University of Padova

Department of Mathematics "Tullio Levi-Civita"

Master Thesis in Cybersecurity

Enhancing Network Security and Facilitating Firewall Rule management through Automated Firewall Rule management tool and integration with Discovery tools

Supervisor
Prof. Nicola Laurenti
University of Padova

Co-supervisor

Master Candidate
Muhammed Emir UYSAL

Student ID
2053407

Academic Year
2022-2023

"There is a secret bond between slowness and memory, between speed and forgetting.

A man is walking down the street. At a certain moment, he tries to recall something, but the recollection escapes him. Automatically, he slows down.

Meanwhile, a person who wants to forget a disagreeable incident he has just lived through starts unconsciously to speed up his pace, as if he were trying to distance himself from a thing still too close to him in time.

In existential mathematics that experience takes the form of two basic equations: The degree of slowness is directly proportional to the intensity of memory; the degree of speed is directly proportional to the intensity of forgetting."

— Milan Kundera

Abstract

In the ever-evolving landscape of cybersecurity, organizations face the constant challenge of fortifying their networks against an array of sophisticated threats. This master's thesis delves into the development and implementation of an innovative solution aimed at bolstering network security through Automated Firewall Rule Management (AFRM) and seamless integration with Discovery Tools.

The proposed system addresses the limitations of traditional firewall management approaches by introducing automation to the rule creation, modification, and deletion processes. Leveraging advanced algorithms, the Automated Firewall Rule Management tool optimizes rule sets, ensuring the most efficient and effective configuration to safeguard against potential vulnerabilities. This not only enhances the overall security posture but also significantly reduces the burden on network administrators, allowing them to focus on strategic security initiatives.

Moreover, the integration of the Automated Firewall Rule Management tool with Discovery Tools marks a pivotal advancement in network security. By leveraging real-time network insights provided by Discovery Tools, the system adapts dynamically to changes in the network environment. This adaptive approach ensures that firewall rules align with the organization's evolving infrastructure, minimizing the risk of misconfigurations and unauthorized access points.

The research methodology encompasses a comprehensive study of existing firewall management practices, an in-depth analysis of discovery tool capabilities, and the development of a prototype Automated Firewall Rule Management system. The evaluation phase involves rigorous testing in a simulated environment, gauging the system's effectiveness in responding to dynamic network changes and potential security threats.

The anticipated outcomes of this research include a refined understanding of the symbiotic relationship between automated firewall rule management and network discovery tools. Additionally, the developed prototype serves as a practical demonstration of the proposed solution's viability, offering a tangible contribution to the field of network security.

Ultimately, this master's thesis endeavors to empower organizations to fortify their defenses in the face of evolving cyber threats, fostering a more resilient and adaptive network security infrastructure through the integration of cutting-edge Automated Firewall Rule Management and Discovery Tool technologies.

Contents

Listing of figures

Listing of tables

Listing of acronyms

AFRM . . . . . Automated Firewall Rule Management

DMZ . . . . . Demilitarized Zone

LAN . . . . . Local Area Network

ARP . . . . . Fundamental Theorem of Calculus

ACL . . . . . Access Control List

BGP . . . . . Border Gateway Protocol

DoS . . . . . Denial of Service

APT . . . . . Advanced Persistent Threat

CIA . . . . . Confidentiality Integrity Availability

IPAM . . . . . IP Address Administration

SLA . . . . . Service Level Agreements

ITSM . . . . . IT Service Management

GUI . . . . . Graphical User Interface

TOS . . . . . Tufin Orchestration Suite

IDS . . . . . Intrusion Detection System

1 Introduction

The background and context of this research lie in the ever-evolving landscape of network security and the constant need for organizations to protect their digital assets. With the increasing sophistication of cyber threats and the growing complexity of network infrastructures, it has become crucial for businesses to adopt proactive and comprehensive security measures. The research addresses the amalgamation of two critical elements in this endeavor: ethical hacking practices and automated firewall rule management.

[?] Ethical hacking, often referred to as penetration testing, involves simulating cyberattacks to identify vulnerabilities and weaknesses in a network's defenses. These practices have become a fundamental part of enhancing security, as they uncover potential threats before malicious actors can exploit them. On the other hand, automated firewall rule management is a response to the need for efficient management of access control lists and security policies. Firewalls are essential components in network security, and managing their rules manually can be error-prone and time-consuming.

This research seeks to bring these two aspects together, leveraging the power of ethical hacking to identify weaknesses in an organization's security infrastructure and automated tools to swiftly respond to and mitigate these vulnerabilities. It also aims to provide a comprehensive solution by integrating firewall rule management with other business processes, such as Configuration Management Database (CMDB) and workflow applications. The context of this

study is a proactive and holistic approach to network security that seeks to reduce attack surfaces, enhance governance, and ensure compliance with regulatory and corporate standards.

The problem addressed by this research is the increasing threat landscape faced by organizations and the inadequacy of traditional network security measures. Manual firewall rule management, in particular, presents a significant challenge. Organizations often struggle with maintaining accurate, up-to-date rules, which can lead to vulnerabilities and non-compliance with industry regulations and corporate standards. In parallel, the dynamic nature of cyber threats requires a proactive approach to identify and rectify vulnerabilities promptly.

Ethical hacking, as a practice, is an effective means of identifying these vulnerabilities; however, its integration into existing network security governance frameworks is often lacking. The problem, therefore, is two-fold: the inefficiency of manual firewall rule management and the underutilization of ethical hacking as a proactive security measure. The research seeks to explore how the integration of these elements can address these issues and provide a more robust, dynamic, and comprehensive solution for network security.

The research outlines a set of clear and comprehensive objectives:

Evaluate Automated Firewall Rule Management: Assess the effectiveness of automated tools in managing firewall rules, with a focus on reducing attack surfaces and improving network security governance.

Propose Integration Methods: Propose methods for integrating firewall rule management with existing CMDB and workflow applications through scripting and automation.

Assess Additional Cybersecurity Tools: Investigate the impact of additional cybersecurity tools in enhancing the effectiveness of firewall rule management and ethical hacking practices.

Examine Maintenance of Certifications: Investigate the role of periodic maintenance of certifications in ensuring the ongoing compliance and effectiveness of network security measures.

The study holds significant importance in the field of network security and cybersecurity management. With the persistent threat of cyberattacks, the research addresses critical issues that organizations face in managing their security infrastructure effectively. The significance of this study can be summarized as follows:

1. Enhancing Network Security: By integrating ethical hacking practices and automated firewall rule management, the research provides a comprehensive approach to enhancing network security. This is essential in safeguarding an organization's digital assets and maintaining business continuity.

2. Mitigating Vulnerabilities: The research aims to identify and address vulnerabilities proactively, reducing the risk of data breaches and other security incidents.

3. Ensuring Compliance: The study's focus on compliance with regulatory and corporate standards is crucial, especially in industries where data privacy and security regulations are strict. Non-compliance can lead to significant legal and financial repercussions.

4. Efficiency and Productivity: By proposing methods for integrating firewall rule management with existing systems and applications, the research can improve efficiency and productivity in network security operations, reducing manual errors and response times.

Overall, the research's findings are expected to contribute valuable insights and practical solutions to the field of network security and governance, benefitting organizations and the broader cybersecurity community.

Research questions or hypotheses

The questions in mind doing this research are as follows: How do un-automated firewall systems deal with potential attacks? What does automation bring to the table in the context of firewall rule management? One could hypothesize that using a network discovery such as IPFabric and combining it with the Tufin Orchestration tool would create a solid and efficient firewall rule management environment.

A comprehensive Literature Review will be presented in Chapter 2, while the methodology used in conducting the study is explained in Chapter 3. As we step into Chapter 4, the implementation of the network environment, integration of components, and comparison of results as before and after. Chapter 5 mainly consists of discussion points after which we obtain the results and the study comes to a close, presenting a summary and the impact in the relevant field.

2

Background and Literature Review

In the realm of modern networking and cybersecurity, comprehending the fundamental elements that constitute the backbone of secure information exchange is paramount. As technology continues to evolve at an unprecedented pace, the need for a robust understanding of foundational concepts becomes increasingly vital. This master's thesis delves into the intricacies of network security, with a specific focus on firewalls, routers, automated firewall rule management systems, and network discovery tools. To establish a solid foundation for the ensuing discussions, it is imperative to embark on an exploration of these basic components. By elucidating the principles underlying these elements, we can lay the groundwork for a nuanced examination of advanced concepts and methodologies in network security, ultimately contributing to a more comprehensive understanding of the intricate landscape of contemporary information technology.[1][2]

Introduction to Firewalls in Network Security

In the rapidly evolving landscape of information technology, ensuring the security of networked systems has become a paramount concern. As organizations and individuals increasingly rely on interconnected networks for communication, data sharing, and collaborative work, the need to protect these networks from unauthorized access, data breaches, and other cyber threats has never been more critical. Among the essential components of network security, firewalls play a pivotal role in safeguarding networks from malicious activities.[3]

Definition and Purpose of Firewall

A firewall serves as a barrier between a trusted internal network and untrusted external networks, such as the internet. It is designed to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules. The primary purpose of a firewall is to establish a secure perimeter that prevents unauthorized access while allowing legitimate communication to pass through.

Functionality of Firewalls:

Firewalls operate at different layers of the OSI model, including the network layer and the application layer. Network layer firewalls, commonly referred to as packet-filtering firewalls, inspect and filter traffic based on IP addresses, port numbers, and protocols. Application layer firewalls, on the other hand, examine the content of the data packets and make decisions based on the specific applications or services generating the traffic.

Commercial Firewall Solutions:

Numerous commercial firewall solutions, both open-source and closed-source, are available in the market, catering to the diverse security needs of organizations. Open-source firewalls, such as pfSense and iptables, provide cost-effective solutions with customizable features. Closed-source firewall solutions, including Cisco's Adaptive Security Appliance (ASA) and Palo Alto Networks' next-generation firewalls, often offer advanced features, centralized management, and dedicated support.

Involvement in Small-to-Large Networks:

Firewalls are integral to the security posture of networks, irrespective of their size. In small networks, a single firewall device may suffice to protect the entire infrastructure. As networks grow in complexity and scale, the deployment of multiple firewalls, often organized into distinct security zones, becomes necessary. This segmentation enhances security by isolating sensitive data and critical systems from less secure areas.

In large enterprise networks, the concept of a perimeter firewall is complemented by internal firewalls strategically placed to regulate traffic between different segments, such as the DMZ (Demilitarized Zone) and internal LANs (Local Area Networks). Furthermore, advancements in firewall technology have led to the emergence of next-generation firewalls that integrate intrusion prevention, application awareness, and deep packet inspection to provide a more comprehensive defense against sophisticated threats.

In conclusion, firewalls represent a foundational element in the realm of network security, serving as the first line of defense against cyber threats. Their deployment, whether in small business networks or large enterprise infrastructures, is indispensable for maintaining the confidentiality, integrity, and availability of information in an interconnected world. As organizations continue to navigate the dynamic landscape of cybersecurity, understanding the intricacies of firewalls and selecting appropriate solutions will remain a critical aspect of a robust network security strategy.[4]

Role of Routers and L2/L3 Switches in a Network Environment[5]:

Routers:

Routers play a crucial role in directing traffic between different networks by making decisions based on IP addresses. They operate at the network layer (Layer 3) of the OSI model and are responsible for determining the optimal path for data packets to reach their destination. Routers maintain routing tables, which contain information about the network topology, allowing them to make intelligent forwarding decisions.

In a network environment, routers are often employed to connect different subnets or networks, facilitating intercommunication. They establish the boundaries between local area networks (LANs) and connect them to the wider network, including the internet.

L2/L3 Switches:

Layer 2 (L2) switches operate at the data link layer, primarily dealing with MAC addresses to forward frames within a local network. They are essential for creating efficient and high-speed connections within a single subnet.

Layer 3 (L3) switches combine the functionalities of routers and switches. Like routers, they can make routing decisions based on IP addresses, but they operate at higher speeds, resembling the efficiency of switches. L3 switches are often used for inter-VLAN routing, allowing communication between different virtual LANs within a network.

Relationship with Firewalls and External Networks:

Routers, L2 switches, and L3 switches work in conjunction with firewalls to ensure a secure and well-managed network environment.

1. Routers and Firewalls:

- Routers are often the point where traffic enters or exits a network. They can be configured to direct traffic through a firewall, acting as a gateway to filter and control the flow of data between the internal network and the external world, including the Internet.

2. L2/L3 Switches and Firewalls:

- L2 switches are crucial for creating efficient local connections within a subnet, while L3 switches can facilitate inter-VLAN routing. Firewalls can be strategically placed between these switches to monitor and control traffic between different network segments, ensuring that only authorized communication occurs.

Security Concerns:

1. Unauthorized Access:
- Routers, if not properly configured, may allow unauthorized access to the internal network. It is essential to implement robust access control lists (ACLs) and authentication mechanisms to mitigate this risk.

2. L2 Switch Security: - L2 switches are vulnerable to MAC address spoofing and ARP (Address Resolution Protocol) attacks. Implementing port security features and utilizing dynamic ARP inspection can enhance security at the data link layer.

3. L3 Switch and Router Security:
- L3 switches and routers are potential targets for IP spoofing and routing attacks. Employing protocols like BGP (Border Gateway Protocol) securely and implementing ingress and egress filtering can mitigate these risks.

4. Firewall Configuration:
- Misconfigurations in firewall rules may lead to either overly restrictive policies, disrupting legitimate traffic, or inadequate security, allowing unauthorized access. Regular auditing and testing of firewall configurations are crucial to maintaining a secure network perimeter.

5. Denial of Service (DoS) Attacks:
- Routers, switches, and firewalls can be targeted in DoS attacks, impacting the availability of network services. Employing mechanisms like rate limiting, traffic filtering, and intrusion prevention systems can help defend against such attacks.

In summary, routers and switches, along with firewalls, form the backbone of network infrastructure. Proper configuration, monitoring, and security measures are essential to ensure the integrity, confidentiality, and availability of network resources in the face of evolving cyber threats.

Review of Relevant literature

1. A novel approach for detecting advanced persistent threats

   Advanced persistent threat(APT) attacks are deployed by malicious parties. Most importantly, zero-day attacks exploiting unforeseen and unprecedented vulnerabilities in a network, thus can be considered the most damaging. Mitigation of attacks of this sort can be reduced via a combination of artificial intelligence and machine learning application. While artificial intelligence plays a role of creator of attacks, machine learning application gathers the information supplied by AI, to detect probable novel attacks. As for complex networks systems, hacking practices could be used both ways, in defence and in offence.
   [6]

2. Cyber Security and Ethical Hacking: The Importance of Protecting User Data

   Basic security standards are to be met by small-to-big size companies. Such standards exists both domestically and internationally namely NIST and ISO. Before any technical implementation any given company should design a network taking threats, vulnerabilities and cyber-risks in consideration. A group of practices allows organizations to stay safe such as Vulnerability assessment, security analysis, penetration test and use of ethical hacking. Fundamentals of cybersecurity are meant to be in place in order to effectively implement a management tool for various devices that could be found in a network. Hence, building a strong structure and sustain the three pillars, CIA triad, of modern security systems.
   [7]

3. A Firewall Policy Anomaly Detection Framework for Reliable Network Security

   Different types of firewalls bring different solutions and vulnerabilities in terms of either cost or performance. Talking about packet-filtering firewalls, although being relatively economic, they sometimes can be misled by various malicious activities, most commonly IP-spoofing attacks. Since the rules are set by IP addresses and ports, they trust known servers. The anomalies should be detected by a IPS/IDS or an anomaly-based detection framework, ensuring that firewalls perform better in recognising incoming potential threats. Similarly to Tufin's Designer mechanism, a such framework would then recommend configurations for firewalls in-place.
   [8]

4. Automated Firewall Configuration in Virtual Networks

   Configuration of, in particular, packet filter firewalls have been a subject of debate in network security. It is deemed to be crucial optimising the topology and reduce the amount of connections, rules and firewalls altogether. Different methodologies have been suggested as to how to avoid long re-configuration process and likely security breaches afterward. Hence why it is imperative to keep an up-to-date network topology.
   [9]

5. Automatic management of network security policy

   The automatization of network-wide self-configuration is one of the main themes in security. Merging two subnets without having a collusion and shadowing of rules is highly sought after. Due to numerous vendor and models of network devices, it becomes difficult to maange all at the same time. This brings out the need for a centralized man-

agement tool. To keep track of the policies in-place and detect inconsistencies across networks, some goals of such structures are as follows: [10]

(a) Concise and easy on the eye management dashboard,

(b) Composability of devices

(c) Includes different vendors

(d) Readability

(e) Scalability

Automatic detection of firewall misconfigurations using firewall and network routing policies

With a big growth of network size, it becomes difficult to keep track of all the connections and policy configurations. Changes in policies could affect the whole network in terms of routing, which is often the ignored component in a network. To comply with regulations and to prevent security breaches, organizations should figure out inconsistencies, alteration of rules and their lack of. R. Oliviera et al. propose a monitoring and alerting tool Prometheus in order to follow and observe and then address the issues rapidly. These configuration errors could be classified in 4 parts:

(a) Intra-firewall inconsistencies When inconsistencies occur within a sole firewall, it means that certain rules are fully or partially mask, therefore rendering useless other rules. Shadowing, generalization, and correlation are three types of this issue.

(b) Inter Firewall inconsistencies

When rule shadowing happens between firewalls.

(c) Cross path inconsistencies

Crosspath inconsistencies refer to the diversion of packet traveling routes which brings a different set of firewall rules into play and cannot promise a packet to go through to the target destination as intended.

(d) Intra firewall inefficiencies

Inefficiencies show up in two forms: redundancies and verbosities. While neither can be deemed as error, they create a mess of rules, considering a network has numerous rules in place. Verbosities could be more detailed and explicitly explain the rules, whereas redundancies may be put in for future use. However, they both affect the overall readability and manageability of firewall rule management systems.

The article goes on to explain how such a system identifies and then suggests corrections to misconfigurations. A certain algorithm decides how to redress the misconfigurations, and such corrections are also verified afterward.[11]

Detailed explanations of Tufin and IPFabric, their features, and how they address cybersecurity challenges

Comparison of Tufin and IPFabric with other similar tools.[12][13]

Tufin competitors: Tufin is one of the best security platform for medium to large-sized businesses. It is powerful enough to tackle the security requirements of complex working environments.
The top Tufin Competitors include AlgoSec, FireMon, Skybox, RedSeal, Check Point, Lacework, Google Cloud Platform, CyberArk, Cisco Secure Workload, and Illumio.
Tufin is a reliable, popular, highly trusted, and recommended platform for zero-trust security. It has more than 2,900 customers from all around the world, including BlueCross BlueShield, BNP Paribas, Deutsche Bank, IBM, and more. Being a unified security platform, Tufin reduces the time and costs of managing enterprise security. It can handle the complex security needs of large enterprises very well.

Tufin Orchestration Suite offers 3 IT solutions as a bundle: SecureTrack, SecureChange and SecureApp(Enterprise).

All three of them provide work as a team. While Securetrack is a dashboard full of devices, events and status of rules, SecureChange control we requested firewall rules and policy changes. The inclusion of workflows ensures that every process of insertion, deletion, or alteration, goes swimmingly. Lastly, SecureApp covers the application rule setting in such an easy way, up until providing drag-and-drop. It helps users to manage their application on a clear, spacious user interface as well as providing APIs since it has been a feature for all TOS solutions.

1. SecureTrack+

   In the realm of network security, the need for centralized policy management, risk mitigation, and compliance monitoring has become paramount. This subsection explores

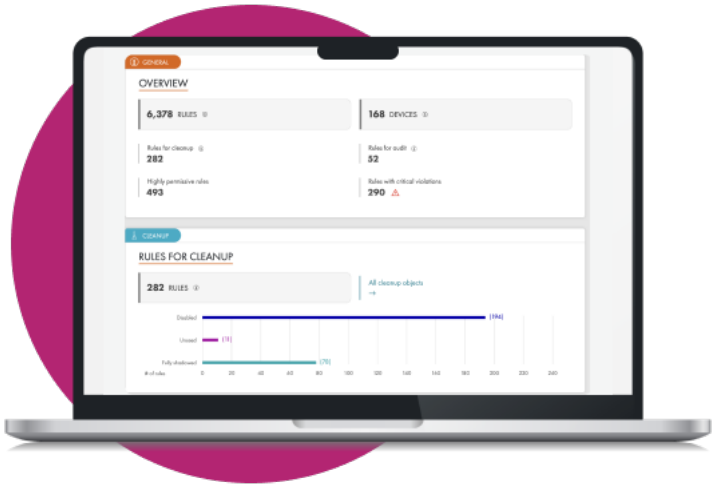

Figure 2.1: SecureTrack GUI

the application of SecureTrack and its features, aligning with industry practices in centralized network security policy management. We delve into how diverse technologies converge within one application.

(a) Centralized Network Security Policy Management

Businesses, regardless of size, must adhere to security standards like NIST and ISO. The foundation lies in building a network with cybersecurity in mind, considering threats, vulnerabilities, and cyber-risks. Security is maintained through procedures like penetration testing, security analysis, vulnerability assessment, and ethical hacking. Implementing a management tool for network devices necessitates a cybersecurity foundation, ensuring a robust framework and upholding the CIA trinity – the three pillars of modern security systems.

(b) Network Segmentation and Visibility

Efficient network segmentation is crucial for security. SecureTrack+ aids organizations in setting and maintaining baseline traffic rules between security zones, enhancing real-time monitoring of policy violations. This results in more effective implementation and management of consistent network segmentation.

(c) Security Policy Management Tools

Tools such as IP Address Administration (IPAM) Integration and Security Policy Builder enhance security policy administration. Real-time monitoring of network traffic logs bridges the gap between intended and actual network segmentation states, offering guidance on necessary policy modifications. IPAM integration streamlines subnet changes, improving risk assessments and violation notifications.

(d) Automated Firewall Rule and Object Management

Automating network object and firewall rule management, as facilitated by SecureTrack+, proves to be financially sensible. It significantly reduces the time required for rule cleanup by identifying and removing unnecessary or redundant rules. Moreover, inactive network objects are identified and decommissioned, enhancing resource efficiency and security.

(e) Firewall Rule Optimization

Automated and consolidated firewall rule optimization, exemplified by tools like Tufin, simplifies rule and object management across multi-vendor systems. Sophisticated search and filtering features minimize the effort needed for maintaining firewall rules, while the Automated Policy Generator optimizes rule bases according to current traffic, adhering to the least privilege principle.

(f) Compliance Monitoring and Risk Awareness

Effective compliance monitoring is essential for network security. SecureTrack+ provides real-time alerts on risky access and policy violations, interfacing with vulnerability management programs. This enables enterprises to order patching based on vulnerability scans and network intelligence.

(g) Cloud Security Policy Orchestration

The orchestration of security policies for cloud environments is gaining popularity. Tufin's agentless, multi-cloud policy management ensures control and segmentation across on-premises and cloud infrastructures. By integrating security controls into the Continuous Integration/Continuous Deployment (CI/CD) pro-

cess, security is facilitated without disrupting DevOps teams' operations.

(h) Data Center Migration and Audit Preparation

Security policy cloning workflows automate the cloning of security policies for new network objects, expediting hardware expansion and data center migration. Automated audit report generation and real-time compliance monitoring accelerate audit preparation by up to 90 percent, adhering to multiple regulatory standards.

In summary, the integration of automation, centralization, and real-time awareness is crucial for enhancing network security in today's dynamic digital environment.

2. SecureChange+

This chapter delves into network change automation and rule lifecycle management, focusing on SecureChange+. This cybersecurity solution aims to achieve continuous compliance and reduce network change Service Level Agreements (SLAs) by up to 90 percent. Explore the literature and industry practices surrounding SecureChange+, revealing its innovative features and implications.

(a) Achieving Continuous Compliance

Continuous compliance is central to network security, and SecureChange+ significantly reduces network change SLAs while ensuring compliance with industry regulations and internal policies. Testimonials emphasize productivity gains, error reduction, and streamlined coordination among teams as key benefits.

(b) Elimination of Backlogs and Workflow Automation

SecureChange+ eliminates network change and rule review backlogs through flexible workflows and automation capabilities. This enhances operational efficiency, reduces risks through auditable processes, and integrates with IT Service Management (ITSM) solutions for seamless workflows triggered by ITSM tickets.

(c) Automation of Rule Lifecycle Management

Automation extends to rule lifecycle management, with SecureChange+ orchestrating rule review processes, identifying expiring rules, and automating recertification. Customization options allow organizations to tailor the rule review process to their specific needs.

(d) Network Topology Intelligence and Dynamic Mapping

SecureChange+ leverages network topology intelligence and dynamic mapping, supporting over 200 million routes for accurate target selection and change design visualization. Path analysis aids troubleshooting, especially in multi-cloud environments, enhancing its functionality.

(e) Proactive Risk Assessment

Proactive risk assessment is pivotal, and SecureChange+ customizes change designs by cross-referencing intelligence from third-party solutions, ensuring continuous compliance with security and industry policies.

(f) Cloud Security Policy Orchestration and CI/CD Integration

SecureChange+ extends to the cloud, providing agentless, multi-cloud policy management. Integrating security guardrails into the CI/CD process streamlines DevOps practices without disrupting workflows.

(g) Vulnerability Awareness and Advanced Audit Readiness

Vulnerability-Based Change Automation injects awareness into the change design process, checking for vulnerabilities during change design. SecureChange+ contributes to advanced audit readiness with real-time compliance monitoring and customizable audit reports.

In conclusion, SecureChange+ signifies a significant advancement in network change automation, showcasing its effectiveness in achieving continuous compliance, eliminating backlogs, and streamlining rule management.

3. SecureApp+

This chapter explores application-based security policy automation, focusing on SecureApp+. Designed for zero-touch change automation, unifying network and cloud security processes, and centralizing policy management, SecureApp+ is examined in the context of existing literature and industry practices.

(a) Achieving Zero-Touch Automation

SecureApp+ aims for zero-touch automation, streamlining change management processes, and minimizing manual tasks. Notably, Tufin-recommended changes receiving administrator approval were automatically implemented, showcasing a cutting-edge approach to security automation.

(b) Central Control Plane and Integration Ecosystem

The adoption of a central control plane is crucial, and SecureApp+ consolidates a heterogeneous environment under a single control plane. Its broad integration ecosystem simplifies achieving network security maturity, supporting leading solutions and enhancing integration with code-free, GUI-based options.

(c) Connectivity Management for Application Deployment

Efficient application deployment is a priority, and SecureApp+ breaks down silos between teams. Offering a central console for managing network-related application changes, it ensures the network aligns with dynamic application requirements. Graphical diagnostic tools aid in troubleshooting and automatic resolution of connectivity issues.

(d) Scalability and Broad Adoption

Scalability is critical, and SecureApp+ supports massive enterprise networks. Trusted by over 2,900 organizations, including Fortune 50 companies, its comprehensive network topology mapping, support for extensive route configurations, distributed architecture, and high availability contribute to its broad adoption.

In summary, SecureApp+ represents a significant stride in application-based security policy automation, focusing on achieving zero-touch automation, a central control plane,

efficient connectivity management, and broad scalability.

In conclusion, SecureApp+ represents a significant leap in the realm of application-based security policy automation. Its capacity to achieve zero-touch automation, unified network and cloud security processes, and centralized policy management is pivotal in addressing the evolving needs of modern cybersecurity.[14]

IPFabric

IP Fabric is a Network Assurance Platform that eliminates 90 percent of the manual labor required to even initiate an automation project by automating discovery and documentation. This is a quick win. IP Fabric then keeps checking to see if your automated processes are in line with your intentions.

IPFabric is a network assurance platform that helps make sure your network is working well. It does this by looking at your network and figuring out what's there, finding any problems, and giving suggestions on how to fix them. The platform uses smart math to draw pictures of your network and show how everything is connected.

One big thing IPFabric is good for is fixing problems and making your network work better. It watches your network all the time, finds any issues, and tells you what might be causing them. This is important because it helps your network stay working well and not have any downtime. IPFabric can also check if your network follows the rules and standards that it's supposed to, which is important for security and following the law.

IPFabric can work with other computer programs too. It has a way for other programs to talk to it, so you can use it with different tools and systems. This makes it easy to add IPFabric to your existing computer setup and use it together with other programs.

When we look at other programs like NetBrain, Forward Networks, Gluware, Itential, Juniper, SolarWinds, and ZPE Systems, we see that each one is good at different things. For example, NetBrain is good at making your network do things automatically, while Forward Networks is good at checking if your network is set up correctly. Gluware and Itential are good for making your network work automatically, Juniper has many different networking tools, SolarWinds is known for watching your network, and ZPE Systems is good at managing

networks.

What makes IPFabric special is that it looks at your whole network and tries to make sure everything is okay all the time. While other programs might be really good at one thing, IPFabric tries to do a little bit of everything to keep your network running well. Also, IPFabric can easily work with other programs, making it a good choice if you want a tool that fits into your existing computer setup.[15]
[15]
IP Fabric Competitors[16] : NetBrain Forward Networks Gluware Itential Juniper SolarWinds ZPE Systems

Combining Tufin OS and IPFabric creates a powerful tool to manage networks with high efficiency and great capability to observe and control.

IT cybersecurity concepts and best practices

Cybersecurity concepts are indispensable in Information Technology (IT) due to their critical roles in protecting sensitive data, maintaining business continuity, ensuring regulatory compliance, mitigating financial losses, defending against evolving cyber threats, safeguarding privacy, preserving intellectual property, upholding reputation, maintaining data integrity, fulfilling ethical and legal obligations, supporting national security, and gaining a competitive edge. In an increasingly digital world, these concepts are essential for organizational sustainability, security, and the protection of individuals' data and privacy. An extended list of best concepts and practices:[17][18][19][20]

1. Risk Assessment: To effectively secure your organization's digital assets, it's crucial to begin with a thorough risk assessment. This process helps you identify vulnerabilities and potential threats specific to your environment.
2. Access Control: Implement stringent access control measures. Ensure that only authorized individuals have access to sensitive information and systems. This involves user authentication, strong password policies, and role-based access.
3. Data Encryption: Protect your data with encryption, both at rest and in transit. This security measure ensures that even if physical storage or network communication is compromised, sensitive information remains safe from unauthorized access.

4. Patch Management: Stay proactive by keeping your software, operating systems, and applications up to date with the latest security patches. Many security breaches occur due to known vulnerabilities that haven't been patched.

5. Firewalls and Intrusion Detection Systems (IDS): Safeguard your network with firewalls that monitor and control incoming and outgoing traffic. Implement intrusion detection systems to identify and respond to suspicious activities promptly.

6. Anti-Malware Solutions: Install antivirus and anti-malware software to detect and remove malicious software that could compromise your systems.

7. Security Awareness Training: Regularly educate your employees and users on security best practices. Human error is a significant source of security breaches, so awareness is key.

8. Incident Response Plan: Develop a comprehensive incident response plan that outlines steps to take in the event of a security breach. Ensure that your employees are familiar with this plan and know how to report security incidents.

9. Network Segmentation: Divide your network into segments to limit the potential impact of a breach. This practice isolates critical systems from less secure ones, enhancing overall security.

10. Regular Backups: Back up critical data and systems regularly, and ensure that these backups are encrypted and stored in an offsite location. This provides a safety net in case of data loss or ransomware attacks.

11. Physical Security: Don't overlook physical security. Protect against unauthorized physical access to servers and networking equipment, as this can lead to data breaches.

12. Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA): Enhance authentication by requiring multiple forms of verification for accessing sensitive systems. This can include something you know (e.g., a password) and something you have (e.g., a smartphone token).

13. Vendor and Supply Chain Security: Ensure that your vendors and suppliers adhere to robust security practices, as they can introduce vulnerabilities to your ecosystem.

14. Logging and Monitoring: Keep detailed logs of system and network activities and regularly review them for signs of suspicious or unauthorized activity.

15. Security Policies and Procedures: Develop and document clear security policies and procedures that are followed throughout your organization to ensure consistency in security practices.

16. Regular Security Audits and Penetration Testing: Conduct routine security audits and penetration tests to identify weaknesses and vulnerabilities in your systems, enabling you to address them promptly.

17. Compliance: Ensure that your security practices align with industry-specific regulations and standards, such as GDPR or ISO 27001, depending on your business and its requirements.

18. Zero Trust Security Model: Embrace a zero-trust security model, which assumes that threats can originate both from within and outside your network. Verify and authenticate every user and device attempting to connect to your network.

19. Continual Learning and Adaptation: Cybersecurity is an ever-evolving field. Stay informed about the latest threats and best practices and adapt your security measures accordingly to stay ahead of evolving threats and challenges.

Given those practices and concepts, it shouldn't be forgotten that IT security is an ongoing event and most companies adopt the Security-by-Design policy. Therefore, while embracing the fundamentals of security, seeking for constant cybersecurity consultation and further expansion in services is the best policy of all.[21]

3
Methodology

Detailed presentation of the real-world IT environment

SecureTrack is a comprehensive solution designed for monitoring and modifying rules on connected devices. In a laboratory setting, various virtualized devices, such as those emulating Amazon Web Services (AWS), Checkpoint, Cisco, f5, Fortinet, Forcepoint, Juniper Networks, Azure, Netfilter, Openstack, Palo Alto, and Zscaler, can be added and tracked. It's important to note that these devices are simulated for lab purposes and do not represent actual physical entities. Despite their virtual nature, they are equipped with purposeful rules categorized into groups like clean up, audit, highly permissive, and critical violation rules. The user interface of SecureTrack offers graphical representations to facilitate observation, inference, and necessary modifications in compliance with specific requirements.[14]

In contrast, IPFabric operates as a physical device within a real-world environment, featuring firewalls, routers, and a network. Its primary function is to automatically detect changes, such as additions or removals, in a monitored network concerning rules and devices. Unlike SecureTrack's virtual lab environment, IPFabric operates in a tangible, physical setting with genuine networking components..

The objective is to implement IPFabric in different network environments and gather modification information periodically and automatically which is then to be used by Tufin. In this

way, firewall rule modifications are handled at speed without interaction. In the case of device implementation or removal, depending on the device type the procedure changes. Some devices can be entertained either hands-on or automatically from the script.[15]

The research methodology employed in this study involves a hands-on approach gained through a year-long internship, focusing on Automated Firewall Rule Management (AFRM) and Integration with Discovery Tools for Enhanced Network Security. The methodology integrates practical experiences with Tufin, an automated firewall rule management tool, and IPFabric, a network discovery tool. The primary activities undertaken during the internship include the integration of these tools, the implementation of a workflow in Tufin Securechange, and the development of scripts for specific automation tasks.

The integration of Tufin and IPFabric was a key aspect of this research. This process involved the seamless interaction between the automated firewall rule management capabilities of Tufin and the network discovery functionalities of IPFabric. Specifically, the integration focused on the editing, adding, and removing of devices within the network based on insights derived from IPFabric. The details of this integration, including the workflow and specific functionalities enabled through the integration, will be elaborated upon in this chapter.

The case study was conducted partly within the real-world IT environment and the LAB environment of Kirey Group. This environment served as the testing ground for the integration of Tufin and IPFabric, providing a dynamic and authentic setting to evaluate the effectiveness of the automated processes. The IT environment comprises a webserver to access Tufin, Tufin Server, and IPFabric server device, offering a practical context for assessing the impact of automated firewall rule management and network discovery integration.

Data collection for this research involved a combination of practical implementation and code development. The key tools used for data collection included Tufin, IPFabric, and Securechange. The data collection process encompassed the creation and execution of scripts within the Tufin Securechange workflow.

Given the sensitivity of the activities conducted within the internship at Kirey Group, ethical considerations and data privacy concerns are paramount. The presentation of findings and code snippets is limited to complying with the company's ownership and confidential-

ity requirements. This section will delve into the ethical considerations, emphasizing the importance of protecting proprietary information and respecting data privacy throughout the research process.

4

Case Study

Detailed presentation of the real-world IT environment

To start with, SecureTrack is the solution where devices are connected, monitored and their rules modified. In the Lab part that I have been working on, there are 67 different devices with brands such as the following(Figure x): Amazon Web Services(AWS), checkpoint, Cisco,f5, Fortinet, Forcepoint, Juniper networks, Azure, Netfilter, Openstack, Palo Alto, and Zscaler. All devices that are being monitored on Tufin are created for Lab purposes and are not real concrete devices.

However, they are stacked with purposeful rules, which then be separated by groups as rules for clean up, rules for audit, rules highly permissive and rules with critical violations.

To meet compliance needs, the user interface provides various graphs to observe, infer, and make modifications where they are necessary.

On the other hand, IPFabric is a device located in a physical environment decorated by real-life firewalls, routers, and a network. Its purpose is to auto-discover the changes(removal or addition) in an observed network in terms of rules, and devices altogether.

Currently, the network environment related to IPfabric consists of 21 devices.

The objective is to implement IPFabric in different network environments and gather modification information periodically and automatically which is then to be used by Tufin. In this way, firewall rule modifications are handled at speed without interaction. In the case of device implementation or removal, depending on the device type the procedure changes. Some devices can be entertained either hands-on or automatically from the script.

Implementation of the integration

The implementation requires a couple of scripts and configuration files to correctly function. Aforementioned scripts are about exporting data out of IPFabric and then importing the changes onto Tufin.

It is better to work separately between two platforms for a couple of reasons. They can be adjusted for another integration with ease, and the cleanliness of the code is one of the fundamentals in programming.

Firstly, I constructed a script so as to constantly detect device changes between two chosen snapshots which are the ultimate and the penultimate snapshots. While also the ability to observe the configuration changes at disposal, It is not necessary and out-of-scope for this study.

Moreover, IPFabric gives out basically all the information related to any machine that has been discovered, such as timestamps, last update, power status, etc. Avoiding the verbosity via filtering capabilities is a great move at this stage.

At the end of the first phase, the output is created in 'CSV' format which is very easy to handle and work on using Python.

On the other hand, the second part involves more intricacies compared to the first part. Tufin SecureTrack offers integration capabilities via API for only selected from chosen devices among all supported vendors. As seen in (Figure 1) the structure of supported devices is like this.

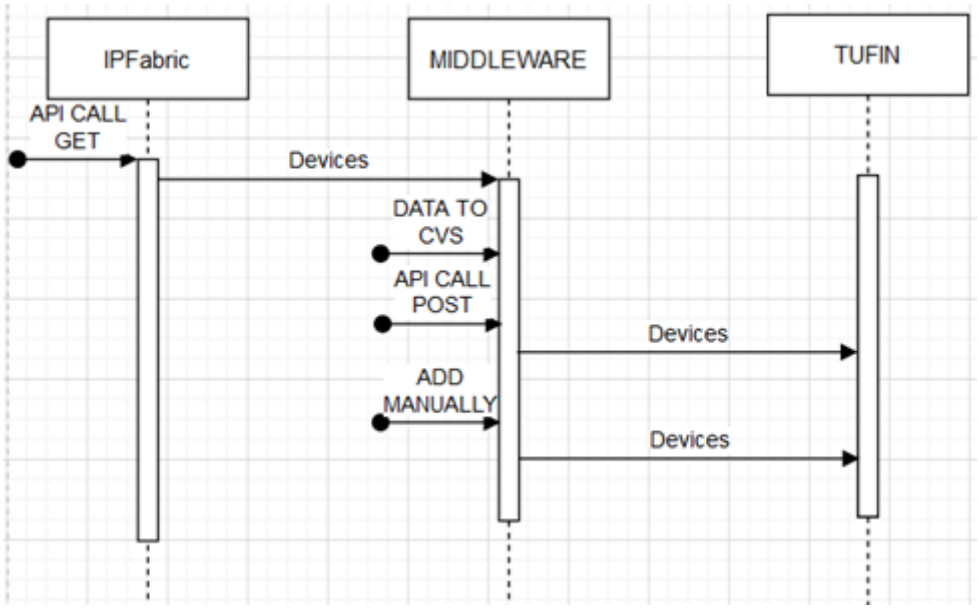

Figure 4.1: Workflow

Therefore, the importation task bifurcates into two paths, which is followed by another division between supported devices.

For devices that are supported by API calls and no authorization required: Straightforward import of devices solely based on name, IP address, and indicated domain of which they are supposed to be part. For devices that are supported by API calls and authorization required: Devices are manually added using the graphical user interface(GUI) or by a script that accepts authorization information as input For devices that are not supported by API calls: Devices are manually added using the GUI.[14]

Data collection process

Snapshots play a crucial role in facilitating change management within the IP Fabric framework. To ensure the system stays updated and reflective of the evolving network landscape, it is imperative to regularly initiate IP Fabric discovery. This process can be conveniently scheduled by navigating to the designated section at Settings → Advanced → Snapshots → Timed Snapshots.

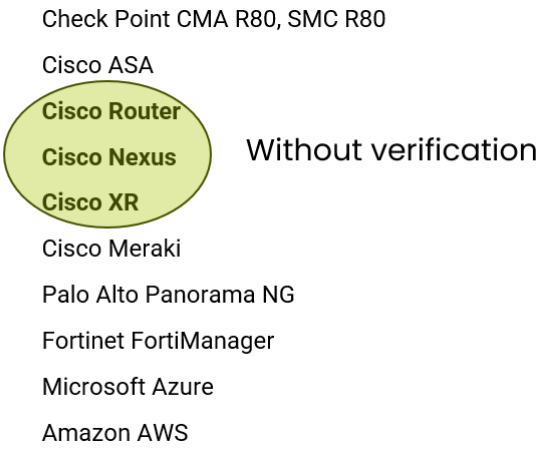

Figure 4.2: Supported Devices

For instance, a practical implementation involves automating a discovery run every 10 minutes past the hour, creating a recurring schedule (e.g., 0:10, 1:10, 2:10, 3:10, and so forth) to ensure frequent and timely updates.

The concept of Timed Snapshots within IP Fabric involves a thoughtful scheduling mechanism. In a hypothetical scenario where a snapshot is set to occur every hour, and each snapshot takes approximately 4 hours and 20 minutes to be fully created, the subsequent snapshot will be automatically scheduled once the previous one concludes. This ensures a seamless and continuous process, with the scheduled time aligning with the next available period as determined by the configured cron setup.

The IP Fabric platform operates by systematically gathering data from the network at regular intervals, facilitating the generation of comprehensive analytics that offer profound insights into the network's infrastructure. The culmination of this data collection process results in the creation of a digital snapshot that encapsulates the entirety of the network's configuration and status at the specific moment of discovery.

It is crucial to note that IP Fabric does not engage in real-time monitoring of the network. Instead, its approach revolves around periodic data collection, allowing users to benefit from a historical perspective and a detailed overview of the network's characteristics. This deliberate strategy empowers network administrators with the ability to analyze trends, identify patterns, and make informed decisions based on a comprehensive understanding of the network's state

at different points in time.[15]

Data collection is primarily connected with the implementation itself. As far as this study is concerned, the data is received from a company network in which an IPFabric product is already integrated.

During the initial phase of network discovery, the deployment of IP Fabric necessitates the utilization of the OVA image, which is made available upon request. The platform's successful initialization is contingent upon the provision of accurate credentials, ensuring seamless access to active network devices through SSH/Telnet protocols. Essential to this process is the configuration of the security perimeter to facilitate effective communication from the IP Fabric platform to the network devices, specifically accommodating the mentioned Command Line Interface (CLI) protocols.

Moreover, for enhanced customization and efficiency, administrators have the option to specify a singular IP address as the starting point for the discovery process. This provides a targeted approach to the initial data collection, allowing for a more focused exploration of the network infrastructure. By following these meticulous steps during the inaugural setup, IP Fabric establishes a robust foundation for subsequent network analytics and insights, delivering a comprehensive understanding of the network's topology and configuration.

This particular network environment includes a variety of IP-based active network devices, such as switches, routers, firewalls, load-balancers, WAN concentrators, wireless controllers, and wireless access points.

Test scenarios involve mainly a series of comparisons of 'Snapshots' taken from the network. Since the objective of this implementation is transferring the changes without any personnel communication to our automation tool on the other side, changes of rules and changes in devices are extracted via API calls and basic scripting.

Results before and after integration

One of the standout improvements is the enhanced understanding of network topology, which has empowered security teams with a more profound insight into the intricate relationships among devices and configurations. This newfound clarity serves as the cornerstone for

more informed rule management decisions. With a comprehensive view of the network infrastructure provided by IPFabric, security professionals can now make strategic choices when creating, modifying, or deleting firewall rules. This heightened awareness ensures that rules align seamlessly with the dynamic network environment, reducing the risk of misconfigurations and vulnerabilities.

Automation emerges as a key driver in the success of this integration. The automated rule optimization processes implemented through Tufin ensure continuous alignment with network changes. This automation not only expedites the rule management workflow but also contributes to the overall efficiency of security operations. Redundant or conflicting firewall rules are efficiently identified and resolved, leading to a more streamlined and optimized rule set. The impact is tangible – a security infrastructure that is both responsive and efficient in adapting to the evolving threat landscape.

Perhaps most crucially, the integration has resulted in a significant improvement in the identification and resolution of potential vulnerabilities. Security teams now benefit from real-time insights provided by IPFabric, allowing for proactive measures to be taken. The minimized window of exposure to potential risks is a testament to the effectiveness of the integrated solution. Faster response times to security events and network changes are a direct result of this proactivity, ensuring that security professionals can swiftly address emerging threats, ultimately fortifying the organization's cyber defenses.

The integration's impact extends beyond technical enhancements to the operational realm. Streamlined workflows have substantially reduced the manual efforts required for routine rule management tasks. Security teams can now redirect their focus from repetitive, time-consuming processes to more strategic initiatives. This shift in focus allows organizations to allocate resources more effectively, fostering an environment where security professionals can proactively address emerging threats and contribute to the overarching cybersecurity strategy.

In conclusion, the successful integration of IPFabric and Tufin reveals a paradigm shift in network security management. The improved understanding of network topology, automation of rule optimization processes, efficient vulnerability resolution, faster response times, streamlined workflows, and enhanced operational efficiency collectively contribute to a more resilient and adaptive cybersecurity infrastructure. This integration not only addresses current

challenges but positions the organization to navigate the evolving threat landscape with confidence and agility.

5
Discussion

The study serves mainly to demonstrate the adaptability and integrability of herein two tools, Tufin and IPFabric. Integration of the two tools(Tufin and IPFabric) decreases the considerable amount of time to update the topology consistently.

The integration of a network discovery tool, such as IPFabric, and an automated firewall rule management tool, like Tufin, offers a comprehensive set of advantages for optimizing network security and management. IPFabric, functioning as an analytical tool, plays a pivotal role in providing a detailed and up-to-date understanding of the network infrastructure. Through its network discovery capabilities, IPFabric maps out the entire network, identifies devices, and captures their configurations, contributing to enhanced visibility.

This clear visibility extends to accurate device information, ensuring that the automated firewall rule management tool can make well-informed decisions when creating, modifying, or deleting rules. The dynamic adaptation to network changes becomes a noteworthy advantage as IPFabric continuously monitors the network for real-time insights into modifications in device configurations and network topology. The integration allows the automated tool to adapt dynamically to these changes, ensuring that firewall rules remain aligned with the evolving network environment.

Moreover, the analytical capabilities of IPFabric include the identification of redundant or

conflicting configurations within the network. When integrated with an automated firewall rule management tool, this information facilitates efficient rule optimization. Redundant rules can be identified and removed, resulting in a streamlined and effective set of firewall rules.

IPFabric's proactive identification of potential security vulnerabilities and risks further enhances the security posture. Integrating these insights into the automated firewall rule management process enables the tool to proactively address vulnerabilities, contributing to a more resilient security infrastructure by reducing the exposure window to potential threats.

The streamlined workflows and reduced administrative burden are additional benefits of this integration. IPFabric's role in streamlining network discovery processes provides a foundation for automation, allowing the integrated solution to automate tasks related to rule creation, modification, and deletion. This, in turn, reduces the administrative burden on network security teams, enabling them to focus on strategic initiatives rather than manual rule management tasks.

In essence, the combined strengths of IPFabric and an automated firewall rule management tool create a holistic and adaptive approach to network security. This integration enhances visibility, accuracy, and efficiency in managing firewall rules, contributing to a resilient and responsive network security infrastructure.

The integration of a network discovery tool like IPFabric with an automated firewall rule management tool such as Tufin has significant practical implications, leading to notable improvements in both network security and operational efficiency. This integration facilitates a more accurate and real-time understanding of the network infrastructure, thereby enhancing overall security awareness. To capitalize on this, it is recommended to regularly leverage insights from IPFabric for proactive optimization of firewall rules and conduct periodic security audits to promptly identify and address potential vulnerabilities.

Furthermore, the dynamic adaptation to network changes is a key benefit of this integration, allowing for real-time adjustments to firewall rules based on insights provided by IPFabric. To fully capitalize on this capability, organizations should establish automated processes that respond promptly to network changes, ensuring that firewall rules remain aligned with the evolv-

ing network topology. Regular reviews and updates of firewall rules are also recommended to maintain a responsive security posture.

The streamlined workflows resulting from the integration, coupled with the reduction in the administrative burden on network security teams, highlight the importance of investing in training to ensure that teams are proficient in utilizing the integrated tools. Continuous refinement of automated workflows is advised to further streamline operational processes and maximize efficiency.

Proactively identifying and mitigating potential security vulnerabilities based on IPFabric's analytical capabilities is another practical implication of this integration. To fully leverage this capability, organizations should establish automated workflows that respond to vulnerabilities identified by IPFabric and implement a proactive vulnerability management strategy to stay ahead of potential threats.

The integration also enables data-driven decision-making by providing rich data on network configurations and security events. Organizations are recommended to establish processes that use the analytics generated by IPFabric and Tufin to inform strategic decisions related to network security and rule management.

Continuous monitoring of network changes and compliance with security policies is facilitated by the integrated solution. To ensure ongoing adherence to industry regulations and organizational policies, it is recommended to implement regular audits and compliance checks using the integrated tools.

Lastly, organizations should consider the scalability of the integrated solution to accommodate future growth and changes in the network environment. Regular assessments of scalability, along with proactive planning for future enhancements and updates, are advised to ensure the continued effectiveness and relevance of the integrated solution in the evolving landscape of network security.

References

[1] G. Vigna, F. Valeur, J. Zhou, and R. Kemmerer, "Composable tools for network discovery and security analysis," 02 2002, pp. 14– 24.

[2] D. Rountree, "Chapter 3 - securing network access," in *Windows 2012 Server Network Security*, D. Rountree, Ed. Boston: Syngress, 2013, pp. 45–87. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9781597499583000030

[3] F. V. Manuel Cheminod, "An optimized firewall anomaly resolution," *Journal of Internet Services and Information Security*, vol. 10, pp. 22–37, 2 2020.

[4] J. Kizza, *Firewalls*, 04 2017, pp. 251–274.

[5] F. Ali, "A study of technology in firewall system," 09 2011, pp. 232–236.

[6] J. Al-Saraireh and A. Masarweh, "A novel approach for detecting advanced persistent threats," *Egyptian Informatics Journal*, vol. 23, no. 4, pp. 45–55, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1110866522000470

[7] A. Al-Hawamleh, A. Alorfi, J. Al-Gasawneh, and G. Al-Rawashdeh, "Cyber security and ethical hacking: The importance of protecting user data," *Solid State Technology*, vol. 63, 12 2020.

[8] C. Togay, A. Kaşif, C. Catal, and B. Tekinerdogan, "A firewall policy anomaly detection framework for reliable network security," *IEEE Transactions on Reliability*, vol. PP, pp. 1–9, 07 2021.

[9] D. Bringhenti, G. Marchetto, R. Sisto, F. Valenza, and J. Yusupov, "Automated firewall configuration in virtual networks," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, pp. 1–1, 01 2022.

[10] J. Burns, A. Cheng, P. Gurung, S. Rajagopalan, P. Rao, D. Rosenbluth, A. Surendran, and Martin, "Automatic management of network security policy," vol. II, 02 2001, pp. 12–26 vol.2.

[11] R. Oliveira, L. Sihyung, and H. Kim, "Automatic detection of firewall misconfigurations using firewall and network routing policies," 01 2009.

[12] M. Rahman, A. Pakstas, and F. Wang, "Network topology generation and discovery tools," *in: Proc. of the 7th EPSRC Annual Postgraduate Symposium on the Convergence of Telecommunications, Net-working and Broadcasting (EPSRC PGNet 2006)*, 12 2008.

[13] S. T. Help. (2023) Software testing help. [Online]. Available: https://www.gartner.com/reviews/market/network-automation-tools/vendor/ip-fabric/product/ip-fabric-automated-network-assurance-platform/alternatives

[14] Tufin. Tufin. [Online]. Available: https://www.tufin.com/

[15] IPFabric. Ipfabric. [Online]. Available: https://docs.ipfabric.io/6.2/

[16] Gartner. Gartner. [Online]. Available: https://www.gartner.com/reviews/market/network-automation-tools/vendor/ip-fabric/product/ip-fabric-automated-network-assurance-platform/alternatives

[17] J. Dsouza, L. Elezabeth, V. P. Mishra, and R. Jain, "Security in cyber-physical systems," 02 2019, pp. 840–844.

[18] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for iot: Security issues, challenges, solutions and recommendations," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 280–308, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667345223000238

[19] S. T. Prasad, "Ethical hacking and types of hackers," *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)*, vol. 11, no. 2, pp. 24–27, 2014.

[20] B. S. Rawal, G. Manogaran, and A. Peter, *The Basics of Hacking and Penetration Testing*. Singapore: Springer Nature Singapore, 2023, pp. 21–46. [Online]. Available: https://doi.org/10.1007/978-981-19-2658-7_2

[21] A. Tetskyi, V. Kharchenko, and D. Uzun, "Neural networks based choice of tools for penetration testing of web applications," 05 2018, pp. 402–405.

Acknowledgments

I dreamt of living abroad, making a living abroad. Yet I couldn't imagine the place to this would be of all places Padova whose name I have ever heard because of Alessandro Del Piero in my childhood. I would like to thank my family who raised and helped me become the man I am today. Further, I want to thank my friends for having shared joyful and memorable days. Special thanks to my deskmate, colleague, and good friend Berk. Lastly, grazie mille Mary.