An Effective Utilization of Bastion Host Services in Cloud Environment

G. Vijayababu, D. Haritha, R. Satya Prasad

Abstract: ***Now a days the cloud computing offers huge benefits, security issues are major concerns that setback from enjoying the full range of advantages it offers. Bastion Host is specifically designed for network security that is placed on the network perimeter which provides protection in the form of patches, authentication, encryption, and eliminates unnecessary software and services and is a well-known concept. This paper discusses Bastion Host services, types and bastion host in a cloud environment AWS. The Priority Queue method for effective utilization of services is proposed and the results are promising in terms of improving throughput and resource utilization.***

Index Terms: ***AWS, Bastion Host, DMZ, VPC***

I. INTRODUCTION

Bastion Hosts are designed for secure information flow between the public network and a private network. Bastion hosts sit on the network perimeter. It can play multiple roles such as router, DNS, FTP, SMTP, News, and/or Web servers. The responsibility of the network administrator is to identify *the services needed on Bastion host to resist the possible attacks. The Hardening of Bastion hosts allow them to resist attacks from external sources thus protecting the internal network. Hardening involves securing the machine, configuring the required services, installing the necessary patches, controlling the services and protocols, locking the user accounts via modifying the Access Control Lists (ACLs),disabling all unnecessary TCP and UDP ports and running the security audit to establish a baseline. The task of the administrator is to do thorough testing of ACLs and unblocking or blocking the networking application without losing the required features. The usage of limited services reduces the resource utilization and throughput. In the existing systems the overhead of the network administrator is to identify the required services, check their healthiness, installations of required services and uninstallations of rest of the services. The various ways of identifying the required services and their installation, controlling and grouping the services without compromising the resource utilization and throughput are to be explored. Here the focus is on proposing the effective utilization of services using priority queue for the services which are needed. This method helps to reduce the overhead of the administrators, fastens the services and helps to increase the resource utilization and throughput.

Necessity of Bastion Hosts on AWS

Bastion host responsible for allowing access from an external network (Internet for instance) to a private network. As it's placed in a demilitarized zone, it should reduce the chances of infiltration. For instance, when there are Linux instances launched in a subnet of Amazon VPC, bastion host can be used in this environment to lessen the risk of letting in the SSH connections from an external network.

Basically, bastion hosts instances are placed in the public subnet that are invoked using either RDP or SSH. It acts as a jump box or jump server, after the establishment of the remote connection to the bastion host, and then permits to use SSH or RDP to log in to other instances (of the private subnets) in Virtual Private Cloud. Fundamentally Bastion host acts as a bridge between the private and public networks via the internet once configuration is done well with the help of Network ACLs and the security groups. Outside the corporate firewall or the DMZ are the areas where the bastion host is generally hosted. It has the high probability of being accessed by the untrusted computers or internet. However, in some circumstances, it can play a different role such as Email Server, Web server, FTP Server, Proxy Server, DNS Server, Honey pots etc.[1]

II. CHOOSING THE BASTION HOST OFFERED SERVICES

All types of services that a site required to access the Internet or offer to the Internet, services that are not secured providing directly via packet filtering, are provided by Bastion host.

The services which are not meant to access the Internet, should not be installed on a bastion host. For example, if the booting services are provided to the internal hosts, then it leads to compromising the bastion host and corresponding services will be available to the public network.

Services that are provided by the Bastion Host can be classified into four types:

A. Secured Services:

Packet filtering can be used for secured services and if a pure-proxy firewall is used, then the most conventional way of doing so is to use only the bastion host or shouldn't be provided by any means.

B. Insecure services as normally provided but be able to secure

Bastion host can be availed to host such kind of services.

C. Insecure services as normally provided but will not be possible to secure

If, in case, these types of services are certainly needed, only then such services should be provided that too on a victim host (as already discussed) and also should be disabled.

Revised Manuscript Received on May 06, 2019
G Vijayababu, CSE Deparment, JNTUK, Kakinada, India.
Dr.D.Hariha, CSE Deparment, SRKIT, Vijayawada, India.
Dr.R.SatyaPrasad, CSE Deparment, Acharya Nagarjuna University, Guntur, India.

D. **Unused Services or Services which do not work in collaboration with Internet**

This type of services must be disabled.

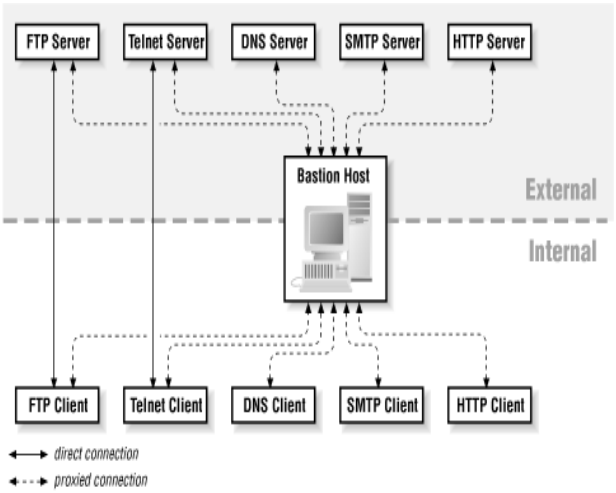

Figure 2.1 Different kind of Internet services can be run on Bastion Host

Electronic mail (SMTP) is one of the basic services provided by bastion hosts. There are some of the information services that the system would want to provide or access such as, File Transfer Protocol Services (FTP), Hyper Text Transfer Protocol Services (HTTP) etc.

Domain Name System (DNS) becomes mandatory to support any of these services (including SMTP).It lies beneath all the other protocols by giving the way to translate the IP addresses to hostnames and hostnames to IP addresses. Apart from that it also provides additional data about the hosts and sites.

Most of the services that are intended for private networks becomes vulnerable to attacks and can be exploited from external network which gives chances to the attacker who can succeed in breaching the security of the bastion host. The services that are not required should be uninstalled and only the required services should be installed.

For the most part, A set of instructions need to be followed carefully to design a hardened bastion host with high degree of security that allows it to provide services to the public network.

MULTIPLE HOSTS Vs MULTIPLE SERVICES

As a best practice, in a single bastion host there should be only one service running at a time. For example, when a web server is needed, configure it on a bastion host. And along with that if an FTP server is also needed then configure it on a separate bastion host. Additionally, if a DNS Server is also needed, then that should be configured on different bastion host. At this point of time, each host is designated for one strong objective. As a result, if there is a problem with one of the services that will not disturb the other services as each one of them are individually placed in different bastion host. Managing the services also becomes easier.

Firstly, this “One-Service One-Bastion host” model clearly demands heavy financial investments. And in fact, most of the services really do not require the dedicated machine. Secondly, it becomes cumbersome to manage multiple bastion hosts. It doesn’t sound good having one firewall when it’s made up of hundreds of individual machines.

That leads to make trade-off between the two types of services (i.e. distributed and centralized)on choosing the right service type. Services can be grouped together into units based on some fundamental principles mentioned below

A. Service segregation based on dependency

If there are services that an organization depends on (like a customer-visible web site) but could live without that service for a while (like an IRC server), that should be configured on a different machine.

B. Service segregation based on the targeted audience

One machine should be dedicated for the services that are used by the in-house users. (for example, staff of the organization) and similarly there should be another machine to host the services that are available for external users (such as clients, customers etc.) and one distinct machine should be allotted for housekeeping services (DNS for instance) that are used only by other computers. Otherwise, in case of an educational organization (such as universities, colleges etc.) services for staff should be hosted on one machine and another one to host the services for the students.

C. Service segregation based on trustworthiness

If the services are identified that they are trustworthy then all such services can be installed together on one machine and all the other services that are not trustworthy on a different machine. Still to be on much safer side, each untrusted service can be put on a separate machine, as they're the ones will probably interfere with other entities.

D. Segregation of services based on data confidentiality

One machine should hold the services that are needed to use the confidential data and the publicly accessible data services should be laid on another machine.

These principles at times will become redundant (insignificant services that are used by a certain user group are not reliable and work only with public data). At some instances, they will be contradicting.

III. MULTIPLE BASTION HOSTS

If all the services that are significant to the private network users(for instance proxy servers, SMTP servers etc.) are handled by one bastion host and the other services which are not important for the private network users (Anonymous FTP server for instance) but delivered to the Internet are handled by another bastion host, then the performance of the services that are used by the private network users will not be brought down by the external users’ activities. [2]

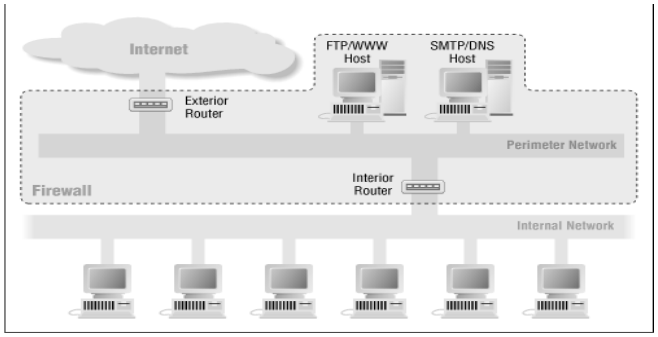

Fig 3.1 Architecture using multiple bastion hosts

For better performance, there can be multiple bastion hosts even though the services are not provided to the public network. Certain resource-intensive services, Usenet news for instance, are effortlessly detached from other. And for the sake of better performance, possibly multiple bastion hosts can also be employed with the same services. However, that can become a challenging task to do the load balancing since it may require lot of services to be configured for such servers. Hence, creating several hosts for individual services works good only if the usage is calculated in advance.

In case, as a fallback system, if the firewall is equipped with surplus bastion hosts where each additional host is enabled to provide the required services on failure of the primary host, on the same firewall, for instance, several bastion hosts are configured and designated either as a DNS servers for a certain domain, or similarly multiple hosts are configured as SMTP servers, or both, so that, if the primary bastion host is down or overburdened, the next available host can take over the DNS and/or SMTP pursuit. Nevertheless, the limitation here is, this approach is supported only by a fewer services

There can be another reason for maintaining; there can also be a security reason for maintaining multiple bastion hosts where the hosts are segregated in such a way that they do not interfere with each other's data set of services. For instance, one HTTP server is dedicated only for the customers across the Internet, and the another one for the rest of all others. Given that two servers, different set of data can be offered to customers. And if the less loaded or more powerful machines are used, then performance can be enhanced further.

To eradicate the probability of one server can be used to compromise the other, it's possible to have two different machines where one machine is to run the HTTP server and the other machine is for running the anonymous FTP server.

IV. BASTION HOST ON AWS

When it comes to the question that is it okay to have Bastion host over the public network with the private instances for remote connectivity obviously answer is yes. The connectivity flowing can be seen in the Figure 4.1 from the end user to required resources on private subnet through a bastion host.

One of the cloud platform services available in the industry is **Amazon Web Services (AWS)** which offers services such as database storage, content delivery, high degree of security and much more which are beneficial to scale up the businesses.

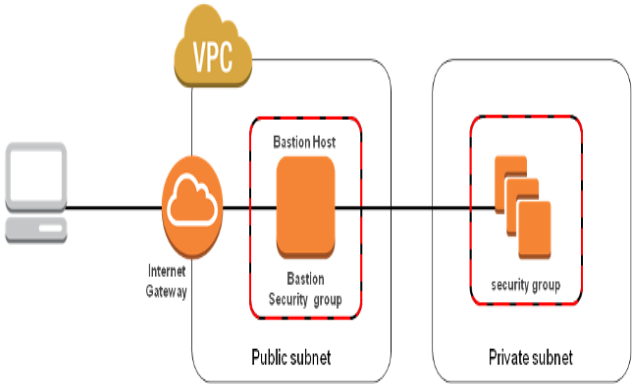

Fig 4.1 Bastion host on AWS

Virtual Private Cloud (VPC) is one of the fabulous services provided by Amazon. Amazon VPC provides an isolated environment where the services can be hosted on a private network and which is can't be access from the public network. Nevertheless, it's possible to communicate with other peers on the same network. This helps to keep the access from intruders from the internet. [3]

One point to remember while planning bastion host for infra of AWS is that it shouldn't be used for any purposes other than what is initially planned for, as that could cause security breach. Instead, investigate toughening the chosen operating system for still more stronger security.

Bastion Host and Screened Subnet

The screened host is added with the additional layer of security by the bastion host when the internal network is isolated from the public network.

The bastion host stands as a shield to protect the internal network from internet attacks. As a result, internal hosts are safe even if an attacker manages to get through the bastion host is maintained out of the way by perimeter network. The measures required to be considered for hardening the bastion host and its configuration.

1) Required ports based on specific services need to be considered and all remaining ports should be closed in a Firewall system.
2) Intrusion detection system (IDS/IPS) such as a snort etc. are maintained.
3) In order to avoid DoS (Denial of Service) attacks, flooding attacks, and spoofing there should be specific security settings.
4) Auditing should be done regularly.
5) Ensures that its software are up to date in the market to cope-up with the growing business demands.
6) Perhaps special kernel security patches are run.
7) Except the admin account, all the other user accounts are locked up.
8) Either the logs are encrypted (SSH) or they are stored in disks.
9) All the other software that are installed by the end user such as MySQL etc. and network servers such as Apache etc. are uninstalled from bastion host

10) For the sake of network traffic and for the network buffers TCP/IP stack will be aligned accordingly.
11) In order to improve the server security /etc/sysctl/conf is customized.

the bastion host acts as proxy server based on the security policy design bastion host allows or rejects the connection.

Elementary steps to create a bastion host in the infrastructure of AWS are:

1) Initially it should Launch an EC2(Elastic compute cloud) instance.
2) Then as per the need OS hardening should happen.
3) Suitable Security Groups should be set up.
4) Implement either the SSH in case of Linux connectivity or RDG for Windows connectivity.
5) Identify all the active Available Zones, which are in use, and install an AWS bastion host in each of the AZ (Availability Zones).

For maintaining the stringent security, the Security Groups play a vital role to make this solution work (More about AWS security groups here. Basically, a Security Group, which is used to permit the bastion host connectivity for the already available private instances, should be created first and the only acceptable inbound requests for that SG should be SSH or RDP from the bastion hosts across AZ (Availability Zones).And this SG should be applied to every private instance which requires connectivity.

Secondly, create a security group to be applied to the bastion host. As far as possible, inbound and outbound traffic should be restricted at the protocol level itself. The inbound rule base should accept SSH or RDP connections only from the specific IP addresses(usually those of your administrators). It is required to avoid allowing wide open access and outbound connection should again be restricted to

SSH or RDP access to the private instances of the AWS infrastructure. An easy way to do this is to populate the 'Destination' field with the ID of the security group you're using for your private instances.

Asymmetric key access is required for authentication purpose over SSH, and RDP connections. If the system in the local network is trying to establish connection with the bastion host that will not be a problem and it is easy to store private keys locally. As soon as connected to the bastion host private keys are needed to log-into the corresponding private instances from it

As recommended by AWS, connections pertaining to Windows instance should be implemented by Remote Desktop Gateway where the Linux instances should be implemented using SSH agent forwarding.

Need of eliminating the private keys on bastion host is eliminated in both the solutions. Along with all other factors, the resiliency and high availability of services should always be considered.

V. RESULTS

Linux Bastion host on AWS

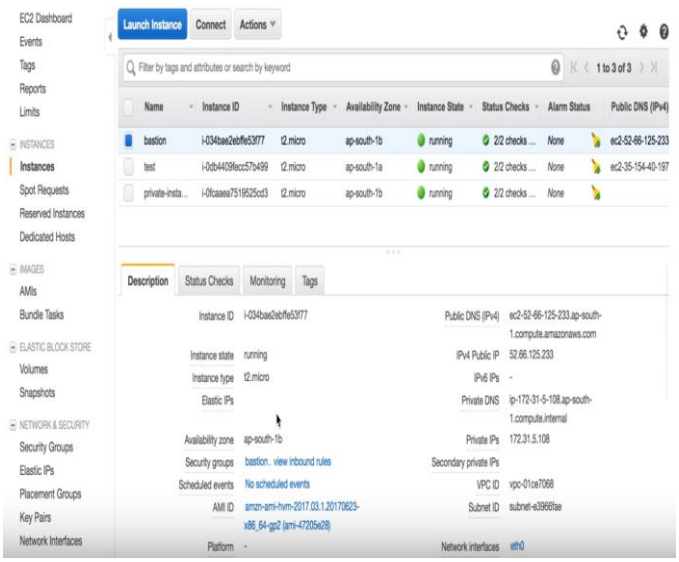

Fig 5.1 Setup Bastion host for SSH forwarding on AWS

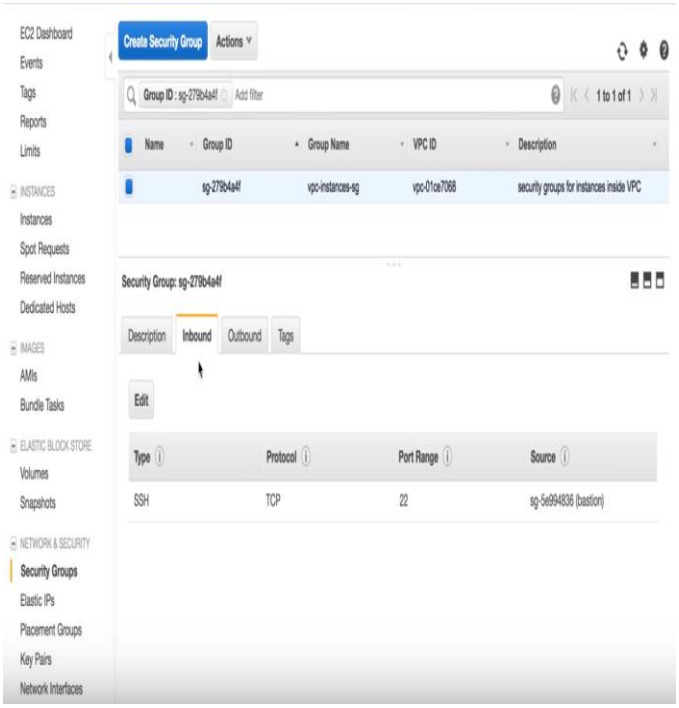

Fig 5.2 Inbound rules for Bastion security group

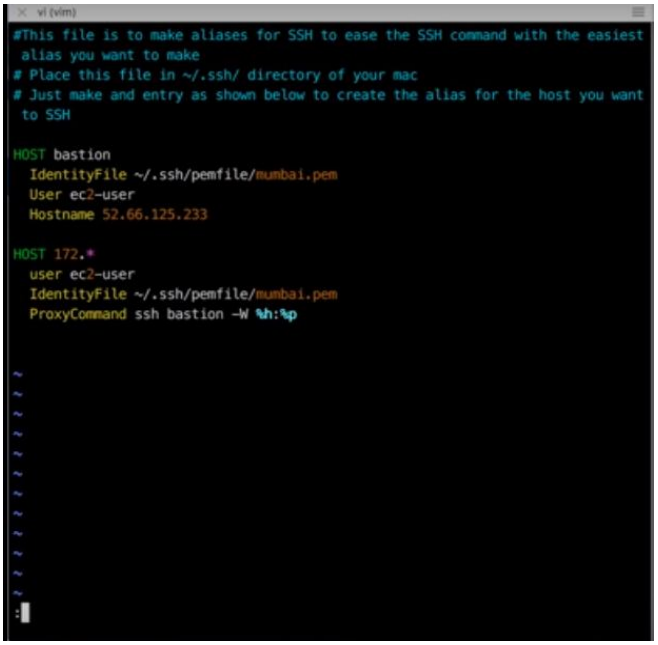

Fig 5.3 Configuring Bastion host

Fig 5.4 An attempt to bypass the Bastion host and permission denied

VI. IMPROVEMENT IN THROUGHPUT

The bastion host is installed with only required services which are decided by the network administrator. Perhaps that can be comprised of proxy applications for SMTP,DNS, POP and HTTP. Detailed audit information is maintained by each proxy by logging. It includes detailed data of the traffic, information of each connection, and the duration of with respect to the connection. [4]

For identifying and handling intruder attacks audit log becomes an important tool.In a firewall configuration there can be multiple bastion hosts. It is preferred to have single service on each bastion host. Depending on the resources and requirements of the site the number of required bastion hosts are calculated. For the sake of better performance same service can be installed on multiple bastion hosts. Only If the usage is predicted in advance then this approach of creating multiple hosts for individual services works effectively. If a service is fixed on a specific bastion host, the machines security can be breached. This problem can be avoided by using multi-homed multiple bastion hosts. This proposal focuses that the logs of multiple bastion hosts can be monitored and can be used to identify the utilization of the services as shown in the figure below.

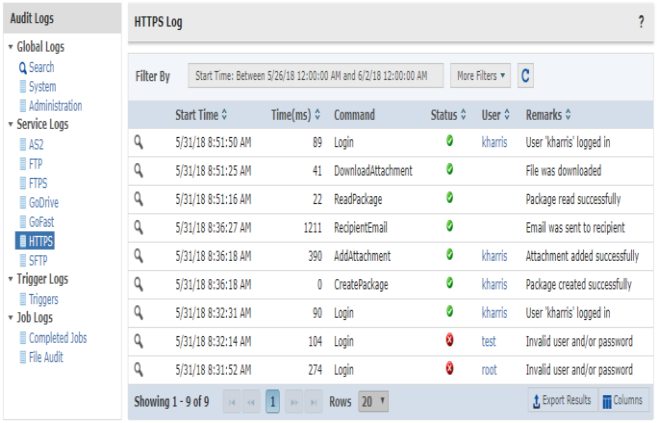

Fig 6.1 Audit log of proxy

After examining the logs of all the proxies with respective to traffic, the services can be prioritized with the help of the priority queue and accordingly the services can be distributed, or multiple bastion hosts can be configured to balance the load automatically. Proxy server which are idle or handles less traffic can be uninstalled temporarily to mitigate the low throughput and the required proxy can be installed in that place which leads to better throughput and resource utilization.

VII. CONCLUSION

This work emphasizes a new method for effective utilization of bastion host services using priority queue for the required services. Incorporating the proposed system of implementing multiple bastion hosts in AWS with priority queue and respective proxy services, will provide better security and more throughput.

REFERENCES

1. Chris Cant &Simon Wiseman, Simple Assured Bastion HostsComputer Security Applications Conference, 1997. Proceedings., 13th Annual
2. Chapman, D. Brentand Elizabeth D. Zwicky, Building Internet Firewalls, Sebastopol CAOReilly&Associates2000
3. https://cloudacademy.com/blog/aws-bastion-host-nat-instances-vpc-peering-security/
4. Oppliger, R., Internet Security: Firewalls and Beyond Communications of the ACM, May 1997.

AUTHORS PROFILE

G.Vijayababu is a Research Scholar in the department of Computer Science and Engineering department, JNTUKakinada. He is working as Sr.Assistant Professorin the Computer Science and Engineering department, SRK Institute of Technology since March 2010. His area of research is Computer networks and Information security.

Dr D.Haritha is working as Professor and Head of the Computer Science and Engineering department in SRK Institute of Technology since May 2008. She has 28 years of teaching experience. She obtained Ph.Ddegree from University of Hyderabad in 2007 for her thesis entitled "Ink and Toner analysis in Questioned Documents using Color Image Processing Techniques". Her research interests include Computer Vision, Network Security and Artificial Intelligence.

Dr R.Satya Prasad is working as Professor in the Computer Science and Engineering department, Acharya Nagarjuna University since Nov 1990.He has 28 years of teaching experience.He obtained Ph.Ddegree from Acharya Nagarjuna University in 2007 for his thesis entitled "Half Logistic Software Reliability Growth Model".He has successfully guided 26 PhDScholars and also published 155 International Journals so far. Hisresearch interests includeSoftware Engineering, Network Security and Image processing.