UNIVERSITY OF PADOVA

DEPARTMENT OF MATHEMATICS "TULLIO LEVI-CIVITA"

MASTER THESIS IN CYBERSECURITY

ENHANCING CYBERSECURITY POSTURE THROUGH INTEGRATION OF FIREWALL MANAGEMENT AND MICRO-SEGMENTATION TOOLS

SUPERVISOR
PROF. ALESSANDRO BRIGHENTE
UNIVERSITY OF PADOVA

CO-SUPERVISOR
PROF. MAURO CONTI

MASTER CANDIDATE
NURI BERK CIFTPINAR

STUDENT ID
2041268

ACADEMIC YEAR
2023-2024

“Anyone who has never made a mistake has never tried anything new.”
— Albert Einstein

Abstract

In an era marked by evolving cyber threats, the imperative for robust cybersecurity posture has become paramount. This thesis delves into the realm of advanced cybersecurity strategies, focusing on the integration of cutting-edge technologies to fortify network defenses. The research explores the harmony and integration benefits between firewall management and micro-segmentation tools. This integration provides an automatization of real-time data transmission for enhanced security.

The study begins by elucidating the foundational concepts of firewall management, micro-segmentation and their individual roles in safeguarding enterprise networks. Then, continues with the details of the utilized brands during research and dives into, what they are and how they work.

A significant portion of the thesis is dedicated to the explanation and integration of firewall management and micro-segmentation tools, showcasing the symbiotic relationship between these technologies. The research presents a comprehensive analysis of the mechanisms involved in the seamless coordination of firewall policies and micro-segmentation strategies.

The implementation aspect of the study unveils a developed framework that exemplifies the successful integration of firewall management and micro-segmentation tools. The solution that is developed for a special case, also ensures not only enhanced security but also streamlined operations through the automated real-time transmission of critical data.

The results are evaluated to demonstrate the integration's effect on cyber resilience and monitoring efficiency and shown with more of a qualitative perspective due to privacy policies the quantitative results are restricted. However, the fact that all the machines that are required to be imported, is achieved in the lab environment with 100/100 accurate transmission and providing real-time monitoring. This quantitative results can be broadened via performing various attack scenarios and observing real-life scenarios. To sum up, the goal is to provide better visibility, effective control over IT systems simultaneously and illustrate a significant reduction in vulnerabilities in this way.

Contents

Listing of figures

Listing of tables

Listing of acronyms

AFRM	Automated Firewall Rule Management
CIA	Confidentiality Integrity Availability
GDPR	General Data Protection Law
HIPAA	Accountability Act
ICS	Industrial Control Systems
IoT	Internet of Things
IPAM	IP Address Management
IPS	Intrusion Prevention Systems
IT	Information Technology
ITSM	IT Service Management
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NGFW	Next Generation Firewall
OT	Operational Technology
PCI DSS	Payment Card Industry Data Security Standard
QoS	Quality of Service
ROI	Return on Investment
SaaS	Software as a Service
SDN	Software-defined networking
SIEM	Security Information and Event Management
SLA	Service-level Agreement
SOAR	Security Orchestration, Automation, and Response

SOX	Sarbanes–Oxley Act
USP	Unified Security Policy
UTM	Unified Threat Management
VCA	Vulnerability-based Change Automation

1 Introduction

In an era that is dominated by connectivity and wide digital networks the importance of robust cybersecurity measures and efficient precautions cannot be overstated. As organizations increasingly rely on intricate IT infrastructures to facilitate their operations, safeguarding sensitive data and critical assets becomes a paramount concern. The continuous evolution of cyber threats necessitates the development of innovative and comprehensive security strategies to ensure the resilience of organizational networks.

This thesis explores a novel approach to fortifying cybersecurity defenses by seamlessly integrating two cutting-edge technologies: Tufin, a firewall management tool, and Akamai Guardicore, a micro-segmentation solution. By combining the strengths of these tools, the research aims to create a unified and responsive cybersecurity framework that is capable of addressing the dynamic and sophisticated nature of contemporary cyber threats by increased visibility and monitoring in the first place.

The selected firewall orchestration tool, Tufin, is famous for its ability to streamline and automate the management of firewall policies across diverse network environments. Tufin empowers organizations to maintain a centralized view of their firewall configurations, facilitating efficient policy implementation and continuous monitoring. Concurrently, Akamai Guardicore's micro-segmentation capabilities provide granular control over network traffic, allowing for the segmentation of network assets into isolated security zones. This enhances the overall security posture by restricting lateral movement within the network and minimizing the attack surface.

The crux of this thesis lies in the development and implementation of an integration script designed to bridge the gap between Tufin Orchestration Tool and Akamai Guardicore Segmentation. This integration facilitates the seamless transmission of data and assets between the two environments, enabling real-time updates to firewall policies based on the dynamically changing micro-segmentation configurations. The synergy between Tufin and Guardicore is anticipated to create a responsive cybersecurity ecosystem capable of adapting to emerging threats promptly.

This research endeavors to contribute to the cybersecurity domain by providing a practical and effective solution that leverages the strengths of both firewall orchestration and micro-segmentation. Next chapters will delve into the technical aspects of the integration script, the methodologies employed and the empirical results obtained through the implementation of the proposed solution. Through this exploration, we aim to elucidate the potential of this integration in fortifying organizational cybersecurity postures, ultimately contributing to the adaptive and resilient cybersecurity strategies in an ever-evolving digital landscape.

Main strong points of the research:

1. Increased Network Security:

   The integration of Tufin and Akamai Guardicore is designed to elevate network security by creating a cohesive defense mechanism. The dynamic exchange of real-time data between the firewall orchestration tool and the micro-segmentation solution ensures that security policies are promptly updated to respond to emerging threats. This approach not only strengthens the overall security posture but also minimizes the window of vulnerability, enhancing the organization's resilience against cyber-attacks.

2. Efficient Visibility and Monitoring:

   The research focuses on improving the efficiency of network visibility and monitoring. Tufin's firewall orchestration capabilities provide centralized visibility into firewall configurations, while Akamai Guardicore's micro-segmentation enhances granular control over network traffic. The integration script facilitates the seamless exchange of data, ensuring that security administrators have a comprehensive and real-time view of the network. This heightened visibility enables swift identification of potential security incidents and facilitates proactive responses to mitigate risks.

3. Mitigating Vulnerabilities: The integration code plays a pivotal role in mitigating vulnerabilities within the network. By dynamically updating firewall policies based on the micro-segmentation configurations, the research aims to reduce the attack surface and restrict unauthorized lateral movement within the network. This proactive approach to vulnerability management contributes to a more resilient cybersecurity infrastructure, safeguarding critical assets against potential exploitation.

4. Ensuring Compliance: A key aspect of the research involves addressing regulatory and compliance requirements. The integrated approach aligns firewall policies with micro-segmentation configurations, ensuring that security measures are in accordance with industry standards and regulatory mandates. This not only enhances the organization's ability to meet compliance requirements but also fosters a culture of cybersecurity governance.

5. Efficiency and Productivity: The seamless integration of Tufin and Akamai Guardicore is geared towards optimizing operational efficiency and productivity. Automation of firewall policy updates based on micro-segmentation changes reduces manual intervention which allows security teams to focus on strategic initiatives. This is not only streamlines security operations but also enhances overall productivity by freeing up resources for more value-added tasks.

   Overall, it is anticipated that the research's conclusions will benefit organizations as well as the larger cybersecurity community by offering insightful analysis and workable solutions to the fields of network security and governance.

Research Questions and Hypotheses

Is it possible to integrate different tools that work in the security field with different purposes? Would it be logical to make an efficient integration and is this meaningful? What is the contribution of both automation and segmentation? We could assume that using Tufin Orchestration Tool and combining it with the Akamai Guardicore segmentation tool would create a solid and efficient visibility and monitoring that increases overall security.

Chapter 2 will include a comprehensive Literature Review, Chapter 3 will provide an explanation of the study's methodology. As we move into Chapter 4, The lab environment and code skeleton will be explained. Chapter 5 evaluates and discusses the obtained results and study comes to the close, presenting a summary and the impact in the relevant field.

2
Background and Literature Review

Since the networks are expanding day by day, the need for security is getting more attention. Hackers have always been renowned as a severe security threat. Ethical hacking is an important form of hacking. It is a type of hacking that doesn't hurt any individual, association, or gathering. It is done with a positive intent to find out the security loop-holes in the current infrastructure of some organizations [1].

Security is the condition of being protected in opposition to danger or loss. From the perspective of networks, it is also called information security. Computer security is required because most organizations can be damaged by both adversarial and unintentional harmful software or intruders. There are several forms of damage which could be interrelated with the attack process and the producer or executor of the adversarial attack [2].

There are security issues in data governance such as data risks arising from the diversification of new technology applications, data risk due to human factors which can be both from hacker attacks or human operation problems, lack of adequate understanding of data governance leads to data risks, data security governance technology application level issues and the risks arising from data exchange. These data security governance problems can be solved with the improvement of the legal system and raising awareness of data security protection, scenario-based data security governance and building a data security governance framework [3].

There are essential software metrics. A software metric is a common way to quantify a certain aspect of a software product. Metrics are typically used to assess a software's capacity to accomplish a predetermined goal. One popular information security model that is frequently used is called CIA (Confidentiality, Integrity, and Availability). They are principal keys for developing a software that is safe. The CIA triad is a foundational security model. When designing any secure system, one of the most crucial steps is often to make sure that the three aspects of the CIA triad are protected [4].

There are various kinds of attack types, tools and attacks based on the goal. However, there are also various ways and tools to prevent and discover the adversarial attacks to the system, network, data and information [5] [6]. Main ideas to increase the network security could be, improving firewall technology level, optimizing and upgrading encryption technology, improving identity verification technology, leveraging the advantages of cloud computing and blockchain technology, establishing an intelligent system for identifying information security issues [7].

Firewalls

Security is one of the crucial challenges for software applications that requires some solutions in different levels, such as device level, network level and application level. For addressing network-level security, various custom network security protocols and different firewalls have been developed. A firewall can be hardware or software and also can be combined with both. The fundamental use of a firewall is monitoring the network traffic to allow or block the traffic by using a set of rules [8]. There are different types of firewalls [9], such as packet-filtering firewall, proxy firewall, stateful inspection firewall, application-layer firewall, unified threat management (UTM) firewall, next-generation firewall (NGFW) and threat-focused NGFW [10].

To understand the mentality and the working principles of firewalls we can take a look at the main differences between different types of firewalls. For example, a packet-filtering firewall does not know whether one packet is related to another packet but a stateful inspection firewall investigates the traffic to determine the context of the packet. Another instance is that, a proxy firewall checks the packets in the application layer, and the UTM firewall combines the functionalities of stateful inspection firewalls and intrusion prevention systems (IPS). NGFW firewalls utilize various properties. It includes capabilities of standard firewalls, IPS, and application awareness and control.

Order	Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
1	TCP	192.152.1.*	ANY	128.172.26.*	80	ALLOW
2	TCP	192.152.1.72	ANY	128.172.*.*	80	DENY
3	TCP	192.152.1.*	ANY	128.172.26.2	80	ALLOW
4	TCP	ANY	ANY	ANY	80	ALLOW
5	TCP	151.*.*.*	ANY	108.56.56.1	53	DENY
6	TCP	151.126.*.*	ANY	108.56.56.1	53	ALLOW
7	UDP	216.22.14.*	ANY	124.24.*.*	53	ALLOW
8	UDP	216.22.14.1	ANY	124.24.*.*	53	DENY
9	ANY	ANY	ANY	ANY	ANY	DENY

Table 2.1: Firewall Policy Ruleset [12]

A packet-filtering firewall is basically a rule-based system that consists of an ordered ruleset and operates in the network and transport OSI layers [11]. Rules consist of fields which can be grouped into filtering and action fields. An ordinary firewall rule model usually consists of some filtering fields such as the protocol field, the source IP address, the source port number, the destination IP address, and the destination port number and the action field. When a packet arrives, it passes through the condition of the rules one by one until completely matching the filtering fields of a rule. In such a case, the action of the rule is executed.

The table Table 2.1 represents a firewall policy ruleset, outlining the specific configurations for handling network traffic based on various criteria. [12] Each row in the table corresponds to a rule that defines how the firewall should process incoming or outgoing packets. The columns provide details about the order of the rule, the protocol (TCP or UDP), source IP addresses and ports, destination IP addresses and ports, and the intended action (ALLOW or DENY). For example, the first rule (Order 1) allows TCP traffic from any source IP in the range 192.152.1.* to any destination IP in the range 128.172.26.* on port 80. Conversely, the second rule (Order 2) denies TCP traffic from the specific source IP 192.152.1.72 to any destination IP in the range 128.172.*.* on port 80.

Rule Management

Rule Management is an already important standalone concept but especially when the setup includes automation and orchestration tools, rule management becomes a crucial component of network security. Rule management includes the process of defining, organizing, monitoring, and maintaining the rules and policies that govern the behavior of security devices and software in a network.

Rule management allows network administrators to specify which users, devices, or systems are allowed or denied access to specific network resources. By defining access control rules, organizations can prevent unauthorized access and reduce the attack surface, enhancing overall security. Furthermore, effective traffic filtering is essential to avoid or at least minimize the risk of any attack and any malware. Rules can help to decide how to filter the network traffic, by specifying protocols, ports, and IP addresses are allowed or blocked.

A proper rule management ensures that the policies are always compliant and enforced regarding the current needs across the network. Usually organizations must stick to specific regulatory requirements and internal security policies. Automation combined with orchestration tools can help to manage the compliance process better and helps organizations to reduce the risk of human error. Moreover rule management the coherence between policies all across the network

If there is an anomaly, in other words if there is any suspicious or malicious activity, rules can be configured to trigger an alert or can be configured to use automated responses. An effective rule management should provide properly tuned and updated rules to respond to evolving threats in real-time.

Resource optimization and scalability can also be provided by an effective rule management process. It helps in optimizing network resources by ensuring that rules are only in place when needed. The unnecessary traffic bottlenecks can be avoided or any performance issues that can result from overburdened security devices. As networks grow and evolve, managing security rules becomes more and more complex. Automation and orchestration tools can simplify the scalability of rule management and this makes it easier to adapt to changing network requirements.

One of the crucial things that is provided by an advantageous rule management process is extensive monitoring. Moreover, effective rule management includes the ability to monitor and audit rule usage. In addition, extensive and proper monitoring provides the opportunity to easily troubleshoot and make security analysis. The network environments are generally dynamic, and changes in network configurations cannot be avoided. The correct management of rules provides that the changes to security rules are carefully controlled, documented, and properly tested to avoid unwanted consequences.

