Bachelor's thesis

Degree Programme in Information Technology

NINFOS 13

2017

Väänänen Ossi

Chang Liu

INVESTIGATING NETWORK SECURITY THROUGH FIREWALL UTILITIES

CASE: CISCO ASA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology

2017 | 46

ChangLiu

INVESTIGATING NETWORK SECURITY THROUGH FIREWALL UTILITIES

- CASE OF CISCO ASA

Firewalls are important components of any system for information security as they are the initial line of defense against attacks on security. This thesis explores the network security component through the use of firewalls and their features. All enterprises make use of firewalls as these systems function to provide enterprises with an adequate level of safety against attacks and damages. Firewalls are secure, however, it is possible to make them even more secure through using timely implementation and secure databases. This thesis discusses the case of CISCO ASA implementation with regard to an enterprise. It can be concluded that firewall systems especially CISCO ASA, when appropriately implemented, result in offering good security for networks in many cases of attacks.

KEYWORDS:

Network security, Firewall. DDoS

TABLE OF CONTENTS

FIGURES

LIST OF ABBREVIATIONS

IP	Internet Protocol
ACL	Access Control List
IPS	Intrusion Prevention System
UTM	Unified Threat Management
VPN	Virtual Private Network
MSP	Managed Service Provider
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
IDS	Intrusion-Detection System
ICMP	Internet Control Message Protocol
DoS	Denial of Service
DNS	Domain Name System
DDoS	Distributed Denial of Service
SYN	Synchronize
ACK	Acknowledgement
TCB	Transmission Control Block
QoS	Quality of Service
CPU	Central Processing Unit
NIC	Network Interface Controller
VSG	Virtual Security Gateway
XML	Extensible Mark-up Language
API	Application Programming Interface

1 INTRODUCTION

The first defense line of any information system against security threats is a firewall. One factor which concerns the network users is the bad connectivity inside the network and to outside destinations and the quality of network performance. The strict settings of security result in a weak network performance and the permanently strict settings make the network performance weaker. When evaluating the effectiveness of network security, assessing the firewall platforms and their impact on network performance is very crucial.

An enterprise network can only be called secured when it is secured against any threat, which might corrupt the whole network. Due to this, securing the network is one of the most important components to do. Internet-based work has increased over the last few decades. A lot of work is required in order to make the network safe and secure for work. In order to develop a secured network, the network administrators must have an excellent knowledge of the type of attacks a network may be subject to. As each attack is different, the mitigation technique used by the administrator of the network impacts the overall network. The network administrator identifies the vulnerabilities that need to be secured by risk analysis. It helps them to build a strong and secured network as they have all the information about the risks. After this, the security policies are made for providing necessary information to network users and high security.

The secondary aim of this thesis lies in exploring a secured network for an enterprise which is able to prevent the enterprise network from all threats. The thesis contains information about the different attacks and explains their mitigation techniques. It describes the various approaches of performing risk analysis and the significance of security policies.

There is also specific focus in this thesis on the attack types related to DDoS. DDoS is a distributed denial of service and a kind of attack of DOS wherein several systems are compromised and this, in conjunction with the application of Trojans, is utilized for targeting an individual system which causes a service denial attack. This type of attack is a serious type of attack and causes a failure of network security by disabling the firewall.

The primary aim in this thesis lies in investigating the security of network through utilities in firewalls. The research will focus on the various types of attacks and strategies to mitigate the same. Through the case study, it becomes possible to investigate the primary aim.

The research will focus on answering the following questions:

- What is the significance of performance analysis delivered by firewalls in an enterprise?

- What potential risks and attacks encourage the enterprise to adopt firewall systems and what is basis of selection?

- How can concepts of risk analysis and attack mitigation to be applied to ensure maximum success in terms of network security for an enterprise?

There are several chapters in this thesis. The current chapter is the first introductory chapter which highlights the significance of this research, the purpose, the objectives and aims along with the research questions investigated. The second chapter is a literature review chapter in which information from referential sources has been brought together. The reference material available or secondary data collected in the second chapter has played an essential role in formulating the conclusion of this research. Third chapter is the research methodology in which the case study research significance has been highlighted. The third chapter provides information on several data collection techniques and the most appropriate for this

thesis. The fourth chapter is the case study discussion and analysis and the final chapter consists of the concluding remarks.

2 EVALUATION OF FIREWALLS AND RESEARCH

A firewall is a device offering network security which is responsible for granting or rejecting the access over network when a flow of traffic happens between a trusted region and an untrusted area over the web. The firewall is responsible for acting as a point of demarcation or a traffic warden within the network as every communication needs to flow from it and this is the area where traffic is given access or access is rejected (Wu and Shan 2011, 1). Access controls are enforced through firewalls using a model for positive control stating that only the defined traffic within the policy of firewall is permitted over the network but the remaining traffic is not allowed.

There has been a major evolution of firewall technology for maintaining pace with the continuously changing needs of security. Major difficulties can be faced in envisioning a world in the absence of firewalls. Established initially as an approach to allow or restrict external accessibility to specific resources of the network, current capability is enjoyed by firewalls to enforce policies of network security, internet activity of logging and security of business exposure to external threats (Kaur and Rao 2014, 1). Firewalls can be identified as extremely effective to support strong authentication of users, enforce policies of network society and activity of internet based logging. Companies consider the utilization of firewalls as the defense of network perimeter for making efficient decisions of security and protecting all hosts from external attacks on private networks. From this point, the firewall of an organization ends up becoming the sole zone of risk from the attacks on internet, while hosting the safety of internet-based work. However, firewalls are not effective in protecting the hosts in connection with internet network without being involved with the enterprise firewall (Jadhav and Agrawal 2013, 4). The use of internet connection without any reliability upon the infrastructure of a company results in exposing the user or host to any specific attack. Firewalls end up offering weak

protection against threats or unknown attacks, such as Trojans or malware. However, a firewall can be successful in complementing anti-virus solutions with the dynamic settlement of new rules on the basis of malware. Even though deployment of firewalls can take place as hardware and software appliances, these systems have the ability of performing real-time introspection of network traffic without affecting any throughput (Budka et al. 2014, 7). A major combination of rules consistently filtering packets of data finally affects the performance of network further causing bottlenecks. In the future, firewalls should be differentiating between illegitimate and legitimate traffic for identifying and plugging new threats automatically. The capabilities of anti-malware scanning are not beyond the firewalls capabilities in the current era, but the present performance of network affects the crucial needs of running an enterprise.

2.1 Access control units

Initially, the function of firewall was performed through the ACLs Access control lists (ACLs). These often exist in routers.

Essentially, ACLs are rules written out for determining whether the access to network needs to be given or not for a particular address of Internet Protocol (IP).

An ACL, for example, could have a line stating that every traffic from 172.168.2.2 IP should not be granted access and so on (Vasu et al. 2014, 16). There is an advantage associated with these ACLs because of their higher performing ability and scalability but they do not have the ability to read past the headers of packet which only provides information of rudimentary nature over the traffic (Rhodes-Ousley 2014, 12). Therefore, the packet filtering of ACL itself does not have the capability of keeping threats away from the networking systems.

2.2 Proxy-based firewall systems

Proxy-based firewall systems are responsible for acting as middleware as they are able to accept every request of traffic coming within the network. This is done by the system through real traffic recipient impersonation across the network. After inspecting if the system decides on granting access. Then the firewall proxy sends the data to the recipient computer (Kaur and Rao 2014, 1). The reply of the destination computer then is then sent towards the proxy which in turn repackages the data with the proxy server source address. With this process, it becomes possible for the proxy firewall to stop the connection taking place between two devices so as to ensure that it is the key machine over the networks talking about the external world (Kaur and Singh 2014, 5). These firewalls can indulge in completely inspecting content and making decisions of granting access depending upon the information's granular level and specificity. Such a nuance is attractive for network administrators but every application requires its individual proxy at the level of application (Jadhav and Agrawal 2013, 4). Networks with proxy firewall further suffer degraded performance of traffic and various limitations within the support of application and generalized functions. This leads ultimately towards issues of scalability which makes it easy to implement the pull-offs. For such reason, this type of firewall is not adopted by many people. As a matter of fact, even though proxy firewalls are popular, the issues of scaling and performance caused limit the desire of adopting them.

