Global Information Assurance Certification Paper

SANS GIAC Security Essentials

Practical Assignment

GSEC 2001

Secure System Architecture and Design

Submitted by:

Rozana Rusli

December 2001

Secure System Architecture and Design

1.0 Purpose

This documentation provides basic security guidelines and some best practices that worth considering when designing and implementing a network that connects to the Internet. Most of the principles are best suited for organizations of medium sizes that offer access to their resources via the Internet. It does not discuss any particular network design concept but rather a more general basic principle that makes up a good system architecture and design. It also does not match to any specific threats and their methods of mitigation. The guidelines are drawn from lessons learned from current network issues and problem faced by most organizations today.

2.0 Introduction

The security architecture and design of a site refers to the overall layout, the security and network strategy, and the design of the organization or system application. This includes important issues such as network trusts, trusted hosts access, trusted user access, connections to the outside world, and how these connections interact with the site. All of these are of special interest when planning for a secure network design.

The objective of a secure network design is to ensure that the network is protected from attacks and for data availability, integrity and confidentiality. The driver process for implementing network security is through security policy. A security policy is a formal statement, supported by a company's highest levels of management, regarding the rules by which employees who have access to any corporate resource abide. Security architecture should be designed by integrating the network design requirement and IT services offered through the network infrastructure. This is to ensure that the network security architecture and design meet organization objectives.

3.0 Background

Most organizations implement simple network design or what is known a 2-tier network design. The basic 2-tier network design implementation consists of only the DMZ and the private network as its two main network segments. There is no segregation between servers and users workstations in the internal network, with both sharing the same network segmentation. This raises the level of risk from internal attacks such as session hijacking and network sniffing. The risk is further alleviated since internal access control and network monitoring are mostly insufficient. With the absence of Intrusion

Detection System in a network, all attempts made to compromise the integrity of the network will not be detected. Network monitoring tool, ideally, facilitates the detection and evasion of any potential network problems before they noticeably affect the quality of service to its end-users. Such preventative measures can often result in cost savings in the long run.

Most organizations feel that their networks are secure when they already have a firewall in place. However statistic shows that most intrusion occurred despite the presence of firewalls. From the 2001 CSI/FBI Computer Crime and Security Survey, 64% of respondents detected unauthorized use of computer systems in the last 12 months. 40% detected "system penetration" even though 95% had a firewall and 61% had an IDS. Attacks increase the risk of being on the Internet. Without proper and careful security planning, the environment can get even riskier.

4.0 Basic Guidelines

The guidelines are broken down into main components that address an effective network security environment and network operational management.

4.1 Network segmentation

To design a secure network, consideration such as separating the location of servers based on functionality and accessibility is crucial. This helps on mitigating risks as well as to ease the maintenance and management of the network. This can be achieved by implementing separate network segments based on its network policy that governs the flow of traffic in a network. The main network segments that cut across most organizations' network requirements for connecting to the Internet are basically as follows.

a. DMZ – Demilitarized Zone segment

This is the network that lies in front of the firewall. Its only real protection is the border router where some access filters could be applied. Only public service requirements would be positioned within the DMZ such as Remote Access Servers. It is also to host system that monitors all inbound and outbound traffic coming from the firewall and the Internet ie IDS. However any system on the DMZ should be completely stripped down and fully secured. This includes making sure all patches are up to date, compilers

are disabled, all unneeded services are removed, all unneeded accounts are removed and so forth.

b. Semi-Public segment (Screened subnet)
This network lies behind the firewall. It is called semi-public since connections could both come from the public and private network. Ideally, both external and internal traffic must go through the firewall to get to this network, and are tightly controlled and logged by the firewall. This network segment is to provide access to resources like rudimentary DNS service, Mail server, and Web server. Any extranet requirement is also positioned within this network. Since access is allowed from public, it is best that all servers are completely stripped down or hardened and fully secured. This is also a termination point for connectivity to external Business partners.

c. Trusted segment
This network is also located behind the firewall. The network is connected to the third interface of the same firewall or behind another internal firewall. This network is only accessible by trusted hosts. Trusted hosts are hosts that are authorized to access the servers in the network due to its known identity such as IP address or MAC address. This network segment is to provide access to production servers mainly running internal and private applications that require stringent security policy. Servers that are hosting highly sensitive information are positioned within this network segment. This includes the application server, Intranet server, and internal mail server. These are mainly database servers.

d. Private segment
This network segment is hosting the users workstations. It is not providing any server application services. Access from outside is restricted. This network should behave like a diode. It is only a one-way traffic where only outgoing traffic is allowed. It needs to be separated from the servers to minimize internal security risk such as session hijacking and network sniffing. This can be achieved using a router or other filtering device.
A graphical presentation of the network segments discussed above is depicted in the Figure 1.0.

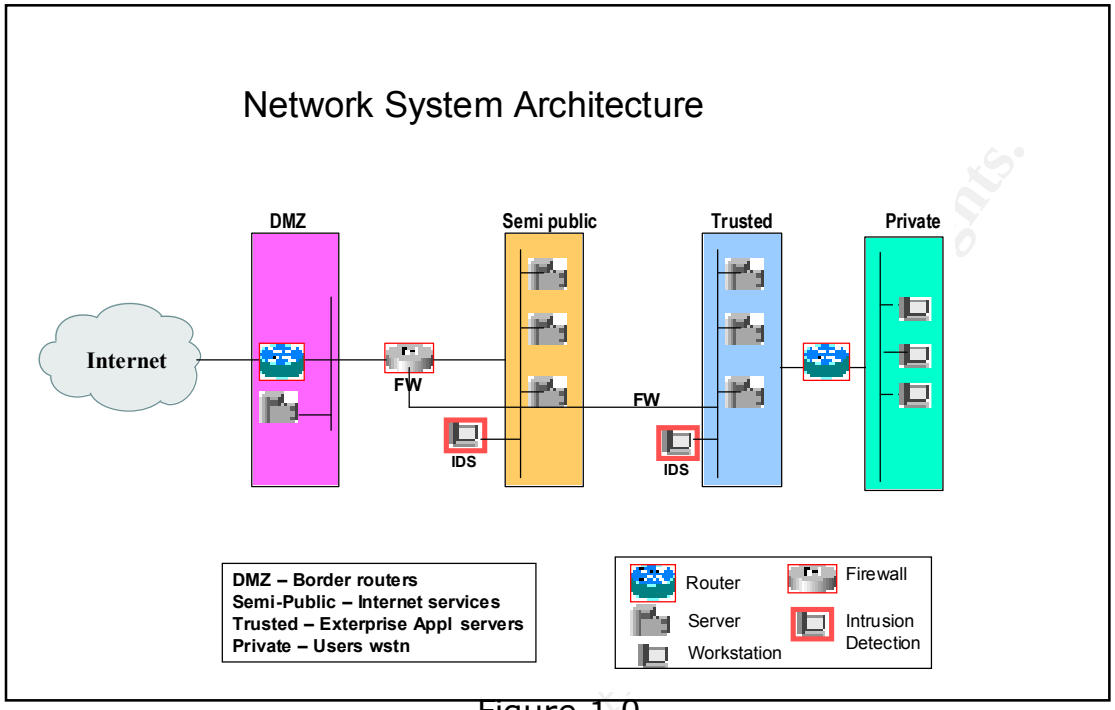

Figure 1.0

4.2 Critical networking services

With regard to Internet best practices, critical Internet services such as DNS, mail and web are best be separated into dedicated servers to minimize risk as well as ensuring reliable system performance.

Mail server is best run on a dedicated machine looking at the volume of mail, which is commonly high. Internet mail is considered as one of a mission critical application by most organizations in view of the growing reliance of users in using it as a prime platform in communicating with the rest of the world in its daily business operations. This is to prepare for a 100% uptime and availability.

Most organizations offer online services over the Internet, which then makes the web and DNS as critical services. And this would require these services to be run on dedicated servers to minimize other system interruptions and downtime. It is recommended for all these services to be run on a stripped down machine with the operating system fully hardened.

Separating services not only enhance system availability it also contributes to a more secure system implementation. A 2-tier application design approach is best suited for web-based database application accessible from the Internet. Adopting this approach requires it to separate the two critical services, Web and

Database. The web access is only accessible to the web server also commonly known as the staging server residing in the semi-public segment. While the database server resides in the private network segment allowing only restricted access coming from a trusted host that is the web server. Such implementation will minimize risk of unauthorized access to the database server where critical information may reside.

4.3 IP addressing Scheme

It is best for an organization to adopt private IP address for its private Network. Private IP should be the standard IP assignment for the private network implementation. This is to allow for ease in IP address management and distribution. In addition this would allow for better security control since private IP is not routable in the Internet. In a large organization, it is advised that a proper IP addressing scheme be adopted.

Private RFC 1918 addresses are as follows:

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

4.4 Network Management and Monitoring

For an enterprise network, the network needs to be monitored and managed from a central location. A network of a considerable size requires it to be managed using a Network Management System. It is very important to have this for network administrator to monitor on-going activities on the network. All connectivity from the external networks can be easily monitored and controlled. SNMP strings can be added to the router configuration with limited access to specified workstation or server such as network management server. The bandwidth utilization can be monitored by any network monitoring software such as the most widely used is MRTG- Multi Router Traffic Grapher. It is a free software which is downloadable from the Internet; http://mrtg.hdl.com/mrtg.html. Such implementation allows for proper control and monitoring measure. It could support such planning and projection work for enhancement and upgrade of the network infrastructure.

For network monitoring function, Intrusion Detection System located at critical network segments are required and supported by a central logging server which maintains audit trails of all critical server access and activities. The central logging server correlates logs from multiple servers allowing the network

administrator to effectively analyze the logs for intrusion trends and traffic patterns. Review of the logging can be automated by installing security log analyzer software such as :

Unix – Swatch
ftp://ftp.stanford.edu/general/security-tools/swatch
NT – Ntlast
http://www.ntobjectives.com
(Refer to http://www.whitehats.com for other log analyzer tools)

4.5 High Availability/Redundancy

With the Internet becoming increasingly important, a redundant link to the Internet becomes pertinent for business resumption. The Internet link can be optimized for fail-over and redundancy purposes. Should the primary connection fail, connection to the outside world is terminated. A secondary connection allows for high availability to mission critical application in an Internet network implementation. To achieve higher availability it is preferred for an organization using the Internet as a serious business tool to have links connecting to two different Internet Service Providers (ISPs). With the use of a load balancer, access to the application hosts can be further optimized.

By establishing secondary or backup servers for all critical services such as web, mail, and DNS allows for backup and redundancy option. The firewall is another critical service that requires doing automatic fail-over for high redundancy access to critical networks.

5.0 Conclusion

Although the infrastructure can successfully be used to create a secure environment, it is not the only factor for an optimum network security. An awareness of the importance of security and accountability within an organization should be created. Establishing good security policy, staying up to date on the latest development in the hacker and security communities, maintaining and monitoring all system with sound system administration practices are amongst the heart of best practices in network security.

References:

Brenton, Chris. "*Advanced Perimeter Protection and Defense In-Depth*." *SANS Security DC 2000 Conference Proceedings*, Washington

Brenton, Chris. "*Firewalls 101: Perimeter Defense with Firewalls*." *SANS Security DC 2000 Conference Proceedings*, Washington, D.C.: July 2000.

"*Cisco IOS Security Architecture*", May 1995. URL: http://www.cisco.com/warp/public/614/9.html

"*Address Allocation for Private Internets*", Feb 1996. URL: http://www.faqs.org/rfcs/rfc1918.html

"Computer Security Institute – Computer Crime and Security Survey" , Mar 2001. URL*:* http://www.gocsi.com/prelea/000321.html

"*Network Security Audit – System Architecture and Design*". MIMOS Consulting Group, MIMOS Berhad.

****

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor