Short Review Paper

Deployment of bastion host, RED before firewalls to improve security and efficiency

N. Chiranjeeva Rao* **and Shankha De**
Dept. of Computer Science Engg, Bhilai Institute of Technology, Durg, CG, India
raonchiranjeev@gmail.com

Available online at: www.isca.in
Received 10th April 2017, revised 4th July 2017, accepted 15th July 2017

Abstract

Firewalls are one of the most important equipment required to protect the Networks these days. Network threats are on all-time high and upgradation of firewalls is a continuous and ongoing process. This paper aims at suggesting improvements in the firewall performance and improving security by attaching a Bastion host before firewall to reduce threats reaching firewall. It includes the detailed description of a bastion firewall as an External DNS Server and a proxy server. The paper also includes a model of packet filtering which may be used to detect and reject packets at an earlier stage using RED. Thus the number of packets which reach the firewall are lesser as compared to a direct exposure to firewall. These alterations improve the firewall efficiency which is a major requirement in the current scenario.

Keywords: Networks, Firewall, Bastion host, Firewalls efficiency, Firewalls threats.

Introduction

A Bastion Host can be any system which is completely exposed to attacks in any of the networks. This system can be used on the public side of a network before a firewall. Use of Bastion host (Figure-1) improves the security of a system by exposing the Bastion Hostto all the threats instead of a firewall and thus provide a shield for a firewall.

RED or Random Early Detection (Figure-2) is a technology which is used to improve the firewall efficiency by dropping all the unneeded packets at an early stage so that the traffic at the firewall is much lesser compared to a traditional firewall thus improving its performance[1].

The Bastion Host is placed on the public side of a demilitarized zone (Figure-1) and is in an unprotected position without a firewall or a filtering router cover. It thus plays a critical role in securing a Firewall from direct exposure as well as the internal Network.

Configuration of bastion host

Bastion Host as a DNS Server: A Bastion Host can act as an External DNS Server different from an internal DNS Server. All the DNS data can be maintained in a DNS Server placed internally. The DNS server thus placed inside can be configured in such a manner that it can forward all the queries to the Bastion Host (External DNS Server) and vice-versa (Figure-3).

In the above arrangement the traffic instead of coming directly to the internal DNS Server through firewall can be made to pass through Bastion Host. This host can be allowed to pass specific traffic directly to internal DNS server instead of passing through firewall thus improving its efficiency. The firewall can be configured to bypass the traffic for this arrangement. Description of some rules are shown here which needs to be configured in the firewall (also shown in Table format in Table-1). The rules are abbreviated as R1 for rule 1, R2 for rule 2 and so on. All queries meant for Internal DNS Server can be send to the Bastion Host as follows.

R1: All UDP traffic meant for port 53 and above port 1023 for internal DNS server can be send to port 53 and port 1053 of the Bastion Host Server through firewall.

R2: The TCP traffic meant for above port 1023 of Internal Server can be diverted to Port 53 in the Bastion Host bypassing firewall.

R3: UDP packets meant for Port 53 of Bastion host to be diverted to Port 53 or above Port 1023 of the Internal DNS Server through firewall.

R4: TCP packets having the ACK bit set for Port 53 on the Bastion Host are to be diverted to ports above 1023 on the internal DNS server through firewall.

R5: UDP packets targeted for ports above 1023 of the Bastion Host are to be diverted to Port 53 on the Internal DNS Server through firewall.

R6: TCP packets targeted for ports above 1023 on the Bastion Host can be diverted to Port 53 on the Internal DNS Server through firewall.

R7: The UDP packets which have the ACK bit set for Port 53 of the Internal DNS Server can be diverted to ports above 1023 on the Bastion Host bypassing firewall.

R8: TCP packets which have the ACK bit set for Port 53 of Internal DNS Server can be diverted to Ports above 1023 of Bastion Host bypassing Firewall.

Bastion host as a proxy server: A fortified bastion host or a bastion server can be deployed before the firewall, which can help reduce many of the security threats. A bastion host can be laid between the intranet and the internet. All the traffic from the intranet can be directed through Bastion Host thus exposing it to all the possible threats from the internet. Thus by concentrating all the traffic on a server the firewall and the intranet can be protected from direct exposure to threats.

Though the bastion host do not provide any service to the intranet, it receives a request from the internet for an intranet service, which in this case may be a firewall. When Proxy Server Programs are added on the Bastion Hosts, they relay requests to the Internal Server instead of the Firewall. The information thus received from Bastion Host can be diverted to the firewall thus safeguarding it from a direct attack.

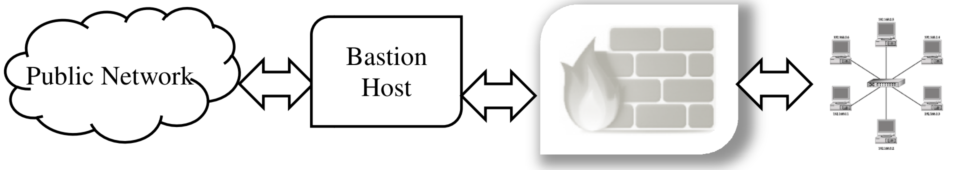

Figure-1: Bastion Host before a firewall.

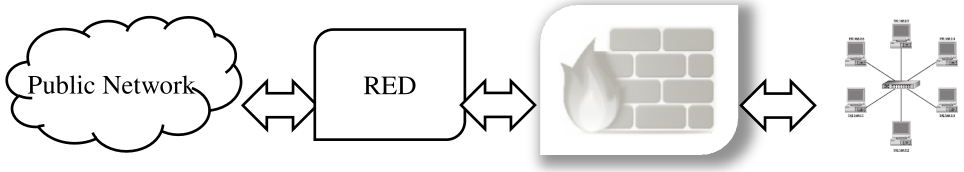

Figure-2: Random Early Detection (RED) before a firewall.

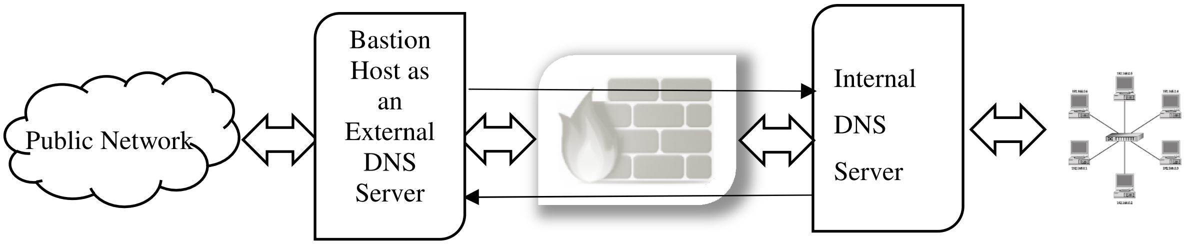

Figure-3: Bastion Host Deployed as an External DNS Server.

Table-1: Description of some rules which needs to be configured in the firewall.

Rules	Directions	Source Address	Destination Address	Protocols	Source Port	Destination Port	ACK flag	Actions
R1	Out	Internal DNS	BH	UDP	53, >1023	53	*	Permit
R2	Out	Internal DNS	BH	TCP	>1023	53	Any	Permit
R3	In	BH	Internal DNS	UDP	53	53, >1023	*	Permit
R4	In	BH	Internal DNS	TCP	53	>1023	Yes	Permit
R5	In	BH	Internal DNS	UDP	53, >1023	53	*	Permit
R6	In	BH	Internal DNS	TCP	53	53, >1023	Any	Permit
R7	Out	Internal DNS	BH	UDP	53	53, >1023	*	Permit
R8	Out	Internal DNS	BH	TCP	53	>1023	Yes	Permit

Thus if any attack takes place it is the bastion host which gets affected and the firewall and the intranet will be safeguarded. Just by resetting the bastion server to its original configuration any major failure can be avoided. In order to make the bastion host secure, the bastion host comprise of the most basic services which can be easily reconfigured. It will not have the complex facilities as DNS Services, Email Services etc.

In order to provide better security, the Bastion Hosts can be placed on a private subnet which further secure the hosts by isolation. Even if an attacker is successful in accessing the subnet, rest of the intranet can stay protected. Another option is to place a filtering router which reviews packets coming from the private subnet by checking authenticity.

Intranet administrators can be alerted if someone breaks the proxy. The bastion host can keep a log of all access to it and could be backed up on a separate machine connected by a serial port. Accessing the log remotely is thus not possible. The administrators can examine the logs for breaking and ensure safety. Monitoring systems with alarms can also be deployed to safeguard the same. Auditing software can be used to check server software for any alterations made by attackers and thus rectify the possibility of any intrusion.

Use of random early detection in firewall for efficiency

Security policy in a firewall contains a set of filtering rules. A set of rules R1, R2, R3 are defined and at any stage if the rules are breached then the packet is not allowed to go further and is rejected. By rejecting a packet early speed of filtrations by firewall can be increased thus improving the intranet speed. Some techniques which may be used are Policy Boolean Expression Relaxation (PBER), Field Value Set Cover (FVSC) and Self Adjusting Binary Search on Prefix Length (SA-BSPL).

Saafa Zeidan and Zouheir Trabelsi came to a conclusion that by increasing the policies in a firewall security, the discarding packets by default deny rule is delayed thus affecting the performance of the arrangement. This is a poor indicator of time consumption in the process of filtering.

To improve performance an RED technique can be used which will reject maximum number of packets at an early stage thus reducing the time consumed in filtering. FVSC and PBER can be used to evaluate and to adapt to the traffic dynamics thus improving early rejection. Next technique SA-BSPL use property of Splay Tree Data structure to change the behavior of traffic dynamically. The last accessed node is root of the Splay Tree. Packet rejection can be done at an early stage by putting the minimum node close to that of the root. PBER and FVSC present some such algorithms which can be used to maximize the rejection of packets at an early stage. These are those packets which are not needed and thus improve the speed and efficiency of a firewall. Binary Search can also be applied on the prefix length for every policy-field which have a* dynamic Splay Tree data structure. It also maintains the minimum node of Splay Tree at a very high level such that the packets are rejected earlier.

Conclusion

This paper, proposes a firewall with an enhancement so as to improve its efficiency and Security. The first method was using a Bastion server for security management. Two types of bastion hosts deployments were discussed. In the last part, use of RED for improving firewall efficiency was discussed. This model can be used to reject the traffic which is unwanted at the initial (early) stage and thus improve the performance of the firewall. This model is also very useful for traffics of high rejection rates. In the future work, improvement in the mathematical model of RED and better deployment techniques of Bastion host, Honey Pots can be considered.

References

1. Zeidan Safaa and Trabelsi Zouheir (2011). A Survey on Firewall's Early packet rejection techniques. International Conference on Innovations in Information Technology, IEEE, 203-208.
2. Hamed H., El-Atawy A. and Al-Shaer E. (2006). Adaptive Statistical Optimization Techniques for Firewall Packet Filtering. Proceeding of IEEE INFOCOM, 1-12
3. Al-Shear E., El-Atawy A. and Tran T. (2009). Adaptive Early Packet filtering for Defending firewalls against DoS Attack. Proceeding of IEEE INFOCOM, 1-9.
4. Taluja Sachin, Kumar Verma Mr. Pradeep and Lal Dua Rajeshwar (2012). Network Security Using IP firewalls. *International Journal of Advanced Research in Computer Science and Software Engineering*, 348-354.
5. Ganesh Ashwin, Sudarsan Anirudhan, Vasu Krishna Ajay and Ramalingam Dinesh (2014). Improving Firewall Performance by Using A Cache Table. *International Journal of Advances in Engineering & Technology*, 7(5), 1594-1607.
6. Zwicky Elizabeth D., Cooper Simon and Chapman Brent D. (2000). Building Internet Firewalls: Internet and Web Security. 2nd Edition, O'Reilly Media, Inc. ISBN: 1-56592-871-7.
7. Stalling William (2011). Cryptography and Network Security: Principles and Practice. Pearson Education, 5th edition.