Cryptography: System Security MCA Semester-IV

Paper Code : MCACS4T15

Firewall-Demilitarized Zone (DMZ)

Ms. Sushmita Chakraborty

Assistant Professor

Dept. of MCA, Patna Women's College

email-id: sush123.chakraborty@gmail.com

UNIT:4- FIREWALL-DEMILITARIZED ZONE

In computer security, a **DMZ** or demilitarized zone (which is sometimes referred as perimeter network or screened subnet) is a physical or logical sub network that contains and exposes an organization external facing services to an untrusted, usually larger, network such as the internet.

The purpose of a DMZ is to add an additional layer of security to an organization's LAN, an external network node can access only what is exposed in the DMZ while the rest of the organization's network is firewalled.

FIREWALL-DEMILITARIZED ZONE(CONT…)

The more secure approach to creating a DMZ network is a dual –firewall configuration, in which two firewalls are deployed with the DMZ network positioned between them. The first firewall- also called the perimeter firewall – is configured to allow external traffic destined to the DMZ only. The second or internal, firewall only allows traffic from the DMZ to the internal network. This is considered more secure because two devices would need to be compromised before an attacker could access the internal LAN.

FIREWALL-DEMILITARIZED ZONE(CONT…)

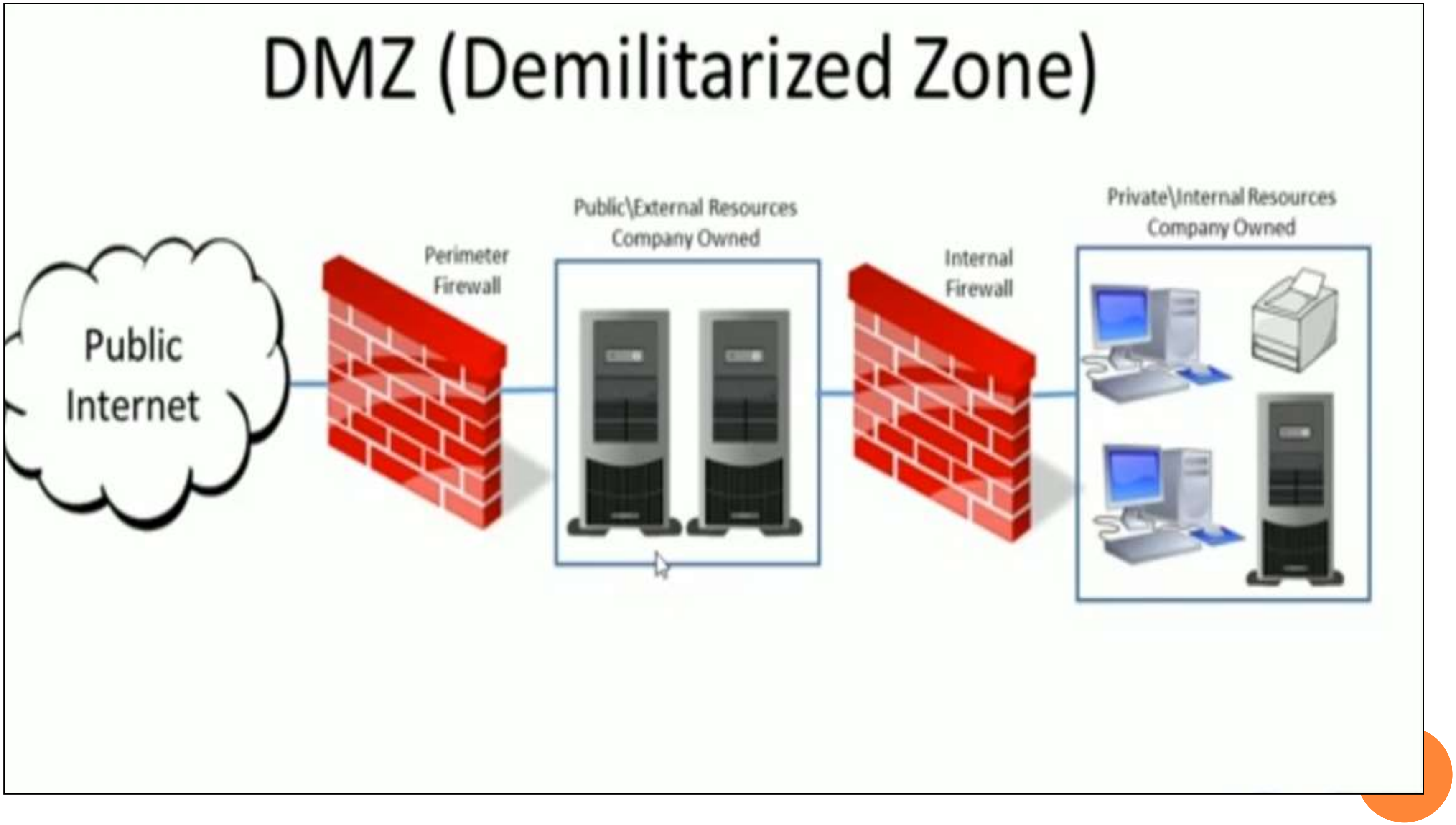
As a DMZ splits a network, security controls can be tuned specifically for each segment. For example, a network intrusion detection and prevention system located in a DMZ and providing web services could be configured to block all traffic except HTTPS request to TCP port 443.