2.3 State-full inspection firewall

Inspection of network through state-full inspection firewall types is generally considered as firewalls of third generation. Such a filtering has two characteristics. Firstly, it engages in classifying the traffic through viewing at the port of destination. Secondly, it has the capability of tracking the range of traffic by ensuring that every

interaction is being monitored. This takes place for each connection particularly until there is closure of the connection (Chen et al. 2014, 13). Such properties further result in adding functionality for the access of control. These firewalls further have the ability to grant or reject the access not only over port or protocol but also over the history of packets in the table state. When such firewalls obtain packets, they only result in checking the table state for finding whether the connection has been established already or whether a request for the packets incoming has been made through the inner host (Wu and Shan 2011, 1). If these conditions are not apparent, the access to the packet then becomes subjected to the firewall security policy ruling (Vasu et al. 2014, 16). The filtering with state-full nature has scalability and transparency for the users. However, the added protection layer results in adding complexity for the infrastructure of network security and firewalls of state-full nature face problems when trying to handle applications of dynamic nature such as H.323 or SIP. Under this type of firewalling method, there is another significant system which is the system for unified threat management. Such solutions were defined initially as the state-full inspection firewall consolidation with IPS (Intrusion Prevention System) into an individual appliance and anti-virus. The definition of UTM (Unified Threat Management) over time has expanded to include various related networks and functions of security. It is essential to acknowledge that the UTMs success depends on the efficiency of state full inspection which has its basis on the decisions of firewalls. These decisions precede all the function-related components (Rhodes-Ousley 2014, 12). This is due to the components of UTM. These are present within an individual device consisting of downstream services of security with effective nature. Therefore, the workload for every component of security behind these firewalls helps in determining the access control strength. Though these, UTMs help in providing various functions of security within individual product but still the technology with access control fundamentals in the firewall remains not changed.

2.4 Next generation firewall

These firewalls had been created in response to the evolving application sophistication as well as malware. Malware developers and developers for applications have outwitted majorly the ports depending upon the traffic classification through developing techniques for port evasion into the programs. Malware today piggybacks such applications for entering the networks and it has become networked increasingly. These firewalls have acted as a platform for enforcing policy on network security and inspecting network traffic. These next generation firewall systems are determined through 5 attributes. The first attribute is first generation firewall standard capabilities (Kaur and Rao 2014, 1). This is inclusive of filtering the packet, inspecting the protocol of state-full nature, translation of network address and connectivity of VPN (Virtual Private Network).

The second attribute is true integration of preventing intrusion. This is inclusive of the support for facing vulnerability and signatures facing threat. It includes rules based suggestions depending upon the activity of IPS. The total of such collaboration of functions through the next generation firewalls is higher than the parts of individual nature.

The third attribute is complete visibility stack as well as identification of application. This has the ability to enforce policy at the layer of application in an independent nature from protocols and ports.

The fourth attribute is the intelligence of extra-firewall. It has the ability to take data from externalized sources and making decisions of improved nature (Kaur and Singh 2014, 5). Examples are inclusive of blacklists being created and have the ability of mapping traffic to the customers and groups through use of active basis of directories.

The final attribute is modern threat landscape adaptability. It has the ability to support up gradation based paths for integrating newer feeds of data as well as techniques for addressing threats in the future. In-line support is a crucial attribute offering minimum degradation of performance or network operations disruptions.

Installing a firewall is a process utilized for control traffic of network within and external to internal network of an organization. In most situations, such systems have 2 interfaces of networks with one being external and other being internal (Jadhav and Agrawal 2013, 4). The process of firewall can engage in controlling tightly what has been permitted for traversing from a side to the other. A company wishing to deliver external web server access can result restricting every arriving traffic at the firewall. This is excluding the 80 port. Not all the related traffic can be allowed due to the presence of internalized network.

As one evaluated the firewalls for their customers or to utilize a part of the offering of security as a service, there are several solutions to look at. It becomes essential to look at either performance or security and in most of the cases both have to be looked at (Chen et al. 2014, 13). A firewall without a doubt needs to be such that it enhances securities and performed tasks such as limited access of remote nature to the network, resulting in blocking a port or making attempts at scanning IP and also stopping essential loggers from keystrokes monitoring. Taking the time for educating the customers over the roles of firewall is essential to prohibit access of unauthorized nature and prevent files of malicious nature from being obtained through the networks. This is henceforth an essential part of a solution of security (Eslahi et al. 2014, 12). However as crucial as security of network is, one cannot allow it to start trumping needs of a business for performance of computing. The customers are such that they require the ability of optimizing productivity so that they have the ability of providing a customer service level which makes them not only competitive but also highly productive in terms of resources.

This makes the next generation firewalls to be more competitive in terms of performance. Such firewalls are essential security puzzle pieces. They address various needs of security for the clients inclusive of advanced detection of threat, virus blocking through dual layer, detecting intrusion and preventing intrusion as well as protecting against ransom or malware (Gontarczyk et al. 2015, 15). It further provides managers of IT and the MSPs (managed service provider) with the ability to look through applications and customers in order to offer a higher level of network protection. These firewalls are further responsible for featuring intelligent regulation of traffic which provides priority to essential systems and also allows in identifying malicious traffic accurately so that there is no bottlenecking of safe traffic.

In the current era, firewalls of next generation have key reliability upon similarly analysed layer of application. The key focus lies in the introspection of deep packet. Until this point, there can be use of next generation firewalls for the implementation of features like firewalls of web application, integration of user identity and prevention and detection of intrusion (Guo et al. 2015, 8). Adding up the services of virtual private network in firewalls is practically widespread across organization. This is because it is successful in allowing employees off-site for the accessibility of business resource to communicate across insecure connections of network like public services of Wi-Fi. Firewalls act in the form of packet filtering system with network data packets discarded in a silent way by the analysis of data within the literal packets (He et al. 2014, 11). The overall accomplishment is to look at the address of destination, the protocol and the number of port used. There is a crucial ability of retaining the packets of data with the availability of sufficient information for making judgments in context with the state.

For MSPs looking at an offering using SaaS, it is essential to look at a solution of security which is profitable in terms of deployment and management. It is crucial to look for such firewalls is crucial which would not need more configuration of manual nature as well as management which easily eats up the resources of labour and

drives the expenses higher (Jadhav et al. 2013, 4). It is furthermore crucial to look at a solution which can offer management of centralized nature to all the customers to help them control the costs and enhance the profits simultaneously.

2.5 Assessing risks and threats through empirical evidence

The firewalls with packet filtering operate on the basis of rules that involve headers of TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) or IP. These do not attempt at establishing a check of correlation between distinct sessions. Deep packet inspection is carried out through intrusion detection or prevention system. Gateways of applications do view at the contents of packet but these remain for particular application itself (Chen et al. 2014, 13). They do not view any packet-based suspicious data. These systems furthermore look for suspicious information consisted within packets. They make attempts at examining a correlation between several packets for identifying attacks such as scanning the port, mapping the network and service denial. The IDS (Intrusion-detection system) or identification systems are of two types inclusive of signature based IDS and IDS based on anomaly. Signature-based IDS are such that it requires a database of acknowledged attacks consisting of clear signatures. A signature is defined through its types and packets order characterizing a specific attack. Limitation of such type of IDS is that only the attacks which are known can be identified. A false alarm can be thrown by IDS (Wu and Shan 2011, 1). False alarms can happen when normal stream of packet matches with attacks signature. Snort is a powerful example of IDS.

