A COMPREHENSIVE STUDY ON FIREWALL FOR IOT DEVICES, POLICIES, AND SECURITY ISSUES

[1]KALUKHE SIDDHESH VIKAS SUSMITA, [2]KAILAS, [3]DEVASIS PRADHAN

[1,2]Final Year Students, [3]Assistant Professor
Department of Electronics & Communication Engineering, Acharya Institute of Technology
Dr. Sarvepalli RadhaKrishnan Road, Soladevanahalli, Bengaluru -560107
Email: - devasispradhan@acharya.ac.in

Abstract - As networked communications continue to expand and grow in complexity, the network has increasingly moved to include more forms of communication. The fourth industrial revolution is creating an environment in which everything will be interconnected and intelligent. Internet Of Things is the cornerstone of this new era. With the advent of the internet of things, privacy and security of sensitive data has become a major concern. As the tools used for an attack become more sophisticated with the use of Artificial Intelligence and Machine Learning. According to Threatpost, this year has seen a 100 percent surge in IoT infections observed over wireless networks. IoT devices are now responsible for 32.72 percent of all infections observed in mobile and Wi-Fi networks – up from 16.17 percent in 2019. The usage of IoT in different applications is expected to rise rapidly in the coming years. The IoT allows billions of devices, peoples, and services to connect with others and exchange information. Due to the increased usage of IoT devices, the IoT networks are prone to various security attacks. The deployment of efficient security and privacy protocols in IoT networks is extremely needed to ensure confidentiality, authentication, access control, and integrity, among others. In this paper, an extensive comprehensive study on security and privacy issues related to Firewall for IoT Devices.

Keywords - Firewall; Firewalling; IoT; Network; Security; Policies

I. INTRODUCTION

IoT security is involved in Low Power Wide Area Network LPWAN, the IoV, wearable devices, and other industries. A wide range of devices are connected to the internet in a home-network scenario. These IoT devices are mostly sensors which are low powered, low compute and have limited resources. To assess the security properties of Smart Home installations, it is important to consider the basic security challenges that occur in installations of IoT devices. Some manufacturers have produced and sold IoT devices that do not include sufficient security features. This has resulted in serious harm, both economic and otherwise, to specific parties and to the general public. The Major security issues are Identity and Authentication, Access Control, Protocol and Network Security, Privacy, Trust and Governance, Fault Tolerance.

The main concept behind IoT is not only to integrate multiple appliances, device to one processing unit, but to also make the whole network portable. The present Firewalls have to connect the user Subnet through a wire and from the Firewall to the Default Gateway has to be a wired connection. Although some new Firewalls allow the Subnet to be WLAN but Firewall to Gateway connection has to be a wired connection. This makes the IoT structure static and the portability of IoT is reduced. Thus we came up with a Firewall Device which is portable, strong and cost efficient.

Nowadays the adoption rate of IoT devices is very high, more and more devices are connected via the internet. According to appraisal [3], there are 30 billion connected things with approximately 200 billion connections that will generate revenue of approximately 700 billion euros by the year 2020. Now in China, there are nine billion devices that are expected to reach 24 billion by the year 2020. In future, the IoT will completely change our living styles and business models. It will permit people and devices to communicate anytime, anyplace, with any device under ideal conditions using any network and any service [4]. The main goal of IoT is to create Superior world for human beings in the future. Fig. 1 shows the concept of IoT with their capabilities.

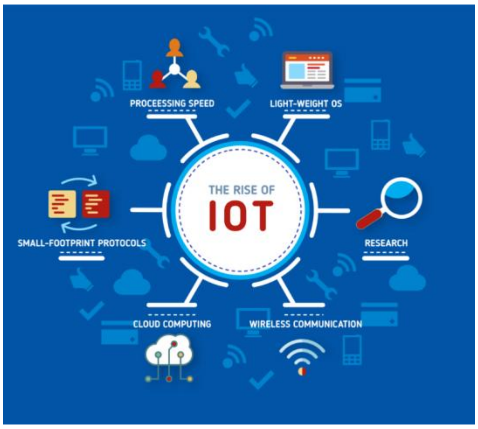

Figure 1. Concept of IoT

II. IOT ERA

The IoT era As networked communications continue to expand and grow in complexity, the network has increasingly moved to include more forms of communication. This has ushered in the era of the Internet of Things (IoT). No longer dependent upon person-to-person interaction, communications are made directly between simple devices, or between simple devices and complex systems. These connections between millions of IoT devices create demand for new services, unlocking new business opportunities to improve efficiency and quality of service. IoT technology is expected to spread exponentially across many industries, with growth estimated to surpass 20 billion connected devices by 2021. 1 Within the Internet of Things, Communication Service Providers play an important role. This role can vary widely from, for example, a focus on offering IoT centric connectivity, like LoRA (long range) and LTE-M (Long Term Evolution (4G), category M1), to more advanced IoT services, including hosting IoT applications and offering IoT security services.

III. FIREWALL

Traditionally, the firewall was placed as a gatekeeper on the network edge. It acted as an all-encompassing control point, inspecting network traffic as it traveled across this perimeter. Sitting at the network's ingress/egress point, the firewall was responsible for validating communications: internal network traffic was considered inherently trustworthy, and external traffic was considered inherently untrustworthy. Rule sets and policies were created and enforced at this single point of control to ensure that desired traffic was allowed into and out of the network and undesirable traffic was prevented.Fig.2 shows traditional concept of Firewall.

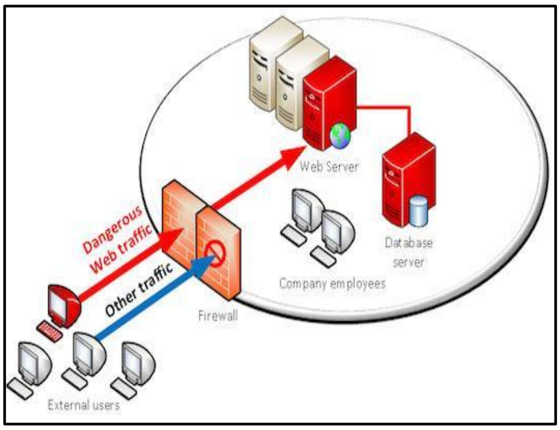

Figure2. Traditional network firewall approach

IV. WHY FIREWALLING?

As our networks evolve to accommodate new ways of doing business, so too must our network security. In the current world of distributed IT assets, the firewall is still central to a robust security posture. However, firewall requirements have increased significantly to protect the wide array of network infrastructures, connected devices, and operating systems from advanced threats. Consequently, our "traditional" firewall devices are being augmented by a mixture of physical and virtual appliances—some are embedded into the network while others are delivered as a service, are host-based, or are included within public cloud environments. Some are even taking on new form factors, such as clustered appliances that scale to large traffic requirements, software that runs on personal devices, SD-WAN routers, and secure Internet gateways.

The activity of sharing threat intelligence across all these disparate firewall devices, regardless of their location, is vital for uniform threat visibility and a strong security posture. To make the full shift and better secure today's networks, businesses must move away from the traditional "perimeter" approach. Instead they've got to establish strategic enforcement points across the entire network fabric, closer to the information or applications that need to be protected.

V. WHAT IS FIREWALLING?

Firewalling can provide an agile and integrated approach for centralizing policies, advanced security functionality, and consistent enforcement across your increasingly complex, heterogeneous networks. It should deliver comprehensive protections, visibility, policy harmonization, and stronger user and device authentication. Firewalling should also benefit from the sharing of threat intelligence across all control points to establish uniform threat visibility and control—dramatically cutting the time and effort needed to detect, investigate, and remediate threats.Enforcement points are everywhere across today's heterogeneous networks. Figure 3. shows Firewalling is delivering consistent threat prevention functionality with consistent policy and threat visibility so you can prevent, detect, and stop attacks faster and more accurately, everywhere.

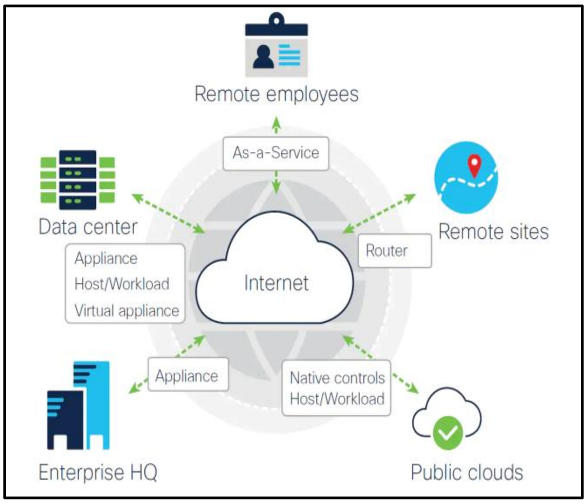

Figure3. The core tenants of firewalling as a means to address the security challenges of modern networks

VI. TYPES OF FIREWALL

6.1 Packet Filter Firewall

Packet filtering applies a set of rules to each packet and based on outcome, decides to either forward or discard the packet. A packet filtering router should be able to filter IP packets based on information included source IP address, destination IP address, TCP/UDP source port and TCP/UDP destination port. It is used to block connections from specific hosts or networks, block connections to specific hosts or networks, block connections to specific ports and block connections from specific ports. In Packet filtering IP packets are either forwarded or discarded without checking their contents . This type of firewall allows all traffic between "trusted" hosts. All the packets that are incoming to the networks will be checked in detail by the packet filtering firewall. The firewall system checks basic information that resides in the packet such as source and destination address, source and destination port numbers, protocol and others that are related. Then, a comparison will be made between information on the packets with the rules, which had been configured on the firewall system.

6.2 Stateful Packet Inspection firewall

Stateful-inspection is an enhancement of the packet filter technology. Besides inspecting individual packet content, the Stateful-inspection also inspects the attributes of the multi-packet flows. A dynamic or "stateful packet inspection" also referred to as connection–state filtering packet in which firewall maintains a table of active TCP sessions and UDP sessions. Each entry in the state table records the sessions, source and destination IP address and port numbers and the current TCP sequence number. Entries are created only for those TCP connections or UDP streams that satisfy a defined security policy. The packets associated with these sessions are permitted to pass through the firewall. Sessions that do not match any policy or any packets received that do not match an existing table entry are denied [2]. It only allows packets belonging to an allowed session so it is more secure than packet filtering. A stateful inspection firewall ensures that packets belong to an existing session and it can authenticate the user when the session is established. Firewall system checks each field in the IP packet like the source address, destination address, protocol type(TCP, UDP and others), port number and service type(Telnet, FTP and others). It records all detailed information of each and every packet that passes through the network in a log file [4]. The rules that are used for filtering will be applying based on that information. In addition, it examines the packet header information from the network layer of the OSI model to the application layer to verify that the packet is part of a legitimate connection and the protocols are behaving as expected.

6.3 Application-gateway firewall

An application-gateway firewall [3] is simply a type of proxy server that provides proxies for specific applications. The most common implementations of application gateway firewalls provide proxy services, such as mail, file transfer protocol (FTP) and telnet, so that they do not run on the actual firewall, which increases security. The source or destination Internet protocol (IP) address, however, can be used to accept or reject incoming connections. Application Level firewalls also determine permissible conditions and events when a proxy connection has been established. An FTP proxy can restrict FTP access to one or more hosts by allowing the get command and at the same time, preventing the put command. A telnet proxy can terminate a connection if the user attempts to perform a shell escape or to gain root access. Application-gateway firewalls are not limited only to applications that support TCP/IP services, however. These tools can similarly govern conditions of usage for a variety of applications, such as financial or process control applications.

The two basic types of application-gateway firewalls are:

1) Application-generic firewalls
2) Application-specific firewalls.

The application-generic type provides a uniform method of connection for every application, regardless of type [5]. The application-specific firewall determines the nature of connections to applications on an application-by-application basis.

Application-gateway firewalls are the best-selling of all types of firewalls. Nevertheless, they have some notable limitations. Most significantly, for every TCP/IP client for which the firewall provides proxies, the client must be aware of the proxy that the firewall runs on its behalf. Therefore, each client must be modified accordingly. A second limitation is that, unless one uses a generic proxy mechanism, every application needs its own custom proxy.

6.4 Network Address Translation (NAT) Firewall

Network address translation allows a network to use one set of network addresses internally and a different set when dealing with external networks. Network address translation does not provide any security by itself but it helps to hide the internal network layout and to force connections to go through a choke point. The choke point does the translation. Like packet filtering, network address translation works by having a router do extra work. In this case, not only does the router send packets on, but it also modifies them. When an internal machine sends a packet to the outside, the network address translation system modifies the source address of the packet to make the packet look as if it is coming from a valid address. When an external machine sends a packet to the inside, the network address translation system modifies the destination address to turn the externally visible address into the correct internal address. The network address translation system can also modify the source and destination port numbers (this is sometimes called Port and Address Translation or PAT).

6.5 Proxy firewall

Application proxy firewalls are also more secure than packet filtering, but are generally slower than stateful inspection. Two TCP connections are established in an application proxy firewall: one between the packet source and the firewall, another between the firewall and the packet destination. Application proxies intercept arriving packets on behalf of the destination, examine application payload, and then relay permitted packets to the destination [3]. It is called a proxy server, because it acts as a deputy or substitute and decides about flow of applications. Internal users contact the proxy server using HTTP or TELNET. The proxy servers ask the user about a remote host with which the user wants to set up a connection for actual communication. The proxy server now accesses the remote host on behalf of the user and passes the packet of the user to the remote host. The proxy changes the IP address in the packets from the end user’s IP address to its own. Thus the IP address of the computer of the internal users is hidden from the outside world.

VII. EMBEDDED FIREWALL WITH IOT DEVICES

A firewall provides the missing layer of security for embedded devices, blocking attacks that authentication and encryption can’t. The firewall must be efficient, consuming minimal system resources and scaling to a wide range of devices, from small 8-bit systems running a minimal or no operating system to a sophisticated multi-core system running a commercial real-time operating system (RTOS). Desktop firewalls don’t meet the needs of embedded devices. Windows and Linux-based firewalls, while effective, are large and aren’t easily portable to small embedded devices. They also include filtering that isn’t relevant for embedded devices.

Most recent embedded systems include a network interface. Some provide password protection or encrypted protocols such as SSH or SSL, but they aren’t enough. If they were, we wouldn’t be reading about security breaches in the popular media. Older systems are even more vulnerable. Their original designers often assumed they were part of a closed “safe” network and omitted security, but many are now connected to a more open network with no protection at all.

These devices need a resource-friendly security solution specifically designed to provide sensible defensive capabilities against a variety of Internet-based attacks. Embedded firewalls provide an ideal solution. The firewall is integrated directly into the communication stack at the link layer of the supported protocol and configured with a set of rules specifying what communication is allowed.

VIII. EXTENDING SECURITY CONTROLS

Under the premise of a traditional firewall, since all internal traffic and authorized users were inherently trustworthy (and external traffic wasn’t), protecting the entire organization was accomplished at the network perimeter. This network perimeter became the logical security control point to protect the entire organization. All network traffic, whether originating from the headquarters, a data center, or remote worker, was funneled through this single control point.

With a firewalling approach, consistent security controls are deployed to provide full visibility, unified policy, and comprehensive threat visibility. These security controls enable stronger user and device authentication across increasingly heterogeneous environments. They gather, share, and respond to context about users, locations, devices, and more to ensure devices meet defined security requirements. Using consistent security controls at every micro-perimeter, security teams can start to automate tasks (such as auto-quarantine out-of-compliance users and devices, block questionable domains across all security controls, and support effective microsegmentation). In firewalling, full visibility provides a holistic view of all security alerts and indicators of compromise, and shared threat intelligence delivers the most up-to-date threat detection to any connected device.

IX. CLOUD-BASED MANAGEMENT

Firewalling promotes a stronger security posture by supporting centralized, cloud-based management to help security teams cut through complexity and align policies throughout the organization. Templates can improve policy design and consistency by writing a policy once and scaling its enforcement across tens of thousands of security controls throughout a network. The use of standard policy templates to rapidly deploy new devices helps reduce configuration errors.

As organizations grow, new deployments automatically inherit the latest policies. A scalable policy management system integrates multiple security features into a single access policy and optimizes policies across security devices to identify inconsistencies and quickly correct them.cloud-based management solution takes a team’s capabilities to the next level. They can quickly identify risks across all devices, bringing them to a more consistent and secure state. With a single management console, objects can be compared across all devices to uncover inconsistencies and optimize the current security posture. Personnel can streamline policy management, improve efficiency, and achieve more consistent security while reducing complexity.

X. IOT SECURITY THROUGHOUT THE NETWORK

Interconnected networks of IoT devices include multiple points of vulnerability, each of which requires its own security solution. Most IoT security solutions focus on providing security within the device itself. Data centers create an additional point of vulnerability. Virtually all IoT devices communicate to applications via centralized or distributed data centers, creating a well recognized need to protect these servers against attacks and data breaches. The IoT Firewall is a User-Plane firewall, deployed in the Service Provider's core network, that features key differences from traditional network firewalls to allow better efficiency when deployed within the IoT domain. The IoT Firewall provides device-aware, application-centric firewall policies. This allows Service Providers to offer IoT security services without the need to host the IoT application in their data centers, or directly manage the IoT application. The primary security threats mitigated by the IoT Firewall are:

1) Network threats: The IoT Firewall prevents DDoS (Distributed Denial of Service) and application-layer attacks which may disrupt the integrity and availability of the Service Provider's network.
2) Device threats: IoT Firewall ensures that devices are only connecting to 'safe' locations and prevents devices from connecting to unknown services. This reduces the chances of devices being compromised through malware and blocks malicious 'ThingBot' C&C (command and control) communication to stop devices from being exploited remotely.
3) Service abuse: This capability prevents IoT devices from being used unexpectedly, which can result in revenue leakage for the Service Provider or the application owner (for example, stopping a connected car SIM from being used in another device to stream Netflix).

XI. CHALLENGE

IoT is one of the biggest contributors to the rising importance of the network edge. As the number of network devices grows, so does network vulnerability—more devices represent a greater threat target. Most IoT devices are narrowly focused with limited power, memory, and bandwidth—they cannot prioritize security features or even allow for software patches. Once breached, an IoT device is one of the easiest ways for hackers to gain network access and move horizontally to launch a system-wide attack in search of sensitive and confidential data.

A quick glance at the latest headlines shows why dynamic security is more important than ever. IT teams are figuring out how to effectively create, enforce, and manage consistent security policies without adding complexity. Network segmentation is an old but reliable way to implement a security strategy that minimizes threats and protects valuable resources and data. And with an Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) architecture, policies and workloads can move seamlessly across and within various enterprise sites.

XII. CONCLUSION

Applying IoT technology yields both opportunities and security risk, so the challenges with IoT devices in relation to security are huge. A careful assessment of security risk must precede any IoT implementation to ensure that all the relevant, underlying problems are discovered. Without sufficient data security and data protection, IoT will not be successful in the long run. Therefore, every IoT manufacturer is challenged to complement all phases of development processes through to the operation of the equipment with appropriate security measures. In future work, it is important to develop a framework for realizing and evaluating security risk within IoT to ensure confidentiality, integrity and availability.

REFERENCE

[1] D. J. Cook et al., "MavHome: An agent-based smart home," IEEE International Conference on Pervasive Computing and Communications, San Diego, CA, USA, pp. 521-524, 2003

[2] N. King, "Smart home - A Definition," Milton Keynes: Intertek Research and Testing Centre, 2003

[3] Statista, 2015 [Online]. Available: https://goo.gl/89rRIa

[4] August and Xfinity, "The Safe and Smart Home: Security in the Smart Home Era," 2016 [Online]. Available: http://goo.gl/UGWb5Z

[5] V. Srinivasan et al., "Protecting your daily in-home activity information from a wireless snooping attack," 10th international conference on Ubiquitous computing, pp. 202-211, 2008

[6] B. Ur et al., "The current state of access control for smart devices in homes," Workshop on Home Usable Privacy and Security, 2013

[7] S. Notra et al., "An experimental study of security and privacy risks with emerging household appliances," IEEE Conference on Communications and Network Security, pp. 79-84, 2014

[8] V. Sivaraman et al., "Network-level security and privacy control for smart-home IoT devices," Wireless and Mobile Computing, Networking and Communications, pp. 163-167, 2015 [9] T. D. P. Mendes et al., "Smart home communication technologies and applications: Wireless protocol assessment for home area network resources," Energies, vol. 8, no. 7, pp. 7279-7311, 2015

[9] C. Debes et al., "Monitoring Activities of Daily Living in Smart Homes: Understanding human behavior," IEEE Signal Processing Magazine, vol. 33, no. 2, pp. 81-94, 2016

[10] C. Lee et al., "Securing smart home: Technologies, security challenges, and security requirements," IEEE Conference on Communications and Network Security, pp. 67-72, 2014 [12] K. Islam et al., "Security and privacy considerations for wireless sensor networks in smart home environments," Computer Supported Cooperative Work in Design, IEEE 16th International Conference on, pp. 626- 633, 2012

[11] H. Chan and A. Perrig, "Security and privacy in sensor networks," Computer, vol. 36, no. 10, pp. 103-105, 2003

[12] M. Abdur Razzaq, R. A. Sheikh, A. Baig, and A. Ahmad, “Digital image security: Fusion of encryption, steganography and watermarking,” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 5, 2017.

[13] S. Singh and N. Singh, “Internet of things (iot): Security challenges, business opportunities & reference architecture for e-commerce,” in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE, 2015, pp. 1577–1581.

[14] K. Rose, S. Eldridge, and L. Chapin, “The internet of things: An overview,” The Internet Society (ISOC), pp. 1–50, 2015.

[15] H. Ning, H. Liu, and L. T. Yang, “Cyberentity security in the internet of things,” Computer, vol. 46, no. 4, pp. 46–53, 2013.

★★★