The Zen Guide to Routing Security Policy: Towards a Unified and Replicable Government Networks Routing/BGP Security Policy.

November, 2023.

Executive Summary

In an era where digital connectivity is paramount, the security of the Border Gateway Protocol (BGP) is of critical importance. This executive summary provides an overview of the Zen Guide to Routing Security Policy, a comprehensive approach designed to enhance the security and integrity of government network routing infrastructure using BGP.

Key Challenges and Solutions: The guide begins by outlining the unique challenges in securing BGP, a protocol foundational to the Internet's global routing system. The decentralized and interconnected nature of BGP introduces vulnerabilities that can be exploited by malicious actors. The guide emphasizes the need for robust routing security policies, particularly in government networks that are often targets of sophisticated cyber threats. To address these challenges, the Zen Guide proposes a set of best practices and strategies that balance consistency in security posture with the flexibility to adapt to diverse network environments and evolving threats.

The Zen Approach: At its core, the Zen Guide advocates for a harmonious and balanced approach to BGP security. This approach transcends technical measures, integrating mindfulness and simplicity in security practices. It calls for stripping away unnecessary complexities and focusing on essential measures that directly address fundamental vulnerabilities. The guide highlights the importance of simplicity in configurations, minimization of dependencies, and reduction of the attack surface to achieve a more resilient and manageable routing security posture.

Best Practices for BGP Security: The guide details specific best practices, including the adoption of MANRS (Mutually Agreed Norms for Routing Security) principles. These principles empower organizations to proactively shape a secure and resilient routing environment, reducing common threats to routing. The guide also discusses the critical role of collaboration among stakeholders, technical expertise, and policy advocacy in enhancing routing security.

Target Audience and Application: This guide serves as an invaluable resource for policymakers, government agencies, network administrators, and network operators. It offers a comprehensive understanding of the challenges and solutions in BGP security, providing actionable insights for developing and implementing effective routing security policies.

In conclusion, the Zen Guide to Routing Security Policy is a pivotal resource for securing the global routing system. Its holistic approach, combining technical, policy, and philosophical elements, offers a pathway to more secure, resilient, and reliable Internet routing infrastructures, particularly within government networks.

I. Routing Security in Context.

Securing the Border Gateway Protocol (BGP) poses significant challenges due to the complex and interconnected nature of the global routing system. BGP, being the de facto protocol for inter-domain routing, is responsible for exchanging routing information among autonomous systems (ASes) worldwide. However, ensuring the security and integrity of BGP operations is a complex task that requires addressing various challenges [13].

BGP, as the core routing protocol of the Internet, faces numerous challenges in maintaining a secure and resilient infrastructure. The decentralized nature of BGP, coupled with the interconnectedness of networks, introduces vulnerabilities that can be exploited by malicious actors. To overcome these challenges, adhering to best practices becomes crucial. This white paper discusses some of the challenges of BGP security policy and explores potential solutions to mitigate the associated risks.

Governments in today's interconnected world heavily rely on networks for crucial functions and sensitive information exchange. Robust routing security policies are essential to protect against sophisticated cyber threats that exploit vulnerabilities in routing infrastructure. State-sponsored attacks and malicious actors continuously target government networks, prompting policymakers to reassess security measures and develop comprehensive strategies. The proposed Zen guide to routing security policy serves as a valuable resource, providing best practices to fortify routing infrastructure. It offers a holistic approach, encompassing critical security measures such as Resource Public Key Infrastructure (RPKI). Policymakers, government agencies, network administrators and network operators can leverage this guide to proactively address routing security challenges, establish a solid foundation for network security, and play their part in securing the global routing system.

II. The Quest for a Replicable BGP Security Policy and its Challenges.

Developing a replicable BGP security policy that can be effectively implemented across different organizations and network environments presents significant challenges. Government networks, in particular, face additional complexities due to their diverse environments, unique network architectures, and varying security requirements. Government entities differ in size, scope, and operational needs, which directly impact the design and implementation of a BGP security policy. Balancing the need for a consistent security posture while allowing for customization and adaptability adds further complexity to the development process[1],[3],[10],[11].