Another type is the anomaly type which helps in creating a normal network operation traffic pattern. During the mode of IDS, it views the patterns of traffic which is unusually statistical. Examples of these are inclusive of unusual load of ICMP (Internet Control Message Protocol) and port scans exponential growth. The key

challenge faced by this type of deployment is the issue of differentiating general traffic and traffic of unusual nature.

Firewall performance has been a subject of study in only few studies. Less work is even done within the field of analyzing firewall performance. Mostly the available work is of the consideration to enhance the management of configuration related to firewall systems and detect whether any configuration has been missed. The firewall performance has been studied by researchers such as Salah et al through use of a model named, analytical queue model based upon the chain of Markov. Firewalls are analyzed by this methodology subjected to general flow of traffic along with the flow of attack for DoS (Denial of Service). Several kinds of operations of firewalls were examined by other researchers (Wu and Shan 2011, 1). In the study the researchers tested the various firewalls performance as well as security inclusive of Cisco ASA, and filter of packet and SPLAT checkpoint. With regard to performance, only the throughput was considered by the researchers along with the maximum concurrent relationship number. The research results from the investigation depicted that Cisco ASA has a performance which is good in comparison to the other types involved in the study. When it comes to security, simple tests were performed by them and it was reported by them that firewalls have showed a good type of resistance.

The influence of firewall implementation over the performance of networks has also been studied by researchers. Their results from simulation depicted that use of firewalls enhances the display of networks and average time from response. Moreover, they suggested that use of firewalls of parallel nature is essential for performance of network's improvement. The performance of applying layered firewalls has been investigated by researchers. This has been done by them with regard to time of response and utilization of network. The results of simulation resulted in proving that firewalls result in degrading the network performance on the whole.

In a study it has been proven by researchers that there are vulnerabilities existing (jang et al, 2015). They conducted an experiment to evaluate and model firewalls with Linux Kernel with focus over the security vulnerabilities caused by error and violations of resulting security. In the study by Albert et al, (2005), it has been shown that use of DNS (Domain Name System) can be rebound. This rebinding can help in circumventing the firewalls and disrupting the web. They further proposed the utilization of an individual tool known as the DNS wall for combatting circumvent of firewalls. In brief, it can be said that there is a gap in literature research in the sense that no studies previously have been done to show a comprehensive analytical procedure over the influence of firewalls on the performance of networks.

3 DDOS ATTACK ANALYSIS

This section will explain the analysis on the types of DdoS attacks that are present. There are different types of such attacks and explanation of each is crucial from the perspective of this analytical discussion.

3.1 Bandwidth depletion attack

There exist basically two kinds of attacks under DDoS (Distributed Denial of Service). The first type is the bandwidth depletion attack. It has been designed for flooding the network of the victim with traffic of unwanted nature which results in preventing the traffic of legitimate nature to go into primary systems of the victim. These attacks furthermore are of 2 key types (Jang et al. 2015, 3). The first one is the attack through flooding which includes the secondary systems of victim to send major traffic volume to a system of victim. It will congest, eventually the bandwidth of the system of the victim. The second one is the attack through amplification which is inclusive either of the attacker or the system of the victim for sending messages to an IP address through broadcasting it (Kaur and Singh 2014, 5). This will, eventually result in causing every system within the subnet to be explored through the address being broadcasted for sending a message to the system of the victim.

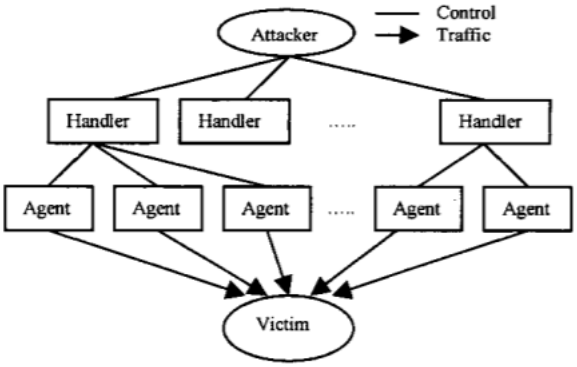

Figure 1: DDoS attacks' architecture.

Source: (Kaur and Rao 2014, 1)

3.2 Resource depletion attack

Another type of major attack is attack by resource depletion. In the resource depletion attacks through DDoS, the attacker is responsible for sending a packet with malformed information. This, in turn, is tied up with the network resources and results in exhausting the resources of system. This takes place in such a manner that there are no resources remaining for users of legitimate nature.

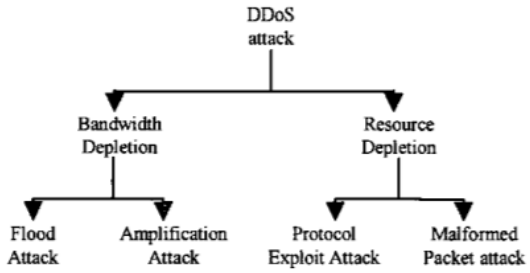

Figure 2: Classification of DDoS attack

Source: (Kong 2014, 8)

3.3 Smurf attack

The Smurf attacks are a DDoS attack wherein the major quantity of ICMP packets along with the spoofed source IP of the intended victim is broadcasted to the network of computer with the use of address of IP broadcast. It is identified from the research that majority of the devices on network are designed in such a manner that they send a reply to the IP address of source. It is realized that if the amount of devices and machines on the network are large that are receiving and responding to the packets, then the computer of the victim will encounter a flood of traffic. This flood reduces the performance of the computer to an extent that it becomes difficult to function on it.

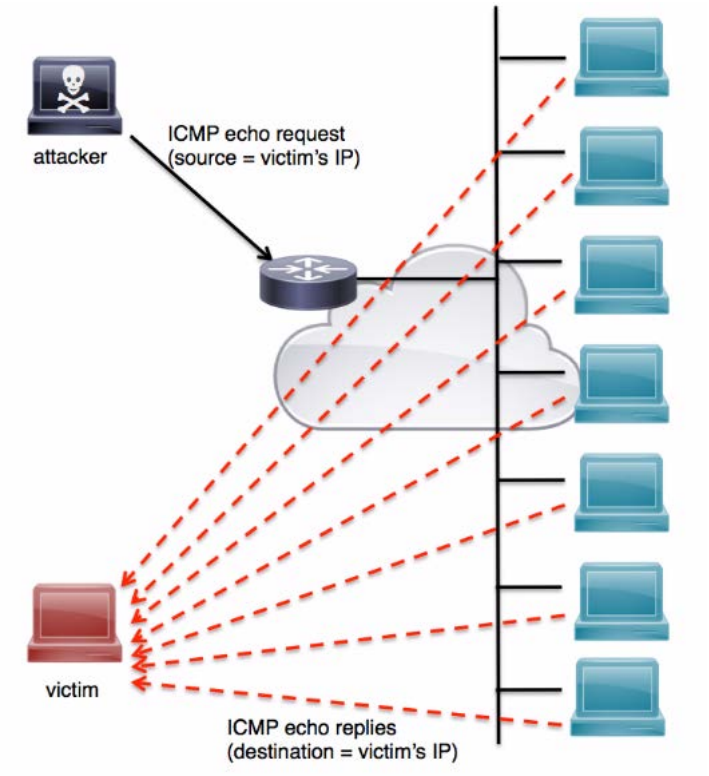

Figure 3: Process of Smurf attack.

Source: (Cisco 2013)

The Smurf attacks can be prevented by the administrators over the networks which imply that reduced number of networks encounters the vulnerability related to the Smurf attacks. It is found that the following configuration of the Cisco router enables the prevention of packets forwarding to the address of broadcast. The configuration is:

Router (config-if) # `no ip directed-broadcast`.

This example configuration does not protect the network from being a target of the Smurf attack. However, it prevents the participation of the network within the Smurf attack which causes the problem.

