Securing Networks with ELK Stack

Building zero trust network defense

Ram Patel

www.bpbonline.com

First Edition 2024

ISBN: 978-93-55519-542

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Dedicated to

To my parents, ***Vinodbhai*** *and* ***Shashikalaben****, the foundation of my world; to* ***Jemini****, my partner in life's voyage; to my sons,* ***Panth*** *and* ***Dev****, who are the source of endless pride and joy; and to my extended family, the warm embrace that enriches my life.*

To my mentors, ***Sanjay****,* ***Joe****,* ***Bijay****,* ***Omri****,* ***Rob****,* ***Neil, Li*** *and others— Whose mentorship has meticulously carved the path of my professional journey.*

About the Author

Ram Patel stands at the forefront of network architecture innovation at Intel, a leading Fortune 500 company, where he has amassed over 16 years of experience in the networking and network security field. Ram has consistently expanded his expertise to stay ahead of the technological curve with Software Defined Networking, Zero Trust Network, IoT/Private 5G, in addition to traditional networking fields such as enterprise, datacenter, and manufacturing local area network.

His professional interests and work are deeply rooted in network and network security, with a particular focus on network security, resiliency, efficiency, and observability. Ram is dedicated to solving business challenges and making a positive impact on his organization. His commitment to innovation is highlighted by his pioneering use of automation, software-defined networking, and the observability platform ELK to enhance network and network security observability. This forward-thinking approach has not only optimized his company's infrastructure but has also influenced vendor product features and roadmaps.

As a thought leader, Ram has co-authored influential papers on emerging networking topics, showcasing his profound understanding and foresight in the field. His contributions have been instrumental in shaping the future of network architecture, making him a key player in the evolution of network and security practices. He holds a Bachelor's degree in Electronics and Communication Engineering and various industry certifications in networking.

About the Reviewers

- **Poonam Agarwal** is a passionate DevOps practitioner with extensive professional experience in observability tools - ELK stack, Prometheus, and Splunk. She has exceptional skills in Container technologies, Configuration management, and infrastructure provisioning. Additionally, she works globally as a DevOps corporate trainer and coaches hundreds and thousands of students.

  She loves communicating with customers and stakeholders, providing tailored solutions to complex issues.

  She is currently working as an independent DevOps Consultant and DevOps Coach.

- As an accomplished information system engineer at Consultadd, **Akash** expertly manages and implements Elasticsearch, Logstash, and Kibana (ELK) technologies to enhance enterprise data management and analytics. With technical acumen, Akash develops scalable Elasticsearch solutions for effective data indexing and creates complex data pipelines using Logstash for smooth integration. Additionally, Akash leverages Kibana to craft intuitive data visualizations that aid in real-time business intelligence and decision-making. Esteemed clients like Quizlet, Morgan Stanley, and Apple value Akash's ability to turn complex data into actionable insights. Currently pursuing a master's in information systems at the State University of New York, Akash stays at the forefront of industry advancements, ensuring that technology implementations deliver long-term value.

Acknowledgement

I would like to extend my sincere gratitude to everyone who contributed to the completion of this book.

First and foremost, I extend my heartfelt appreciation to my family, mentors, colleagues, and friends for their unwavering support and encouragement throughout this journey. Their love and encouragement have been a constant source of motivation.

I am immensely grateful to BPB Publications for their guidance and expertise in bringing this book to fruition. Their support and assistance were invaluable in navigating the complexities of the publishing process.

I would also like to acknowledge the reviewers, technical experts, and editors who provided valuable feedback and contributed to the refinement of this manuscript. Their insights and suggestions have significantly enhanced the quality of the book.

Last but not least, I want to express our gratitude to the readers who have shown interest in our book. Your support and encouragement have been deeply appreciated.

Thank you to everyone who has played a part in making this book a reality.

Preface

In an era where cybersecurity threats are ever-evolving and increasingly sophisticated, the need for robust, adaptive security frameworks has never been more critical. This book, "Securing Networks with ELK Stack" aims to equip readers with a comprehensive understanding of these pivotal technologies and their applications in modern network security.

