10-2019

Can Routers Provide Sufficient Protection against Cyber Security Attacks?

David Leal

Sanjeev Kumar

Scientific Research Publishing

Journal of Information Security, 2019, 10, 302-310
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Can Routers Provide Sufficient Protection against Cyber Security Attacks?

David Leal, Sanjeev Kumar*

Cyber Security Research Lab, Department of Electrical/Computer Engineering, The University of Texas Rio Grande Valley, Edinburg, Texas, USA
Email: sj.kumar@utrgv.edu, *sjkumar1@ieee.org

How to cite this paper: Leal, D. and Kumar, S. (2019) Can Routers Provide Sufficient Protection against Cyber Security Attacks? *Journal of Information Security*, **10**, 302-310.
https://doi.org/10.4236/jis.2019.104017

Received: June 9, 2019
Accepted: October 28, 2019
Published: October 31, 2019

Abstract

Nowadays many devices that make up a computer network are being equipped with security hardware and software features to prevent cyber security attacks. The idea is to distribute security features to intermediate systems in the network to mitigate the overall adverse effect of cyber attacks. In this paper, we will be focusing on the Juniper J4350 router with the Junos Software Enhanced, and it has security-attack protections in the router. We are going to evaluate how the Juniper router with built-in security protections affected the overall server performance under a cyber security attack.

Keywords

Denial of Service (DOS) Attack, TCP/SYN Flood Attack, Policies, Trusted Zones, Untrusted Zones

1. Introduction

Cyber security attacks have become one of the biggest problems these days. Many research works have been done [1]-[14] to highlight security vulnerabilities of systems and servers as impacted by Cyber Security attacks. As a result, an increasing amount of security hardware and software mechanisms are being deployed onto computers and servers. However, this approach is found to consume a lot of computer resources, which in turn results in overall slowdown of the computer system and slow communication.

Besides computers, more security features are being added to Internet devices such as routers. When configuring the security of the router's built in firewall, there are two questions that most people consider "What kind of changes can we make to the network using the router?" and "How will the changes made using the router affect the performance of the network?" For this paper, we investigate

the security features of the Juniper J4350 router [12]-[19] and to find out how increasing the security offered by the Juniper J4350 router affected the connection rate supported by the web server under cyber security attack. To understand the effect, we created a benchmark scenario where we used server without the router and compared its performance with another scenario where the server was connected to the router with security enabled at the router. In Section 2, we discuss the security attack used in this experiment, and we explain how the TCP/SYN attack worked to affect the performance. We also explain the security features of the router to protect the network and how they prevent hackers from affecting the network. In Section 3, we discuss the experimental setup to test the security setting of the router's firewall and how it affected the connection rate of the users that are trying to communicate with the web server. This was done by using two different network configurations, one of which didn't deploy the router, whereas another configuration used the router with security deployed on it to prevent the security attacks from arriving to the web server. In Section 4, experimental results are presented and compared for two scenarios to show how effective the router's security was for the network, and Section 5 presents conclusion of the paper.

2. Background Information

When setting up the configuration of many devices manufactures tend to put a recommended setting to be considered in a default mode which would be an optimized setting for new users to use in the lack of a customized configuration. Most people that are not very familiar with security configurations and not sure what various protections would be offered and whether they really needed a protection, end up putting more security than they really needed. In most cases, having more security may sound good, but is the extra security worth which comes at the expense of exhausting more of the router's resources. For this section, we will discuss the router configurations and what protection the router's security offers against a common TCP based cyber-attack [13]-[22].

2.1. TCP/SYN

The DDoS attack that was used for router's evaluation in this paper was the TCP/SYN flood attack, which is where the attacker prevents the completion of the 3-way handshake needed for successful establishment of an end to end connection at the layer-4 of the TCP/IP protocol stack [13] [14] [15] [16]. 3-way handshake is shown in **Figure 1**.

The 3-way handshake is a method for two end to end computers to first establish a connection before data traffic is sent between the computers as shown in **Figure 1**. The 3-way handshake starts with the client sending a TCP packet to the server, with the SYN flag set, which is like the computer asking if the sever can have a connection with the client. The server then replies with a TCP packet that has SYN + ACK flags set where the ACK is the server saying that it can

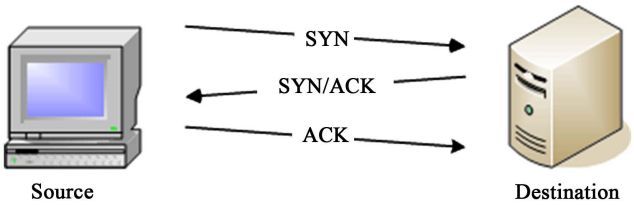


Figure 1. Client-server three-way handshake.

make a connection with the client, and the SYN is the server making sure if it can make a connection with the client. Then the client responds with a packet that has an ACK flag set confirming the establishment of a connection with the server shown in Figure 1. Data exchange between client and server follows the 3-way handshake is completed. In case of the TCP/SYN flood attack, the attacker sends only the packets with the SYN flag set and never completes the 3-way handshake. The server never receives the final ACK packet in response to the SYN-ACK packet sent in the second portion of the handshake. This creates half-open connections at the server that waits for the final ACK response to arrive until it times out. This incomplete 3-way handshake is shown in Figure 2.

When the attacker creates these half-open connections, it consumes the server's resources, and hence interrupts legitimate users from being able to create successful connections with the server.

2.2. TCP SYN-Proxy Protection

One of the features offered by the Juniper J4350 Router's built-in security features is to provide DDoS protections and to help mitigate TCP/SYN flood attacks. One of the commonly used SYN-Proxy protections [10] [11] [12] [13] allows the user to set a threshold on how many half-open connections can pass through the router before its SYN-Proxy protection is activated. When the number of half-open connections exceeds a pre-set threshold value then according to router's SYN-Proxy security protection mechanism, the router terminates clients-to-server connection, and creates a separate TCP connection between itself and the network to make sure that the 3-way handshake is completed for legitimate connections. If the TCP connections are legitimate, then the router establishes the connections with the server. However, if the three-way handshake is not completed between the router and the client then the half-open connection is dropped before even reaching the server.

3. Experiment Set up

For the experiment, we configured the Juniper J4350 router with Junos Software Release [9.2R1.10] (Export edition) Enhanced Services OS Junos in a star topology network as seen in Figure 4, and used Category 6 Ethernet cables to connect all the network devices.

Apple iMac Pro Server was used as an attack target, which deployed an Intel Xenon 2.8 GHz quad-core processor with a 12 Giga Bytes of RAM, and Microsoft

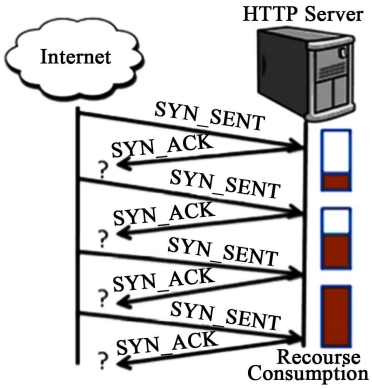


Figure 2. TCP/SYN flood attack [13].

WINDOWS 2012 Enterprise R2 server. TCP/SYN flood attack traffic was measured in the range of 0 Mbps (baseline) to 1000 Mbps with increments of 100 Mbps with randomly sourced IP addresses. The firewall was enabled by default on the target Windows server.

3.1. Scenario 1: Baseline Configuration and Server Performance without Router

For baseline configuration, we directly connected (**Figure 3**) the attacker's network (shown as Untrusted network) and the legitimate client's network (shown as Trusted network) with victim server using a Linksys SRW2024, a 24-port Gigabit Switch that had no firewall. This helped to establish a baseline for the number of legitimate connections that could be supported directly by the server under attack conditions of various magnitudes and in the absence of security protection provided by the Juniper Router J4350.