3.4 TCP SYN attack

The TCP SYN (synchronize) attack is the SYN flood that is part of the denial of service attack. The attacker in this case transmits a SYN requests succession on the system of the victim for the consumption of sufficient resources of server in order to make it unresponsive to the traffic of legitimate nature. It is to consider that the services of messages are exchanged by the client and server when a TCP connection to server is started by the client (Li 2015, 10). The three way handshake of TCP takes place for all connections that are based on the TCP protocol. However, the SYN flood attack takes place through not providing with the ACK (Acknowledgement) code that was expected by system which results in the wait time. However, the half-open connections within the attack result in binding of resources on the server and eventually surpassing the availability of server resources. This results in the inability of the server to connect any kind of clients and causes the service denial and deprivation of resources (Li et al. 2013, 6). The following figures (Fig 4 and 5) illustrate the common TCP 3 Way handshake and demonstration of the attack.

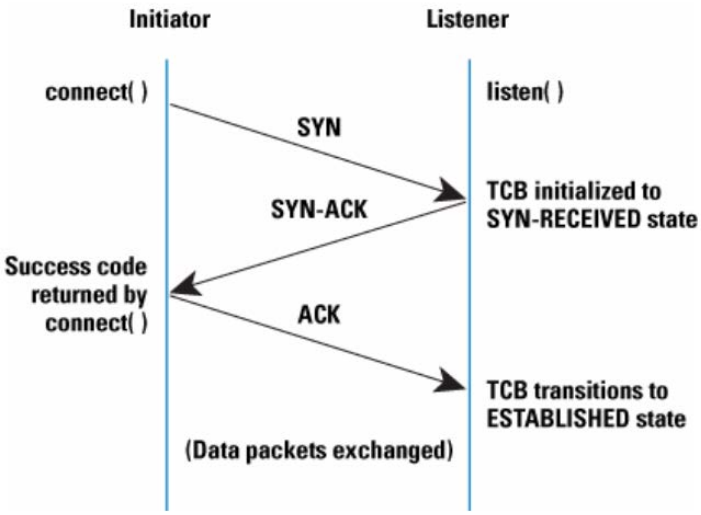

Figure 4: Common TCP 3 way handshake

Source: (Wesley 2006, 5)

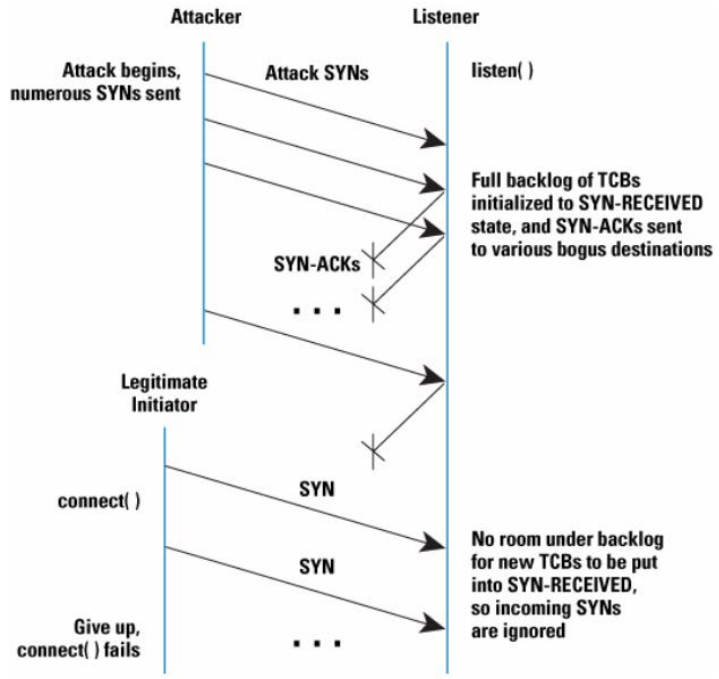

Figure 5: Demonstration of TCP SYN attack

Source: (Wesley 2006, 5)

Figure 5 illustrates that large number of TCBs (Transmission Control Block) are present within the SYN received due to which the initiation of legitimate connection is unable to be formed by the server. This inability has been caused due to the depletion of resources.

3.5 DDoS attacks analysis in firewall performance

In recent years, there has been a stronger demand for analyzing the network firewalls performance when under attacks through DDoS (Li and Oprea 2016, 8). If firewalls in networks are designed poorly for withstanding the attacks of DDoS, then the complete protected network security gets on higher risk of failing. There is an enhancement in demand particularly to indulge in analysis, modeling and network firewalls performance simulation for predicting how efficient the firewall in network is, for predicting the network firewall effectiveness and efficiency under the attacks of DDoS (Rao et al. 2016, 11). This, in turn, helps the designers of firewalls as well as administrators of system to understand essential parameters and bottlenecks which influence this performance along with performing the requires tuning for gaining performance of optimal nature. Analysis of performance furthermore can help in providing answers quickly to various design and operation related questions. This further helps the designers of firewalls in carrying out an individual design cut for reducing the design alternative sets (Rhodes-Ousley 2014, 12). Then they make use of simulation processes or experimentation for assessing the performance of assets of some good designs prior to systems being build and deployed into individual environments of networks.

Even after the fact that firewalls represent one of the essential failure points at the time when attack of DDoS is taking place, there still not exist any standardized procedures to evaluate the performance of firewall during the attack (Pal et al. 2014, 5). Such software is still required to prevail in the market as per the knowledge

collected. The key reason for this lies in the fact that implementation of firewalls widely vary and this makes it problematic for carrying out comparisons between direct performance and indirect one. With rise in deployment of firewalls in firms, it will be seen that over the network there is a question which arises. This question is with regard to whether the products being purchased by these firms stands up and is able to sustain the heavy loads relatively or not. All of the three systems of firewalls utilized within such a set up comprise of state-full networks (Patel 2015, 4). These networks have the ability of keeping track of the connection related state network that is travelling throughout it. Through keeping a record of the state of connection, the firewalls of state-full type result in providing addition of efficiency with regard to the inspection of packet. This is due to the fact that for current connections, the firewall only requires checking the table state rather than checking the packet in opposition to the rule set of firewall (Shin et al. 2016, 4). This can be of an extensive form. Such stale relationships are removed from the table state. For preventing the table state from being filled, sessions are timed out when no traffic is being passed for a specific time period.

During DDoS attacks, even though the firewalls have state-full appearance, every packet set is such that it traverses a firewall of state-full nature. This results in consuming the resources on simple state across such firewalls resulting in creation of chokepoint in DDoS (Shukhman et al. 2015, 8). There is no doubt that firewalls have limited state table resources, it becomes much easier for those attacking to generate enough traffic. This traffic is well-formed and generated in a programmatically configuration. This results in satisfying and passing the rules on firewall policies. This will, eventually result in choking up the bandwidth for traffic legitimacy from the real customers (Smirnov and Halimon 2015, 7). This, in turn, will lead towards services denial of the applications and servers lying beneath the firewalls. In addition, in most of the situations, enough firewall exhaustion of state-full nature is possible because of the traffic attacking. This attack causes the

firewalls of state-full nature to fall over essential and then they fail in forwarding traffic (Vasu et al. 2014, 16). Therefore, the state-full nature firewalls result in surrendering invariably to the attacks of DDoS even in a more rapid manner than services would have done without there being any firewalls at all.

4 EMPIRICAL RESEARCH OF THE CASE STUDY

This section will explain the various research methodology used within this research. There is important information in this section with regard to the design of this research, justification for such a design, advantages of using a case study and similar significant data.

4.1 Research Design

The research method selected for this research is case study. The secondary source is identified to be more useful for this research. This is taken into account as the use of experimentation in order to determine the importance of the firewalls performance delivered in the organizational setting would have provided with less effective and accurate results (Yu 2016, 6). This is found as the experimentation would require developing an environment where the security of firewall is required to be tested. However, this would be needed in real time with the use of s second computer that can surpass the firewall and create an attack. Furthermore, the following details of the experiment showcase that its conduct will not only be difficult and time-consuming but also it will be highly cost –ncurring. Therefore, the case study approach has been selected.

