International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 13, No.1 (Jan-2023)

http://dx.doi.org/10.12785/ijcds/130116

Analysis and Evaluation of Network and Application Security Based on Next Generation Firewall

***Md. Shamimul Islam[1], Mohammed Asraf Uddin[1], Dr. Md. Dulal Hossain[1], Dr. Md. Shakil Ahmed[1] and Dr. Md. Golam Moazzam[2]**

[1]*Institute of Computer Science, Atomic Energy Research Establishment, Bangladesh Atomic Energy Commission, Bangladesh*
[2]*Department of Computer Science, Jahangirnagar University, Bangladesh*

Received 17 Jan. 2022, Revised 21 Dec. 2022, Accepted 12 Jan. 2023, Published 31 Jan. 2023

Abstract: To design and deploy wired and wireless secured network infrastructure, ensuring network and application security is a major challenge for any scientific organization. Such kind of organization faces security challenges to protect data, sensitive information, and assets as a lot of people are connected within their integrated network system. In this modern era, Next-Generation Hardware Firewall (NGFW) acts as an advanced security element to protect networks and applications. In this paper, our research experiments were held over the Atomic Energy Research Establishment (AERE) under Bangladesh Atomic Energy Commission (BAEC) network zone where Secured network infrastructure by configuring the NGFW firewall has been established for its network security purpose. In this paper, we have applied various network and application policy and rules over the AERE NGFW firewall. Then, we have analyzed and gathered statistical network data using the NGFW firewall in terms of different network security parameters. For this research work, we have collected data from 09 December 2020 to 09 December 2021. Further, the data are being used to evaluate the network and application security parameters of AERE. Finally, we illustrated how network and application security is being achieved by the NGFW firewall and provides future steps to embrace a better network infrastructure development for any scientific organization like AERE.

Keywords: NGFW Firewall, Network Security, Threats, Network Infrastructure etc.

1. INTRODUCTION

Bangladesh is moving rapidly towards the digitization process in every sector like financial, research, educational, government and non government offices etc., with the accomplishment of the vision of "Digital Bangladesh-2021". With the emersion of ICT based development, most of the Bangladeshi organizations are developing of its network based infrastructure (LAN, WAN, Intranet, Extranet etc). At this perspective, protection of inter-connected systems such as computers, servers, mobile devices, electronic systems, networks application data is a very challenging issue [1] [5]. So, insufficient network security can be huge potential threats for any organization in terms of data, network and application [1] [7] [15]. It also causes violation of confidentiality, integrity and availability. Thus, it is very crucial matter to implement strong network and organizational policy over prominent network protocols. Network policy consists of strong set of rules, regulation and activities implementation over a structured designed and developed network framework by an organization in which a network administrators can be able to prevent and monitor unauthorized access, misuse of network, correction, restriction, provides confidentiality, and integrity maintaining for the network resources [2]. IPSec protocol, Secure Sockets Layer (SSL), Secure Shell (SSH), Hyper Text Transfer Protocol Secure (HTTPS), Kerberos etc., are the most prominent network security protocols to govern data flow over a network. To secure the network, firewall strategies (both software and hardware firewall) are being implemented to ensure organizations network security. A firewall acts as a shielding barrier between trusted internal network and outside network. Mostly firewall is a kind of security devices that protect a host computer or entire network against malicious attacks. Firewall is mainly two types as its nature- software firewall and Hardware firewall. Software firewall performs under a specific host Operating System (OS) through applications and port number and its implication area is limited. In this paper, we have discussed about network-based hardware firewall which is used for the security purpose of large network and communication technology. Usually, Hardware firewall is being configured between internal network core router and ISP gateway. It can prevent a network by preserving security and ensures safety against unauthorized access or external network [3]. Hardware firewall may be in different categories considering its performance activities. The layer 4 category firewall is

E-mail address: shamimul@baec.gov.bd,asrafbaec@gmail.com,edhossain@gmail.com,shakilahmed.baec@gmail.com,khokan@juniv.edu

used to NAT, blocking or allowing traffic, tracking active and inactive connections, support virtual private network (VPN) connections and routing etc., purpose. Such kinds of layer 4 firewalls examples are Packet Filtering Firewall, Circuit Level Firewall, Stateful Inspection Firewall, Application Level Firewall etc., [3][7]. On the other hand, Next Generation hardware firewall (NGFW) execution capability is much wider than layer 4 hardware firewall. For the experiment, we have collected statistical data as an experimental data using NGFW firewall at AERE, BAEC to analysis and evaluate network and application security in terms of miscellaneous cyber security parameters. We have considered the network traffic monitoring, intrusion prevention and detection of application, URL and content filtering, IP and ports filtering, malware threat analysis, network insider user activities monitoring, file filtering, decrypting traffic etc., category to evaluate and measure network and application security. The remaining section is organized as follows. In section 2, related works and activities have been described. Design and development related research to build up a better network infrastructure using NGFW firewall has been illustrated in section 3. Experimental statistical data analysis and obtained results are analyzed in section 4. Finally, the paper is concluded in section 5 along with the future directions.