Automation and Orchestration Tools

Since the cyberworld continues to expand and the companies are getting bigger and bigger, the context of cybersecurity also widens and new concepts are evolving to provide efficiency, speed and easy management. In this sense, automation and orchestration tools are essential components of a company's defense against cyber threats. These tools help security teams to streamline their workflows and respond to incidents more efficiently and enhance overall security posture. Let's take a deeper look at each headings.

Researches shows that the benefits of this Orchestration and Automatization tools can be increased by combining several technologies. For example, leveraging AI within these processes not only contributes to the identification and mitigation of emerging threats but also facilitates a dynamic and adaptive security infrastructure, ultimately resulting in improved overall system performance [13].

The adoption of Containerization and VM technologies offers significant performance efficiencies and space gains [14]. VMs enable the creation of isolated environments, optimizing resource allocation and enhancing scalability, while Container technologies provide a lightweight, portable solution for packaging and deploying firewall configurations. The integration of such technologies into orchestration and automation tools not only contributes to a more agile and resource-efficient cybersecurity infrastructure but also allows for greater flexibility in managing diverse network environments [15].

Automation:

First of all, automation refers to the use of technology to perform tasks and processes with minimal human intervention. In cybersecurity, automation involves using software and scripts to handle routine, repetitive, or time-sensitive security tasks. It is better to reduce human error and make the system work continuously and instant. Some examples of automated cybersecurity processes include:

- Patch management: Automatically applying software updates and security patches to systems and applications. In this way, the systems that are patching on-time ensures efficiency and up-to-date solutions
- Log analysis: Automatically scanning and analyzing logs for suspicious activities or patterns. This can provide better monitoring systems, better analyze opportunities and alert systems in general.
- User provisioning and deprovisioning: Automatically granting or revoking access privileges for users based on predefined criteria.
- Phishing email detection and response: Automatically identifying and blocking phishing emails or isolating compromised systems.

The goal of automation in cybersecurity is to reduce the burden on security analysts, speed up response times and minimize the likelihood of human error. Automated processes can be triggered by predefined events or criteria, such as specific security alerts or the detection of anomalies.

Orchestration:

Orchestration is the process of coordinating and integrating multiple automated tasks and processes to achieve a specific objective. In cybersecurity, orchestration tools act as the "conductor" of various security tools and technologies, ensuring they work together in harmony to respond to threats and incidents effectively. Some common use cases for orchestration in cybersecurity include:

- Incident response: Orchestrating the different and various components configurations at one place, investigation of the assets and flows and the remediation of security components and processes, involving various security tools like firewalls, SIEM (Security Information and Event Management) systems and other endpoint protection solutions.
- Threat intelligence sharing: Automatization and coordination of the sharing of threat intelligence data with other organizations or security platforms to improve collective responses and defenses.

- Workflow automation: Creating and managing workflows for tasks like user access management, compliance reporting and security policy enforcement. Especially this helps to reduce the errors during firewall rule management in Tufin.
- Security policy enforcement: Automatization of the application of security policies and configurations across the organization's network and systems.

Orchestration tools assist security teams to maintain consistency and efficiency in the operations by connecting various security technologies and making them work in harmony. They often use predefined workflows, decision trees, and conditional logic to determine the appropriate actions to take based on the context of the incident.

The combination of automation and orchestration in cybersecurity can greatly enhance an organization's ability to detect, to respond, and to mitigate security threats on time and in an effective manner. These tools can also help organizations adapt to the evolving threat landscape by enabling rapid responses and reducing the risk of human error in critical security processes.

Topology

A topology refers to the inclusive layout of the network components and the connections between them. These connections include firewalls, routers, switches and other devices. Network topology is important for designing, implementing, and managing secure networks. It helps to define how data flows within the network and how security measures are applied to protect the network from various threats. Network topology can differ based on the specific architecture in an organization according to its specific needs and requirements.

A network topology usually depends on some factors such as the organization's size, budget, security requirements, and scalability. Additionally, network topology helps network administrators to manage and to maintain the security infrastructure wıth the impact on the factors like the ease of troubleshooting, scalability and the ability to implement security policies effectively. Thus, network topology is a fundamental concept in network security as it helps to shape the security strategy and architecture of an entire network.

There can be different kinds of network topologies such as Tree, Star, Mesh, Hybrid and etc. A network topology can directly affect the QoS (Quality of Service) which could be evaluated by using round-trip times, convergence times, and HTTP load performance, revealing differences in performance characteristics for various network configurations. The comparison and evaluations with real-life scenarios [16].

Mainly, automation and orchestration tools are used to automate tasks and workflows as it is obvious from the names. However, there are also beneficial various functions that came together with these tools such as, streamline network management, the topology, path management and rule management that are critical for automation and orchestration tools to manage efficiently and secure the network

Since automation and orchestration tools rely on a clear understanding of the network's topology to function effectively it is essential to know how devices are connected, where the choke points are and how data flows through the network. This information is vital for creating automation scripts and orchestration workflows. It is important to enforce security policies consistently across the network. So, the topology allows us to visualize and determine where to deploy security rules that could be firewall policies or intrusion detection/prevention rules whether in specific network segments or devices.

A consistent understanding of the network's topology is crucial to provide a scalable automation and a proper orchestration. Since a network may possibly grow, evolve and change, these tools need to adapt to new devices and connections consistently. If Automation tools can automatically discover new devices and adjust workflows accordingly, a clear visualization and understanding of the topology will be ensured and this will help both professionals and the tools directly. Automation tools can automatically discover new devices and adjust workflows accordingly.

Ensuring efficient and secure workflows is essential. Automation and orchestration tools can optimize network operations and security by streamlining repetitive tasks. A good understanding of the topology is important because if there is a network issue or a security incident, it helps us to quickly identify the root cause and to respond quickly. Automation tools can assist in diagnosing problems by providing real-time information about the network's structure and traffic patterns.

So, the network topology is a foundational element in the effective use of automation and orchestration tools in network management and security. These tools rely on accurate and up-to-date knowledge of topology to enforce security policies, optimize workflows, and respond to incidents more efficiently and effectively.

Tufin

Tufin offers Security Policy Automation for an Enterprise, enabling you to secure the network and cloud environments and deploy a Zero Trust Architecture using one of the most powerful security policy automation technologies. With Tufin, you can achieve end-to-end network security across your hybrid enterprise infrastructure, all powered by a single solution designed to serve both your network and cloud security teams [17].

Tufin provides you the opportunity to manage the firewall policies efficiently, including parts as: rule optimization, cleanup and risk analysis. It enables you to define and enforce security policies across the network structure. This ensures consistency and compliance. Also, Tufin provides automation capabilities to reduce errors and to speed up the process, to be more general, to increase the performance. With Tufin it is easy to track and manage the changes to firewalls and network device configurations. This helps organizations in the audit phase too. With this, it is easy to meet the regulatory and compliance requirements. Also, Identifying potential vulnerabilities and risks are easy with the provided functions of the tool.

The increased visibility with the topology tool helps us to investigate the whole network map as well as providing the chance to dive deep into the details and examining certain scopes in the whole network. The software consists of three main parts that are securetrack, securechange and secureapp.

You can execute Policy Management flawlessly. Handling the complexity of policy management across hybrid-cloud environments is not an easy thing to do. With Tufin it is not just about managing but it is about mastering. The whole process is organized to let you operate as fast as your business needs, starting from providing the global policy standards to the automatized rule management and efficiently handling security policy violations.

The concept "agility" meets network security. In today's rapidly evolving cyber landscape, continuous and consistent security across hybrid-cloud networks is crucial. After understanding the network security posture, Tufin also actively improves it. With the collaboration that is done, it deploys applications with verified security and in this way shrinks the attack surface. All in all the system becomes agile,reliable and gains uncompromising network protection.

Tufin also provides compliance clarity and rapid audit responses. The compliance, delays and uncertainties are usually costly. Tufin offers a clear path. It guarantees continuous compliance from General Data Protection Law (GDPR) to the Health Insurance Portability and Accountability Act (HIPAA). The ability to run instant audits and illustrate immediate proof of adherence makes manual processes outdated and old-school. Proactive compliance and rapid audit readiness contributes both effectiveness and functionality.

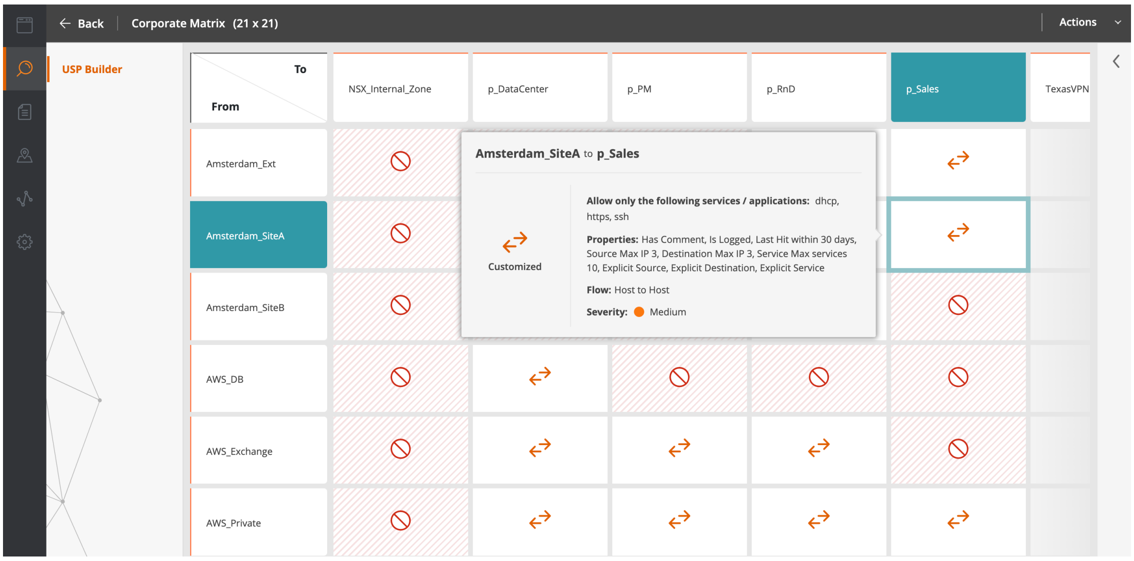
SecureTrack+

SecureTrack+ provides centralized network security policy management, risk mitigation, simplified segmentation and compliance monitoring across firewalls, NGFWs (Next Generation Firewalls), routers, switches, SDN (Software defined networking) and hybrid cloud. Mainly, it introduces holistic visibility, and consolidates the management of your network segmentation policies across both on-premises and cloud. SecureTrack+ allows you to establish a baseline of allowed and blocked traffic between security zones and monitor in real time for violations, making it easier to implement and manage consistent network segmentation. The main properties and some screenshots will be given in the following parts.

Tufin monitors network traffic logs in real time. Also, security policy builder helps us to illuminate the gaps between your desired segmentation and reality. In addition it ensures instructions on the changes required to close those gaps.

By utilizing IP Address Management (IPAM) Integration SecureTrack+ increases the accuracy of risk assessments and violation alerts by automatically populating and maintaining any subnet changes.

A Unified Security Policy (USP) is shown in Figure 2.1 Apart from easily seeing the From-To information and if the traffic is blocked,allowed or customized information. By clicking in a specific rectangle that is given you can investigate the information more detailed. For example, you can see which protocols are allowed or blocked, flow information, properties and the severity level.



To From	NSX_Internal_Zone	p_DataCenter	p_PM	p_RnD	p_Sales	TexasVPN
Amsterdam_Ext	🚫				⇄	
Amsterdam_SiteA	🚫				⇄	
Amsterdam_SiteB	🚫				🚫	
AWS_DB	🚫	⇄	🚫	🚫	🚫	
AWS_Exchange	🚫	⇄	⇄	⇄	🚫	
AWS_Private	🚫	⇄	⇄	⇄	⇄	

Amsterdam_SiteA to **p_Sales**

⇄ Customized

Allow only the following services / applications: dhcp, https, ssh

Properties: Has Comment, Is Logged, Last Hit within 30 days, Source Max IP 3, Destination Max IP 3, Service Max services 10, Explicit Source, Explicit Destination, Explicit Service

Flow: Host to Host

Severity: ● Medium

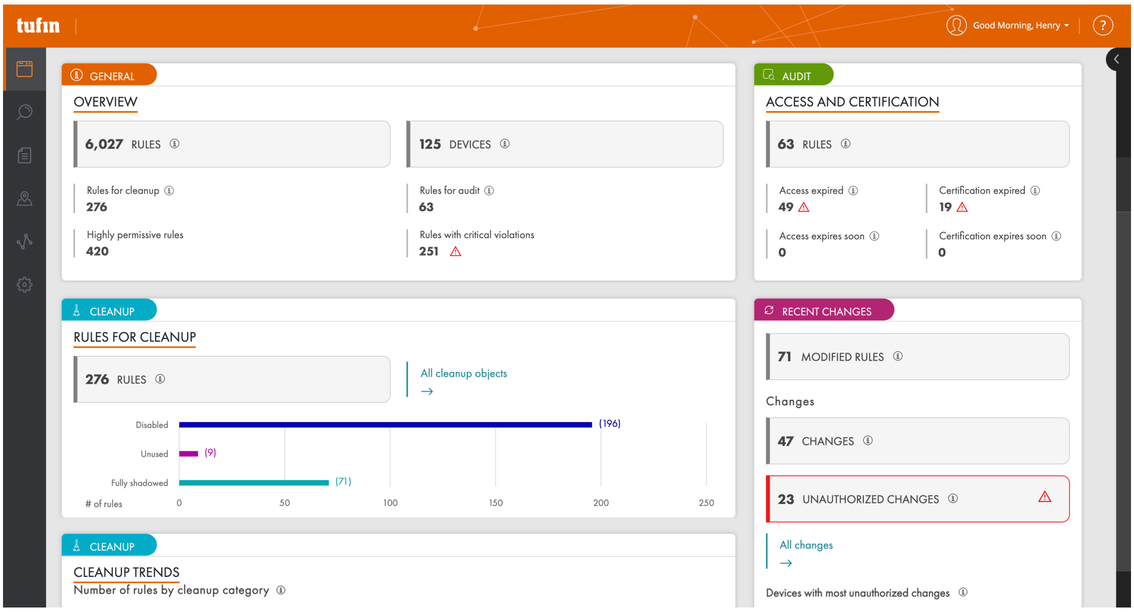
Figure 2.1: USP Builder

SecureTrack+ Provides automated firewall rule and network object cleanup that delivers immediate ROI (Return on investment).

With Firewall Rule Cleanup property, SecureTrack+ ensures the opportunity to automatically detect and alert on unused, shadowed, redundant, overly permissive rules and enables automatic rule decommissioning. According to Tufin, clients have reduced their time spent on rule cleanup by 90/100.