4.2 Initially considered experiment design

An assessment-based methodology was initially considered for this this research thesis to evaluate distinct firewall kinds with regard to security and also performance. However, the case study approach was found to be effective after considering the details below. It is Always desired to have firewalls which are not only secure but also resilient to attack but degradation of performance in these is an

issue. With the current advancements that the Internet has gone through and the multimedia application extensive use through users has resulted in making QoS networks to gain priority among users (Budka et al. 2014, 7). In order to assess the different firewalls, a proper procedure is required to ensure that business requirements and client requirements are met.

The firewall performance is generally tested under distinct loads of traffic while taking into consideration various metrics for evaluating the performance of firewall. There are metrics inclusive of throughput, delay, jitters and rate of packet loss. Throughput is the real payload received per time unit. Delay is the time taken by packets to be transferred from the destination source (Chen et al. 2014, 13). Jitter is responsible for measuring the variation within received packets delay. Packet loss rates, on the other hand, are ratios of the packets which are lost to the total packets transmitted. Hence, the utilization of these metrics will be required in the experiment.

Unlike the evaluation of QoS (Quality of Service), security does not become a quantity of absolute nature and no approach of either quantitative or qualitative nature exists for evaluating it. Therefore, the testing bed would consist of 2 personal computers and a network of firewall when the first computer is responsible for representing the victim and can be considered to be protected through the system of firewall (Li 2015, 10). The second computer is responsible for representing attackers that will generate attacks through firewalls. If the computer attacking is able to manage successfully reading related data, scanning the ports opened or making the computer of the victim busy or not able to perform related tasks, then the attack will be regarded successful and the firewall system would have then failed the testing (Kong 2014, 8). If the attacker fails completely to cause any of the problems mentioned above, then the firewalls would have been regarded to successfully pass the testing. Finally when the attacker succeeds partially, then it will be concluded

that the firewall failed the test partially. The attack details and the tools to destruct attacks will also be discussed.

Within this section, the focus is on describing the testing bench utilized for conducting the experiment along with presenting the tools of software utilized for collecting and analyzing the results from the test.

.

Figure 6: Description of test bench and hardware

Figure 6 provides information on testing bench and the hardware utilized for such a test. For the experimental testing, testbeds are required and this has been illustrated by the 2 computers that have a direct connection with a firewall. These computers taken under considerations for the experiment were notebooks with specifications of discrete nature (Kaur and Rao 2014, 1). The specifications were inclusive of CPU (Central Processing Unit), Model of NIC (Network Interface Controller) and a system for operations. The CPU had Intel core I5 with 2.24 GHz processor. The model of NIC had realtek with Gigabit family of RTL. The system of operations was Ubuntu with 7 Windows and 11.04 Ubuntu upgrade was present.

In order to conduct the experiment, firewalls based on the network are required to be used (2 in number). These were inclusive of Cisco ASA and the firewalls packet filter (Kaur and Singh 2014, 5). The ASA 5510 Cisco is known as an appliance for adaptive security which helps in providing higher firewall performance and services of VPN. It is generally suitable for businesses which are small and medium in size and branch offices from remote enterprises are easily deployed with appliances of

cost effective nature. When it comes to the packet filter, the 2811 router of Cisco can be used with ACL of extended nature being present (Jang et al. 2015, 3). Even though the setting of testbed implemented is simplified in nature with a computer for generating traffic, still the traffic generated helps in mimicking the traffic which might be generated from a complicated network present within major sized organizations.

Synchronization in accurate manner is required to be performed for clocks running on laptops. This is essential for avoiding any error in the results over jitter and delay. For ensuring precise synchronization of clock, the Atom Time Pro software is needed to be used. This connects frequently to servers globally for adjusting the devices time used within the experimentation (Jadhav et al. 2013, 4). In order to communicate with the team server, a connection namely, out of band is effective for guaranteeing that there will not be any interference with the load of traffic.

The traffic testing is obtained through the use of a tool called as IP traffic generator. This generator is an information generation technique and a tool for the networks of IP which can help in generating traffic at TCP and UDP at distinct rates (He et al. 2014, 11). In order to test the firewalls, different loads are used inclusive of light, heavy and medium. The traffic furthermore should consist of 16 connections concurrently with packets inclusive of 500, 10000 and 30000. These packets are required to be generated for every load based connection that is light, medium or heavy. Two distinct types of packets are required to be utilized and taken into consideration inclusive of 512 and 1460 bytes.

4.3 Case Study Approach

It was found that conducting this experiment would have not provided with the actual results as the attacker used in the experiment would be simulated due to which the strengths and techniques of the actual attacker could be undermined and underestimated (Guo et al. 2015, 8). Therefore, the case study has been used in

which the mitigation of the attack with the use of Cisco security firewalls could be analysed to gain insight of the manner in which real and actual real time threats and attacks can be mitigated in the organizations (Gontarczyk et al. 2015, 15). It is found that the case study will be able to demonstrate the general and specific risks along with attacks that can be encountered in the running systems of firewall within the enterprise. Furthermore, the analysis of case study will be able to illustrate the application of risk analysis and attack mitigation for the maximized network security of an organization. According to the researchers, the use of case study is effective when the impact of an independent variable such as the firewall is required to be assessed on the dependent variable of enterprise network security (Eslahi et al. 2014, 12). The firewall is considered as independent variables as any other factor does not influence the firewall but it is the firewall that can either enable the network security or result in the network attack within an organization.

4.4 Case Study on Stroock and Stroock and Lavan LLP

This case study is based on the organization of Stroock & Stroock & Lavan LLP operating in the legal industry in order to provide services to the industry of finance. This is a midsize organization consisting of 300 attorneys. The law firms that entail service to the financial organizations are required to undertake the due diligence audits for the clients (Cisco 2016). In order to facilitate the effective audit, newer approaches towards the security has been identified as critical by the Information Security Director of the organization namely James Forrest.

According to the Forrest, there is an increase in the client security requirements and these have been recorded. This was identified as micro segmentation is often required by the clients of Stroock & Stroock & Lavan for the mitigation of lateral threats movement (Li et al. 2013, 6). This was a critical requirement that was met with the use of Cisco Virtual Security Gateway.

The organization had been operating in the market of New York City for more than 13 decades and operates offices within Miami, Los Angeles and Washington, D.C (Cisco 2016). The organization is renowned for the department of corporate that is responsible for the representation of several top level institutions of finance. Therefore, one of the critical requirements of the organization was to ascertain that the high standard of the security is met that as expected by their clients (Li and Oprea 2016, 8). Forrest further states that the organization provides with the security audits for the client since it provides with the position of defensible nature on the increment of the security. The organization was following the traditional approach until recently towards the network access control due to which the rules were applied at every core switch along with manual updating practices (Cisco 2016). However, stronger requirements of the clients for the segmentation of the network resulted in the organization to take the virtual approach into consideration.

The organization was striving towards providing both fluid experience of management and flexibility for addressing the newly surfaced requirements (Cisco 2016). The challenges such as the compliance demonstration during the client security audits, central segmentation and network access control along with the protection of the informational assets and critical data centre have been found. This has resulted in the Stroock & Stroock to identify the virtual firewall systems that can provide with the robust performance, micro segmentation and centralized control.

This unique challenge and the changing needs of the clients resulted in the adoption of the Cisco Virtual Security Gateway (VSG) (Cisco 2016). Therefore, as a solution, the Cisco VSG as a firewall of distributed nature along with its integration with the Nexus 100V Switch of Cisco was considered and implemented. The Cisco Prime Network Services Controller was utilized in order to reach centralized management.

