International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 01 | Jan 2021 www.irjet.net p-ISSN: 2395-0072

Overview Towards Modern Day Intranet Security

Mr. Siddharth Singh

Student, Semester-III, MSC(I.T.), Keraleeya Samajam's Model College, Dombivali East, Thane, Maharashtra, India

---

Abstract - *The main objective of the study is to give overview on modern day use of intranet within an organization. The challenges faced by day-to-day organization while creating on-premise intranet or buying intranet services from cloud has been included in this paper. The latest vulnerabilities and threat that originates inside or outside the organization and the use of proxy server to secure your web log and intrusion prevention system to overcome any type of attack..*

Key Words: Intranet security; cloud and on-premise intranet; Internal and external threats; proxy server and their use; Intrusion Prevention System;

1. INTRODUCTION

1.1 Intranet is a restricted computer network used in sharing information, operational systems, and other computing resources within a corporation with the help of world wide web software. It is used to secure the network from getting access by unknown outside network so that the organization sensitive data or critical business critical information like projects details, employees data, etc.

1.2 **Intranet security-** Intranet security compromise of internal and external threats like weak password, unauthorized access, other vulnerability or attacks. Protecting intranet data is the primary objective of an organization like a robust intranet system.

1.3 WORKNG SOLUTION OF INTRANET

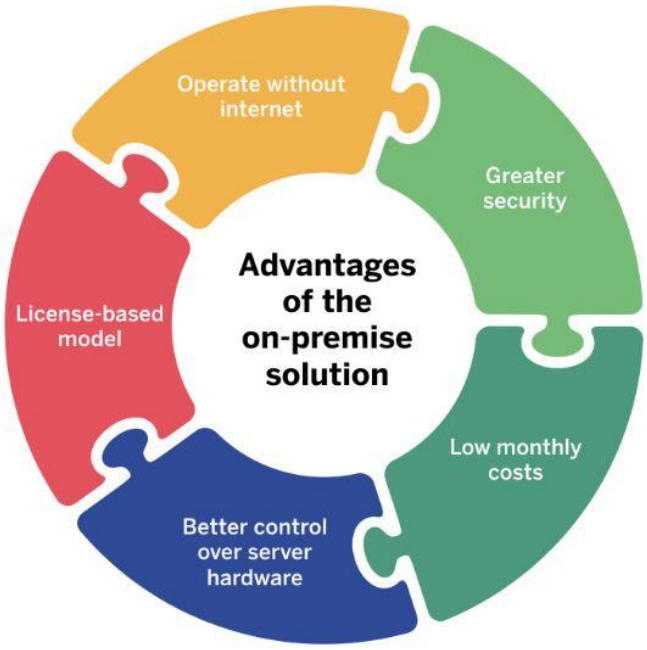
Intranet works on two methods and they are On-premise solutions and Cloud-based solutions. Depending upon the choice of the organization

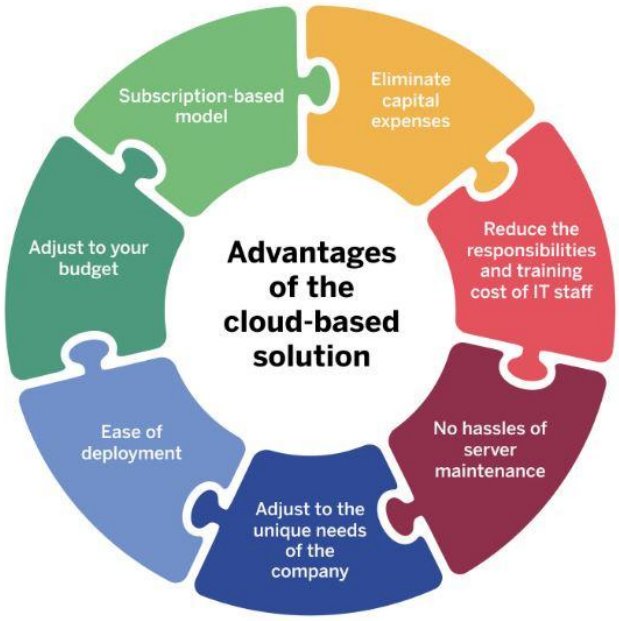
1.3.1 On-Premise Solution- The main reason why an organization wants to create their own intranet on-premise setup is-

- **Improved Security-** Security is a most important aspect of each and every organization in today's world. Since every IT resources are gathered in one space, so that it will be less likely accessible by hacker or any other intruders.
- **More Control-** Organization having complete control of their IT resources and softwares will lead them to carry out various operations and other activities.
- **Operate Without Internet-** No need for internet is required for any activity within an organization.
- **In-depth Customization-** An organization can carry out any customization to their intranet setup according to their business needs. A firm can customize certain aspects to achieve a more convenient and efficient results.
- **Integration of Current Processes-** For proper working of the intranet software, an organization needs to integrate all heir required business plan. When the intranet platform is been hosted, integration becomes very much easy and effective for the organization.

The cons of on-premise solution of an intranet-

- **Up-Front Costs-** The more the cost the more the expense of the on-premise based intranet. The cost depends upon the factors like- Hardware, area, licensing fees, etc. The new start ups or mid-firm organizations can be out of reach for the on-premise solution.
- **Possible Limit Mobile Access-** Mobile and tablet access towards any business software are increasing day by day. But on-premise solution does not always give access to mobile intranet connectivity and still their are certain organization which did not give access to their mobile device to enter in to their network or they make it much more difficult by using vpn hurdles as it can limit the functionality of the employees device.
- **Lack Of IT Support-** Their can be a issue while installing a new piece of software and for resolving his issue, an organization needs to hire internal IT professional or to increase the number of professionals depending upon the increase in hardware ad software in intranet.





1.3.2 Cloud-Based Solution-

The cloud is day-to-day a most crucial aspect of many professional and cloud-based software are growing day by day among the many organizations. Some of the services which have made cloud-based intranet service more beneficial-

- **Cost Savings-** Cloud intranet software provide less cost compare to on-premise solution as per business needs of the organization. In cloud intranet software, a organization doe not require to spend money on any IT resources.
- **Remote-Friendly-** This is the most beneficial features, as it will operate business of an organization remotely.
- **Improved IT-** Their are various reputed cloud softwares vendor which provide high quality IT support to their client.
- **Seamless Update-** Any new update rolled out by cloud vendors will be applied to their client quickly and easily.

The cons of cloud-based solution of an intranet-

- **Lack of Control-** Some organization wants full control over their intranet IT resources rather than depending upon the cloud vendors.

2. INTRANET THREATS

Most of the vulnerabilities that occur usually comes from internal threat. There are basically two types of threats to intranet system. They are internal and external threats:

2.1 Internal Threats- Most of the vulnerabilities that occur usually comes from internal threat. Internal security threats pose challenges to organizations intranet. The types of internal threats are:

- **Weak Password-** Nowadays network administrators with good password practice can secure the work effectively. The network administrators need to have the knowledge about how the weak password or writing password anywhere can lead to an attack. The network administration must set account locking after certain number of attempts, set password expiration and train the new employees about the password policies.
- **Unauthorised Access-** The right employees should have the right access to the specific information. For example, employee in Finance department should not have access to the sensitive information of marketing or HR department. Network administrator perform this by applying the roles by department, location, job title. The Access permission should be verified on every day so that, an ex-employee of that organization till now have the access to that department information may result in information security risk or loss.
- **Bring Your Own Device(BYOD)-** Since, increase in the mobile use, many of the organization have allowed BYOD policy. BYOD policy has much more security risk. The biggest problem arises if employee loses his/her device or device get stolen which can be a major

problem and it can lead to legal implication of client's sensitive data. For this problem, the IT department should start remote wiping as soon as they knew about it so that, the data in the device get erased before it can be accessed by wrongful hands.

2.2 External Threats

- **Network Attacks-** An invasion on your network is known as network attack. In this attack, the attacker will be able to analyse your environment, gain unauthorised access to any data. To protect data from network attack, intrusion prevention system is used.
- **Security Breaches-** Sometimes intranet might encounter suspicious traffic. It can be include things like phishing, spam, malware and adware. To block such type of traffic from entering the network, we can use most effective email filters and firewall. Email filter will not allow the threat from reaching the inbox and firewall integrated with latest antivirus software and email filter will safeguard the network.

3. WHY TO CHOOSE PROXY SERVER FOR INTRANET SERVICES FOR SECURITY

3.1 **To Control Internet Usage Of An Organization-** Most organization setup proxy server to monitor the use of the internet by their employees. Most organization doesn't want to access to specific website at their work time and they configure the proxy server to deny access to that specific site. Organization can also monitor and log all the web request, so that the organization will be able to record the web sites been accessed by their employees.

3.2 **Bandwidth Savings and Improved Speeds-** A better overview of a network performance will be recorded by a good proxy server. Proxy servers can save a copy of popular websites in a form of cache memory- so when you ask for google.com, the proxy server will check the most recent coy of that website and send it back. For example, within an organization their are 100 employees who are accessing website www.google.com at the same time from same proxy server, the poxy server sends only one request to that website as this will improve the network performance and saves bandwidth.

3.3 **Privacy benefits-** Proxy server use to change the IP address and other information web request contains to provide more security and privacy by not allowing destination server to get the details of the original request.

3.4 **Improved Security-** The man purpose of the proxy servers are to provide security benefits. Encrypting the web request by configuring the proxy server helps from offensive attacker from getting your transactions. Now a days, company can configure their proxy servers with the vpn so that, organization can keep track of employees record remotely and the employees have access to the organization internal data and resources.

4. RISK RELATED TO PROXY SERVER

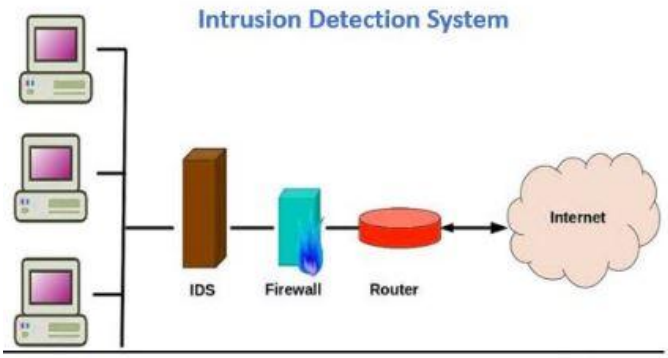
4.1 **Free Proxy server-** As the free proxy services are likely to be very much risky even though the services are using ad-based model to earn money. Free proxy servers do not invest high on their backend hardware or on their encryption techniques. This will result in lower performance. Some of the free proxy servers are use to get the confidential data.

4.2 **Browsing History Log-** Whenever we use a proxy server to get some privacy and security but the vendor saves all this information without encrypting it. Check with vendor about the law enforcement policy thy follow.

4.3 **No Encryption-** Proxy server without encryption is like passing your data as plain text so that it's confidentiality or integrity of that data can be compromised.

5. NEED OF INTRUSION PREVENTION SYSTEM ON INTRANET

5.1 **Intrusion Prevention System(IPS)-** IPS is a technique used to detect and prevent the system from network security/threat by examining the flow of network traffic to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to target application. Following a successful attack on the application -system, the attacker can disable the target application, or can potentially have all the admin access and permissions to the compromised application. The below figure shows the working of IPS:



5.2 An intrusion prevention system works by actively scanning forwarded network traffic for malicious activities and known attack patterns. The IPS engine always check the network traffic and continuously compares the bitstream with its internal signature database for known attack patterns. A network packet which acts malicious can be dropped by IPS to check the malicious activity, and follow up this action by blocking all future traffic from the attacker's IP address or port. legal and genuine traffic can continue without getting any disruption in service.

Complicated observation and analysis will also be performed by IPS, such as watching and reacting to suspicious traffic patterns or packets. Detection mechanisms can include:

- Address matching
- HTTP string and substring matching
- Generic pattern matching
- TCP connection analysis
- Packet anomaly detection
- Traffic anomaly detection
- TCP/UDP port matching

An IPS keep the log file of record information related to any observed events, notify security administrators, and produce reports. All the latest security updates are patched to IPS automatically so that, it will be helpful in securing a network to monitor and block emerging Internet threats.

5.3 Intrusion Countermeasures

Many IPS not only detects the threat but also prevent the threat from doing any further damage. They use several response techniques, which involve:

- Changing the security environment
- Changing the attack's content
- Sending automated alerts to system administrators, notifying them of possible security threats.
- Dropping detected malicious packets.
- Resetting a connection.
- Blocking traffic from the offending IP address.

5.4 IPS Classifications

The four major types of intrusion detection system are:

- Network-based intrusion prevention system (NIPS)
- Wireless intrusion prevention system (WIPS)
- Host-based intrusion prevention system (HIPS)
- Network behavior analysis (NBA)

5.5 IPS Detection Methods

The majority of intrusion prevention systems based on one of the three detection methods: signature-based, statistical anomaly-based, and stateful protocol analysis.

- Signature-based detection
- Statistical anomaly-based detection
- Stateful protocol analysis detection

6. CONCLUSIONS

In our paper, we have tried to explain about intranet. We have learned about how intranet services are deployed in modern time period and how it is being upgraded day by day as a new security threats emerges day-to-day and use of proxy server with intranet services for privacy and security. We have also discussed in brief about intrusion prevention system which is been the key most feature of intranet security.

7. REFERENCES

[1]https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/

[2]http://www.differencebetween.net/technology/internet/difference-between-intranet-and-vpn/

[3]https://www.myhubintranet.com/intranet-security/#:~:text=Security%20Breaches,to%20block%20this%20suspicious%20traffic.

[4]https://www.interact-intranet.com/security/

[5]https://ieeexplore.ieee.org/document/5453682

[6]https://www.unily.com/cloud-intranet-solutions-for-the-enterprise#:~:text=A%20cloud%20intranet%20provides%20employees,collaborate%20and%20drive%20productivity%20effectively.

[7]https://socpub.com/articles/premise-vs-cloud-based-intranets-16355

[8]https://www.scnsoft.com/blog/intranet-security-best-practices

[9]https://www.myhubintranet.com/hosted-intranet-security/

[10]https://powell-software.com/en/intranet-security-for-remote-work/

[11]https://axerosolutions.com/blogs/timeisenhauer/pulse/182/cloud-intranet-software-vs-on-premise-solutions

[12]https://www.varonis.com/blog/what-is-a-proxy-server/

[13]https://www.barracuda.com/glossary/intrusion-prevention-system