Journal of Computer, Internet and Network Security
Volume 10, Issue 2, May-August, 2025
ISSN: 2457-0176 (Online)

Safety Summons: Network Security Services

D. Prasad
Assistant Professor
Department of CSE
St. Martin's Engineering College, Hyderabad
Email Id: *prasad.d525@gmail.com*

Abstract

Network security and cryptography is a subject too wide ranging to coverage about how to protect information in digital form and to provide security services. However, a general overview of network security and cryptography is provided. Network security is a complicated subject, historically only tackled by well-trained and experienced experts. When many systems are connected in a network it is very important to safe guard the data in each system. However, as more and more people become "wired", an increasing number of people need to understand the basics of security in a networked world. Our paper covers different kinds of threats & firewalls in the network by implementation of different security services using various security mechanisms. Generally, the logical conclusion is to use both kind of algorithms and their combinations to achieve optimal speed and security levels. It is hoped that the reader will have a wider perspective on security in general, and better understand how to reduce and manage risk personally.

Keywords: *Security Functions, SDN, Firewall, DDoS Attack.*

INTRODUCTION

A basic understanding of computer networks is requisite in order to understand the principles of network security. In this section, we'll cover some of the foundations of computer networking, and then move onto an overview of some popular networks. The impressive development of computer networks has reached the point, where security becomes essential. Users want to exchange data in a secure way. The problem of network security is a complex issue. Network security means a protection of the network assets.

Interface to Network Security Functions (I2NSF) defined a framework and interfaces for interacting with Network Security Functions (NSFs). The I2NSF framework allows heterogeneous NSFs developed by

Different security solution vendors to be used in the NFV environment by utilizing the capabilities of such products and the virtualization of security functions in the NFV platform. In the I2NSF framework, each NSF initially registers the profile of its own capabilities into the system in order for themselves to be available in the system. In addition, the Security Controller registers itself to the I2NSF user so that the user can request security services to the Security Controller.

Software-Defined Networking (SDN): A set of techniques that enables to directly program, orchestrate, control, and manage network resources, which facilitates the design, delivery an operation of network services in a dynamic and scalable manner.

Firewall: A service functions at the junction of two network segments that inspects every packet that attempts to cross the boundary. It also rejects any packet that does not satisfy certain criteria for, for example, disallowed port numbers or IP addresses.

Centralized Firewall System: A centralized firewall that can establish and distribute policy rules into network resources for efficient firewall management. These rules can be managed dynamically by a centralized server for firewall. SDN can work as a network-based firewall system through a standard interface between an SDN switch and a firewall functions as a vitual network function (VNF).

Centralized VoIP Security System: A centralized security system that handles the security functions required for VoIP and VoLTE services. SDN can work as a network-based security system through a standard interface between an SDN switch and a VoIP/VoLTE security function as a VNF.

Centralized DDoS-attack Mitigation System: A centralized mitigates that can establish and distribute access control policy rules into network resources for efficient DDoS-attack mitigation. These rules can be managed dynamically by a centralized server for DDoS-attack

mitigation. The SDN controller and switches can cooperatively work as a network-based firewall system through a standard interface between an SDN switch and a firewall function as a VNF running in the SDN controller.

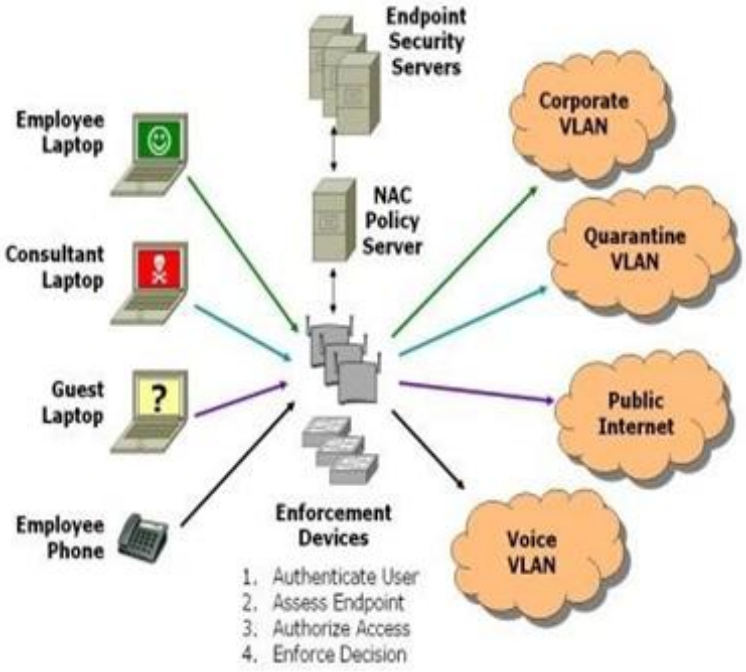

Figure no.1: Overview of Network Security

RELATED WORK

A centralized VoIP/VoLTE security system can monitor each VoIP/VoLTE flow and manage VoIP/VoLTE security rules controlled by a centralized server for VoIP/VoLTE security service called VoIP Intrusion Prevention System (IPS). The VoIP/VoLTE security system controls each switch for the VoIP/VoLTE call flow management by manipulating the rules that can be added, deleted or modified dynamically.

A centralized VoIP/VoLTE security system can cooperate with a network firewall to realize VoIP/VoLTE security service. Specifically, a network firewall performs basic security checks of an unknown flow's packet observed by a switch. If the network firewall detects that the packet is an unknown VoIP call flow's packet that exhibits some suspicious patterns, then it triggers the VoIP/VoLTE security system for more specialized security analysis of the suspicious VoIP call packet.

The procedure of VoIP/VoLTE security operations in this system is as follows

- A switch forwards an unknown flow's packet to the Switch Controller, and the Switch Controller further forwards the unknown flow's packet to the Firewall for basic security inspection.

- The Firewall analyzes the header fields of the packet, and figures out that this is an unknown VoIP call flow's signal packet (e.g.,SIP packet) of a suspicious pattern.

- The Firewall triggers an appropriate security service function, such as VoIP IPS, for detailed security analysis of the suspicious signal packet. The VoIP IPS analyzes the headers and contents of the signal packet, such as calling number and session description headers [RFC4566].

- If, for example, the VoIP IPS regards the packet as a spoofed packet by hackers or a scanning packet searching for VoIP/VoLTE devices, it drops the packet. In addition, the VoIP IPS requests the Switch Controller to block that packet and the subsequent packets that have the same call-id.

- The Switch Controller installs new rules (e.g., drop packets) into under lying switches.

- The illegal packets are dropped by these switches.

Legacy hardware based VoIP IPS has some challenges, such as provisioning time, the granularity of security, expensive cost, and the establishment of policy. The I2NSF Framework can resolve the challenges through the above centralized VoIP/VoLTE security system based on SDN as follows:

- **Provisioning:** The provisioning time of setting up a legacy VoIP IPS to network is substantial because it takes from some hours to some days. By managing the network resources centrally, VoIP IPS can provide more agility in provisioning both virtual and physical network resources from a central location.

- **The granularity of security:** The security rules of a legacy VoIP IPS are compounded considering the granularity of security. The proposed framework can provide more granular security by centralizing security control into a switch controller. The VoIP IPS can effectively manage security rules throughout the network.

- **Cost:** The cost of adding VoIP IPS to network resources, such as routers, gateways, and switches is substantial due to the reason that we need to add VoIP IPS on each network resource. To solve this, each network resource can be managed centrally such that a single VoIP IPS is manipulated by a centralized server.

- **The establishment of policy:** Policy should be established for each network resource. However, it is difficult to describe what flows are permitted or denied for VoIP IPS within a specific organization network under management. Thus, a centralized view is helpful to determine security policies for such a network.

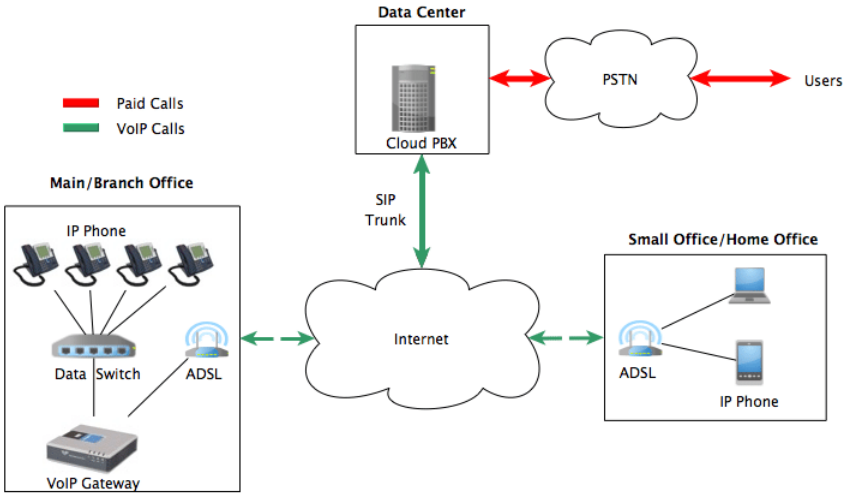

Figure no. 2: Typical VoIP Architecture

SUMMONS IN NETWORK SECURITY

A centralized network can manage each network resource and firewall rules can be managed flexibly by a centralized server for firewall (called Firewall). The centralized network firewall controls each switch for the network resource management and the firewall rules can be added or deleted dynamically.

The procedure of firewall operations in this system is as follows

- A switch forwards an unknown flow's packet to one of the Switch Controllers.
- The Switch Controller forwards the unknown flow's packet to an appropriate security service application, such as the Firewall.
- The Firewall analyzes, typically, the headers and contents of the packet. If the Firewall regards the packet as a malicious one with a suspicious pattern, it reports the malicious packet to the Switch Controller.

The Switch Controller installs new rules (e.g., drop packets with the suspicious pattern) into underlying switches. The suspected packets are dropped by these switches.

Legacy firewalls have some challenges such as the expensive cost, performance, management of access control, establishment of policy, and packet-based access mechanism. The proposed framework can resolve the challenges through the above centralized firewall system based on SDN as follows

- **Cost:** The cost of adding firewalls to network resources such as routers, gateways, and switches is substantial due to the reason that we need to add firewall on each network resource. To solve this, each network resource can be managed centrally such that a single firewall is manipulated by a centralized server.

- **Performance:** The performance of firewalls is often slower than the link speed of network interfaces. Every network resource for firewall needs to check firewall rules according to network conditions. Firewalls can be adaptively deployed among network switches, depending on network conditions in the framework.

- **The management of access control:** Since there may be hundreds of network resources in a network, the dynamic management of access control for security services like firewall is a challenge. In the framework, firewall rules can be dynamically added for new malware.

- **The establishment of policy:** Policy should be established for each network resource. However, it is difficult to describe what flows are permitted or denied for firewall within a specific organization network under management. Thus, a centralized view is helpful to determine security policies for such a network.

- **Packet-based access mechanism:** Packet- based access mechanism is not enough for firewall in practice since the basic unit of access control is usually users or applications. Therefore, application level rules can be defined and added to the firewall system through the centralized server.

Figure no. 3: Network Security Guidelines

CONCULSION

Network Security efficiency of business and communications. At the same time, breakthroughs in technology will provide even greater network security, therefore, greater piece of mind to operate in cutting edge business environments. Provided that enterprises stay on top of this emerging technology, as well as the latest security threats and dangers, the benefits of networks will most certainly outweigh the risks.

REFERENCES

1. Translated by Cheng Peiqing, et al. Computer network security. Publishing House of Electronics Industry, 1994.9
2. Li Wenlong. Face to face with a hacker. internet world.1999(2):2~8

3. Xiao Ze. Research on computer network security analysis model [J]. Journal on Communications, 2012(3):269.
4. Zhang Cheng. Research on computer network security analysis model [J]. Practical Electronics, 20l3(v)=148-149.
5. Hong Yaling. Research on computer network security analysis model [J]. Computer CD Software and Applications, 2013(z):1-152.
6. Wang Yuan. Quantitative Evaluation Method of Network Security Situation [D]. Ph.D. Dissertation, university of science and technology, 2003.
7. Cui Jing, Liu Guangzhong, the basics of computer network [J]. Tsinghua University Press, 2010.07.01.