Global Information Assurance Certification Paper

Extranet: Belt, Suspenders, Elastic WaistBand, and Double Sticky Tape.

Timothy Frost
November 17, 2000

First things first:
There are many definitions of an Extranet verses a DMZ. My purpose is not to present arguments as to what it is and what it is not. So, for purposes of this paper I will use the following definitions:
Intranet: Intranets are internal systems based on Internet technology, designed to connect member of a specific group or single company. A Firewall or other protection system typically protects an Intranet from the world assessable (public) Internet.

Extranet: An Extranet is a private network that uses the Internet protocol and the public telecommunication system, and or Internet to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An Extranet can be viewed as part of a company's Intranet that is extended to users outside the company. It has also been described as a "state of mind" in which the Internet is perceived as a way to do business with other companies as well as to sell products to customers.

The Picture

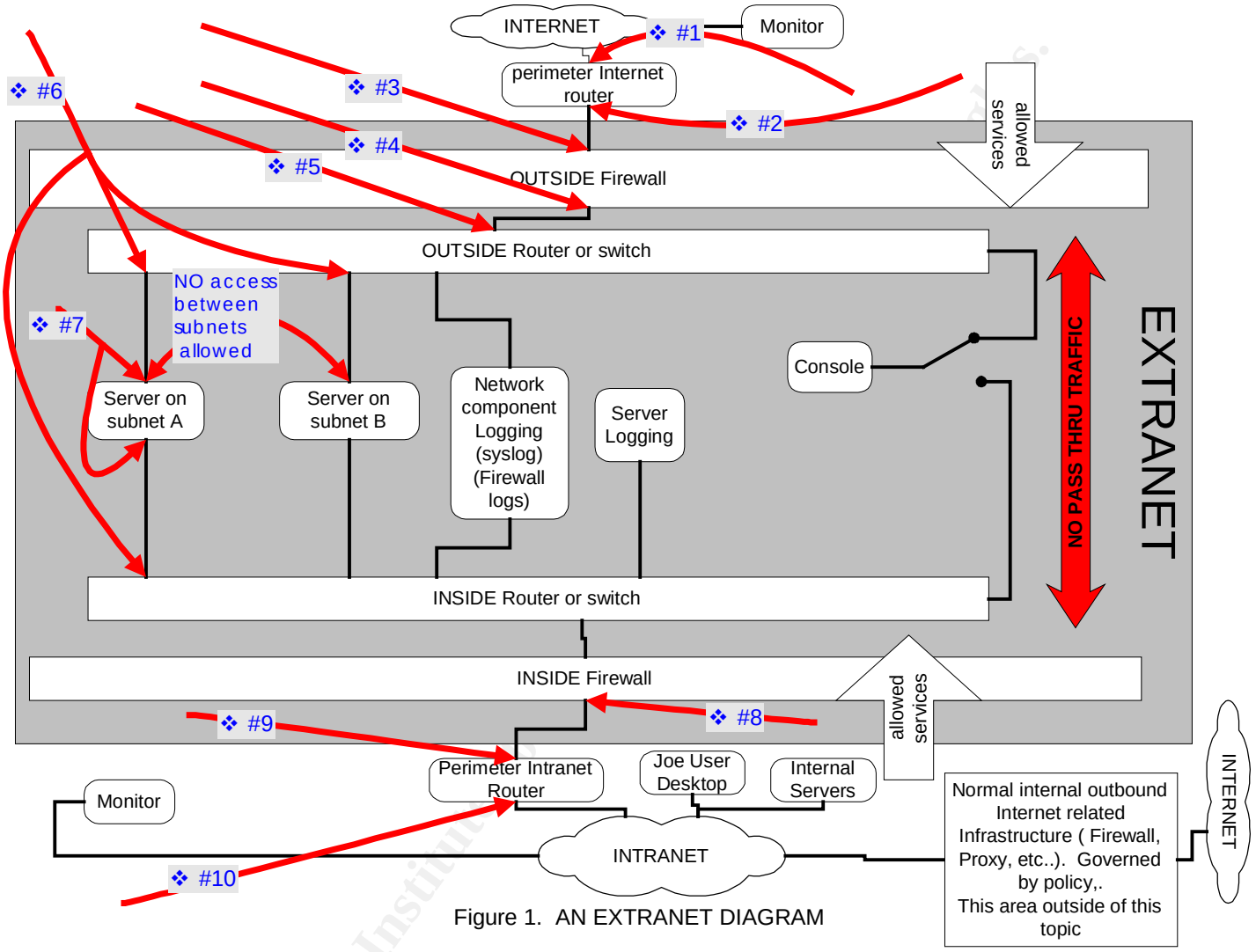

Figure 1. AN EXTRANET DIAGRAM

Is it The Design? Or is it A Fashion Statement?

The two main things that should drive the design are a "Defense in Depth" way of thinking, which will drive your second thing; your Extranet policy. These two must be established before the design may begin. Many things will drive the design of the Extranet. These things will vary greatly depending on the objectives you are seeking. If you do not think with a "Defense in Depth" mentality from beginning to end, your design will eventually demonstrate its weakness.

Once your design phase is underway, these are some of the tried and true philosophies that can be used.

Divide and Conquer. Separate projects and functions. Keep procurement separate from marketing. Product demo's separate from production deliverables. Proposals separate from project collaboration. And so on. When I say separate I mean literally separate hosts. Too many

times we say, “But I can run all three Web sites on the same box”. This will eventually come back to bite you. You may have to run other services on the host that are not required by the first two applications. You may have to open ports on the same box that are not needed by all the applications, thereby increasing your vulnerability to exploit and just plain more things to go wrong.

Keep it simple. Try to use single function hosts. Such as, one box that does nothing but system monitoring, one to collects logs, one host to provide console access to network hardware. This will make troubleshooting easier and faster. It will also reduce risk by not having services running that are not needed to perform the desired function of that particular host.

Know what is running on your hosts. Examine all services that are running on all components, routers, switches, and servers. Routers and switches run default services like SNMP, Telnet, WEB, and so on. You have to always ask your self “Do I need this service.” If the answer is no, then shut it off. If you cannot shut it off then you may be able to block or restrict access to the service. The preferred answer is to shut off the service. This reduces the chance that the service could be exploited via a side door. The same holds true for servers. In Figure 1 (#7) by using a dual homed bastion host you can bind only the services to the NIC that are required the service. Example, SSL (tcp port 443) could be bound to both the outside and the inside interface, but you may want NBSESSION bound only to the inside interface of the server. Can an outside transaction cause an internal reaction?

Layered defenses. The first principle to apply for layered defenses is the “ Principle of Least Privilege.”

Starting with Fig. 1 (#1 and #2), use both inbound and outbound filters on both interfaces. By using Access Control Lists (ACLS) on the first interface to the Internet, permit only the protocols that are permitted by your policy. Such as, Inbound HTTP, and SSL. Permit these protocols only to specific hosts. On the outbound filter of (#1) you would again permit only that which is allowed by policy. Such as, return established, DNS query, outbound SMTP, then deny everything else. Use static host routes to only the hosts that exist. Explicitly deny all ip from RFC 1918 private address space.

Again, do not run remote administration services like SNMP, WEB, or TELNET service on your border router unless you absolutely have to.

Fig. 1 (#3 and #4). For this Extranet an application layer proxy Firewall will be used. Debating the merits of a Proxy versus statefull inspection firewall is not within the scope of this paper. A proxy Firewall will be used for more control over the application layer than a statefull inspection Firewall typically will give you. Use static routes for inside hosts. Use host to host rules whenever possible. Examine both interfaces to make sure you know what ports are listening and why. Remove any unknown ports or services.

Fig. 1 (#5). In this case by using a proxy Firewall the only IP address that should be allowed on this inbound ACL should be the inside address of the Firewall. On the outbound ACL you should only permit known Extranet hosts that need to reply to the Firewall.

Fig. 1 (#6). These interfaces should not allow any traffic to go anywhere except the Firewall. Permit only the protocols and host IP addresses that are required. This will help to minimize the risk that Server on subnet A could be used to obtain access to the Server on subnet B.

Fig. 1 (#7). The servers should only have those services that are required to perform the desired function. In additional to the ACLS on #6, the servers themselves should not have a

default gateway set. You should be able to configure them with static routes only because you are using a proxy Firewall. Routing should be turned off to prevent the forwarding of packets from one side to the other. Virus scanning software should be running at all times. Tripwire may also used to insure integrity of the critical files on the servers.

Fig. 1 (#8). This firewall is the most important Firewall from the aspect of protecting you Intranet resources. You need to be very careful if you allow ANY transactions to be initiated from within the Extranet that would be destined for your Intranet. A recommendation would be to allow only one directional transactions. If data needs to be replicated, backed up, retrieved from the Extranet into the Intranet, then the transactions should be initiated from an Intranet host. This minimizes the risk of allowing an outside world (Internet) transaction from causing an inside world (Intranet) event.

Fig. 1 (#9 and #10) Inbound and outbound ACLS should be used on both interfaces using the "Principle of least Privilege." You should be able to use almost all the same rules as used for the perimeter router.

How to get Dressed

Implementation and construction should be done as much as possible without connecting to the Internet until construction is complete and tested for functionality. The whole Extranet should be able to be constructed and tested "off-line." Look carefully in all logs to see if any packets are hitting ACLS. This will help you verify that you have hardened your hosts the way you think you have. A very detailed documentation process is key to a successful implementation. Data flow, hardware connection, and overview drawings will prove to be invaluable for the entire life of the Extranet.

Look in the Mirror

Test and re-test your policy implementation. Use tools like NMAP, ISS, and SAINT, to try and penetrate your defenses. Make sure that all components are at their respective current patch releases. Test your WEB server applications for logic errors using a tool like ACHILLES.

Are you being true to the "way of thinking" or are you constantly compromising your policies for convenience.

Monitor your systems with something like "WhatsUp Gold". Be careful not to compromise your policy just to do monitoring. Add monitor points if needed.

Your clothes look great, but can you walk.

The Extranet described so far will have some limitations, scaleability issues, and day to day administration. If you have the ability to do "host to host" or " network to host" or "proxy to host" filtering at your firewall, you will be mitigating a lot of risk. However, this will take diligence, research, and ongoing maintenance. You may be fortunate enough to have a limited scope audience that would allow you to achieve this component of the "Principle of Least Privilege."

If your audience must be the "World" then you should spend extra time and effort to harden your applications. This is not to say that you should not spend the time anyway.

One advantage to the single function host and subnets, is that you will be able to mix the access types. World versus limited scope.

Conclusion: The art of not letting your pants fall down.

Building an Extranet from a security perspective is a “Way of Thinking” as much as it is following the “Best Practice” methods.
The Belt = First line of defense (perimeter Internet router)
The Suspenders = The Firewall.
The Elastic Waistband = The core router and or switch.
The Double Sticky tape = Host based security and application security.

REFRENCES

Definition Extranet
http://www.whatis.com/WhatIs_Definition_Page/0,4152,212089,00.html

Overview of Extranet Standards
http://sitesearch.netscape.com/products/whitepaper/extranetstds.html

White Paper
Building a Perimeter Security Solution
with the Cisco Secure Integrated Software
http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/tech/firew_wp.htm

White Paper
SAFE: A Security Blueprint for
Enterprise Networks
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

Department of the Navy
Information Technology Standards Guidance
http://www.doncio.navy.mil/training/ools/itsg/index.html
http://www.doncio.navy.mil/training/ools/itsg/chapter3.html

RFC 1918
http://www.ietf.org/rfc/rfc1918.txt

Michael Wilson
Defense-In-Depth: Design Notes
http://www.7pillars.com/papers/didfinal.htm

The Information Architecture (IA) Project at Lawrence Livermore
Statement of Direction
IA-0401: Unclassified Computer and Network Security Architecture
http://www.llnl.gov/projects/ia/standards/ia0401/ia0401.html#Current-State

SANS Institute NS2000 Monterey, California. Track 1:“Security Essentials Curriculum”
http://www.sans.org

Chuck Semeria, Internet Firewalls and Security
http://www.itmweb.com/essay534.htm

Application Gateways and Statefull Inspection:
A Brief Note Comparing and Contrasting
Revised: 1/22/98
Avolio and Blask, Trusted Information System, Inc.
http://www.avolio.com/apgw+spf.html

Principle of Least Privilege
http://hissa.ncsl.nist.gov/rbac/paper/node5.html