Journal of Social Research

P-ISSN: 2827-9832
E-ISSN: 2828-335x
http://ijsr.internationaljournallabs.com/index.php/ijsr

Implementation of Border Gateway Protocol (BGP) Community for DDoS Flooding Mitigation in the Communication and Information Agency of East Java Province

Adi Dwi Cahyono, Made Kamisutara
Universitas Narotama, Indonesia
Email: adidwica@gmail.com, made.kamisutara@narotama.ac.id

ABSTRACT

Distributed Denial-of-Service (DDoS) attacks are a serious threat to network infrastructure that can cripple services by flooding systems with malicious traffic. This study implements the attributes of the Border Gateway Protocol (BGP) Community together with Remote Triggered Black Hole (RTBH) as an effective mitigation strategy for the Communication and Information Service of East Java Province. The developed solution leverages BGP routing capabilities to quickly identify and discard attack traffic at the network edge through coordinated route marking. Implementation includes the use of BGP Community tags (300:222) to flag dangerous traffic routes, automatic blackhole routing setup through coordination with upstream service providers, and validation of the framework through real-time simulations using GNS3. The results show this solution can mitigate volumetric attacks in seconds, with a 100% blocking rate for marked prefixes while maintaining normal operation for unaffected routes. This approach offers significant improvements in response speed and scalability for government networks facing advanced DDoS threats. The findings of the study provide practical implementation guidance and empirical evidence supporting BGP-based DDoS mitigation, particularly for the Indonesian government's digital infrastructure.

Keywords: *BGP Community, DDoS, RTBH*

INTRODUCTION

Distributed Denial-of-Service (DDoS) attacks are attacks that cause crashes on servers and systems on a network by flooding packets or requests on the network (Kotikalapudi & Kumar, 2023). Because of the development of the network system, the number of users in it is increasing (Bawany et al., 2017; Kambourakis & Kolias, 2017). Therefore, it is very difficult to identify who is a legal user and who is a hacker (Behal et al., 2017). And also as technology develops, the techniques for creating DDoS attacks are also improving. Identifying DDoS attacks is a more complex problem because there are different types of DDoS attack strategies. DDoS flooding techniques continue to evolve, ranging from network layer attacks (Layer 3/4) such as UDP/ICMP floods to application protocol exploits (Layer 7) such as HTTP floods (Alomari et al., 2016; Bhuyan et al., 2015). Volumetric attacks, such as DNS amplification, are capable of generating traffic of up to hundreds of Gbps by exploiting unsecured protocol vulnerabilities (Mirkovic & Reiher, 2015).

In modern network architectures that face the threat of DDoS attacks increasingly massive and complex, the implementation of Routing Trigger Blackhole through the BGP (Border Gateway Protocol) protocol has become a strategic necessity (Kotikalapudi & Kumar, 2023). This technique allows the network to selectively dump traffic that goes to a specific prefix that is being attacked (Abbas & Khan, 2021). The main advantages of this technique are the speed of response and scalability (Shah & Issac, 2018). Since BGP is a protocol that is already used globally in internet route exchange, blackhole routing can be implemented within

seconds of an attack being detected (Zhang et al., 2017). This is especially crucial considering that DDoS attacks often occur suddenly with a very large volume of traffic (Jonker et al., 2019).

The characteristics of modern DDoS attacks that are volumetric and multi-vector require an almost instant response. Traditional techniques such as ACL (Access Control List) or rate-limiting are often not effective enough when dealing with attacks with hundreds of Gbps volumes. By utilizing BGP blackholes, networks can isolate attack traffic at the edge within seconds of detection, preventing overload on the core infrastructure. This mechanism becomes a vital last line of defense when an attack exceeds the capacity of other mitigation (Alotaibi et al., 2022; Farasat & Khan, 2021; Mujtaba, 2012; Zhao et al., 2021).

The scalability of BGP is a key factor in the protocol's success as the backbone of routing on the global Internet. With its ability to handle thousands to hundreds of thousands of route entries, BGP has demonstrated high efficiency in managing routing between autonomous domains (US). However, the ever-growing complexity of managing routing tables is a challenge, especially in terms of memory usage, convergence time, and network stability. Therefore, improving efficiency in route filtering, policy control, and path selection mechanisms is critical to maintaining BGP scalability in the future (Timothy G. Griffin., 2021).

Route tagging using the BGP Community attribute has become a common practice in managing routing policies between domains. By tagging routes using community values, network operators can efficiently relay routing policy information to their BGP partners (Robert Raszuk, Jeff Haas, Alexander Lange, Bruno Decraene, Shane Amante, Paul Jakma, 2023). With the use of this attribute, a route will be formed with a certain tag that will be recognized by the upstream router, the reading of the route tag sent earlier will automatically know what the meaning of the tag is and take action as ordered.

The urgency of this research stems from the escalating frequency and complexity of DDoS attacks, which threaten operational continuity and financial stability. Previous studies have explored solutions such as BGP Blackholing and BGP Communities for route tagging and policy enforcement, yet gaps remain in real-world implementation, particularly in government networks. Challenges like coordination between autonomous systems (ASes) and the risk of misconfiguration during Remote Triggered Black Hole (RTBH) deployment are often overlooked. This study addresses these gaps by proposing a practical framework for implementing BGP Communities in the East Java Provincial Communication and Information Agency's network. The research introduces a structured workflow for RTBH activation, emphasizing speed and accuracy to minimize downtime, while also evaluating scalability and interoperability with upstream ISPs.

The implementation of BGP Community in the network infrastructure of the East Java Provincial Communication and Information Office raises two key questions. First, how can BGP Community be effectively deployed within the agency's existing network architecture to ensure seamless integration and optimal performance? This involves addressing technical challenges such as router configuration, coordination with upstream Internet Service Providers (ISPs), and the establishment of standardized procedures for route tagging. Second, to what extent can BGP Community mitigate DDoS flooding attacks? This question explores the efficacy of the solution in real-world scenarios, including its ability to quickly isolate malicious traffic and prevent network overload during high-volume attacks.

Benefits: This research can enrich the study of computer science and information technology at Narotama University, especially in the field of administration and network security. This research is also expected to strengthen the university's reputation in the development of information technology. This research can provide scientific contributions for research institution or university partners in mitigating cyber incidents, especially DDOS Trafic Flooding. For students, this study provides a deeper understanding of the application of BGP Community in the administration of BGP Routing.

METHOD

The Research Method uses the concept of Network Development Life Cycle (NDLC). Where the concept or method of the system is used to plan, build, and manage a computer network. NDLC is a comprehensive systematic approach to implementing the concept of RTBH.

1. Analysis

For the current topological conditions, there is no router redundancy as shown in the image. sN where public IP is also only recognized on border-level routers and for users to use the NAT feature for access to their Public IP.cThrough this analysis process, important indicators are also found that:

a. Network infrastructure is often the target of volumetric DDoS attacks.
b. Firewall perimeters and traditional IDS/IPS devices are not capable of effectively filtering traffic when backbone bandwidth is saturated.
c. It takes a routing-based solution that can mitigate attacks early l—before traffic reaches the core network

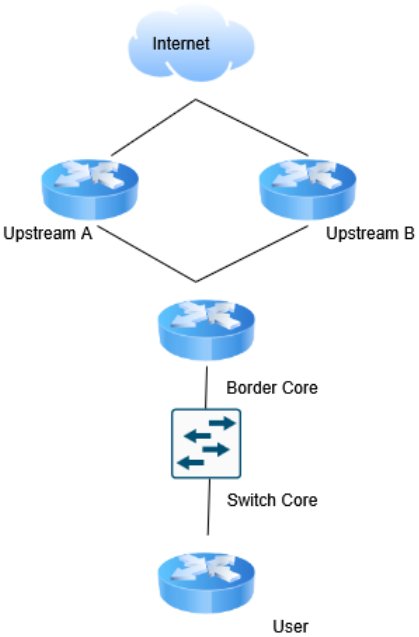

Figure 1. Existing topology
Source: Personal Documents

2. Design

From the results of the study, an approach using Border Gateway Protocol (BGP) Community Filtering was chosen which allows coordination with upstream providers to selectively filter traffic at the global routing level. In this scheme, when a flooding attack is detected to a specific prefix, that prefix can be re-announced to the ISP by adding a custom BGP Community tag.

BGP network architecture that connects an internal Autonomous System (AS400) to two different internet service providers (ISPs), namely ISP A (AS200) and ISP B (AS300), through two different border routers. Router Border A and Router Border B act as an interconnection point between the AS400 and the outside network, and they connect to the Core Router inside the AS400 to distribute routes and data internally. The Distribution Router is in the bottom layer as part of the internal infrastructure that receives routing from the Core Router

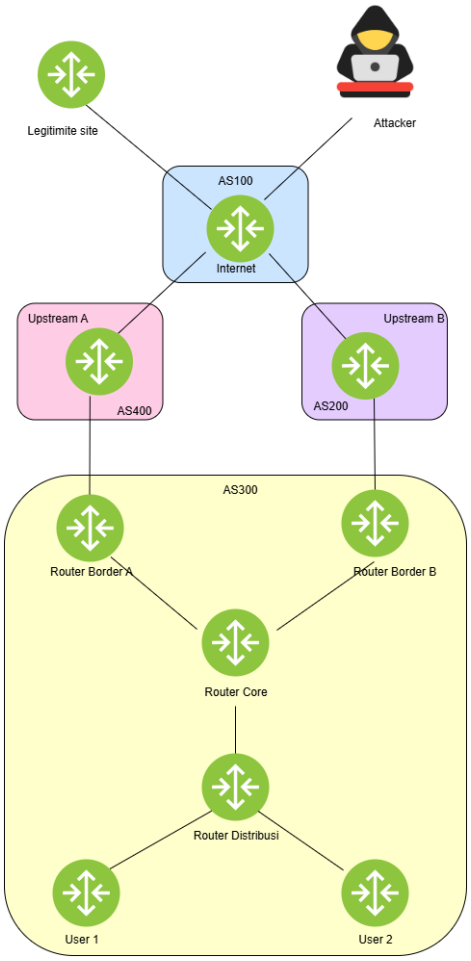

Figure 2. Topology Design
Source: Author's Design, 2023

3. Simulation

In this simulation, each node is connected to a dynamic routing system where each node is connected to a BGP routing.

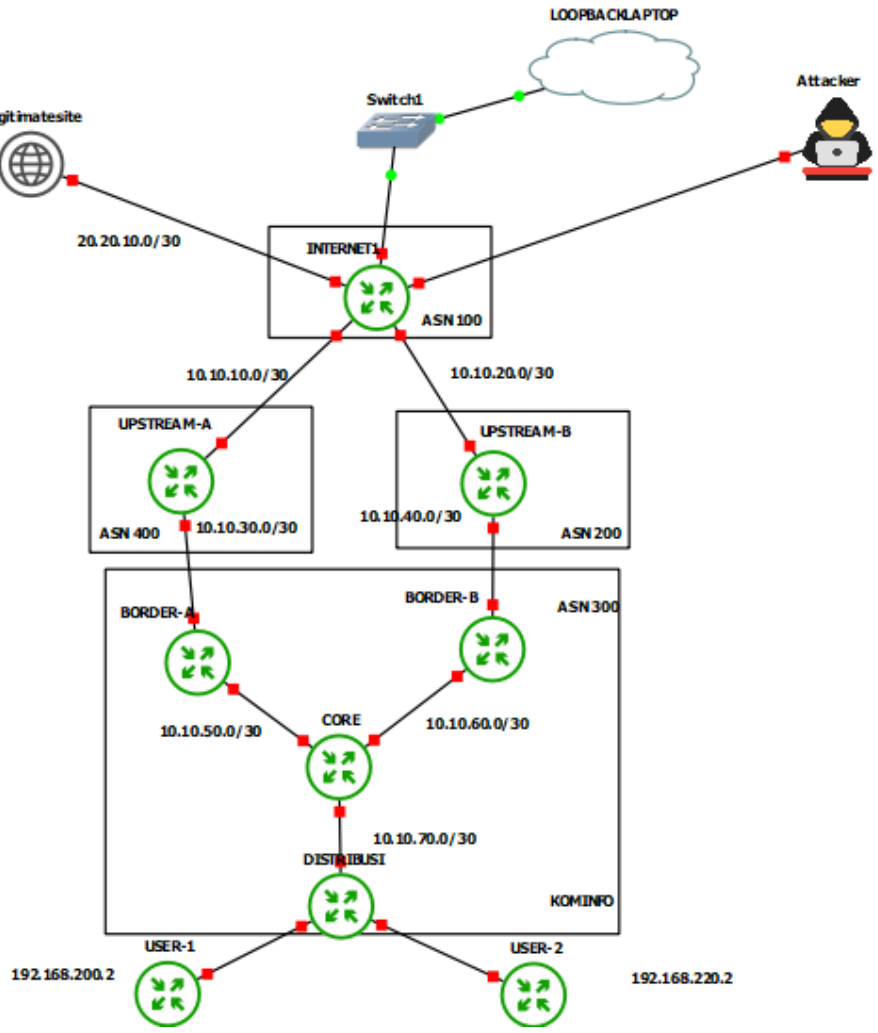

Figure 3 GNS3 Simulation

Source: Author's Design, 2023

Table 1. List of IP Address allocations

Node	IP Address	Information
Trust Site	20.20.10.2	PtP to Internet
Internet	20.20.10.1	PtP Trus Site
	10.10.10.1	PtP Upstream A
	10.10.20.1	PtP Upstream B
Upstream A	10.10.10.2	PtP Intenet
	10.10.30.1	PtP Border A
Upstream B	10.10.20.2	PtP Internet
	10.10.40.1	PtP Border B
Border A	10.10.30.2	PtP Upstream A
	10.10.50.1	PtP Core
Border B	10.10.40.2	PtP Upstream B
	10.10.60.1	PtP Core
Core	10.10.50.2	PtP Border A
	10.10.60.2	PtP Border B
	10.10.70.1	Distribution PtP

Node	IP Address	Information
Distribution	10.10.70.2	PtP Core
	192.168.200.1	PtP User 1
	192.168.220.1	PtP User 2
User 1	192.168.200.2	Distribution PtP
User 2	192.168,220.2	PtP Distibusi

Source: Author's Data, 2023

RESULTS AND DISCUSSION

Implementation

After simulating the network topology and IP address configuration on each router interface, the next step is to configure the AS Number and routing between nodes

1. Configure the AS Number

a. Internet: [admin@Router_internet] > routing bgp instance set default as=100
b. Upstream A: [admin@Ro. Upstream-_A] > routing bgp instance set default as=400
c. Upstream B: [admin@Ro. Upstream_-B] > routing bgp instance set default as=200
d. Border A: [admin@Ro. Border-_A] > routing bgp instance set default as=300
e. Border B: [admin@Ro. Border-_B] > routing bgp instance set default as=300
f. Core: [admin@Router Core] > routing bgp instance set default as=300
g. Distribution: [admin@Ro. Distribution] > routing bgp instance default set as=300

2. eBGP Configuration

a) BGP Peer – Internet to Upstream A:
[admin@ Router_] > routing bgp peer add name=internet-to-upstream_A remote-address=10.10.10.2 remote-as=400
b) BGP Peer – Internet to Upstream B:
[admin@] > routing bgp peer add name=internet-to-upstream_B remote-address=10.10.30.2 remote-as=200
[admin@ Router_internet] > routing bgp network add network=10.10.10.0/29
[admin@ Router_internet] > routing bgp network add network=10.10.20.0/30
[admin@Router_internet] > routing bgp network add network=20.20.10.0/30
c) BGP Peer - Upstream A to Border A:
[admin@Ro.Upstream-_A] > routing bgp peer add name=upstream_A-to-border_A remote-address=10.10.30.2 remote-as=300
[admin@Ro. Upstream-_A] > routing bgp network add network=10.10.10.0/29
[admin@Ro. Upstream-_A] > routing bgp network add network=10.10.30.0/30
d) BGP Peer - Border A to Upstream A:
[admin@Ro. Border-_A] > routing bgp peer add name=border_A-to-upstream_A remote-address=10.10.30.1 remote-as=400
[admin@Ro. Border-_A] > routing bgp network add network=10.10.30.0/30
e) BGP Peer - Upstream B to Border B:
[admin@Ro. Upstream-_B] > routing bgp peer add name=upstream_B-to-border_B remote-address=10.10.40.2 remote-as=300
[admin@Ro. Upstream_-B] > routing bgp network add network=10.10.40.0/30

[admin@Ro. Upstream-_B] > routing bgp network add network=10.10.20.0/30

f) BGP Peer - Border B to Upstream B:
[admin@Ro. Border-_B] > routing bgp peer add name=border_B-to-upstream_B remote-address=10.10.40.1 remote-as=400
[admin@Ro. Border_-B] > routing bgp network add network=10.10.40.0/30

iBGP Configuration

a) OSPF of Routerin Border A :
[admin@Ro. Border-_A] > routing ospf instance set router-id=192.168.0.4 [admin@Ro. Border_A] > routing ospf network add network=10.10.30.0/30 area=backbone
[admin@Ro. Border_A] > routing ospf network add network=10.10.50.0/30 area=backbone
[admin@Ro.Border_A] > routing ospf network add network=192.168.0.4/32 area=backbone

b) OSPF by Routerin Border B :
[admin@Ro. Border_B] > routing ospf instance set router-id=192.168.0.5
[admin@Ro.Border_B] > routing ospf network add network=10.10.40.0/30 area=backbone
[admin@Ro. Border_B] > routing ospf network add network=10.10.60.0/30 area=backbone
[admin@Ro.Border_B] > routing ospf network add network=192.168.0.5/32 area=backbone

c) OSPF by Routerin Core :
[admin@Router core] > routing ospf instance set router-id=192.168.0.6
[admin@Router core] > routing ospf network add network=10.10.50.0/30 area=backbone
[admin@Router core] > routing ospf network add network=10.10.60.0/30 area=backbone
[admin@Router core] > routing ospf network add network=10.10.70.0/30 area=backbone
[admin@Router core] > routing ospf network add network=192.168.0.6/32 area=backbone

d) OSPF in Distribution Routers :
[admin@Ro. Border_B] > routing ospf instance set router-id=192.168.0.7
[admin@Router Distribusi] > routing ospf network add network=10.10.70.0/30 area=backbone
[admin@Ro.Distribusi] > routing ospf network add network=192.168.0.7/32 area=backbone

RTBH Routing implementation configuration

1. Configure filters and apply them to BGP peers on Core Routers

[admin@Router Core] > routing filter add chain=RTBH prefix=192.168.1.0 prefix-length=30 action=accept bgp-communities=300:222

(prefix adjusts how many IPs will be in the blackhole)

From the routing table on Router Border A and Router Border B you will see a prefix sent from Core with the community tag 300:222:

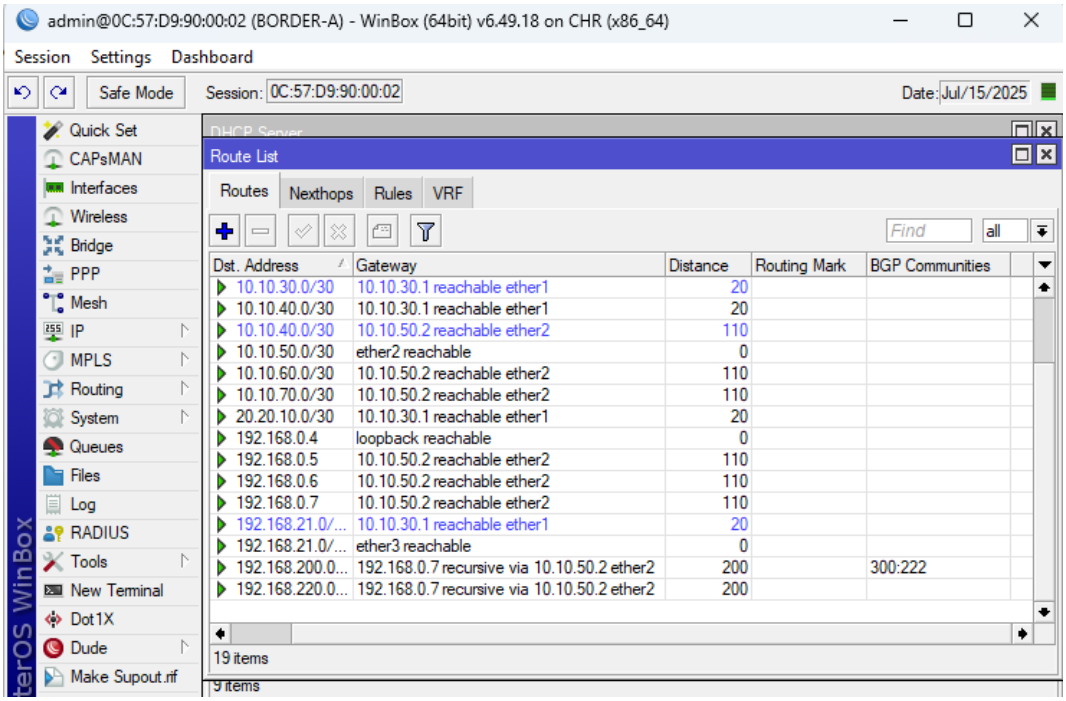

Figure 4. A Routing Table image that has been tagged with community is visible on Router Border A

Source: Author's Documentation, 2023

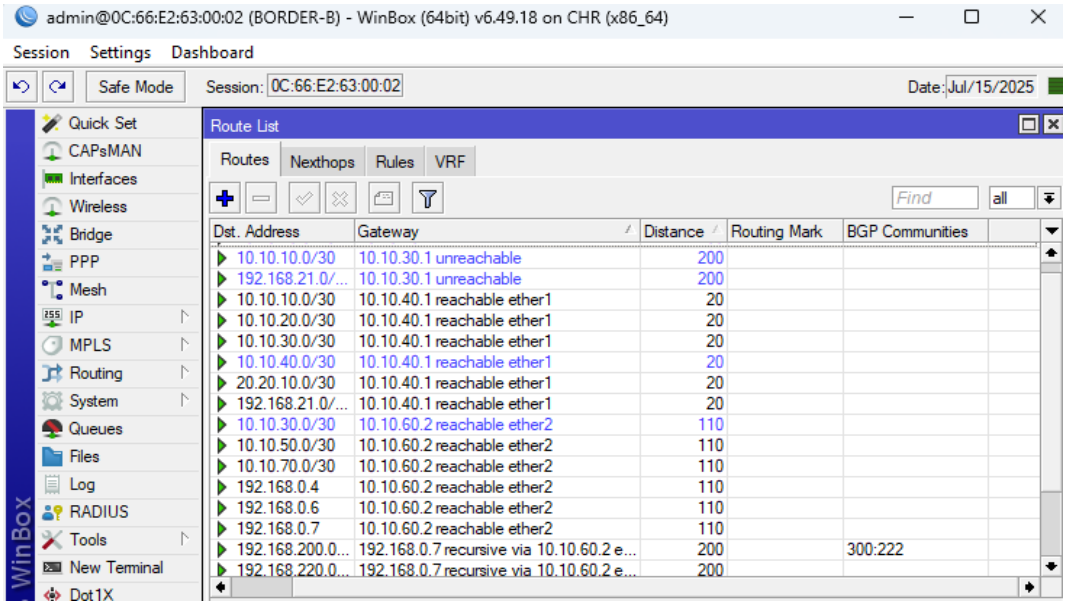

Figure 5. A Routing Table image that has been tagged with a community is visible on Router Border B

Source: Author's Documentation, 2023

2. Upstream

[admin@Upstream-A] > routing filter add chain=in-from-border bgp-communities=300:222 action=accept set-in-nexthop=172.2.0.1 set-type=blackhole

From the routing table on Upstream-A, you will see a prefix sent from the router border with BGP Community 300:222

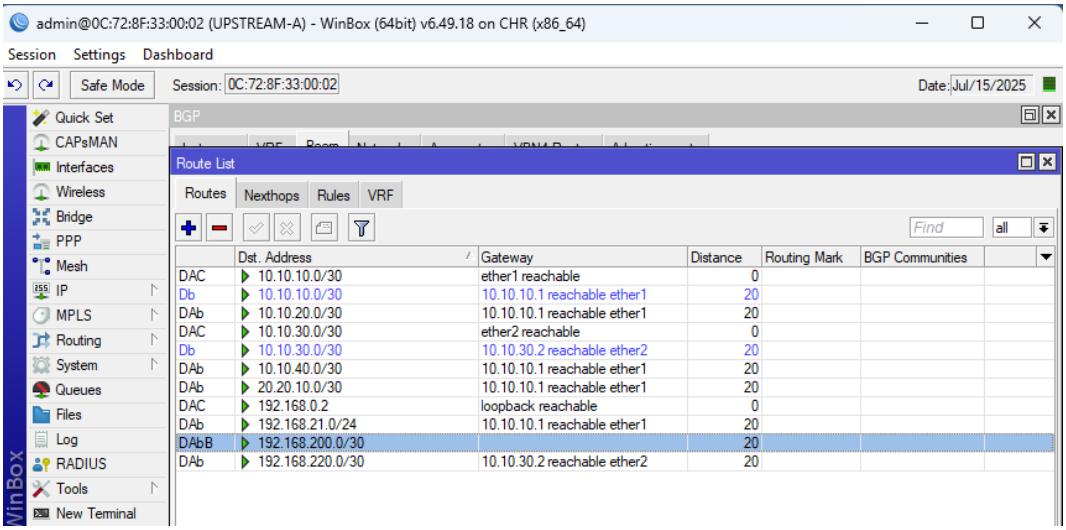

Figure 6. Upstream-A Routing Table with BGP Community 300:222

Source: Author's Documentation, 2023

After the Upstream Router side configures the filter, the ip that is blackholed cannot be accessed and the following is the result of the IP ping from Upstream with destination user 1 192.168.200.2 which is the victim prefix

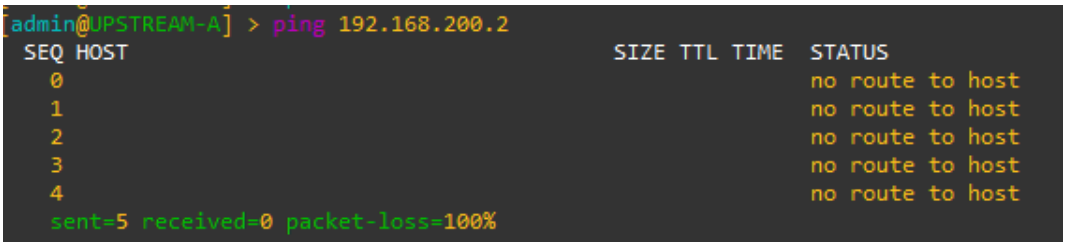

Figure 7. Test ping to ip user 1 is no longer possible

Source: Author's Documentation, 2023

CONCLUSION

After implementing and managing RTBH using the BGP Community, it is evident that this method is an effective, fast, and lightweight approach for mitigating flooding attacks like DDoS by enabling the quick blackholing of attack traffic at the prefix level, thereby preserving service stability and protecting infrastructure from overload. However, its success heavily relies on disciplined configuration, meticulous management, and rapid response from technical teams to avoid errors such as inadvertently blackholing legitimate traffic, which could cause service outages. To optimize implementation, it is crucial to develop clear, structured standard operating procedures (SOPs) to guide operational teams during attacks, enforce strict access control and authorization mechanisms to restrict sensitive BGP community usage, and enhance collaboration with upstream ISPs and Internet Exchange Points (IXPs) to ensure early mitigation before traffic reaches the local network. For future research, exploring automated validation and anomaly detection systems integrated with BGP community controls could further reduce human error risks and improve the speed and accuracy of RTBH activation in dynamic attack scenarios.

REFERENCES

Abbas, N., & Khan, S. (2021). Detection and mitigation of DDoS attacks in software-defined networking: A survey. *Journal of Network and Computer Applications, 181*, 103020. https://doi.org/10.1016/j.jnca.2021.103020

Al-Bahadili, H. (2018). Design and Implementation of BGP Novel Control Mechanism (BGP-NCM). Journal of King Saud University - Computer and Information Sciences, 30(1), 63–71. https://doi.org/10.1016/j.jksuci.2017.02.003

Alomari, E., Manickam, S., Gupta, B., Karuppayah, S., & Alfaris, R. (2016). Botnet-based distributed denial of service (DDoS) attacks on web servers: Classification and art. *International Journal of Computer Applications, 49*(7), 24–32. https://doi.org/10.5120/7651-0919

Alotaibi, H. S., Gregory, M. A., & Li, S. (2022). Multidomain SDN-Based Gateways and Border Gateway Protocol. Journal of Computer Networks and Communications, 2022(1), 3955800.

Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). DDoS attack detection and mitigation using SDN: Methods, practices, and solutions. *Arabian Journal for Science and Engineering, 42*(2), 425–441. https://doi.org/10.1007/s13369-017-2414-9

Behal, S., Kumar, K., & Sachdeva, M. (2017). DDoS attack detection and mitigation techniques: A review. In *Advances in Computer Communication and Computational Sciences* (pp. 509–518). Springer. https://doi.org/10.1007/978-981-10-6846-1_48

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys & Tutorials, 16*(1), 303–336. https://doi.org/10.1109/COMST.2013.052213.190

Farasat, T., & Khan, A. (2021). Detecting and analyzing border gateway protocol blackholing activity. International Journal of Network Management, 31(4), e2143.

Giotsas, V. (2018). CommunityWatch: The Swiss-Army Knife of BGP Anomaly Detection. arXiv preprint arXiv:1806.07476. https://arxiv.org/abs/1806.07476

Jonker, M., Sperotto, A., Pras, A., & van Rijswijk-Deij, R. (2019). Measuring the adoption of DDoS protection services. *ACM Transactions on Internet Technology, 19*(3), 1–25. https://doi.org/10.1145/3289106

Kambourakis, G., & Kolias, C. (2017). DDoS attacks and defenses in cloud environments. In *Cloud Security: Concepts, Methodologies, Tools, and Applications* (pp. 1589–1604). IGI Global. https://doi.org/10.4018/978-1-5225-4999-4.ch074

Kotikalapudi, R., & Kumar, R. (2023). Real-time detection and mitigation of DDoS attacks using machine learning and blackhole routing. *Journal of Information Security and Applications, 72*, 103418. https://doi.org/10.1016/j.jisa.2023.103418

Krenc, T., Beverly, R., & Smaragdakis, G. (2020). Keep Your Communities Clean: Exploring the Routing Message Impact of BGP Communities. arXiv preprint arXiv:2010.00745. https://arxiv.org/abs/2010.00745

Krenc, T., Beverly, R., & Smaragdakis, G. (2021). AS-Level BGP Community Usage Classification. arXiv preprint arXiv:2110.03816. https://arxiv.org/abs/2110.03816

Mirkovic, J., & Reiher, P. (2015). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39–53. https://doi.org/10.1145/997150.997156

Mujtaba, M. (2012). Analysis of Intrusion Detection System (IDS) in Border Gateway Protocol. University of Technology Sydney (Australia).

Shah, S., & Issac, B. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system. *Future Generation Computer Systems, 80*, 157–170. https://doi.org/10.1016/j.future.2016.10.028

Shao, W., Devienne, F., Iannone, L., & Rougier, J.-L. (2015). On the Use of BGP Communities for Fine-Grained Inbound Traffic Engineering. arXiv preprint arXiv:1511.08336. https://arxiv.org/abs/1511.08336

Zhang, J., Xiang, Y., Wang, W., Zhou, W., & Wu, J. (2017). Network traffic classification using correlation information. *IEEE Transactions on Parallel and Distributed Systems, 28*(6), 1681–1693. https://doi.org/10.1109/TPDS.2016.2622682

Zhao, X., Band, S. S., Elnaffar, S., Sookhak, M., Mosavi, A., & Salwana, E. (2021). The implementation of border gateway protocol using software-defined networks: A systematic literature review. IEEE Access, 9, 112596–112606.