The challenge lies in creating a policy that accommodates the diverse range of government entities while addressing their specific security concerns. Factors such as organizational size, network architecture complexity, and criticality of services must be carefully considered. Additionally, the policy must be flexible enough to adapt to evolving threat landscapes and changing security requirements without compromising its effectiveness. Successfully overcoming these challenges requires a comprehensive understanding of government networks, collaboration among stakeholders, and a flexible approach to policy development that can be replicated and tailored across different organizations and operational contexts.

Some of the key challenges- While all networks share common challenges, such as those numbered 1 to 10, government networks face additional unique challenges, specifically those listed from 11 to 17:

1. **Complexity:** routing security policies can become complex, especially in large networks with multiple routers and interconnected systems. For example, consider a government agency with a nationwide network infrastructure spanning multiple locations. They may have dozens or even hundreds of routers and interconnected systems that need to be protected. Managing and updating these policies while ensuring they align with network requirements can be challenging.
2. **Lack of Visibility:** in some cases, network administrators may have limited visibility into the actual routing paths and the behavior of neighboring networks. For instance, consider a government organization that relies on multiple external service providers and relies on their networks for connectivity. The administrators may have limited insight into the internal routing policies and configurations of these external networks. This can make it difficult to detect and address routing security issues effectively.
3. **Dynamic Nature of BGP:** BGP is a dynamic routing protocol that relies on the exchange of routing information between multiple autonomous systems (ASes). For example, imagine a

government agency that operates a large network connected to various external ASes, including Internet service providers and other government entities. The constant changes in network topologies, route advertisements, and BGP peering relationships introduce complexities and increase the chances of misconfigurations and security vulnerabilities.

4. **Scalability:** as networks grow in size and complexity, ensuring routing security at scale becomes more challenging. For instance, consider a multinational corporation with a vast network infrastructure spanning multiple continents and encompassing numerous branch offices, data centers, and cloud environments. Managing a large number of BGP peers, implementing consistent security policies, and handling route updates and filtering can strain network resources and administration efforts.
5. **Interoperability:** networks often connect with multiple service providers and peer with different types of routers and equipment. For example, consider a global enterprise that operates in various regions and relies on different service providers for connectivity. Each service provider may utilize different router models or equipment from various vendors and ensuring interoperability and consistent routing security policies across diverse environments can be a challenge.
6. **Lack of Standardization:** while best practices exist for routing security through things like the Mutually Agreed Norms for Routing Security(MANRS) initiative, there is no universal standard or framework for implementing and enforcing these practices. For instance, consider a scenario where multiple financial institutions operate their own networks and interconnect with each other to facilitate secure transactions. Each institution may have its own interpretation of routing security best practices and implement them according to their specific needs and requirements. This lack of standardization can lead to inconsistencies and variations in routing security policies across different organizations and networks.
7. **Misconfigurations:** misconfigurations in routing security policies can unintentionally disrupt network connectivity or open up security vulnerabilities. For example, a misconfigured filter or ACL may accidentally block legitimate traffic, resulting in service outages or communication issues for customers. Configuring filters, access control lists (ACLs), and route propagation rules incorrectly can have severe consequences.
8. **Operational Overhead:** implementing routing security policies requires ongoing monitoring, maintenance, and updates. For example, consider a large enterprise with a complex network infrastructure spanning multiple locations and serving a diverse set of users and applications. Network administrators need to invest time and effort in regularly reviewing and adjusting policies to ensure they remain effective and aligned with network requirements. This involves monitoring routing updates, analyzing traffic patterns, and making necessary adjustments to

filters, access control lists (ACLs), or routing configurations.

9. **Balancing Security and Connectivity:** striking the right balance between routing security and maintaining efficient connectivity can be challenging. For instance, consider a cloud service provider that needs to ensure secure and reliable connectivity for its customers. Implementing overly strict security policies, such as excessive filtering or stringent access control measures, can inadvertently lead to connectivity issues. Legitimate traffic may get blocked or delayed, causing service disruptions and impacting customer satisfaction. On the other hand, implementing overly permissive policies can increase the risk of routing attacks, such as route hijacking or unauthorized route advertisements. For example, if the provider allows any external route advertisement without proper validation, it could potentially enable malicious actors to manipulate traffic and compromise the integrity of the network.
10. **Education and Awareness:** routing security requires a good understanding of BGP protocols, routing best practices, and the latest security threats. For example, consider a network operations team responsible for managing the network infrastructure of a large educational institution. To effectively implement routing security measures, network administrators must stay informed about the evolving landscape of routing security, including emerging threats and vulnerabilities.
11. **Diverse Network Architectures:** Government entities often have complex and diverse network architectures due to the presence of numerous departments, agencies, and locations. Creating a routing security policy that can accommodate these varied architectures while maintaining a consistent security posture can be challenging.
12. **Varying Security Requirements:** Different government organizations may have distinct security requirements based on the sensitivity of the data they handle and the level of risk they face. Developing a replicable policy that can be tailored to meet the specific security needs of different entities within the government while still maintaining a baseline level of security can be complex.
13. **Legacy Infrastructure:** Government networks often include legacy infrastructure that may not have been designed with modern security considerations in mind. Updating and securing these legacy systems to align with a replicable routing security policy can be a significant challenge, requiring careful planning and resource allocation.
14. **Interoperability and Compatibility:** Government networks frequently interact and exchange data with external entities, including other government agencies, contractors, and service providers. Ensuring interoperability and compatibility between different routing security implementations can be a challenge, especially when dealing with different technologies, protocols, and security standards.

15. **Resource Constraints:** Government entities often operate with limited resources, including budgetary constraints and a shortage of skilled cybersecurity professionals. Developing and implementing a replicable routing security policy may require additional investments in equipment, training, and personnel, which can pose challenges within resource-constrained environments.
16. **Policy Adoption and Compliance:** Even with well-designed policies, ensuring widespread adoption and compliance across various government entities can be challenging. Building awareness, providing training, and enforcing compliance with routing security policies may require a coordinated and ongoing effort.
17. **Evolving Threat Landscape:** The threat landscape is constantly evolving, with new vulnerabilities and attack vectors emerging regularly. A replicable routing security policy needs to be adaptable and responsive to these evolving threats, requiring continuous monitoring, updates, and adjustments to remain effective.

Overcoming these challenges requires a collaborative effort involving industry stakeholders, standardization bodies, and the sharing of best practices. Establishing a community-driven approach to developing replicable BGP security policies can foster knowledge exchange, facilitate the identification of common challenges, and promote the development of standardized frameworks that can be easily implemented and replicated across different organizations. By addressing the diverse needs of various stakeholders and keeping pace with the evolving threat landscape, the development of replicable BGP security policies can significantly enhance the security posture of BGP deployments on a broader scale.

III. The Holy Grails of BGP Security Policy Best Practices

As we strive to make progress in BGP or routing security, we find ourselves engaged in a battle with old habits, legacy systems, and the ever-evolving landscape of Cyber threats. The quest to enhance BGP security is not a simple undertaking; it requires challenging the status quo and overcoming the inertia of outdated practices. In many cases, we encounter networks built on foundations laid long ago, where security considerations were not given the priority they deserved.

These networks often lack the necessary safeguards to protect against modern-day threats. To make significant strides in routing security, we must confront these entrenched norms and embrace a forward-thinking mindset. It is a battle that demands a combination of technical expertise, policy advocacy, and collaboration among stakeholders. By acknowledging the risks associated with outdated practices and the ever-evolving landscape of Cyber threats, the adoption of MANRS principles empowers us to proactively shape a more secure and resilient routing environment.

MANRS is a global initiative that outlines simple, concrete actions organizations can take to reduce the most common threats to routing. With a firm grasp of the latest insights and unwavering determination, we can confidently navigate the path ahead and fortify our networks against potential threats.

Implementing BGP security policy best practices play a pivotal role in safeguarding against potential vulnerabilities and threats that could compromise the core infrastructure of the Internet [5][6][7][11]. The following are BGP security policy best practices with proven strategies and guidelines that empower organizations to fortify their networks, bolster data trustworthiness, and contribute to a secured BGP infrastructure.

1. **Understanding BGP:** BGP is a complex protocol, and it is important to understand how it works in order to secure it. There are many resources available to learn about BGP, including resources hosted in MANRS repositories[1].

2. **Simplicity:** keep the BGP security policy as simple as possible. Complexity can introduce vulnerabilities and increase the chances of misconfiguration. For example, imagine a small-to-medium-sized enterprise that operates a network infrastructure with multiple BGP routers. To maintain a robust routing security posture, the network administrators decide to follow the principle of simplicity. Their BGP security policy includes straightforward measures such as implementing prefix filtering to allow only authorized routes, enabling secure BGP (s-BGP) for authentication and integrity verification, and implementing route validation using RPKI. By adhering to the principle of "do one thing and do it well," the network administrators strike a balance between security and simplicity.

