JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Study of Network Security Process

Shubham Sudhakar kshirsagar
Department of IT
GMVCS Tala
University of Mumbai

Tanuja Nitin Kasbale
Department of IT
GMVCS Tala
University of Mumbai

Ketaki Genaji Nadkar
Department of IT
GMVCS Tala
University of Mumbai

Madiha Murad Maner
Department of IT
GMVCS Tala
University of Mumbai

Prof.Raghvendra Singh
Assistant professor GMVCS & GMVIT
University of Mumbai

Abstract **:**Network Security deals with all aspects related to the protection of the sensitive information assets existing on the network. It covers various mechanisms developed to provide fundamental security services for data communication.Network Security protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solution.. Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an "intranet" to remain connected to the internet but secured from possible threats. The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed.

Keywords :- : Enemies, Effect of enemies, Security.

I. INTRODUCTION

Security is a broad topic and covers a multitude of sins. In its simplest form, it is concerned with making sure that nosy people cannot read, or worse yet, secretly modify messages intended for other recipients. It is concerned with people trying to access remote services that they are not authorized to use. Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone. Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures.

1.1What is network security

A network has been defined as any set of interlinking lines resemblung a network of road as interconnected systeThis defination suits our purpose well, a computer network is simplcy a system of interconnected computers.network security is any activity desiged to protect the usability and integrity of your network and data.

- It includes both hardware and software technology
- .It targets a variety of threats
- It stop them from entering or spreding on your network .
- Effective network security manages accessto the network.

1.2Network security defined

At a foundational level, network security is the operation of protecting data, applications, devices, and systems that are connected to the network.Though network security and cybersecurity overlap in many ways, network security is most often defined as a subset of cybersecurity. Using a traditional "castle-and-moat analogy," or a perimeter-based security approach – in which your organization is your castle, and the data stored within the castle is your crown jewels – network security is most concerned with the security within the castle walls.In this perimeter-based scenario, the area within the castle walls can represent the IT infrastructure of an enterprise, including its networking components, hardware, operating systems, software, and data storage. Network security protects these systems from malware distributed denial-of-service (DDoS) attacks, network intrusions, and more, creating a secure platform for users, computers, and programs to perform their functions within the IT environment.As organizations move to hybrid and multicloud environments, their data, applications, and devices are being dispersed across locations and geographies. Users want access to enterprise systems and data from anywhere and from any device. Therefore, the traditional perimeter-based approach to network security is phasing out. A to security, wherein an organization never trusts and always verifies access, is fast becoming the new method for strengthening an organization's security posture.

1.3 Types of Network Security

Firewall protection

A firewall is either a software program or a hardware device that prevents unauthorized users from accessing your network, stopping suspicious traffic from entering while allowing legitimate traffic to flow through. There are several types of firewalls with different levels of security, ranging from simple packet-filtering firewalls to proxy servers to complex, next-generation firewalls that use AI and machine learning to compare and analyze information as it tries to come through.

Network access control (NAC)

Standing at the frontline of defense, network access control does just that: it controls access to your network. Most often used for "endpoint health checks," NAC can screen an endpoint device, like a laptop or smart phone, to ensure it has adequate anti-virus protection, an appropriate system-update level, and the correct configuration before it can enter. NAC can also be programmed for "role-based access," in which the user's access is restricted based on their profile so that, once inside the network, they can only access approved files or data.

Email security

Email gateways are the number one threate vector for a security breach .attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipientes and send them to sites serving up malware.An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

Cloud security

Cloud security protects online resources – such as sensitive data, applications, virtualized IPs, and services – from leakage, loss, or theft. Keeping cloud-based systems secure requires sound security policies as well as the layering of such security methods as firewall architecture, access controls, Virtual Private Networks (VPNs), data encryption or masking, threat-intelligence software, and disaster recovery programs.

Virtual Private Networks (VPNs)

Avirtual private network encrypts the connection from the endpoint to a network, often over the internet.a remote the vpn uses communication between device and network.A virtual private network (VPN) is software that protects a user's identity by encrypting their data and masking their IP address and location. When someone

is using a VPN, they are no longer connecting directly to the internet but to a secure server which then connects to the internet on their behalf. VPNs are routinely used in businesses and are increasingly necessary for individuals, especially those who use public wifi in coffeeshops or airports. VPNs can protect users from hackers, who could steal anything from emails and photos to credit card numbers to a user's identity.

Data loss prevention (DLP)

Data loss prevention (sometimes called "data leak prevention") is a set of strategies and tools implemented to ensure that endpoint users don't accidentally or maliciously share sensitive information outside of a corporate network. Often put in place to comply with government regulations around critical data (such as credit card, financial or health information), DLP policies and software monitor and control endpoint activities on corporate networks and in the cloud, using alerts, encryption, and other actions to protect data in motion, in use, and at rest.

Mobile device security

Cybercriminals are increasingly targeting mobile device and apps. Within the next 3 years,90 percent of IT organizations may support corporate applications on personal mobile device of course, you need to control which device can access your network. You will also needs to configure their connections to keep network traffic private.

Wireless security

Wireless network are nt as secure as wired ones. Without stringent security measured installing a wireless LAN can be like putting Ethernet ports every where including the parking lot. To preventan exploit from taking hold you need products specifically desinged to protect a wireless network.

Endpoint protection

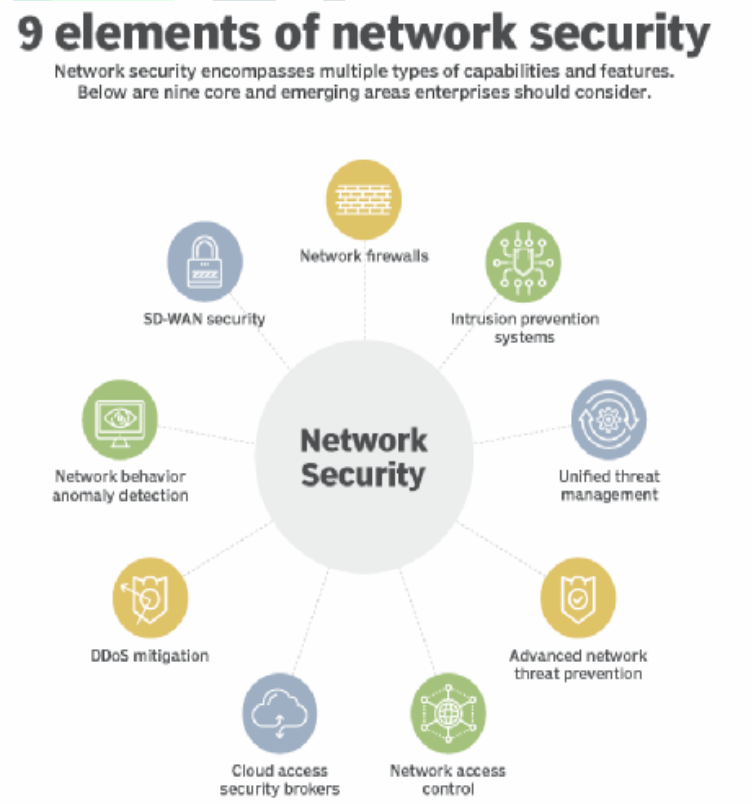
Often requiring a multi-layered approach, endpoint security involves protecting all of the endpoints – laptops, tablets, smartphones, wearables, and other mobile devices – that connect to your network. Although securing endpoints is a complex endeavor, a managed security service can help keep your devices, data, and network safe using antivirus software, data loss prevention, encryption, and other effective security measures.

Unified threat management (UTM)

With UTM appliances, organizations can reduce costs and improve the manageability of network protection and monitoring using multiple network-security tools such as firewalls, VPNs, IDS, web-content filtering, and anti-spam software.

Secure web gateway

This security technology prevents unauthorized network traffic from entering the internal network and protects users and employees that may access malicious websites that contain viruses or malware. Secure web gateways typically include web-filtering technology and security controls for web applications.



How does network security work

At its most fundamental level, secure networking centers on two basic tenets: authentication and authorization. In other words, first you need to make sure that every user in your network is an authentic user that is permitted to be there, and then you need to make sure that each user within your network is authorized to access the specific data that they are accessing.

Network security basics

Network security involves everything from setting and enforcing enterprise-wide policies and procedures, to installing software and hardware that can automatically detect and block network security threats, to hiring network security consultants and staff to assess the level of network protection you need and then implement the security solutions required.

II. PROCESS AND METHODOLOGY

Network Security Architecture

Elements of a Network Security Architecture

A network security architecture includes both network and security elements, such as the following:

- **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 enables businesses to maintain resiliency in the face of a cyberattack or a failure of one or more components of their infrastructure. The architecture should be optimized for daily use during normal business operations and prepare the company to handle reasonable bursts, spikes, or surges in traffic and to appropriately manage potential cyber threats to the organization.

How Does a Security Architect Create a Network Security Architecture?

A security architect is responsible for identifying and working to prevent potential cyber threats to an organization's network and systems. As part of their role, security architects should develop a network and security architecture that provides the visibility and control necessary to identify and respond to cyber threats to an organization's systems. This includes developing a plan for locating security controls to maximize their benefit to the company.

The Check Point Enterprise Security Framework (CESF) defines a process for developing a network security architecture that includes four primary phases:

- **Assess:** This phase of the process is for business and architecture reviews. The key steps in this phase include data capture, business modeling, and risk assessments.
- **Design:** This phase is intended to develop a response to the requirements and to build customized logical design blueprints and recommendations.
- **Implement:** This phase is for professional services, partners, etc. to add low-level design details and deliver statement-of-works for real-world solutions.
- **Manage:** This phase is geared towards continuous development and incremental improvements of the security posture.

Network Security Architecture Frameworks

Network security architectures can be designed based on a few different frameworks. Two of the most widely used models include zero trust and the Sherwood Applied Business Security Architecture (SABSA).

Zero Trust

The zero trust security model is designed to replace traditional, perimeter-based security models that place implicit trust in users, devices, and applications inside of the network. Zero trust eliminates the network perimeter by treating all devices as potential threats regardless of their location.

With a zero trust architecture, all requests for access to corporate resources are evaluated on a case-by-case basis. If the request is deemed legitimate based on role-based access controls (RBACs) and other contextual data, then access is granted only to the requested asset at the requested level for the duration of the current session.

A zero trust security architecture provides deep visibility and control over the actions performed within the corporate network. This is accomplished using a combination of strong authentication systems,

including multi-factor authentication (MFA), and granular access control implemented using micro-segmentation.

The Sherwood Applied Business Security Architecture (SABSA)

SABSA is a model for developing a security architecture based upon risk and business security needs. The model identifies business security requirements at the beginning of the process and works to trace them throughout the entire process of designing, implementing, and maintaining a security architecture.

SABSA includes a matrix for security infrastructure modeling. This includes multiple different layers (contextual, conceptual, logical, physical, component, and operational) and questions to be asked (what, why, how, who, where, and when). At each intersection, the model defines the component of the security architecture that should address that question at that layer.

Architecting Network Security with Check Point

For nearly thirty years, Check Point has set the standard for cybersecurity. Across the ever-evolving digital world, from enterprise networks through cloud transformations, from securing remote employees to defending critical infrastructures, we protect organizations from the most imminent cyber threats.

Check Point provides an integrated cybersecurity architecture designed to secure company networks, clouds and users against modern threats. It consolidates an organization's array of Check Point solutions, and can be managed centrally via a single dashboard. This consolidated security architecture expedites incident detection and response and allows all security solutions to leverage threat intelligence generated by Check Point ThreatCloud, the world's largest threat intelligence database.

Need help designing a secure network, Check Point Security Architects leverage its industry experience and employ independent frameworks, such as NIST CSF, SABSA, and Zero Trust Architecture, to provide advisory and assessment services to secure customer networks from threats. We invite you to sign up for a no-cost Security Risk Assessment today.

Types of network security software and tools

The choice of security policies and tools varies from network to network and changes over time. Strong security often involves using multiple approaches, known as *layered security* or *defense in depth* to give organizations as many security controls as possible. The following are some commonly used types of network security tools and software:

- **Access control.** This method limits access to network applications and systems to a specific group of users and devices. These systems deny access to users and devices not already sanctioned.
- **Antivirus and antimalware.** Antivirus and antimalware are software designed to detect, remove or prevent viruses and malware, such as Trojan horses, ransomware and spyware, from infecting a computer and, consequently, a network.
- **Application security.** It is crucial to monitor and protect applications that organizations use to run their businesses. This is true whether an organization creates that application or buys it, as modern malware threats often target open source code and containers that organizations use to build software and applications.
- **Behavioral analytics.** This method analyzes network behavior and automatically detects and alerts organizations to abnormal activities.
- **Cloud security.** Cloud providers often sell add-on cloud security tools that provide security capabilities in their cloud. The cloud provider manages the security of its overall infrastructure and offers tools for the user to protect their instances within the overall cloud infrastructure. For example, Amazon Web Services provides security groups that control the incoming and outgoing traffic associated with an application or resource.
- **Data loss prevention (DLP).** These tools monitor data in use, in motion and at rest to detect and prevent data breaches. DLP often classifies the most important and at-risk data and trains employees in best practices to protect that data. For instance, not sending important files as attachments in emails is one such best practice.

- **Email security.** Email is one of the most vulnerable points in a network. Employees become victims of phishing and malware attacks when they click on email links that secretly download malicious software. Email is also an insecure method of sending files and sensitive data that employees unwittingly engage in.
- **Firewall.** Software or firmware inspects incoming and outgoing traffic to prevent unauthorized network access. Firewalls are some of the most widely used security tools. They are positioned in multiple areas on the network. Next-generation firewalls offer increased protection against application-layer attacks and advanced malware defense with inline deep packet inspection.
- **Intrusion detection system (IDS).** An IDS detects unauthorized access attempts and flags them as potentially dangerous but does not remove them. An IDS and an intrusion prevention system (IPS) are often used in combination with a firewall.
- **Intrusion prevention system.** IPSes are designed to prevent intrusions by detecting and blocking unauthorized attempts to access a network.
- **Mobile device security.** Business applications for smartphones and other mobile devices have made these devices an important part of network security. Monitoring and controlling which mobile devices access a network and what they do once connected to a network is crucial for modern network security.
- **Multifactor authentication (MFA).** MFA is an easy-to-employ and increasingly popular network security solution that requires two or more factors to verify a user's identity. An example of this is Google Authenticator, an app which generates unique security codes that a user enters alongside their password to verify their identity.
- **Network segmentation.** Organizations with large networks and network traffic often use network segmentation to break a network into smaller, easier-to-manage segments. This approach gives organizations more control of and increased visibility into traffic flow. Industrial network security is a subset of network segmentation, providing increased visibility into industrial control systems (ICSes). ICSes are more at risk to cyber threats because of increased integration with the cloud.
- **Sandboxing.** This approach lets organizations scan for malware by opening a file in an isolated environment before granting it access to the network. Once opened in a sandbox, an organization can observe whether the file acts in a malicious way or shows any indications of malware.
- **Security information and event management (SIEM).** This security management technique logs data from applications and network hardware and monitors for suspicious behavior. When an anomaly is detected, the SIEM system alerts the organization and takes other appropriate action.
- **Software-defined perimeter (SDP).** An SDP is a security method that sits on top of the network it protects, concealing it from attackers and unauthorized users. It uses identity criteria to limit access to resources and forms a virtual boundary around networked resources.
- **Virtual private network (VPN).** A VPN secures the connection from an endpoint to an organization's network. It uses tunneling protocols to encrypt information that is sent over a less secure network. Remote access VPNs let employees access their company network remotely.
- **Web security.** This practice controls employee web use on an organization's network and devices, including blocking certain threats and websites, while also protecting the integrity of an organization's websites themselves.
- **Wireless security.** Wireless networks are one of the riskiest parts of a network and require stringent protections and monitoring. It's important to follow wireless security best practices, such as segmenting Wi-Fi users by service set identifiers, or SSIDs, and using 802.1X authentication. Good monitoring and auditing tools are also needed to ensure wireless network security.
- **Workload security.** When organizations balance workloads among multiple devices across cloud and hybrid environments, they increase the potential attack surfaces. Workload security measures and secure load balancers are crucial to protecting the data contained in these workloads.

- **Zero-trust network access.** Similar to network access control, zero-trust network access only grants a user the access they must have do their job. It blocks all other permissions.

Benefits of network security

The following are the main benefits of network security:

- **Functionality.** Network security ensures the ongoing high performance of the networks that businesses and individual users rely on.
- **Privacy and security.** Many organizations handle user data and must ensure the confidentiality, integrity and availability of data on a network, known as the *CIA triad*. Network security prevents the security breaches that can expose PII and other sensitive information, damage a business's reputation and result in financial losses.
- **Intellectual property protection.** Intellectual property is key to many companies' ability to compete. Securing access to intellectual property related to products, services and business strategies helps organizations maintain their competitive edge.
- **Compliance.** Complying with data security and privacy regulations, such as HIPAA and GDPR, is legally required in many countries. Secure networks are a key part of adhering to these mandates.

Challenges of network security

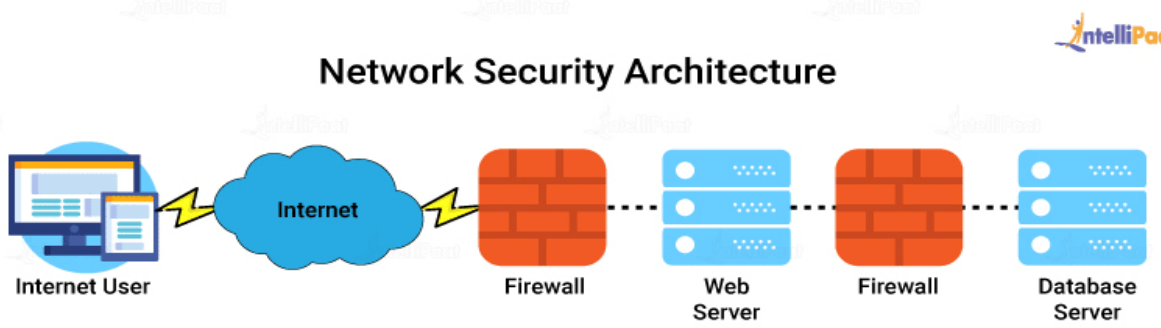
Network security involves a number of challenges, including the following:

- **Evolving network attack methods.** The biggest network security challenge is the rate at which cyber attacks evolve. Threat actors and their methods constantly change as technology changes. For example, new technology, such as blockchain, has led to new types of malware attacks, such as cryptojacking. As a result, network security defense strategies must adapt to these new threats.
- **User adherence.** As mentioned, security is every network user's responsibility. It can be difficult for organizations to ensure that everyone is adhering to network security best practices, while simultaneously evolving those strategies to address the newest threats.
- **Remote and mobile access.** More companies are adopting bring your own device policies, which means a more distributed and complex network of devices for organizations to protect. Remote work is also more prevalent. This makes wireless security more important, as users are more likely to be using a personal or public network when accessing company networks.
- **Third-party partners.** Cloud providers, managed security services and security product vendors often get access to an organization's network, opening new potential vulnerabilities.

Network Security Architecture

The architecture of network security models is the result of a well-thought systematic process. While building the architecture, professionals need to keep in mind the type of security the organization requires. Further, they must design several processes, systems, and tools that will help them prevent all sorts of network attacks. The architecture may comprise elements such as access control lists, firewalls, and other types of network security.

An example of a network security diagram is given below:



Now, you will come across some of the numerous job opportunities available for professionals who have the skills to secure a network.

III CONCLUSION

Hence we Had studies network security. Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used.

We Feel That A Methodology For Network Security Design Is Still Badly Needed. We Believe That Methodologies For Software Development Can Be Used As A Foundation And Have Demonstrated This Using The Demarco Method. Emerging Methodologies May Be Found To Be More Appropriate. Nevertheless, We Have Shown That The Idea Is Feasible. In The Process, We Have Exposed Some Issues That Must Be Addressed By Any Methodology For Network Security Design.

REFERENCES:-

[1]Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference on, pp.1469-1473, 19-23 May 2008.
[2]“Security Overview,” www.redhat.com/docs/manuals/enterprise/RHEL-4- Manual/security-guide/ch-sgs-ov.html.
[3] Molva, R., Institut Eurecom,“Internet Security Architecture,” in Computer Networks & ISDN Systems Journal, vol. 31, pp. 787-804, April 1999.