INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Infrastructure security- Data transfer protection from attacks in named data network

Rajeshwari K R
ashu.keeru@gmail.com
Bangalore Institute of Technology,
Bengaluru, Karnataka

R Nagaraja
profrnnagaraja@gmail.com
Bangalore Institute of Technology,
Bengaluru, Karnataka

ABSTRACT

In recent times, Attacks have become widespread, and they are difficult to detect in networks. It is because of their neighboring, simple and effective characteristics, Denial of Service (DoS), Distributed DoS attacks are recognized as one of the main threats faced by Network Services. To cope with the attacker problem, we have proposed a solution for Infrastructure security for the data transmission in the Named Data Network (NDN) by File Transfer Protocol (FTP), which combines the data encryption, satisfies the requirement of secure data transfer and also using dynamic routing protocols for secure webpages, file access through the routers from an unauthorized access.

We have to check whether the user is the third party or not. If the user is the third party then he fails to login within the limited access time then admin will block that particular IP address. By this, we can provide a satisfied level of security to the infrastructure of the organization. This is simulated in Cisco Packet Tracer.

Keywords: *Named Data Network, Encryption, File Transfer Protocol, Router, IP Address.*

1. INTRODUCTION

This Chapter is to discuss the introduction to the issues of the network, infrastructure security for Named Data Network (NDN) to protect from attacks that face in the organizations. Here is a brief introduction to the existing problems and methods of providing secure file transfer to the legitimate users by avoiding the attackers to the routers or servers in the network architecture.

The technological communication network was a grid-based wireless Adhoc network, where a multiple-hop end-to-end transmission was assumed to be established only when an actual social relationship existed between the end users. The scientific communication network was an intermittent MANETs, in which only a pair of mobile users sharing an actual social relationship were permitted to exchange their information when they find each other within the reliable response range. This network was a generic communication medium, such as a face-to-face or telephonic conversation. Named Data Network (NDN), which is based on data itself, was brought about to deal with some authentication problems. It is novel network architecture, which is for communication built on hierarchically named data. It is one of the trusting Information-Centric Networking (ICN) architecture. If the unauthorized user is logged on to the router it will consume all the information from it and automatically that router will shut down. This information has to send to the server. Here the OSPF and Enhanced Interior Gateway Routing (EIRGP) protocols are maintain the neighbor relationships with adjacent routers in the same area and uses same autonomous system number (ASN).

The main issues come in Wi-Fi networks are very common threats and network hacking attempts. To transfer the data file in a safer and secure way over a network has become a major challenge for the organization. A un-authorization event and the network security measures defined that, how using the network security tools, a better and safe network can be designed and maintained for an organization. Today the IT industries are facing the greatest challenges in the network and application infrastructure are off because of the active attacks like DoS attacks Figure 1.

These attacks are as mentioned before in this chapter as a disruption. The Distributed DoS (DDoS) attacks are referred to as cat- and- mouse and DoS attacks with the single host are infrequently successful in casting a massive damage by Xian Jun Geng and Andrew B. Whinstone. The Dos against Domain Name Server (DNS) could be even more disastrous as the entire

internet infrastructure is built on it. The protocol establishes a framework between network routers in order to achieve default gateway failover if the primary gateway becomes inaccessible, in close association with a rapid-converging routing protocol like EIGRP or OSPF. HSRP routers send multicast Hello messages to other routers to identify them of their significances (which router is preferred) and current status (Active or Standby). The primary router with the highest configured priority will act as a virtual router with a pre-defined gateway IP address and will respond to the Address Resolution Protocol (ARP) or Named Data (ND) request from machines connected to the Local Area Network (LAN) with a virtual MAC address. The Switches are the devices will understand the MAC address, because when a machine was manufactured with the unique address that will be different from other machine and it will understand the Layer-2 devices. If the primary router should fail, the router with the next-highest priority would take over the gateway IP address and answer ARP requests with the same MAC address, thus achieving transparent default gateway failover.

A. Organization of Paper

Chapter II Problem Statement: It describes the motivation and problems are described and need to be solved for motivated issues.
Chapter III Literature Survey: It illustrates the literature review of the existing system and it is a most important way of collecting the details of the opinions of the previous works.
Chapter IV Requirement Collection: Analysis of the overall system requirements.
ChapterV Methodology: It explains the methodologies that we are handling to solve the problems.
Chapter VI Implementation: It will cover all step by step methods of the system.
Chapter VII Result Discussion: It includes the clear discussion of the implemented process output screenshot
Chapter VIII Conclusion and Future Work: It illustrates the conclusion and future enhancement that can be carried over in future.

2. PROBLEM STATEMENT

In this project, we are checking the authorization of the user and give access to the web services. The data transfer request from the client to the server through the router has to be safe from the attacker or intruder. So that router will check the authentication by using the NDN data security packet. In that packet includes the permission rights to access the file that is there on the organization website. The remote servers are there to reduce the admin work to check each and every login activities. The key is generated to every user to avoid the blocking of the accounts. If the attacker when they try to access the information by login to the website for more than limited access time then admin will block that particular IP address to avoid further traffic creation in the network and also avoid the web application server buffering. So for that we are making the router as a firewall device to avoid the attackers. If that router became a firewall device then it will not make the server to send the data security packet for the security purpose.

Figure 1: Organization Network

3. LITERATURE SURVEY

To achieve the thin waist of the Internet architecture, the Internet protocol stack in NDN is changed to focus on the exchange of named data[1]. And in NDN environment, a crucial aspect is that names are hierarchical, thus allowing name resolution and routing in formation to be aggregated across similar names. This aspect is crucial for the scalability of the architecture. This paper [3] focuses on selecting the appropriate filtering location to minimize the amount of filtering routers in the trace back-based packet filtering for defending against the large-scale Bandwidth denial-of-service (BDoS) attacks. The CPSec [2] DLP is implemented in Kernel-level, we developed the system driver as middleware which encrypted the data when the data is written or saved and decrypts the cipher data to plain. All operations deal with the whole I/O request packet (IRP) in kernel-level, and the system works in a mandatory mode thus user or third part process cannot prevent the software to stop or disturb the encryption or decryption operations, the parameters of the CPSec DLP is described in the architecture of CPSec DLP middleware driver implementation is described. In early times, various content-based and opportunistic models were used as overlay solutions to full content-centric requirements. However, these solutions were based on conventional TCP/IP architecture. Nowadays, NDN gets more attention in the wireless area, and to its simple robust communication mechanism.

4. METHODOLOGY

The NDN depends on the information itself, was achieved to manage the remote host get to makes a huge traffic as a result of adjacent hubs may have the record that a client needs to get to, the client can't straightforwardly check the document itself. NDN also provides strong built-in functionalities, like multi-path routing, security primitives, flow balance activities. This network will give the better network architecture rather than the SDN for security problems. Figure 2 illustrates the NDN Communication. Client requests the data by sending the PDU to the router then it will check the details od the user in the OSPF routing table it the user is authorized then it will response back. Then it will find the route from the ACL. Then at the end client will get the response back. The PDU data that is transmitted as a solitary unit among peer substances of a PC arrange. A PDU may contain client information or control data and system tending to.

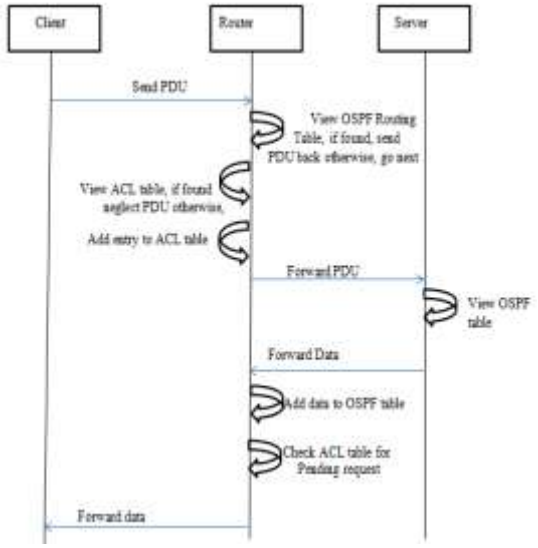

Figure 2: NDN data Transmission

This is the proposed security packet system in which having the combination of six parameters and individual performs their own role in this methodology. These data security packets are defined in the earlier proposed system without using IP address they used only the ND. To get more secure data transfer in the NDN so we add the IP Address and Right List. Each of the parameters is described below as shown in Figure 3.

a. Username: This is the parameter is to identify the authorized user when he/ she have a login to the web services or any other information request to the organization.
b. Password: This parameter will be the unique alpha-numeric characters or system generated password. This should be confidential because to avoid the attackers as suggested in the section 4.1 Network security measures.
c. Date: This is also an important parameter for the security providers view point because to update or checking the route table easily when a user logged into the network service to reduce admin work.
d. Data-Id: This parameter is to specify the use of identification number for the user to access the particular file.
e. IP Address: It is a logical address that understands by the routers, so for this purpose, we added this as a security parameter.
f. Right List: This Parameter is to specify the permissions are granted by the FTP server to the particular file access. To avoid the damage or loss of the information.

Figure 3: Data Security Packet

These permissions can only be given by the admin of the organizer to the authorized users only. To avoid the attackers to delete the data or knowing the important data of the organization so, this is one of the methods we incorporated in this project by using the File Transport Protocol (FTP) server. This includes Write, Read, Delete, Rename and List the username, Password and Subnet Mask of the particular IP address. Figure 4.

The secure shell and AAA authentication method will help to block the particular IP address to avoid the loss of data from the data. After a certain limited time of access by the non-registered user that particular IP will be blocked.
As per the project requirement, we are done only the proof of concept so that not having the more chances of doing in a larger area because the cisco packet tracer is cisco proprietary only the limited usage of protocols and algorithm shows in Figure 5.

5. IMPLEMENTATION

The NDN is established on received hosts, i.e., authenticated users. When a user wants to request the desired file, they will send a PDU to nearby nodes which have a file until reaching the data source node.User1 which received the PDU first and checks whether it has the desired file. If that user1has the file, it will respond the data and corresponding file as a data secure packet to the user.

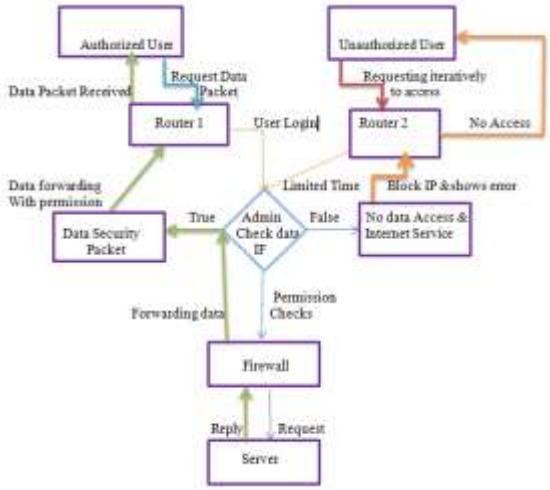

Figure 4: FTP Server permission

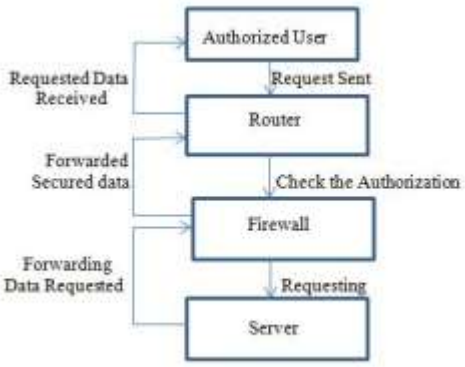

Figure 5: User gets the data from the Secure Shell (SSH)

The legal NDN nodes is used, because the network there may add a number of mobile or static nodes (devices) that are logged in to the network from different location so the this for the security purpose, the file can be encrypted using the RSA algorithm to generate a key to user for the file downloading from the NDN system. This is represented in Figure 6.

In that, each device are configured dynamically by using ARP protocol. In this, there can see how the information of the requested data will transfer from the one user to another user. For a simulation, they only the data packet success but inside the PDU how it takes automatically in the Cisco packet tracer is shown in Figure 7

It is compared and represented in the TCP/IP and OSI reference models. This is the shortest way to trace the data information in the network. It gives complete transmission data in the OSI layers. Figure 6.4 will also show the implementation of PDU in the network.

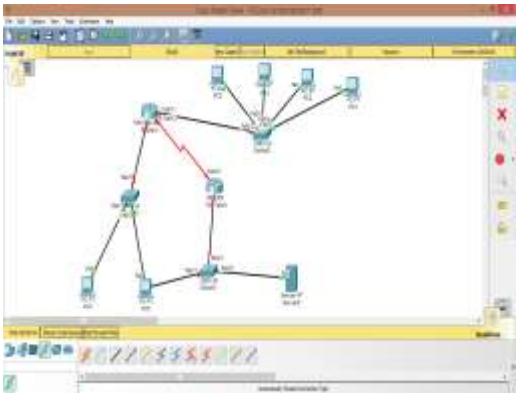

Figure 6: NDN Architecture

As it mentioned in the methodology FTP server configuration is one the main method for the security services providing to the organization. FTP server will give the permission and password to the authorized user to access the file on the organization website.

Table 1 gives some permission for few users are listed there with all the four write, read, delete, rename and list and some user has only read and read, rename, list permission respectively and those are represented in the following Table, it gives the details of the user Amruta have the password and the specific permission only they can do read the file and list the files that are present in the database server.

Table 1: FTP Configuration

Username	Password	Permissions
Cisco	Cisco	WRL
Amruta	123789	R
Kamala	123456	RNL

In this module, it is used to secure the password from the attacker and to encrypt the communication by using IP domain name and it will generate the secure keys and also verify SSH Implementation. The configuration of the SSH method will be represented in Table 2.

Table 2: SSH Configuration

Device	Interface	IP Address	Subnet Mask
Router 1	VLAN1	192.168.13.11	255.255.255.0
PC0	NIC	192.168.13.1	255.255.255.0

Ping the IP address from one user to another user in the command prompt to get the communication establishment. Telnet can also use but it will not much secure method to the user for authentication of username and password, so SSH will reduce the admin work and it will be used as a remote server controller.

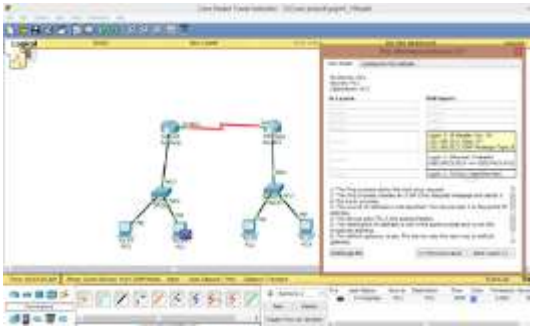

Figure 7: PDU Generation

After the entire authentication, authorization the authenticated user can be easily access without any intervention of the unauthorized party and it successful packet transmission is achieved as shown in the Figure 8.

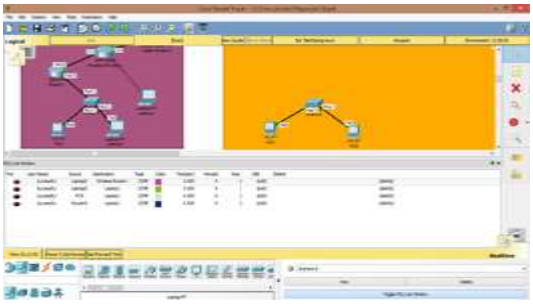

Figure 8: Overall diagram of the successful data secured packet exchanged

6. RESULT DISCUSSION

All the Implemented work is represented in this section by the simulation. OSPF Routing table simulated result is discussed in the Figure 9. In that it simulated the user's database and authentication details for the admin and also for the authorization purpose. That will transfer the data secure packet to the intended user request because of the FTP permissions

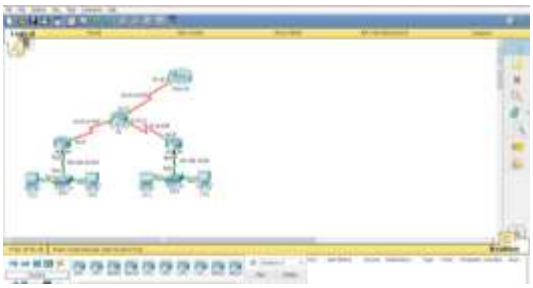

Figure 9: OSPF Routing Table

After the FTP permission, the admin can also restrict the WIFI and Internet access to user so they cannot transfer the files data to the other users without the permission of the admin of the organization. That is shown in the Figure 10. So the admin can block the IP address immediately.

Figure 10: Block the particular IP address

After the limited time of unauthorized user is try to access the file from the website of the Organization that IP will also be blocked or he cannot again try to access after the specified time that is represented in the Figure 11.

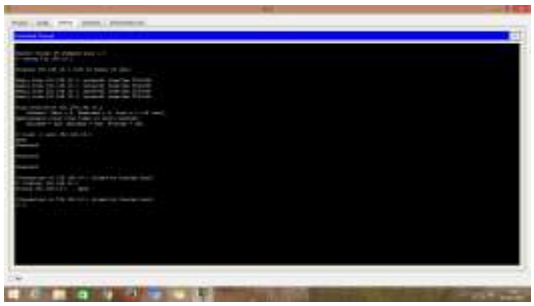

Figure 11: Access time out of the non-user IP

7. CONCLUSION

In this paper after the usage of NDN architecture, the FTP server permission and dynamic routing protocols for securing the user detail and the password. Proposing the Data secure packet to check the authentication of the user is resolved for the problem statement. So by this we can conclude that the unauthorized user is not easier to access the organization service. The authorized user also cannot be easily modifying the data in the organization. Here we can say that from both outside and inside the organization the security is provided by using the devices as a firewall to the server.

8. REFERENCES

[1] FTP-NDN: File Transfer Protocol Based-on Re-Encryption for Named Data Network supporting Non-designated Receivers. IEEE SYSTEMS JOURNALS., Vol 12, 1 March 2018.
[2] CPSec DLP: Kernel-Level content Protection Security System of Data Leakage Prevention. Chinese Journal of Electronics Vol., 26, No.4 July 2017.
[3] Filtering Location Optimization for Defending Against Large-Scale BDoS Attacks
[4] OEFS: On-Demand Energy-Based Forwarding Strategy for Named Data Wireless Ad Hoc Networks. May 17, 2017.