3. **Least Privilege:** implement the principle of least privilege when defining BGP routing policies. Restrict access and permissions to only what is necessary, minimizing the attack surface and potential for unauthorized or malicious actions.Implementing the principle of least privilege in BGP routing policies involves restricting personal access based on roles and responsibilities and narrowing the number of peers or upstream providers.

4. **Authentication and Authorization:** Utilize strong authentication and authorization mechanisms for BGP sessions. Use mechanisms such as BGP MD5 authentication [4] or more advanced methods like BGPsec [12] to ensure that only authorized peers can establish BGP connections and exchange routing information.

5. **Filtering and Validation:** Implement rigorous filtering and validation mechanisms for BGP

[1] https://github.com/manrs-tools

routing updates. Utilize prefix-based filtering, including ingress and egress filtering, to control the announcement and acceptance of BGP routes.

6. **Monitoring and Logging:** Maintain comprehensive monitoring and logging capabilities for BGP operations. Monitor BGP sessions, routing updates, and anomalies to detect and respond to any potential security incidents promptly. Retain detailed logs for auditing, analysis, and incident investigation purposes.
7. **Redundancy and Resilience:** Design BGP networks with redundancy and resilience in mind. Utilize redundant connections, multiple BGP peers, and diverse paths to enhance network availability and mitigate the impact of failures or attacks. Implement robust failover mechanisms to ensure uninterrupted routing in case of link or device failures.
8. **Timely Software Updates and Patching:** Keep BGP routers up to date with the latest software updates and security patches. Regularly review and apply patches provided by the router vendors to address any identified vulnerabilities or weaknesses in the BGP implementation.
9. **Continuous Education and Awareness:** Stay updated on the latest BGP security threats, vulnerabilities, and best practices. Participate in industry forums, attend conferences, and engage with the network security community to enhance your knowledge and share experiences.
10. **Collaboration and Information Sharing:** Foster collaboration and information sharing among network operators, ISPs, and security communities. Participate in BGP security initiatives, such as the Mutually Agreed Norms for Routing Security (MANRS), to promote best practices and collectively improve the security of the global routing infrastructure.
11. **Testing and Validation:** Regularly test and validate BGP security measures to ensure they are functioning as intended. Perform periodic security audits and penetration tests to identify and address any weaknesses or vulnerabilities in the BGP infrastructure.
12. **Implement RPKI:** RPKI is a security framework that can help to prevent BGP hijacking attacks. It allows network operators to publish their routing information in a secure manner, and it allows routers to verify the authenticity of this information. Validate BGP route announcements using techniques such as Route Origin Authorization (ROA) and RPKI.
13. **Secure BGP Sessions:** Protect BGP sessions using Transport Layer Security (TLS) or

IPsec to ensure confidentiality, integrity, and authentication of BGP communications.

14. **Route Dampening:** Implement route dampening mechanisms to suppress the propagation of unstable or flapping routes. This helps to reduce unnecessary routing churn and potential performance issues.

15. **Incident Response:** Establish an effective incident response plan specifically for BGP-related security incidents. Define procedures for detecting, analyzing, and responding to incidents such as BGP hijacking, route leaks, or unauthorized route propagation. This includes having a designated incident response team, clear escalation paths, and predefined communication channels.

16. **Vendor Diversity:** Consider diversifying BGP router vendors within the network infrastructure. Dependence on a single vendor may introduce a single point of failure or increase the impact of vulnerabilities specific to that vendor's equipment. By using equipment from multiple vendors, organizations can mitigate risks and enhance overall resilience.

17. **Access Control:** Enforce strict access control measures for BGP routers and related infrastructure. Implement strong authentication mechanisms, such as two-factor authentication, and restrict administrative access to authorized personnel only. Regularly review and update access control policies to prevent unauthorized access.

18. **Secure Interconnection Points:** Implement security measures at interconnection points such as Internet Exchange Points (IXPs) and peering locations. Ensure that BGP sessions established at these points adhere to security best practices, including proper authentication, filtering, and validation of route announcements.

19. **Network Segmentation:** Implement network segmentation to isolate critical BGP infrastructure from other network components. By separating BGP routers from less critical systems, the impact of a security breach or compromise can be limited, and the overall network security posture can be improved.

20. **Third-party Risk Management:** Assess and manage the security risks associated with third-party connections and peering relationships. Conduct due diligence on potential partners and regularly review existing peering agreements to ensure they align with security best practices.

21. **Regulatory Compliance:** Consider applicable regulatory requirements and compliance frameworks when developing BGP routing security policies. Depending on the industry and

jurisdiction, there may be specific regulations or standards that organizations need to adhere to regarding routing security and data protection.

22. **Threat Intelligence:** Stay informed about emerging threats, vulnerabilities, and attack trends related to BGP routing. Engage with threat intelligence sources(i.e. MANRS, BGPStream[2], RIPE RIS[3], etc.) security vendors, and industry forums to receive timely updates and leverage actionable intelligence for proactive defense.

Drawing upon the routing security best practices outlined above, the Zen guide to BGP/routing security policy presented in the subsequent section, provides network operators and administrators in government networks with a comprehensive roadmap to elevate the security posture of their BGP networks, bolstering the overall security and stability of the Internet's routing infrastructure.

IV. The Zen Guide to BGP/Routing Security Policy

The Zen guide to BGP/routing security encapsulates the philosophy of achieving a harmonious and balanced approach to securing the Border Gateway Protocol (BGP). It emphasizes simplicity, mindfulness, and understanding the true nature of BGP security challenges. Adopting the Zen guide to BGP/routing security means going beyond mere technical measures and embracing a holistic mindset that considers the interplay of technology, human factors, and the overall ecosystem in which BGP operates.

At its core, the Zen guide to BGP or routing security encourages network operators or administrators and organizations to focus on simplicity and clarity in their security practices. Instead of relying on convoluted and complex solutions, it promotes the idea of stripping away unnecessary complexities and adopting straightforward measures that address the fundamental vulnerabilities and threats in BGP. By simplifying configurations, minimizing dependencies, and reducing the attack surface, the Zen guide to BGP/routing security aims to achieve a more resilient and manageable routing security posture.

The figure below, Figure 1, visually depicts the Zen guide to BGP/routing security.

[2] https://bgpstream.caida.org/
[3] https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris

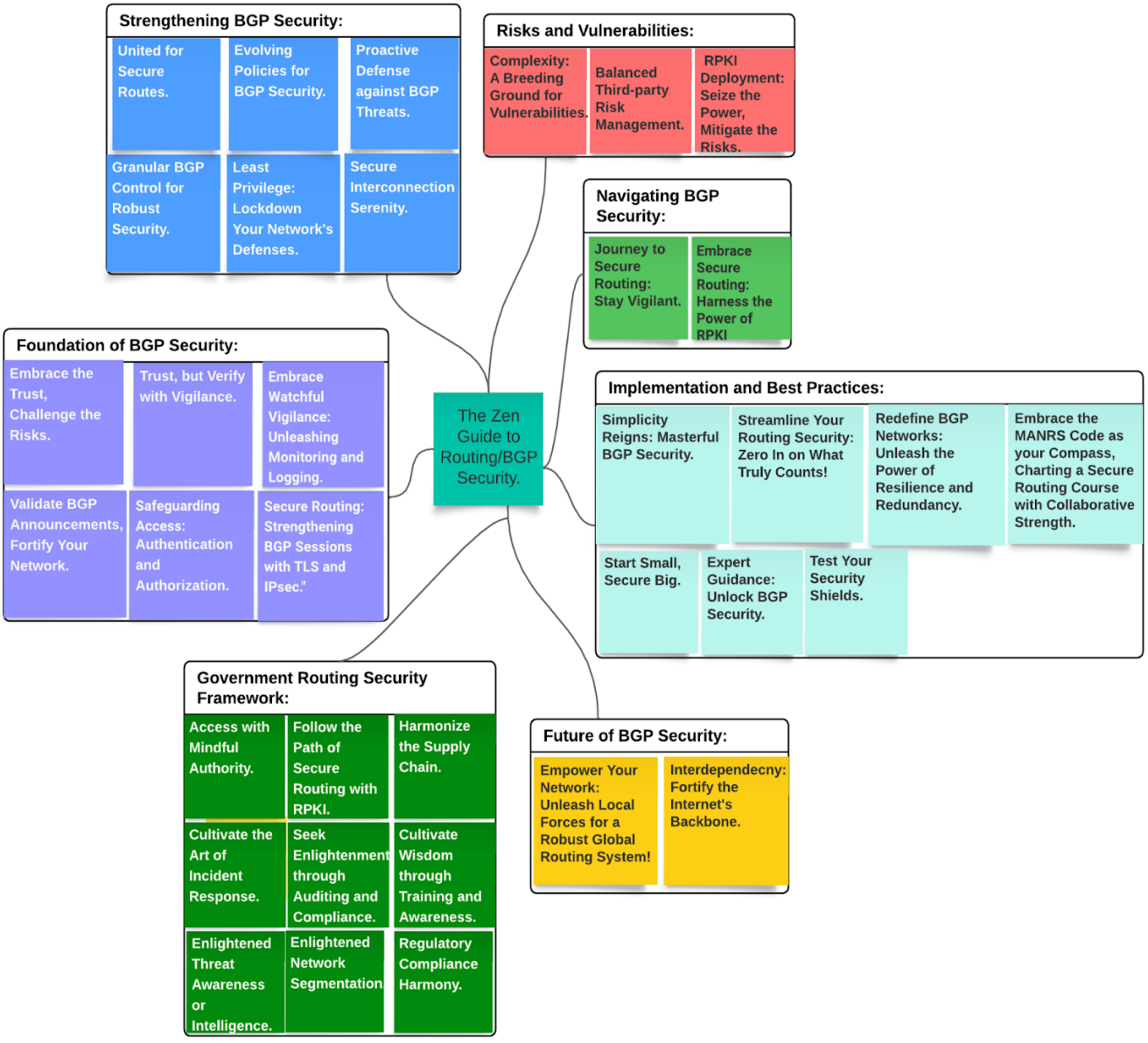

Figure 1- The Zen Guide to BGP/Routing Security: A Visual Representation.

By simplifying configurations and minimizing complexities, network operators can achieve a more resilient and manageable security posture. Adopting a mindful mindset involves staying aware of the dynamic nature of BGP, regularly monitoring routing updates, and promptly responding to potential security incidents. Cultivating a culture of continuous learning and staying informed about emerging threats and best practices enables network operators to adapt and improve their security measures. By embracing the Zen guide to BGP/routing security, organizations can strive for a harmonious and balanced approach that enhances the security and stability of their BGP deployments.

V. Contributors:

Dessalegn Mequanint Yehuala

Harish Chowdhary

Megan Kruse

Ryan Polk

VI. Reference:

[1] Kolkman, Olaf. "Replicable BGP Security Policies: The Missing Link." *NANOG 59*, June 2012.

[2] Bush, Randy. "BGP Security Policies: The Next Frontier." *NANOG 71*, June 2017.

[3] North American Network Operators' Group (NANOG) Routing Security Working Group (RSWG). "Building a Replicable BGP Security Policy: A Community-Driven Approach." NANOG, January 2023.

[4] Murphy, S. (2006, January). BGP Security Vulnerabilities Analysis. Request for Comments (RFC) 4272. Internet Engineering Task Force (IETF). https://datatracker.ietf.org/doc/html/rfc4272.

[5]Ahmad, A. (2023, November 4). BGP security best practices. Retrieved from https://afrozahmad.com/blog/bgp-security-best-practices/

[6] Smith, P., & Rhoden, W. (2002). BGP Design and Implementation. Cisco Press.

[7] Bates, T., Chandra, R., Katz, D., & Rekhter, Y. (1998). Multiprotocol extensions for BGP-4. RFC 2283.

[8] BGP Security Best Practices, by N. Ferguson and R. Huston, RFC 2827, IETF, 2000.

[9] Designing and Implementing a BGP Security Policy for Government Networks, by National Institute of Standards and Technology (NIST), Special Publication 800-50, 2012.

[10] BGP Security Best Practices for Government Networks, by General Services Administration (GSA), 2015.

[11] Developing a Replicable BGP Security Policy for Government Networks, by Defense Information Systems Agency (DISA), 2018.

[12] Lepinski, M., & Sriram, K. (2017, September). BGPsec Protocol Specification. Request for Comments (RFC) 8205. Internet Engineering Task Force (IETF).

[13] Hu, Y., & Perrig, A. (2004). A survey of secure BGP protocols. IEEE Communications Surveys & Tutorials, 6(3), 2-19.