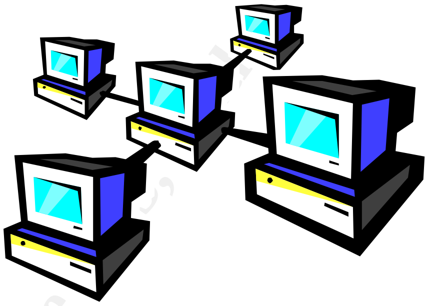
Secure Network Architecture:

Best Practices for Small Business and Government Entities

Stan Jenkins

April 3, 2003



GIAC Security Essentials Certification (GSEC)

Practical Assignment

Version 1.4b (amended August 29, 2002)

Table of Contents

Secure Network Architecture: Best Practices for Small Business and Government Entities

Stan Jenkins

April 3, 2003

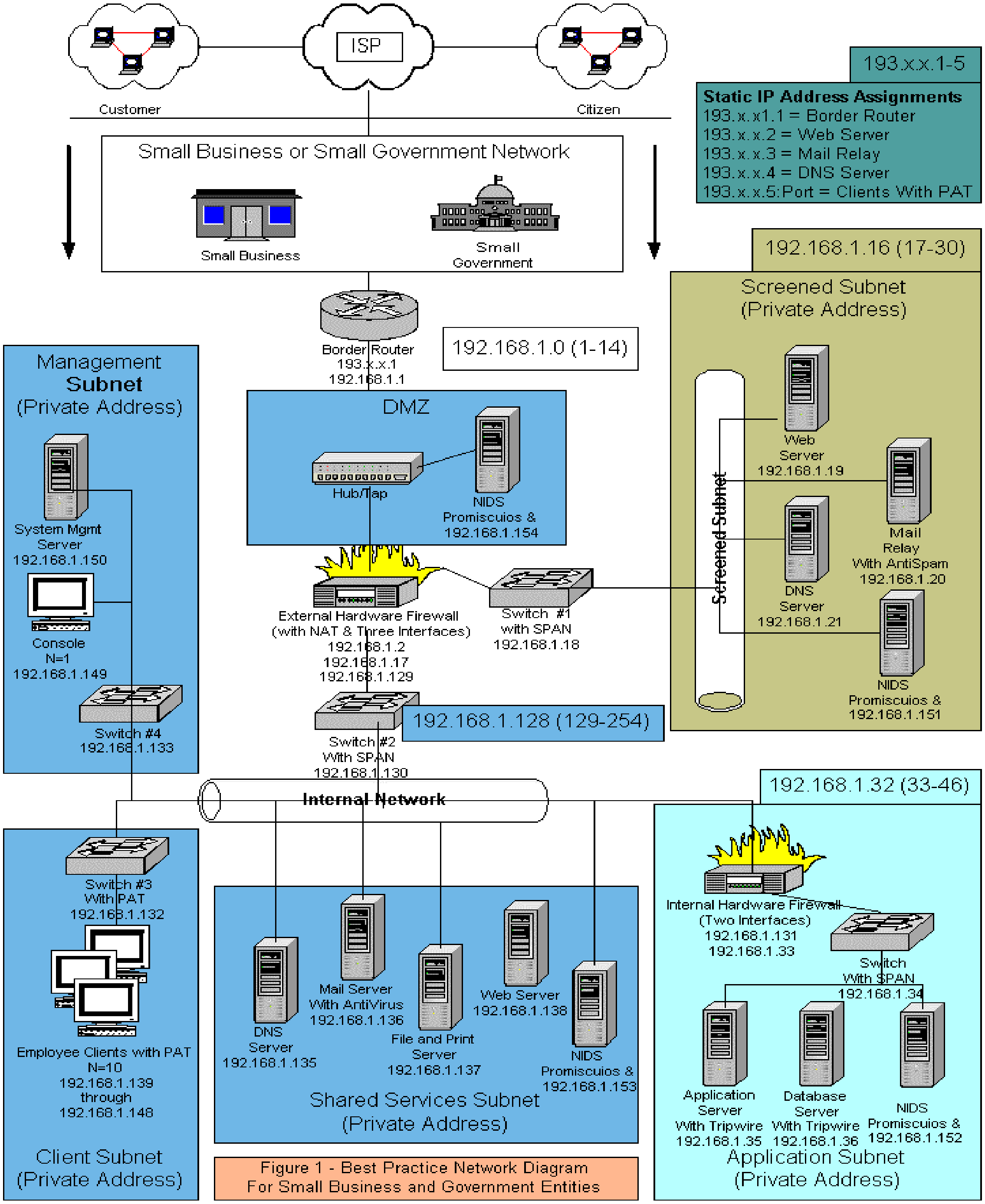
Abstract:

Concerns about network security have never been greater, however most business networks, corporate networks, and government networks continue to be at great risk. This situation is primarily due to the fact that most networks were implemented at a time when security was not a strong business priority. To address this issue, networks must be redesigned with security in mind; and this will not be a trivial task. Network configurations will need to be altered, additional hardware and software will be required, and administration responsibilities will increase. Even in these times of tight budget constraints, it is incumbent upon business and government to address this imperative. Total or partial avoidance of this responsibility is no longer acceptable.

To assist business and government entities in addressing the challenge of protecting their valuable information assets, this paper will analyze an example of a properly designed network, as shown in Figure 1. Best practices, with supporting rationales, will be presented for each network segment. Through the thoughtful and deliberate application of these best practices a secure environment can be established.

Network Diagram:

The network diagram[1], illustrated in Figure 1, depicts a best practice network diagram. Many small businesses and small government agencies should be able to leverage this basic network design to better secure their existing networks. Each major component of this diagram will be discussed at varying levels of detail throughout the remainder of this paper.



ISP
Customer
Citizen
Small Business or Small Government Network
Small Business
Small Government
193.x.x.1-5
Static IP Address Assignments
193.x.x1.1 = Border Router
193.x.x.2 = Web Server
193.x.x.3 = Mail Relay
193.x.x.4 = DNS Server
193.x.x.5:Port = Clients With PAT
192.168.1.16 (17-30)
Screened Subnet (Private Address)
Border Router 193.x.x.1 192.168.1.1
192.168.1.0 (1-14)
Management Subnet (Private Address)
DMZ
Hub/Tap
NIDS Promiscuios & 192.168.1.154
System Mgmt Server 192.168.1.150
Console N=1 192.168.1.149
Web Server 192.168.1.19
Mail Relay With AntiSpam 192.168.1.20
DNS Server 192.168.1.21
NIDS Promiscuios & 192.168.1.151
Screened Subnet
External Hardware Firewall (with NAT & Three Interfaces) 192.168.1.2 192.168.1.17 192.168.1.129
Switch #1 with SPAN 192.168.1.18
Switch #4 192.168.1.133
Switch #2 With SPAN 192.168.1.130
192.168.1.128 (129-254)
Internal Network
192.168.1.32 (33-46)
Switch #3 With PAT 192.168.1.132
Employee Clients with PAT N=10 192.168.1.139 through 192.168.1.148
Client Subnet (Private Address)
DNS Server 192.168.1.135
Mail Server With AntiVirus 192.168.1.136
File and Print Server 192.168.1.137
Web Server 192.168.1.138
NIDS Promiscuios & 192.168.1.153
Shared Services Subnet (Private Address)
Internal Hardware Firewall (Two Interfaces) 192.168.1.131 192.168.1.33
Switch With SPAN 192.168.1.34
Application Server With Tripwire 192.168.1.35
Database Server With Tripwire 192.168.1.36
NIDS Promiscuios & 192.168.1.152
Application Subnet (Private Address)

Figure 1 - Best Practice Network Diagram For Small Business and Government Entities

Client Access:

Customers and citizens will access Internet-based systems through various Internet Service Providers (ISPs). The speed in which they access the Internet will also vary (e.g. dial-in, digital subscribe line, cable, etc). Furthermore, there are many different brands and versions of browser interfaces. It is vital, even in this heterogeneous environment, that the stakeholder have a high degree of confidence that business is being conducted securely. In addition, the stakeholder's privacy should be protected with the same amount of due diligence as is the security of their data.

Business and government entities should publish content that clearly communicates their efforts to secure data and protect the privacy of the stakeholder. Examples include "security seals" which indicate that an entity's web presence has been certified by a trusted third party and privacy statements stating how private data will be handled. Both of these methods are excellent ways to communicate a strong corporate commitment to provide data confidentially and integrity. Use of other less noticeable technologies, such as Secure Sockets Layer (SSL) and encrypted session cookies, also instill stakeholder confidence.

ISP:

Business and government entities procure Internet access through various means. Agreements with local telecommunication companies or with large government agencies (that provide telecommunication services as an intermediary service provider) are classic examples of such arrangements. Transmission speeds vary from low-end connections of 64kbps, to moderate T1 connections, to higher connection speeds of T3, OC3, or even greater. ISPs assign the entity the necessary static public Internet Protocol (IP) addresses to enable business to be conducted with the public. Companies then register these IP addresses to specific domains and define these IP addresses/domains to the appropriate DNS servers. It is not unusual for an ISP to provide border router functionality as a part of this service.

Border Router:

The Internet could not function without routers, in fact high end routers are used to support the backbone of the Internet. Functionally, routers route traffic by using IP addresses. This paper will focus on a particular implementation of routers, referred to as border routers. Border routers are generally considered to constitute the outer most edge of a network perimeter[2]. In some cases, the ISP may manage the border router. In this situation, business and government entities may have to request certain changes be made to the router by the ISP. Border routers are generally considered to be the first line of network defense. Border routers can be required to process a large amount of IP traffic. For this reason, it is a best practice to define a limited set of high level rules in the router's Access Control List (ACL). This method of rule implementation keeps the performance impact to a minimum while at the same time providing an initial filtering point for undesirable or suspicious traffic. The rules in the ACL are applied to the IP traffic as it is routed to the entity's network.

Special care should be taken to ensure that routers are not comprised. To every extent possible, the router ACL should be redundantly defined on interior devices. This redundant definition provides an extra layer of defense in the event that the border router is ever compromised. Administrative passwords should be strong. It is best if administration can be performed locally. If remote administration is required, technologies that provide strong authentication and encryption, such as Secure Shell (SSH) or Simple Network Management Protocol v3 (SNMPv3) should be employed. Use of telnet or earlier versions of SNMPv1 or SNMPv2 should not be allowed, unless occurring through a VPN tunnel. If SNMP community strings are being used, then it is critical that the default string values of "public" and "private" be changed[3]. It is also advisable to block all SNMP traffic from entering the network. This action limits the remote administration of devices via SNMP to just the Internal Network[4]. Ideally, administration should only be allowed from a specific IP address or range of IP addresses. The Management Subnet shown in Figure 1 demonstrates this technique.

DMZ:

A De-Militarized Zone (DMZ) is generally defined as an uncontrolled zone between controlled zones[5]. This term is commonly used by the military. For example, prior to the start of Operation Iraqi Freedom, the military established a DMZ at the border between Iraq and Kuwait. Entering this zone, whether by military or civilian means, would have been risky, since no one controlled this area, and the safety of anyone who entered it cannot be guaranteed. The same is true for the DMZ defined in IT networks. In the past, the term DMZ has been misused within the IT industry. More recently, the IT community has more accurately defined the DMZ as the area between the border router and the external firewall. This is clearly demonstrated in Figure 1.

Due to the fact that DMZs are inherently insecure, only disposable or quickly recoverable and hardened devices/hosts should be located in a DMZ. A conceptual example of this would be remote controlled robots that are used for bomb detection and disposal. It is important to note that devices may not be "cheap" but if necessary, are disposal just the same. In Figure 1, the DMZ contains a hub or tap communicating with a Network Intrusion Detection System running on a hardened host.

NIDS:

Network Intrusion Detection Systems (NIDS) function similar to an activated security alarm system that watches for known behaviors (signatures), which indicate suspicious activity and even system break-ins. NIDS is a critical component for any secure network architecture; providing a key extra layer of defense to a properly designed network. NIDS is typically deployed in strategic locations in the network, with one obvious location being the DMZ. A NIDS sensor in the DMZ has the ability to see all traffic before it enters the firewall. The sensor should be the least sensitive and most active of all the NIDS implementations in a network. For this reason, the sensor in the DMZ will likely be the most active and will report the most false alarms[6].

Network-based IDS excels in certain analytical areas and offers particular strengths that other forms of IDS (i.e. Host and Stack) do not offer. Specifically, economies-of-scale can be provided, due to the fact that a small number of NIDS sensors can analyze traffic for an entire network, while at the same time keep software and administration requirements to minimum. The real time analysis of packets facilitates the detection of malicious or suspicious traffic for both full and fragmented IP traffic. Packet payloads can be analyzed for specific attack signatures. In addition, real time detection greatly inhibits the ability of a hacker to cover their tracks and by its very nature enables a real time response to neutralize an attack as soon as it is detected. Other benefits include security policy verification and validation; and operating system independence (i.e. NIDS it is not dependent on Operating System (OS) logs that could be altered)[7].

Commercial-off-the-Shelf (COTS) NIDS software can be expensive. On the other hand, many NIDS products are freely available. While COTS software does add additional cost, the benefits can be well worth the investment. The value added by commercial products includes sophisticated end-to-end analysis and consolidated reporting functionality. The obvious advantage of such software is at a minimum twofold. First, network attacks can be actively monitored and proactive measures can be taken to protect against intended as well as unintended malicious damage. Second, it should take less staff resources to review and respond to well-designed reporting facilities. With that said, if a business or government entity is operating on a shoestring budget then open source/freeware versions of NIDS software is a viable option. The advantages of this solution is that initial costs are minimal, it forces staff to become intimate with the technology, and later when budgets include money for commercial NIDS, then a more knowledgeable evaluation, selection, and implementation can occur.

The typical NIDS sensor has two Network Interface Cards (NICs), as shown in Figure 1. One NIC has a specific IP address assigned and the other NIC runs in promiscuous mode (without an IP address assigned). All traffic passes through the sensor and a first level filter determines which traffic will be discarded. The remaining traffic is sent to an attack recognition module that scans the IP traffic for suspicious traffic using anomaly, pattern, or frequency techniques. A NIDS sensor is usually connected to a hub, tap, or Switch Port Analyzer (SPAN). A hub arrangement is very economical and the easiest and least complicated to configure. The primary weakness of this design is that hubs can fail during times of high volume traffic. Taps are a more expensive solution, however they provide for fault tolerance. They also scale very well because they provide the ability to monitor multiple ports without adding additional network overhead. Like hubs, SPAN configurations are relatively straight forward to install and management requires no extra hardware. The primary disadvantage of SPAN is that there can only be one span port per switch[8].

Firewall:

Firewalls are used to deny or allow IP traffic from entering a network. Just as was the case with the DMZ, use of this terminology leaves something to be desired. In the construction industry a firewall is a solid wall (usually concrete) that separates physical infrastructure. The two primary purposes of a firewall are to stabilize the building and to slow the spread of a fast moving fire. In the construction industry firewalls would almost never have “holes” that allow “controlled access”. In the IT industry firewalls serve a similar purpose, which is to stabilize infrastructure and limit undesired or potential damaging IP traffic. However, IT firewalls must allow controlled access; therefore the purpose of a firewall is not the same as it is in construction industry. IT firewalls are really “door keepers” that allow access as defined by rules in an ACL. Firewalls rules are never perfect, and cannot always determine if incoming traffic is dangerous. Therefore, other support mechanisms will be needed to deal with this issue.

There are three primary types of firewalls; they are packet filtering, stateful packet inspection, and proxy. This paper will only discuss the first two types (i.e. packet filtering and stateful packet filtering). Packet filtering firewalls are considered “dumb” firewalls, meaning that conditions over time are not considered and rules are applied based on a limited set of information. Stateful packet filtering firewalls are “intelligent”, meaning that the state of the traffic can be analyzed. Stateful firewalls include the software necessary to remember state and determine if incoming or outgoing traffic is legitimate based on a previous flow of traffic.

For small entities, firewalls should generally have two or three interfaces. In Figure 1 the external firewall has three interfaces and the internal firewall (in the Application Subnet) has only two interfaces. Firewalls with more than three interfaces are can be complicated to administer and could introduce security holes if administered incorrectly[9]. One practical example of a firewall with four interfaces would be when an additional publicly addressable screened subnet is required for protocols that cannot be tunneled, such as a VPN utilizing IPSEC. In this scenario one interface would be for the public interface, one for the publicly addressed DMZ, one for the privately addressed DMZ, and one for the Internal Network[10].

VLANS:

Virtual Local Area Networks (VLANs) separate a physical LAN into logical components. This enables the network administrator to establish virtual LANs that reflect the needs and geographical characteristics of the business. VLANs isolate network traffic and therefore improve network performance. VLANs also offer the additional benefit of logical network separation, which has obvious security related advantages. However logical network separation is still not as good as physical separation. Therefore, while the use of VLANs is an acceptable practice, it should not be a cornerstone of any security strategy[11].

Switches:

A switch is the basic network device that connects hosts (servers, workstations, etc) to the network. The switch receives network traffic from devices such as routers, firewalls, and other switches and passes it to the appropriate network host, based on a Machine Address Control (MAC address). Each host device has a unique MAC address, as well as a unique TCP/IP number assigned. The primary functional difference between the IP address and the MAC address is that the MAC address is permanently assigned to the host, while the TCP/IP address can change over time. These two pieces of information when combined together create a unique digital address unlike any other in the world.

Screened Subnet:

Screened Subnets are physical network segments designated to host only servers that need to allow access to and from the Internet. The screened subnet is where information technology assets such as Internet accessible web servers are hosted. This is because, while not totally secure, servers in the Screened Subnet can be secured to an adequate level to conduct business with an acceptable amount of risk. Access requests can originate from external sources such as customers or citizens, as well as from the staff located on the Internal Network. This subnet will utilize one of the three network interfaces on the external firewall. The Screened Subnet shown in Figure 1 hosts a Domain Name System (DNS) Server, Mail Server, Web Server, and Network IDS sensor.

Static IP addresses are assigned to the Web Server, Mail Server, and DNS Server, as shown in Figure 1. The necessary domain registration and DNS entries have to be made so that the client can access the servers via the Internet. The firewall will be configured such that these valid IP address are translated into the appropriate private address using Network Address Translation (NAT)[12].

Web Server (Internet):

In most cases, the Internet accessible Web Server should only have port 80 and 443 listening. It may be necessary to allow port 20 and 21 to be listening for File Transfer Protocol (FTP). However, it is absolutely critical that no unnecessary ports be open or services be started on the Web Server. Furthermore, only pre-defined and well-trusted services/ports should be allowed through the external firewall to the Application and Database Servers. Server administration of the OS should be performed locally if possible; otherwise use of remote control software may be necessary, but should only be allowed from the Management Subnet.

Mail Relay Server:

An extra level of protection can be introduced into the network design by placing a Mail Relay into the Screened Subnet. This server acts as an intermediary and receives SMTP traffic from both the Internet and the Internal Network; it then forwards the traffic to the appropriate destination. The firewall should allow SMTP traffic to flow in and out of the Screened Subnet. It should also allow traffic to flow from the Mail Relay to the Internal Mail Server and visa versa. The addition of a Mail Relay enables the mail to be sent and received from the Internet while at the same time placing the critical email messages (corporate assets) in the Shared Services Subnet[13]. This server should also host antispam software to eliminate bulk unsolicited email from entering the network.

DNS Server:

The same principle that applied to Mail Server separation applies to DNS Server separation. Through the creation of a Split DNS configuration, sensitive DNS information can be placed in the Shared Services Subnet, while public DNS information will be located in the Screened Subnet. The configuration can be established such that internal clients needing DNS information from the Internet can be provided the necessary information from the DNS Server in the Screened Subnet. To further safeguard the information stored on this server, DNS Zone Transfers should not be allowed[14].

NIDS:

NIDS in the Screened Subnet should be less sensitive than in the DMZ. The traffic that this sensor will analyze has already passed through the firewall. Knowing this enables the network administrator to adjust the sensor accordingly[15]. The Network IDS in this subnet is attached to a switch with the Switch Port Analyzer (SPAN) feature. The feature enables a switch to artificially copy unicast packets to a destination port that can be sniffed by a network adapter that is functioning in promiscuous mode. In other words, this feature enables a switch to act like a hub, in that the switch can see the unicast traffic for multiple ports even though once the switch has learned the MAC address for a particular device that traffic is no longer broadcast or multicast to the other ports in the switch[16]. In this case, the SPAN would be defined to monitor ingress and egress packets for the Web, Mail, and DNS servers. The sniffer (e.g. Snort, RealSecure Network Protection, etc) would then replicate any suspicious traffic to the System Management Server in the Management Subnet for further analysis and possible corrective or defensive action.

Shared Services Subnet:

The Shared Services Subnet should only be accessible by hosts that are physically attached to the Internal Network or by specific servers in the Screened Subnet. The only notable exception to this would be remote access connections via a VPN connection to the Internal Network by an authenticated and authorized telecommuter or mobile worker. Some companies, such as CISCO, build VPN solutions into their firewall products. Use of VPN technologies is beyond the scope of this paper. The internal DNS, Mail, Web, and File and Print Servers usually are the heart of this network segment. The network diagram shown in Figure 1 includes a NIDS with a SPAN configuration in this segment to protect these key services.

Mail Server:

The Internal Mail Server receives mail from the internal mail clients as well as from the Mail Relay in the Screened Subnet. The Mail Server is often a robust mail oriented software product such as Microsoft Exchange or IBM Lotus Notes/Domino. Other mail server solutions could be lighter weight products (i.e. Sendmail). In any event, the key point here is that critical mail messages are being stored behind the external firewall and is therefore much more protected from attack. It would also be a best practice to have antivirus software installed and running on the server to protect the server from viruses.

DNS Server:

As was previously discussed in the Screened Subnet, the DNS Server installed in the Shared Services Subnet contains the DNS related information for critical Application, Database, and Infrastructure Servers. It is critical that this information not be readily available via the Internet. Leakage or exposure of this sensitive information could be extremely beneficial to a hacker that is footprinting a network prior to attack[17]. Just as was the case in for the DNS Server in the Screened Subnet, DNS Zone Transfers should not be allowed from this server either.

Web Server (Intranet):

The internal Web Server performs Intranet related tasks and should not be accessible by the Internet. All unnecessary ports and services should be closed and server hardening should be performed. User and administrative passwords should be strong. It is very likely that this server will need to communicate with Application and Database Servers in the Application Subnet. Operating System administration should be performed locally or via the Management Subnet.

File and Print:

Critical File and Print servers should also be located in the Shared Services Subnet and not available via the Internet. File servers obviously would contain critical corporate data assets such as patent information, corporate strategy documents, corporate financial statements, etc. Print servers can also be easily exploited. It is not unusual for the server to be operating an obsolete version of an OS due to specific hardware or business requirements. It is entirely possible that even a network printer could be hacked and used to store undesirable graphic images on large disk drives that often go unused on network printers.

NIDS:

Network IDS sensors in the Shared Services Subnet should be very sensitive and alarms that occur in this subnet should be considered hostile until proven otherwise. False alarms in this zone should be limited, and response to any alarms should be immediate and strongly focused[18].

Application Subnet:

The Application Subnet is where some of the most valuable assets (business logic and data) are located. In the case of business, the theft of application business logic or application data could jeopardize valuable trade secrets, potentially compromising competitive advantage or exposing its customers to potential crime such as credit card and/or identity theft. For governments, loss of data could expose a citizen's sensitive financial or medical related information. In both cases, the loss of trust by the customer or citizen is a certainty. In addition, the customer or citizen may take legal action and seek remedies for any damages that may have occurred.

Data theft is just one of the many different ways that damage could be inflected. Another example is malicious software or "malware", which exists in many forms (viruses, worms, trojans, etc) that can inflect serious damage to the physical infrastructure. Any such damage often requires extensive effort to recover. It is not uncommon for the effected servers to be rebuilt (perhaps from a ghost or even from scratch) and the data to be reloaded from a stable backup.

For the reasons stated above, the Application Subnet should be one of the most protected network segments. In Figure 1, notice that the segment is physically separated from the Internal Network by an additional internal firewall. This additional segmentation provides an extra layer of defense against attacks on critical business assets. Once again, Operating System administration should be performed locally or via the Management Subnet.

Application Server:

The firewall rule set should only allow IP traffic from a specific Web Server in the Screened Subnet to access the Application Server in the Application Subnet. Application Servers should also be protected through the use of Host IDS software (e.g. Tripwire, RealSecure Server Sensor, etc) to determine if unauthorized changes have occurred or suspicious network activity is targeting a specific host. Application code (business rules) must be written securely and should not be susceptible to common hack attempts such as buffer overflows and SQL Injection[19]. Database access via the application should be performed using industry proven techniques. Application code should not store unencrypted passwords within code designed to perform database access. Remote administration of the Application Server should only be allowed from the Management Subnet. Strict control measures for moving code into production should be established and followed.

Database Server:

Database Servers should be one of the most protected servers in the enterprise. Great care should be taken to log all changes to production data. Userids with the privileges to perform select, insert, update, and delete should be role-based and kept to a minimum. Password policies should be strong and strictly followed. If it is determined that a database was hacked or exposed, the immediate question is "what data did the hacker have access to, and was the data stolen or corrupted?". To help answer this question, database auditing mechanisms must be enabled. A unique feature within Oracle 9i, called Flashback Query, offers the ability to actually determine the state of the data at a specific point in time[20]. Database features such as these are exactly what is needed to assist system and database administrators in determining how invasive a particular incident may have been. There must be an understanding that the audit records themselves may have been manipulated in an attempt to cover a hacker's activity. Absolutely, under no circumstances should users be allowed to access or update the database directly without utilizing the application's front-end. Solid backup and recovery processes are essential. It is critical that backups be validated routinely and that adequate storage times are established so that databases can be recovered in the event of an incident. Backups must be physically secured, so that they themselves are not stolen. The use of Host IDS technologies on the database server is also considered a security best practice.

NIDS:

Network IDS sensors in the Application Subnet are implemented just as they are in the Shared Services Subnet and the sensors in the subnet will be just as sensitive and alerts should be taken very seriously; even more seriously than they were in the other subnets.

Management Subnet:

The Management Subnet is an area that many entities do not currently have defined. This however is a very important subnet which should be created, used to host the Network IDS System Management Server, as well as remotely administer others hosts and devices across the network from a single console. Administration should be performed by tools that provide secure transmission of the userid and password when performing authentication of the administrator. Through the establishment of a Management Subnet, ACLs can be defined on the appropriate devices (e.g. firewalls, switches, and hosts) that deny administration access by any device that is not defined to the Management Subnet.

System Management Server:

The System Management Server serves as central repository of information for all of the remote NIDS within the network. Often times this server would have a database, such as MySQL (which is a popular open source relational database engine) installed on it, providing sophisticated analysis and reporting functions. This additional functionality greatly simplifies the need for grueling manual analysis of information.

Console:

The console is obviously used for remote administration of device or hosts (i.e. servers) in the other various subnets. Ideally SSH or Telnet (through a VPN) would be used for the remote administration of network devices. If local administration of servers is not feasible, then remote control software could be used from this workstation. Web Server administration via https is another function that could be performed from this workstation. Physical access to this device would need to be tightly controlled. The normal safety precautions, such as network login, activation of a password protected screen saver, and perhaps even a BIOS password could be used for an extra layer of protection.

Client Subnet:

To minimize the number of valid IP addresses required to provide the network clients with access to the Internet, Port Address Translation (PAT) should be utilized. This can done very easily by assigning each client a non routable private address (as shown in Figure 1) and then making the necessary configurations in the firewall to assign egress traffic the routable address of 193.x.x.5 plus a unique port number[21].

Extra defense measures can also be taken to further secure the internal clients. Additional measures should include the installation of a client based personal firewall, virus protection software, and local data encryption of sensitive data. Use of technology in this manner provides an additional layer of client protection from any probes or malware that may slip through network protection defenses. These defenses also may protect internal clients from their own misguided actions. In other words, it is not unusual for internal clients to violate policy and as a result become vulnerable to attack. Examples of such actions include use instant messaging or installation and use of external modems. Additional physical measures that should be taken include safety locks to protect against physical theft of laptops and regularly backing up any corporate data that is stored locally on a desktop or laptop.

References:

[1] Northcutt, Stephen. Zeltser, Lenny. Winters, Scott. Frederick, Karen Kent. Ritchey, Ronald W. Inside Network Perimeter Security. Indianapolis: New Riders Publishing, 2003. 7.

[2] Northcutt, Stephen. Zeltser, Lenny. Winters, Scott. Frederick, Karen Kent. Ritchey, Ronald W. Inside Network Perimeter Security. Indianapolis: New Riders Publishing, 2003. 4 – 5.

[3] Northcutt, Stephen. Zeltser, Lenny. Winters, Scott. Frederick, Karen Kent. Ritchey, Ronald W. Inside Network Perimeter Security. Indianapolis: New Riders Publishing, 2003. 244 - 245.

[4] Northcutt, Stephen. Zeltser, Lenny. Winters, Scott. Frederick, Karen Kent. Ritchey, Ronald W. Inside Network Perimeter Security. Indianapolis: New Riders Publishing, 2003. 149.

[5] Northcutt, Stephen. Zeltser, Lenny. Winters, Scott. Frederick, Karen Kent. Ritchey, Ronald W. Inside Network Perimeter Security. Indianapolis: New Riders Publishing, 2003. 6.

[6] Sanchez CISSP, Scott C. "IDS Zone Theory Diagram." 28 July 2000. URL: http://infosec.gungadin.com/papers/scott_c_sanchez_cissp-ids-zone-theory-diagram.pdf (4 March 2003).

[7] Laing, Brian. Alderson, Jimmy. "How to Guide-Implementing a Network Based Intrusion Detection System." 2000. URL: http://www.snort.org/docs/iss-placement.pdf (4 March 2003).

[8] Laing, Brian. Alderson, Jimmy. "How to Guide-Implementing a Network Based Intrusion Detection System." 2000. URL: http://www.snort.org/docs/iss-placement.pdf (4 March 2003).

[9] Komar, Brian. Beekelaar, Ronald. Wettern PhD, Joern. Firewalls for Dummies. New York: Hungry Minds, Inc, 2001. 201 – 202.

[10] Komar, Brian. Beekelaar, Ronald. Wettern PhD, Joern. Firewalls for Dummies. New York: Hungry Minds, Inc, 2001. 204.

[11] Northcutt, Stephen. Zeltser, Lenny. Winters, Scott. Frederick, Karen Kent. Ritchey, Ronald W. Inside Network Perimeter Security. Indianapolis: New Riders Publishing, 2003. 350.

[12] "Using NAT and PAT Statements on the Cisco Secure PIX Firewall." URL: http://www.cisco.com/warp/public/110/19.html (21 March 2003)

[13] Northcutt, Stephen. Zeltser, Lenny. Winters, Scott. Frederick, Karen Kent. Ritchey, Ronald W. Inside Network Perimeter Security. Indianapolis: New Riders Publishing, 2003. 333 - 334.

[14] Northcutt, Stephen. Zeltser, Lenny. Winters, Scott. Frederick, Karen Kent. Ritchey, Ronald W. Inside Network Perimeter Security. Indianapolis: New Riders Publishing, 2003. 338 – 339

[15] Sanchez CISSP, Scott C. "IDS Zone Theory Diagram." 28 July 2000. URL: http://infosec.gungadin.com/papers/scott_c_sanchez_cissp-ids-zone-theory-diagram.pdf (4 March 2003).

[16] "Configuring the Catalyst Switched Port Analyzer (SPAN) Feature."
URL: http://www.cisco.com/warp/public/473/41.html#desc (21 March 2003)

[17] Scambray, Joel. McClure, Stuart. Kurtz, George. Hacking Exposed Network Security Secrets and Solutions Second Edition. Berkeley: Osborne/McGraw-Hill, 2001. 27.

[18] Sanchez CISSP, Scott C. "IDS Zone Theory Diagram." 28 July 2000.
URL: http://infosec.gungadin.com/papers/scott_c_sanchez_cissp-ids-zone-theory-diagram.pdf (4 March 2003).

[19] Dyck, Timothy. "OpenHack Wrap." 2003.
URL: http://www.eweek.com/article2/0,3959,743411,00.asp (3 March 2003)

[20] "Oracle 9i Flashback Query." 2002.
URL: http://otn.oracle.com/products/oracle9i/daily/Aug13.html (26 March 2003)

[21] Using NAT and PAT Statements on the Cisco Secure PIX Firewall."
URL: http://www.cisco.com/warp/public/110/19.html (21 March 2003)