ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

Adding Intellegence to the Internet of Things (IoT)

[1] Suresh.H [2] Ravindra S Hegadi
Rayalaseema University, Kurnool (A P)

Abstract: **-- Many people view a firewall as a device to block access to undesirable websites, which is partially true. Emphasis must also be given to blocking requests from the internal network towards the Internet or external network, using undesirable services. This control is still not seen in many implementations.**

***Keywords*:-- Internet of Things; IOT; Firewall; PSsense**

I. INTRODUCTION

The Internet of Things (IoT)1 is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.

II. REAL TIME USAGE

A. Evolution of IoT

IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS), micro services and the internet. The convergence has helped tear down the silo walls between operational technology (OT) and information technology (IT), allowing unstructured machine-generated data to be analyzed for insights that will drive improvements.

B. Development behind the Internet of Things

IPv6's huge increase in address space is an important factor in the development of the Internet of Things. According to Steve Leibson, who identifies himself as "occasional docent at the Computer History Museum," the address space expansion means that we could "assign an IPV6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths." In other words, humans could easily assign an IP address to every "thing" on the planet. An increase in the number of smart nodes, as well as the amount of upstream data the nodes generate, is expected to raise new concerns about data privacy, data sovereignty and security.

C. Practical Application of Iot

Practical applications of IoT technology can be found in many industries today, including precision agriculture, building management, healthcare, energy and transportation. Connectivity options for electronics engineers and application developers working on products and systems

III. PROBLEM RELATED TO DATA SECURITY

When it comes to data integrity and automation of data their lies a loop hole as there is no human intervene. If irrelevant data gets integrated with the next set of chain it leads to serious chain and interdependent issue. Setting up an intelligent firewall helps to some extent but not always as we lack in the defining the source which leads the cause. Many people view a firewall as a device to block access to undesirable websites2, which is partially true. Emphasis must also be given to blocking requests from the internal network towards the Internet or external network, using undesirable services. This control is still not seen in many implementations.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

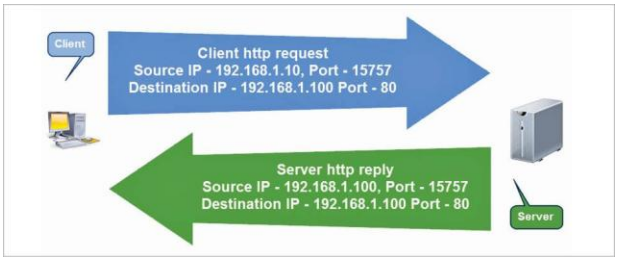

Fig. 1. Concept of Parts

For example, a firewall not configured to block undesirable services will not block malicious software such as viruses, worms, spyware, etc, from sending emails out using email services such as SMTP or from sending outgoing traffic using non-standard ports. This type of traffic could also lead to blacklisting of your static IP address. When these unblocked services infiltrate with our data in the network if the depended IoT objects it leads to catastrophic results. It is crucial that services blocking is enabled along with website filtering to ensure correct firewall configuration.

A. The concept of the port

To explain it in simple terms, imagine a server connected to a single client by a crossover cable. This server is running three different services – HTTP, SSH and FTP. The client system is trying to access these services simultaneously using only one physical cable. This gives rise to two questions:

1. How does the server differentiate between the requests received from different clients? How does it determine which packet is for which service?

2. How does the client differentiate between the replies received from the server? How does it determine which packet is received as reply to which request sent earlier?

The answer lies in the concept of a port – different services run on different ports. The HTTP service runs on Port 80, SSH on Port 22, FTP on Port 21, and so on. In all, there are 65,535 ports.

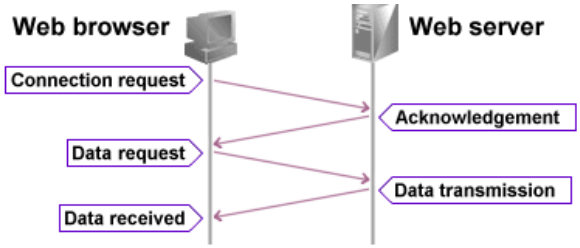

Fig 2. Data Transmission without firewall

While sending requests to the server, the client sends the IP address of the server as part of the IP header and the port number for the service as part of the TCP header. In addition, the client also sends the self IP address as the source IP address, and adds a randomly generated source port as the source port number.

While replying, the server reverses the source and the destination IP addresses so that the packet reaches the client, and also reverses the source/destination port numbers for the client to understand which packet belongs to which service request.

The handshake remains the same for multiple clients and servers. The source and destination IP addresses identify the client and the server, while the source and destination ports identify the service request and the reply. See Figure 1 for quick understanding.

B. The Firewall Configuration Scenario

Let us consider a typical requirement for a company, which would be to allow access depending on the work profile of employees. Let's assume that there are three groups – admins, engineers and accountants with various access requirements.

The first step is to prepare a basic Access Control List (ACL), a sample of which is shown in Table 1. We will use this ACL to configure pfSense for this article. Discussions should be held with all computer users to try and find all the services and websites being used by them, in order to create ACLs. Employees should be asked whether they use a specific website frequently or not. For instance, during such discussions, a website being used once in three months might get

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

identified, which runs on a non-standard port 8080. In the example given in Table 1, it could belong to the Pune Municipal Corporation local body tax division.

Please discuss in detail with computer users and have the patience to create these lists. The more details you get, the fewer reconfiguration calls will be needed later.3

Identify internal IP addresses, external IP addresses, external host names and services required for controlling access, etc. For example, for allowing Gmail access, we need to configure three groups:

1. Gmail Services Port alias group containing the following TCP services (ports) required for Gmail access:
   - IMAPS – 993
   - SMTPS – 465
   - POP3S – 993
   - Submission – 587

2. Gmail Servers IP alias group containing IP addresses for the following servers:
   - smtp.gmail.com
   - imap.gmail.com

3. Group of internal systems required to access Gmail using the mail client.

Table 1. Server Settings and Requirement

Internal Group	External access requirement	Port alias group	External IP alias group
Internal Network	DNS Servers	TCP, UDP, 53	DNS Servers
Admin	Mailing Services to access Gmail using mail client	Gmail Services	Gmail Servers
	Additional Mail Server using SMTP and POP Services	Mail Services	Mail.company-mail.com
	Web browsing	Internet services	Any
	Admin Console of additional mail server	8085	www.mailserver.com
Engg	Mailing Services to access Gmail using the Mail Client		Gmail Servers
	Customer Site FTP Access	FTP Services	ftp.customersite.com
Accounts	Mailing Services to access Gmail using the mail	Gmail Services	Gmail Servers
Internal Group	External access requirement	Port alias group	External IP alias group
	client		
	LBT Pune Website	8080	www.website.com

Think about how to group various internal/external IP addresses and services to create the minimum number of access rules. Create IP and ports alias lists from Firewall – Alias menus.

REFERENCES

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was

[1]http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. (references)

[2] http://opensourceforu.com/2016/09/pfsense-adding-firewall-rules-to-filter-services/

[3]https://doc.pfsense.org/index.php/Installing_pfSense.