3.2. Scenario 2: Network Configuration with Router's Security Protection Enabled

Juniper router J4350 was configured using the company's specifications [17]-[22] and was deployed in the network as shown in **Figure 4**. The router was configured as stateful firewall for monitoring and filtering per connection basis instead of per packet basis. Having the router in Stateful configuration allowed us to create trusted and untrusted zones, configure the firewall and configure policies to control how different zones interacted with each other. A baseline of 10,000 client's connections per second was used to evaluate server performance under no attack conditions. In this experiment, the attacking network was simulated to use one port of the router to send TCP/SYN based DDoS traffic using random IP addresses whereas legitimate client traffic used another port of the router to be routed to the server. The router port (port 3) serving the target server contained a mix of traffic from legitimate connections and the attack traffic and hence simulating an attack condition experienced by the target server. The deployed router also implemented security protections which prevented the TCP/SYN based DDoS traffic from reaching the target server.

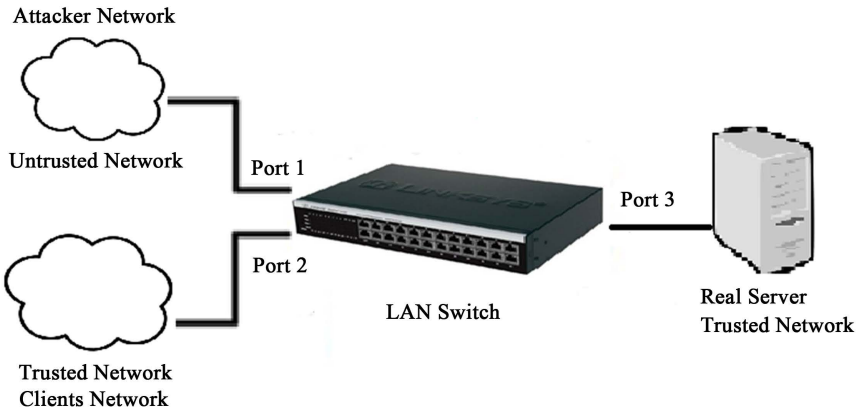


Figure 3. Baseline experimental setup for server without router's security protection in the network (a switch was used instead).

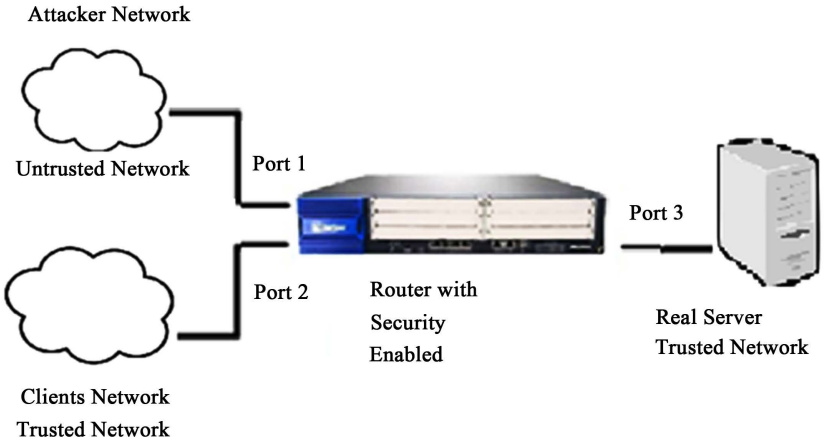


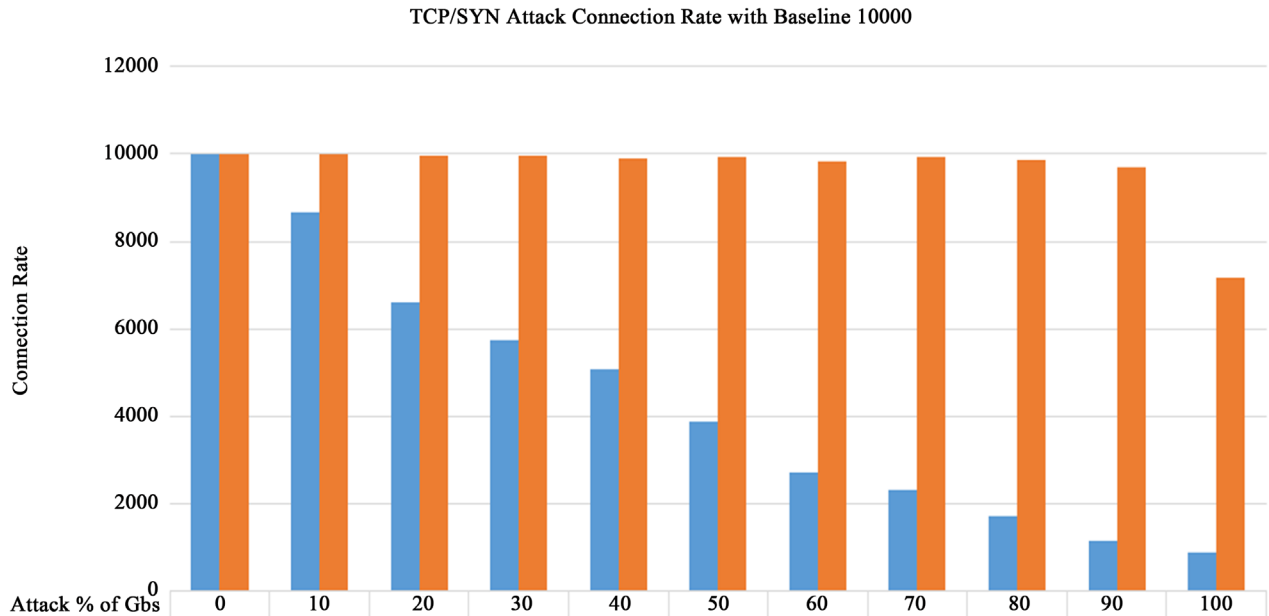
Figure 4. Experimental setup for router with real server.

4. Experimental Results and Discussion

In this experiment, we measured the performance under two scenarios as mentioned below to understand the effectiveness of security provided by the router with built-in protection mechanisms against TCP/SYN based DDoS attacks.

Scenario 1: Under this scenario, there was no Juniper router (and hence no protection mechanisms) deployed (Figure 3) in the network. Instead, a switch was deployed with no built-in security, and all legitimate and attack traffic were allowed to pass through the switch to the target server. The target server deployed only its default protection mechanism provided by the host-based firewall. The target server didn't deploy any additional intrusion prevention mechanisms to defend against DDoS attacks. Under this scenario, we measured the number of legitimate client connections that could be established by the end server under the attack conditions (Figure 5).

Scenario 2: Another scenario was established as shown in Figure 4, where the Juniper router (instead of a LAN switch) was deployed with its security mechanisms to prevent against the DDoS attacks. Under this scenario, we again measured the number of legitimate client connections that could be established by the



Attack % of Gbs	0	10	20	30	40	50	60	70	80	90	100
Real Server with Router	10000	8674	6619	5729	5079	3893	2728	2307	1715	1162	900
Real Server no router	10000	9984	9958	9954	9909	9914	9842.5	9945	9878	9707	7155

Figure 5. Legitimate connection rate with and without router's attack prevention efforts.

end server under attack conditions (Figure 5).

Under both scenarios, the TCP/SYN based DDoS attack was used in the range mentioned earlier and the impact on the legitimate client connection was measured at an increment of 10% of maximum link capacity. Figure 5 shows the comparative result under two scenarios as mentioned above. The number of legitimate client connections established under Scenario 1 was shown in orange in Figure 5. Whereas the number of legitimate client connections established under Scenario 2 was shown in blue in Figure 5.