2. RELATED WORK

Several research works has been published about network security and Next Generation Firewall related activities. Some researchers discussed about effects of firewall on network performance. Some of them investigated the previous data and illustrated the survey of network firewall. A few works has been done about implementation and analysis using different network simulator. Some researcher discussed about configuration and misconfiguration of firewall and network security violation in specific areas. In [4], the authors reviewed several papers based on firewall security issues focusing on traditional firewalls; its evolution, security issues, various policies and the concept of distributed firewall.Svoboda et al. [5] provided a current overview of modern network monitoring approaches using high speed bandwidth internet in both wired and wireless network to design network architecture, features and comparison between network monitoring approaches. In [6], various types of firewalls operations have been examined by the researchers. They tested the security and performance of different firewalls including: Cisco ASA, packet filter, and Checkpoint SPLAT. The researchers also studied the information security by applying a set of attacks and observing the reaction of the firewalls. Real experiments on different types of firewalls including personal and network-based has been tested and performed. In [7], multiple levels of firewall including the difference between layer 4 firewall and advanced Next Generation Firewall has been discussed. Kenneth et al. [8] investigated about modern firewall policy history and surveyed of network firewall. They showed that to implement firewall various methodologies are being used to filter network traffic over OSI 7 (seven) layers. W. Konikiewicz et al. [9] provided the data of performance analysis of CISCO ASA and Juniper firewalls on packet traffic based on bandwidth and server response time. Within research in [10] and [11], the authors presented paper based on Markov chain technology for the performance evaluation of firewall. The methodology analyzes firewalls that are subject to normal traffic flows as well as Denial of Services (DoS) attack flows. Other literature [12] [13] gives us an idea to define role of firewall on computer networks and implementation of those firewalls on hardware or software on combination both. A Review in Recent Development of Network Threats and Security Measures is discussed at [14]. Their research mainly concerned about increased security related studies with the web data. In [15], advanced data security within network applying secured algorithm has been discussed. Data confidentiality technique within a network has been ensured according to specified algorithms. All the above discussed paper, the research and survey related works has been done based on implementation, configuration and misconfiguration of firewalls, impact of firewall on network performance, comparison of different firewalls etc., parameters. A very few research has been done about designing and developing of a secured network framework by implementing firewall policy and analyzing of network statistical data in terms of various network and application security parameters. In addition, most of the cases real time a specific statistical data analysis by implementing Hardware firewalls is being avoided. In this paper, we have tried to find out how much firewall policy is effective in terms of network and application security within an organization network boundary like AERE. Our study will help an organization administration and network administrator to find out its current network security status. They will be able to cope up with miscellaneous network and application threats.

3. METHODOLOGY: NETWORK DESIGN AND POLICY IMPLEMENTATION

To design and develop a secured network infrastructure and evaluate statistical network data in terms of different network and application security parameters, we have chosen Atomic Energy Research Establishment (AERE), Savar as an experimental zone which is a regional multidisciplinary research organization under Bangladesh Atomic Energy Commission (BAEC). AERE's network infrastructure has been formed with both wired and wireless system. A significant number of LAN based IP connection and wireless access points have been configured to different machines and individuals to broadcast network traffic within AERE. A number of switches, DMZ switches, Branch router, Alexa enabled device, IoT based devices, host machines, routers, different types of server and media converters are interconnected with each other to maintain flow of network traffic smoothly within the different institutes of AERE. In this perspective, maintain network and application security to these machine and individuals has become a major challenging issue for AERE. For security purpose, a modern CISCO based next generation firewall

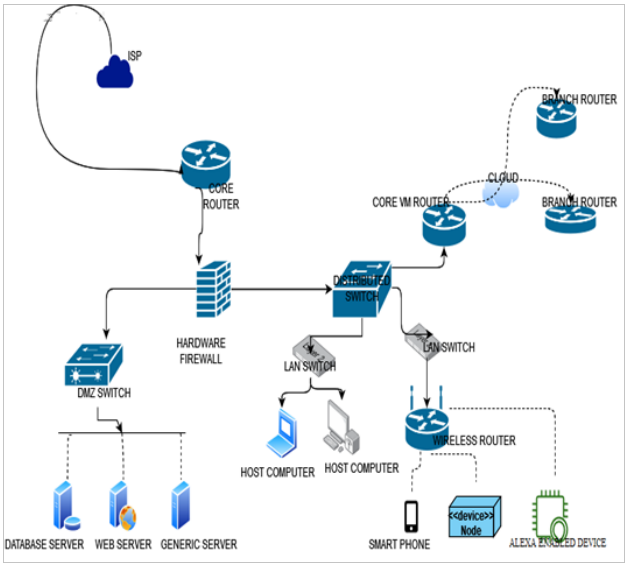


Figure 1. Designed Network Structure of AERE, BAEC

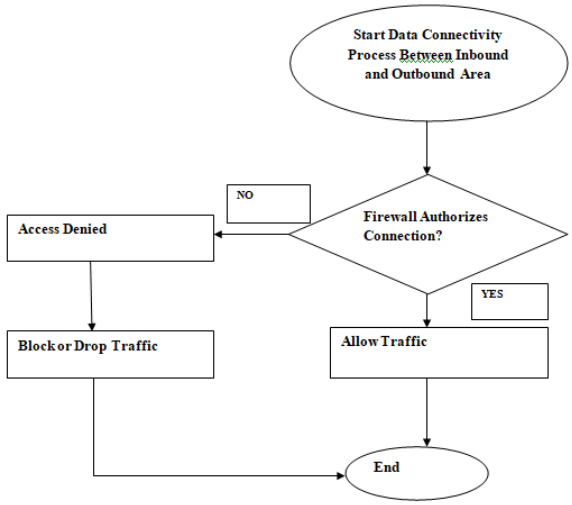


Figure 2. Traffic Access Flow using NGFW Firewall

Figure 3. Segmentation using NGFW Firewall at AERE

has been configured to filter and monitor network traffic within the ingress and egress zone. This firewall acts as a barrier between inbound and outbound traffic. In the Figure 1, the designed and developed network at AERE has been illustrated. In this designed and developed network a CISCO based hardware firewall has been configured between AERE core router and internal distributed DMZ switches. The ingress traffic and egress traffic has been controlled by implemented NGFW firewall policy. The firewall policy consists of a set of defined rules implemented by network administrator and organization which checks data packets coming from the Internet, extranet, servers or any external networking system to the inside network or traffic that outbound. Firewall drops, block, authorizes or permits network data traffic according to predefined firewall policy. In the Figure 2, secured network and application data traffic flow strategy diagram between AERE network and WAN has been shown. The configured NGFW firewall at AERE operates on the all seven OSI layer. It is not also capable of tracking active connections but also has the capabilities of tracking location based via geo-location databases, users, application, sessions, ports, services and IP addresses etc. The NGFW firewall is used to segment traffic between host and system, intrusion prevention and detection, content and application filtering, URL filtering, decrypting traffic, sandboxing etc.

A. *Segmentation*

Network segmentation is a kind of architectural network security approach in which network zones are divided into multiples segments to control traffic flow and improve monitoring activity. To implement firewall segmentation, the NGFW firewall needs to set policy and rules in a specific way in which secures network segmentation can be formed at desired network boundary and outside network via physical links or VLANS. By segmentation, the entire traffic crossing into NGFW firewall is being monitored and routed in secured way. The NGFW firewall segmentation is very much effective to prevent unauthorized connections and against malicious activity. Created NGFW firewall segmentation policy and rules for the inside zone IPs to WAN and vice versa at AERE network infrastructure is shown In the Figure 3

B. *Intrusion Detection and Prevention Using NGFW Firewall Policy*

Intrusion detection system (IDS) and intrusion prevention System (IPS) can be a standalone system within any network segment. IDS detect intrusions and miscellaneous network threats wherein IPS can not only detect but also prevent, block or drop identified intrusion and threats. IDS and IPS can be classified into LAN network based, wireless based, network behavior anomaly detection and host based. Considering NGFW firewall, both IDS and IPS can be integrated within it. Every kind of NGFW firewall is workable according to its predefined algorithm and heuristics. Specified policy and a set of rules need to be defined within NGFW firewall for the successful action of IDS and IPS.

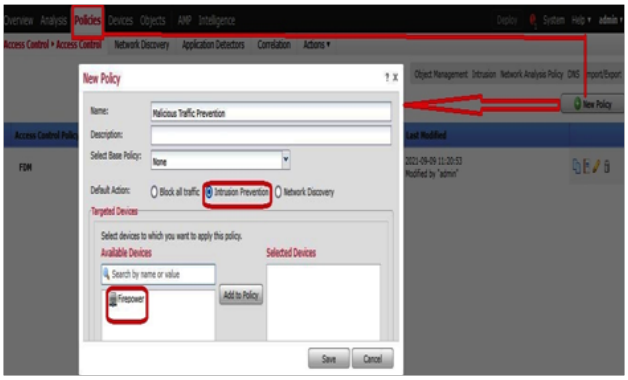


Figure 4. Intrusion Prevention System Policy Add at AERE NGFW Firewall

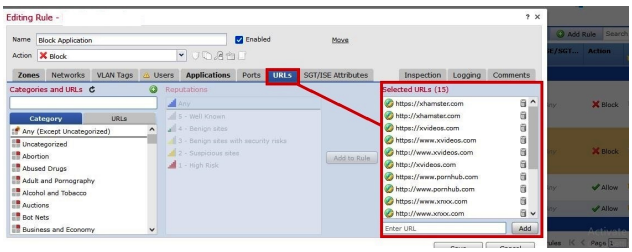


Figure 5. URL Policy Add procedure in NGFW firewall

In the Figure 4, IPS and IDS implementation configuration policy within CISCO NGFW firewall at AERE is shown.

C. Content, URL, Port and Application Filtering

NGFW firewall monitors the traffic and activate it IPS to protect the application and content that traverse within a vulnerable attacks. In such kind of activity, rules and policy are being applied to the NGFW firewall. URL, IP and Application filtering are being performed according to the predefined set of rules and policy implied by organization network administrator. For URL filtering, the NGFW checks its database for the list of domains and respective categorization. Based on categorization, firewall permits or blocks the specified domains of a network access. Usually, categories of domain which are not allowed to the network may contain websites that are related to hacking, nudity, phishing, dating, anonymizing services or violence etc. Similarly, different ports, services and specified local IP addresses can be filtered for blocking, allowing or dropping according to predefined set of NGFW firewall policy and rules. From the below Figure 5, Figure 6, Figure 7, and Figure 8 application filtering, URL filtering, ports filtering and specified user filtering policy configuration implementation strategy using CISCO NGFW firewall at AERE is shown.

D. Sandboxing

Sandboxing is the process of having cloud based platform that execute the specified files which contains malware or not. Sandboxing helps a user within the internet world to verdict before downloading a file whether it is malicious or

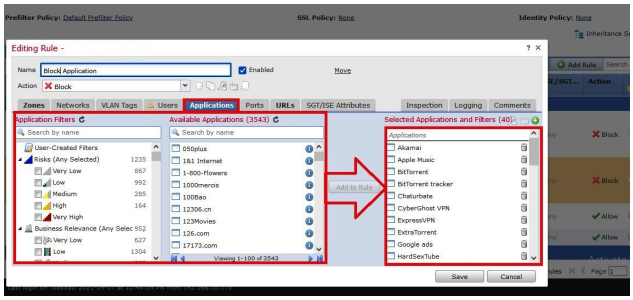


Figure 6. Application Filtering Procedure in NGFW firewall

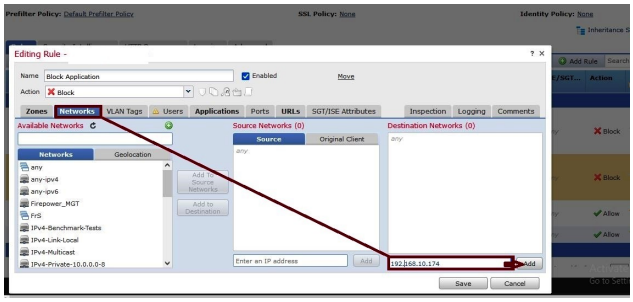


Figure 7. IP Filtering Procedure in NGFW firewall

not. In this modern era, many platforms provide sandboxing facility. Every kind of NGFW firewall has integrated sandboxing fancily by its own heuristic algorithm and process. In Sandboxing process, specified content like documents, pdf files, executive files, scripts, mscab files, audio or video files etc., are being executed. According to a set of malware policy or default policy within the NGFW firewall that has its own heuristic algorithm detects malware of files before being downloaded or uploaded. Sandboxing process helps to detect host receiving malware and intrusion within network trajectory. In the Figure 9, and Figure 10 Sandboxing process and Malware Policy configuration using CISCO integrated Sandboxing facility in NGFW firewall is shown.

E. Decrypting Traffic, Monitoring Unknown Traffic and Web Application Firewall

The NGFW firewall acts as decryption of traffic by installing desirable certificates. Decrypting traffic is needed

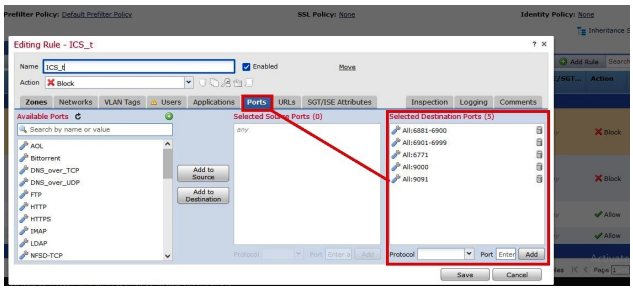


Figure 8. Port Filtering Procedure in NGFW firewall

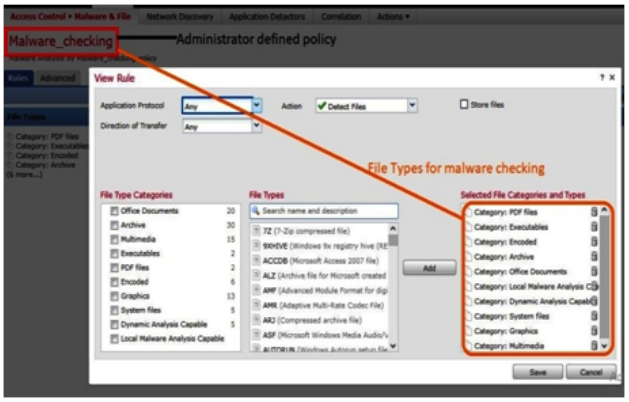


Figure 9. Malware Policy Configuration procedure in NGFW firewall

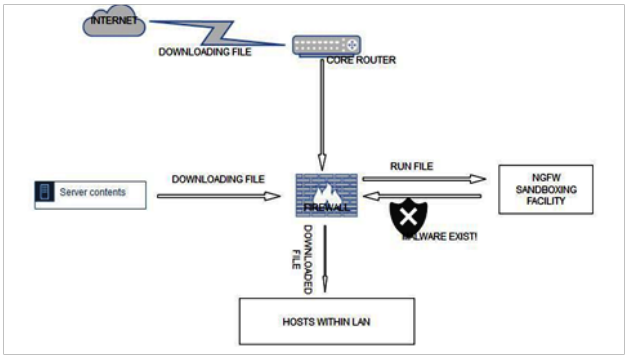


Figure 10. Malware Content Analysis Procedure by Sandboxing within NGFW Firewall

to inspect content threats. Decrypting traffic enhances network security within network. In some cases, decrypting traffic cannot be done. In such cases, the NGFW firewall categorizes that traffic as unknown traffic and classified the risk like low, medium or high level risks. The NGFW firewall takes action like block, drop or warnings to the user based on the risk category. By adding more features in HTTP protocol, the NGFW also acts as WAF (web application firewall) detect and stop vulnerable network threats. To protect threats on the HTTP protocol, the NGFW activity is more reliable and guaranteed.

F. Wireless Intrusion Prevention and Detection System (WIDPS)

Many high end NGFW firewall like CISCO firewall that integrates wireless intrusion detection and prevention system (WIPDS) monitors a wireless LAN network's access points signal, frequency spectrum and other security threats of wireless system. WIPDS of NGFW is able to analyze radio frequency of wireless access point and block unknown radio signal. To avoid MAC spoofing and man in the middle attack related attacks, WIPDS also provides MAC address filtering with DHCP connection or confined wireless secured network by IP-MAC bindings. WIPDS is capable of authorized connection with the access points. Sensors of specified access points and management servers within

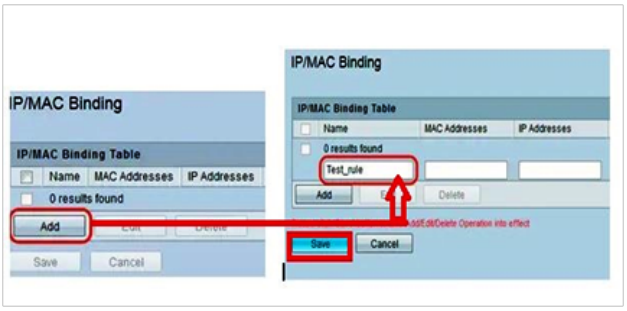


Figure 11. IP/MAC Bindings Procedure within NGFW Firewall

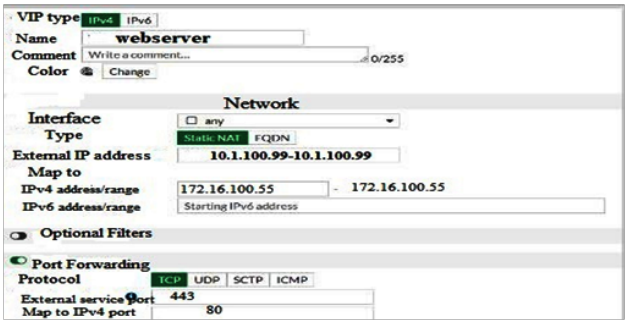


Figure 12. Port Forwarding Policy Add in NGFW firewall

LAN who takes appropriate action by receiving information by the sensors. Sensors, database servers which stores information and console of WIPDS all are integrated within a NGFW firewall that performs as a whole system. An IP/MAC binding is a kind of network security approach for the wireless access points security which can be configured by NGFW firewall. In the Figure 11, IP/MAC Bindings Procedure within NGFW Firewall is shown.

G. Port Forwarding

Port forwarding is a very popular and trusted policy to make a secured network. It maps one to none mapping. it translates public IP and ports to private IP and ports for packet data transmission Port Forwarding secures vulnerable port of potential devices from hackers where actual host and ports is unknown to the intruder. It completely avoids direct internet traffic. In the Figure 12, port forwarding policy within NGFW firewall has been shown where actual port 443 that listens is hidden within port 80 in private network.

H. Why NGFW CISCO Firewall at AERE is Efficient

Hardware firewall acts as foundation of network security at AERE network which has been configured between AERE CISCO core router and distributed switch. It performs as filter or barricade between internets services provider (ISP) and AERE LAN network. This configured firewall is used not only for controlling TCP and UDP access, traffic monitoring, NAT or VPN connections as layer 4 firewall do but also performs on every layer of seven (7) OSI layer. The configured CISCO based NGFW

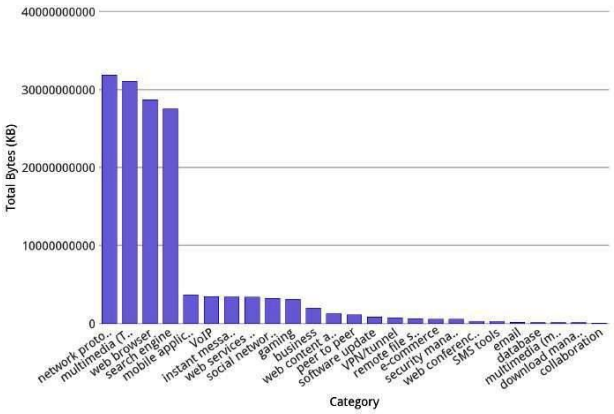
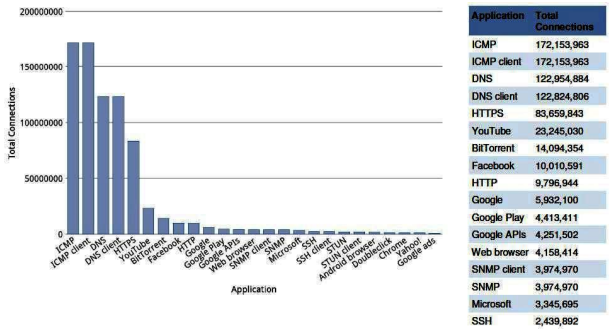


Figure 13. Used Data Traffic by Top Application Category within AERE Network



Application	Total Connections
ICMP	172,153,963
ICMP client	172,153,963
DNS	122,954,884
DNS client	122,824,806
HTTPS	83,659,843
YouTube	23,245,030
BitTorrent	14,094,354
Facebook	10,010,591
HTTP	9,796,944
Google	5,932,100
Google Play	4,413,411
Google APIs	4,251,502
Web browser	4,158,414
SNMP client	3,974,970
SNMP	3,974,970
Microsoft	3,345,695
SSH	2,439,892

Figure 14. Connection Initiated by Top Application by AERE Network User

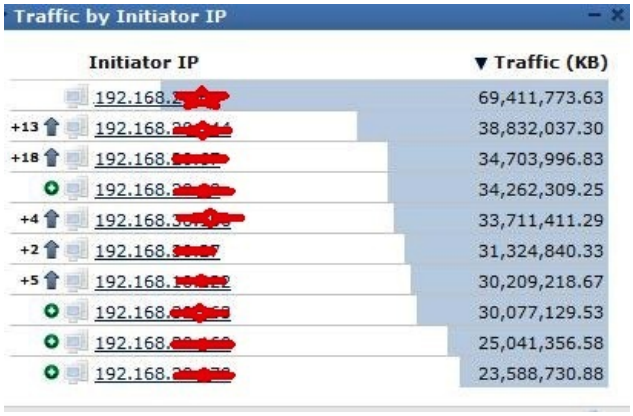


Figure 15. Top Ten Consumed Data User at AERE Network

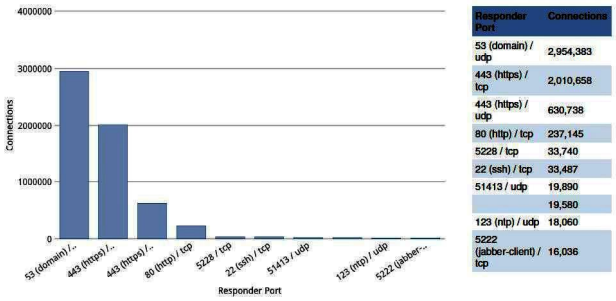
firewall covers the security feature in wide range area in terms of controlling LAN traffic monitoring, users, ports and sessions, application, file inspection, unauthorized login, decrypting traffic, Wi-Fi protection like MAC-IP filtering, man in the middle attack prevention, radio frequency control, malware intrusion detection and prevention, malformed network packets, IP spoofing prevention[1] [5] [7]. Its performance is satisfactory in terms of throughput, network access capacity, slowdown process and latency.

4. EXPERIMENTAL DATA ANALYSIS AND RESULTS

In this section, we have collected the statistical AERE network data within 2020-12-12 to 2021-12-12 time period. Then we have evaluated and analyzed these data in terms of different network security parameters. In a nutshell, this part obtains the detail description network data analysis using NGFW firewall.

A. Network Traffic or IP Monitoring

NGFW firewall plays an important role to analysis of data traffic that enters to a specified network or leaves from that network. The NGFW is capable of tracking IP initiator within the network, figure out data traffic by application risk category, traffic monitoring for miscellaneous application to track which application consumes the most traffic, connection by application etc. It also evaluates risky application from the initiated total connections within a network. To track these active network connections and analysis, the NGFW converts the network layer data in presentation layer by decoding network streams. In the Figure 13, we have investigated the result of application category that consumes the most traffic at AERE network. In the Figure 14, NGFW firewall at AERE illustrated the consumed data from total initiated connection according to application category. The NGFW provides clear overview of which specific local user consumes how much amount of data. From these data, we can achieve overall network user data & their used application data and internet browsing behavior etc. Based on these data, the administrator can control network data traffic, clustering zones, restrict user and application, allow or block or limit the local user internet usage, detect unrecognizable users. In a nutshell, based on user control policy of NGFW firewall, organization like AERE manages its network user and application services. In the Figure 15, the top most ten (10) network user of AERE is shown wherein In the Figure 16, NGFW firewall shows the result of the total connection initiated using different ports. These figures illustrate the overview of maximum consumed data user of AERE network and used ports for data connection.



Responder Port	Connections
53 (domain) / udp	2,954,383
443 (https) / tcp	2,010,658
443 (https) / udp	630,738
80 (http) / tcp	237,145
5228 / tcp	33,740
22 (ssh) / tcp	33,487
51413 / udp	19,890
	19,580
123 (ntp) / udp	18,060
5222 (jabber-client) / tcp	16,036

Figure 16. Responder Ports for Connection Request at AERE Network User

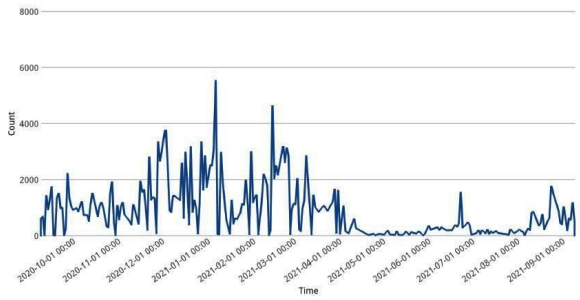


Figure 17. Initiated Intrusion Attacks Attempt Count over AERE Network

B. *Intrusion Attacks Detection and Prevention Data Analysis*

NGFW firewall is much effective to perform as a standalone system to detect and prevent intrusions. To drop or block the intrusions, every kind of NGFW uses its own heuristics algorithm and procedure. It can detect and prevent malware intrusions both on integrated network system and specific host of network parallel. In the Figure 17, the graphs illustrated the intrusion attacks attempts scenario over the AERE Network from December 2020 to September 2021 time period. The table 1 is the full classified details about the dropped or blocked miscellaneous intrusion attempts by the NGFW firewall. The NGFW firewall also detects the specified types of attack id occurred over network like web application attacks or SQL injection or network Trojan etc., under the classified intrusion events. To prevent this suspicious activity, the NGFW firewall blocks or drops the traffic and ensure only authorized access at the network.

C. *File Filtering, URL Filtering and Content Filtering*

For File filtering, every kind of NGFW firewall applies its own heuristic algorithm and data structure process to handle the miscellaneous file types. The NGFW firewall inspects every kind of file types within network when it's being downloaded or uploaded. The NGFW firewall applies it sandboxing to detect malware over the files. Then it drops or blocks that malware in those files. In the Figure 18, is the data of file types that are being inspected by NGFW firewall at AERE network. In the Figure 19, , we got the result of action taken by NGFW firewall over the malware affected files when being downloaded or uploaded. The NGFW firewall is effective to protect a network considering URL filtering. The content which can be accessed via http or https is being protected by NGFW. NGFW firewall can only accept the categories of domains according to firewall policy to the internal network users. It prevents user to access malicious content over http or https protocol by categorization database. As In the Figure 20, , we see that the mentioned URL of the figure cannot be accessed to the AERE network user as it is categorized as suspicious domain within NGFW firewall domain list. In the table 2, the NGFW firewall at AERE illustrated the application list that is associated with its allowed or denied connection number statistics according to NGFW policy.

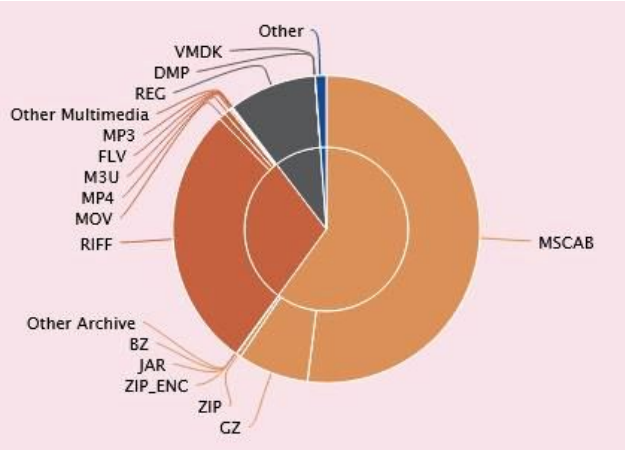


Figure 18. No. of Categorized Inspected File Types by NGFW Firewall

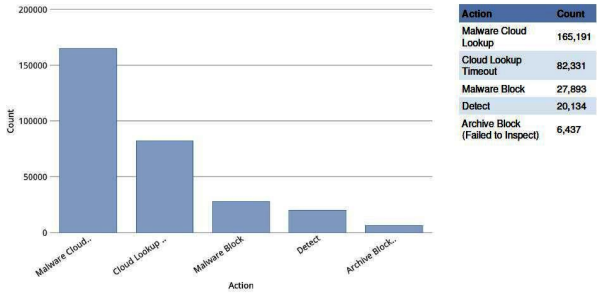


Figure 19. NGFW firewall Initiated Action against Infected Files

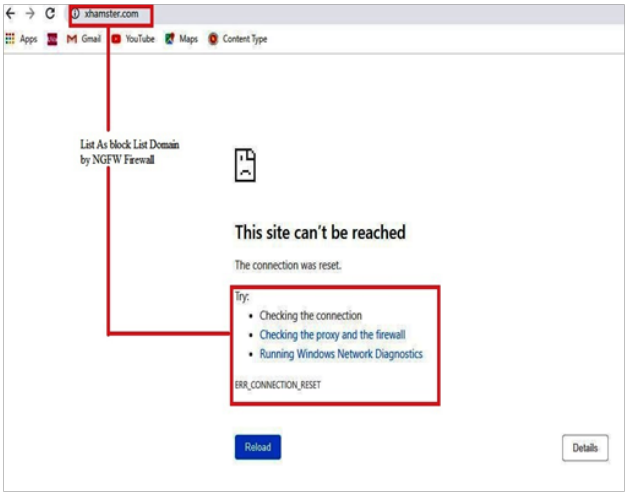


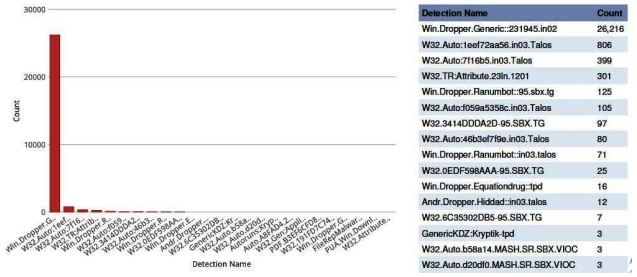
Figure 20. URL Content Blocked by NGFW Firewall for AERE Network User

TABLE I. NO. OF DROPPED OR BLOCKED CLASSIFIED INTRUSION ATTEMPTS BY NGFW FIREWALL AT AERE NETWORK

CLASSIFICATION	COUNTS
A Network Trojan was Detected	207,893
Attempted Administrator privilege Gain	264
Potential Corporate Policy Violation	230
Web Application Attack	220
Misc. Activity	24
Attempted privilege Gain	1

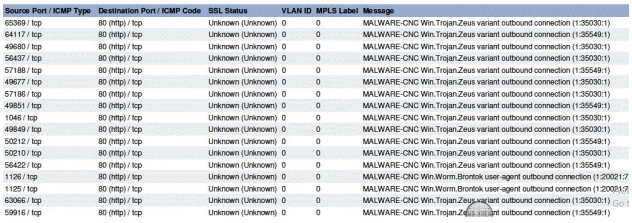
TABLE II. TABLE II. NO OF ALLOWED AND DENIED CONNECTION FOR APPLICATION AND CONTENT WITHIN APPLICATION BY NGFW FIREWALL AT AERE

Application	Allowed connection	Denied connection
ICMP	173,154,365	–
ICMP client	171,154,365	–
DNS client	112,859,033	–
YouTube	23,345,765	–
BitTorrent	14,101,160	–
Facebook	10,012,907	21
HTTP/ HTTPS	9,798,159	43,355
Google	5,933,624	–
XVideos	–	38,970
XVideos	–	1,536



Detection Name	Count
Win.Dropper.Generic::231945.in02	26,216
W32.Auto:1eef72aa56.in03.Talos	806
W32.Auto:7f16b5.in03.Talos	399
W32.TR:Attribute.23ln.1201	301
Win.Dropper.Ranumbot::95.sbx.tg	125
W32.Auto:f059a5358c.in03.Talos	105
W32.3414DDDA2D-95.SBX.TG	97
W32.Auto:46b3ef7f9e.in03.Talos	80
Win.Dropper.Ranumbot::in03.talos	71
W32.0EDF598AAA-95.SBX.TG	25
Win.Dropper.Equationdrug::tpd	16
Andr.Dropper.Hiddad::in03.talos	12
W32.6C35302DB5-95.SBX.TG	7
GenericKDZ:Kryptik-tpd	3
W32.Auto.b58a14.MASH.SR.SBX.VIOC	3
W32.Auto.d20df0.MASH.SR.SBX.VIOC	3

Figure 21. No. of Detected Malware Threats by NGFW Firewall



Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	VLAN ID	MPLS Label	Message
65369 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)
64117 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35549:1)
49680 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)
56437 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)
57188 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35549:1)
49677 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)
57186 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)
49851 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35549:1)
1046 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)
49849 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)
50212 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35549:1)
50210 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)
56422 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35549:1)
1126 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Worm.Brontok user-agent outbound connection (1:20021:7
1125 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Worm.Brontok user-agent outbound connection (1:20021:7
63066 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)
59916 / tcp	80 (http) / tcp	Unknown (Unknown)	0	0	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35549:1)

Figure 22. Detection of Malware Content Message using Port Scanning by NGFW Firewall

D. Malware Threat Analysis

Malware content can be attached within any files when being downloaded or uploaded or access any websites or with any suspicious mail attachment. It creates vulnerable situation to a network and associated host within a network. NGFW firewall detects specific malware content or ransomware and takes proper action against it. In the Figure 21 , gives the counted data about detected specified malware contents by different classified network attacks when the user of AERE browse the websites over the internet or download or upload file. Based on the detected malware contents the NGFW firewall takes appropriate action like blocking or dropping that malware or malware, cloud checking and clearing the specific files. For the prevention of these types of attacks, the NGFW firewall activates its intrusion detection and prevention role simultaneously. According to preventive steps, the NGFW secures a network and prevents download suspicious files or access malicious content based websites. A NGFW firewall plays a significant role to detect malware contents by port scanning. Port scanning is use to determine which service we can connect to. Hackers use ports scanning to access the host within a network. Network administrators implement policy or rules on NGFW firewall to get rid of unwanted scanning.In the Figure 22 , shows the identified malware content message by TCP port scanning at AERE network.

5. Conclusions and Future Work

Ensuring network and application security within an organization is a challenging task. Day by day variation of network and application threats is increasing in the world. To meet this challenge, every organization needs more research and broad security area. NGFW firewall is a fundamental network and application security tool that is used for different network and application data security, collecting analyzing data and security policy-making perspectives. An organization always needs to analyze the network data and take proper steps to improve its network

and application security area. In our research, we have tried to design a better network framework at AERE using CISCO-based NGFW firewall. Then we have set different firewall policies and rules according to the AERE network security perspective. According to firewall policy and rules, our configured firewall performs on the network on all seven OSI layers. We have collected statistical data and analyzed these data using the NGFW firewall in terms of different network and application security parameters. We investigated the effectiveness of NGFW firewall against various network and application threats. In the future, we will try to analyze data by integrating VPN for remote access, multilayer firewall within a network infrastructure. Advanced secured web systems integration on NGFW will be also our study area. Furthermore, our future works will also be comprised of performance evaluation of different firewalls in terms of throughput, network latency, and comparison network security parameters among those firewalls.

6. ACKNOWLEDGMENT

We are very grateful and thankful to Nuclear Cyber Security LAB of Institute of Computer Science (ICS), AERE, and BAEC to provide data and carry out this research work. [1] [2][3] [4][5][6][7][8][9] [10][11][12][13][14] [15]

REFERENCES

[1] "Cyber security tutorial homepage, https://www.javatpoint.com/cyber-security-tutorial,last accessed 2022/01/14."

[2] R. Alsaqour, A. Motmi, and M. Abdelhaq, "A systematic study of network firewall and its implementation," *International Journal of Computer Science & Network Security*, vol. 21, no. 4, pp. 199–208, 2021.

[3] "Cyber security tutorial homepage, https://www.w3schools.in/cyber-security, last accessed 2022/01/11."

[4] A. Chopra, "Security issues of firewall," *Int. J. P2P Netw. Trends Technol*, vol. 22, no. 1, pp. 4–9, 2016.

[5] G. I. P. V. Svoboda, J., "Network monitoring approaches: An overview," *Int J Adv Comput Netw Security*, vol. 5, no. 2, pp. 88–93, 2016.

[6] T. Hayajneh, B. J. Mohd, A. Itradat, and A. N. Quttoum, "Performance and information security evaluation with firewalls," *International Journal of Security and Its Applications*, vol. 7, no. 6, pp. 355–372, 2013.

[7] "Cyber security tutorial homepage, https://www.w3schools.com/cybersecurity, last accessed 2021/10/10."

[8] K. Ingham, S. Forrest *et al.*, "A history and survey of network firewalls," *University of New Mexico, Tech. Rep*, 2002.

[9] W. Konikiewicz and M. Markowski, "Analysis of performance and efficiency of hardware and software firewalls," *Journal of Applied Computer Science Methods*, vol. 9, 2017.

[10] K. Salah, K. Elbadawi, and R. Boutaba, "Performance modeling and analysis of network firewalls," *IEEE Transactions on network and service management*, vol. 9, no. 1, pp. 12–21, 2011.

[11] Z. Trabelsi, S. Zeidan, and K. Hayawi, "Denial of firewalling attacks (dof): The case study of the emerging blacknurse attack," *IEEE Access*, vol. 7, pp. 61 596–61 609, 2019.

[12] S. Dandamudi and T. Eltaeib, "Firewalls implementation in computer networks and their role in network security," *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, vol. 2, no. 3, 2015.

[13] S. Islam, H. Ali, A. Habib, N. Nobi, M. Alam, and D. Hossain, "Threat minimization by design and deployment of secured networking model," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 135–144, 2018.

[14] R. Dastres and M. Soori, "A review in recent development of network threats and security measures," *International Journal of Information Sciences and Computer Engineering*, 2021.

[15] M. S. Islam, M. Begum, K. Muntarina, and M. Golam, "A robust technique to encrypt and decrypt confidential data within image," *International Journal of Engineering Science Invention (ISSN)*, 2015.

Md. Shamimul Islam was born in Satkhira, Bangladesh, on 28th October, 1988. He received the B.Sc. and M.Sc. Degree in Computer Science and Engineering from the Jahangirnagar University, Bangladesh in 2011, and in 2012 respectively. He worked at Samsung R&D Institute Ltd., Bangladesh from 1 Oct, 2012 to 31 Dec, 2014 as a Software Engineer. From 27th July, 2016 to 27 June,2021 he has worked as a Scientific Officer of Computer Science Division in Bangladesh Atomic Energy Commission (BAEC). Currently he is working as senior scientific officer at institute of computer science in Bangladesh Atomic Energy Commission (BAEC). He is a member of Bangladesh Computer Society. His research interest includes Network and Cyber Security, Communication Engineering, IoT, Artificial Intelligence; Machine learning and Image Processing etc.

Mohammed Asraf Uddin is currently working as a Senior Experimental Officer in the Institute of Computer Science, AERE, BAEC, Dhaka. He has received his B.Sc from National University and M.Sc in Computer Science from Southern University Bangladesh. His research interest in database management system, Network security System, Artificial intelligence and Digital Images Processing etc.

Dr. Hossain has been working at Bangladesh Atomic Energy Commission (BAEC) for more than 18 years. He actively involves in the R&D, and training activities in BAEC. He received his PhD in Innovation Technology Management, MS in Electrical & IT Engineering from Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea, and BS in Electrical & Electronic Engineering from Chittagong University of Engineering Technology (CUET), Bangladesh. Hossain's research interest includes; (i) Nuclear innovations/knowledge management (ii) Nuclear cyber security, (iii) Computer security in nuclear facilities. His articles have appeared in several international

Dr. Md. Shakil Ahmed received his PhD in Computer Science from the University of Liverpool, UK. He also obtained his bachelor's as well as master's degrees, both in Applied Physics and Electronics, from the University of Dhaka, Bangladesh. His PhD research was in the area of 'Data Mining 'or 'Knowledge Discovery in Databases'. His current research interests include Data Mining, Decision Support System, Data Warehousing, Pattern Recognition, Expert System, and Distance Learning. He started teaching online postgraduate programmes with the University of Liverpool in 2002. Currently he is working as a Chief Scientific Officer at the Institute of Computer Science, Bangladesh Atomic Energy Commission.

Dr. Golam Moazzam is currently working as a professor in the department of computer science and engineering of Jahangirnagar University, Savar, Dhaka. He has received his B.Sc and M.Sc from the same department and later on received his Phd. from there. His research interest includes Database Management System, Digital Electronics, Data Structures and Algorithms, Digital Image Processing etc.