This implementation enabled Stroock & Stroock to meet the requirements of the clients for the micro segmentation through offering direct compliance evidence in the

real time (Cisco 2016). The organization was able to undertake real time compliance with the audits of client, reduced the risk, provided virtual security, integrated the firewall with big data and became equipped for the future.

5 DISCUSSION

This case study analysis addresses the three key research questions of this research thesis. It has been identified in the case study analysis that the following products of Cisco were deployed by Stroock & Stroock in order to meet the changing and growing client requirements and increasing the organizational level of security (Eslahi et al. 2014, 12). The products deployed by Cisco for Stroock & Stroock were the Cisco Virtual Security Gateway integrated with the Cisco's Nexus 1000V Switch. These two products were deployed in deep combination due to which it can be considered as a single system. The second product deployed was the Cisco Prime Network Services Controller.

These Cisco products were implemented by Stroock and Stroock for the purpose of resolving the challenges of compliance demonstration during the client security audit, central segmentation along with the network access control and the protection of not only the key data centre but also the information based assets (Gontarczyk et al. 2015, 15). Addressing these concerns as challenges was critical for the legal firm Stroock and Stroock. This was due to their clientele demand for increasedsecurity and assurance for protection from the attacks as identified by the literature.

It has been recognized that the primary focus of the Stroock and Stroock was to ensure that the commonly encountered DDoS attacks do not take place either on their own server or on the servers of the clients that they audit (Guo et al. 2015, 8). Therefore, special consideration was paid by the Information System Director of the legal firm was to find such firewalls that could ensure that no attacks take place. This is the main security objective among this and other global organizations but also to ensure that risk and threat of such attacks could be mitigated (He et al. 2014, 11). Often, improper control and lack of state of the art technology results in the incidences such as security attacks and breaches that are preventable with the

present technology. Therefore, the organization in the case study was required to recognize the importance of the firewall's performance for the organizations.

The first research question can be addressed with the identification that the Cisco Virtual Security Gateway was selected by Forrest upon realizing the importance of the firewall for this organization as this system provides with the acceleration of the performance through the offloading of packet intensive processing for performance optimization (Jadhav et al. 2013, 4). Moreover, active standby mode based deployment of the Cisco VSG enables the high level of availability. The primary business requirement of obtaining extended firewalling service based on zone within the virtual machines through the segmentation was enabled with the facilitation of cloud security by this system. The organizational need of centralized management was fulfilled with the implementation of the VSG (Jang et al. 2015, 3). The network security of the enterprise was enabled with the complementary functionalities of ASA 1000V that provides with the context aware and zone based performance in terms of the security for the enterprise enabling a comprehensive security portfolio.

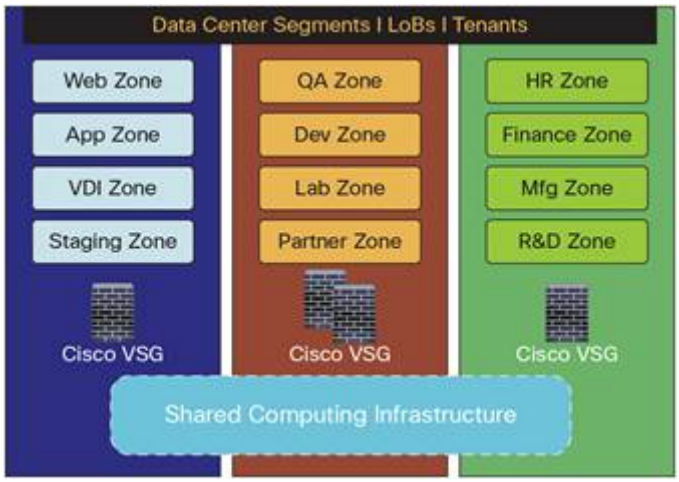

Figure 7: Trusted access control and monitoring based on zone with the VSG.

Source: (Cisco 2016)

The Cisco ASA 1000V Cloud Firewall provides with the comprehensive security to the enterprise across physical, virtual and cloud environments. The security capabilities of the VSG are enhanced with the ASA 1000V to further enhance the portfolio of security (Kaur and Singh 2014, 5). This enables the firewall to deliver multi-tenant state of the art security, protection against the network attacks and default functionality of gateway.

It is identified with the analysis that the Cisco Prime Network Services Controller is additionally employed by the ASA 1000V Cloud Firewall (Cisco 2016). This allows the firewall to provide scalable and rapid deployment with the policy management that is driven by template on the security profiles in a dynamic manner. Moreover, the flexibility is achieved by the organization within the management through the help of XML (Extensible Mark-up Language) API (Application Programming Interface) resulting in the programmable integration with the orchestration tools and management of third party (Kaur and Rao 2014, 1). The firewall facilitates the management interfaces relevant with their job role for the security, server and network administrators and ascertains the governance of collaborative nature.

In order to address the second research question, the solutions attained with the deployment of the Cisco systems can be reviewed to identify the general and specific attacks and risks that can be encountered in running firewall systems within an enterprise (Kong 2014, 8). According to the studies, some of the major risks related to the consumer data theft and unauthorized access to the enterprise data are prevailing across the field of network security (Cisco 2016). This leads to the demand among the consumers of Stroock and Stroock to move from the traditional systems towards the more secure and comprehensive firewalls. Central network access control and segmentation were required in order to maintain the defence surrounding the legacy applications with the use of older systems and enabling access of internet to some users along with restricting their access for the internal and critical information assets and data infrastructure (Li 2015, 10). Therefore, real

time compliance was enabled with the implementation Cisco systems as the walk through and screen shots could be provided to clients by the organization. Furthermore, flexible risk mitigation provided by the system ensures that the DDoS security attacks and data theft are prevented.

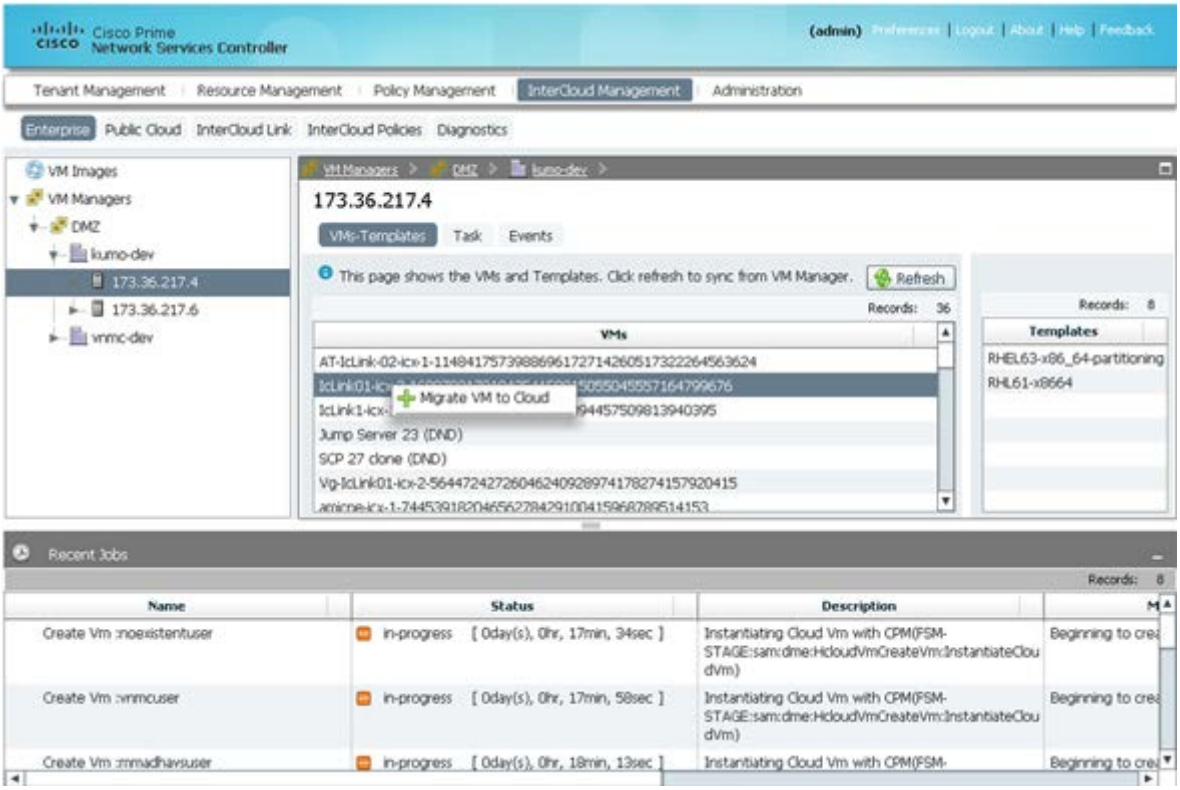

Figure 8: Cisco Prime Network Services Controller Interface for the Enterprise

Source: (Cisco 2016)

