International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Securing Cloud Environments with Bastion Hosts

Satish Kumar Malaraju

Technology Architect (DevSecOps), California-US

Abstract

As organizations increasingly migrate to cloud environments, securing cloud-based resources becomes paramount to protect sensitive data, critical applications, and infrastructure from unauthorized access and malicious attacks. Among the various security measures available, the implementation of a bastion host, or jump server, plays a pivotal role in fortifying cloud defenses. A bastion host acts as a controlled access point, providing secure entry to internal cloud resources, such as private instances within a Virtual Private Cloud (VPC), by mediating communication between external users and the cloud infrastructure. This paper delves into the concept and significance of bastion hosts in cloud security, examining how they serve as a gateway that allows authorized users to access private resources while minimizing the attack surface and reducing direct exposure to the internet. The research highlights key principles such as the enforcement of strict access controls, multi-factor authentication, role-based access policies, and continuous monitoring as essential components in configuring and managing bastion hosts securely. Additionally, the paper explores various best practices for bastion host deployment, including network segmentation, secure protocols, and logging, to mitigate vulnerabilities and enhance the resilience of cloud environments. By examining potential security risks, common challenges, and evolving trends in bastion host design and management, this paper provides actionable insights and recommendations for organizations to effectively implement bastion hosts as part of their comprehensive cloud security strategy. The study ultimately aims to offer a deeper understanding of the critical role bastion hosts play in safeguarding cloud infrastructure and ensuring robust security in modern cloud environments.

Keywords: Bastion host, cloud security, jump server, Virtual Private Cloud (VPC), access control, encryption, multi-factor authentication, role-based access, network segmentation, cloud infrastructure, secure protocols, logging, cloud security best practices.

1. Introduction

As organizations continue to embrace cloud computing for its flexibility, scalability, and cost-effectiveness, the need for robust security measures has become more critical than ever. Cloud environments host an increasing amount of sensitive data and mission-critical applications, making them attractive targets for cyberattacks. The evolving landscape of threats—ranging from data breaches to ransomware attacks—demands a comprehensive approach to securing cloud infrastructure. Traditional security measures, such as firewalls and intrusion detection systems, must be complemented by strategies specifically tailored for cloud-based resources. Among these strategies, the use of bastion hosts has emerged as a fundamental component of cloud security.[2][3]

A bastion host, often referred to as a jump server, is a specialized system designed to securely mediate access between external users and the internal cloud network. Its primary function is to provide a secure entry point for administrators and users who need to access private resources within a Virtual Private Cloud (VPC) or similar isolated environments. By acting as a tightly controlled access point, a bastion host minimizes the attack surface of the cloud infrastructure, preventing direct access to sensitive instances from the outside world. This security mechanism significantly reduces the risk of unauthorized access, ensuring that only authorized individuals can interact with critical cloud resources, often after passing through several layers of authentication and security checks.[7][8]

The purpose of this paper is to explore the key aspects of bastion hosts as a security solution within cloud environments. Specifically, it will address three primary objectives: first, why organizations should use bastion hosts to enhance cloud security; second, how to implement and configure a bastion host effectively; and third, best practices, tools, techniques, and alternatives for securing cloud access. In doing so, the paper will provide a comprehensive understanding of the role bastion hosts play in securing cloud-based infrastructures and offer guidance on their deployment and management.

The structure of this paper is organized into several sections that will provide a deep dive into each of these key topics. The first section will explore the rationale behind the adoption of bastion hosts, highlighting their advantages in safeguarding cloud environments. The subsequent sections will focus on the technical aspects of bastion host implementation, including configuration and integration with existing security frameworks. Finally, the paper will examine best practices, tools, and alternatives to bastion hosts, offering actionable recommendations for organizations to ensure their cloud security posture remains resilient against emerging threats. Through this exploration, the paper aims to equip readers with the knowledge needed to effectively utilize bastion hosts as a central component of their cloud security strategies.

2. Why use Bastion Host?

A bastion host, also known as a jump server, is a specialized system designed to provide secure access to a private network or cloud environment. Positioned as a gateway between external users and an organization's internal resources, a bastion host serves as the entry point for all administrative access to servers and applications within a Virtual Private Cloud (VPC) or other isolated environments. Typically, bastion hosts are configured to allow limited access, often via secure protocols such as SSH (for Linux) or RDP (for Windows), and they act as a controlled checkpoint that can be closely monitored and secured. Rather than allowing direct connections to critical resources, users must first authenticate and pass through the bastion host before reaching the desired internal systems.[4][6]

In a typical cloud architecture, private instances, which host sensitive applications and data, are placed in private subnets and lack direct internet access. To access these private instances securely, a bastion host is employed. By placing the bastion host in a public subnet within the VPC, it becomes the sole instance with a public IP address, accessible from the internet. Meanwhile, the private instances remain safely isolated in the private subnet, shielded from direct exposure to the public internet. Administrators first connect to the bastion host and then use it as a springboard to access the private instances via SSH or RDP, depending on the operating system. This configuration minimizes the attack surface and significantly reduces the risk of unauthorized access and potential breaches.

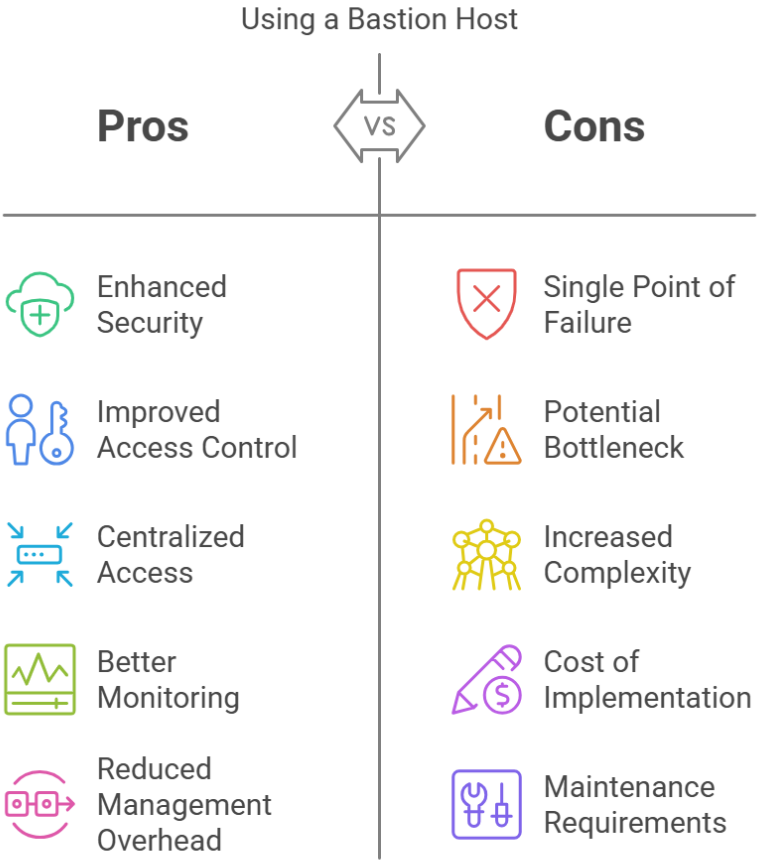
The Key Benefits of Using a Bastion Host for Cloud Security are

- **Enhanced Security:** By acting as a single point of entry into a cloud environment, the bastion host reduces the attack surface and minimizes exposure to external threats. It acts as the only publicly accessible instance, ensuring that other cloud resources, especially sensitive data and applications, are shielded from direct exposure to the internet. This layered approach to security helps defend against malicious actors attempting to exploit weaknesses in the cloud environment.
- **Improved Access Control:** A bastion host serves as the gatekeeper to private cloud resources, requiring users to authenticate themselves through it. By enforcing strict authentication measures, such as username/password combinations, SSH keys, or multi-factor authentication (MFA), organizations ensure that only authorized users can connect to internal instances. This robust access control mitigates the risk of unauthorized entry into critical systems.
- **Centralized Access Control:** The bastion host simplifies access management by centralizing control over the authentication process. Security controls, such as identity and access management (IAM) policies, can be implemented on the bastion host to govern access to private instances. Additionally, multi-factor authentication (MFA) and other strict policies can be enforced to enhance security further. This centralized approach to access control simplifies security audits and makes it easier to track and manage permissions, ensuring that only those with the proper credentials can access sensitive cloud resources.
- **Improved Monitoring and Logging:** Since all access to private instances goes through the bastion host, it becomes the central point for monitoring and logging all activities. This allows for detailed auditing and analysis of who accessed which resources, when, and how. The ability to monitor access to private instances in real-time and maintain comprehensive logs enhances security and simplifies compliance with industry regulations.[5][9]
- **Reduced Management Overhead:** Using a bastion host helps reduce the administrative burden of managing SSH keys for each individual instance. Rather than distributing and managing keys for every internal system, administrators only need to maintain and distribute keys for the bastion host itself. This streamlines the process of key management and reduces the potential for security lapses, such as outdated or misplaced keys.
- **Network Segmentation:** Bastion hosts are also valuable tools for implementing network segmentation. By isolating critical resources within private subnets and requiring access through the bastion host, organizations can create distinct security zones. For example, a bastion host could grant a user access to specific resources, such as a human resources database, while denying access to other systems, such as the financial database. This segmentation helps control access to sensitive data and limits exposure to the broader network.

  Bastion hosts are designed to mitigate several risks inherent in cloud environments. One of the primary threats is unauthorized access, whether by attackers exploiting weak security configurations or by legitimate users inadvertently exposing sensitive systems. A bastion host reduces this risk by providing a secure, controlled entry point for users.
- **Prevention of Direct Access:** By ensuring that all administrative access passes through a bastion host, the direct exposure of private cloud resources to the public internet is eliminated. This prevents attackers from targeting individual cloud instances or services directly, as they must first bypass the security measures of the bastion host.[10][13]

- **Reduced Lateral Movement:** Once attackers gain access to a network, they often attempt to move laterally across systems to escalate privileges or find valuable data. Bastion hosts can limit lateral movement by isolating access to only those systems that need it, preventing attackers from easily navigating the internal network.
- **Segmentation of Sensitive Resources:** In complex cloud architectures, bastion hosts can be used to segment access to particularly sensitive resources. For example, an organization might use a bastion host to control access to a database or a file storage system, ensuring that only specific users can interact with those critical systems while isolating them from other less sensitive resources.

Figure 1: Pros vs cons of Bastion Host



Controlled access is a cornerstone of cloud security. Cloud resources, unlike on-premises systems, are often accessible from anywhere with an internet connection, significantly increasing the attack surface. Without strict access controls, malicious actors could exploit vulnerabilities and gain unauthorized access to sensitive data or applications.

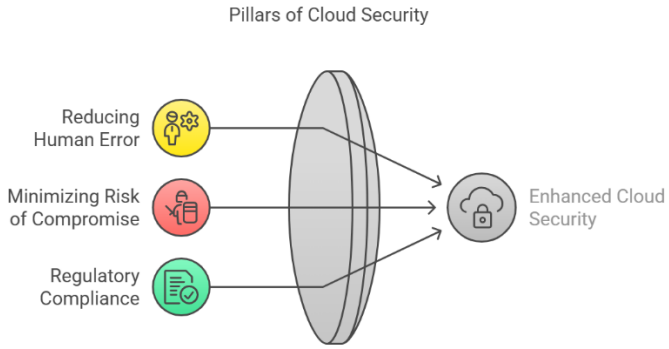
A bastion host allows organizations to enforce tight access policies, ensuring that only authenticated and authorized users can interact with the cloud infrastructure. This controlled access is vital for:

- Reducing Human Error: By requiring users to go through the bastion host, it becomes easier to manage who can access what resources and for what purpose. This reduces the likelihood of human errors,

such as accidentally exposing services or misconfiguring security settings.

- Minimizing Risk of Compromise: Limiting access to a well-defined, secure entry point means that even if an attacker compromises a single user's credentials or gains access to the bastion host, the attacker must bypass multiple layers of security before they can access critical resources.[12][14]
- Regulatory Compliance: Many industries are subject to strict compliance standards and regulations (e.g., HIPAA, GDPR, PCI-DSS). Bastion hosts help ensure that only authorized individuals have access to sensitive data, supporting compliance with these regulations by logging and controlling access in a clear and auditable way.

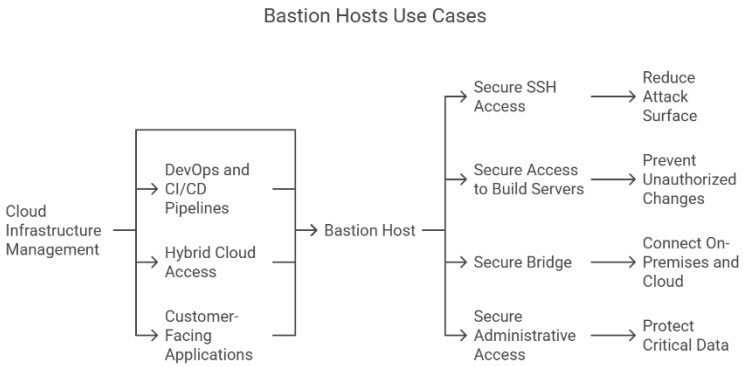
Figure 2: Pillars of Cloud security



Some of the Real-World Examples and Use Cases could be:

- **Cloud Infrastructure Management:** A common use case for bastion hosts is for administrators managing cloud-based systems. For example, a team managing an AWS environment may use a bastion host to provide secure SSH access to EC2 instances that are part of a private subnet. This setup ensures that administrators can manage resources without exposing those instances to the internet, significantly reducing the attack surface.
- **DevOps and CI/CD Pipelines:** In a DevOps environment, where developers and operations teams are responsible for deploying and maintaining applications in the cloud, bastion hosts can provide secure access to private build servers or environments. This ensures that only authorized DevOps engineers can deploy or modify code in sensitive environments, preventing unauthorized changes or access to production systems.
- **Hybrid Cloud Access:** In hybrid cloud environments, where an organization uses both on-premises infrastructure and public cloud services, bastion hosts can provide a secure bridge between on-premises systems and cloud resources. For example, an organization may use a bastion host to securely connect its on-premises Active Directory server with a cloud-based database or application, ensuring secure communication between the two environments.
- **Customer-Facing Applications**: A company hosting customer-facing applications in the cloud may use bastion hosts to allow secure administrative access to the application backend. By restricting administrative access to only certain user roles and routing this access through a bastion host, the organization can protect critical customer data and ensure the security of its infrastructure.[16][15]

Figure 3: Bastion Hosts use cases



In summary, bastion hosts provide a critical security layer that enhances the safety of cloud environments by enforcing controlled access, minimizing attack surfaces, and allowing for better management and monitoring of cloud infrastructure. Through real-world use cases and best practices, organizations can harness the full potential of bastion hosts to create secure, reliable cloud environments.

3. Types and Alternatives of Bastion Hosts

As organizations continue to embrace cloud computing and adopt a variety of cloud platforms, the need for secure and efficient access management remains critical. Bastion hosts play a vital role in securing cloud environments, but the type and implementation of a bastion host can vary depending on several factors, including the cloud platform, deployment model, and management preferences. Understanding the different types of bastion hosts, their characteristics, and their specific use cases will help organizations choose the best option for their cloud security strategy.

There are four types of Bastion Hosts:

- **Traditional Bastion Host:** In traditional on-premises environments, bastion hosts were typically self-hosted servers placed within a demilitarized zone (DMZ). These servers were designed to act as intermediaries between external users and the internal network. Traditional bastion hosts were often deployed on dedicated hardware or virtual machines, requiring the organization to manage security patches, updates, and maintenance manually. This model was well-suited for environments where cloud-based services were not yet prevalent and where all infrastructure was located on-premises.[4][11]
- **Modern Cloud-Based Bastion Hosts:** With the advent of cloud computing, the concept of bastion hosts evolved to suit the flexibility and scalability of cloud environments. Modern cloud-based bastion hosts are typically deployed within a Virtual Private Cloud (VPC) and are often implemented as scalable, highly available instances on cloud platforms like AWS, Azure, or Google Cloud. Unlike traditional bastion hosts, cloud-based solutions benefit from the automation, elastic scaling, and integrated security features offered by cloud providers. These cloud-native bastion hosts allow organizations to quickly scale their security infrastructure as their cloud footprint grows, while also taking advantage of integrated monitoring, logging, and access control tools offered by the cloud platform. Cloud-based bastion hosts can be automatically scaled based on usage, and can be easily integrated with other security tools and services like identity and access management (IAM), multi-factor authentication (MFA), and security groups.

- **Self-Hosted Bastion Hosts:** A self-hosted bastion host is an instance or server that an organization manually sets up, configures, and manages. This type of bastion host can be deployed on-premises or within a cloud environment and provides the organization with complete control over the configuration, maintenance, and security. Self-hosted bastion hosts are often preferred by organizations that have specific compliance or security requirements or that wish to maintain a high level of control over their infrastructure. However, self-hosting a bastion host comes with the responsibility of handling updates, patches, and ensuring that the bastion host remains secure. For cloud environments, self-hosted bastion hosts are typically deployed as virtual machines (VMs) within a VPC and can be customized to fit an organization's specific needs.
- **Managed Bastion Hosts:** A managed bastion host is a service offered by cloud providers that takes care of the deployment, management, and security of the bastion host for you. Cloud providers, such as AWS, Azure, and Google Cloud, offer managed bastion host services as part of their security toolsets. Managed bastion hosts often come pre-configured with security best practices, such as integration with IAM services, automatic patching, logging, and advanced monitoring. The primary benefit of using a managed bastion host is the reduction of administrative overhead. Organizations can focus on their core operations while relying on the cloud provider to manage the security, availability, and scaling of the bastion host. Additionally, cloud providers ensure that the bastion host is always up to date with the latest security patches, reducing the risk of vulnerabilities.

Table 1: Types of Bastion Host in Summary

Type of Bastion Host	Pros	Cons	Differences
Traditional Bastion Host	- Full control over configuration and security.	- Requires manual management, updates, and security patches.	- Typically self-hosted on dedicated hardware or VMs.
	- Can be tailored to specific compliance needs.	- High maintenance cost.	- Suited for on-prem environments.
	- Can be hosted on-premises or in a private cloud.	- Limited scalability and flexibility.	- Requires significant management effort.
		- Higher risk of human error.	
Modern Cloud-Based Bastion Host	- Easily scalable and highly available.	- May incur higher ongoing costs due to scalability and cloud resources.	- Deployed in cloud environments (VPC).
	- Integrated security tools (e.g., IAM, MFA, logging).	- Requires reliance on the cloud provider.	- Benefits from cloud features such as elastic scaling and integrated security.

	- Automation and elastic scaling capabilities.	- Less control over infrastructure.	- Faster deployment and management.
	- Built-in monitoring and logging services from cloud providers.		
Self-Hosted Bastion Host	- Complete control over deployment and configuration.	- Requires manual management of patches, security updates, and monitoring.	- Manual setup and configuration.
	- Allows for customized security setups.	- High maintenance burden.	- Often deployed on-prem or in a private cloud.
	- Can be deployed in specific environments.	- More complex setup for scaling.	- Suitable for organizations needing high control or custom configurations.
Managed Bastion Host	- Low administrative overhead.	- Less control over infrastructure.	- Cloud-provider-managed solution.
	- Automatically updated with the latest patches.	- Dependent on the cloud provider for security and uptime.	- Pre-configured with security best practices.
	- Integrated with cloud security services (IAM, monitoring).	- Potential higher costs due to the service model.	- Focused on simplifying management and security with minimal user effort.
	- Scalable based on need.		

Each major cloud platform has its own implementation and offering for bastion hosts. Here's an overview of how each platform supports bastion hosts:

Table 2: Major Cloud Platform and Bastion host offerings

Cloud Platform	**Bastion Host Implementation**	**Key Features**	**Access Control & Security**	**Alternative Methods**
AWS	EC2 instance in a public subnet within a VPC	- IAM for access control	- IAM policies for access control	- **AWS Systems Manager Session Manager**

				(Access without bastion host or open ports)
		- CloudWatch for monitoring	- Integration with CloudWatch and GuardDuty for security monitoring	- **Amazon EC2 Instance Connect** (Secure access without SSH key management)
		- GuardDuty for threat detection	- Multi-factor authentication (MFA)	
Azure	**Azure Bastion** (Fully managed service)	- Secure RDP and SSH access	- Integration with Azure Active Directory (AAD) for authentication	- Does not require traditional bastion host setup or open ports for access to VMs
		- Integration with Azure Active Directory (AAD) for authentication	- Logging and monitoring through Azure Monitor and Azure Security Center	
		- No need for public IP on VMs		
Google Cloud	Custom bastion hosts on Compute Engine or **Cloud IAP** (Identity-Aware Proxy)	- Cloud IAP for secure SSH/RDP access	- IAM for access control	- **Cloud IAP** (Eliminates need for traditional bastion host, allowing secure access directly to instances behind the firewall)
		- Traditional SSH-based bastion host configuration	- Integration with Google Cloud's security tools and logging services	
			- Logging through Cloud Logging	

When deciding on the appropriate bastion host solution for a cloud environment, several factors must be considered:

- **Cloud Provider Ecosystem:** If an organization is heavily invested in a specific cloud platform, it is often best to use that platform's native bastion host service (e.g., AWS EC2 Instance Connect, Azure Bastion, or GCP IAP) as it integrates seamlessly with other cloud services like IAM, monitoring, and logging.

- **Security Requirements:** For highly regulated environments or those with stringent security requirements, a self-hosted bastion host might be preferable, as it offers complete control over the configuration and access management. However, for organizations seeking simplicity and automated patch management, a managed solution may be the better option.
- **Cost Considerations:** Managed bastion hosts can be more expensive due to the convenience and integrated services they offer. Self-hosted bastion hosts might be more cost-effective but require additional time and effort to manage and secure.
- **Scalability Needs:** For organizations that anticipate needing to scale their cloud resources quickly, cloud-based bastion hosts (especially managed solutions) are generally more flexible and easier to scale. Self-hosted bastion hosts can be scaled manually but may require additional resources and configuration.
- **Integration with Zero Trust Security Models:** Zero Trust models require that no user, inside or outside the network, should be trusted by default. Bastion hosts can be integrated into Zero Trust models, but it is essential to ensure that bastion hosts themselves are securely configured and access is tightly controlled. Organizations should assess whether using traditional bastion hosts is compatible with their Zero Trust approach or if alternative solutions (such as identity-based access) would be more appropriate.[17][18]

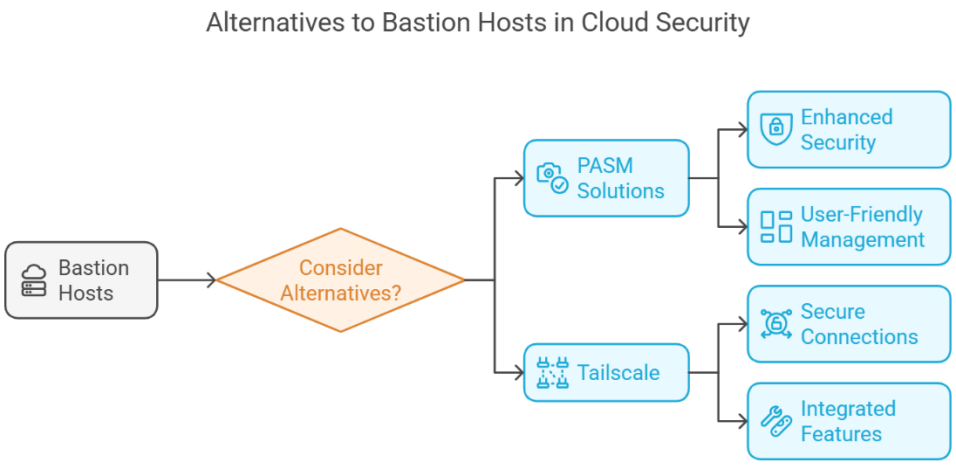
In conclusion, choosing the right type of bastion host depends on several factors, including the cloud platform being used, the level of control and management required, security policies, and the specific needs of the organization. Whether opting for a traditional self-hosted bastion host, leveraging a cloud-based managed service, or selecting a platform-specific solution, organizations should carefully evaluate their cloud security requirements to ensure that the chosen approach enhances the protection of their cloud environment.

While bastion hosts are widely recognized as an effective method for securing cloud environments, they are not the only viable solution. Here are a few alternative approaches that can complement or even replace the need for a bastion host:

- **Privileged Account and Session Management (PASM) Solutions:** PASM solutions provide a more comprehensive approach to managing privileged access across your cloud infrastructure. These tools centralize access control, offer session recording for auditing purposes, and ensure secure password management. PASM solutions can be a safer and more user-friendly alternative to bastion hosts by providing greater visibility and control over privileged access activities.
- **Tailscale:** Tailscale offers a secure, VPN-like connection between your devices and cloud environment, which can eliminate the need for a traditional bastion host. By leveraging mesh networking, it ensures seamless and secure access without the complexity of managing individual bastion host setups. Tailscale also integrates features like access control and automatic key rotation, making it a flexible and modern alternative to traditional bastion host-based approaches.

  These alternatives present different ways to enhance security while potentially reducing the overhead of managing bastion hosts.

Figure 4: Alternatives to bastion hosts



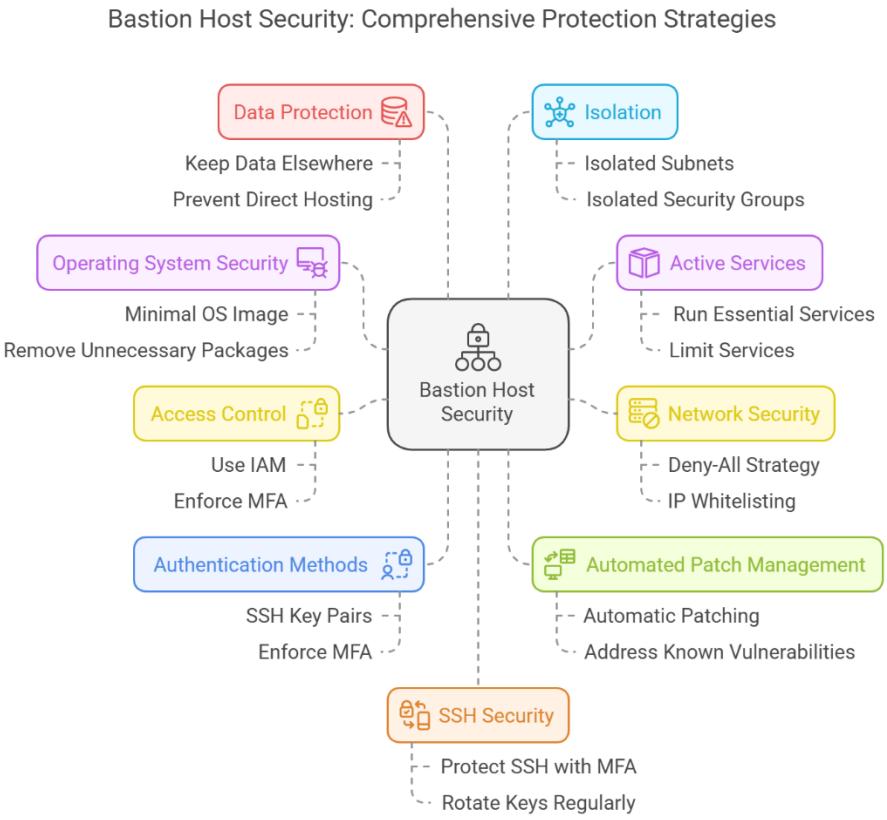
4. Best Practices for Bastion Host Security

To secure bastion hosts effectively, it is crucial to adopt several best practices. First, choose a minimal operating system and remove unnecessary packages to reduce potential vulnerabilities. Only essential services should run, such as the SSH daemon, and regular patching of the operating system and applications is vital. For network security, lock down networking capabilities with a deny-all strategy and restrict access through IP whitelisting or VPNs. Unused ports should be blocked, and network vulnerability scanners should be used to detect potential threats.

Access control is paramount, so limit user accounts and use IAM policies to manage access. Strong authentication methods, including SSH key pairs and multi-factor authentication (MFA), should be enforced. Avoid storing sensitive data on the bastion host and automate patch management to stay ahead of known vulnerabilities.

The bastion host should be isolated in its own security group and subnet, away from direct exposure to the internet. SSH connections must be protected with MFA, and keys should be rotated regularly. Continuous auditing and monitoring are essential for identifying suspicious activity, and access should be restricted to authorized IP addresses. Finally, a solid backup and recovery strategy is crucial in case the bastion host is compromised.[2][1]

Figure 5: Security Measures



5. Conclusion

In conclusion, bastion hosts play a vital role in securing your cloud environment by serving as a controlled and auditable entry point for accessing private instances. They help minimize the attack surface and strengthen your overall security posture.

Key takeaways include choosing the right type of bastion host based on your security needs and the complexity of your environment, whether it's a single-bastion, dual-bastion, or internal bastion host configuration. It's essential to follow security best practices to ensure proper configuration and protection, and leverage available tools and technologies to manage the bastion host effectively. As the cloud security landscape evolves, continuous evaluation and improvement of your security measures, including the bastion host configuration, are necessary to stay ahead of emerging threats.

By implementing these strategies, you can enhance the security of your cloud infrastructure, safeguarding it from unauthorized access and cyber threats.

6. References

1. Karame, Ghassan O., et al. "Securing cloud data under key exposure." *IEEE Transactions on Cloud Computing* 7.3 (2017): 838-849.
2. Jeyachandran, Aravind, and M. Poongodi. "Securing Cloud information with the use of Bastion Algorithm to enhance Confidentiality and Protection." *Int. J. Pure Appl. Math* 118 (2018): 223-245.
3. Karame, Ghassan O., et al. "Securing cloud data in the new attacker model." *Cryptology ePrint Ar*

chive (2014).
4. Amrulla, Goodubaigari, et al. "A Survey of: Securing Cloud Data under Key Exposure." *International Journal of Advanced Trends in Computer Science and Engineering* 7.3 (2018).
5. Nam, Jaehyun, et al. "{BASTION}: A security enforcement network stack for container networks." *2020 USENIX Annual Technical Conference (USENIX ATC 20)*. 2020.
6. Wheeler, David M., Damilare D. Fagbemi, and Jc Wheeler. "Securing the loT Cloud." *The IoT Architect's Guide to Attainable Security and Privacy*. Auerbach Publications, 2019. 115-156.
7. Bauer, Michael D. *Building secure servers with Linux*. " O'Reilly Media, Inc.", 2002.
8. JESSEY, NANDIGUM, and NV KALYANI. "Securing Cloud Data Under Key Exposure." (2018).
9. Nagata, Masaki, et al. "Development of Secure Safety Confirmation System Using Virtual Private Cloud." *2018 Eleventh International Conference on Mobile Computing and Ubiquitous Network (ICMU)*. IEEE, 2018.
10. Kaushal, Deepika. *Bootstrapping a Private Cloud*. MS thesis. Purdue University, 2020.
11. Herath, Pushpa. "Azure Cloud Security for Absolute Beginners."
12. Vora, Zeal. *Enterprise Cloud Security and Governance: Efficiently set data protection and privacy principles*. Packt Publishing Ltd, 2017.
13. Narula, Saakshi, and Arushi Jain. "Cloud computing security: Amazon web service." *2015 Fifth International Conference on Advanced Computing & Communication Technologies*. ieee, 2015.
14. Szefer, Jakub M. *Architectures for secure cloud computing servers*. Diss. Princeton University, 2013.
15. Integrating Identity and Access Management for Critical Infrastructure: Ensuring Compliance and Security in Utility Systems. Suchismita Chatterjee. 2022. IJIRCT, Volume 8, Issue 2. Pages 1-8. https://www.ijirct.org/viewPaper.php?paperId=2412105
16. Suchismita Chatterjee , 2021. "Advanced Malware Detection in Operational Technology: Signature-Based Vs. Behaviour-Based Approaches", ESP Journal of Engineering & Technology Advancements 1(2): 272-279.
17. Mansukhani, Bhupesh, and Tanveer Zia. "The Security Challenges and Countermeasures of Virtual Cloud." *Security Research Centre (SECAU) Conference*. Edith Cowen University, 2012.