IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111230

Review Paper on Network Security

Pratiksha Rajurkar[1], Vijay M. Rakhade[2], Ashish B. Deharkar[3]

Final Year Student, Computer Science Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[1]

Professor, Computer Science Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[2]

Assistant Professor, Computer Science Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[3]

Abstract: Network security has become major crucial to personal computer users, bureaucratic, and the services. With the arrival of the internet, security became a crucial anxiety as well as the past of security approve a better understanding of the disclosure of security technology. The internet complex itself allows for many securities risks to happen. If the architecture of the internet is adapted, it can bring to the possible attacks that can be sent over the network. Aware the attack methods allow us to emerge with proper security.

Keywords: Firewall, Threats, Network Security, Network Security Architecture.

I. INTRODUCTION

The world is fetching more interconnected due to Internet and new networking technology. There is a big amount of personal, commercial, military, and government data on networking infrastructures worldwide. Network security is fetching of greatest importance because of intellectual property that can be easily developed through the internet. There can be breach in intellectual property. Network Security defends your network and data from breaches, intrusions and additional threats. This is a huge and overarching term that describes hardware and software solutions as well as procedures or rules and configurations relating to network use, accessibility, and overall threat protection.

II. NETWORK SECURITY

Network Security keeps your network and data since breaches, intrusions and other threats. This is a huge and overarching term that describes hardware and software solutions as well as procedures or rules and configurations relating to network use, accessibility, and overall threat protection.

Network Security contains access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption and more. System and network technology is a key technology for a extensive variety of applications. Networks and applications essential security. While, network security is a serious requirement, there is a significant lack of security systems that can be implemented easily.

III. NETWORK SECURITY ARCHITECTURE

Networks essential have security embedded into their very design. A network security architecture provides a basis for an organization's cyber defences and helps to protect all of the company's IT assets. Now, we debate the components of a network security architecture, how it benefits businesses, and dissimilar models for generating a secure network architecture.

Elements of a Network Security Architecture

A network security architecture contains both network and security elements, such as the subsequent:

- **Network Elements:** Network nodes (computers, routers, etc.), communications protocols (TCP/IP, HTTP, DNS, etc.), connection media (wired, wireless), and topologies (bus, star, mesh, etc.).
- **Security Elements:** Cybersecurity devices and software, secure communications protocols (e.g., IPsec VPN and TLS), and data privacy technologies (classification, encryption, key management, etc.).

The Purpose of a Network Security Architecture

A well-designed cybersecurity architecture allows businesses to keep resiliency in the face of a cyberattack or a disaster of one or additional components of their infrastructure. The architecture should be enhanced for daily use through normal

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111230

business operations and make the company to handle reasonable bursts, spikes, or surges in traffic and to properly manage potential cyber threats to the organization.

The labels a process for developing a network security architecture that contains four primary phases:

- Assess: This phase of the procedure is for business and architecture reviews. The key phases in this phase include data capture, business modelling, and risk assessments.
- Design: This phase is proposed to develop a response to the requirements and to build customized logical design blueprints and approvals.
- Implement: This phase is for professional services, partners, etc. to enhance low-level design specifics and deliver statement-of-works for real-world solutions.
- Manage: This phase is pitched towards continuous development and incremental improvements of the security posture.

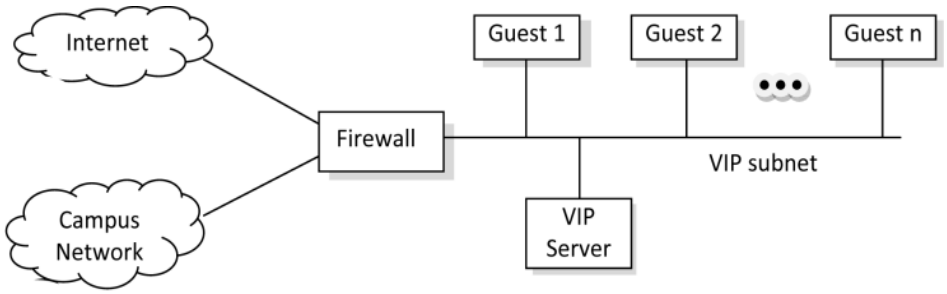

Fig.: Network Security Architecture

IV. FIREWALL

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic founded on an organization's previously recognised security policies. At its maximum basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's key purpose is to agree non-threatening traffic in and to possess dangerous traffic out.

The Different Types of Firewalls

There are numerous types of firewalls, and one of the major tasks that companies face when trying to protected their sensitive data is finding the right one. First off, a firewall – a network firewall – is a network appliance designed to express and enforce a perimeter. They can be organised at the connection between an organization's internal network and the public Internet or internally inside a network to perform network segmentation.

Hardware Firewalls: These firewalls are executed as a physical appliance deployed in an organization's server room or data centre. While these firewalls have the benefit of running as "bare metal" and on hardware designed specifically for them, they are also embarrassed by the limitations of their hardware (number of network interface cards (NICs), bandwidth limitations, etc.).

Software Firewalls: Software firewalls are executed as code on a computer. These firewalls contain both the firewalls built into common operating systems and virtual appliances that contain the full functionality of a hardware firewall but are implemented as a virtual machine.

Cloud Firewalls: Organizations are gradually moving serious data and resources to the cloud, and cloud-native firewalls are designed to follow suit. These virtual appliances are explicitly designed to be deployed in the cloud and may be accessible as either standalone virtual machines or as a Software as a Service (SaaS) offering.

Individually of these different firewall form factors has its advantages and disadvantages. While a hardware firewall has contact to optimized hardware, its abilities can also be constrained by the hardware it uses. A software firewall may have a little lower performance but can be easily updated or extended. A cloud firewall, but, takes advantage of all of the profits of the cloud and can be deployed near to an organization's cloud-based properties.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022
DOI: 10.17148/IJARCCE.2022.111230

V. THREATS

Information Security threats can be several like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

Threat can be whatever that can take benefit of a vulnerability to breach security and negatively alter, erase, harm objector objects of interest.

Software attacks resources attack by Viruses, Worms, Trojan Horses etc. Numerous users believe that malware, virus, wombats are all similar things. But they are not similar, only similarity is that they all are malicious software that acts differently.

Malware is a combination of 2 standings- Malicious and Software. So, Malware essentially means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system.

Types of security threats

The NIST definition above conditions that a threat can be an event or a condition. An incident, in this case, also contains natural disasters, fire, and power outage. It is a same general concept. In cybersecurity, it is extra common to talk round threats such as viruses, trojan horses, denial of service attacks.

Phishing emails is a social engineering threat that can reason, e.g., loss of passwords, credit card numbers and further sensitive data. Threats to information properties can cause loss of confidentiality, integrity or availability of data. This is likewise known as the CIA triad.

The CIA triad, together with three other well-known security concepts, is the origin for the STRIDE threat model. When listing possible threats, it is convenient to use an existing classification as a starting point. STRIDE is the most recognised classification, proposed by Microsoft in 1999. The name comes from the initial letters of the dissimilar categories, which also kinds it easier to recall them.

VI. CONCLUSION

Network security is a significant field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analysed to determine the necessary variations in security technology. The security technology is frequently software based, but many common hardware devices aroused. The current development in network security is not very remarkable.

REFERENCES

[1] Harris, S. *CISSP All-in-One Exam Guide, Fifth Edition* (McGraw-Hill Professional, 2010).
[2] McClure, S., Scambray, J., and Kurtz, G. *Hacking Exposed, Sixth Edition* (McGraw-Hill Professional, 2009).
[3] McClure, S., Scambray, J., and Kurtz, G. *Hacking Exposed, Seventh Edition* (McGraw-Hill Professional, 2012).
[4] NIST SP 800-27 Rev A, *Engineering Principles for Information Technology Security*.
[5] The New Lexicon Webster's Encyclopedic Dictionary of the English Language. New York: Lexicon.
[6] R.T. Morris, 1985. A Weakness in the %.2BSD Unix TCP/IP Software. Computing Science Technical Report No. 117, AT&T Bell Laboratories, Murray Hill, New Jersey.
[7] S.M. Bellovin. Security Problems in the TCP/IP Protocol Suite. Computer Communication Review, vol. 19, No. 2, pp. 32-48, April 1989.