Our journey begins with an in-depth exploration of **zero trust network architecture** (**ZTNA**). As traditional perimeter-based security models become obsolete, ZTNA emerges as a fundamental paradigm shift. We will delve into the foundational principles of zero trust, emphasizing the importance of verifying every access attempt, regardless of its origin, and adopting a posture of never trust, always verify. This section outlines practical deployment strategies and provides insights into overcoming common challenges associated with implementing ZTNA in various organizational contexts.

Next, we transition to the ELK Stack—a powerful trio consisting of Elasticsearch, Logstash, and Kibana. These open-source tools collectively form a robust platform for searching, analyzing, and visualizing log data in real-time. We guide readers through the essentials of setting up and configuring the ELK Stack, illustrating how it can be leveraged to gain deep visibility into system operations, detect anomalies, and enhance overall security posture.

The final section of this book is dedicated to Elastic Security, an extension of the ELK Stack tailored specifically for security analytics and threat detection. We discuss the integration of Elastic Security into existing infrastructure, its capabilities in identifying and mitigating threats, and the benefits of leveraging Machine Learning for advanced threat detection. Real-world case studies provide practical examples of how organizations have successfully implemented Elastic Security to protect their digital assets.

Throughout this book, our goal is to bridge the gap between theoretical concepts and practical application. Whether you are a network/security professional seeking to enhance your knowledge, a network/security architect looking to implement these technologies, or an enthusiast eager to understand the cutting-edge developments in network security, this book offers valuable insights and actionable guidance.

We hope that by providing a thorough examination of zero trust network architecture, the ELK Stack, and Elastic Security, this book will serve as a vital resource in your journey toward creating a secure, resilient, and future-ready cybersecurity environment.

Chapter 1: Introduction to Zero Trust Network Architecture– This chapter introduces the fundamental concepts of **zero trust network architecture** (**ZTNA**). It covers the relevance of zero trust today, the principles and framework of ZTNA, and its key components. The chapter also explores the numerous benefits of ZTNA, such as enhanced security, improved data protection, and simplified compliance, while concluding with key points and questions to reinforce your understanding.

Chapter 2: Zero Trust Network Architecture: Design and Deployment Strategies– Focusing on the practical aspects of ZTNA, this chapter discusses design principles, policy governance, and the essential components like Policy Decision Point and Policy Enforcement Point. It also delves into deployment strategies, including network segmentation and application security, offering insights into enterprise deployment and best practices.

Chapter 3: Zero Trust Network Architecture: Data Gathering Strategies– This chapter highlights the importance of data gathering in ZTNA, detailing the types of data to be collected and the methods and tools for data collection. It covers endpoint data, security event logs, and threat intelligence, along with techniques for data analysis and the integration of behavioral analytics, ensuring data privacy and security throughout the process.

Chapter 4: Overview of ELK Stack and its Capabilities– An introduction to the ELK Stack (Elasticsearch, Logstash, and Kibana) and its capabilities, this chapter explores the features of each component, including full-text search, Machine Learning, data enrichment, and visualization. It provides an overview of the benefits of using the ELK Stack for comprehensive data analysis and monitoring.

Chapter 5: Design of ELK Stack Components– This chapter discusses the architectural considerations for deploying the ELK Stack, focusing on scalability, high availability, security, and network integration. It covers various deployment strategies, from single node to cloud-based setups, and offers best practices for benchmarking and optimizing your ELK Stack deployment.

Chapter 6: Data Ingestion with ELK– Covering the critical aspect of data ingestion, this chapter explains the importance of aggregating data sources and maintaining data quality. It includes detailed instructions for using Logstash and Beats for data collection, processing, and enrichment, with practical configuration examples and solutions for real-time and historical data analysis.

Chapter 7: Data Visualization with ELK– This chapter emphasizes the importance of data visualization in network security and how Kibana can be used to create meaningful

visualizations. It covers the selection of data sources, advanced visualization techniques, and the use of tools like the Time Series Visual Builder and Vega for in-depth data analysis.

Chapter 8: Effective Dashboards with Kibana– Focusing on the creation and customization of Kibana dashboards, this chapter explains how to tailor dashboards to specific needs, utilize filters and queries, and share or embed dashboards. It provides practical examples and advanced KQL queries to enhance the usability and functionality of your dashboards.

Chapter 9: Unlocking Insights: ELK's Machine Learning Capabilities– This chapter explores the Machine Learning capabilities of the Elastic Stack, including anomaly detection, root cause analysis, and natural language processing. It discusses how to integrate these features with other Elastic Stack components to establish effective alerting and notification systems for proactive security management.

Chapter 10: Introduction to Elastic Security– Introducing Elastic Security, this chapter covers its components like Elastic SIEM, endpoint security, and security analytics. It explains the integration with other security tools and practical applications such as threat hunting and XDR to enhance your organization's security posture.

Chapter 11: Threat Detection and Prevention– This chapter provides a comprehensive approach to threat detection and prevention, discussing various types of security threats and the integration of Machine Learning and rule-based detection techniques. It includes real-world examples and practical applications for identifying and mitigating different types of attacks.

Chapter 12: Incident Response and Investigation– Focusing on incident response capabilities, this chapter outlines the process of incident investigation using Elastic Security. It provides real-world examples of detecting malware, insider threats, data exfiltration, and more, along with best practices and considerations for effective incident response.

Chapter 13: Compliance and Reporting– The final chapter emphasizes the importance of compliance and reporting in cybersecurity. It covers various compliance frameworks and how to use Elastic Security for compliance data collection and reporting. Practical use cases include regulatory compliance, device compliance, and log audit trails, providing a comprehensive guide to maintaining and demonstrating compliance.

Chapter 14: Introduction to Zeek– This chapter provides an introduction to Zeek, detailing its operation, evolution, and its crucial role in network security. It covers the structure of Zeek deployments, including installation and cluster setup, and explores Zeek's data model and logging capabilities. The chapter also discusses Zeek's integration with various security tools and platforms, highlighting its adaptability and extensibility, and concludes with future directions for Zeek.

Chapter 15: Zeek Data Collection and Analysis– Focusing on Zeek's data collection capabilities, this chapter explains how to configure Zeek to capture specific network data types, including packet capture, protocol parsing, and content extraction. It discusses built-in analysis tools for identifying network threats and the integration of threat intelligence. The chapter also covers best practices for using Zeek in network data collection and analysis, ensuring efficient and effective network monitoring.

Chapter 16: Unlocking Synergies: Zeek and Elastic Security Integration in Action– Zeek and Elastic Security Integration in Action: This chapter explores the integration of Zeek with Elastic Security, demonstrating the practical applications of this synergy in threat hunting, incident response, and network monitoring. It delves into data correlation techniques, enriching Zeek data with external sources, and optimizing the deployment of both tools. Real-world success stories from various industries illustrate the effectiveness of this integration.

Chapter 17: Future Directions for Elastic Security– This chapter examines the future of Elastic Security, highlighting the latest trends and challenges in network security. It discusses the role of Elastic Security in the era of cloud and IoT, its integration with AI for enhanced security operations, and safeguarding AI ecosystems. The chapter includes case studies and best practices for continuous learning, enhanced monitoring, and cultivating a culture of cybersecurity awareness.

Chapter 18: A Unified Recap: Safeguarding Networks with ELK– The final chapter provides a comprehensive recap of the key takeaways from the book. It revisits the foundational concepts of zero trust network architecture, the design and deployment of ELK Stack components, data ingestion and visualization with ELK, the capabilities of Elastic Security, and the integration of Zeek. The chapter concludes with next steps for readers to continue advancing their network security knowledge and practices.

By covering these topics in depth, this book aims to be an essential resource for security professionals, system administrators, and anyone interested in modern network security. We hope it equips you with the knowledge and tools to implement and leverage zero trust network architecture, the ELK Stack, and Elastic Security effectively.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/9ufznne

The code bundle for the book is also hosted on GitHub at
https://github.com/bpbpublications/Securing-Networks-with-ELK-Stack.
In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
Introduction to Zero Trust Network Architecture

Introduction

Today's rapidly evolving cybersecurity landscape, traditional network security models that relying on perimeter defenses are no longer sufficient to protect organizations against sophisticated cyber threats. The concept of zero trust network has emerged as a promising approach to address the limitations of traditional security models. This chapter introduces the fundamental principles of zero trust networks and explores their significance in securing modern networks. Refer to the following figure:

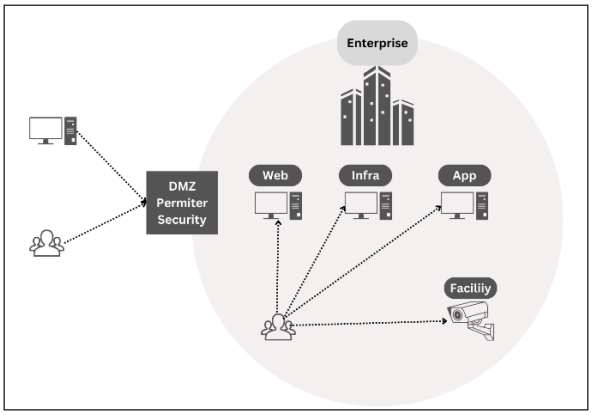

Figure 1.1: *Legacy network security model*

Legacy network security architectures often face several drawbacks, leading to increased vulnerability and challenges in addressing modern cybersecurity threats. Some common drawbacks include:

- **Perimeter-centric focus:** Legacy security relies heavily on perimeter defenses, assuming that once inside the network, everything is trustworthy. In today's dynamic and distributed environments, this approach is no longer sufficient, as threats can originate from both external and internal sources.
- **Static access controls:** Traditional security models often use static access controls, assigning fixed permissions to users based on their roles. This can lead to over-permission or under-permission, making it difficult to adapt to changing user roles or requirements.
- **Complexity and maintenance:** Legacy security solutions tend to be complex, with numerous point solutions for different security needs. This complexity makes it challenging to manage and maintain, increasing the likelihood of misconfigurations and vulnerabilities.
- **Limited visibility:** Legacy architectures may lack comprehensive visibility into network traffic and user activities. This makes it difficult to detect and respond to advanced threats or anomalies in real-time.
- **Inability to adapt to cloud environments:** As organizations increasingly move to cloud-based infrastructures, traditional security models struggle to adapt. Legacy solutions may not effectively secure cloud-native applications and services.

Structure

The chapter covers following topics:

- Introduction to zero trust
- Relevance of zero trust network architecture today
- Zero trust network architecture framework
- Benefits of zero trust network

Objectives

This chapter provides a comprehensive understanding of zero trust network and its relevance in modern network security. The chapter introduces the key principles and components of the zero trust network architecture framework. It will explain the benefits and advantages of implementing a zero trust approach.

Introduction to zero trust

Zero trust network is an information security framework that challenges the traditional assumption of trust within a network. Unlike the traditional perimeter-based security model, zero trust operates on the principle of *never trust, always verify*. In other words, it assumes that no user or device should be inherently trusted, regardless of their location or previous authentication.

The core idea behind zero trust is to ensure that every user, device, and network resource is continuously authenticated, authorized, and monitored before granting access to sensitive data or resources. This approach eliminates the notion of a trusted internal network and treats every interaction as potentially malicious until proven otherwise.

Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

An analogy that can help understand the concept of zero trust is comparing it to accessing a secured building or facility.

Imagine you want to enter a high-security building. In a traditional security model, you would present your identification card at the entrance, and once you are inside, you are trusted and granted access to all areas within the building. The assumption is that anyone who made it through the entrance is trustworthy.

Now, let us apply the zero trust principle to this scenario. In a zero trust model, even if you have an identification card, you are not automatically trusted upon entering the building. Instead, at each checkpoint and area within the building, you are continuously verified and granted access based on specific permissions and requirements.

Here is a simplified example:

- **Entrance:** Upon arrival at the entrance, you present your identification card and undergo identity verification. However, adhering to the zero-trust model, this initial verification does not automatically grant unrestricted access to the entire building. If the identification card or verification fails, access to the building is denied, ensuring that only authenticated individuals proceed.
- **Checkpoint 1**: Having successfully passed the entrance, you reach Checkpoint 1, where the purpose of your visit is thoroughly validated. Additional information or credentials specific to the area you intend to access are required. If the purpose of your visit is not successfully validated, or if the provided information is insufficient, access beyond this point is denied.
- **Checkpoint 2:** Assuming you have successfully navigated Checkpoint 1 and moved to the floor housing the IT department, you encounter another checkpoint. This checkpoint verifies your authorization to access a particular floor or area. If

the authorization is not valid or if the required access token is not provided, access to the designated floor is denied.

- **IT department access:** Upon passing Checkpoint 2, you gain access to the IT department. However, even within this department, additional restrictions may exist based on your role and the specific resources you need to access. If your role or credentials are not aligned with the required access levels, you may be restricted from entering certain areas within the IT department, ensuring a granular and role-based access control. For instance, certain server rooms or sensitive data repositories may demand additional layers of authentication or approval. If these are not successfully completed, access to these specific resources is denied, maintaining the zero-trust model's emphasis on continuous verification and strict access controls at each stage of the process. The following figure illustrates an example of physical security access:

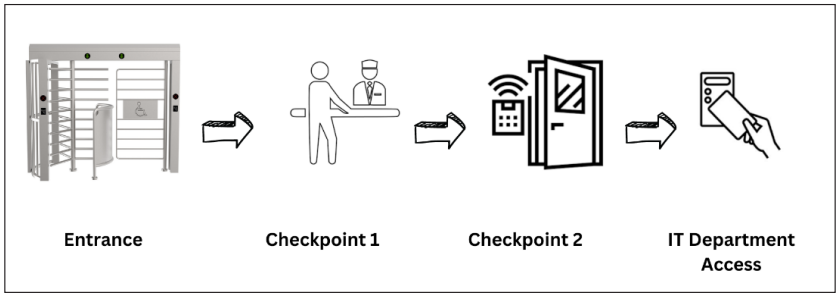

Figure 1.2: *Physical security access*

Throughout this entire process, the zero trust model ensures that you are continuously verified and authorized based on the principle of never trust, always verify. Each checkpoint assesses your identity, purpose, and authorization before granting access to the next level of the building. This approach eliminates the assumption of trust based on initial entry and ensures that access is granted on a need-to-know and least-privilege basis.

The analogy highlights that in a zero trust model, trust is not granted once and is assumed throughout the network or building. Instead, trust is continuously evaluated and verified at multiple checkpoints and based on specific criteria, resulting in a more secure and controlled access environment. The following figure illustrates this process:

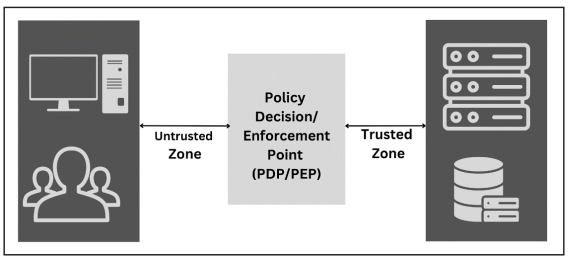

Figure 1.3: *Zero Trust Network Architecture Model*

The figure illustrates the **Zero Trust Network Architecture** (**ZTNA**) framework, highlighting the segregation of network components into different zones based on trust levels. On the left side of the diagram, we have the untrusted zone, where users or devices accessing the network are initially considered untrusted. This zone represents external networks, remote locations, or potentially compromised devices.

In the middle of the figure, we find the **Policy Decision Point** (**PDP**) and **Policy Enforcement Point** (**PEP**). These components form the core of the zero trust model. The PDP evaluates access requests, enforces access policies, and makes dynamic decisions based on user/device identity, security posture, and contextual information. The PEP, positioned between the untrusted and trusted zones, enforces these policies, controlling traffic flow and verifying the authenticity and authorization of requests before granting access to the trusted zone.

Finally, on the right side of the diagram, we have the trusted zone, representing the server infrastructure or protected resources. This zone comprises critical systems, applications, and data that require secure access. Access to resources in the trusted zone is strictly controlled, ensuring that only authorized and authenticated users or devices from the untrusted zone can gain entry based on the policies set by the PDP.

The figure visually represents the key concept of zero trust, which is to assume zero trust in any user, device, or network and continuously verify trust at each stage of the access process. By segmenting the network into different zones and implementing robust access controls and policy enforcement, organizations can establish a secure and resilient architecture that protects critical assets from potential threats originating from untrusted sources.

Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (that is, local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, **Bring Your Own Device** (**BYOD**), and cloud- based assets that are not located within an enterprise-owned network boundary. Zero trust focus on protecting resources (assets, services, workflows, network accounts, and so on.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.

Relevance of zero trust network architecture today

ZTNA is gaining prominence in today's cybersecurity landscape due to several key factors:

- **Evolving perimeter:** Traditional network security models rely heavily on perimeter defenses, assuming that internal networks are inherently trusted. However, the boundaries of modern networks have expanded significantly with the adoption of