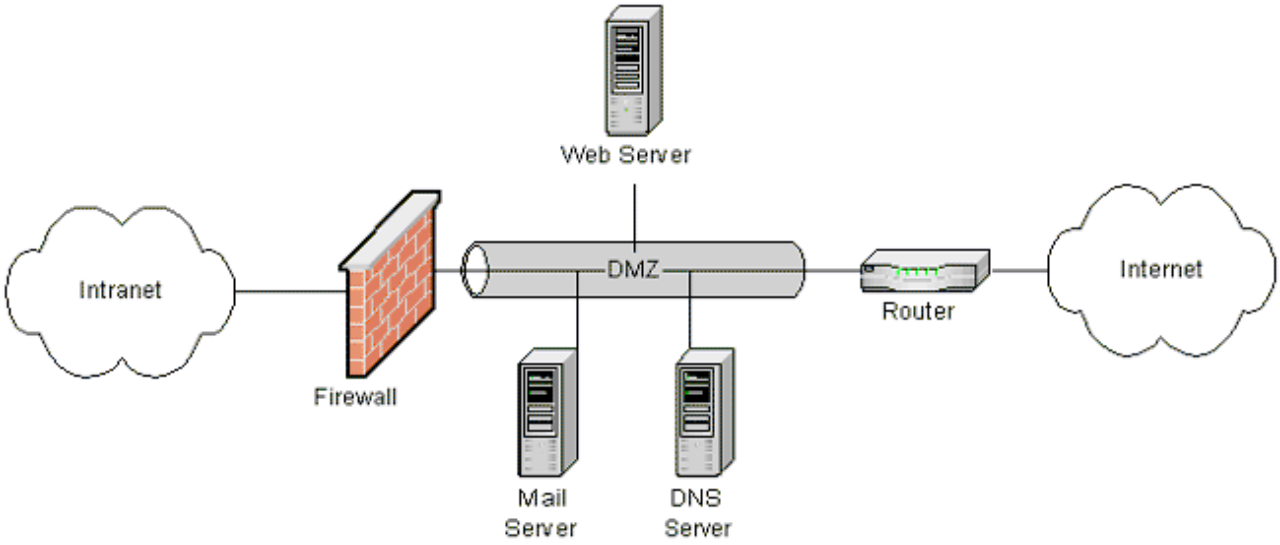
Global Information Assurance Certification Paper

Network Security by Design
Chris Stanley
October 9, 2000

Designing a secure computer network is no longer a simple matter of installing a firewall between the Internet-router and the corporate network, with the corporate website in between. While this classic approach is still widely used, it opens the corporation to a wide variety of security problems, both internally, on the corporate “intranet” and externally, on the “DMZ – demilitarized zone”.

Figure 1 - Classic DMZ



The Outside Problem

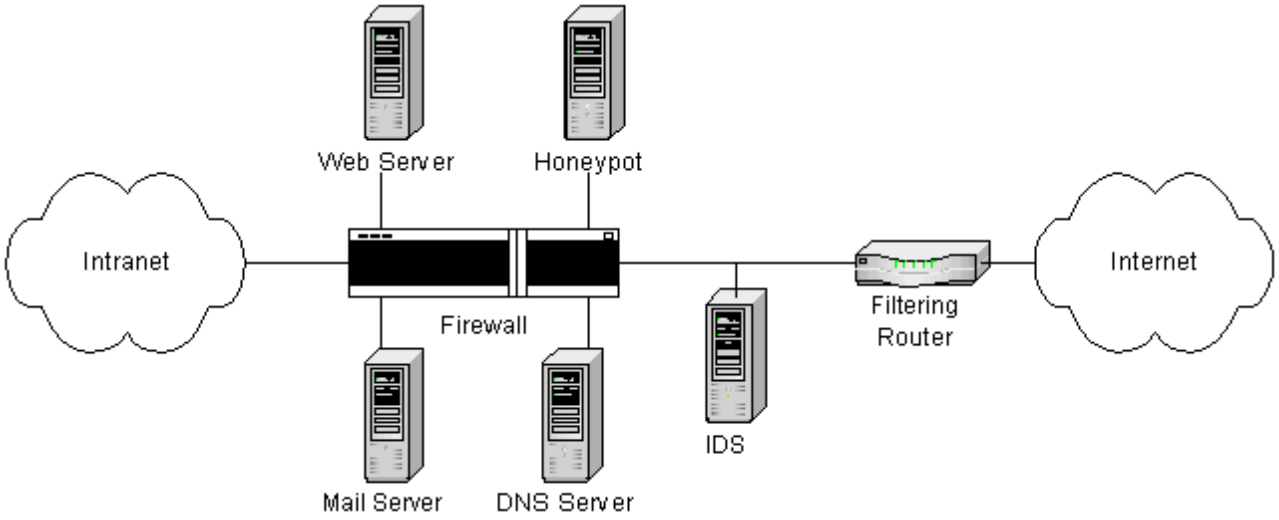
The most discussed problems with the classic DMZ model, and the easiest problems to fix, involve the lack of protection this provides to the DMZ servers. Organizations, including SANS, have done a tremendous job over the last several years to raise awareness to this issue.[1]

The most common solution is to strengthen the perimeter router, which separates the DMZ from the Internet. Some similar, stronger, implementations place the DMZ components behind a third firewall interfaces. The addition of network-based intrusion detection systems and possibly honeypots can strengthen the DMZ protections even further.[2]

Some strong honeypot implementations will further use the firewall to redirect port-specific traffic to the honeypot while still directing authorized traffic to the real application server. For example, attempts to telnet to the corporate web server may be directed to the honeypot, while web requests are sent as expected to the web server.

The advent of faster, multiple interface firewalls introduces new options to further restrict security. Installing each Internet-accessible device behind its own firewall interface. In this structure, a breach on one device will not, in and of itself, pose risk to the other “DMZ” devices.

Figure 2 - Contemporary DMZ



When combined with screening firewalls and/or network and/or host-based intrusion detection systems that screen out and eliminate attack patterns, the external network can be made quite secure.

The Partner Problem

Working inside from the DMZ, securing links to extranet business partners and across the corporate WAN need to be addressed. While distinct issues, there are some common solutions.[3] Modern availability of ATM and gateway-to-gateway VPN solutions are among the more recent improvements.[4] These technologies can be easily leveraged to provide scalable, secure remote connectivity.

Of course, the individual LAN networks connected across the WAN can be secured using the same methods as the rest of the corporate internal network, with broader services provided as needed.

Agreements with extranet partners related to LAN configuration and/or service restrictions help to secure the end of the link controlled by the partner.

The Remote Access Problem

Corporate competition requires computing outside the typical work environment, such as homes and hotels. Typically, remote access is either provided directly into the internal network via remote access (RAS) devices or internal information is made available via the Internet. The amount and/or types of resources needed by corporate users determine the approach. Further, the more access that is required the stronger the authentication scheme typically required.

For example, for organizations that just require remote e-mail access, configuring Internet-based authenticated SSL access to the mail server is common. When full peer services are required, use of token or other one-time passwords are recommended.

Additionally, VPN client standards have emerged and are beginning to make an impact.[5]

Despite the improvements in technology in this area, this remains one of the most common unchecked perimeters.[6]

The Inside Problem

But the corporate network security problem that is just really beginning to be addressed from a network-design perspective is the intranet vulnerabilities. For a long time, the FBI has identified between 70% and 80% of “attacks” originating from internal sources – disgruntled employees, corporate spies, marketers of corporate information, etc. Year 2000 data lists this number at 71%[7], due not to a decrease in internal hackers, but an increase in external hacking.

Many corporations implement security practices to protect the “internal perimeters”, through corporate war dialing, to identify modems configured to answer and dial-out modem-banks to protect dial-out connections. These are critical measures, but often insufficient because they are reactive.

In addition to the use of anti-virus software, configured for automatic virus signature update, another emerging approach involves the use of PC-based firewall. Some PC firewalls provide for remote, automatic configuration, which further enhances these products.

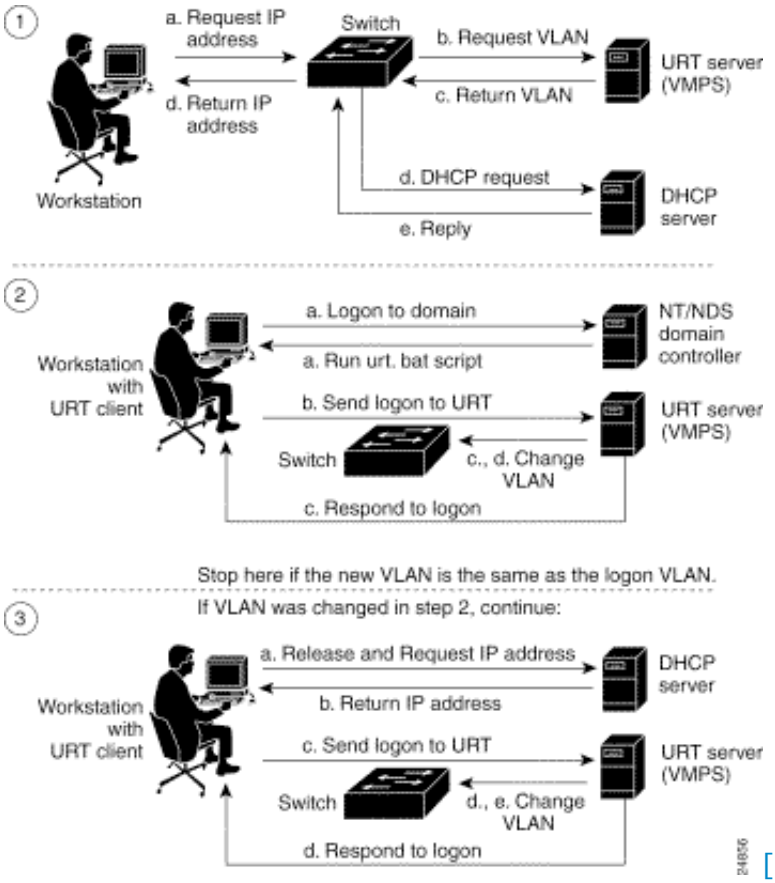
But in most environments, physical access to the network – the ability or inability to plug a device into the network – remains the primary means of internal network security.[8] Unfortunately, most corporate environments do not provide enough physical protections to stop access before it occurs.

Physical connectivity need not provide network access. One of the oldest solutions for this problem was static IP mapping with hub ports secured to a specific Ethernet-card mac address. While this provided very high overhead, for some time this was effective. As operating systems have made it easier to spoof a mac address, this has become less effective.

Some organizations use authentication as a basis for DHCP assignments, typically in a two-step assignment method. In this model, a device receives an IP assignment on startup, which is restricted to only an authentication point, for example, a web server. Upon successful authentication, a new DHCP assignment is made to an address with possibly broader accesses.

The advent of network switching provides some added advantages. No longer does physical location need to dictate network access. Through authenticated DHCP systems, dynamic VLAN allocations can be made which direct a user to the appropriate sub-network, no matter the physical location. Cisco's User Registration Tool (http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/fam_prod/user_reg/1_2_1/use_reg/index.htm) is one example of two-stage DHCP with dynamic VLAN assignments.

Figure 3 – Two-stage DHCP with Dynamic VLANs (Cisco URT)



[9]

Even with these methods of network access security, the disgruntled employee still has full rein. The next step is to close the otherwise open internal network.

Isolating enterprise servers and services from clients and limited-access LAN servers provides some advantages. The principles applied to the DMZ can then be applied to this internal server network. The more this backbone network is isolated the more security can be realized. And the use of intrusion detection and/or honeypots on the internal

network can help spot problems before then become breaches.

Conclusions

Ultimately, the more the risk sources and risk targets can be isolated, the better the network design. However, the ultimate purpose of the network is providing services, so a balance must be made between manageability and security. The CEO will only tolerate lost connectivity so many times and limiting this to hardware failures rather than operator error is well advised. Cost is, of course, also a factor.

Also, any network security plan relies on the secure implementation of the components. Default passwords, SNMP community strings, management access settings, etc., must be properly configured. Trained, qualified staff must administer this equipment and be given the time needed to keep things up to date. But much of the typical infrastructure and knowledge could be leveraged to provide security services currently lacking in many corporate networks.

---

[1] SANS Resources. “A Consensus of the High Impact, Low Cost, Core Actions for a Program of System and Network Security.” *Essential Security Actions: Step-by-Step.* 1999. URL: http://www.sans.org/newlook/resources/esa.htm

[2] Allen, Julia, Alan Christie, William Fithen, John McHugh, Jed Pickel and Ed Stoner. “State of the Practice of Intrusion Detection.” CMU/SEI-99-TR-028 and ESC-TR-99-028. January 2000. URL: http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028chap04.html

[3] Greenlee, M. Blake and Dale G. Peterson. “TCC: Frame Relay Security Guide.” 1999. URL: http://www.tccsecure.com/cgi-bin/auth.pl?file=framerelay_security_guide.htm&session=35f6c3c61b015f2f#3

[4] Laubach, M. and J. Halpern. “Classical IP and ARP over ATM.” RFC 2225. April 1998. URL: http://www.cis.ohio-state.edu/htbin/rfc/rfc2225.html

[5] Hollandsworth, Jon. “Overview of IPSEC Manageability and Security.” *Information Security Reading Room*. July 25, 2000. URL: http://www.sans.org/infosecFAQ/IPSEC.htm

[6]Allen, Christie, Fithen, McHugh, Pickel and Stoner.

[7] Congress, Senate, Committee on Judiciary, Subcommittee for the Technology, Terrorism and Government Information. “Statement of the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime.” *FBI Press Room – Congressional Statement – 2000 – Cybercrime.* March 28, 2000. URL: http://www.fbi.gov/pressrm/congress/congress00/cyber032800.htm

[8] McCumber, John R. “Network Security Basics: Is You LAN as Secure as Your Physical Plant.” April 1996, URL: http://www.simon-net.com/LibraryArticle.asp?Provider_ID=23&Volume=6&Issue_No=3&Section_ID=12

[9] Cisco Systems. “URT-based VMPS Logon Processing.” URL: http://www.cisco.com/univercd/illus/2/56/24856.gif