Webology (ISSN: 1735-188X)
Volume 15, Number 2, 2018

Analysis And Deployment Of Security Policies In Computer Networks At The Gateway Level

Anupoju Venkata Malleswara Rao[1], Shaheda Akthar[2]

[1]Research Scholar, Dept. of CSE, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India.

[2]Lecturer in Computer Science, Department of Computer Science, Govt. College for Women, Guntur, Andhra Pradesh, India.

Abstract:

Securing a network mainly involves applying policies and procedures to protect different network devices from unauthorized access. Network security is crucial for protecting business-critical infrastructure and assets, minimizing the attack surface, and preventing advanced attacks. Network security solutions use a layered approach to protect networks internally and externally. A network security policy delineates guidelines for computer network access, determines policy enforcement, and lays out the architecture of the organization's network securityenvironment and states how the security policies are implemented throughout the networkarchitecture. The network security policies are protecting users who are accessing the Internet against web-based threats. It does so by preventing malicious traffic that may result in malware infection or network intrusion. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented. This studywill analyze the aspects of policies and how to protect the network from cyberattack and improveoverall security posture, implementation of good practices, need of internet security and deployment of security policies at the Gateway Level.

Keyword Network; Internet; Security; Malware; Infrastructure; Vulnerabilities; Policies; Gateway; Cyber Attack.

Introduction:

The information is one of most valuable assets of the organization, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is not a core competency of most organizations, it has become a key business enabler, and not just an IT option. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Without adequately protected enterprise network and other security procedures and policies, the ability of the enterprise to carry out its business is not assured. Any vulnerability could cripple the enterprise preventing it from carrying out its normal business for days and weeks impacting its earnings and profitability. The security threats to business assets are becoming increasingly more sophisticated. Advanced attacks use multiple methods to determine/exploit/spread network vulnerabilities. It has become a business requirement that a rigorous information security management system be put in place.

Literature Survey:

This section presents different security mechanisms for network security activities. 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. Sankeerth Vangala has stated that the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development taking place in the same technologies being currently used. Although some security issues were observed, the security tools such as firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding intellectual property for the near future [1]. Purna Chandra Sethi and Prafulla Kumar Behera have stated that the Network security and QoS is an important field that is increasingly getting attention as the Internet expands. What is going to drive the Internet security most is the enormous and complex set of applications being executed over Internet. The issue of security is similar to an immune system. The immune system fights off attacks and builds itself to fight the security threats. Similarly, the network security will be able to function as an immune system. So, it has to be improved to such level such that information can't be leaked [2]. ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization [3]. Raghav Arora and his team have stated that the Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different defence and detection mechanisms were developed to deal with these attacks [4]. Australian Cyber Security Centre has advised and information about how to protect yourself and your business online. When there is a cyber security incident, also provide clear and timely advice to individuals, businesses and critical infrastructure operators [5]. Juniper Networks has guided to configure security zones, address books and address sets, security policy applications and application sets, and security policies [6]. Cato enables customers to gradually transform their networking and security infrastructure for the digital business [7]. Palo Alto Networks, the global cybersecurity leader, continually delivers innovation to enable secure digital transformation—even as the pace of change is accelerating and it has implemented various network security products [8].

Network:

A computer network is a group of computers that use a set of common communication protocols over digital interconnections for sharing resources located on or provided by the network nodes. A network may be small where it may include just one system or maybe as large as what one may need.

Types of Computer Networks: Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN).

Network Security:

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented [1]. Network security has become more important to personal computer users, organizations, and Govt. departments like military, defence, navy, etc. 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.

Network design is a well-developed process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development [1].

When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message [2].

When developing a secure network, the following need to be considered:

1. Access – Authorized users can communicate to and from a particular network
2. Confidentiality – Information in the network remains private
3. Authentication – Ensure the users of the network
4. Integrity – Ensure the message has not been modified in transit
5. Non-repudiation – Ensure the user does not refute that he used the network

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack.

The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavor [2].

To lessen the vulnerability of the computer to the network there are many products available. These tools are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. Businesses throughout the world are using a combination of some of these tools. "Intranets" are both connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in the network. Understanding the security issues of the internet greatly assists in developing new security technologies and approaches for networks with internet access and internet security itself [2].

Information security:

Information security is the safeguarding of information confidentiality, integrity, and availability. The goals of information security are to ensure business continuity, to maintain legal compliance, and to achieve competitive edge. For example, organizations with a committed client base and an established partner network need to demonstrate to their partners, shareholders, and clients that they have identified and measured their security risks and implemented a security policy and controls that will mitigate these risks [3].

Technology for Internet Security:

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different defense and detection mechanisms were developed to deal with these attacks [4].

1. Cryptographic Systems

Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

2. Firewall

A firewall is a typical border control mechanism or perimeter defence. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front line defence mechanism against intruders. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

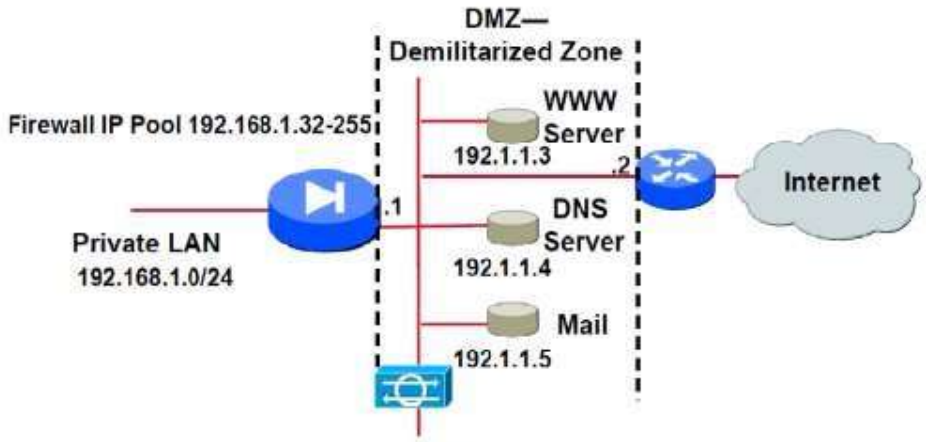

Fig. Firewall for the Internet Access

3. Intrusion Detection Systems

An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

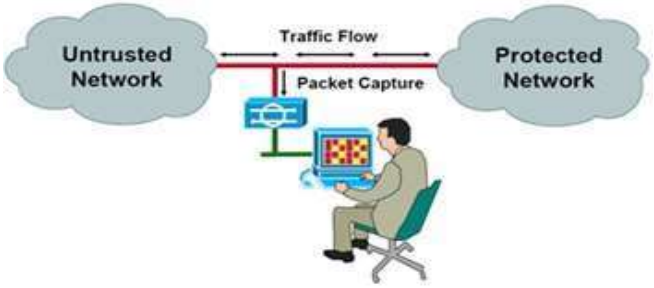

Fig. Intrusion Detection

4. Anti-Malware Software and scanners

Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so-called anti-Malware tools are used to detect them and cure an infected system.

5. Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to server by certificates. Clients present a certificate to the server to prove their identity.

Gateway Security:

A gateway is a boundary system that separates different security domains and acts as the first line of defence to provide security capabilities for an organisation and its systems. In doing so, a gateway provides policy enforcement mechanisms for data flows by only permitting data to flow between different security domains in accordance with an organisation's security policy. A common example of a gateway data flow is between an organisation's internal network and the internet [5].

A gateway is comprised of a collection of physical and logical components that enforce a security policy to manage access to, and transfer of, data from one security domain to another. In a cloud service provider model, or a managed service provider model, a gateway may be abstracted to a set of security services and capabilities that are exposed to consumers.

Factors that heavily influence an organization's gateway design include [5]:

- Business and operational requirements and strategies
- Technical capabilities
- Confidentiality, integrity, availability and privacy requirements
- Threat modelling, risk appetite and risk management strategies
- Integrations between self-hosted and cloud services
- Sourcing and service delivery models
- Location and number of data centres and office locations
- Availability of staff to design and sustain gateway capabilities

A gateway should be deployed as a combination of physical and logical components and capabilities that operate collectively as a single integrated solution. There are a number of architectural approaches to gateway design an organization can consider [5]:

- Monolithic - provides all gateway security functions through one centrally managed system (for example a Secure Internet Gateway).
- Disaggregated - provides service-specific gateway functions through discrete but interoperable systems, which do not share a common control plane.
- Hybrid gateways - provides all required gateway services through a mixture of central and disaggregated service offerings and control planes.

Regardless of the architectural model deployed, it is critical that gateway services and cyber security defence capabilities evolve to support an organization's changing business and risk management needs.

Security Policy:

A security policy, which can be configured from the user interface, controls the traffic flow from one zone to another zone by defining the kind(s) of traffic permitted from specified IP sources to specified IP destinations at scheduled times.

Policies allow you to deny, permit, reject, encrypt and decrypt, authenticate, prioritize, schedule, filter, and monitor the traffic attempting to cross from one security zone to another. You decide which users and what data can enter and exit, and when and where they can go.

A security policy allows you to safely enable applications, users, and content by classifying all traffic, across all ports, all the time. A number of frameworks exist to help organizations assess their security risks, implement appropriate security controls, policies and comply with governance requirements as well as privacy and information security regulations.

To secure their business, organizations must control access to their LAN and their resources. Security policies are commonly used for this purpose. Secure access is required both within the company across the LAN and in its interactions with external networks such as the Internet.

The security policies enforce rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall. From the perspective of security policies, the traffic enters one security zone and exits another security zone. This combination of a from-zone and to-zone is called a context. Each context contains an ordered list of policies. Each policy is processed in the order that it is defined within a context [6].

Network Security Policy:

A network security policy delineates guidelines for computer network access, determines policy enforcement, and lays out the architecture of the organization's network security environment and defines how the security policies are implemented throughout the network architecture.

Network security policies describes an organization's security controls. It aims to keep malicious users out while also mitigating risky users within your organization. The initial stage to generate a policy is to understand what information and services are available, and to whom, what the potential is for damage, and what protections are already in place.

The security policy should define the policies that will be enforced – this is done by dictating a hierarchy of access permissions – granting users access to only what they need to do their work.

These policies need to be implemented in the organization written security policies and also in IT infrastructure – firewall and network controls' security policies [7].

A cyber security policy is part of overall IT security. A cybersecurity policy defines acceptable cybersecurity procedures. Cybersecurity procedures explain the rules for how anyone with potential network access can access the corporate resources, whether they are in the physical offices, work remotely, or work in another company's offices (for example, customers and suppliers), send data over networks. They also determine how organizations manage security patches as part of their patch management policy [7].

A good cybersecurity policy includes the systems that the business is using to protect the critical information and are already in place, including firewalls. It should align with the network segmentation and micro-segmentation initiatives.

Network policy management tools and solutions are available. Organizations use them to automate tasks, improving accuracy and saving time. The Security Management Solution simplifies and automates network security policy management to make your enterprise more agile, more secure and more compliant – all the time.

It automatically builds a network map of the entire hybrid network and can map and intelligently understand the network security policy across the hybrid and multi-vendor network estate. It can auto-discover application connectivity requirements, proactively analyze risk, rapidly plan and execute network security changes and securely decommission firewall rules – all with zero-touch and seamlessly orchestrated across your heterogeneous public or private cloud, and on premise network environment [7].

Internet Gateway Security Policy:

Information and Cyber Security Policy deals with protecting its business assets against possible malicious actions targeted on its business assets to negatively impact the business, and to ensure business continuity.

Gateway Security is a network security paradigm that involves various solutions which filter unwanted traffic/malware at the point of entry in the network itself. Providing gateway security has long been a high priority for organizations since it enables them to protect the outbound transmission of confidential information, facilitate compliance, improve employee productivity and optimize the use of valuable IT resources—improving overall business continuity [8].

Generally, internet gateway security policy has two main security goals:

- **Reduce/control the chance of a successful intrusion**
  - Port-based security policies that either block everything in the interest of network security, or enable everything in the interest of the business, a security policy to ensure safe enable of applications across all ports, for all users, all the time, while simultaneously scanning all traffic for both known and unknown threats.
- **Detect the presence of an attacker**
  - A internet gateway security policy provides built-in mechanisms help to identify gaps in the rule base and detect alarming activity and potential threats in the network.

To achieve these goals, the internet gateway security policy uses application-based rules to allow access to specific applications by user, while scanning all traffic to detect and block all known threats, and send unknown files to identify new threats and generate signatures to block them.

The policy is based on the following methodologies. The policy can ensure detection and prevention at multiple stages of the attack life cycle [8].

Inspect All Traffic for Visibility: It cannot protect against threats if cannot see, you must make sure that full visibility into all traffic across all users and applications all the time. To accomplish this:

- Deploy Global Protect to extend the security platform to users and devices.
- Enable decryption so the firewall can inspect encrypted traffic.
- Enable User-ID to map application traffic and associated threats to users or devices.
- If company policy allows user's devices on the network, the unsanctioned device access control service enables users to access your cloud applications from personal devices, from any location, without inadvertently putting your data or organization at risk. The service redirects traffic through the firewall for policy enforcement and threat prevention.

The firewall can then inspect all traffic—inclusive of applications, threats, and content—and tie it to the user, regardless of location or device type, port, encryption, or evasive techniques employed using the native App-ID, Content-ID, and User-ID technologies.

Complete visibility into the applications, the content, and the users on the network is the first step toward informed policy control [8].

Reduce the Attack Surface: After context into the traffic on the network—applications, their associated content, and the users who are accessing them—create application-based Security policy rules to allow those applications that are critical to the business and additional rules to block all high-risk applications that have no legitimate use case.

To further reduce the attack surface, enable attach File Blocking and URL Filtering profiles to all rules that allow application traffic to prevent users from visiting threat-prone web sites and prevent them from uploading or downloading dangerous file types (either knowingly or unknowingly). To prevent attackers from executing successful phishing attacks, configure credential phishing prevention [8].

Prevent Known Threats: Enable the firewall to scan all allowed traffic for known threats by attaching security profiles to all allow rules to detect and block network and application layer vulnerability exploits, buffer overflows, DoS attacks, and port scans, known malware variants, (including those hidden within compressed files or compressed HTTP/HTTPS traffic). To enable inspection of encrypted traffic, enable decryption.

In addition to application-based Security policy rules, create rules for blocking known malicious IP addresses based on threat intelligence from reputable third-party feeds [8].

Detect Unknown Threats: Forward all unknown files for analysis to identifies unknown or targeted malware (also called Advanced Persistent Threats or APTs) hidden within files by directly observing and executing unknown files in a virtualized sandbox environment in the cloud[8].

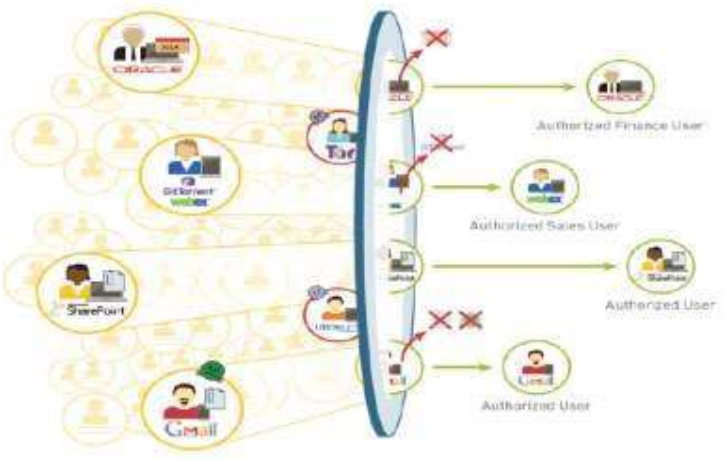

Fig. Traffic to detect and block all known threats

Need of Internet Gateway Security Policy:

To protect the network from cyber-attack and improve overall security posture, implement an internet gateway security policy. A policy allows to safely enable applications, users, and content by classifying all traffic, across all ports, all the time.

In most of cases, the Internet Service Providers (ISPs) are receiving blocking instructions to block specific content in a particular domain. By blocking through the IP address is not an effective solution to block the URL's as it would block access to the entire domain instead of blocking required content in the domain. In such a case, ISPs are not complying with the DoT mandate. At present, most of the ISPs are blocking the URL's with IP address at router level. IP based filtering includes incurring additional load and processing overhead on existing routers.

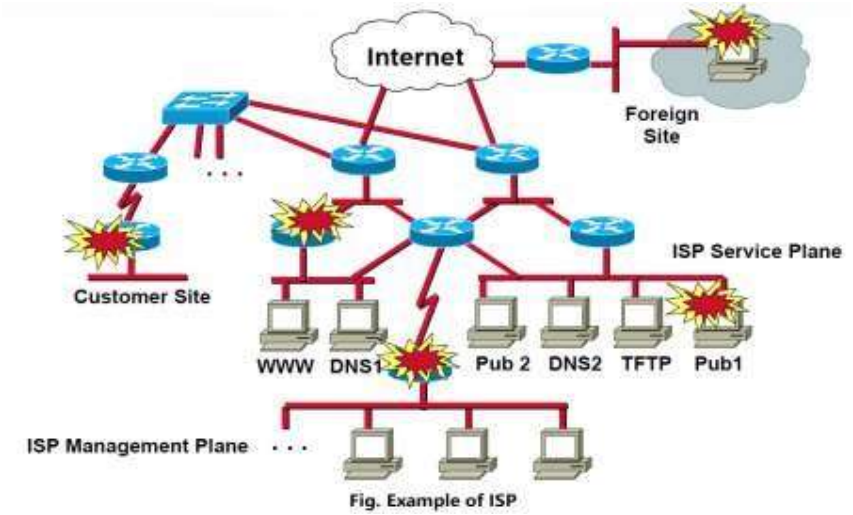

Fig. Example of ISP

The URL based or port-based security policies that either block everything in the interest of network security, or enable everything in the interest of your business, the security policy allows you to safely enable applications by classifying all traffic, across all ports, all the time, including

encrypted traffic. By determining the business use case for each application, you can create security policy rules to allow and protect access to relevant applications.

Hence, ISPs are proposing solution to meet the DoT mandatory requirement.

- Identify applications irrespective of port, protocol, evasive tactic or encryption
- Identify and control users irrespective of IP address, location, or device
- Protect against known and unknown application-borne threats
- Provide fine-grained visibility and policy control over application access and functionality

To mitigate the risk of breaking applications when moving from a port-based enforcement to an application-based enforcement. Find that some of the applications that were being allowed through existing port-based policy rules are not necessarily applications that you want to continue to allow or that you want to limit to a more granular set of users.

Unlike a port-based policy, a security policy is easy to administer and maintain because each rule meets a specific goal of allowing an application or group of applications to a specific user group based on your business needs. Therefore, you can easily understand what traffic the rule enforces by looking at the match criteria [8].

Deployment of Internet Gateway Security Policy:

Moving from a port-based security policy to an application-based security policy may seem like a daunting task. However, the security risks of sticking with a port-based policy far outweigh the effort required to implement an application-based policy. And, while legacy port-based security policies may have hundreds, if not thousands of rules. It may be streamlined set of rules that align with the goals, simplifying administration and reducing the chance of error. Because the rules in an application-based policy align with the requirement and acceptable use policies, you can quickly scan the policy to understand the reason for each and every rule.

As with any technology, there is usually a gradual approach to a complete implementation, consisting of carefully planned deployment phases to make the transition as smooth as possible, with minimal impact to end users. Generally, the workflow for implementing gateway level security policy is [8]:

- **Need to protect - Assess and identify -** The first step in deploying a security architecture is to assess the requirement and identify the valuable assets and biggest threats to those assets are. For example, if it is a technology company, then the intellectual property is most valuable asset of the company. In this case, one of the biggest threats would be source code theft.
- **Network using segments and zones** - Traffic cannot flow between zones unless there is a security policy rule to allow it. One of the easiest defenses against lateral movement of an attacker that has made its way into your network is to define granular zones and only allow access to the specific user groups who need to access an application or

resource in each zone. By segmenting network into granular zones, it can prevent an attacker from establishing a communication channel within the network (either via malware or by exploiting legitimate applications), thereby reducing the likelihood of a successful attack on the network.

- **Identification of application allow list** - Before creation of an internet gateway security policy, maintain the inventory of the applications want to allow on the network, and distinguish between those applications and officially sanction and simply want users to be able to use safely. After that identify the applications (including general types of applications) want to allow, map them with the specific rules.
- **Create User Groups for accessing the applications** - After you identify the applications plan to allow, it must identify the user groups that require access to each one. Because compromising an end user's system is one of the cheapest and easiest ways for an attacker to gain access to the network, it can greatly reduce the attack surface by only allowing access to applications to the user groups that have a legitimate business need.
- **Decryption of the Traffic for full Visibility and Threat Inspection** - The network can't protect against threats, can't see and inspect. Transport Layer Security (TLS) traffic accounts for more than half of the traffic on a typical network and is growing. This is why encrypted traffic is a common way for attackers to deliver threats. For example, an attacker may use a web application such as Gmail, which uses TLS encryption, to email an exploit or malware to employees accessing that application on the corporate network. Or, an attacker may compromise a web site that uses TLS encryption to silently download an exploit or malware to site visitors. If you do not decrypt traffic for visibility and threat inspection, you leave open a huge attack surface.
- **Create Security Profiles for the Internet Gateway** — Command and control traffic, CVEs, drive-by downloads of malicious content, phishing attacks, APTs are all delivered via legitimate applications. To protect against known and unknown threats, you must attach stringent security profiles to all Security policy allow rules.
- **Define the Initial Internet Gateway Security Policy -** Using the application and user group inventory conducted, can define an initial policy that allows access to all of the applications want to allow by user or user group. The initial policy to create must also include rules for blocking known malicious IP addresses, as well as temporary rules to prevent other applications you might not have known about from breaking and to identify policy gaps and security holes in your existing design.
- **Monitoring and Fine tuning the policy** - After the temporary rules are in place, it can begin monitoring traffic that matches to them so that can fine tune the policy. Because the temporary rules are designed to uncover unexpected traffic on the network, such as traffic running on non-default ports or traffic from unknown users, it must assess the traffic matching these rules and adjust the application allow rules accordingly.

- **Removal of the temporary rules** - After a monitoring period of several months, it should see less and less traffic hitting the temporary rules. When reach the point where traffic no longer hits the temporary rules, it can be removed.
- **Maintain the rule base** - Due to the dynamic nature of applications, it must continually monitor application allow list and adapt the rules to accommodate new applications that it can decide to sanction as well to determine how new or modified App-IDs impact the policy.

Conclusion and Future Work:

Organizational information security programs must be designed to assist organizations in identifying, adopting, and improving information security practice, in order to ensure that the organization can sustainably protect its business environment by creating a security culture based on the business rather than a traditional technologist centric environment. Effective information security programs highlight the development, communication, and publication of endorsed information security policies; and ensure a comprehensive understanding of the current-state security, while driving towards a realistic and business-based target-state.

People put more and more attention on the security of computer network using Artificial Intelligence and Machine Learning Models and Algorithms. Under the situation of the fast development of the network security industry and the acceleration of the information process, a variety of new technologies will continue to apply. Network security has immeasurable opportunities, which becomes a hot area for researchers to explore, its development is of great strategic significance, and the future network security technology will make more considerable progress. Researchers should completely realize the safety factors to establish reasonable objectives and relevant laws and regulations. As a future work, we are studying how to improve the network security using AI & ML algorithms, apply the security policies & profiles to strengthen the entire network.

References:

[1] Sankeerth Vangala, Network Security: History, Importance, and Future, Southern New Hampshire University.

[2] Purna Chandra Sethi and Prafulla Kumar Behera, “Methods of Network Security and Improving the Quality of Service – A Survey” in International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE).

[3] ISO/IEC 27002:2005(en) - Information technology - Security techniques - Code of practice for information security management.

[4] Raghav Arora, Rana Rahul Sathyaprakash, Saurabh Rauthan, Shrey Jakhetia, “Internet Security and Privacy” International Journal of Computer Science and Information TechnologyResearch ISSN 2348-120X (online) Vol. 2, Issue 3, pp: (467-475), Month: July - September 2014, www.researchpublish.com

[5] Australian Cyber Security Centre, “Gateway Security Guidance Package: Gateway Security Principles”.

[6] Juniper Networks, Engineering Simplicity, "Security Policies User Guide for Security".
[7] Cato Networks, "Network Security: Threats, Tools, and Best Practices".
[8] Palo Alto Networks, TECHDOCS, "Internet Gateway Best Practice Security Policy"
[9] Algosec, "Secure application connectivity any where"
[10] R. Bhuvana Indumathi & R. Bhuvaneswari, "Network Security", International Journal of Current Research and Modern Education, Special Issue, January, Page Number 50-52, 2017.
[11] McGrawHill Education, The Complete Reference™, Information Security, Second Edition: Mark Rhodes-Ousley, www.it-ebooks.info.
[12] Karen Scarfone, Paul Hoffman, "Guidelines on Firewalls and Firewall Policy", Recommendations of the National Institute of Standards and Technology, U.S. Dept. of Commerce, NIST Special Publication 800-41 Revision 1.
[13] January 2008, in book: Securing Information and Communications Systems: Principles, Technologies, and Applications (pp.139-170), Chapter: Chapter 8. Network Security, Publisher: Artech House, Natalia G. Miloslavskaya, National Research Nuclear University MEPhI, Sokratis K. Katsikas, Norwegian University of Science and Technology.
[14] R. Bhuvana Indumathi & R. Bhuvaneswari, "Network Security", International Journal of Current Research and Modern Education, Special Issue, January, Page Number 50-52, 2017.
[15] Brijesh Aggarwal, "Network Security", Dept. of Applied Science and Humanities, Dronacharya College of Engineering.
[16] Grigoris Antoniou, Matteo Baldoni, Piero A. Bonatti, Wolfgang Nejdl, Daniel Olmedilla – "Rule-Based Policy Specification".
[17] "Computer and Information Security Handbook" by John Vacca, The Morgan Kaufmann Series in Computer Security.
[18] G. Pavlov, J. Karakaneva, "Information Security Management System in organisation" Trakia Journal of Sciences, Vol. 9, No 4, pp 20-25, 2011.