As per the website of Cisco, the above figure has been provided. Figure 8 depicts the controller interface for prime network services deployed for Cisco. The systems employed by the law firm provided with the intrusion prevention systems for all the locations of the organization in order to enable internal threat activity visibility. This is critical to the enterprise network security as it allows the organization to foresee and prevent the potential attacks and threats (Li et al. 2013, 6). This brings the focus

of this argument to the primary threats and risks associated with the running firewalls in enterprise. One of the recently recognized threats is the internal attack that can be caused by the dissatisfied information technology employees. The possibilities of the organization providing employee with devices with such devices being stolen are another critical security threat (Li and Oprea 2016, 8). Furthermore, it is critical for the virtual systems to have strong data level encryption for the protection of enterprise data. The implementation of the Cisco VSG and Cisco Prime Network Services Controller ensures that not only the threats of attacks and risks are mitigated but also the strong firewall does not let any DDoS attack to take place within the enterprise network (Rao et al. 2016, 11). Hence, this addresses the second research question.

It is identified from the case study analysis that applications of the effective risk analysis helpthe organization to foresee any potential attack or threat that can compromise the network security enterprise. The consideration to the attack mitigation provided by the Cisco systems ensures that any potential threat that can occur is mitigated before its occurrence (Rhodes-Ousley 2014, 12). The context-aware and granular security policies of VSG ensure that the virtual machines and their movement are dynamically secured. Furthermore, they ensured that the errors across the network, security and server teams are reduced and the collaboration is encouraged.

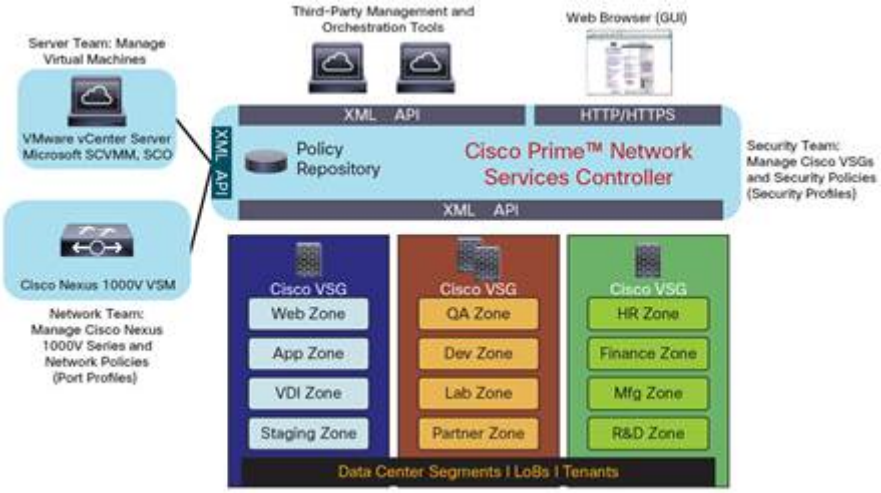

Figure 9: Administration model of Cisco Prime Services Controller for VSG management

Source: (Cisco 2016)

This is evident in Figure 9 wherein Cisco prime services controller administration model has been established by the company management which was managed by the company. This is particularly helpful for the enterprise since these teams can effectively control the network environment and with identification of the potential attack or threat to mitigate adversities (Shukhman et al. 2015, 8). The system entails the distinguished administrative responsibilities that ensure that the prompts of the DDoS attacks do not surpass the firewall. This allows the network security of the enterprise to be maximized at all times (Pal et al. 2014, 5). The fact that the early identification of the threats and attacks are enabled by the Cisco systems is exemplary for the network security management. The enterprise network security is able to function centrally and mitigates the attacks or threats allowing complete security to the organization and their associates (Shin et al. 2016, 4). The third research question has been addressed as Stroock and Stroock were able to analyse the critical logs with the functionality of the Cisco firewall (Patel 2015, 4). Therefore, it can be considered that the outcome achieved through the deployment

of the Cisco systems have simplified the audits of clients and compliance for the organization in an on-going manner.

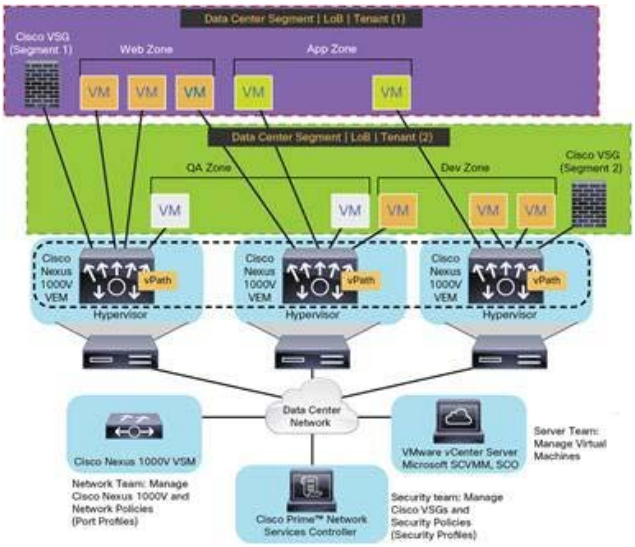

Figure 10 Cisco VSG offering maximized security across Dynamic VM Environment

Source: (Cisco 2016)

The options of flexible micro segmentation have maximized the enterprise network security which provided mitigation of more risk exposure than the total cost of system acquisition resulting in attaining maximized return on the investment within security and achieving the essential security for the enterprise network protection (Smirnov and Halimon 2015, 7). The implementation of both Cisco VSG and Prime Network Services Controller streamlines the policies and security services management across all organizational settings.

6 CONCLUSION

It has been identified from the analysis and discussion that there is a variety of network attacks that can cause serious damage and incur costs to the organization due to data theft and security attacks. Therefore, the vulnerabilities, threats, assets and existing controls have been identified along with establishing that the security policies and the effective security policy designs are essential for efficiency security mechanisms and security services adoption. Hence, the analysis of the case study proves the primary thesis objective that the effective security concepts are critical for the enterprise network security.

The three key research questions of this research thesis have been addressed with the use of case study that showcases a successful enterprise network protection. The organization of Stroock and Stroock has achieved network security effectively by identifying the firewall that can improve the security of the organization and facilitate the compliance with the client audits. The main requirements of the Stroock and Stroock for the central segmentation and network access control were in alignment with the level of protection offered by the Cisco VSG and Prime Network Services Controller. The concern and the prevailing security issue to protect the information assets and critical data centre security experienced by the global organizations and this organization was met by the deployment of the Cisco systems. The case study analysis enabled addressing the first research question by establishing the importance of the firewalls performance delivery within the organizations. The packet intensive processing and coupling of the security facilitated by the three systems Cisco VSG, Cisco Nexus 1000V Switch based Firewall and Cisco Prime Network Services Controller provided with the multi-tenant based comprehensive security and firewalling services to the Stroock and Stroock addressing the initial research question.

The second research question was addressed with the identification of the attacks and risks as perceived by the case study organizations and prevailing global network security issues. It was found that the enterprise encounter issues from the securing the information of employee devices in the cases of theft and internal attack deployed by disgruntled employees to the external network attacks and theft of valuable enterprise data that can result in incurring large costs. Along with the identification of the attacks and risks, the wide range of network DDoS based attacks was identified by this research and it is found that these attacks can be effectively mitigated with the deployment of the Cisco systems in the discussed combination. The firewall system powered by the Cisco Nexus 1000V Switch and integrated within the Cisco VSG ensured that the security capabilities are maximized in order to ensure that the enterprise network is protected from the potential and severe attacks. It was found that the Cisco firewalls further use the Cisco Prime Network Services Controller for the effective and comprehensive network security and classification of the packets to differentiate from the legitimate interactions from the illegitimate. Hence, the third research question can be addressed through the consideration of these capabilities and central management of the system along with the network, server and security teams' collaboration that ensures the potential threats and attacks to be identified earlier in the process. It identifies the threat upon initial contact to ensure that the attacks are mitigated and maximum level of network security is delivered to the enterprise as in the case of Stroock and Stroock.

It is considered that the future direction for the research on the enterprise network security in the context of firewall can be performed by undertaking primary research that utilizes the Cisco VSG, Prime Network Services Controller. The integrated firewall and tests of security offered along with any potential areas that can be improved through deploying DDoS attacks to the computer can be performed under the scope of Cisco systems. It can be concluded that the effective firewall systems

such as Cisco can be used by the global organizations in order to prevent and mitigate potential attacks and to attain comprehensive enterprise network security.

References

Budka, K., Deshpande, J. and Thottan, M. "Network Security." Communication Networks for Smart Grids. Springer London, 2014. 209-225.

Chen, Z., Dong, W., Li, H., Zhang, P., Chen, X. and Cao, J. "Collaborative network security in multi-tenant data center for cloud computing." Tsinghua Science and Technology 19.1 (2014): 82-94.

Case Study of Stroock & Stroock & Lavan LLP. “Case Study of Stroock & Stroock & Lavan LLP”. Cisco. 2016. Web. 2017

Eslahi, M., Naseri, M., Hashim, H., Tahir, N. and Saad, E. "BYOD: Current state and security challenges." Computer Applications and Industrial Electronics (ISCAIE), 2014 IEEE Symposium on. IEEE, 2014. 123-134

Gontarczyk, A., McMillan P., and Pavlovski C., "Cyber Security Zone Modeling in Practice." Proceedings of the 10th International Conference on Information Technology and Applications (ICITA), Sydney, Australia (2015): 15-29.

Guo, H., Tang T., and Wu D. "The Research of Private Network Secure Interconnection Scheme in Large-Scaled Enterprises." Genetic and Evolutionary Computing. Springer International Publishing, 2015. 419-426.

He, X., Chomsiri T., Nanda P., and Tan, Z.“Improving cloud network security using the Tree-Rule firewall”. Future Generation Computer Systems 20.1 (2014): 116-126.

Jadhav, S. and Agrawal, R. “Fast and Scalable Method to Resolve Anomalies in Firewall Policies”. International Journal of Advanced and Innovative Research (IJAIR) 2.3 (2013): 753-756.

Jang, H., Jeong, J., Kim, H. and Park, J. "A survey on interfaces to network security functions in network virtualization." Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on. IEEE, 2015. 110-122.

Kaur, T., Malhotra, V. and Singh, D. “Comparison of network security tools-firewall, intrusion detection system and Honeypot”. Int. J. Enhanced Res. Sci. Technol. Eng 2.1 (2014): 200-204.

Kaur, K.and Rao, D. “Automation the process of unifying the change in the firewall performance”. International Journal of Computer Science and Network Security (IJCSNS) 16.1 (2014): 77. Print.

Kong, L. "Research of building enterprise network security system based on cloud computing technology." BioTechnology: An Indian Journal 10.20 (2014). 154-161.

Li, J. "The research and application of multi-firewall technology in enterprise network security." International Journal of Security and Its Applications 9.5 (2015): 153-162.

Li, Y., Luo, Y., Wei, Z., Xia, C. and Liang, X. "A Verification Method of Enterprise Network Reachability Based on Topology Path." Computational Intelligence and Security (CIS), 2013 9th International Conference on. IEEE, 2013. 119-124.

Li, Z. and Oprea, A. "Operational security log analytics for enterprise breach detection." Cybersecurity Development (SecDev), IEEE. IEEE, 2016. 297-304.

Rao, J., Chari, S., Pendarakis, D., Sailer, R., Stoecklin, M., Teiken, W. and Wespi, A. "Security 360°: Enterprise security for the cognitive era." IBM Journal of Research and Development 60.4 (2016). 1-11.

Rhodes-Ousley, M. Information security the complete reference. New York: McGraw Hill Professional, 2014. Print. 14-25.

Pal, P., Atighetchi, M., Soule, N., Ishakian, V., Loyall, J., Grant, R. and Sinclair, A."Secure and QoS-Managed Information Exchange Between Enterprise and Constrained Environments." Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC), 2014 IEEE 17th International Symposium on. IEEE, 2014. 159-163.

Patel, A. "Network performance without compromising security." Network Security 2015. 1 (2015): 9-12.

Shin, S., Xu, L., Hong, S. and Gu, G. "Enhancing Network Security through Software Defined Networking (SDN)." Computer Communication and Networks (ICCCN), 2016 25th International Conference on. IEEE, 2016. 26-29.

Shukhman, A., Polezhaev, P., Ushakov, Y., Legashev, L., Tarasov, V. and Bakhareva, N. "Development of network security tools for enterprise software-defined networks." Proceedings of the 8th International Conference on Security of Information and Networks. ACM, 2015. 229-236.

Smirnov, Y. and Halimon, V. "Double Layer Gateway Model for Connection Between Production Network and Enterprise Network." International Review of Automatic Control (IREACO) 8.1 (2015): 44-50.

Vasu, A. K., Sudarsan, A., Ayyappan, P., Ganesh, A., & Gokul, V “Improving Firewall Performance by Eliminating Redundancies in Access Control Lists”. International Journal of Computer Networks 6.5 (2014): 92-107. Print

Wang, L., Jajodia, S., Singhal, A., Cheng, P. and Noel, S. "k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities." IEEE Transactions on Dependable and Secure Computing 11.1 (2014): 30-44.

Wu, D. and Shan, S. Meta-analysis of network information security and Web data mining techniques. New York: Atlantis Press, 2011. 39. Print.

Xu, Y. and Dong, F. "Research on Multi-Core Network Equipment Virus Defense System." Applied Mechanics and Materials. Vol. 738. Trans Tech Publications, 2015. 202-210.

Yao, W., Gong, L. and Xu, X. "Design and Implementation of Security Network Optimization." Advanced Materials Research. Vol. 977. Trans Tech Publications, 2014. 345-349.

Yu, T., Fayaz, S., Collins, M., Sekar, V. and Seshan, S. "PSI: Precise Security Instrumentation for Enterprise Networks." Proc. NDSS, 2017. 15-29.

Yu, S. "Design of an Electronic Commerce Platform with Network Security using J2EE for Cloud Computing." International Journal of Simulation--Systems, Science & Technology 17.15 (2016). 10-15.

A Cisco Guide To Defending Against Distributed Denial Of Service Attacks "A Cisco Guide To Defending Against Distributed Denial Of Service Attacks". Cisco, 2013, Web. 2017.

Wesley, M. E. "Defenses Against TCP SYN Flooding Attacks". The Internet Protocol Journal 9.4 (2006): 1-44. Print.