Based on comparative results in Figure 5, it can be noticed that as the attack was increased, we can notice the difference in the number of legitimate connections that was established with the server under two scenarios *i.e.* when a switch was deployed (without router's security protection in Scenario-1), and another with protection available at the intermediate system (Scenario-2), when the Juniper router was used with its security features enabled.

Interestingly and counter intuitively, the number of legitimate connections established with the server was found to be higher in Scenario-1 when no security mechanism to prevent the attack traffic was deployed. In this Scenario-1, there was no router (with its built-in security) checking all connections for being malicious. On the contrary, when the Juniper router was deployed with its security enabled to mitigate cyber-attacks, it was found that the router was dropping more of the good connections from the clients when it was attempting to prevent more attack traffic from reaching the server. In effect for this network, the router became a bottleneck and more legitimate connections were affected when the attack traffic increased. With the increase in the attack traffic, the router with

its security checking mechanism appeared to be busier dropping the malicious traffic, which in turn also slowed down the legitimate traffic from reaching the server. The collateral damage to the legitimate traffic was very high (**Figure 5**) when the attack traffic load was high in this case of good faith attempt by the router to protect against the malicious attack traffic.

It was obvious that most of good connection loss was happening at the router when we compare the situation with the scenario-1 where a switch was deployed instead. In Scenario-1, the router was replaced with a 24-port Gigabit Switch that had no firewall. This allowed both, the legitimate clients traffic and the DDoS attack traffic to reach the real target server. It was possible that the server may have had some built-in prevention mechanism against TCP/SYN based DDoS attack as shown in previous publication [8], which may have helped the target server support more of legitimate traffic without allowing the attack traffic to do much damage.

5. Conclusion

Based on the results obtained from the TCP/SYN Flood attack experiments that were simulated in this paper, we observed that by having extra security and attack prevention mechanism on a Juniper J4350 Router was beneficial in preventing attack but it also becomes a bottleneck to the network performance in the sense that it was also slowing down the connection rate for the legitimate traffic. It was observed that most of the connection slowdown was happening at the Juniper router. This became clear when we removed the router with a 24-port Gigabit Switch that had no attack prevention mechanism, and most of the defense was limited to the end system, which was using the operating system from Microsoft *i.e.* "MICROSOFT'S WINDOWS 2012 ENTERPRISE R2" server. This showed that even though the Juniper router had a built-in attack prevention mechanism, the router itself became a bottleneck due to excessive resource taken to stop the security attacks and hence affecting the overall good legitimate web connections.

Acknowledgements

This research work is based upon work supported in part by US National Science Foundation and Lloyd Bentsen Jr. Endowment fellowship.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Gunnam, G. and Kumar, S. (2017) Do ICMP Security Attacks Have Same Impact on Servers? *Journal of Information Security*, **8**, 274-283. https://doi.org/10.4236/jis.2017.83018

[2] Kumar, S. and Gomez, O. (2010) Denial of Service Due to Direct and Indirect Attacks in LAN Environment. *Journal of Information Security*, **1**, 88-94. https://doi.org/10.4236/jis.2010.12010

[3] Kumar, S. (2006) PING Attack—How Bad Is It? *Computers and Security Journal*, **25**, 332-337. https://doi.org/10.1016/j.cose.2005.11.004

[4] Sundar, K. and Kumar, S. (2016) Blue Screen of Death Observed for the Microsoft's Server 2012 R2 under Denial of Service Attacks. *Journal of Information Security*, **7**, 225-231. https://doi.org/10.4236/jis.2016.74018

[5] Kumar, S. and Gade, R. (2015) Windows 2008 vs. Windows 2003: Evaluation of Microsoft's Windows Servers under Cyber Attacks. *Journal of Information Security*, **6**, 155-160.

[6] Baez Jr., R. and Kumar, S. (2014) Apple's Lion vs. Microsoft's Windows 7: Comparing Built-In Protection against ICMP Flood Attacks. *Journal of Information Security*, **5**, 123-135. https://doi.org/10.4236/jis.2014.53012

[7] Surisetty, S. and Kumar, S. (2012) Microsoft's Windows 7 vs. Apple's Snow Leopard: An Experimental Evaluation of Resilience against Distributed Denial of Service (DDoS) Attacks. *IEEE Security and Privacy*, **10**, 60-64. https://doi.org/10.1109/MSP.2011.147

[8] Kumar, S. and Petana, E. (2008) TCP Protocol Attacks on Microsoft's Windows XP-Based Computers. *International Conference on Networking*, April 2008, 238-242.

[9] Kumar, S., Valdez, R. and Gomez, O. (2006) Survivability Evaluation of Wireless Sensor Networks under DDoS Attack. *International Conference on Networking*.

[10] Kumar, S. (2005) Impact of Distributed Denial of Service (DDoS) Attack Due to ARP-Storm. The Lecture Notes in Computer Science, Springer-Verlag, Berlin. https://doi.org/10.1007/978-3-540-31957-3_113

[11] Surisetty, S. and Kumar, S. (2010) Is Apple's iMac Leopard Operating System Secure under ARP-Based Flooding Attacks? *International Conference on Internet Monitoring and Protection*, Barcelona, 9-15 May 2010. https://doi.org/10.1109/ICIMP.2010.30

[12] Gade, R., Vellalacheruvu, H. and Kumar, S. (2010) Performance of Windows XP, Windows Vista and Apple's Leopard Systems under a DDoS Attack. *International Conference on Digital Society*, St. Maarten, 10-16 February 2010, 188-191. https://doi.org/10.1109/ICDS.2010.39

[13] Kumar, S. and Sekhar, R. (2011) Experimental Evaluation of Juniper Network's Netscreen-5GT Security Device against Layer 4 Flood Attacks. *Journal of Information Security*, **2**, 50-58. https://doi.org/10.4236/jis.2011.21005

[14] Vellalacheruvu, H.K. and Kumar, S. (2011) Effectiveness of Built-In Security Protection of Microsoft's Windows Server 2003 against TCP SYN Based DDoS Attacks. *Journal of Information Security*, **2**, 131-138. https://doi.org/10.4236/jis.2011.23013

[15] Eddy, W.M. (2006) Defenses against TCP SYN Flooding Attacks. *The Internet Protocol Journal*, **9**. http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-34/syn-flooding-attacks.html

[16] Juniper Networks, Inc. (2008) Attack Detection and Defense Mechanisms. http://www.juniper.net/techpubs/soft-ware/screenos/screenos5x/ce_v4_5_0.pdf

[17] JUNOS® Software Security Configuration Guide. https://www.juniper.net/documentation/software/junos-security/junos-security10.1

/junos-security-swconfig-security/junos-security-swconfig-security.pdf

[18] Security Configuration Guide for J-Series Services Routers and SRX-Series Services Gateways PDF. http://www.juniper.net/techpubs/software/junos-es/junos-es92/junos-es-swconfig-security/junos-es-swconfig-security.pdf

[19] JUNOS® Software J Series Services Routers Hardware Guide. http://www.juniper.net/techpubs/hardware/junos-jseries/junos-jseries96/junos-jseries-hardware-guide/j-series-hardware-guide.pdf

[20] Junos® OS Ethernet Interfaces Configuration Guide. http://www.juniper.net/techpubs/en_US/junos12.3/infmation-products/topic-collections/config-guide-network-interfaces/book-config-guide-network-interfaces-ethernet.pdf

[21] J-Series Services Router Quick Start. http://www.juniper.net/techpubs/software/jseries/junos85/jseries85-quick-start/publications-list.html

[22] Juniper Router Guide. http://www.juniper.net/techpubs/software/junos-security/junos-security10.0/junos-security-admin-guide/junos-security-admin-guide-TOC.html