Also by using Automatic Unused Object Identification and Network Object Decommissioning, SecureTrack+ can identify and remove network objects (server/subnet/range), which are no longer used due to hardware replacement or network architecture changes.

In Figure 2.2 the cleanup page is demonstrated. At a glance you can see the overview section that shows how many rules and devices exist. Also, the related information to the rules such as "rules for cleanup" and "high permissive rules". In the Devices side you can see "Rules for audit" and "Rules for critical violations". Moreover, up to your will, you can investigate more deeper information using Audit, Cleanup, Recent Changes and Cleanup sections that are shown. In the audit section you can see access and certification information, here it is shown that for 63



tufin

Good Morning, Henry ▾

GENERAL

OVERVIEW

6,027 RULES ⓘ

125 DEVICES ⓘ

Rules for cleanup ⓘ
276

Rules for audit ⓘ
63

Highly permissive rules
420

Rules with critical violations
251 ⚠

AUDIT

ACCESS AND CERTIFICATION

63 RULES ⓘ

Access expired ⓘ
49 ⚠

Certification expired ⓘ
19 ⚠

Access expires soon ⓘ
0

Certification expires soon ⓘ
0

CLEANUP

RULES FOR CLEANUP

276 RULES ⓘ

All cleanup objects
→

RECENT CHANGES

71 MODIFIED RULES ⓘ

Changes

47 CHANGES ⓘ

23 UNAUTHORIZED CHANGES ⓘ ⚠

All changes
→

Devices with most unauthorized changes ⓘ

CLEANUP

CLEANUP TRENDS

Number of rules by cleanup category ⓘ

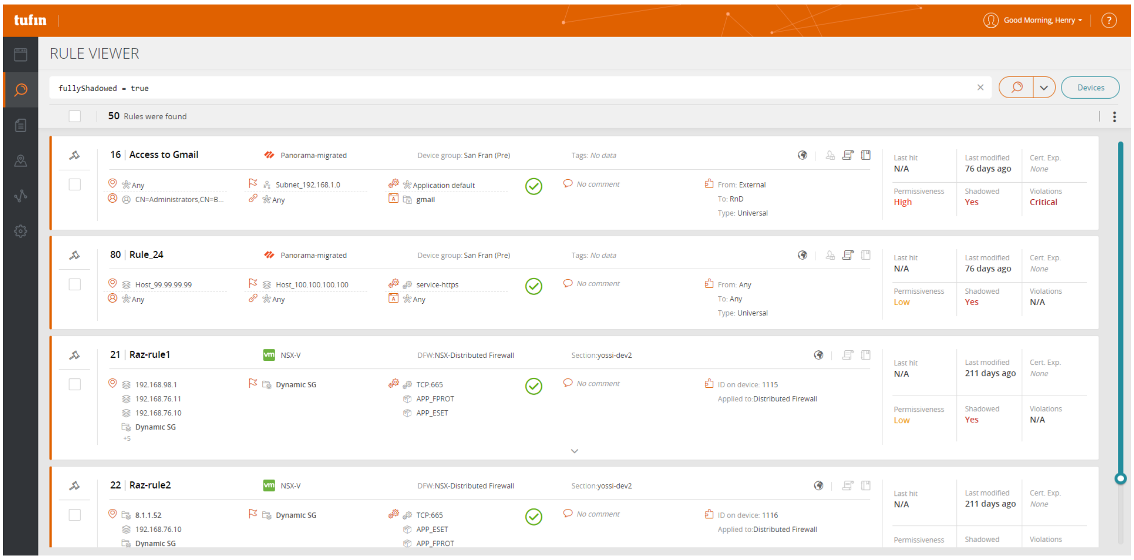
Figure 2.2: Cleanup Page

rules 49 access is expired and for 19 rules certification expired.

From this GUI you can see the recent changes which helps you to understand what is happening recently. Figure 2.2 illustrates that there are 71 Modified Rules and related to these rules, 47 changes and 23 unauthorized changes exist. In addition, In the Cleanup section there is a bit more detailed information for rules for cleanup. It is shown that there are 276 rules with 196 Disabled 9 Unused and 71 Fully shadowed.

Tufin helps you to automate firewall management and rule base optimization. Tufin assures simple firewall management even though they are produced from various different vendors by providing a central repository of all the firewall rules and objects. The advanced search mechanism and filtering system reduces the time and effort associated with firewall management.

The Automated Policy Generator automatically determines, based on existing traffic, who/what truly requires access, optimizing firewall rule bases in accordance with least privilege principles. This unique capability not only makes firewall optimization attainable for overstretched firewall teams, but it allows optimization to become part of a repeatable firewall management process.



fullyShadowed = true

50 Rules were found

16 Access to Gmail — Panorama-migrated — Device group: San Fran (Pre) — Tags: No data
Any — Subnet_192.168.1.0 — Application default — No comment — From: External
CN=Administrators,CN=B... — Any — gmail — To: RnD — Type: Universal
Last hit N/A — Last modified 76 days ago — Cert. Exp. None
Permissiveness High — Shadowed Yes — Violations Critical

80 Rule_24 — Panorama-migrated — Device group: San Fran (Pre) — Tags: No data
Host_99.99.99.99 — Host_100.100.100.100 — service-https — No comment — From: Any
Any — Any — Any — To: Any — Type: Universal
Last hit N/A — Last modified 76 days ago — Cert. Exp. None
Permissiveness Low — Shadowed Yes — Violations N/A

21 Raz-rule1 — NSX-V — DFW:NSX-Distributed Firewall — Section:yossi-dev2
192.168.98.1 — Dynamic SG — TCP:665 — No comment — ID on device: 1115
192.168.76.11 — APP_FPROT — Applied to:Distributed Firewall
192.168.76.10 — APP_ESET
Dynamic SG
+5
Last hit N/A — Last modified 211 days ago — Cert. Exp. None
Permissiveness Low — Shadowed Yes — Violations N/A

22 Raz-rule2 — NSX-V — DFW:NSX-Distributed Firewall — Section:yossi-dev2
8.1.1.52 — Dynamic SG — TCP:665 — No comment — ID on device: 1116
192.168.76.10 — APP_ESET — Applied to:Distributed Firewall
Dynamic SG — APP_FPROT
Last hit N/A — Last modified 211 days ago — Cert. Exp. None
Permissiveness — Shadowed — Violations

Figure 2.3: Rule Viewer

There is an overview of Rule Viewer In Figure 2.3. You can see the search bar on the top. and the rules according to your filter will be shown at the bottom. For each rule, the name, the device group and tags exist. On the right part the information regarding Last hit, Last modified, Certification, Permissiveness, Shadowed and Violations information.

In this figure, since the fullyshadowed = true condition has been used, all the rules that has been filtered come with the information Shadowed Yes in the right part of the screen. Here in this screen you can see the destination IP addresses and source IP addresses following with the protocols that you can use.

Compliance monitoring across thousands of network and cloud resources ensures real-time risk awareness. The responsible network and security teams can see any risky access and firewall security policy violations in real-time from a central dashboard. They can also receive the related alerts which helps them to notice and rapidly intervene. SecureTrack allows you to monitor network changes. Furthermore, It compares them to security/compliance policies and prioritizes violations according to criticality.

SecureTrack+ integrates with your vulnerability management solution, allowing you to cor-

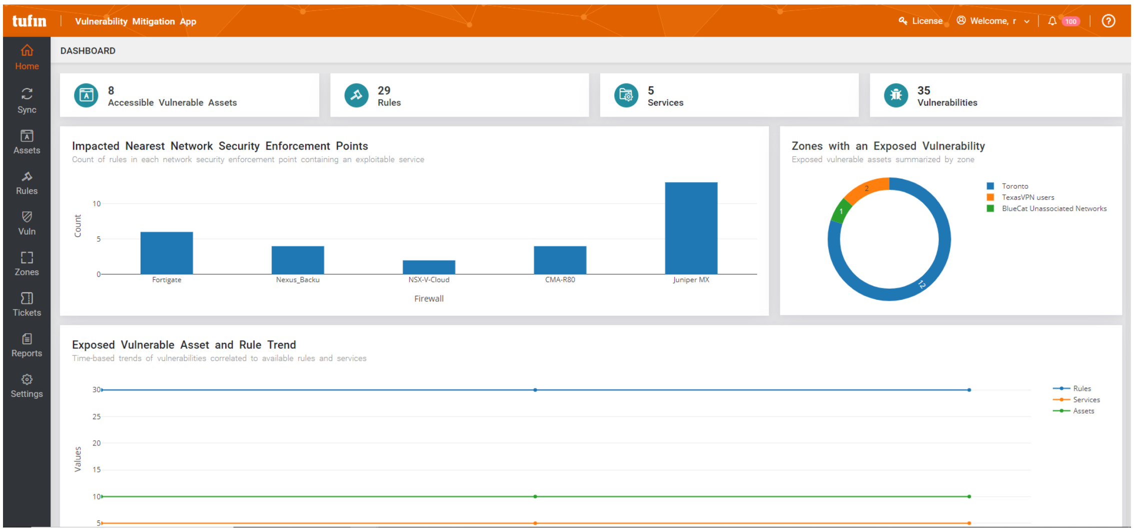

tufin
Vulnerability Mitigation App
License
Welcome, r
100
Home
Sync
Assets
Rules
Vuln
Zones
Tickets
Reports
Settings
DASHBOARD
8
Accessible Vulnerable Assets
29
Rules
5
Services
35
Vulnerabilities
Impacted Nearest Network Security Enforcement Points
Count of rules in each network security enforcement point containing an exploitable service
Count
10
5
0
Fortigate
Nexus_Backu
NSX-V-Cloud
CMA-R80
Juniper MX
Firewall
Zones with an Exposed Vulnerability
Exposed vulnerable assets summarized by zone
2
1
12
Toronto
TexasVPN users
BlueCat Unassociated Networks
Exposed Vulnerable Asset and Rule Trend
Time-based trends of vulnerabilities correlated to available rules and services
Values
30
25
20
15
10
5
Rules
Services
Assets

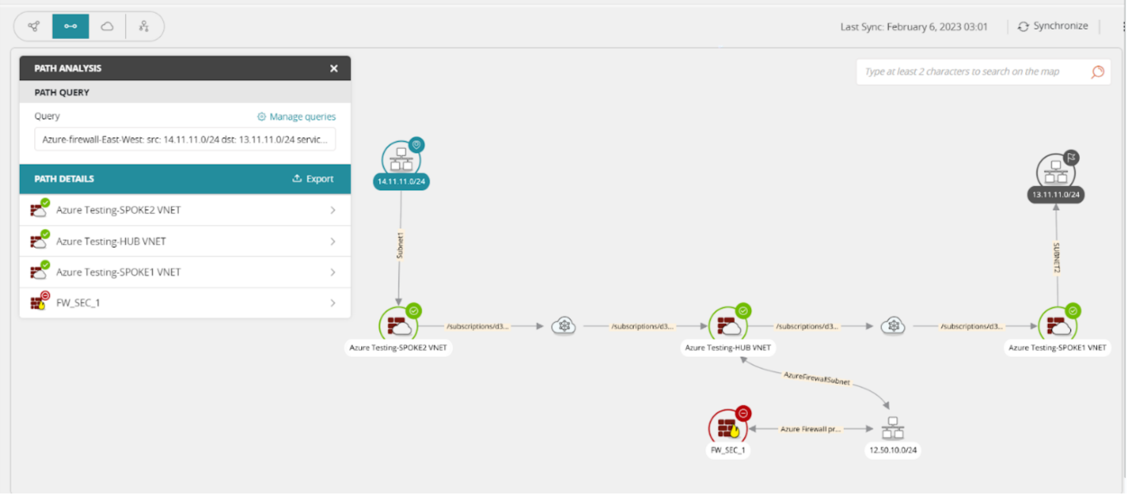
Figure 2.4: Dashboard

relate network intelligence with vulnerability scanning data. This allows you to prioritize patching faster. Simply you can mitigate the vulnerabilities

The Dashboard shown in Figure 2.4. At a glance we can see that there are several graphs to support the visualization and the information that we can grasp. The data in the upside of the page basically mentions accessible vulnerable assets, rules, services, vulnerabilities. The first graph, which is a bar chart, illustrates "Impacted Nearest Network Security Enforcement Points" the count of rules in each network security enforcement point containing an exploitable service.

Also a useful circle graph on the right side of the page is given which is Zones with an Exposed Vulnerability Exposed vulnerable assets summarized by zone. In this example you can see that the zones are given colors and names which are blue, orange, green; Toronto, TexasVPN users, BlueCat Unassociated Networks respectively to increase the perception and intelligibility.

In the bottom side of the page there is another type of a graph which is Exposed Vulnerable Asset and Rule Trend that simply shows Time based trends of vulnerabilities correlated to available rules and services. The blue color given for rules, Orange for services and green for assets with the matched values on the left side.



Query: Azure-firewall-East-West: src: 14.11.11.0/24 dst: 13.11.11.0/24 servic...

- Azure Testing-SPOKE2 VNET
- Azure Testing-HUB VNET
- Azure Testing-SPOKE1 VNET
- FW_SEC_1

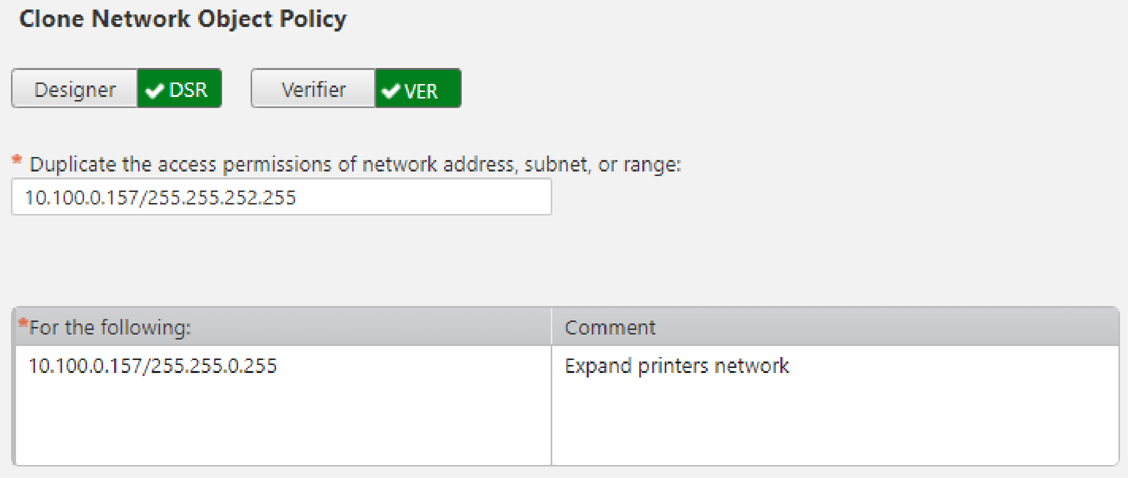
Figure 2.5: Topology

You can extend network security policy orchestration and automation to the cloud. Only Tufin ensures agentless, multi-cloud policy management. You can utilize the benefits of cloud-native infrastructure, maintain enterprise-wide visibility and control, and optimize segmentation across both on-premises and cloud.