There are various ways to design a network with a DMZ. The two basic methods are to use either one or two firewalls, though most modern DMZs are designed with two firewalls. The basic approach can be expanded on to create complex architectures, depending on the network requirements

FIREWALL-DEMILITARIZED ZONE(CONT…)

A single firewall with at least three network interfaces can be used to create a network architecture containing a DMZ. The external network is formed by connecting the public internet- via internet service provider (ISP) connections- to the firewall on the first network interface. The internal network is formed from the second network interface and the DMZ network itself is connected to the third network interface.

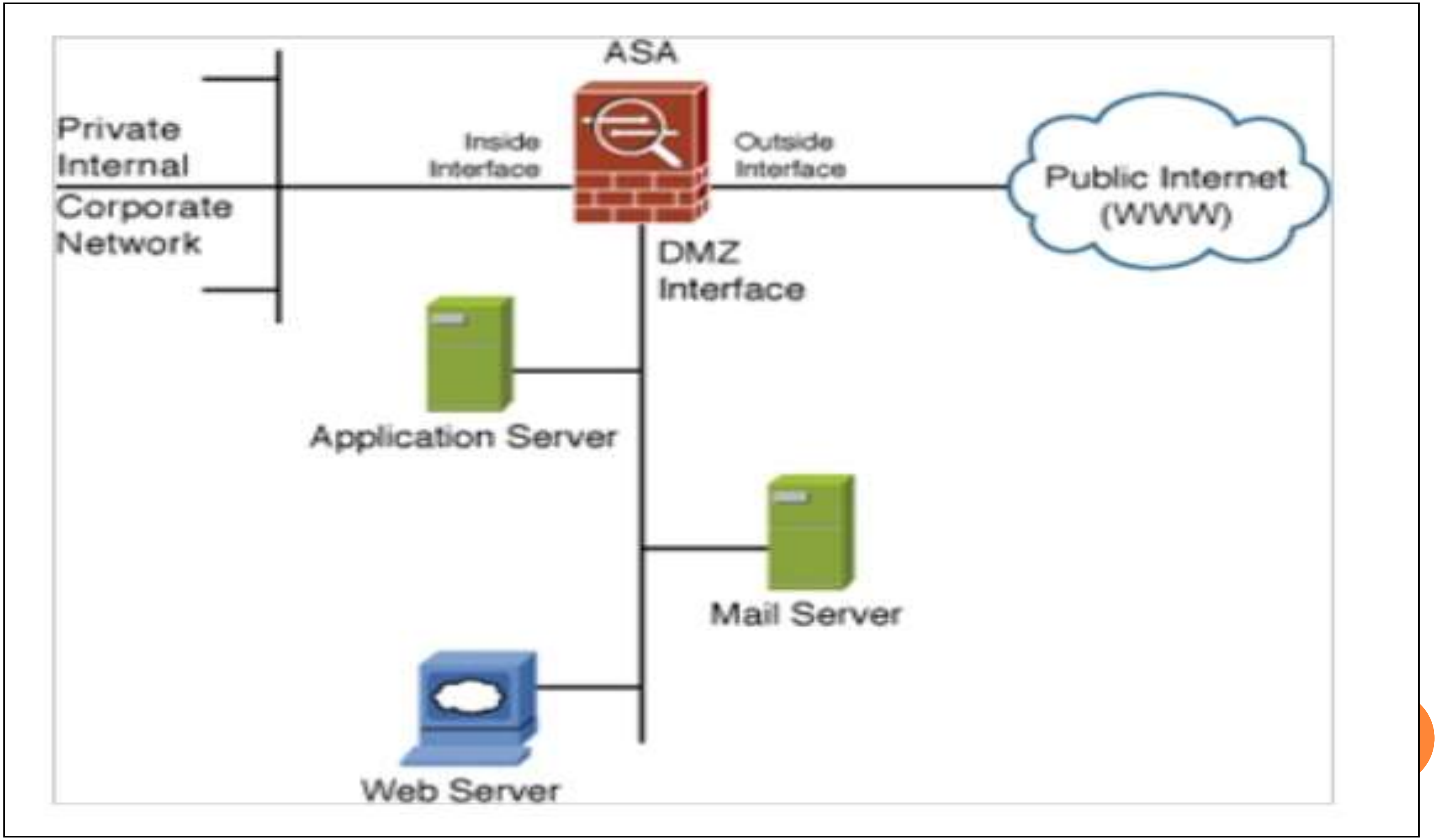
DMZ (Demilitarized Zone) Network



DMZ (Demilitarized Zone)

Public Internet
Perimeter Firewall
Public\External Resources Company Owned
Internal Firewall
Private\Internal Resources Company Owned

DMZ Placement and Function



DMZ Placement and Function

In the above fig. the segment connected to the DMZ interface contains the mail, web, and application servers. Rules applied the DMZ interface prevent traffic from the internet from going beyond the segment attached to it.

Benefits of DMZ

The biggest benefit to a DMZ is in isolating all known internet requests to the servers on the DMZ and no longer allowing them into your internal network. However, some additional benefits to deploying a firewall with a DMZ can help in a better way to understand what happens in your network and thereby increases security.

- Auditing DMZ traffic
- Locating an IDS on the DMZ
- Limiting routing updates c three interface
- