Volume No:2, Issue No:5 (October-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Effective Network Security Policies at the Gateway Level in Computer Networks

Anupoju Venkata Malleswara Rao
Ph.D. Scholar,
Acharya Nagarjuna University,
Nagarjuna Nagar, Guntur,
Andhra Pradesh, India.

Dr.Shaheda Akthar
Lecturer in Computer Science,
Department of Computer Science,
Govt. College for Women,
Guntur, Andhra Pradesh, India.

Abstract:
As the internet grows and computer networks become larger and superior, network security has become one of the most significant factors to consider in any network. The Network security consists of the policies adopted to prevent the system and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security is essential for both public and private networks, which are used in day to day IT activities; conducting transactions that has to communicate among businesses, government agencies and individuals. Traditionally, Internet Service Providers (ISPs) used to block the Uniform Resource Locator's (URL) with IP address at router level with the evolution of different security threats such as malware, email, web and social network based attacks, it would be very difficult to protect the network with the traditional methods and requires latest technologies such as Content and URL based filtering methods to protect or safe guard that has to the network and continuously evolve with the latest trends to secure the network. There are wide range of technologies and methods to protect the network. This paper will examine the network security weakness w.r.t to the router and firewall network devices at ISP level and to overcome the limitations with latest trends in the technology, such as content and URL based filtering to get the greater control over the traffic that passes through the network.

Keywords:
Network Security, Routers, Firewalls and Network Management.

Introduction:
In today's era, almost every organization uses a computer and has a computer network to send, receive and store information. Whether it's sending emails through the network, storing documents, or serving information through a web server, it is very important to focus on the security, and especially when the network contains sensitive, confidential and personal information provided. The Network security affects that has too many organizations, whether they are large or small depend on system and government organizations. If the network security is breached and that an intruder can do all sorts of harm. That's why people need aware of that and to be educated about network security and that how to secure their computer and network process. Systems are required to be updated regularly as well as new security flaws are discovered. The system has without being up to date, it makes it easy for an access then hacker to gain unauthorized access to the system.The purpose of network security is essentially to prevent loss, through the system and misuse of data. There are a number of potential pitfalls in that may arise and set as well if network security is not implemented properly individual guidelines. Some of these are:

Breaches of confidentiality:
Each business will be identify with the need to keep certain moment for that critical information privately taken from competitor eyes.

Data destruction:
Data is most valuable commodity for an individual setup and enterprises alike. It is a testament to its importance with it when the proliferation of today available latest backup technology is considered.

Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Destruction of data can be severely cripple the victim concerned for communication.

Data manipulation:

A system break-in may be easily detectable, as some hackers can tend to leave the tokens of their accomplishment. However, data manipulation is a more sneaking threat than that. Data values can be changed in that, while that may not seem to be a serious concern, the significance becomes immediately apparent when financial information is question like that.

There are many more potential threats that can destroy a system.

Security Attacks:

Not only do you have to attention on security, also have to be aware of the types of security attacks that can happen only on your computer network. Before we go on to discuss about the types of security attacks, an attacker may aim to do that one of the following:

Interruption:

Interruption is an attack on availability of the service such as Deny of Service attack (or DOS). An interruption attacks aim to make the resources unavailable during anattack is called as DOS attack in which, the servers so the service was inaccessible to its users.

Interception:

Interception is an attack of gaining unauthorized access to a system. It can be simple eavesdropping such as packet sniffing or simply copying of information.

Modification:

Modification attacks and tampers with a resource. It aims to modify or change the information that is being communicated with two or more parties. One example of modification attack could be sending information to one party and instead redirecting the trafficto another.

Fabrication:

Fabrication attack is also known as copying and it by passes authenticity checks, and essentially mimicking or impersonating information. In this sort of attack usually inserts new information, or records extra information. It is mainly used to gain access to information or a service.

Keeping the above in mind, there are two types of attacks whose aim to compromise the security of a network – passive attack and an active attack.

Passive Attack:

A passive attack splits into two types. The first type of passive attack is to simply monitor the transmission between two parties and to capture the information from that is sent and received. The attacker does not intend to interrupt the service, but only see the information. The second type of attack is traffic analysis. If information is encrypted, and it will be very difficult to read the information being sent and received, but the attacker simply observers the information from, and tries to make sense out of it; or to simply determine the identity and location of the two parties i.e. sender and receiver.

A passive attacks are harder to detect as there is less impact to the information communicated.

Active attack:

On the other hand, an active attack aim to cause interruption, and it is usually set and easily recognized. An active attack will modify or change an information or interrupts the service. There are four types of an active attack:

Masquerade:

To disguise as someone to gain access to others system with their user account to gain more privileges. For example, a user of a system break-in the user name and password of System Administrators to be able to pretend that system they are them.

Reply:

To capture data or information to send it, or a copy it elsewhere.

Modification:

To alter or modify the information being sent or received.

Denial of service:

To cause an interruption to the network

Even though a passive attack doesn't have any harmful but it is just as corrupt as an activate attack, if not worse.

Volume No:2, Issue No:5 (October-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Security Services:

Security services is a service that provides a system with a specific kind of protection. The X.800 OSI Security Architecture defines six major security service categories, that once a system satisfies these six categories, the system is X.800 compliant.

Confidentiality:

To protectinformation from being read or accessed by un-authorized personnel.

Authentication:

Ensures that no one can impersonate someone to be rightfully authorized to access a services they should not access.

Integrity:

Ensures data cannot be interchanging and messages that are sent and received have not been captured, read, duplicated, changed or replayed to another party.

Non-repudiation:

Prevents the sender or receiver from rejecting the transmission of a both the parties message. The sender and receiver are able to be proved that they sent or did not send or received a message.

Access control:

Toprevent and limits to certain system services and applications to certain users.

Availability:

Ensures the service is only available to authorized users and not available to users who do not have access to the application.

Focus of implementation of Network Security:

Deter:

To educate people and obstruct people to break into systems for unlawful and malicious reasons.

Prevent:

To put in place measures to prevent unauthorized access. This can be authorizing uses with special access, encrypting communication, and improve security systems.

Detect:

To become aware of a security crack or breaches. This could be setting up logs to record who has login the system or accessed system or used the system.

Correct :

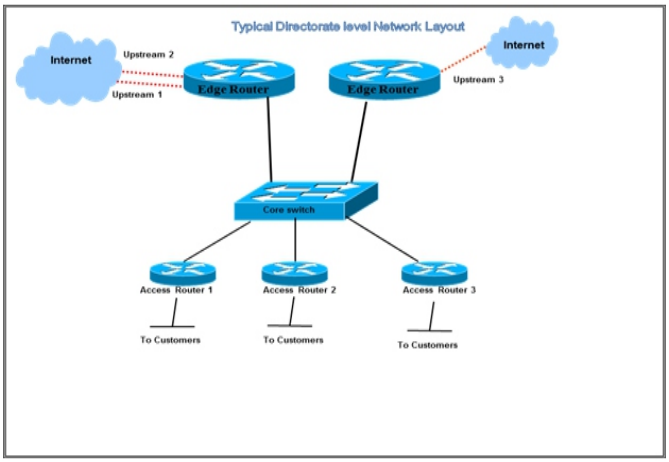
To implement a fix to the security flaw discovered in a system. If someone has penetrated the security of the system, implement measures to avoid it from happening again.

Router:

A router is a networking device that forwards data packets between WAN networks. Routers uses routing function to choose the best path to deliver the traffic from source to destination. Routers acts as a gateways and will be connected to one more networks (such as upstream networks). Routers uses forwarding and routing tables to find the best path to forward the packets. Routers can also be configured to act as a line of defence for your network and they must be configured to filter bogus networks and only allow to pass legitimate traffic as defined by the by the network administrators.

Present security mechanism deployed at a Typical ISP Network

The ISP Networks consists of Routers and Layer 3 Switches which are interconnected to serve the customer base. The figure depicts a typical network topology at an ISP NOC.



India has earned itself a very good reputation of an IT superpower. Internet Service Providers (ISPs) of India has played a crucial role in accomplishing this status.

Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)

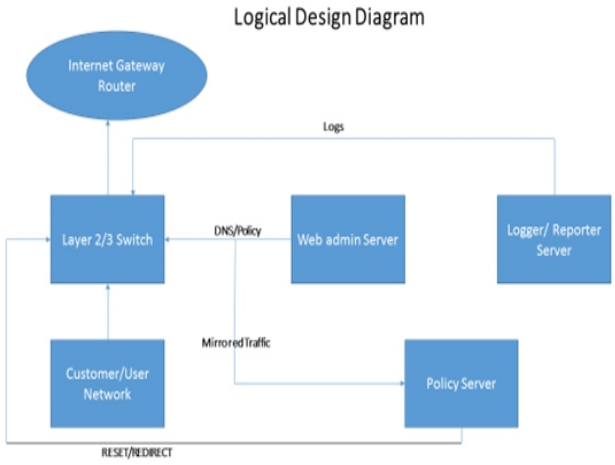
International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Today, ISPs across over the country are synonymous with excellent Infrastructure and Statutory support. ISPs are providing Data Communication services including Value Added services to IT/IT Enabled Services (ITES) related industries. Today's, ISP's face a huge challenge to manage their network security devices, as the technology grows and the challenge to maintain an optimum network security require huge efforts with the increase threats and growing concern from the Regulatory authorities to regulate the Internet access and content at certain level to safeguard the individuals and Institutions privacy. ISPs are receiving blocking instructions to block specific content in a particular domain and by blocking the Domain/URL's with IP address at router level. In most of cases, we 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, we are not complying with the regulatory authority's mandate. As the conventional techniques causes high CPU consumption and high latency issues due to millions of URL analysis requests need to be processed by the routers to check for the blacklisted domains which will impact the network devices performance, which will impact the core function of the routers to switch packets through the gateway.

Content based security mechanism at ISP Gateway level:



A model of Gateway Level Content based URL filter is available to address this issue. The URL filtering device is used to cache the data traversing the network and predefined group based on the domain can be created in the policy server.

The created the blacklist and whitelist of website in the policy server will check the traffic passing through the network. Additionally, we can create filters based on the requests to block the content from certain domain/websites. The results shows that the proposed scheme typically eliminates at least 90% of memory requirements as compared to a common hashing table solution. In ISP, enterprise, and other networks, URL filtering is widely used to prevent users to access unwanted things and malicious web sites. Several service and device providers like Fort iGATE, Juniper, Cisco, Websense, Checkpoint etc. provide network-based URL filtering (NUF) as a solution to classify, monitor, and control web traffic. NUF provides that has two important benefits over gateway-based URL filtering which analyses the URLs by simply comparing them with the local database in a gateway setup and updating the database continuously.

However, URL filtering vendors reported that they receive over million requests for URL categorization per day. A wide range of techniques have been proposed for improving web applications, like web access security, URL forwarding and lookup engine, and web proxy caching. Web content filtering is one of the popular approaches to provide web access security. The main key function of this method is the classification on web pages. It provides a hierarchical method for classifying a large collection of web content. In the works of different machine-learning-based approaches are used to implement web content filtering. Although those methods provide adequate filtering results, it seems to take too much time to complete the process each web page by multiple intelligent techniques. In contrast, Network URL Filter and Gateway Level URL Filter are more appropriate for ISP, enterprise, and other networks.

Conclusion:

This paper aims to discuss the security limitations in router and firewall systemswith respective tothe filtering techniques to achieve stronger secure networks without compromising or exposing the computer networks when connected to the Internet. At present, most of the Internet Service Providers are blocking the URL's with IP address at router level. IP based filtering methods may put additional load and processing overhead on router CPU to process the packets as well as to filter the traffic leaving the router. In recent times, the number blocking instructions from government bodies have increased to block

Volume No:2, Issue No:5 (October-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

specific content/page in particular website/social page. ISPs are finding it difficult to block such requests through the IP address, as it would block access to the entire domain instead of blocking required content in the domain and thus, this mechanism is not an effective solution to block the URL's.In such a case, ISPs are not complying with the DoT mandate. The methods discussed in this paper may address the filtering mechanism using certain strings or content based traffic specific to URLs passing through the Internet Gateway. We have presented suitable tips and inputsto achieve a strong security to protect the network from vulnerabilities, threats, and attacks by implementing the security configurations on router and firewall.

References:

[1]National Communications System, Public Switched Network Security Assessment Guidelines, National Communications System publication, 2000.

[2] Swanson Marianne and Federal Computer Security Program Managers' Forum Working

[3] Group, Guide for Developing Security Plans for Information Technology Systems, NIST Special Publication 800-18, 1998.

[4] Kim H., "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, FEBRUARY 2004.

[5] Rybaczyk P., "Cisco Router Troubleshooting Handbook ", M&T Books, 2000.

[6] Jo S., "Security Engine Management of Router based on Security Policy," proceedings of world academy of science, engineering and technology, volume 10, ISSN 1307-688, 2005.

[7] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. 2009,

[8] C.-K. Chu and W.-G. Tzeng, "Identity-Based Proxy Re-encryption without Random Oracles," Proc. Information Security Conf. (ISC '07), vol. 4779, pp. 189-202, 2007.

[9] Adi Shamir, "Identity-based cryptosystems and signature schemes". In Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985.

[10] The Importance of Network Security And The Types Of Security Attacks by Jack Cola On March 6, 2011.