Tufin can be easily integrated to your CI/CD process to serve as the security gatekeeper for the DevOps team, so they do not need to change the way they work. Only using alerts, which is a simple step, Tufin significantly reduces risks for the organization while trimming workload. Tufin will alert on access changes that violate segmentation policies and proactively block the changes pre-deployment.

Topology Map is one of the crucial parts of Tufin, because it increases the visibility and everything starts from seeing what we have. In Figure 2.5, the topology map of a path analysis is demonstrated. First of all, here the topology map shows the path from the source 14.11.11.0/24 to destination 13.11.11.0/24. On the left you can see the path analysis given with two main parts which are path query and path details respectively. In path details the firewalls that a package should pass are given with a list as it is shown in the visual map on the right. You can understand if a package is blocked in a specific firewall or it is allowed by looking at the signs and the color on the top right of each firewall symbol.

It provides hardware expansion and data center migration safer and faster. The network ob-



Clone Network Object Policy

Designer ✓ DSR

Verifier ✓ VER

* Duplicate the access permissions of network address, subnet, or range:

10.100.0.157/255.255.252.255

*For the following:	Comment
10.100.0.157/255.255.0.255	Expand printers network

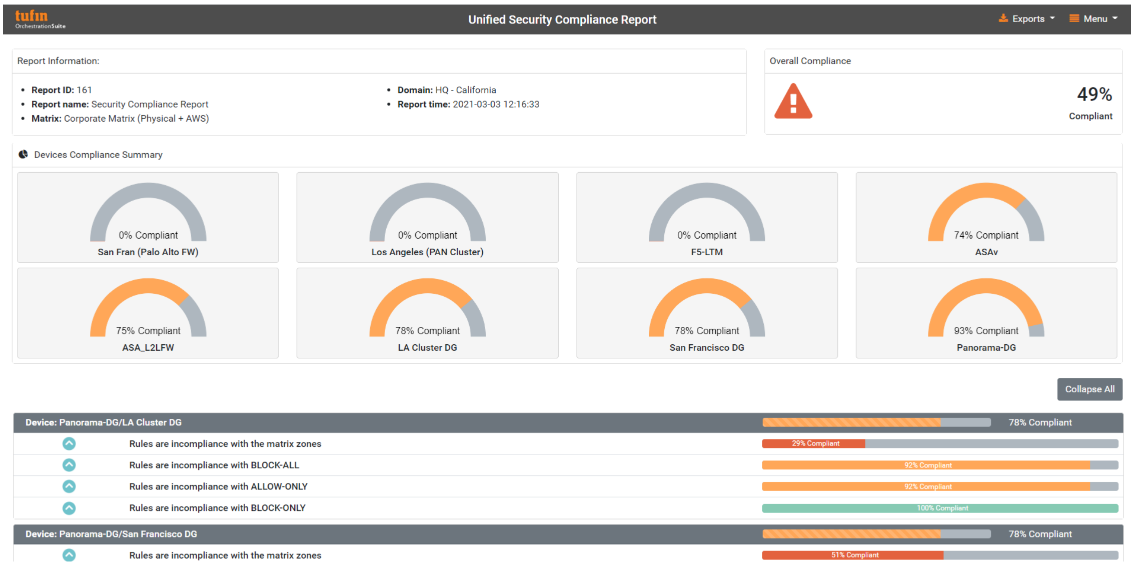
Figure 2.6: Clone Network Object Policy

ject policy cloning workflow seriously reduces manual tasks and the human error related with data center migration, hardware expansion and/or hardware replacement, as it automatically clones the security policy of existing servers/subnets/ranges to newly added ones.

A piece of a workflow In Figure 2.6 Clone Network Object Policy is illustrated. Each workflow has different steps. In this screenshot it is shown that the designer and verifier has approved and the IP addresses are given with the related subnet masks. To increase the intelligibility, the comment section exists if there is any need.

In addition to real-time compliance monitoring for risky changes and violations, SecureTrack+ provides the first step to continuous compliance with an automated audit trail that allows you to rapidly generate various customizable audit reports that comply with regulatory standards, such as PCI-DSS, SOX, NERC-CIP, HIPAA, GDPR and more. So that you can reduce audit prep by up to 90/100.

In Figure 2.7 there is a Unified Security Compliance Report. On the top you can clearly see the Report information which include Report ID, Report Name, Matrix, Doman and Report Time. On the right the Overall Compliance given with a clear, exact percentage. In the middle "Device Compliance Summary" is given. In the bottom of the page, statistics for incompliance is given by grouping the data with either matrix zones or block-allow and only-all properties.



Unified Security Compliance Report

Report Information:

- **Report ID:** 161
- **Report name:** Security Compliance Report
- **Matrix:** Corporate Matrix (Physical + AWS)
- **Domain:** HQ - California
- **Report time:** 2021-03-03 12:16:33

Overall Compliance

49%
Compliant

Devices Compliance Summary

0% Compliant San Fran (Palo Alto FW)	0% Compliant Los Angeles (PAN Cluster)	0% Compliant F5-LTM	74% Compliant ASAv
75% Compliant ASA_L2LFW	78% Compliant LA Cluster DG	78% Compliant San Francisco DG	93% Compliant Panorama-DG

Device: Panorama-DG/LA Cluster DG	78% Compliant
Rules are incompliance with the matrix zones	29% Compliant
Rules are incompliance with BLOCK-ALL	92% Compliant
Rules are incompliance with ALLOW-ONLY	92% Compliant
Rules are incompliance with BLOCK-ONLY	100% Compliant
Device: Panorama-DG/San Francisco DG	78% Compliant
Rules are incompliance with the matrix zones	51% Compliant

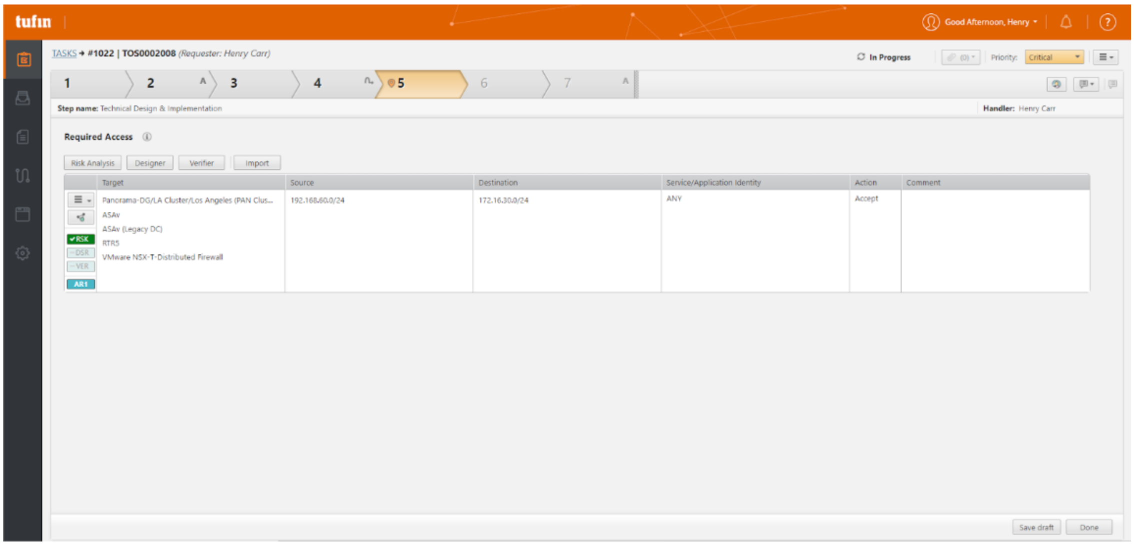
Figure 2.7: Unified Security Compliance Report

What is Secure Change+

The primary difference between SecureTrack+ and SecureChange+ is, SecureTrack is focusing on monitoring and auditing in the existing network security policies to provide compliance and security. On the other hand SecureChange+ focuses on managing the process of making efficient and secure changes to these policies. These two components work together in a complementary manner.

To be more detailed, SecureChange+ helps you to achieve continuous compliance and to reduce network change Service Level Agreements (SLA) by up to 90/100 with network change design automation and rule lifecycle management. You can eliminate network change and rule review backlogs. With Tufin you can utilize the existing resources more than you do before by providing flexible workflows and automation that can dramatically reduce your time spent on network changes and rule lifecycle management.

Repeatable, auditable and policy-driven processes also reduce risk for your organization, while making it easier for you to implement and maintain more advanced network segmentation. Tufin integrates with IT Service Management (ITSM) solutions, allowing for a ticket in your ITSM to trigger a workflow within Tufin.



TASKS → #1022 | TOS0002008 *(Requester: Henry Carr)*

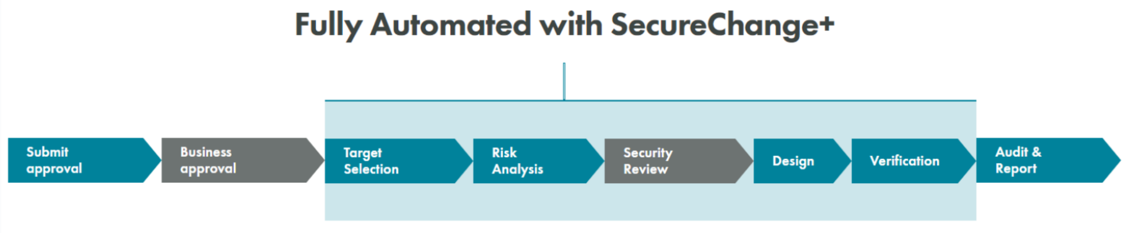
In Progress   Priority: Critical

Step name: Technical Design & Implementation   **Handler:** Henry Carr

Required Access

Target	Source	Destination	Service/Application Identity	Action	Comment
Panorama-DG/LA Cluster/Los Angeles (PAN Clus... ASAv ASAv (Legacy DC) RTR5 VMware NSX-T-Distributed Firewall	192.168.60.0/24	172.16.30.0/24	ANY	Accept	

Figure 2.8: Technical Design and Implementation



Access Request Workflow - a unified change process enables collaboration and visibility across teams.

Figure 2.9: SecureChange+ Automated Workflow

There is a workflow example in Figure 2.8. Step 5, Technical Design Implementation is shown. Here on the top you can see the ID and requester. Then the workflow steps are shown and you can track which step you are following at the moment. The handler also given on the right top side. Also, you can find the target, source, destination, service/application identity, action and comment parts. Number of workflow examples can be increased as access/decommission request, group modification, rule modification, rule recertification.

We can roughly say that ”Business Approval” ensures that policy changes align with the organization's business goals, while ”Security Overview” focuses on the technical aspects of designing, verifying, and documenting these changes to enhance network security and operational efficiency. These components help organizations to make a balance between the business needs and the security requirements in their network policies. We can explain the rest of the Figure 2.9 as following:

- Submit approval: The initial stage of the SecureChange+ workflow. In this step, users can submit change requests for alterations to the network security policies. SecureChange+ can be used directly or can be integrated with your ITSM to submit the requests with your ITSM.

- Target Selection: Target Selection is a critical component of the workflow where SecureChange+ uses advanced network analysis techniques to identify. Automatically identifies firewall targets and security groups based on real-time, full path analysis of your network.

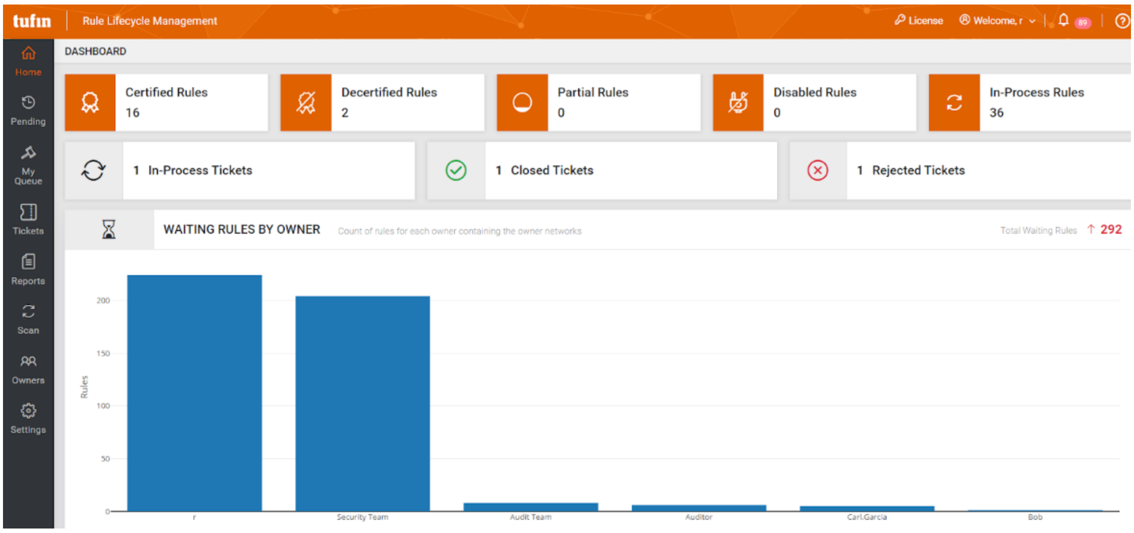
- Risk Analysis: In this phase, SecureChange+ uses a proactive approach. Automatically performs risk assessment against the policy, vulnerability data and other third-party security intelligence to prevent policy change violations and prevent access to risky assets.

- Design: SecureChange+ leverages its intelligence to automatically suggest the most efficient set of changes necessary across network devices and security groups to process a request ticket.

- Verification: The Verifier automatically tests to confirm that your change was implemented. This step focuses on validating whether the new configurations align with the desired security and operational standards.

- Audit Report: SecureChange+ maintains a comprehensive record of each change request, including details on who initiated the request, approvals obtained, verification and testing results, and the changes made. Simply all changes made are documented and reportable.

Tufin orchestrates rule review across owners with an automated recertification process. It identifies expiring or expired rules and maps them to owners, eliminating many of the manual steps normally required. So, you can automate rule lifecycle management.



DASHBOARD

Certified Rules 16

Decertified Rules 2

Partial Rules 0

Disabled Rules 0

In-Process Rules 36

1 In-Process Tickets

1 Closed Tickets

1 Rejected Tickets

WAITING RULES BY OWNER Count of rules for each owner containing the owner networks

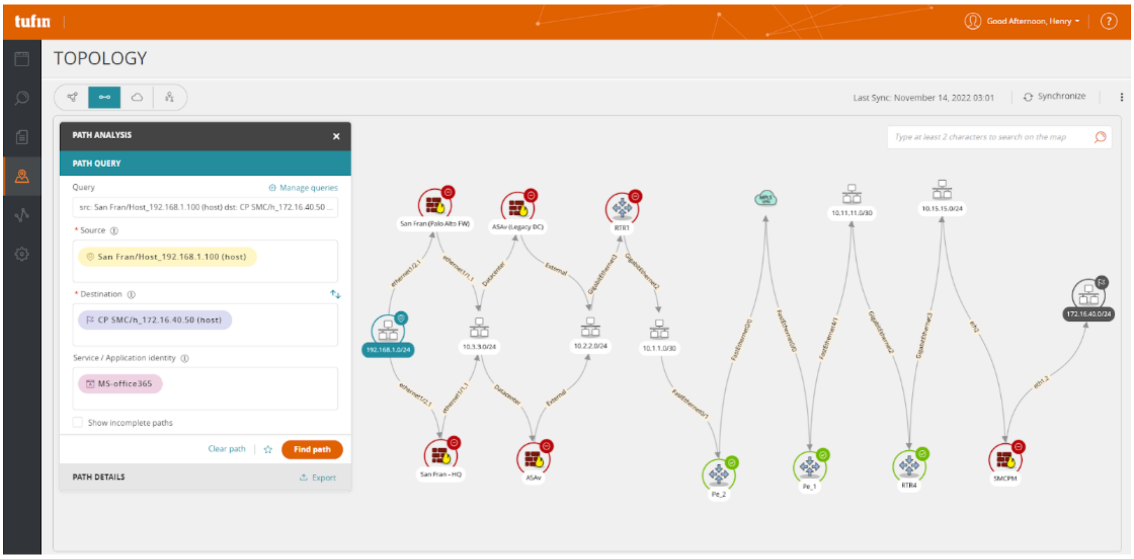
Total Waiting Rules ↑ 292

Figure 2.10: Dashboard Graphs

SecureChange+ gives you the option to customize your rule review process so that it satisfies the unique requirements of your company, which will increase the effectiveness of your network security policy administration. To share duties effectively, you can identify inactive owners for rule reassignment. The portal also helps to coordinate rule review among numerous owners, speeding up the procedure. In order to keep your network policies current and secure, SecureChange+ uses automated rule certification that makes modifications when necessary, and decommissioning when it is appropriate. Also, the system keeps an accurate audit trail, ensuring compliance and accountability with the record of all policy-related operations.

Dashboard is shown in Figure 2.10. You can see that rules are categorized on the top of the page as Certified Rules, Decertified Rules, Partial Rules, Disabled Rules, In-Process Rules. There are three sections following as In Process Tickets, Closed Tickets and Rejected Tickets given with its associated numbers. Also, there are statistics for waiting rules by the owner. The total waiting rule number is also given on the right.

By harnessing SecureChange+'s topology intelligence it provides highly accurate target selection and dynamic visualization of proposed change designs, in this way Tufin becomes outstanding in the competition. This offers detailed path analysis and efficient verification of successful access additions, enabling quick troubleshooting. Also, the platform's path analysis capabilities include controlling and simulating network traffic patterns, including those in



TOPOLOGY

PATH ANALYSIS

PATH QUERY

Query: src: San Fran/Host_192.168.1.100 (host) dst: CP SMC/h_172.16.40.50 ...

* Source: San Fran/Host_192.168.1.100 (host)

* Destination: CP SMC/h_172.16.40.50 (host)

Service / Application identity: MS-office365

□ Show incomplete paths

PATH DETAILS

Last Sync: November 14, 2022 03:01

Figure 2.11: Tufin Topology

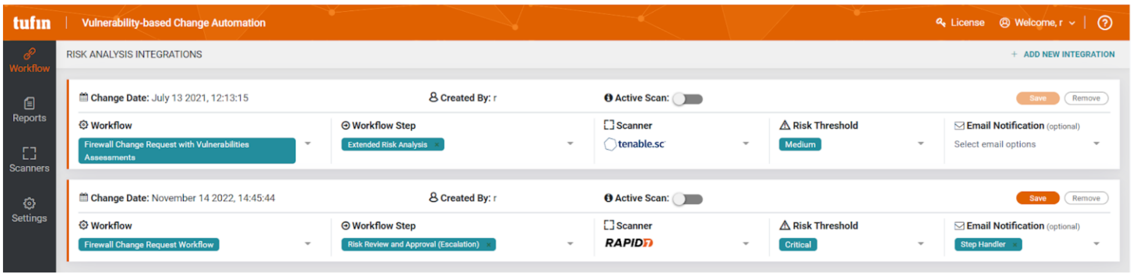
multi-cloud environments. By supporting over 200 million routes, this reduces downtime.

The topology is given in Figure 2.11. The main structure is the same and most of the entire page is very similar to the previous example. A complex network structure is illustrated here and in the path analysis part you can notice the difference as source, destination and services can be examined more detailed and clear here.

Proactive risk assessment allows you to include third-party security intelligence. SecureChange enables continuous compliance with internal policies and industry regulations, such as PCI-DSS, NERC-CIP, and HIPAA.

Proactive risk assessment is part of the network change design process. This investigates the proposed changes against your security/compliance policies and it can be personalized to cross-reference intelligence from third-party solutions, such as vulnerability management tools, SIEM, SOAR and endpoint threat detection tools.

Third-party integrations are vital for building a robust and adaptable security ecosystem with Tufin. The wide range in various fields of cybersecurity is precious including the pioneer vendors and critical areas in the market.



Change Date: July 13 2021, 12:13:15 | Created By: r | Active Scan:

Workflow: Firewall Change Request with Vulnerabilities Assessments
Workflow Step: Extended Risk Analysis
Scanner: tenable.sc
Risk Threshold: Medium
Email Notification (optional): Select email options

Change Date: November 14 2022, 14:45:44 | Created By: r | Active Scan:

Workflow: Firewall Change Request Workflow
Workflow Step: Risk Review and Approval (Escalation)
Scanner: RAPID7
Risk Threshold: Critical
Email Notification (optional): Step Handler

Figure 2.12: Risk Analysis Integration

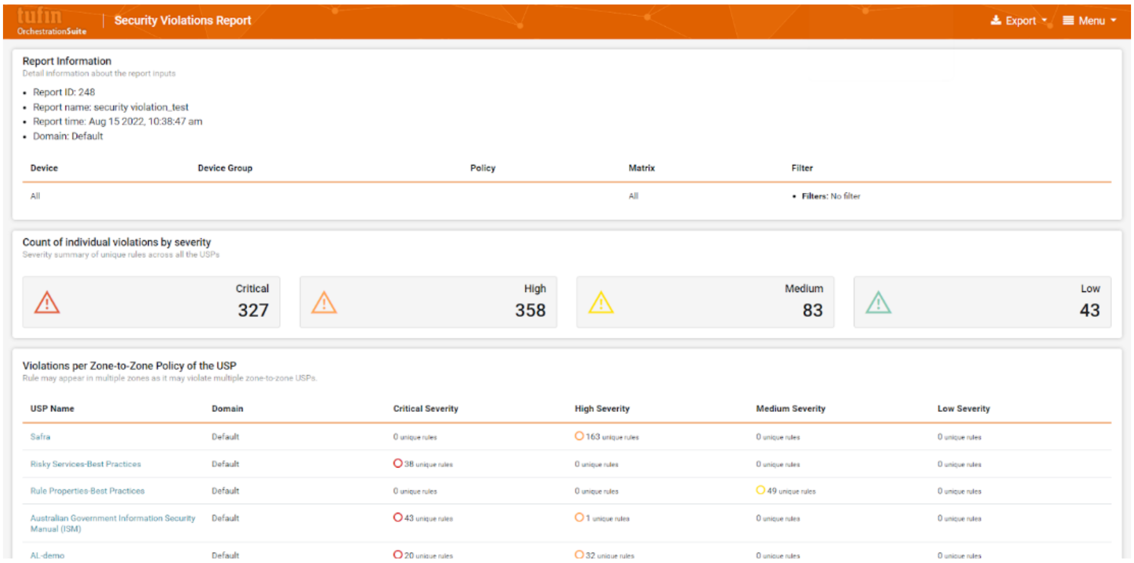
Extending network security policy orchestration and automation to the cloud have benefits. Agentless, multi-cloud policy management is offered by Tufin. So that we can take the full advantage of cloud-native infrastructure, maintain enterprise-wide visibility and control, and optimize segmentation across on-prem and cloud.

In a sense integrating safety barriers into the CI/CD process has benefits. Tufin easily integrates into your CI/CD process to serve as the security gatekeeper for your DevOps team, so that they do not need to change the way they work. When access modifications are made that go against segmentation policies, Tufin alerts the user and prevents the changes from being deployed. This straightforward action can significantly lower risk for your company while reducing workload.

Integrating vulnerability awareness into the change design process is crucial for many reasons such as, maintaining a secure and compliant network environment, reducing risks and costs, and enhancing operational efficiency and overall security. Vulnerability-based Change Automation (VCA) integrates vulnerability awareness into the change design process, by checking for vulnerabilities on source and destination during the change design process.

In Figure 2.12. Risk Analysis integrations demonstrated. The change date time has shown on the left top of each integration. In the same line the creator is shown and there is a toggle button for "Active Scan". On the bottom workflow, workflow step, scanner, risk threshold and the optional email notification sections exist.

It is essential to have an advanced audit readiness with enterprise-wide change logging. As with SecureTrack+, SecureChange+ provides real-time compliance monitoring and a variety of customizable audit reports that align with regulatory standards, such as PCI-DSS, NERC-CIP,



Report Information
Detail information about the report inputs

- Report ID: 248
- Report name: security violation_test
- Report time: Aug 15 2022, 10:38:47 am
- Domain: Default

Device	Device Group	Policy	Matrix	Filter
All			All	• **Filters:** No filter

Count of individual violations by severity
Severity summary of unique rules across all the USPs

Critical	High	Medium	Low
327	358	83	43

Violations per Zone-to-Zone Policy of the USP
Rule may appear in multiple zones as it may violate multiple zone-to-zone USPs.

USP Name	Domain	Critical Severity	High Severity	Medium Severity	Low Severity
Safra	Default	0 unique rules	○ 163 unique rules	0 unique rules	0 unique rules
Risky Services-Best Practices	Default	○ 38 unique rules	0 unique rules	0 unique rules	0 unique rules
Rule Properties-Best Practices	Default	0 unique rules	0 unique rules	○ 49 unique rules	0 unique rules
Australian Government Information Security Manual (ISM)	Default	○ 43 unique rules	○ 1 unique rules	0 unique rules	0 unique rules
AL-demo	Default	○ 20 unique rules	○ 32 unique rules	0 unique rules	0 unique rules

Figure 2.13: Security Violations Report

HIPAA, GDPR and more. However, SecureChange+ enables a higher level of audit readiness by offering a thorough audit trail for network changes, complete change accountability, and audit-ready reports. All related tickets and every change is logged and reportable.

What is SecureApp. (Enterprise)

SecureApp is an application-centric network security management solution. By using SecureApp, organizations can view their network topology from a functional perspective and easily monitor and control communication between applications and services in their network, even if the user has no prior network management experience. With this approach, network security teams and application teams can communicate better, deploy applications more quickly, and increase business agility. The main properties that are offered with SecureApp can be listed as follows [17].

- Visibility and control: Obtain real-time visibility into business applications with a central repository of all application connectivity needs, current connectivity status, and any open SecureChange tickets.

- Application connectivity management: Obtain a thorough and accurate understanding of application connectivity from beginning to end. After connections are set up and an application is defined, SecureApp uses network topology intelligence to show connectivity status continuously. It also provides graphical diagnostic tools to help you understand, troubleshoot and automatically repair connectivity issues.

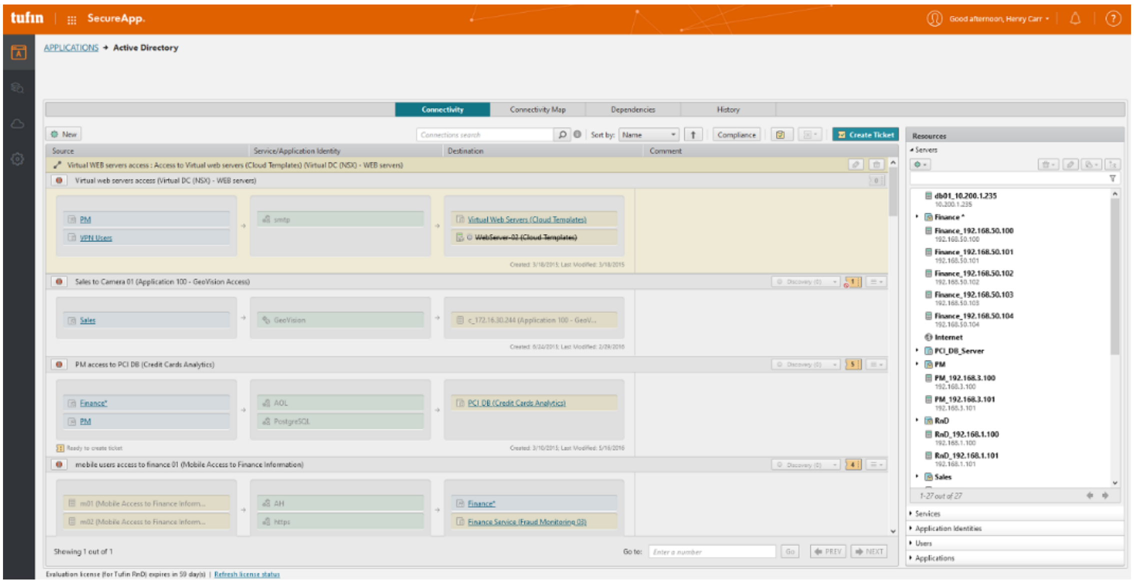
- Streamline operations, improve collaboration: By providing a central console for all network-related application changes, which guarantees that the network is always in line with shifting application requirements, you can reduce conflict between siloed teams. Application teams do not need information on the network topology to define application components and their relationships.

- Security change automation: Define, implement, monitor, and maintain application connectivity through a highly automated process. By specifying connection resources in SecureApp, you can create, update, or decommission an application connection. With a single click, you can also start an automated change workflow by creating the relevant ticket in SecureChange.

Security Violations Report is a critical tool in managing and improving an organization's cybersecurity posture. It helps to identify and respond to security incidents while helping comply with regulations. In Figure 2.13 the security violations report has shown. Report Information shown on the top including Report ID, Report name, Report time and Domain. Also the Device, Device Group, Policy, Matrix, Filter parameters are given. Count of individual violations by severity is categorized into four that are Critical, High, Medium and Low. Then the Violations per Zone-to-Zone Policy of the USP is given with details of USP Name, Domain and associated severities.

Figure 2.14 shows an application page that is Active Directory in this case. You see the Connectivity page. By clicking new you can add a new Connection, Connection to Application or Application Interface. The light yellow title starts with Virtual WEB demonstrating an interface while the group of light-grey rectangles show Connections here. You can see that each connection is separated on the top into four as Source, Service, Destination and Comment (optional).

After adding a Connection you can edit by drag and drop using the properties on the right which are also divided as Servers, Services, Application Identities, Users, Applications. You can also easily delete by clicking on the top right of each connection. Create Ticket on the right



Virtual WEB servers access : Access to Virtual web servers (Cloud Templates) (Virtual DC (NSX) - WEB servers)

Virtual web servers access (Virtual DC (NSX) - WEB servers)

PM, VPN Users → smtp → Virtual Web Servers (Cloud Templates), ~~WebServer-02 (Cloud Templates)~~

Created: 3/18/2015; Last Modified: 3/18/2015

Sales to Camera 01 (Application 100 - GeoVision Access)

Sales → GeoVision → c_172.16.30.244 (Application 100 - GeoV...

Created: 6/24/2015; Last Modified: 2/29/2016

PM access to PCI DB (Credit Cards Analytics)

Finance*, PM → AOL, PostgreSQL → PCI DB (Credit Cards Analytics)

Ready to create ticket

Created: 3/10/2015; Last Modified: 5/16/2016

mobile users access to finance 01 (Mobile Access to Finance Information)

m01 (Mobile Access to Finance Inform..., m02 (Mobile Access to Finance Inform... → AH, https → Finance*, Finance Service (Fraud Monitoring 03)

Showing 1 out of 1

db01_10.200.1.235
10.200.1.235
Finance *
Finance_192.168.50.100
192.168.50.100
Finance_192.168.50.101
192.168.50.101
Finance_192.168.50.102
192.168.50.102
Finance_192.168.50.103
192.168.50.103
Finance_192.168.50.104
192.168.50.104
Internet
PCI_DB_Server
PM
PM_192.168.3.100
192.168.3.100
PM_192.168.3.101
192.168.3.101
RnD
RnD_192.168.1.100
192.168.1.100
RnD_192.168.1.101
192.168.1.101
Sales

1-27 out of 27

Evaluation license (for Tufin RnD) expires in 59 day(s) | Refresh license status

Figure 2.14: Applications

top allows you to choose a workflow and sends it to the SecureChange for control.

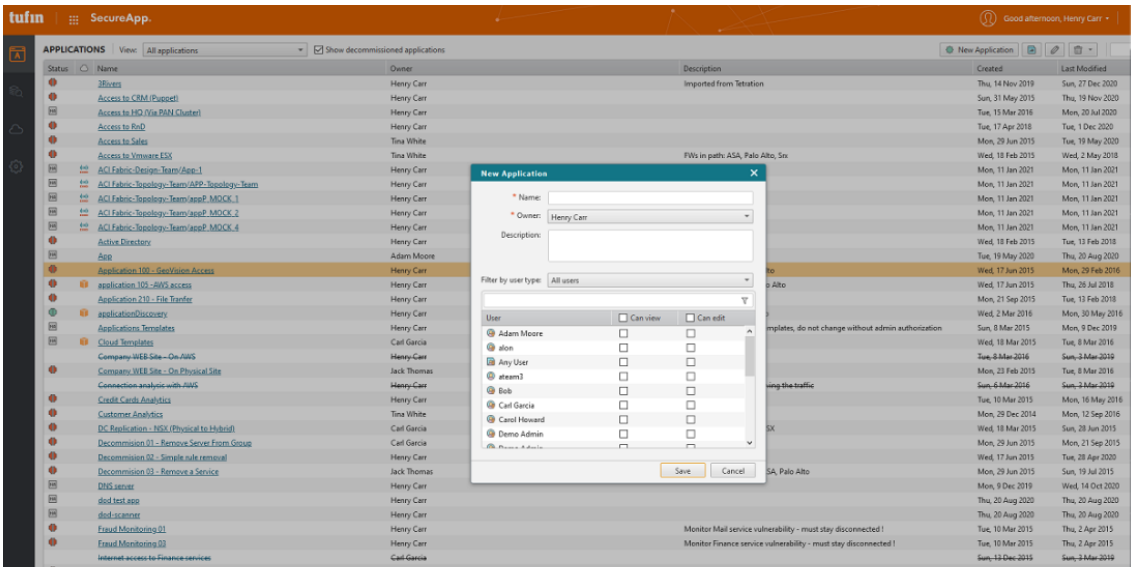
New application can be created as it is illustrated in Figure 2.15. Here you see the properties have to be given as Name, Owner and Description that are followed by the authorizations of other users. We can authorize them to be able to view and edit options by using the provided list.

What is Segmentation?

Network segmentation and microsegmentation are both strategies used in network security to enhance protection against cyber threats. They involve dividing a network into smaller and isolated segments to control and restrict access which limits the potential impact of security incidents.

1. Network Segmentation:

   Network segmentation can be defined as dividing a larger network into smaller segments or subnetworks. Each segment typically contains a specific group of resources, users or services.



APPLICATIONS View: All applications ☑ Show decommissioned applications

Status	○	Name	Owner	Description	Created	Last Modified
		3Rivers	Henry Carr	Imported from Tetration	Thu, 14 Nov 2019	Sun, 27 Dec 2020
		Access to CRM (Puppet)	Henry Carr		Sun, 31 May 2015	Thu, 19 Nov 2020
		Access to HQ (Via PAN Cluster)	Henry Carr		Tue, 15 Mar 2016	Mon, 20 Jul 2020
		Access to RnD	Henry Carr		Tue, 17 Apr 2018	Tue, 1 Dec 2020
		Access to Sales	Tina White		Mon, 29 Jun 2015	Tue, 19 May 2020
		Access to Vmware ESX	Tina White	FWs in path: ASA, Palo Alto, Srx	Wed, 18 Feb 2015	Wed, 2 May 2018
		ACI Fabric-Design-Team/App-1	Henry Carr		Mon, 11 Jan 2021	Mon, 11 Jan 2021
		ACI Fabric-Topology-Team/APP-Topology-Team	Henry Carr		Mon, 11 Jan 2021	Mon, 11 Jan 2021
		ACI Fabric-Topology-Team/appP_MOCK_1	Henry Carr		Mon, 11 Jan 2021	Mon, 11 Jan 2021
		ACI Fabric-Topology-Team/appP_MOCK_2	Henry Carr		Mon, 11 Jan 2021	Mon, 11 Jan 2021
		ACI Fabric-Topology-Team/appP_MOCK_4	Henry Carr		Mon, 11 Jan 2021	Mon, 11 Jan 2021
		Active Directory	Henry Carr		Wed, 18 Feb 2015	Tue, 13 Feb 2018
		App	Adam Moore		Tue, 19 May 2020	Thu, 20 Aug 2020
		Application 100 - GeoVision Access	Henry Carr	to	Wed, 17 Jun 2015	Mon, 29 Feb 2016
		application 105 -AWS access	Henry Carr	o Alto	Wed, 17 Jun 2015	Thu, 26 Jul 2018
		Application 210 - File Tranfer	Henry Carr		Mon, 21 Sep 2015	Tue, 13 Feb 2018
		applicationDiscovery	Henry Carr	o	Wed, 2 Mar 2016	Mon, 30 May 2016
		Applications Templates	Henry Carr	mplates, do not change without admin authorization	Sun, 8 Mar 2015	Mon, 9 Dec 2019
		Cloud Templates	Carl Garcia		Wed, 18 Mar 2015	Tue, 8 Mar 2016
		~~Company WEB Site - On AWS~~	~~Henry Carr~~		~~Tue, 8 Mar 2016~~	~~Sun, 3 Mar 2019~~
		Company WEB Site - On Physical Site	Jack Thomas		Mon, 23 Feb 2015	Tue, 8 Mar 2016
		~~Connection analysis with AWS~~	~~Henry Carr~~	~~ving the traffic~~	~~Sun, 6 Mar 2016~~	~~Sun, 3 Mar 2019~~
		Credit Cards Analytics	Henry Carr		Tue, 10 Mar 2015	Mon, 16 May 2016
		Customer Analytics	Tina White		Mon, 29 Dec 2014	Mon, 12 Sep 2016
		DC Replication - NSX (Physical to Hybrid)	Carl Garcia	SX	Wed, 18 Mar 2015	Sun, 28 Jun 2015
		Decommision 01 - Remove Server From Group	Carl Garcia		Mon, 29 Jun 2015	Mon, 21 Sep 2015
		Decommision 02 - Simple rule removal	Henry Carr		Wed, 17 Jun 2015	Tue, 28 Apr 2020
		Decommision 03 - Remove a Service	Jack Thomas	SA, Palo Alto	Mon, 29 Jun 2015	Sun, 19 Jul 2015
		DNS server	Henry Carr		Mon, 9 Dec 2019	Wed, 14 Oct 2020
		dod test app	Henry Carr		Thu, 20 Aug 2020	Thu, 20 Aug 2020
		dod-scanner	Henry Carr		Thu, 20 Aug 2020	Thu, 20 Aug 2020
		Fraud Monitoring 01	Henry Carr	Monitor Mail service vulnerability - must stay disconnected !	Tue, 10 Mar 2015	Thu, 2 Apr 2015
		Fraud Monitoring 03	Henry Carr	Monitor Finance service vulnerability - must stay disconnected !	Tue, 10 Mar 2015	Thu, 2 Apr 2015
		~~Internet access to Finance services~~	~~Carl Garcia~~		~~Sun, 13 Dec 2015~~	~~Sun, 3 Mar 2019~~

New Application

* Name:

* Owner: Henry Carr

Description:

Filter by user type: All users

User	□ Can view	□ Can edit
Adam Moore	□	□
alon	□	□
Any User	□	□
ateam3	□	□
Bob	□	□
Carl Garcia	□	□
Carol Howard	□	□
Demo Admin	□	□

Save Cancel

Figure 2.15: New Application

The primary goal is to improve network security by creating boundaries and controlling the flow of traffic between segments. If an attacker gains access to one segment, segmentation can help prevent lateral movement to other parts of the network.

2. Microsegmentation:

Microsegmentation is an advanced form of network segmentation that involves dividing the network into very small segments. It is often used on a per-application basis. It provides granular control over communication flows within the network.

The main objective is to increase security by restricting communication between individual workloads or applications. This limits the attack surface and helps to prevent of the lateral spread of threats. Microsegmentation is particularly valuable in cloud environments and data centers with complex architectures.

The security contribution of micro-segmentation combined with a correct and robust configuration should not be discarded. There are frameworks that are developed to be able to assess and quantify the effectiveness of micro-segmentation in reducing the enterprise network assets risk of exposure to insider and outsider threats such as [18].

Contributions to Security;

- Limiting Lateral Movement:

  Network Segmentation restricts the lateral movement of attackers, by dividing the network into segments. Basically, even if an intruder gains access to one segment, the ability to move laterally to other segments is limited which reduces the potential impact of a security breach. On the other hand, microsegmentation offers a more granular approach by restricting communication between specific applications or workloads. This is especially effective in preventing the lateral spread of malware within a network.

- Containment of Threats:

  Network Segmentation helps contain and isolate security incidents. If a breach occurs in one segment, the impact is limited to that segment which prevents the compromise of the entire network. To increase this segmentation microsegmentation could be used which provides even more precise containment by isolating individual applications or workloads. This prevents attackers from moving laterally within the network and limits their ability to compromise critical assets.

- Enhanced Access Control:

  Network Segmentation allows organizations to implement access controls based on the principle of least privilege. Users and devices only have access to the resources required for their specific roles. However, to be able to control a more granular level microsegmentation could be used which allows organizations to define and enforce communication policies at the application or workload level.

- Adaptability to Dynamic Environments:

  Recently, to make changes to your network, there is no need to have a big problem on your network, since the technology evolves day by day, it becomes a continuous need. network segmentation provides a flexible approach to adapt to changes in the network architecture which might be crucial. Also, microsegmentation offers agility in dynamically changing environments, such as cloud platforms, where workloads and applications are frequently deployed, scaled or decommissioned.

Overall, both network segmentation and microsegmentation contributes significantly to the network security by reducing the attack surface, limiting lateral movement and providing more fine-grained access controls. These strategies are particularly important in the modern cybersecurity landscape where threats are sophisticated and organizations need robust defenses to protect their critical assets.

Zero-Trust Segmentation

The Zero-Trust approach employs a multidimensional strategy for handling transactions, incorporating principles like least privilege, network micro-segmentation, and micro-perimeters, which limit access to assets and resources strictly required for specific functions in industrial networks [19].

Zero-Trust segmentation is a security approach that follows the idea of "Do not trust in any user, system, or network by default, even if they are inside the corporate network". Traditional security models often rely on the concept of a trusted internal network, assuming that once a user or device is inside the network perimeter, they can be trusted. However, with the increasing sophistication of cyber threats and the rise of remote work and cloud computing, this assumption has proven to be risky.

Zero-Trust segmentation operates on the principle of ”never trust, always verify.” It assumes that threats can come from both external and internal sources and requires continuous authentication and authorization, regardless of a user's or device's location. The main goal is to minimize the potential attack surface and reduce the risk of lateral movement within a network.

Key components of zero-trust segmentation can be counted as, micro-segmentation, least privilege user access, continuous monitoring and authentication, network visibility analysis and dynamic policy enforcement. By implementing zero-trust segmentation, organizations usually aim to enhance their security posture and better protection against internal and external threats by ensuring ultimate reduction of the risk of data breaches and unauthorized access.

Akamai Guardicore Segmentation

Simply, Akamai Guardicore Segmentation provides a simple and fast way to enforce zero trust principles intuitively within the network. You can eliminate the risk in the network by utilizing microsegmentation [20].

An organization's critical assets could be protected with Guardicore Segmentation, which is briefly, fast, simple and intuitive.

It is fast because it is not using a slow infrastructure segmentation approach, it uses software-based segmentation to prevent attackers reaching your sensitive information. It is simple because it is easy to deploy and manage which provides visibility and control to the IT team. These are fundamental requirements to enforce Zero Trust principles across your data centers, multiclouds, and endpoints. It is intuitive because it prevents malicious lateral movement in your network through the application of precise segmentation policies based on visual insights from across your entire environment.

Guardicore is a robust way to achieve Zero Trust segmentation because it allows you to reduce the attack surface, to prevent lateral movement. So, it allows you to secure critical IT assets. To be more detailed, you reduce the risk without the need for costly security hardware with a software-based micro-segmentation approach. You detect lateral movement and real-time threats across the entire cyberattack kill chain with a single platform. You protect critical assets from ransomware by easily enforcing Zero Trust principles across hybrid cloud ecosystems.

A strong base for workload protection and compliance is the granular isolation and segmentation of the network applications and their components. Akamai Guardicore Segmentation provides an ongoing management process of the microsegmentation policy by enabling deep application dependencies mapping and policy enforcement. It delivers complete and flexible solutions for microsegmentation.

The key properties can be listed as, wide coverage, deep visibility, intuitive workflow and granular policies. Each of these key properties is crucial to provide an efficient security.

How does it work?

Guardicore collects detailed information about the organization's IT infrastructure by using a mix of network-based data collectors, agent-based sensors, virtual private cloud flow logs from cloud providers and integrations that enable agentless functionality. A highly automated and adaptable labeling process that integrates with existing data sources, like orchestration systems and configuration management databases, gives this information related context.

Network map

After the collection of the required information, the output is a dynamic map of the entire IT infrastructure that allows security teams to view activity with user- and process-level granularity on a real-time or historical basis. The development of segmentation policies is made quick, simple, and grounded in the actual workload context by combining these in-depth insights with AI-powered policy workflows.

Templates

Pre-built templates for the most popular use cases simplify the process of creating policies. Since policy enforcement is entirely independent of the underlying infrastructure, complex network changes or downtime are not necessary when creating or changing security policies. Furthermore, policies are followed by the workload regardless of its location, be it public cloud environments or on-premises data centers. This segmentation capabilities are complemented by a sophisticated set of threat defense and breach detection capabilities, as well as by Akamai Hunt, same brand threat hunting service.

Comprehensive protection at scale

In any environment you can protect workloads in complex IT environments with a combination of on-premises workloads, virtual machines, legacy systems, containers and orchestration, public/private cloud instances and IoT/OT

It simplifies security management with one platform that provides network visualization, segmentation, threat defense, breach detection capabilities and guided policy enforcement for Zero Trust initiatives.

You can protect your most important digital assets first, then grow up to safeguard your entire company without adding more complexity, altering your infrastructure, or creating performance bottlenecks.

Comparisons and Reviews

Tufin and Guardicore emerge as standout tools in cybersecurity, particularly in the niche of network security policy management and enforcement. Tufin's strength lies in its comprehensive approach to automating and orchestrating security policies across diverse and complex network infrastructures. The platform excels in providing organizations with a centralized console for policy management, ensuring that security configurations align with industry compliance standards. Tufin's robust automation capabilities streamline workflows, enhancing the efficiency of security policy implementation and ensuring a proactive response to emerging threats.

Notable Tufin competitors include leading names such as AlgoSec, FireMon, Skybox, RedSeal, Check Point, Lacework, Google Cloud Platform, CyberArk, Cisco Secure Workload and Illumio. Tufin is famous for its reliability, popularity, and high level of trust, Tufin is widely recommended as a cornerstone for zero-trust security strategies. With a substantial user base exceeding 2,900 clients worldwide, including industry giants like BlueCross BlueShield, BNP Paribas, Deutsche Bank, and IBM, Tufin has proven its reputation [17].

Similarly, Guardicore stands out as a cutting-edge tool with a focus on micro-segmentation and advanced threat detection. Guardicore's unique approach to visualizing and segmenting network flows within data centers contributes to enhanced security postures. The platform's automation features enable rapid response to security incidents, reducing dwell time and minimizing potential damages. Guardicore's ability to provide granular visibility into network traffic and apply segmentation policies based on application behavior is lauded by users for its effectiveness in preventing lateral movement of cyber threats.

Prominent competitors of Akamai Guardicore Segmentation include Trend Micro Deep Security, Prisma Cloud, Singularity Cloud, Sophos Central, Microsoft Defender for Cloud, CloudGuard Cloud Native Security platform, Trellix Cloud Security, and ColorTokens Xtended ZeroTrust Platform. Akamai Guardicore Segmentation is recognized for its robust security measures and widespread adoption. Positioned as a key player in the realm of zero-trust security strategies, Akamai Guardicore boasts a substantial user base, with organizations such as CNH Industrial, GM Korea Company, Australian Taxation Office, Tapestry, TD Ameritrade, State

Of California, Credit Suisse Group AG, and MetLife, Inc., among its users [21]. This reflects the platform's trustworthiness and its ability to cater to the security needs of diverse industry leaders.

So overall, Tufin earns acclaim for its adaptability in navigating dynamic network landscapes, positioning itself as the top choice for organizations in search of a comprehensive and scalable solution for orchestrating security policies. Simultaneously, Guardicore stands out as an exceptional tool, particularly favored by organizations prioritizing defense-in-depth strategies. Its strength lies in intelligent segmentation and automated threat response that solidifies Guardicore's role in safeguarding critical assets against evolving cybersecurity threats. These comparisons can be made and reviews can be seen in several web sources[21] [22].

3 Methodology

Detailed presentation of the IT environment

SecureTrack is a complete solution for keeping an eye on and changing rules on linked devices. Different virtualized devices can be added and tracked in a lab environment. These include devices that emulate Cisco, f5, Fortinet, Forcepoint, Azure, Amazon Web Services (AWS), Checkpoint, Netfilter, Openstack, Palo Alto, Juniper Networks, and Zscaler. It's crucial to understand that these gadgets are lab simulations and do not correspond to real-world physical objects. Even though they are virtual, they are equipped with purposeful rules categorized into groups like clean up, audit, highly permissive and critical violation rules. SecureTrack's user interface provides graphical depictions to aid in observation, inference, and required adjustments in accordance with particular specifications [17].

On the other hand Akamai Guardicore utilizes SaaS management, but on-premises management options are also available. The infrastructure can be built in on-premises data centers, public cloud or branch sites. Aggregators and collectors are used to collect information and coordinate with SaaS management points. Aggregated information is presented via the GUI of Guardicore to provide easy monitoring and management. Then the assets that are seen by Guardicore can be labeled to implement segmentation and to provide more security.

The objective is to provide integration of Guardicore to the Tufin network environment and with this way gather modification information periodically and automatically which is then to be used by Tufin. This integration is executed via developing an extensive script which uses API calls to obtain information from Guardicore, followed by selecting, editing and parsing phases to make this information processable and meaningful from the perspective of Tufin.

The research methodology employed in this study involves a hands-on approach gained through half a year-long internship, focusing on Automated Firewall Rule Management (AFRM) and Integration with Micro-Segmentation Tool for Network Security. The methodology integrates practical experiences with Tufin which is an automated firewall rule management tool and Akamai Guardicore that is a micro-segmentation tool.

The integration of Tufin and Guardicore was the key aspect of this research. This process involved the seamless interaction between the automated firewall rule management capabilities of Tufin and the network discovery followed by segmentation labeling functionalities of Guardicore. Specifically, the integration focused on the acquisition of assets and the related data from Guardicore and parsing this information for Tufin especially utilizing correct labeling within the existing Guardicore topology. This chapter will go into more detail about the specifics of this integration, such as the workflow and features that are made possible by it.

The case study was conducted in a licensed virtual LAB environment of Kirey Group. This environment provided a dynamic and an approximate real-world setting to assess the efficiency of the automated processes, acting as a testing ground for the integration of Tufin and Guardicore. The LAB environment comprises a web server to access Tufin, Tufin Server, and Guardicore, that provides a useful framework for evaluating the effects of network visibility, segmentation and automated firewall rule management.

The collection of data processes for this research includes a combination of both practical implementation and code development. The lab environment helped to create foundations then extra test machines were added and removed if necessary. The key tools that are used can be listed as I mentioned before: Tufin Orchestration Tool and Akamai Guardicore Segmentation Tool. The data collection process encompassed the accessing to Guardicore interface followed by extraction and acquisition of real-time data.

Data privacy and ethical issues are critical because of the sensitive nature of the activities carried out during the internship at Kirey Group. The results and sample code are only presented in a way that complies with the ownership and confidentiality policies of the company. The ethical parts will be covered in detail in this section, emphasizing the importance of protecting proprietary information and respecting data privacy throughout the research process.

4

Case Study

Nowadays, since the technology and innovations are improving rapidly, threats and malwares are following this trend too. There are unknown and new-born threats everyday, along with adversarial hackers. This kind of an atmosphere forces us to build a strong infrastructure and efficiently working security lines to be able to provide CIA which are crucial concepts of information security known as confidentiality, integrity and availability. The system always has to be able to produce and continue to work in any scenario, while providing the secrecy of internal information. In this case, it is inevitable that using only one vendor or one device to protect the entire of a wide network because each vendor has different strong sides or better economic tradeoffs with performance.

This study aims to connect two different tools that are Tufin Orchestration Tool and Akamai Guardicore Segmentation Tool by providing real-time data transmission from one to another. This integration splitted into two different main scripts to connect API's. First one is mainly designed to receive information from Akamai Guardicore Segmentation and the second one's main purpose is to integrate this collected data to Tufin atmosphere properly. Due to company's I will proceed by explaining what the pieces of code do as much as possible, but since it is not possible or ethical to share the code due to the company's privacy policy, I will explain it as much as possible with qualitative expressions regarding the purpose of the work done and the benefits it provides.

Guardicore API's connection

The code is written in Python and the script serves the purpose of interacting with the Guardicore API to authenticate, retrieve, and process information related to assets, labels, saved maps and visibility graphs (flows). These API connections are obtained from Akamai Guardicore Segmentation's original lab environment which was provided with the initiatives of Kirey-Group.

During the development and test processes Postman is used for a shortcut to try if API calls are working. Then the script is developed by using different IDE's Pycharm and VSCode. The script follows a structured sequence of steps to achieve its objectives.

Acquired payloads are taken with the json format to be able to better visualize and process later. The primary information that is obtained has been synced to the dictionary type that is described manually because the information was in a wide range on the first step then I had to strain it to acquire the perfect form that is proper for later processes and usage. Then the recreated data is written to the related csv file by using for loops.

Authentication:

The script begins by establishing a secure connection to the Guardicore API endpoint (https://lab4-a.td.guardicore.com) and authenticating using a provided username and password. The obtained access token is crucial for subsequent API requests, ensuring secure and authorized access to Guardicore resources.

Fetching Asset Information:

After successful authentication, the script sends a GET request to retrieve information about assets. These assets likely represent network entities such as hosts and virtual machines. The retrieved asset details, including identifiers, names, and network interface information, are then processed and stored in a CSV file named output.csv.

Fetching Label Information:

A subsequent GET request is made to obtain information about labels. Labels in Guardicore typically categorize or tag assets based on certain criteria, aiding in organizing and managing network entities. The script retrieves label information and uses them for further processing for this dataset.

Fetching Saved Maps:

The script continues by sending another GET request to retrieve information about saved maps. Saved maps in Guardicore represent predefined visualizations or configurations of the network. The script extracts the UUID of the first saved map for future reference.

Fetching Visibility Graph (Flows) Information:

A subsequent step involves sending a POST request to fetch information about visibility graphs, commonly referred to as flows. These flows represent network connections or traffic between different entities. The script specifies a time range and other parameters in the payload for this request. The obtained flow information, including details like source and destination IP addresses, protocol, ports, group names, and asset names, is then processed.

To conclude, the script serves as an automation tool for accessing and extracting valuable information from the Guardicore API. It performs authentication, retrieves and processes data related to assets, labels, saved maps, and flows, and organizes this information into CSV files for further analysis or reporting purposes. The structured approach of the script ensures systematic data handling and enhances the efficiency of security or network management workflows. Thus, contributes to overall cybersecurity posture and automatization.

The outstanding benefits and contributions can be given as;

Organization Benefits: The script enhances organizational efficiency and data management by automating interactions with the Guardicore API. Automation streamlines repetitive tasks, reducing manual errors and saving valuable time. By extracting and organizing asset, label, map, and flow data into CSV files, the script facilitates comprehensive network analysis. This organized data can be leveraged for strategic decision-making, resource optimization, and overall network governance. Moreover, the script's ability to process and store information in a structured manner contributes to better data hygiene, aiding in compliance with organizational data management standards.

Contribution to Security: The code significantly contributes to security by enabling controlled access to Guardicore resources through secure authentication. It ensures that only authorized users with valid credentials can interact with the API, mitigating the risk of unauthorized access. By fetching information about assets and flows, the script provides valuable insights into the network's topology and current traffic patterns. This visibility aids security teams in identifying potential security threats, anomalies, or malicious activities. The automated extraction of flow details allows for the proactive monitoring of network connections, enhancing the organization's overall security posture.

Contribution to Visibility: One of the primary contributions of the script is to enhance visibility into the Guardicore-protected network. By retrieving and processing information about assets, labels, and flows, the script creates organized datasets that offer a comprehensive view of the network's structure and dynamics. Visibility into labeled assets and their relationships allows network administrators to categorize and understand different segments of the network. Additionally, the extraction of flow information contributes to real-time visibility into network traffic patterns, aiding in the identification of communication trends, potential bottlenecks, or unexpected deviations from normal behavior.

Contribution to Automation and Orchestration: The script plays a pivotal role in advancing automation and orchestration within the organization. Through the automation of API interactions, it reduces the manual effort required for data retrieval and processing. This automation ensures consistency and repeatability in tasks, fostering a more reliable and predictable network management environment. Moreover, by extracting information about saved maps, the script sets the stage for potential orchestration scenarios. The UUID of saved maps can be used as a reference for automated configuration adjustments or for triggering orchestrated responses based on specific network conditions. This aligns with the broader industry trend towards automating routine tasks and orchestrating complex workflows to enhance operational efficiency.

Tufin integration

This part of the code provides the integration with Tufin. It is written in Python. It is a longer and more complex code compared to the Guardicore data acquisition part.

Let's break down the key components of the code;

Configuration File and Setup:

The script reads configuration settings from a file. In this scenario, the configuration file includes parameters specific to Tufin, such as Tufin API endpoints, authentication credentials and other relevant details.

The script uses the configparser library to read configuration parameters from a file. These parameters include a username, password, and the URL of the security application's API. Importing Libraries:

The script imports several Python libraries, including pandas, os, requests, urllib3, json, datetime, time, zlib, sys, csv, pathlib, configparser, and IPNetwork. These libraries are used for handling data, making HTTP requests, working with dates, and managing configurations.

Disabling SSL Warnings:

The code disables SSL warnings related to insecure requests using the urllib3 library. This helps while dealing with self-signed certificates during development or testing, it can pose a significant security risk in a production environment.

Disabling SSL warnings should be approached with caution, and it should only be done after thoroughly assessing the security implications and ensuring that it is done for legitimate reasons.

Network Object and Application Definitions:

The script defines structures (network-object, application, application-interfaces, connection) that seem to represent different elements within the network security application. These elements include network objects, applications, application interfaces, and connections.

Service Handling:

The script retrieves existing assets,flows from the Akamai Guardicore Segmentation application using the API endpoint. It then iterates through the services specified in the CSV file and checks if each component already exists.

Payload Handling:

A function is used to construct a JSON payload for creating or updating a component. It includes details such as device name, type, port, relevant labels and ip addresses.

IP Address and Netmask Handling:

The IPNetwork library is imported to handle IP addresses and netmasks. The netmask-list dictionary maps subnet sizes to their corresponding netmasks.

Connection Handling:

The part of the script that deals with creating and updating connections would be adapted to Tufin's terminology and API structure. Tufin has its own way of representing connections and policies, so the script interacts with the Tufin API accordingly.

The script defines two dictionaries, connection-source and connection-destination, to store information about source and destination connections, respectively. The script updates connection information by making PUT requests to the corresponding API endpoints for source and destination connections. It uses the connection id obtained earlier to construct the URLs for updating source and destination connections.

Error Logging and Exception Handling:

The script contains a try-except block to catch any errors that may occur during the execution of the main logic. If an error occurs, it prints an error message and logs the error details.

The log-errors function is used to log errors by appending them to a CSV file (errors.csv). It logs information about lines in the CSV file that were not processed successfully.

Logging errors in a security context offers crucial benefits by aiding in the rapid identification and resolution of issues within an application, facilitating debugging and troubleshooting. Moreover, error logs serve as an early detection mechanism for potential security incidents, providing a trail of events for forensic analysis in the case of breaches. Compliance with industry regulations is reinforced through comprehensive logging practices and continuous monitoring of error logs enables proactive identification of abnormal patterns or potential security threats. By addressing recurring issues and patterns revealed in error logs, organizations can enhance their overall security posture, ensuring a robust and resilient system against potential vulnerabilities and threats.

Main Execution:

The main function serves as the entry point for the script. It reads a CSV file containing assets, iterates through each line, and performs various actions based on the information in each line.

The main tasks include creating or checking the existence of assets, application interfaces, and network objects. It also handles the creation of interface connections and logs errors for duplicate entries.All the details are tailored to the specific requirements and API structures of Guardicore and Tufin.

The script significantly contributes to network security by providing automatization. By creating and updating applications, interfaces, services and connections based on information from a CSV file, the script ensures consistent and error-free application of security policies. This automation aligns with best practices for reducing the risk of misconfigurations, enhancing overall network security.

Furthermore, the script plays a crucial role in the integration with Guardicore, a security solution known for its micro-segmentation capabilities. This integration allows for seamless communication with Guardicore's features, contributing to a more robust security posture. The script's emphasis on error handling and logging provides visibility into potential issues, enabling administrators to promptly address security concerns.

From an automation and management perspective, the script significantly streamlines the deployment of security policies. By automating the configuration of applications, interfaces, and services, it reduces manual intervention and minimizes the likelihood of human error. This not only enhances operational efficiency but also ensures a consistent and standardized application of security policies across different components of the network.

In terms of visibility and monitoring, the script logs errors encountered during execution, offering a valuable tool for monitoring and troubleshooting. The parsing of information from a CSV file further contributes to visibility into the current state of the network. The dynamic construction of JSON payloads based on the parsed data enables the script to adapt to varying configurations, providing administrators with a comprehensive view of network changes introduced through automation.

The script's use of dictionaries for data representation and manipulation enhances its flexibility and efficiency. Dictionaries are employed to represent applications, interfaces, services, and connections, allowing for dynamic and structured processing of data. This approach contributes to the script's adaptability to diverse network configurations specified in the input data, supporting its role in network automation and security management.

5
Discussion

In the ever-evolving landscape of cybersecurity, the imperative to fortify network defenses has led to the exploration of innovative solutions and integrations. As a master's student in science, my thesis endeavors to address this imperative through a comprehensive investigation and integration of two prominent security tools: Tufin, a firewall orchestration tool, and Akamai Guardicore, a micro-segmentation solution. The title of my thesis, "Enhancing Cybersecurity Posture through Integration of Firewall Management and Micro-Segmentation Tools," encapsulates the essence of this research. This internship-combined thesis delves into the intricacies of seamlessly merging the capabilities of these distinct tools, aiming to achieve a symbiotic relationship that enhances real-time visibility, monitoring, and overall security efficacy.

Achievements and Challenges

The primary achievements include the establishment of seamless communication between Tufin and Guardicore, facilitating real-time data synchronization from Guardicore to Tufin. This integration aims to enhance the overall cybersecurity posture by combining the strengths of both tools.

Key actions taken during the project involved the development of a script for extracting relevant data and assets from the Guardicore environment. This ensured that only pertinent information was transferred to Tufin for analysis and orchestration. Additionally, a robust system was implemented to update Tufin's database in real-time, reflecting the latest threat intelligence and network changes detected by Guardicore.

An emphasis was placed on optimizing the integration script to enhance efficiency and minimize both latency and accuracy in data transfer. This was crucial to prevent introducing bottlenecks or performance issues during the integration process.

The most significant challenge encountered was determining the criteria for selecting relevant data from Guardicore. Striking the right balance between comprehensive visibility and avoiding information overload required careful consideration. Additionally, ensuring seamless integration between Tufin and Guardicore, given their different purposes in the security domain, posed challenges related to data formats, protocols, and APIs. Addressing potential security risks, such as unauthorized access or data leaks, demanded a thorough security assessment and the implementation of appropriate safeguards.

The successful integration of Tufin and Guardicore validates the hypothesis that it is indeed possible to integrate security tools with distinct purposes, creating a more holistic cybersecurity solution. The efficiency and meaningfulness of the integration were demonstrated through the contributions of both tools to solid visibility and monitoring. Leveraging Tufin's orchestration capabilities and Guardicore's micro-segmentation, the combined solution enhances overall security by effectively managing access and mitigating potential threats. The integration underscores the valuable contributions of automation and segmentation in strengthening an organization's cybersecurity defenses.

Subjects experienced in depth

First of all a deep understanding of automatization and orchestration concepts in the realm of cybersecurity was acquired. The significance of automating repetitive tasks and orchestrating various security processes was explored. This knowledge proved crucial in developing an integration script that facilitated seamless communication between Tufin and Guardicore, contributing to the efficient and streamlined management of firewall policies and micro-segmentation configurations.

The integration project provided a comprehensive understanding on the concepts of segmentation and micro-segmentation. Understanding the principles of dividing networks into distinct segments and the finer-grained control offered by micro-segmentation was essential. This knowledge formed the basis for leveraging Guardicore's micro-segmentation capabilities to enhance the precision and adaptability of security policies, creating a more robust defense against potential threats.

Topology emerged as a critical aspect of the learning process, emphasizing the importance of understanding the structure and interconnections within a network. The project underscored how the topology of a network influences the effectiveness of security measures. Consideration of network topology followed by a clear understanding was crucial in ensuring that the integration between Tufin and Guardicore was tailored to the specific structure and requirements of the organization, leading to a more context-aware and efficient cybersecurity solution.

Data collection methodologies were a key focus to create a clear starting point, particularly in the context of gathering relevant information from the Guardicore environment. The process involved identifying and extracting pertinent data and assets while maintaining a balance to prevent information overload. This learning was pivotal in crafting a data collection strategy that ensured only essential information was transferred to Tufin for real-time analysis, aligning security measures with the dynamic nature of the network.

Understanding API connections and proficiently navigating data sources were fundamental skills developed during the development process. The integration script relied on effective API connections between Tufin and Guardicore to enable seamless communication. Additionally, the project required careful consideration of the data to be chosen for transfer, striking a balance between comprehensive visibility and avoiding unnecessary information. This knowledge was crucial in ensuring the integration was both efficient and meaningful, contributing to the overall success of the cybersecurity enhancement initiative.

Future Work

From a scientific perspective, future work in the area of cybersecurity integration could involve the development of similar tools tailored to achieve integrations with a diverse array of security tools. Extending the success achieved in integrating Tufin and Guardicore, the creation of tools adaptable to different security environments and purposes would significantly contribute to the field. By understanding the underlying principles of integration and employing standardized methodologies, these tools could streamline the process of incorporating new security solutions into existing infrastructures. This approach not only enhances the scalability of cybersecurity integrations but also fosters a more cohesive and interoperable security ecosystem.

A promising avenue for future research involves the refinement of integration tools to simplify the data selection process. Designing an integration tool that intelligently assesses and selects data, based on the unique characteristics of both the source and target tools could alleviate a major challenge faced during the integration process. This entails developing algorithms or machine learning models that understand the context of the data within the source tool and the requirements of the target tool, optimizing the efficiency of information transfer. Such enhancements would contribute to making integrations more adaptive, reducing the manual effort required for data selection and ensuring that only the most relevant information is exchanged.

A prospective direction in cybersecurity research involves investigating the feasibility and efficiency of unified security solutions that encompass a wide range of functionalities. While such comprehensive platforms could potentially obviate the need for integration, it's crucial to consider the associated costs and performance implications. Developing a singular tool that provides all security functions might be financially burdensome and might not be as efficient as a specialized tool for each function. Future work could delve into optimizing unified solutions, striking a balance between cost-effectiveness and performance, ensuring that organizations can achieve robust cybersecurity without compromising efficiency or breaking the bank. This approach would require a nuanced evaluation of the trade-offs associated with centralized versus integrated security architectures.

References

[1] M. A. M. B. A. M. Ashraf, A. Zahra and S. Zafar, *Ethical Hacking Methodologies: A Comparative Analysis*. Mohammad Ali Jinnah University International Conference on Computing (MAJICC), Karachi, Pakistan, 2021, pp. 1-5, 2021.

[2] M. B. A. R. S. Patil, A. Jangra and P. Kulkarni, *Ethical hacking: The need for cyber security*. IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 2017, pp. 1602-1606, 2017.

[3] J. Y. W. Jiang and Y. Tan, *Research of Cybersecurity Measures for Data Governance*. International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballar, India, 2023, pp. 1-6, 2023.

[4] A. Q. A. Al-Far and S. Almajali, *Measuring Impact Score on Confidentiality, Integrity, and Availability Using Code Metrics*. International Arab Conference on Information Technology (ACIT), Werdanye, Lebanon, 2018, pp. 1-9, 2018.

[5] S. S. D. Naidu and V. Murarka, *Network Security Tools for Rapid Inspection*. 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2023, pp. 1-5, 2023.

[6] P. Keshavamurthy and S. Kulkarni, *Early Detection of Reconnaissance Attacks on IoT Devices by Analyzing Performance and Traffic Characteristics*. IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 2023, pp. 187-193, 2023.

[7] L. Liu, *Discussion and Practice of Computer Network Information and Network Security Protection Strategy*. 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Harbin, China, 2020, pp. 1810-1813, 2020.

[8] F. Jaidi, *FW-TR: Towards a novel generation of firewalls based on trust-risk assessment of filtering rules and policies, in Proc.15th Int. Wireless Commun. Mobile Comput. Conf., 2019, pp. 1043–1048.*, 2019. [Online]. Available: https://www.researchgate.

net/publication/334632947_FW-TR_Towards_a_Novel_Generation_of_Firewalls_Based_on_Trust-Risk_Assessment_of_Filtering_Rules_and_Policies

[9] S. d. Krit and E. Haimoud, *Overview of firewalls: Types and policies: Managing windows embedded firewall programmatically*. International Conference on Engineering MIS (ICEMIS), Monastir, Tunisia, 2017, pp. 1-7, 2017.

[10] J. Liang and Y. Kim, *Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall*. IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2022, pp. 0752-0759, 2022.

[11] H. Zimmermann, *OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection*. IEEE Transactions on Communications, vol. 28, no. 4, pp. 425-432, April 1980.

[12] C. C. C. Togay, A. Kasif and B. Tekinerdogan, *A Firewall Policy Anomaly Detection Framework for Reliable Network Security*. IEEE Transactions on Reliability, vol. 71, no. 1, pp. 339-347, March 2022.

[13] A. T. R. Vast, S. Sawant and V. Badgujar, *Artificial Intelligence based Security Orchestration, Automation and Response System*. 6th International Conference for Convergence in Technology (I2CT), Maharashtra, India, 2021, pp. 1-5, 2021.

[14] A. C. Risdianto and E. C. Chang, *OctoBot: Human Activity Orchestration System for Cybersecurity Experiment and Exercise*. International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2020, pp. 22-28, 2020.

[15] A. Malviya and R. K. Dwivedi, *A Comparative Analysis of Container Orchestration Tools in Cloud Computing*. 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2022, pp. 698-703, 2022.

[16] H. S. Yoo and W. E. S. Yu, *Building a QoS Testing Framework for Simulating Real-World Network Topologies in a Software-defined Networking Environment*. International Conference on Engineering and Emerging Technologies (ICEET), Kuala Lumpur, Malaysia, 2022, pp. 1-6, 2022.

[17] Tufin, *Tufin*, Online. [Online]. Available: https://www.tufin.com/

[18] M. A. K. N. Basta, M. Ikram and A. Walker, *Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework*. NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 2022, pp. 1-7, 2022.

[19] L. S. Cruz and I. E. Fonseca, *Industrial Control Systems in Environments with Zero Trust Architecture: Analysis of Responses to Various Attack Types*. Workshop on Communication Networks and Power Systems (WCNPS), Brasilia, Brazil, 2023, pp. 1-7, 2023.

[20] Guardicore, *Akamai Guardicore Segmentation*, Online. [Online]. Available: https://www.akamai.com/

[21] 6sense, *6sense*, Online. [Online]. Available: https://6sense.com/tech/network-security/guardicore-market-share

[22] Gartner, *Gartner*, Online. [Online]. Available: https://www.gartner.com/reviews/market/network-automation-platforms

Acknowledgments

In the beginning of my Bachelor's degree, if anyone told me that I would study cybersecurity for a masters degree abroad and in Italy, I would not believe it because this scenario wasn't something that I ever thought about. But luckily, my research about Italy started thanks to my aunt. She saw an Italy shape on my cup after a Turkish coffee. Now, here I am, graduating from the Master's degree.

I would like to thank my family who raised me and supported me a lot. I always felt the love coming from them. The support I felt, was precious to me.

Thank you Università degli Studi di Padova for providing this education including the scholarship opportunity for us and for the guidance that came from all of my dear instructors during whole degree. Especially thank you to my advisors with the thesis Prof. Alessandro Brighente and Prof. Mauro Conti.

Also my dear cousin Utku Tahan. He is brother to me, thanks to his guidance I progressed a lot. I want to thank my friends for having shared joyful and memorable days. Lastly, special thanks to my dear friend, deskmate and colleague Muhammed Emir Uysal.