Global Information Assurance Certification Paper

Designing a DMZ
Assignment Version 1.2b
Scott Young
March 26, 2001

Introduction

DMZ stands for DeMilitarized Zone. A DMZ is your frontline when protecting valuables from direct exposure to an untrusted environment. SI Security defines a DMZ as, "A network added between a protected network and an external network in order to provide an additional layer of security." A DMZ is sometimes called a "Perimeter network" or a "Three-homed perimeter network."

A DMZ is a glowing example of the Defense-in-Depth principle. The Defense-in-Depth principle states that no one thing, no two things, will ever provide total security. It states that the only way for a system to be reasonably secured is to consider every aspect of the systems existence and secure them all. A DMZ is a step towards defense in depth because it adds an extra layer of security beyond that of a single perimeter.

A DMZ separates an external network from directly referencing an internal network. It does this by isolating the machine that is being directly accessed from all other machines. Most of the time the external network is the Internet and what is in the DMZ is the web server but this isn't the only possible configuration. A DMZ can be used to isolate a particular machine within a network from other machines. This might be done for a branch office that needs its own Internet access but also needs access to the corporate network. In DMZ terminology, an internal connection is generally thought of as having more secret or valuable information than an external network. An easy way to understand which is the external and internal network is to ask yourself which network am I protecting from the other.

Separation is important. Any system should have its important applications separated. This acts as system of checks and balances to make sure that if any one area goes bad that it cannot corrupt the whole. The value of separation is recognized by the government. Our government has three branches the executive, the legislative, and the judicial. That same design is needed on a computer system. It is important to separate information so an attacker can't get to all the systems. It would be bad enough for the attacker to get to the web server but if that attacker can get through the web server to your database then that's even worse. This is the type of problem that a DMZ is designed to prevent.

A DMZ's separation will degrade performance. If configured correctly the degradation in performance is usually minimal and seldom noticeable. However, it does exist and you need to be aware of it. This effect on performance must be calculated in the total cost of implementing a DMZ. Usually the performance drop is nominal and the security increase is significant.

How do I design a DMZ?

Start by asking yourself what do I want to protect? Or what is most valuable to me? Then ask yourself what is the entrance point into this system? Or what is my front door? These questions might sound easier to answer than they actually are. You may actually find that you have more than one entrance to your system such as an Internet connection and dial-up connections. It is suggested in this situation that you have two different DMZ's. This is because you're going to

have different configurations for each of those access types. That means extra vulnerabilities. Remember security is minimalism.

What did you say was your front door? It will usually be a web server. You should put two network cards in this machine. Configure the default gateway for one NIC to the outside firewall if outward traffic is needed and configure the default gateway for the other NIC to the inside firewall if inward traffic is needed. Later on I explain why to use dual NICs. Then take that machine and make sure there are no other programs, resources, or utilities on it other than its main reason to function. Put those other things on your internal network if needed. It is also a good idea to configure the machine in the DMZ with a completely different set of log on names and password than any other machines. This is so if an attacker can obtain a password on the machine in the DMZ they still don't have a password to a machine on the internal network.

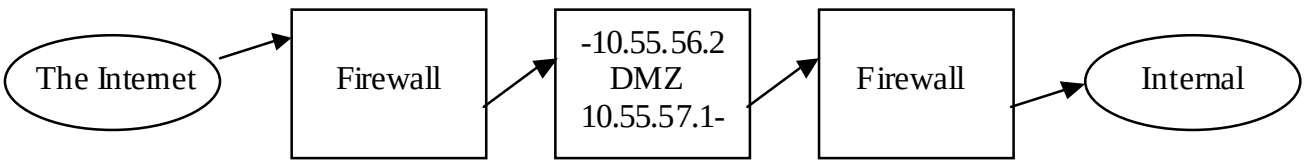
What did you say was most valuable to you? Take those machines and put them on the internal network. Make sure you understand how these machines communicate with the machines you are going to put in the DMZ so you can setup the firewall correctly to allow the needed traffic through. This means knowing what protocols and ports are being used. It may also mean knowing what applications are being used in the event that you're using an application proxy.

The most secure network configuration for a DMZ is to separate your external network, your demilitarized zone, and your internal network by putting them all on different subnets. The reason you want to do this is that network traffic can't transverse to different subnets without being routed. This alone significantly limits network access. If you put your DMZ on adifferent subnet, you will then hold the key to which traffic can go into and out of your DMZ. Without a DMZ, if someone were to compromise your frontline the perpetrator could then quite possibly have access to the entire network. However, with a DMZ the perpetrator only has access to the compromised machine and not the valuable machines outside the DMZ.

Setting your systems up like this will require reconfiguring your DNS to recognize the new IP addresses that you gave the machines. If you have an application in your DMZ that calls another machine by name you will need to configure the LMHOST file. The LMHOST file will tell the machine the IP address and domain of the machine that it is trying to call by name. Without these changes, some machines may not be able to communicate with each other.

How do I setup my firewalls?

This paper will just cover how setting up a firewall relates to setting up a DMZ. A complete guide how to setup a firewall is outside the scope of this paper. You can use one firewall or two to make a DMZ. Some firewalls have a optional setting that says if the firewall crashes it allows all traffic through. If this setting is set and the one firewall crashes then you no longer have a DMZ. This is just one example to illustrate the point that using two firewalls is a more secure configuration. Two firewalls further separate the external and internal networks. Using two firewalls, you need one in front of the DMZ and one behind it. The one in front of the DMZ should be between the external network (probably the Internet) and your DMZ.(probably a web server) The other firewall should be between the DMZ and the internal network as the below diagram shows.



The most secure configuration is for each of the firewalls or web servers to have dual NICs. Of course this is not the only possible configuration but it is the most secure. The firewall in front of the DMZ should only allow the minimum required traffic through. For web servers, this is typically only TCP port 80 for HTTP and/or TCP port 443 for SSL. You will have to determine what is the minimum allowed for your application. Do not assume that because one firewall had a rule to allow a certain type of traffic that all of your firewalls will need the same rules. Know your system. Know what rules are needed for each individual machine. The firewall in between the DMZ and the internal firewall will probably need different rules than the firewall in front of the DMZ. It will need rules to allow traffic through to whatever it needs to access on your internal network. An example of one such service might be a SQL database. In that case, you'd probably open TCP port 1433.

It would further increase your security to have different types of firewalls on each side of your DMZ. This would increase your security because it decreases the chances of the attacker knowing how to get through two different firewalls. Different firewalls have different strengths, features, and bug. More importantly, in the event that a bug exists on one of your firewalls it decreases the chances of the bug existing on both of them. The one catch to that is to make sure you know how to configure both firewalls correctly because an incorrectly configured firewall is the same as no firewall.

Why do I need dual NICs?

It is possible for a machine within a DMZ not to have dual NICs but that would not be the most secure configuration. The need for dual NICs is a frequently argued point but most will eventually agree dual NICs provide greater security. If dual NICs are not used then you must rely on a router. This could result in all of the machines inside and outside of the network being connected in one way or another to the same router at some point. On the lowest end of the OSI model, the physical layer, this creates little to no protection where as dual NICs do. There are plenty of attacks and common hacking techniques that are capable of taking down a router or bypassing its routing table. Also, if the router were to fail or was compromised, it could allow a breach even higher on the OSI model depending on the router and the failure. Dual NICs give an extra physical layer of separation that wouldn't otherwise be there.

How can I use DCOM with a DMZ?

DCOM has some problems working through firewalls. At first glance, it might appear as if using DCOM through a firewall would be an easy task but it is not. Thorough instructions on how to setup this configuration are beyond the scope of this paper. I will cover the primary area most people have problems with. I am covering this because how to use DCOM in a DMZ is very important information to the functionality and practicality of a DMZ. As people become more security conscious, the desire to use a DMZ is going to increase. With that will be an increase in the need to use DCOM through firewalls. Currently there is very little information on how to do this configuration.

The problem with using DCOM through a firewall is that you have to restrict the ports and protocols it uses. DCOM by default selects randomly from a wide variety of ports. So when setting up your firewall it is hard to create a rule allowing the traffic because it is hard to predict which port it will use. If you go into the DCOM Configuraion UI, dcomcnfg.exe, it will appear

that restricting ports is a simple task. But you will soon discover that your settings are not saved properly after you exit the application. If you make changes to which ports DCOM should use, exit the application, and then reboot and reload it the settings are gone. It will appear as if you never entered those settings at all. More importantly, DCOM will not use those settings. Microsoft is aware of this flaw and has released a few help pages on the subject. (4) Refer to the references at the end of this paper for a link to these help pages.

Restricting the ports that DCOM uses requires editing the registry. As always, before making any registry changes, make a boot disk and make a full backup of the registry.
- Run Regedt32.exe.
- Go to "*HKEY_LOCAL_MACHINE\Software\Microsoft\RPC\Internet*".
  If this key doesn't already exist then create it.
- Under this key create a value called "*Ports*" of type "*REG_MULTI_SZ*".
- Set the value to equal whatever port range you wish for DCOM to use.
  Such as *"2000"* or *"2000-2005"*. Plan for one port per application using DCOM.
- Go to "*HKEY_LOCAL_MACHINE\Software\Microsoft\RPC\Internet*".
- Under this key create a value called *"PortsInternetAvailable"* of type "*REG_SZ*".
  Set this value to "*Y*". This tells DCOM that these ports are to be used internally.
- Go to "*HKEY_LOCAL_MACHINE\Software\Microsoft\RPC\Internet*" .
- Under this key create a value called *"UseInternetPorts"* of type "*REG_SZ*".
  Set this value to "*Y*". This tells DCOM that these ports are to be open versus closed.

(Do not include the quotation marks in your entries into the registry just what is inside of the quotes.)

Make sure that you make the changes exactly as described above or DCOM may not work correctly or worse problems may occur. After you have made these changes, you will need to reboot the machine. Perform these changes to every machine that needs to connect to a machine inside the DMZ and using DCOM.

You will then need to create a new rule in the firewall to allow this traffic through. You want to add that rule to the firewall between the DMZ and the internal network. This rule should allow just the ports you entered in the registry for NT4.0. For Windows 2000 this rule should allow the ports you entered in the registry and port 445. DCOM in Windows 2000 requires the use of port 445. This is enough information to get DCOM to work through a firewall but if you require more information on this refer to:
http://www.microsoft.com/technet/isa/isadocs/CMT_DMZ3Home.htm

There are some other things you can do to secure DCOM further. First, only use the protocol TCP. TCP has more inherent security than other protocols. This can be done in the UI under the "Default Protocols" tab. Secondly, select a higher level of default authentication from the "Default Properties" tab such as "Packet Integrity" or "Packet Privacy". Choosing either of these two will cause a further slight performance drop but it is more secure. Getting into this any deeper is more along the lines of a paper about securing DCOM. For that you can refer to the article "Using Distributed COM with Firewalls" by Michael Nelson. It can be found on Microsoft's web site and there is a link to this site in the references. (6)

Troubleshooting

After you've setup your DMZ, make sure it is working. Check every application that you will need to use and every aspect of that application's functionality to ensure it still works properly. If something isn't working correctly then research the ports and protocols of the application. Make sure there is a rule for that in the appropriate firewall and that the application knows the new IP address of the machine that it is calling. It may even be necessary to detect what traffic the application is generating with a sniffer. You should always know exactly what your system is doing anyway.

Why do I want a DMZ?

If you don't have a DMZ and your initial frontline perimeter is broken then the game is up. There are new bugs found all the time in software. Even if you have hardened your operating system and have a firewall, there is still the possibility that the software on those systems might contain a bug that an attacker could exploit. When you consider all the IIS bugs and DOS attacks it may only be a matter of time until your initial perimeter is violated. Then the attacker has access to whatever vital information you have on those systems such as your SAM files and databases. A DMZ hides your important information an extra step away from an attacker.

Do I need a DMZ?

Some of the things to consider when deciding if a DMZ is right for you are:
- The price of the hardware and software of the extra machines needed to implement a DMZ
- The slight decrease in performance
- The cost of the time to implement the DMZ
- The cost of down time the system suffers from adding on the DMZ
- The lowered level of accessibility to an attacker

The price of the additional software and hardware to implement a DMZ pales in comparison to the cost if the internal network is successful compromised.

Conclusion

A DMZ greatly increases the security of a network. Any network with a web server and even one other machine can benefit from a DMZ. A DMZ is not only useful for a system that contains valuable or private information. Any one that wants to add an extra layer of protection to a machine can benefit from a DMZ. A DMZ, if properly configured, can quickly increase the security of any network. This is because there are twice as many machines for an attacker to compromise to get to anything valuable. This greatly increases the skill required of an external hacker to compromise the internal network and thus lowers the threat of the internal network being compromised. Of course, the defense-in-depth principle must be remembered and practiced, but a DMZ does provide a significant increase in security.

References:

1. SI Security, "DMZ Support Provides Secure Configuration for Multiple NICs",
URL: http://www.ssimail.com/zoneguard.htm

2. Johns, Paul, "E-Commerce Security",
URL: http://www.microsoft.com/technet/ecommerce/ecomsec.asp (April 2000)

3. Microsoft Technet, "Three-Homed Perimeter Network Configuration",
URL: http://www.microsoft.com/technet/isa/isadocs/CMT_DMZ3Home.htm

4. Michael Nelson, "Determining Windows 2000 Network Security Strategies",
URL: http://www.microsoft.com/technet/win2000/dguide/chapt-17.asp

5. Chuck Semeria, "Internet Firewalls and Security",
URL: http://www.3com.com/nsc/500619.html

6. Michael Nelson, "Using Distributed COM with Firewalls",
URL: http://www.microsoft.com/Com/wpaper/dcomfw.asp

Last Updated: July 26th, 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 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
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
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
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS