DMZ Implementations

Table of Contents

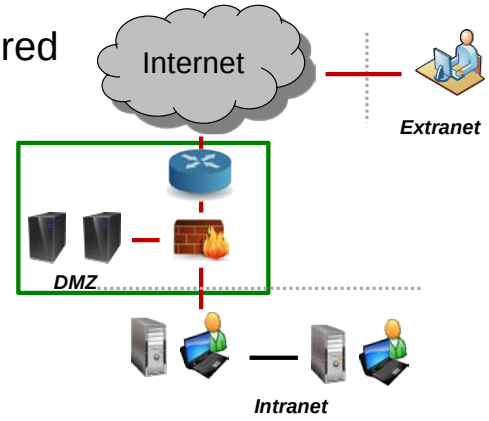
DMZ – De-Militarized Zone

Publicly accessible network, defined by perimeter protection devices

Contains servers with ***public*** information

Defined ingress and egress rules

Strong security and monitoring required



**102 I like putting servers in a shared services network.

This is a place, not a thing; and it contains both public information and semi-public information.

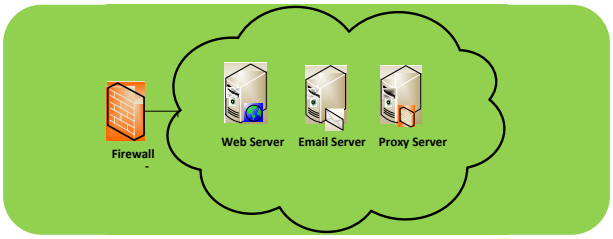
When we look at our mail server that's sitting here, we're taking mail from the big bad internet, out here; and all we're doing is sending the appropriate mail backwards in here.

So in this demilitarized zone we have that shared services. We have to do different kinds of monitoring based on traffic destination.

DMZ Reiteration -1

The DMZ is a special zone within a network where servers, that are intended to be publicly accessible are connected.

A DMZ allows an organization to host content or provide external access while limiting access to more sensitive information contained on servers inside the network on the Intranet.



**103 So remember, it's a special zone within your network that is intended to be publicly accessible and connected to; but only in controlled ways.

So what we want to do is we want to organize the host content to provide external access; and then limit the more sensitive information contained on the servers to internal access.

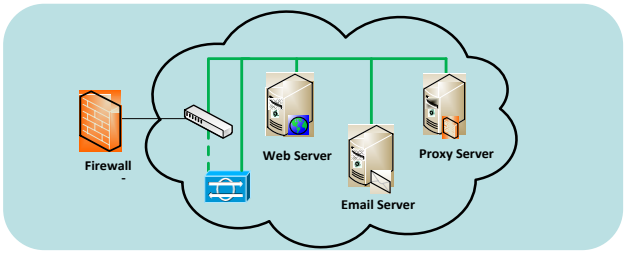
DMZ Reiteration -2

DMZ servers usually include web, mail, and application servers.

Perimeter control devices define the boundaries of the DMZ.

- Ingress and egress rules are highly recommended to strictly control access to the servers and the information they contain.

Strong security and monitoring are required on these systems as they are publicly accessible via the Internet.



**104 DMZs are usually protecting the services that we share: web, mail, DNS and some application servers.

The perimeter controlled devices define the boundaries for the DMZ. So they will say: Hey, you know what? That firewall that's there, or that intrusion prevention system that's there, is going to have a certain set of rules on it.

Those rules must match your business process. They must match-- the things that you do on the internet, it must be matched in that set of rules.

And your way of doing business, your particular type of business, is going to be very different than that person's or that person's or mine. So you have to be ready for that.

You're going to have to do lots and lots of monitoring here. This is not a set it and forget it kind of thing. Because this is where the attackers are going to go.

Now theoretically you could outsource this entire activity to somebody else for them to do; and that would relieve you of the responsibility of regular review.

But it does not relieve you of the decision-making process.

DMZ Implementations

DMZ can be constructed in many different ways.

The core components are a set of routers and firewalls.

- Generally, the bare minimum to create a DMZ

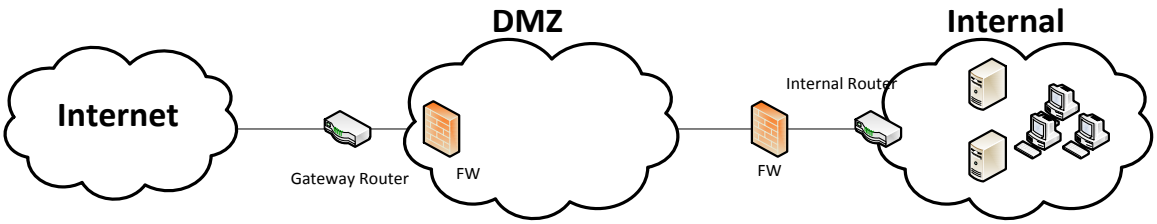
Add servers to the DMZ to meet specific requirements.

- VPN
- Web
- DNS
- Proxy

**105 DMZs don't have to be made one way. But they usually contain the same components. They're going to have some routers and some firewalls in some organized fashion here.

Bare DMZ

A minimal DMZ includes components such as firewalls, a gateway router, and internal router(e.g., gw->fw1->fw2->intrtr)



**106 And when we talk about "the bare minimum DMZ" it usually consists of two firewalls. So we've got our internal network, and it's protected by one set of firewall rules that are different than the firewall rules that are out here for our shared services. We put two different firewalls up.

Now some vendors out there are not going to be happy with me. Do not use the same firewall from the same vendor. Why? Because the attack that is good for the external firewall-- and if that one is cut through and attacked and actually taken over and controlled by the adversary-- the

exact same- the exact same attack is going to be susceptible for the second firewall. So use two different ones.

Web Servers

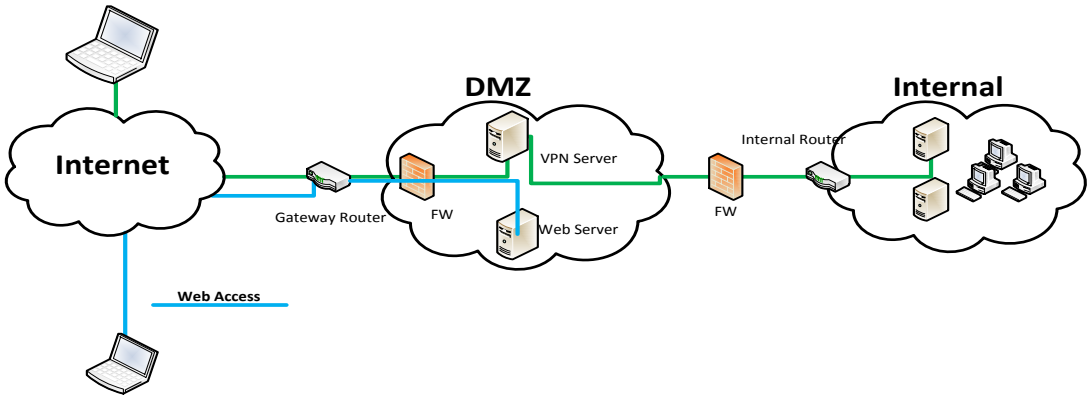
Web Servers

Typically public-facing servers

Often the launching point into a target's network

Have known vulnerabilities

- Misconfiguration in server or operating system software
- Vulnerabilities / bugs in server or operating system software
- Vulnerabilities from default installations



CERT | Software Engineering Institute | Carnegie Mellon University 107

**107 Okay well what about web servers, how do we protect them? Well we put them in the shared services network here; and we create one set of rules going out this way.

Look, here's our Virtual Private Network server sitting up here. We also put that in the DMZ. And what we say is: From the outside, when they want to do virtual private networking they'll go through the

firewall; and the only destination they will be allowed to go to is this VPN server. We've created one set of rules there.

We've done any kind of authentication that we needed to do here; and we abstracted something, usually in a Radius server. And then we will allow it to pass back that VPN service through this firewall.

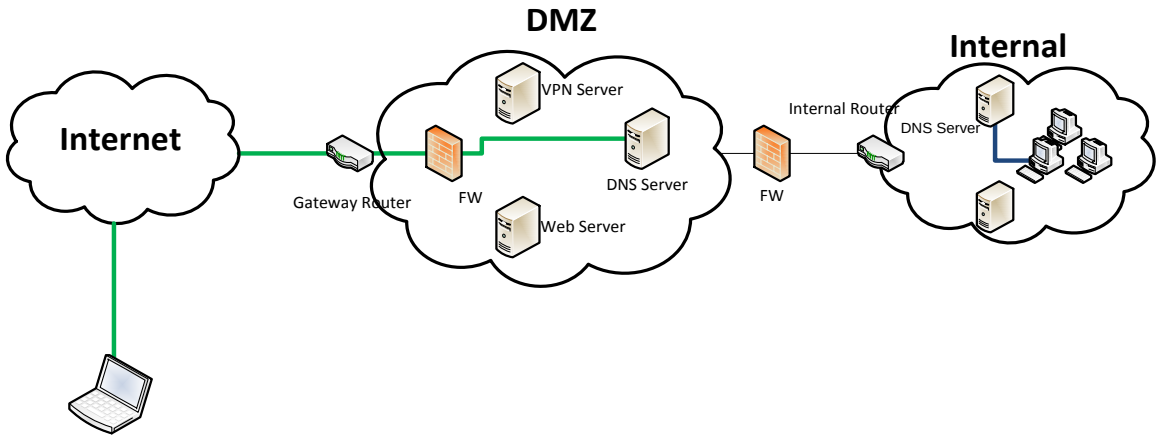
This firewall will now say anything from the VPN server is perfectly acceptable to go back; and it may be only to a few hosts back there. It might to all; but it may be to a few.

One set of rules here that manage this relationship. One set of rules here that manage this relationship. And the only way that they would get us is if they would attack the firewall, compromise the firewall, pass through and attack the VPN server; and then compromise it to go back here. And then that traffic from the VPN server would not be your normal traffic.

DNS Servers

Placing a DNS server inside the DMZ will prevent external DNS requests from accessing the internal network.

Additional protection can be provided by installing a second DNS server on the internal network.



**108 Where's our DNS server sit? Well in this diagram here, when people from the internet want to resolve our web server's name, they use our own internal DNS server. That also could be used by internal; but I don't think you do that.

Notice we've got one DNS server for answering public requests to resolve this web server and maybe a mail server.

This DNS server that's sitting back here is only fulfilling requests for these clients to the rest of the planet. It is used as a pass through DNS server; not for validating any requests from the internet.

So anything that came back here and was requested as a service, when we got to this firewall, this firewall would say: Wait a minute, I'm not even going to allow you to query DNS back here; and if there's a response that comes from here, that goes outbound, I'm not going to allow that.

Now if this DNS server is making a request of an internet service, when it's going out here and it's communicating, well that's very different. I'm not resolving for a client; I'm resolving for my clients, at that point.

Unified Threat Management (UTM)

Unified Threat Management (UTM)

Appliance that combines multiple security applications

- All-in-one solution (Next Generation Firewall)

Installed at network border

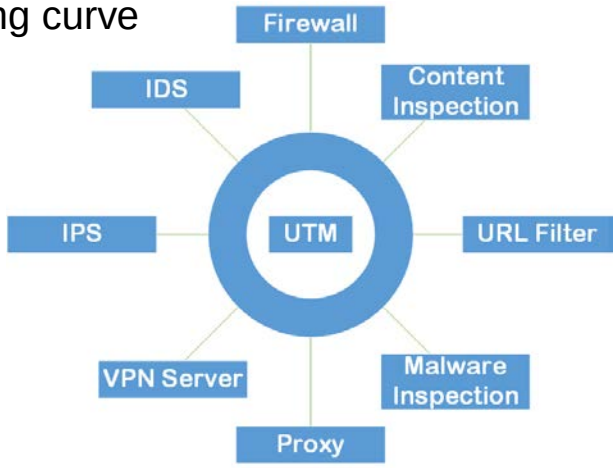
Reduced complexity/learning curve

Small footprint

Great for small businesses

Disadvantage

- Single point of failure
- Vender dependency



CERT | Software Engineering Institute | Carnegie Mellon University 109

**109 Now we run into the UTM:

Unified Threat Management; otherwise known as the all-in-one device. It takes care of all of our needs for ourselves.

Good news: We can get it all in one package.

Bad news is: Single point of failure.

Good news is: Rich services that we may not otherwise be able to afford to manage and deal with in a small network.

Bad news is: We're paying somebody else; and they have to abstract all of our requirements and make them match all of the other requirements of all of their other clients.

So Unified Threat Management says: This is great for small business. But realize that you're getting a more vanilla solution; and that may not be appropriate in your network.

UTM – URL Filter

Filter outgoing HTTP requests

- Blocks
- Allows
- Redirects

User Defined – matches criteria for domain names and paths

Category-based – matches request against third-party provided lists

- Adult Content
- Social Sites
- Shopping
- Etc.

CERT | Software Engineering Institute | Carnegie Mellon University 110

**110 What does the Unified Threat Management do? Well let's look at a couple of these components here.

URL Filtering. We won't let you go to shopping sites or ESPN or anything else that's inappropriate; and we can manage that on a group by group basis.

We can define the match criteria on the domain names, the paths, the IP addresses.

We can also look at the type of content that's being flown across this URL filtering.

We can be very, very specific with certain analysis engines where we can say: You are allowed to go to Facebook; but you're not allowed to go to Farmville. That might be- might not be an appropriate use of our internet bandwidth.

Remember today with an end-user's ability to actually surf the internet off of their phone or their small device, not using up any of our bandwidth, it may be that you say: We won't allow anything except for business traffic.

UTM – Content Inspection

UTM – Content Inspection

Block data based on the content rather then where it originates

- Specific file types – .zip, .exe, java, etc.

Data Loss Protection (DLP) – inspect text strings to prevent sensitive information such as social security and credit card numbers from leaving the network

- Email messages
- Attachments

**111 Content Inspection. What does the attachment look like? What

does the attachment contain? What kind of emails are you sending outbound?

In content inspection we can get very, very granular and create a data dictionary for Data Loss Prevention.

Users on my network back here say: We'd like to send out the serial numbers- I mean, the Social Security numbers and information about our customers to a vendor.

And it comes along; and the Data Loss Prevention system goes: Well this looks like a serial number. I'm not going to send that stuff.

And it sends a message back to the user and says: This has been quarantined; are you sure? They send back a message to their manager and say: Hey manager, take a look at this; is this appropriate?

And the Data Loss Prevention tool will actually look at the email messages and the attachments. It will actually inspect the web traffic; if you've got it set up and designed for that. That's very special purpose.

UTM – Malware Inspection

Inspect inbound traffic for malicious software and block it

Anti-virus on the firewall!

Based on signatures from third-party providers

**112 Malware inspection. So inbound traffic that's coming to my UMTS-- we can have anti-virus signatures built into this to say: I'm not going to allow that content through because it is some sort of malware.

I could also do it for anti-virus.

And the real trick with this is is making sure that whatever vendor you choose, they're doing a really good job of updating their signatures; and producing those signatures for you to install in your Unified Threat Management tool.

Notices