4D36BLFCT2 source = audittrail sourcetype = audittrail

Figure 4.45: Audit index search.

- Then we select save as alert and give a title to the alert and adjust other settings.



Save As Alert

Settings

Title: connection attempt

Description: Optional

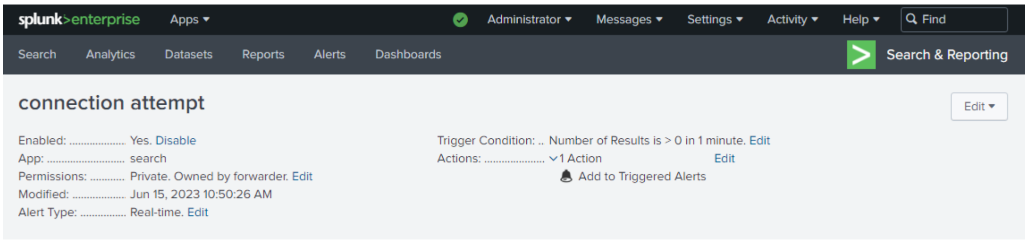
Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Expires: 24 hour(s)

Figure 4.46: Server login attempts.

- And here we can see the alert created.



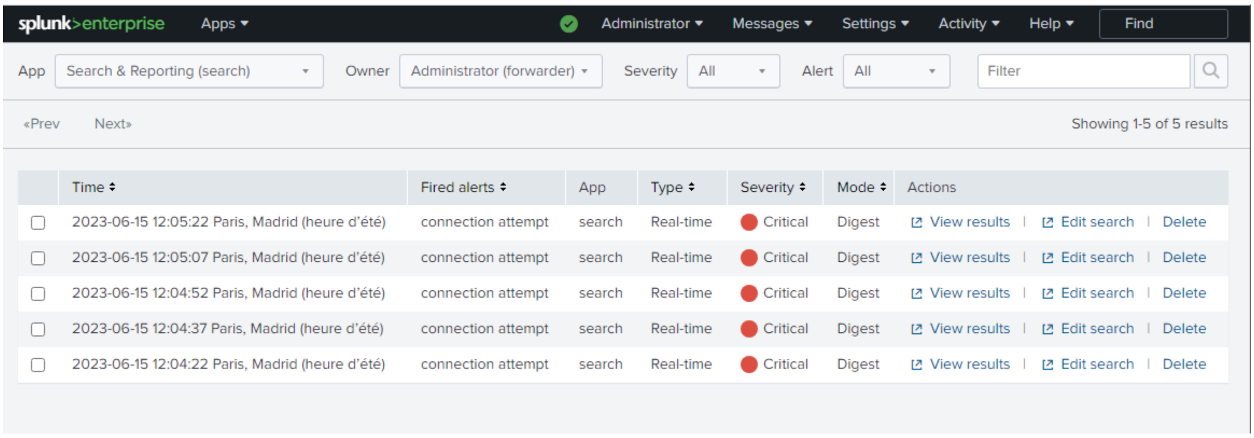
connection attempt

Enabled: Yes. Disable
App: search
Permissions: Private. Owned by forwarder. Edit
Modified: Jun 15, 2023 10:50:26 AM
Alert Type: Real-time. Edit

Trigger Condition: Number of Results is > 0 in 1 minute. Edit
Actions: 1 Action Edit
Add to Triggered Alerts

Figure 4.47: Alert created.

- We can view any triggered alerts by selecting an activity in the Splunk bar and clicking 'triggered alerts'



App: Search & Reporting (search) Owner: Administrator (forwarder) Severity: All Alert: All Filter

Showing 1-5 of 5 results

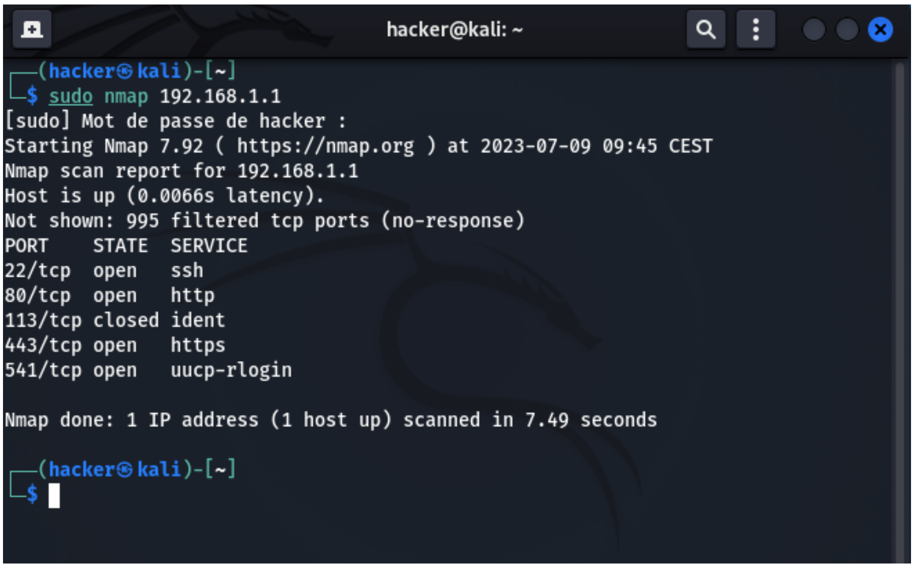
	Time	Fired alerts	App	Type	Severity	Mode	Actions
□	2023-06-15 12:05:22 Paris, Madrid (heure d'été)	connection attempt	search	Real-time	● Critical	Digest	View results | Edit search | Delete
□	2023-06-15 12:05:07 Paris, Madrid (heure d'été)	connection attempt	search	Real-time	● Critical	Digest	View results | Edit search | Delete
□	2023-06-15 12:04:52 Paris, Madrid (heure d'été)	connection attempt	search	Real-time	● Critical	Digest	View results | Edit search | Delete
□	2023-06-15 12:04:37 Paris, Madrid (heure d'été)	connection attempt	search	Real-time	● Critical	Digest	View results | Edit search | Delete
□	2023-06-15 12:04:22 Paris, Madrid (heure d'été)	connection attempt	search	Real-time	● Critical	Digest	View results | Edit search | Delete

Figure 4.48: Alerts.

4.4.3.3 Simulation of an attack scenario

In this section, we will perform a deployment test of the Splunk security software. To do this, we will set up a virtual machine (Kali Linux).
It is crucial to emphasize that this test must be conducted within a controlled and authorized environment, adhering to established security policies and relevant laws. The purpose of this test is to simulate a targeted attack on the network infrastructure equipment being monitored by Splunk. The aim is to evaluate the efficiency of this solution in the real time detection of attacks, incidents, and malicious activities.

1. **Attack attempt**
   On the virtual machine (Kali Linux), we are conducting a security test using the command line to simulate an attempt to attack the FortiGate firewall. "sudo nmap 192.168.1.1" This command is used in this context to perform a network scan on the IP address 192.168.1.1.
   Scanning this IP address with Nmap helps in gathering information about open ports, services running on those ports, and potential vulnerabilities in the FortiGate firewall. This information can be valuable for assessing the security posture and identifying potential weak points that may be exploited during a simulated attack.

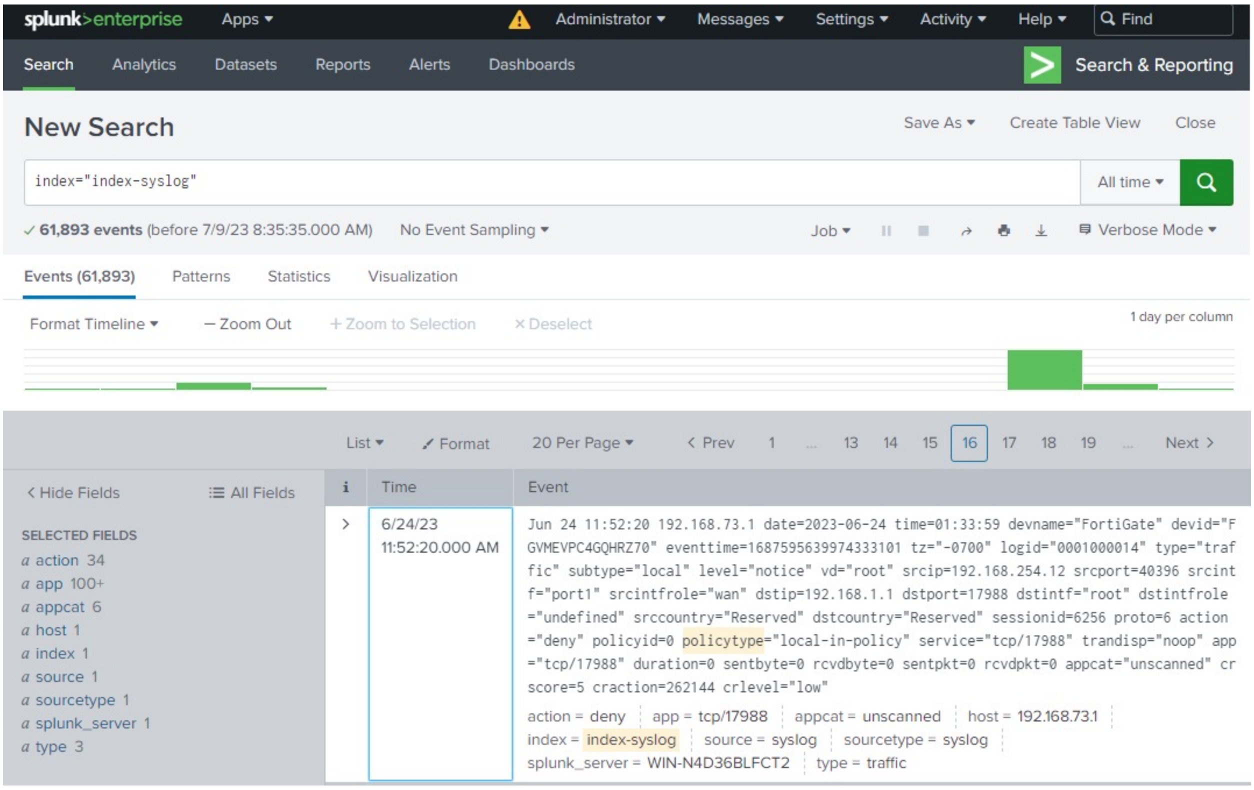


```
┌──(hacker㉿kali)-[~]
└─$ sudo nmap 192.168.1.1
[sudo] Mot de passe de hacker :
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-09 09:45 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0066s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
113/tcp closed ident
443/tcp open   https
541/tcp open   uucp-rlogin

Nmap done: 1 IP address (1 host up) scanned in 7.49 seconds

┌──(hacker㉿kali)-[~]
└─$ ▮
```

Figure 4.49: Ports Scanning Attack.

2. **Result Test**

   After executing the attack attempt, Splunk provides a comprehensive display of detailed information regarding the events and logs it has gathered as shown in Figure 4.50.



```
index="index-syslog"
```

✓ 61,893 events (before 7/9/23 8:35:35.000 AM)

SELECTED FIELDS
a action 34
a app 100+
a appcat 6
a host 1
a index 1
a source 1
a sourcetype 1
a splunk_server 1
a type 3

6/24/23
11:52:20.000 AM

```
Jun 24 11:52:20 192.168.73.1 date=2023-06-24 time=01:33:59 devname="FortiGate" devid="F
GVMEVPC4GQHRZ70" eventtime=1687595639974333101 tz="-0700" logid="0001000014" type="traf
fic" subtype="local" level="notice" vd="root" srcip=192.168.254.12 srcport=40396 srcint
f="port1" srcintfrole="wan" dstip=192.168.1.1 dstport=17988 dstintf="root" dstintfrole
="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=6256 proto=6 action
="deny" policyid=0 policytype="local-in-policy" service="tcp/17988" trandisp="noop" app
="tcp/17988" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 appcat="unscanned" cr
score=5 craction=262144 crlevel="low"
```

action = deny | app = tcp/17988 | appcat = unscanned | host = 192.168.73.1
index = index-syslog | source = syslog | sourcetype = syslog
splunk_server = WIN-N4D36BLFCT2 | type = traffic

Figure 4.50: Syslog logs.

Final deployment result

Regarding the work performed, we started by installing the Splunk security software and configuring it for deployment on the proposed network infrastructure mentioned earlier in this chapter. This also includes configuring Splunk tools for real-time monitoring. The tests conducted, as well as the visualization results, have demonstrated the crucial role of Splunk in this context.
In addition, we have also conducted tests to evaluate its effectiveness. These tests included simulating an attack scenario to assess the capabilities of Splunk in detecting and responding to security threats.

Conclusion

In conclusion, this chapter has presented the implementation details of the proposed SIEM solution using Splunk Enterprise. We discussed the new deployment architecture, the development environment, the settings of the monitoring environment, and the steps for installing and configuring Splunk. By following these steps, a robust SIEM system has been successfully established, capable of efficiently collecting, analyzing, and managing log data from various sources. This system enables effective security monitoring and threat detection, enhancing overall cybersecurity.

General Conclusion and Future Perspectives

In conclusion, this master thesis project focused on the implementation of a SIEM solution using the Splunk Enterprise tool, specifically within the context of Sonelgaz Bejaia. The project successfully established a robust system that efficiently collects, analyzes and manages log data from various sources. The implementation of the SIEM solution in Sonelgaz Bejaia brings several important benefits. It enables effective security monitoring by centralizing and correlating log data from diverse sources, allowing for prompt detection and response to potential security incidents. The system enhances the organization's cybersecurity posture by providing insights into its security landscape and enables proactive measures to mitigate risks. Continuous improvement and fine-tuning of the SIEM solution should be a priority, including refining log data collection and analysis processes, implementing advanced correlation techniques, and integrating additional security tools. Expanding the solution to cover a broader range of security domains, such as incorporating threat intelligence feeds and user behavior analytics, can enhance its effectiveness. Integration with incident response processes and automation can improve incident handling while exploring emerging technologies like machine learning and artificial intelligence can enhance anomaly detection and predictive analytics.

Appendix A

This section presents the steps for installing the GNS3 software and associated virtual machines.

A.1 Graphical Network Simulator-3 (GNS3) Installation steps

GNS3 (Graphical Network Simulator) is a network simulation and emulation software that allows users to design, simulate, and troubleshoot complex network topologies. To install GNS3, you need to begin by downloading the executable file from the official GNS3 website at
https://www.gns3.com. Once the download is complete, launch the executable file and run it, following any provided on-screen instructions or steps illustrated in a figure. During the installation process, patiently wait for it to complete. Once finished, click on "Finish" to exit the installer.

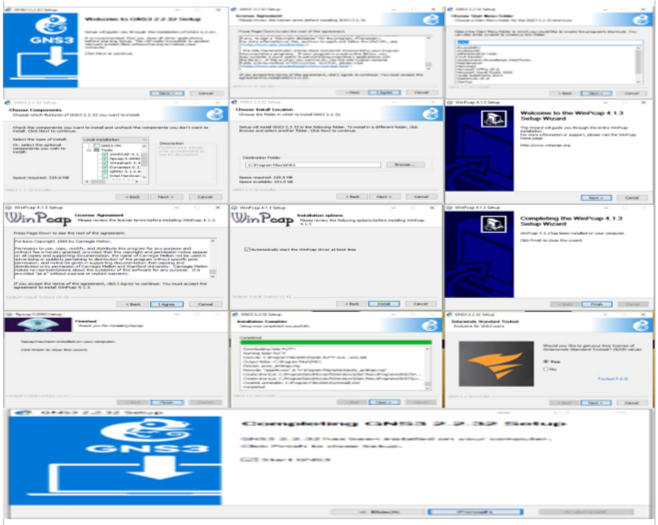
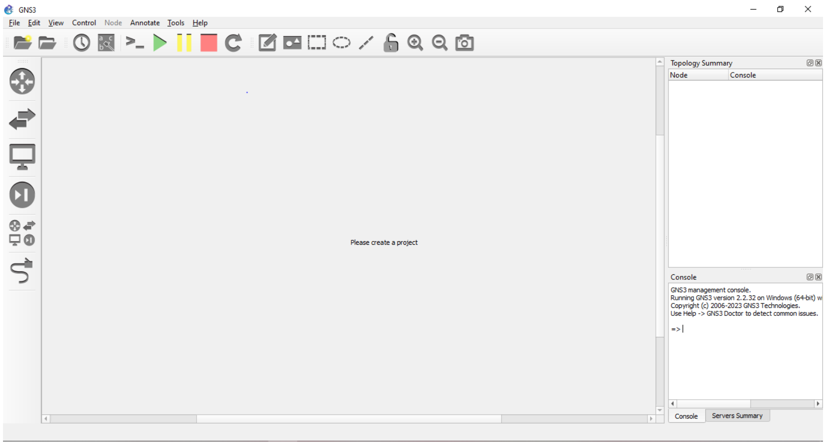


Figure A.1: GNS3 Installations steps.

The following figure shows the GNS3 interface:



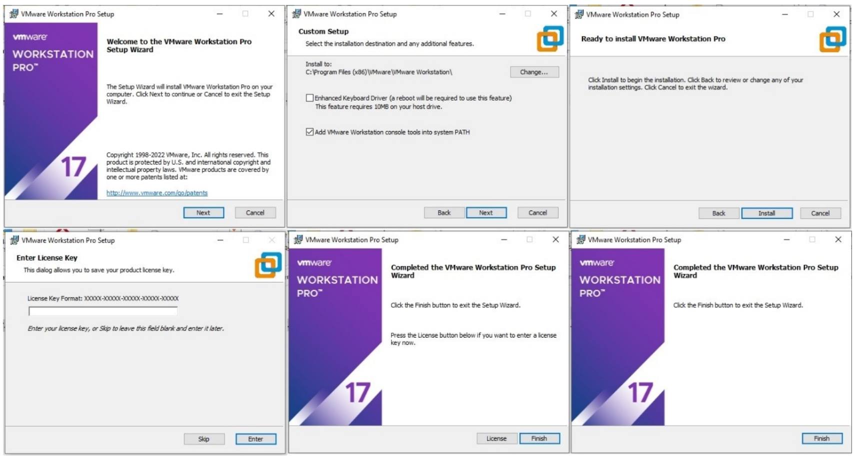
```
GNS3 management console.
Running GNS3 version 2.2.32 on Windows (64-bit) w
Copyright (c) 2006-2023 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

Figure A.2: GNS3 interface.

A.2 VMware Workstation Installation Steps

VMware Workstation is virtual machine software for running multiple operating systems on a single computer. It supports x86 and x86-64 systems and enables simultaneous operation of Microsoft, Linux, and other OS instances. VMware Workstation facilitates seamless integration between the host and virtual machines, ensuring compatibility with hardware resources like hard disks, USB devices, and CD-ROMs. Device drivers are installed through the host machine.

To install VMware Workstation, we obtain the installer from the official website and check system requirements. Running the installer, we accept the End User License Agreement and select installation options. We can enter the license key or proceed with the trial version, customize data sharing preferences, and review the installation summary. Once started, we wait for the installation to complete and then click the button to finish the process.



Welcome to the VMware Workstation Pro Setup Wizard

The Setup Wizard will install VMware Workstation Pro on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Copyright 1998-2022 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at:

http://www.vmware.com/go/patents

Custom Setup

Select the installation destination and any additional features.

Install to:
C:\Program Files (x86)\VMware\VMware Workstation\

□ Enhanced Keyboard Driver (a reboot will be required to use this feature)
This feature requires 10MB on your host drive.

☑ Add VMware Workstation console tools into system PATH

Ready to install VMware Workstation Pro

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Enter License Key

This dialog allows you to save your product license key.

License Key Format: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Enter your license key, or Skip to leave this field blank and enter it later.

Completed the VMware Workstation Pro Setup Wizard

Click the Finish button to exit the Setup Wizard.

Press the License button below if you want to enter a license key now.

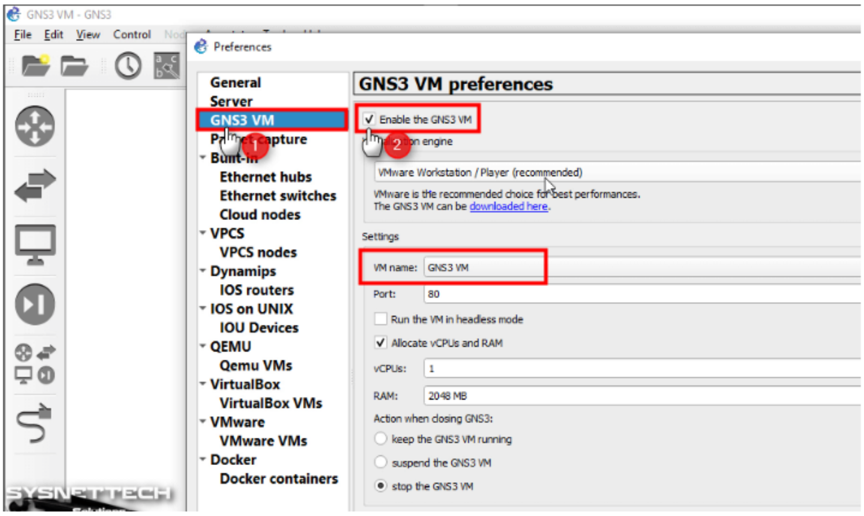
Completed the VMware Workstation Pro Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure A.3: VMware workstation installation.

Link to GNS3:
we start by clicking on the GNS3 VM option. Next, we select the "Enable the GNS3 VM" option from the settings in the right section. After confirming the virtual server's name imported in the VM Name section, we click the OK button.

Additionally, we have the option to modify the port number of the virtual server and configure the GNS3 VM to be turned off when closing the GNS3 program.



GNS3 VM preferences

☑ Enable the GNS3 VM

Virtualization engine: VMware Workstation / Player (recommended)

VMware is the recommended choice for best performances.
The GNS3 VM can be downloaded here.

Settings

VM name: GNS3 VM

Port: 80

☐ Run the VM in headless mode

☑ Allocate vCPUs and RAM

vCPUs: 1

RAM: 2048 MB

Action when closing GNS3:

○ keep the GNS3 VM running

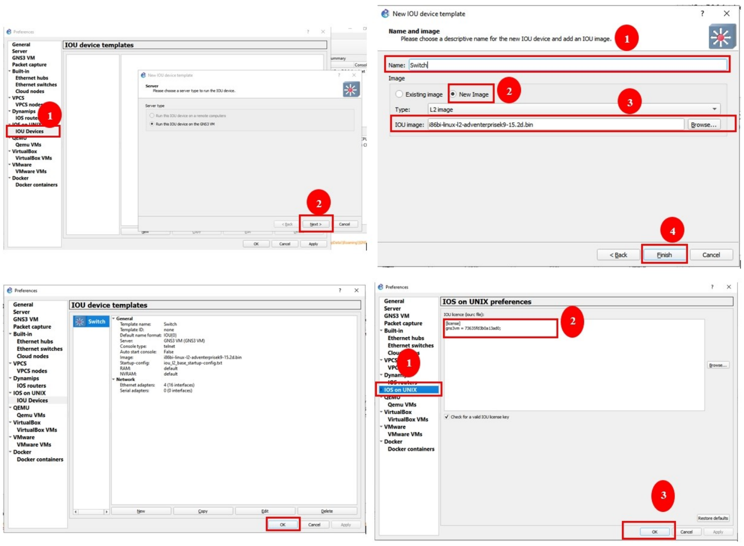
○ suspend the GNS3 VM

● stop the GNS3 VM

Figure A.4: Link VM to GNS3.

A.3 Import network simulation devices

Switch:
To import a switch into GNS3, we browse for the IOU or VPCS file to import. then we select the appropriate template for the switch and review the provided information. Finally, we proceed with the import process by following the on-screen instructions.



New IOU device template

Name and image
Please choose a descriptive name for the new IOU device and add an IOU image.

Name: Switch

Image

○ Existing image ● New Image

Type: L2 image

IOU image: i86bi-linux-l2-adventerprisek9-15.2d.bin

IOU device templates

General
Template name: Switch
Template ID: none
Default name format: IOU{0}
Server: GNS3 VM (GNS3 VM)
Console type: telnet
Auto start console: False
Image: i86bi-linux-l2-adventerprisek9-15.2d.bin
Startup-config: iou_l2_base_startup-config.txt
RAM: default
NVRAM: default
Network
Ethernet adapters: 4 (16 interfaces)
Serial adapters: 0 (0 interfaces)

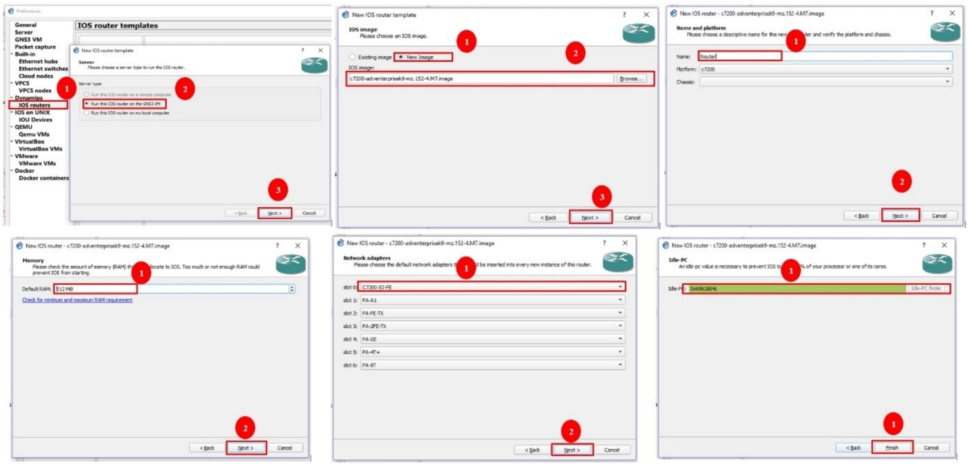
IOS on UNIX preferences

IOU licence (iourc file):
[license]
gns3vm = 73635fd3b0a13ad0;

☑ Check for a valid IOU license key

Figure A.5: Import Switch.

Router:
To import a router we configure a router template. Then, we import the router image by browsing for the IOS file and selecting the suitable template.



Preferences — IOS router templates — Dynamips — IOS routers

New IOS router template — Server: Please choose a server type to run the IOS router. Server type: ● Run this IOS router on the GNS3 VM

New IOS router template — IOS image: Please choose an IOS image. ● New Image. IOS image: c7200-adventerprisek9-mz.152-4.M7.image

New IOS router - c7200-adventerprisek9-mz.152-4.M7.image — Name and platform: Name: Router; Platform: c7200

Memory: Default RAM: 512 MiB

Network adapters: slot 0: C7200-IO-FE; slot 1: PA-A1; slot 2: PA-FE-TX; slot 3: PA-2FE-TX; slot 4: PA-GE; slot 5: PA-4T+; slot 6: PA-8T

Idle-PC: Idle-PC: 0x6062dd4c

Figure A.6: Import Router.

FortiGate firewall

To import a FortiGate firewall into GNS3, we need to obtain a compatible FortiGate firewall image with a (.qcow2) extension. After acquiring the image file, we open the GNS3 interface and navigate to the "File" option in the top menu. From there, we select "Import appliance" and locate the FortiGate firewall image file we obtained. We patiently wait for the import process to complete. Once finished, we will find the FortiGate firewall listed in the GNS3 workspace, ready for use.

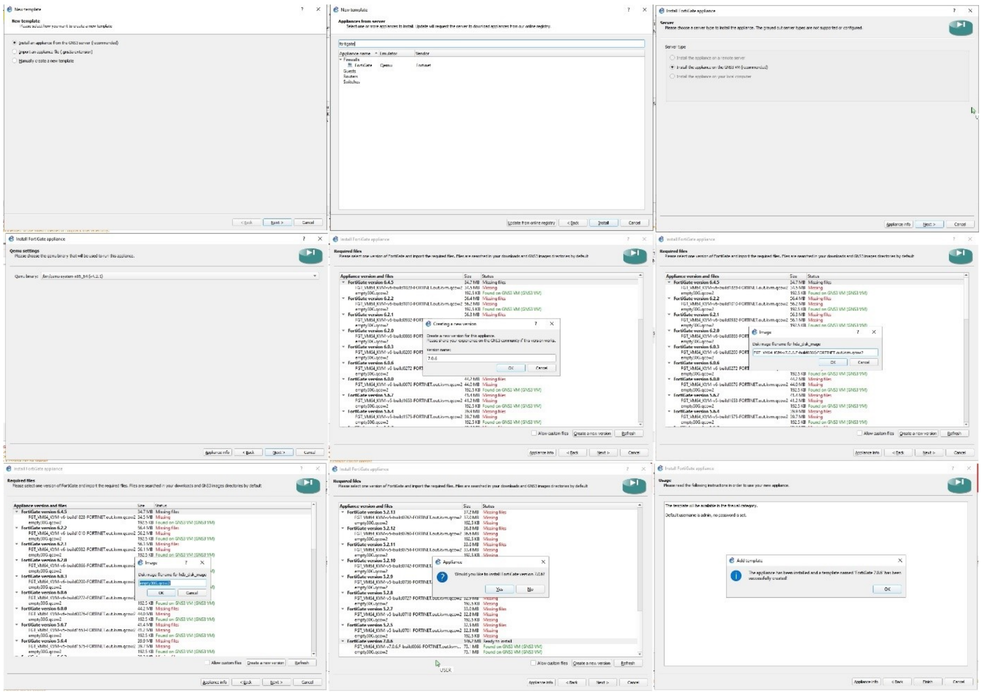


Figure A.7: Import Fortigate firewall.

A.3.1 Installation of virtual machines

Ubuntu Desktop: ubuntu desktop introduces various improvements such as an improved user interface design, performance optimization measures, and crucial security updates, the aim is to create an operating.

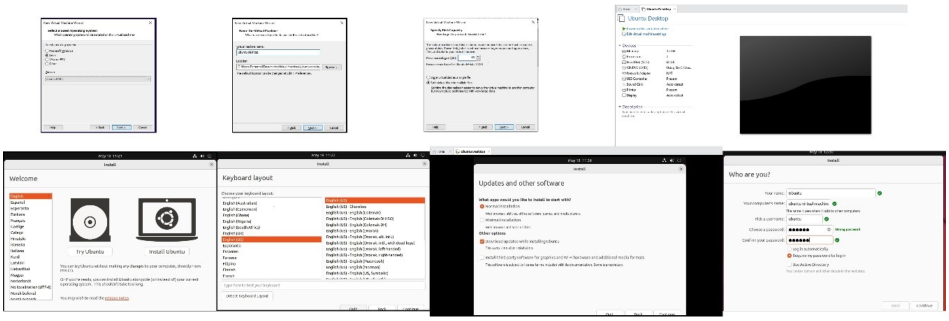


Figure A.8: Ubuntu desktop installation.

Windows Server 2022 offers enhanced security protocols, optimized performance, and superior scalability, making it the ideal choice for modern data centers. Its advanced integrations enable effortless implementation of Azure services, ensuring smooth operation across functions, especially in hybrid cloud use cases.

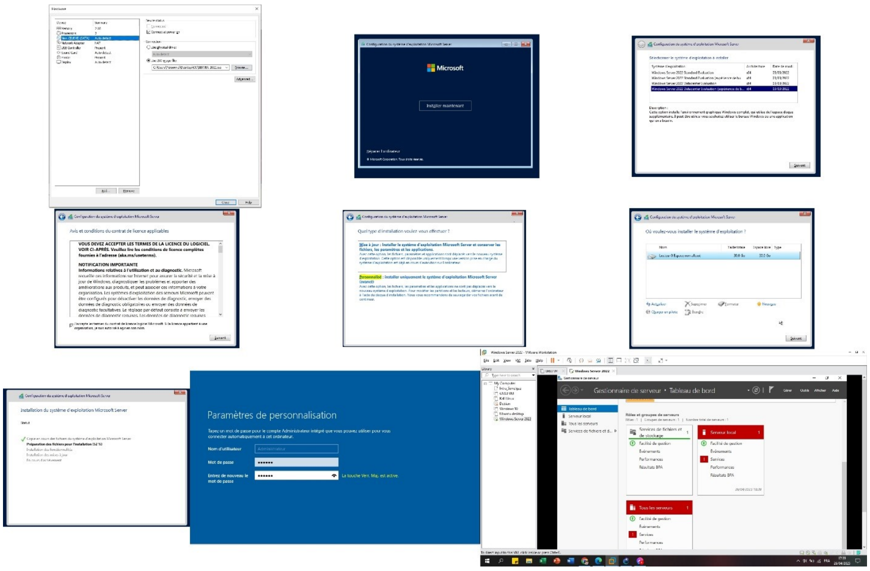
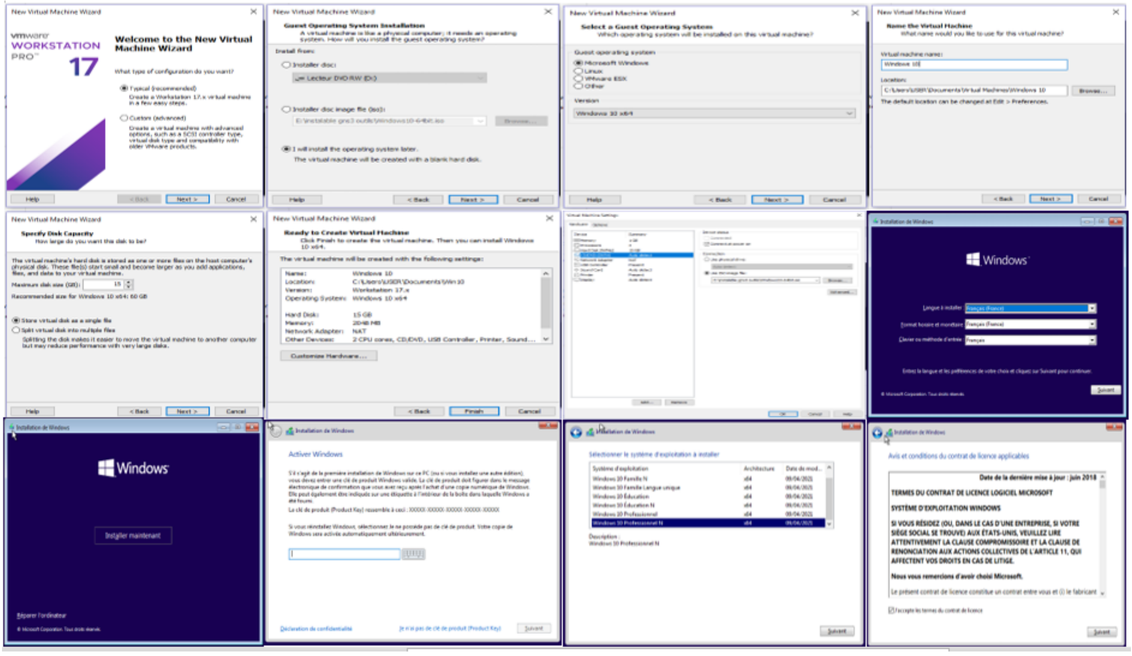


Figure A.9: Windows server installation.

Windows 10: Is a highly popular operating system that was developed by Microsoft. The sophisticated yet understandable interface caters to users from varying backgrounds while the compatible nature of the system ensures it can be utilized on numerous hardware devices or with different software programs. Due to regular feature updates packed with added levels of security protection, this OS remains flexible enough for both personal use and business purposes.



New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

● Typical (recommended)
Create a Workstation 17.x virtual machine in a few easy steps.

○ Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

New Virtual Machine Wizard

Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:
Lecteur DVD RW (D:)

○ Installer disc image file (iso):
E:\installable gns3 outils\Windows10-64bit.iso

● I will install the operating system later.
The virtual machine will be created with a blank hard disk.

New Virtual Machine Wizard

Select a Guest Operating System
Which operating system will be installed on this virtual machine?

Guest operating system
● Microsoft Windows
○ Linux
○ VMware ESX
○ Other

Version
Windows 10 x64

New Virtual Machine Wizard

Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:
Windows 10

Location:
C:\Users\USER\Documents\Virtual Machines\Windows 10

The default location can be changed at Edit > Preferences.

New Virtual Machine Wizard

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 15

Recommended size for Windows 10 x64: 60 GB

● Store virtual disk as a single file
○ Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

New Virtual Machine Wizard

Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Windows 10 x64.

The virtual machine will be created with the following settings:

Name:	Windows 10
Location:	C:\Users\USER\Documents\Win 10
Version:	Workstation 17.x
Operating System:	Windows 10 x64
Hard Disk:	15 GB
Memory:	2048 MB
Network Adapter:	NAT
Other Devices:	2 CPU cores, CD/DVD, USB Controller, Printer, Sound....

Installation de Windows

Langue à installer : Français (France)
Format horaire et monétaire : Français (France)
Clavier ou méthode d'entrée : Français

Entrez la langue et les préférences de votre choix et cliquez sur Suivant pour continuer.

© Microsoft Corporation. Tous droits réservés.

Installation de Windows

Réparer l'ordinateur

© Microsoft Corporation. Tous droits réservés.

Installation de Windows

Activer Windows

S'il s'agit de la première installation de Windows sur ce PC (ou si vous installez une autre édition), vous devez entrer une clé de produit Windows valide. La clé de produit doit figurer dans le message électronique de confirmation que vous avez reçu après l'achat d'une copie numérique de Windows. Elle peut également être indiquée sur une étiquette à l'intérieur de la boîte dans laquelle Windows a été fourni.

La clé de produit (Product Key) ressemble à ceci : XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Si vous réinstallez Windows, sélectionnez Je ne possède pas de clé de produit. Votre copie de Windows sera activée automatiquement ultérieurement.

Déclaration de confidentialité

Je n'ai pas de clé de produit (Product Key)

Installation de Windows

Sélectionner le système d'exploitation à installer

Système d'exploitation	Architecture	Date de mod...
Windows 10 Famille N	x64	09/04/2021
Windows 10 Famille Langue unique	x64	09/04/2021
Windows 10 Éducation	x64	09/04/2021
Windows 10 Éducation N	x64	09/04/2021
Windows 10 Professionnel	x64	09/04/2021
Windows 10 Professionnel N	x64	09/04/2021

Description :
Windows 10 Professionnel N

Installation de Windows

Avis et conditions du contrat de licence applicables

Date de la dernière mise à jour : juin 2018

TERMES DU CONTRAT DE LICENCE LOGICIEL MICROSOFT

SYSTÈME D'EXPLOITATION WINDOWS

SI VOUS RÉSIDEZ (OU, DANS LE CAS D'UNE ENTREPRISE, SI VOTRE SIÈGE SOCIAL SE TROUVE) AUX ÉTATS-UNIS, VEUILLEZ LIRE ATTENTIVEMENT LA CLAUSE COMPROMISSOIRE ET LA CLAUSE DE RENONCIATION AUX ACTIONS COLLECTIVES DE L'ARTICLE 11, QUI AFFECTENT VOS DROITS EN CAS DE LITIGE.

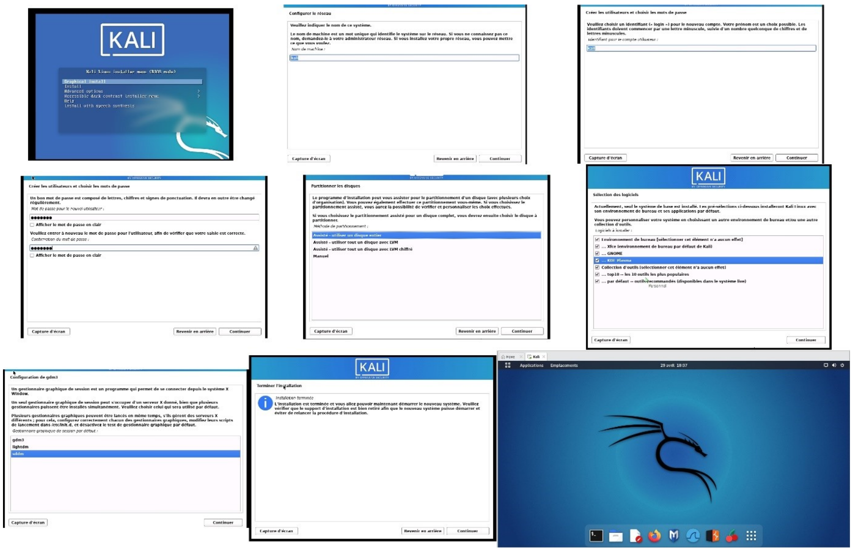
Nous vous remercions d'avoir choisi Microsoft.

Le présent contrat de licence constitue un contrat entre vous et (i) le fabricant

☑ J'accepte les termes du contrat de licence

Figure A.10: Windows 10 installation.

Kali Linux : Is an exceptional operating system designed explicitly for advanced penetration testing activities under ethical boundaries with remarkable efficiency. The vast array of pre-installed tools and utilities available on the platform has been particularly useful to security experts worldwide.



```
Kali Linux installer menu (BIOS mode)
Graphical install
Install
Advanced options                       >
Accessible dark contrast installer menu >
Help
Install with speech synthesis
```

Configurer le réseau

Veuillez indiquer le nom de ce système.

Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez-le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.

Nom de machine :
kali

Créer les utilisateurs et choisir les mots de passe

Veuillez choisir un identifiant (« login ») pour le nouveau compte. Votre prénom est un choix possible. Les identifiants doivent commencer par une lettre minuscule, suivie d'un nombre quelconque de chiffres et de lettres minuscules.

Identifiant pour le compte utilisateur :
kali

Créer les utilisateurs et choisir les mots de passe

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Mot de passe pour le nouvel utilisateur :
●●●●●●●
☐ Afficher le mot de passe en clair

Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.

Confirmation du mot de passe :
●●●●●●●
☐ Afficher le mot de passe en clair

Partitionner les disques

Le programme d'installation peut vous assister pour le partitionnement d'un disque (avec plusieurs choix d'organisation). Vous pouvez également effectuer ce partitionnement vous-même. Si vous choisissez le partitionnement assisté, vous aurez la possibilité de vérifier et personnaliser les choix effectués.

Si vous choisissez le partitionnement assisté pour un disque complet, vous devrez ensuite choisir le disque à partitionner.

Méthode de partitionnement :
Assisté - utiliser un disque entier
Assisté - utiliser tout un disque avec LVM
Assisté - utiliser tout un disque avec LVM chiffré
Manuel

Sélection des logiciels

Actuellement, seul le système de base est installé. Les pré-sélections ci-dessous installeront Kali Linux avec son environnement de bureau et ses applications par défaut.

Vous pouvez personnaliser votre système en choisissant un autre environnement de bureau et/ou une autre collection d'outils.

Logiciels à installer :
☑ Environnement de bureau [sélectionner cet élément n'a aucun effet]
☑ ... Xfce (environnement de bureau par défaut de Kali)
☑ ... GNOME
☑ ... KDE Plasma
☑ Collection d'outils [sélectionner cet élément n'a aucun effet]
☑ ... top10 -- les 10 outils les plus populaires
☑ ... par défaut -- outils recommandés (disponibles dans le système live)

Configuration de gdm3

Un gestionnaire graphique de session est un programme qui permet de se connecter depuis le système X Window.

Un seul gestionnaire graphique de session peut s'occuper d'un serveur X donné, bien que plusieurs gestionnaires puissent être installés simultanément. Veuillez choisir celui qui sera utilisé par défaut.

Plusieurs gestionnaires graphiques peuvent être lancés en même temps, s'ils gèrent des serveurs X différents ; pour cela, configurez correctement chacun des gestionnaires graphiques, modifiez leurs scripts de lancement dans /etc/init.d, et désactivez le test de gestionnaire graphique par défaut.

Gestionnaire graphique de session par défaut :
gdm3
lightdm
sddm

Terminer l'installation

Installation terminée
L'installation est terminée et vous allez pouvoir maintenant démarrer le nouveau système. Veuillez vérifier que le support d'installation est bien retiré afin que le nouveau système puisse démarrer et éviter de relancer la procédure d'installation.

Figure A.11: Kali Linux installation.

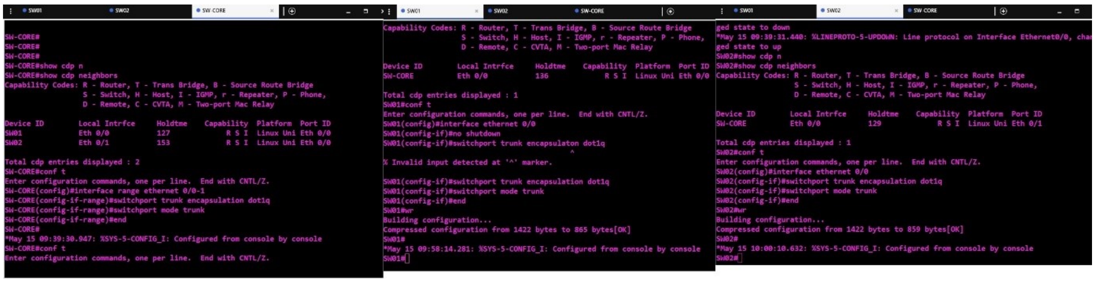
Appendix B

To set up a basic network topology, we need to consider the devices, connections, and addressing scheme. In this section, we will present our basic network topology configuration.

B.1 Configuration of a basic network topology

B.1.1 Configuration of trunk ports

A trunk port is a network port on a switch that is used to carry traffic for multiple VLANs (Virtual LANs). It allows for the transmission of data from multiple VLANs over a single physical link. Here are the steps of configuration:



```
SW-CORE#
SW-CORE#
SW-CORE#
SW-CORE#show cdp n
SW-CORE#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SW01             Eth 0/0           127              R S I  Linux Uni Eth 0/0
SW02             Eth 0/1           153              R S I  Linux Uni Eth 0/0

Total cdp entries displayed : 2
SW-CORE#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-CORE(config)#interface range ethernet 0/0-1
SW-CORE(config-if-range)#switchport trunk encapsulation dot1q
SW-CORE(config-if-range)#switchport mode trunk
SW-CORE(config-if-range)#end
SW-CORE#
*May 15 09:39:30.947: %SYS-5-CONFIG_I: Configured from console by console
SW-CORE#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SW-CORE          Eth 0/0           136              R S I  Linux Uni Eth 0/0

Total cdp entries displayed : 1
SW01#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW01(config)#interface ethernet 0/0
SW01(config-if)#no shutdown
SW01(config-if)#switchport trunk encapsulaton dot1q
                                              ^
% Invalid input detected at '^' marker.

SW01(config-if)#switchport trunk encapsulation dot1q
SW01(config-if)#switchport mode trunk
SW01(config-if)#end
SW01#wr
Building configuration...
Compressed configuration from 1422 bytes to 865 bytes[OK]
SW01#
*May 15 09:58:14.281: %SYS-5-CONFIG_I: Configured from console by console
SW01#
```

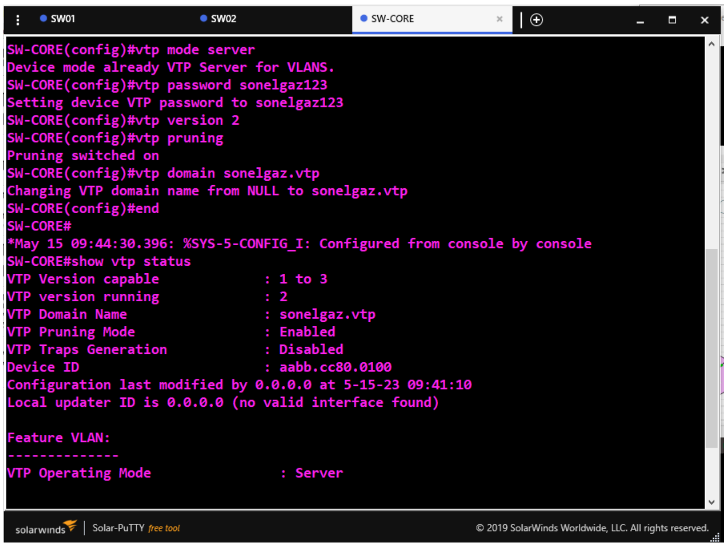
```
ged state to down
*May 15 09:39:31.440: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, cha
ged state to up
SW02#show cdp n
SW02#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SW-CORE          Eth 0/0           129              R S I  Linux Uni Eth 0/1

Total cdp entries displayed : 1
SW02#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW02(config)#interface ethernet 0/0
SW02(config-if)#switchport trunk encapsulation dot1q
SW02(config-if)#switchport mode trunk
SW02(config-if)#end
SW02#wr
Building configuration...
Compressed configuration from 1422 bytes to 859 bytes[OK]
SW02#
*May 15 10:00:10.632: %SYS-5-CONFIG_I: Configured from console by console
SW02#
```

Figure B.1: Trunk configuration.

B.1.2 Configuration of VTP protocol

VTP (VLAN Trunking Protocol) is a Cisco proprietary protocol used for managing VLANs (Virtual Local Area Networks) on a Cisco switch infrastructure. It allows for easy VLAN configuration and synchronization across multiple switches in a network.

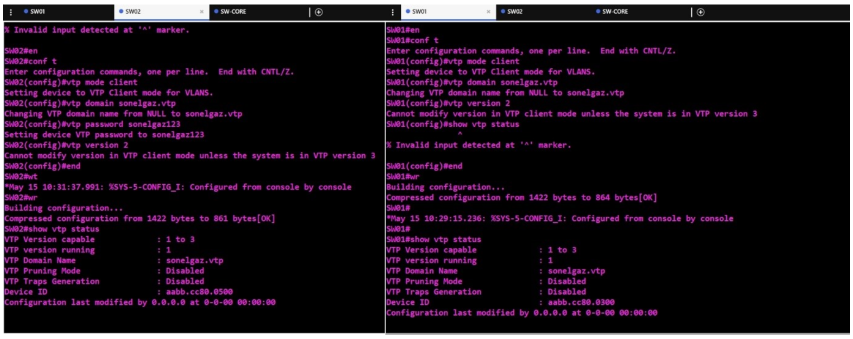
VTP in Server mode



```
SW-CORE(config)#vtp mode server
Device mode already VTP Server for VLANS.
SW-CORE(config)#vtp password sonelgaz123
Setting device VTP password to sonelgaz123
SW-CORE(config)#vtp version 2
SW-CORE(config)#vtp pruning
Pruning switched on
SW-CORE(config)#vtp domain sonelgaz.vtp
Changing VTP domain name from NULL to sonelgaz.vtp
SW-CORE(config)#end
SW-CORE#
*May 15 09:44:30.396: %SYS-5-CONFIG_I: Configured from console by console
SW-CORE#show vtp status
VTP Version capable              : 1 to 3
VTP version running              : 2
VTP Domain Name                  : sonelgaz.vtp
VTP Pruning Mode                 : Enabled
VTP Traps Generation             : Disabled
Device ID                        : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 5-15-23 09:41:10
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                 : Server
```

Figure B.2: VTP server mode.

VTP in Client mode



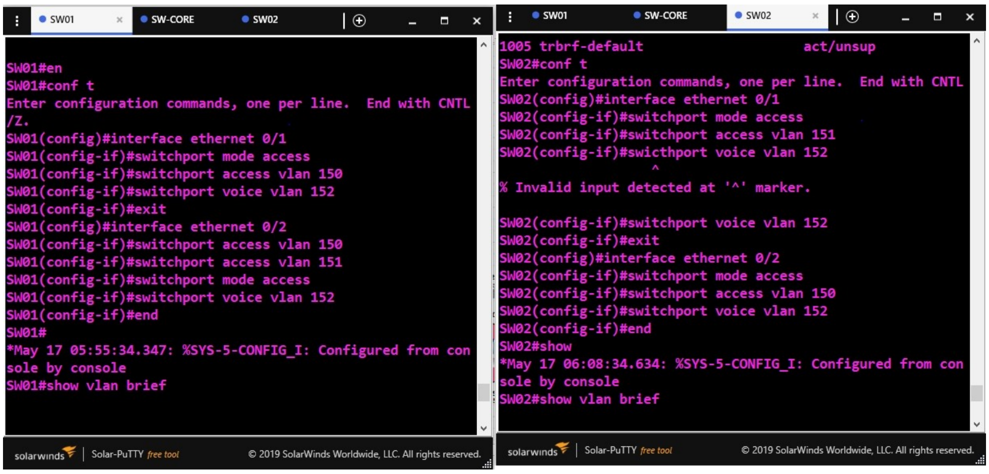
```
% Invalid input detected at '^' marker.

SW02#en
SW02#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW02(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SW02(config)#vtp domain sonelgaz.vtp
Changing VTP domain name from NULL to sonelgaz.vtp
SW02(config)#vtp password sonelgaz123
Setting device VTP password to sonelgaz123
SW02(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
SW02(config)#end
SW02#wt
*May 15 10:31:37.991: %SYS-5-CONFIG_I: Configured from console by console
SW02#wr
Building configuration...
Compressed configuration from 1422 bytes to 861 bytes[OK]
SW02#show vtp status
VTP Version capable              : 1 to 3
VTP version running              : 1
VTP Domain Name                  : sonelgaz.vtp
VTP Pruning Mode                 : Disabled
VTP Traps Generation             : Disabled
Device ID                        : aabb.cc80.0500
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

```
SW01#en
SW01#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW01(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SW01(config)#vtp domain sonelgaz.vtp
Changing VTP domain name from NULL to sonelgaz.vtp
SW01(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
SW01(config)#show vtp status
               ^
% Invalid input detected at '^' marker.

SW01(config)#end
SW01#wr
Building configuration...
Compressed configuration from 1422 bytes to 864 bytes[OK]
SW01#
*May 15 10:29:15.236: %SYS-5-CONFIG_I: Configured from console by console
SW01#
SW01#show vtp status
VTP Version capable              : 1 to 3
VTP version running              : 1
VTP Domain Name                  : sonelgaz.vtp
VTP Pruning Mode                 : Disabled
VTP Traps Generation             : Disabled
Device ID                        : aabb.cc80.0300
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Figure B.3: VTP Client mode.

B.1.3 VLAN port assignment

When configuring VLANs (Virtual Local Area Networks) on a network switch, one of the important steps is to assign ports to specific VLANs.This process allows you to control network traffic by segmenting it into different virtual LANs based on specific criteria.



```
SW01#en
SW01#conf t
Enter configuration commands, one per line.  End with CNTL
/Z.
SW01(config)#interface ethernet 0/1
SW01(config-if)#switchport mode access
SW01(config-if)#switchport access vlan 150
SW01(config-if)#switchport voice vlan 152
SW01(config-if)#exit
SW01(config)#interface ethernet 0/2
SW01(config-if)#switchport access vlan 150
SW01(config-if)#switchport access vlan 151
SW01(config-if)#switchport mode access
SW01(config-if)#switchport voice vlan 152
SW01(config-if)#end
SW01#
*May 17 05:55:34.347: %SYS-5-CONFIG_I: Configured from con
sole by console
SW01#show vlan brief
```

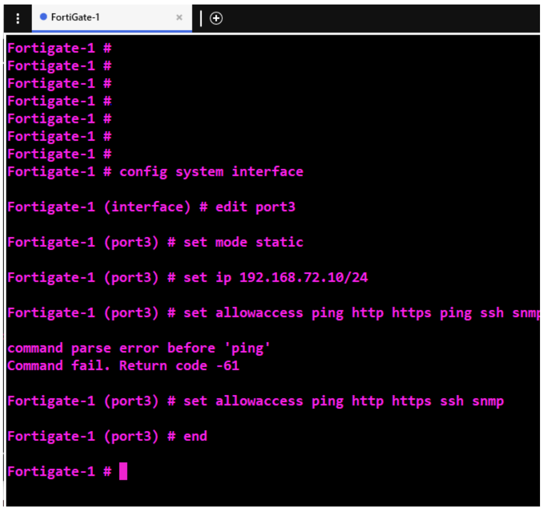
```
1005 trbrf-default                    act/unsup
SW02#conf t
Enter configuration commands, one per line.  End with CNTL
SW02(config)#interface ethernet 0/1
SW02(config-if)#switchport mode access
SW02(config-if)#switchport access vlan 151
SW02(config-if)#swicthport voice vlan 152
                   ^
% Invalid input detected at '^' marker.

SW02(config-if)#switchport voice vlan 152
SW02(config-if)#exit
SW02(config)#interface ethernet 0/2
SW02(config-if)#switchport mode access
SW02(config-if)#switchport access vlan 150
SW02(config-if)#switchport voice vlan 152
SW02(config-if)#end
SW02#show
*May 17 06:08:34.634: %SYS-5-CONFIG_I: Configured from con
sole by console
SW02#show vlan brief
```

Figure B.4: Port assignment.

B.1.4 FortiGate firewall configuration

B.1.4.1 Configuring the IP address of port 3 on the FortiGate VM

By following these steps, we will be able to restart the FortiGate VM, login to the console using the "admin" username, and configure the IP address and subnet mask for port3 as well as enable HTTP access.

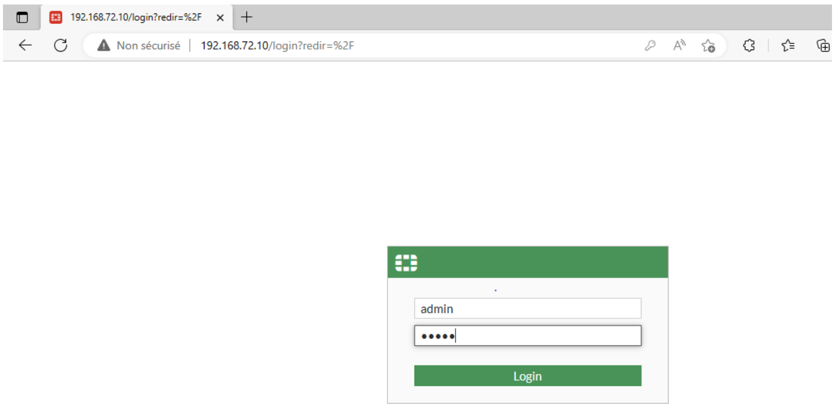


```
Fortigate-1 #
Fortigate-1 #
Fortigate-1 #
Fortigate-1 #
Fortigate-1 #
Fortigate-1 #
Fortigate-1 #
Fortigate-1 # config system interface

Fortigate-1 (interface) # edit port3

Fortigate-1 (port3) # set mode static

Fortigate-1 (port3) # set ip 192.168.72.10/24

Fortigate-1 (port3) # set allowaccess ping http https ping ssh snm

command parse error before 'ping'
Command fail. Return code -61

Fortigate-1 (port3) # set allowaccess ping http https ssh snmp

Fortigate-1 (port3) # end

Fortigate-1 #
```

Figure B.5: Fortigate firewall Configuration in CLI mode.

B.1.4.2 Log in to the FortiGate web manager

After configuring the IP address and subnet mask for port 3, we can proceed by opening a web browser and entering the configured IP address for port 3. This will direct us to the login page where we need to enter the username "admin" and the corresponding password. Finally, we click on the "Login" button to proceed.



192.168.72.10/login?redir=%2F

Non sécurisé | 192.168.72.10/login?redir=%2F

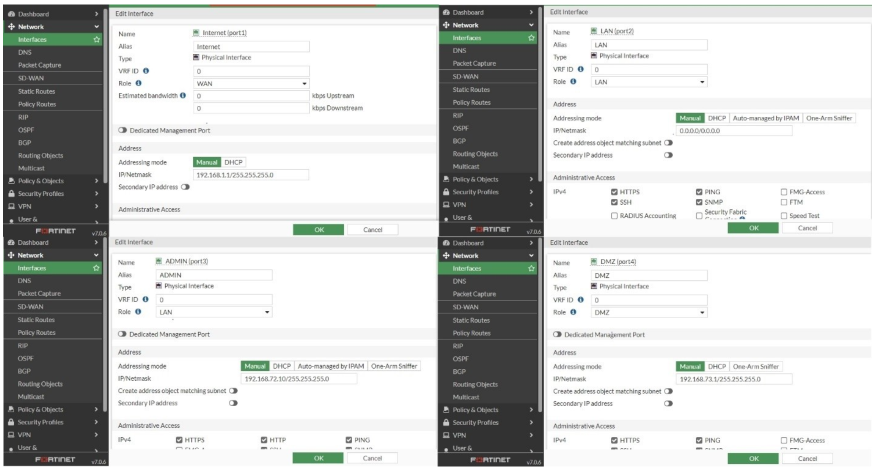
admin

•••••

Figure B.6: FortiGate web manager.

B.1.4.3 Configurations of ports

In the "System" menu, we navigate to "Network" and select "Interfaces". From there, we configure the interfaces according to our requirements. Once we have made the necessary changes, we click on the "OK" or "Apply" button to save the modifications.



Edit Interface

Name: Internet (port1)
Alias: Internet
Type: Physical Interface
VRF ID: 0
Role: WAN
Estimated bandwidth: 0 kbps Upstream, 0 kbps Downstream
○ Dedicated Management Port
Address
Addressing mode: Manual | DHCP
IP/Netmask: 192.168.1.1/255.255.255.0
Secondary IP address ○
Administrative Access

Edit Interface

Name: LAN (port2)
Alias: LAN
Type: Physical Interface
VRF ID: 0
Role: LAN
Address
Addressing mode: Manual | DHCP | Auto-managed by IPAM | One-Arm Sniffer
IP/Netmask: 0.0.0.0/0.0.0.0
Create address object matching subnet ○
Secondary IP address ○
Administrative Access
IPv4: ☑ HTTPS ☑ PING ☐ FMG-Access ☑ SSH ☑ SNMP ☐ FTM ☐ RADIUS Accounting ☐ Security Fabric ☐ Speed Test

Edit Interface

Name: ADMIN (port3)
Alias: ADMIN
Type: Physical Interface
VRF ID: 0
Role: LAN
○ Dedicated Management Port
Address
Addressing mode: Manual | DHCP | Auto-managed by IPAM | One-Arm Sniffer
IP/Netmask: 192.168.72.10/255.255.255.0
Create address object matching subnet ○
Secondary IP address ○
Administrative Access
IPv4: ☑ HTTPS ☑ HTTP ☑ PING

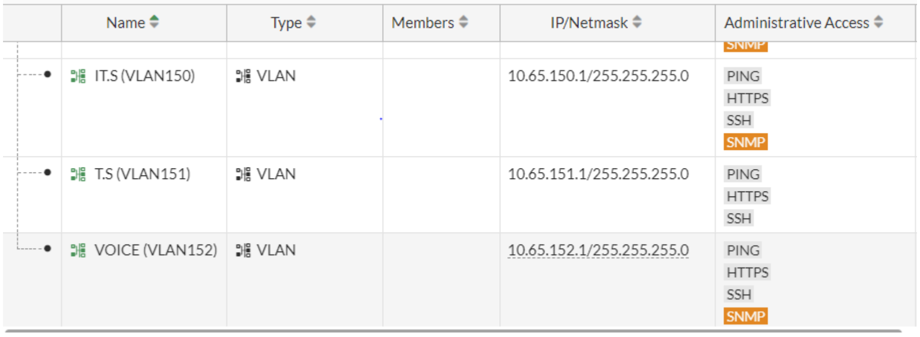
Edit Interface

Name: DMZ (port4)
Alias: DMZ
Type: Physical Interface
VRF ID: 0
Role: DMZ
○ Dedicated Management Port
Address
Addressing mode: Manual | DHCP | One-Arm Sniffer
IP/Netmask: 192.168.73.1/255.255.255.0
Create address object matching subnet ○
Secondary IP address ○
Administrative Access
IPv4: ☑ HTTPS ☑ PING ☐ FMG-Access

Figure B.7: Ports configurations.

B.1.4.4 VLAN configuration

To configure a VLAN, we first select the interface. Then, we set the mode to VLAN, specify a VLAN ID, and optionally assign an IP address and subnet mask to the VLAN interface. This configuration allows the interface to function as a virtual interface, enabling network segmentation and potential Layer 3 communication within the VLAN.

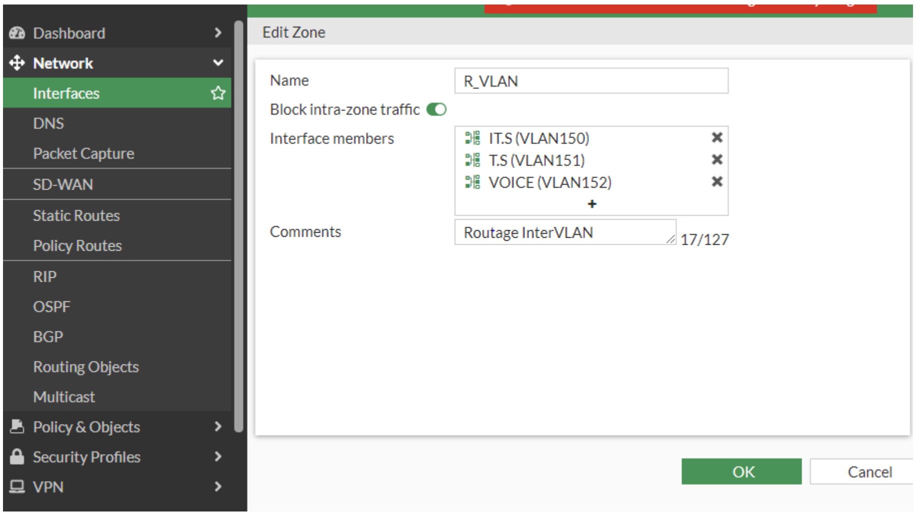


Name	Type	Members	IP/Netmask	Administrative Access
				SNMP
IT.S (VLAN150)	VLAN		10.65.150.1/255.255.255.0	PING HTTPS SSH SNMP
T.S (VLAN151)	VLAN		10.65.151.1/255.255.255.0	PING HTTPS SSH
VOICE (VLAN152)	VLAN		10.65.152.1/255.255.255.0	PING HTTPS SSH SNMP

Figure B.8: Vlan configuration.

B.1.4.5 Inter-VLAN routing

Configuring inter-VLAN routing facilitates the flow of traffic between VLANs on the FortiGate device. This enables seamless communication and connectivity among devices and networks that belong to different VLANs, all while preserving network segmentation and upholding security measures.



Edit Zone

Name: R_VLAN

Block intra-zone traffic

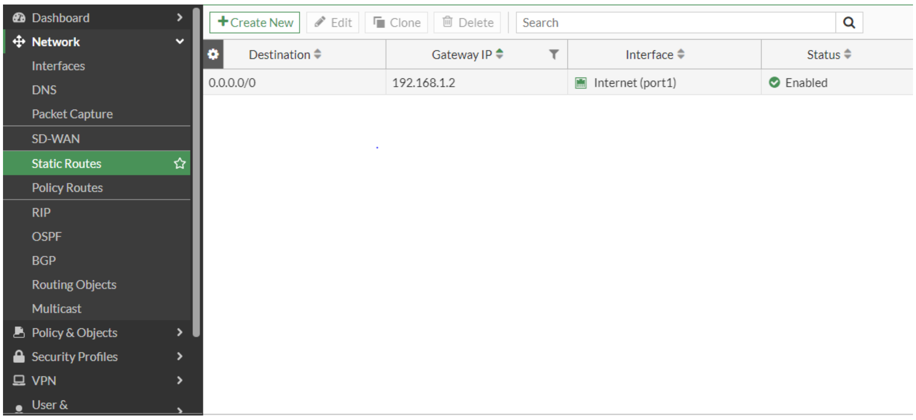
Interface members: IT.S (VLAN150), T.S (VLAN151), VOICE (VLAN152)

Comments: Routage InterVLAN 17/127

Figure B.9: Inter-VLAN.

B.1.4.6 Static route configuration

To add a default route (static route) on a FortiGate firewall, we Navigate to the "Network" menu and select "Static Routes". we Create a new static route with the destination set as "0.0.0.0/0". we choose the outgoing interface and enter the default gateway IP address provided by your ISP. Save the changes, and the default route will be added to FortiGate's routing table.

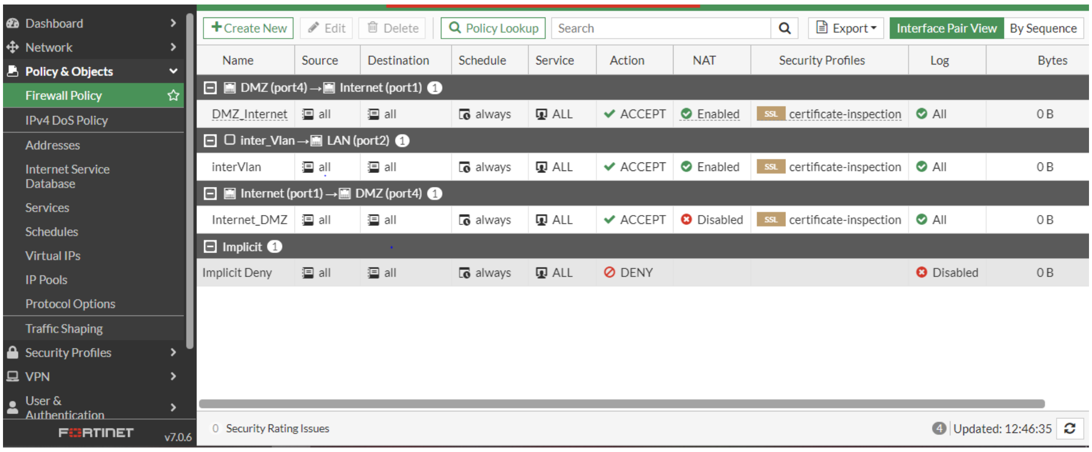


Destination	Gateway IP	Interface	Status
0.0.0.0/0	192.168.1.2	Internet (port1)	Enabled

Figure B.10: Static route.

B.1.4.7 Configuring policies in Fortigate

To create a policy in FortiGate that controls traffic flow and applies security rules, we start by accessing the FortiGate administration interface using SSH or HTTPS. Next, we navigate to the "Policy & Objects" section or the "Firewall" menu and click on "Policy & Objects" to create a new policy. Then, we click on "Create New" to begin configuring the policy. Once we have set the desired parameters, we click "Apply" to save the policy. The policy will then take effect and control traffic based on the defined rules.



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
DMZ (port4) → Internet (port1) 1									
DMZ_Internet	all	all	always	ALL	ACCEPT	Enabled	SSL certificate-inspection	All	0 B
inter_Vlan → LAN (port2) 1									
interVlan	all	all	always	ALL	ACCEPT	Enabled	SSL certificate-inspection	All	0 B
Internet (port1) → DMZ (port4) 1									
Internet_DMZ	all	all	always	ALL	ACCEPT	Disabled	SSL certificate-inspection	All	0 B
Implicit 1									
Implicit Deny	all	all	always	ALL	DENY			Disabled	0 B

0 Security Rating Issues

4 Updated: 12:46:35

Figure B.11: Firewall policies.

Appendix C

C.1 SPL Language

The Splunk Processing Language (SPL) is a language that encompasses numerous commands, functions, arguments, etc., designed to make the most of Splunk's capabilities and fully leverage the power of its indexing engine.

C.2 Components of SPL

SPL consists of the following components:

- **Search Terms:** These are the keywords or expressions you are searching for.
- **Search Terms:** These are the keywords or expressions you are searching for.
- **Commands:** The actions you want to perform on the result set, such as formatting or counting the result.
- **Clauses:** How to group or rename fields in the result set.

C.2.1 Syntax

Every SPL query begins with the source, which is the set of events being analyzed, followed by a pipe or vertical bar: `"|"`. Multiple queries can be chained together by adding a pipe at the beginning of each one.

Bibliography

[40] Atif Ahmad, Sean B Maynard, and Sangseo Park. “Information security strategies: towards an organizational multi-strategy perspective”. In: *Journal of Intelligent Manufacturing* 25 (2014), pp. 357–370.

[41] David T Bourgeois et al. “Information systems for business and beyond”. In: (2019).

[42] Axel Buecker et al. *IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager*. IBM Redbooks, 2010.

[43] W Chai. “What is the CIA triad? Definition, explanation and examples”. In: *WhatIs. com, Jan* (2021).

[44] Department of Defense. “Trusted Computer System Evaluation Criteria (TCSEC)”. In: (1985).

[45] Espace Numérique Entreprises. *Sécurité des Systèmes d’Information Guide pratique à l’usage des dirigeants*. 1st. Villa Créatis - 2, rue des Mûriers: DIRECCTE Rhône-Alpes, 2010.

[46] Commission of the European Communities. *Information Technology Security Evaluation Manual (ITSEM)*. 1st. Rue de la Loi 200, B-1049 Brussels: Telecommunications, Information Market and Exploitation of Research, 1993.

[47] Suh Charles Forbacha and Mbuya Josiah Anyam Agwu. “Design and Implementation of a Secure Virtual Private Network Over an Open Network (Internet)”. In: *American Journal of Technology* 2.1 (2023), pp. 1–36.

[48] Gustavo González-Granadillo, Susana González-Zarzosa, and Rodrigo Diaz. “Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures”. In: *Sensors* 21.14 (2021), p. 4759.

[49] Gustavo González-Granadillo, Susana González-Zarzosa, and Rodrigo Diaz. “Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures”. In: *Sensors* 21.14 (2021), p. 4759.

[51] Karen Ann Kent and Murugiah Souppaya. “Guide to Computer Security Log Management:.” In: (2006).

[52] Anjanee Kumar, Monika Chauhan, and AK Jain. “The Forensic Investigation of Cloud Computing Using Different Techniques: Challenges, Issues & Security Risks”. In: *Indian Journal of Forensic Medicine and Pathology* 14.2 (2021).

[53] B Santos Kumar et al. “Intrusion detection system-types and prevention”. In: *International Journal of Computer Science and Information Technologies* 4.1 (2013), pp. 77–82.

[54] Pengbo Nie et al. “Coverage-directed Differential Testing of X. 509 Certificate Validation in SSL/TLS Implementations”. In: *ACM Transactions on Software Engineering and Methodology* 32.1 (2023), pp. 1–32.

[55] San Joaquin Delta College Patrick McClanahan. *INFORMATION SECURITY.* LibreTexts, 5/15/2023.

[56] Kai Rannenberg. “Recent Development in Information Technology Security Evaluation-The Need for Evaluation Criteria for Multilateral Security.” In: *Security and control of information technology in society*. Citeseer. 1993, pp. 113–128.

[57] Andrew Regenscheid and Karen Scarfone. “Recommendations of the national institute of standards and technology”. In: *NIST special publication* 800 (2011), p. 155.

Webography

[1] https://eternalsunshineoftheismind.wordpress.com/2013/02/17/information-system-problems/. (accessed 26/02/2023).

[2] https://newinti.edu.my/importance-of-information-systems-for-businesses/. (accessed 26/02/2023).

[3] https://www.k2e.com/articles/align-cybersecurity-and-business-goals/. (accessed 26/02/2023).

[4] https://www.fortinet.com/resources/cyberglossary/cia-triad. (accessed 26/02/2023).

[5] https://confidentvms.com/integrity-accuracy-reliability-and-non-repudiation/. (accessed 26/02/2023).

[6] https://lucbordeleau.com/les-echelons-de-la-securite-informatique/. (accessed 26/02/2023).

[7] https://www.f5.com/labs/learning-center/threats-vulnerabilities-exploits-and-their-relationship-to-risk. (accessed 26/02/2023).

[8] https://www.baeldung.com/cs/security-interruption-interception-modification-fabrication. (accessed 02/03/2023).

[9] https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-in-2022-fbi/. (accessed 02/03/2023).

[10] https://www.techtarget.com/whatis/definition/ISO-27001. (accessed 02/03/2023).

[11] https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy. (accessed 02/03/2023).

[12] https://www.comodo.com/ids-in-security.php. (accessed 02/03/2023).

[13] https://www.exabeam.com/explainers/siem/a-siem-security-primer/. (accessed 20/03/2023).

[14] https://www.verizon.com/articles/internet-essentials/antivirus-definition/. (accessed 02/03/2023).

[15] https://forum.huawei.com/enterprise/en/the-overview-of-the-intrusion-prevention-system-ips-part-01/thread/810773-867. (accessed 02/03/2023).

[16] https://www.springboard.com/blog/cybersecurity/security-analyst-requirements-salaries/. (accessed 02/03/2023).

[17] https://www.scaler.com/topics/what-is-cryptography/. (accessed 15/03/2023).

[18] https://sematext.com/glossary/log-file/. (accessed 15/03/2023).

[19] https://www.securonix.com/what-is-siem/. (accessed 20/03/2023).

[20] https://community.microfocus.com/cyberres/b/sws-22/posts/sim-sem-and-siem-definitions-and-choosing-the-right-enterprise-solution. (accessed 20/03/2023).

[21] https://www.crowdstrike.com/cybersecurity-101/observability/log-file/. (accessed 06/04/2023).

[22] https://www.crowdstrike.com/cybersecurity-101/observability/log-file-formats/. (accessed 06/04/2023).

[23] https://community.microfocus.com/cyberres/b/sws-22/posts/sim-sem-and-siem-definitions-and-choosing-the-right-enterprise-solution. (accessed 06/04/2023).

[24] https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM. (accessed 06/04/2023).

[25] https://www.ridgewall.co.uk/news-article/what-is-a-siem-and-why-is-it-integral-to-your-security. (accessed 07/04/2023).

[26] https://laredoute.io/blog/what-is-security-information-and-event-management-siem/. (accessed 07/04/2023).

[27] https://www.techopedia.com/7/31201/security/whats-the-difference-between-sem-sim-and-siem. (accessed 07/04/2023).

[28] https://www.comparitech.com/net-admin/siem-tools/. (accessed 12/04/2023).

[29] https://www.techrepublic.com/article/siem-tools/. (accessed 12/04/2023).

[30] https://www.knowledgehut.com/blog/database/what-is-splunk. (accessed 02/05/2023).

[31] https://mindmajix.com/overview-of-splunk-architecture. (accessed 02/05/2023).

[32] https://www.socinvestigation.com/splunk-architecture-forwarder-indexer-and-search-head/. (accessed 02/05/2023).

[33] https://hkrtrainings.com/splunk-architecture. (accessed 02/05/2023).

[34] https://www.sonelgaz.dz/fr. (accessed 25/03/2023).

[35] https://www.netsolutionworks.com/datasheets/Dell_Networking_N3000_Series_SpecSheet.pdf. (accessed 25/03/2023).

[36] https://www.cisco.com/web/ANZ/cpp/refguide/hview/router/2600.html. (accessed 25/03/2023).

[37] https://www.convergedsystems.com/ip-office-500-v2.html. (accessed 25/03/2023).

[38] https://www.fortinet.com/fr/products/next-generation-firewall. (accessed 25/03/2023).

[39] https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/what-is-v45096464-d43e1648/how-symantec-endpoint-protection-technologies-prot-v97539434-d43e1669.html. (accessed 25/03/2023).

Abstract

In today's computer network environments, a significant volume of security log data is generated, posing a challenge for organizations in terms of handling and utilizing this data effectively. To address this challenge and enhance information security, centralized log management, and analysis, organizations can leverage Security Information and Event Management Systems (SIEMs). SIEMs play a crucial role in assisting organizations with compliance regulations and mitigating the risk of network intrusions by enabling comprehensive monitoring, detection, and response to security incidents. This thesis specifically focuses on implementing a SIEM solution using Splunk, a leading platform, to strengthen the security posture and enhance threat detection capabilities in the Sonelgaz organization, which can serve as a reference for other entities seeking to enhance their information security and centralized log management capabilities. The study emphasizes the benefits and challenges associated with implementing a SIEM solution, particularly utilizing Splunk, and provides recommendations for optimizing its usage to maximize threat detection and incident response capabilities.

Keywords: SIEM implementation, Splunk, centralized log management, threat detection, information security.