HOW TO ESTABLISH A HIGHLY SECURE HIGH AVAILABLE AND RELIABLE NETWORK ENVIRONMENT.

ABSTRACT

This research paper presents how to establish a network with high availability, reliable and highly secure network environment. Main objectives of this network design are,

a. A reliable network to interconnect branch offices and headquarters.
b. Remote access to network for employees.
c. Implementing a large data center.
d. Implementing a disaster recovery plan.
e. Implementing a maintenance plan.
f. IP PBX to communicate among branches.
g. Video conferencing capabilities among regional branches.

The network setup; main server in the office headquarters with disaster recovery plant, web server in the branch office, located in a different country. And two data centers in each location for high availability purpose.

INTRODUCTION

The rise in organized crime use of the Internet, cyber espionage, growing data theft, and the increasing sophistication of network attacks are all examples of the real threats faced by organizations these days. According to the past experience most of the attackers looking for the vulnerabilities of the network because attack should be conducted through the network in most of the cases. So implementing highly secure network is most essential to any organization. As a key enabler of the business activity, networks need to be designed with security in mind, and to ensure the confidentiality, integrity and availability of applications, endpoints and the network itself. These days many threats are coming from both outside and inside effects. So it is highly recommended to secure the environment from both of those threats. The Internet edge design incorporates security as an important component of the network architecture, where a rich set of security technologies and capabilities are deployed in a layered approach, but under a common strategy.

In this proposed design, it is clearly describe the secure design strategies of the network which are located in two different places. Disaster Recovery (DR) plan is also proposed here. So that it will highly concern about the security of the network. Not only that, it will concerned on high availability as well. In this example an office environment consists with a DR site. There are some facilities on the network which are described above. Also it is concerned about forensic friendly environment for investigation the log reports of incidents. Also maintains plan such as auditing and log report reviewing etc. Intrusion detection and prevention capabilities are also described broadly in this design.

NETWORK DESIGN

As mentioned office headquarters having a main server and DR site located in one country and branch office is located in another. Then three locations were identified in the network. They are;

a. Headquarters site.
b. Branch site.
c. Disaster recovery site.

According to the scenario, following are facilities and requirements that organization have;

a. IP PBX to communicate among the branches.
b. Video conferencing among the regional branches.
c. Remote access to the network for employees.
d. Reliable network connection to interconnect headquarters and branches.
e. Normal office desktop access to the employees.

Following are the factors considered during the network design;

a. Fulfill all the above mentioned facilities and requirements.
b. High security of the network.
c. Reliability of the network.
d. High availability of the network.
e. Disaster recovery plan.
f. Forensic friendly environment.
g. Service level standers.
h. Economic considerations (will not be highly considered).
i. Maintains plan.

Security is mainly considered during the design of the network, but when we consider the design phase we should consider about confidentiality, integrity, and availability (CIA) of the system. These three factors should be balanced in any system. Otherwise there will be huge problems arise from both customer side and employee side. As mentioned above high availability for both ends are highly concerned. Disaster recovery plan should be realistic and executable at any time. Also if any incident happened there should be a capability of the investigation what had happened, how it happened and what cause it to be happened? That is forensic friendly environment. Also there should be a regular audit on network related equipment (both software and hardware) in security concern. Finally, economic factors should be considered but it should not be harmful to the security of the network.

Firewall configurations

Document all firewall rule changes.

Firewall management products provide a central dashboard that provides full visibility into all firewall rule bases, so all members of the team have a common view and can see who made what change, when made it and from where. This makes troubleshooting and overall policy management much easier and more efficient. So it is essential to document all the firewall rules from the beginning and also all the changes during the operation process should be documented.

Install all access rules with minimal access rights.

A firewall rule is made up of three fields: source (IP address), destination (network/subnet) and service (application or other destination) (Anon, 2017). Normally common practice has been to assign a wide range of objects in one or more of those fields. This will become insecure network. According the user level, firewall rules should be configured. There are some users who required accessing some web applications where others do not required as per the official commitment. So when configure the firewall it is required to allocate dedicated IP address to the each user and MAC address of the each device should bind with IP address. So according to the official requirements firewall rules can be set to which IP address can access to which port and which web application. All the firewall

rules should comply with the policy of the organization.

Rules:

a. Permit IP "any-any" - Allows all traffic from any source on any port to any destination. This is the worst type of access control rule. It contradicts both of the security concepts of denying traffic by default and the principal of least privilege. The destination port should be always specified, and the destination IP address should be specified when practical (Support.rackspace.com, 2017).
b. Only ports 80 (HTTP) and 443 (HTTPS) should be configured to access the web server
c. Give specific IP address to access to the database.
d. Allow SSH traffic for port 22 for specific IP address.

Perform a complete firewall review at least twice per year.

Firewall reviews also are a critical part of the maintenance of firewall rule base. Networks and services are not static so your firewall rule base should not be either (Anon, 2017). As corporate policies evolve and compliance standards change, we need to review how we are enforcing traffic on the firewalls. This is a good place to clean up all those redundant rules that have been replaced by new rules.

IDS/ IPS configuration

With IPS, it is best to concentrate at the perimeter and at externally facing services such as FTP, email, and Web services. There are classifications for most exploits, spyware, and malware that could find their way into the environment (Best Practices for Deploying Intrusion Prevention Systems, n.d.). It is important to classify threats so that they can be dealt with effectively as a group, whenever possible. Managing threats individually can be daunting. However, at many levels there are often commonalities between threats in how they act, infect, and spread.

Threat classification

Authentication and authoritative issues. This could include:

a. Privileged access - acquiring administrative credentials (such as root) without proper authorization.
b. User access - acquiring the credentials of a user without proper authorization.

Malware. This could include:

a. Worms - matching known service exploits or perhaps acting similar to a known exploit.
b. Code execution - the execution of arbitrary exploit code on a targeted system that may install unwanted components such as keyboard loggers.

Denial of Service (DoS) - denies service to legitimate uses. This could include:

a. Ping of death.
b. Syn flood.

Application-based attacks - attempts to exploit vulnerabilities in certain kinds of servers by means of buffer-overflow and injection-attack attempts including:

a. Web-based injection attacks that try to gain access to information or privileges outside the domain of the application.
b. Buffer-overflow attacks aimed at general applications or services.
c. DNS usurping and spoofing.

Tuning an IDS

There are four points of concern. These four points are true positives, false positives, true negatives and false negatives (Sans.org, 2017).

	Positive	Negative
True	True Positive: Alerted on intrusion attempt	True Negative: Not alerted on benign activity
False	False Positive: Alerted on benign activity	False Negative: Not alerted on intrusion attempt

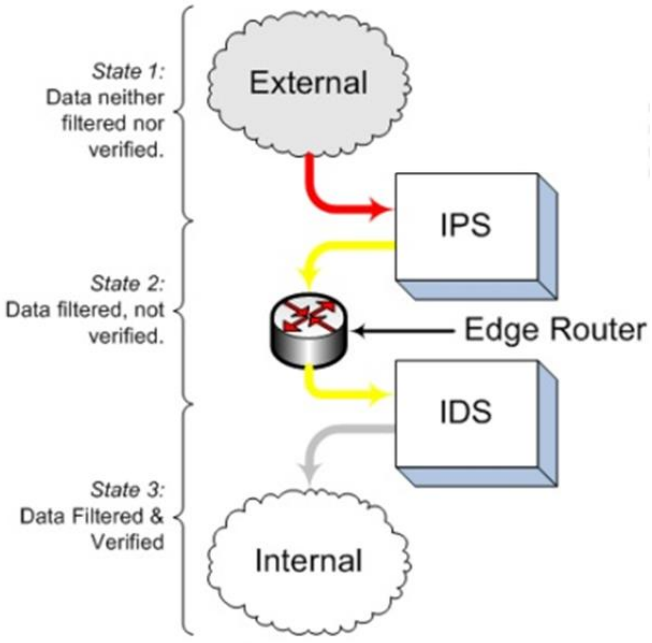
True positives occur when the system alerts on intrusion attempts or other malicious activity. False negatives are somewhat of a null situation but are important nonetheless. The false negative is comprised of the system failing to alert on malicious traffic. The IDS were tuned according to the above categorizations and also it was configured to save logs for auditing and forensic investigations if required.

Placing a IPS/IDS

When placing IPS/IDS following points were considered;

a. Behind firewalls and WAN routers.
b. In front of server farms or similar collections of resources.
c. At other network access points.

IDS and IPS connected separately as per the figure below. Also Bandwidth requirements should be considered when placing the IPS and IDS.



Best practices adapted

a. Proactive, real-time prevention of attacks.
b. Patch management.
c. Configured according to the company policy.
d. Configured not to disturb the high availability of the network.

Achieving high availability

Achieving high availability is most important in the network. There should be redundancy network as well as redundancy components also should be there.

Load balancing is most important when we consider on high availability of the network. Load balancer distributes network or application traffic across a number of

servers. They are used to increase availability and reliability of applications. They improve the overall performance of applications by decreasing the burden on servers associated with managing and maintaining application and network sessions, as well as by performing application-specific tasks (F5.com, 2017). In this case load balancer is used in before the servers to smooth functioning of the network.

Also there are number of redundancy routers are located in the network to address the system failures. Circuit diversity is also more important when designing of the network. According to the diagram all the VPNs and outside PSTN connections have redundancy path to connect if there is any failure in the network. Also DR site also located in different location for address any disaster situation.

IPS and IDS also located only for the necessary end points to reduce the unnecessary slowness of the network.

Disaster recovery plan

Disaster recovery plan is another important factor in network designing. DR site should geographically locate in separate place to the main site and there should be good communication with the DR site in any situation. According to the level of redundancy, this network have a primary connection and then a secondary connection set up, so that people can get to those applications when there is a disaster (SearchDisasterRecovery, 2017). Bandwidth of the DR site also considered when designing the network to overcome unexpected slowness of the network during the disaster situation.

Also synchronization of the both server in DR site and main site is very important. All the data in the servers should be backup in the backup servers. It means replication of the data as required.

All the network infrastructures were replicated. For example, DNA failover to make sure that production URL is pointing to the DR site after the failover. Firewall rules (or anything security related) in the primary datacenter, is support to replicate to the DR site on an ongoing basis.

When apply OS patch, upgrade firmware, or perform any kind of configuration management to the hardware in the primary site, we need to have a strategy to do those on the DR site on an on-going basis (Anon, 2017).

DR plan should be documented and it should be practice once a year.

IP PBX communication

VoIP PBX brings with it risks that can't be ignored. Among them, denial-of-service attacks, privacy breaches, and theft of services are very popular. For voice communication separate VLAN is allocated in each site with IP calling facility with the firewall it is a best way to secure the network. Firewall rules should deny all Internet access to IP PBX servers, gateways, and phones, and should limit access between the phone VLAN and IP PBX (Network Computing, 2017). Allocate better control bandwidth to the IP PBX will reduce Denial of Service attacks. Limit the UDP and TCP ports that can access the IP PBX from the VLAN by using the access control lists by installing a firewall to limit the TCP and UDP ports that are vulnerable. Use of VoIP phones with the encryption is also good practice.

Mail server configuration

With a mix of email services on-premises and in the cloud, we can stay on top of securing two different platforms with two different architectures. This also gives high availability of the mail system.

In this setup, there are some mailboxes are in Office 365 and some are on own email servers, set up connectors to enable mail flow in both directions. Mail flow is enabled between Office 365 and any SMTP-based email server. Firewall is configured in order to open port 25 with the Office 365. Customization can be done for mail flow between two servers. Also synchronization between two servers should be done.

Maintains plan

Routine maintenance of servers should be done, including defragmentation, disk space monitoring, event log monitoring and patch management (B&B Networks Inc, 2017). Also analyze data security measures regularly and determine vulnerabilities; Network security measures; Database security measures; Platform security measures; Application security measures; Employee file permissions, password policies; physical access to critical assets; analyze change management policies and procedures.

Network security measures are very important. There should be good practice of maintaining the network devices, software upgrading, updating, and patch management. Also all the system logs should be keep and review by an audit. Maintain plan should be done for DR site also. Firewalls should be audited regularly and ensure the firewall rules are sufficient to protect the environment and unnecessary rules must be deleted if they are no longer required. All the network devices such as switches, routers and IPS/IDS should be audited and ensure the security measures of each devices.

Forensic friendly environment

Creating a forensic friendly environment is essential in order to address any security related incidents. Therefor it is required to have logs on each and every event on the system. System log server should implement to review all of the incidents. Other than that all the routers switches should configure to store logs as much as possible. IDS/ IPS logs are most important log repots for that it is required to implement Log-based Intrusion Detection Systems (LIDS) addition to the Network-based Intrusion Detection Systems (NIDS). LIDS are also used to detect computer misuse, policy violations and other forms of inappropriate activities (Sans.org, 2017).

Log management infrastructure is most important in forensic friendly environment design (Sans.org, 2017). Log management infrastructures typically perform several functions that assist in the storage, analysis, and disposal of log data. These functions are normally performed in such a way that they do not alter the original logs. General functions of log management infrastructure include log parsing, event filtering and event aggregation. On the storage side, log management has to provide for log rotation, log archival, log compression, log reduction, log conversion, log normalization and log file integrity. Event correlation, log viewing and log reporting are some of the analysis functions of a log management infrastructure.

CONCLUSION

In any network design security will be the main factor. Most of the attacks are coming through the network vulnerabilities. This proposed network design illustrates the secure design of the network in order to prevent inside and outside threats. Other than the security it concerned on high availability of the network, reliability of the network and auditing of the network. Also firewall configurations and DR site implementation was discussed.

REFERENCES

1. Anon, (2017). [online] Available at: https://www.networkworld.com/article/2247110/network-security/top-5-best-practices-for-firewall-administrators.html [Accessed 11 Oct. 2017].

2. Support.rackspace.com. (2017). *Best practices for firewall rules configuration*. [online] Available at: https://support.rackspace.com/how-to/best-practices-for-firewall-rules-configuration [Accessed 11 Oct. 2017].

3. Best Practices for Deploying Intrusion Prevention Systems. (n.d.). Wick Hill.

4. Sans.org. (2017). *Cite a Website - Cite This For Me*. [online] Available at: https://www.sans.org/reading-room/whitepapers/intrusion/network-ids-ips-deployment-strategies-2143 [Accessed 7 Oct. 2017].

5. F5.com. (2017). *Load Balancer*. [online] Available at: https://f5.com/glossary/load-balancer [Accessed 9 Oct. 2017].

6. SearchDisasterRecovery. (2017). *Disaster recovery planning and network services*. [online] Available at: http://searchdisasterrecovery.techtarget.com/feature/Disaster-recovery-planning-and-network-services [Accessed 9 Oct. 2017].

7. Anon, (2017). [online] Available at: http://www.thegeekstuff.com/2011/08/it-disaster-recovery/ [Accessed 11 Oct. 2017].

8. Network Computing. (2017). *Is Your IP PBX Secure?*. [online] Available at: http://www.networkcomputing.com/infrastructure/your-ip-pbx-secure/708097298 [Accessed 11 Oct. 2017].

9. B&B Networks Inc. (2017). *Network Administration and Proactive Maintenance*. [online] Available at: https://www.bb-networks.com/network-admin-duties-proactive-maintenance/ [Accessed 11 Oct. 2017].

Author; Manoj Rasika Koongahawatte
191 AEM 029
RTU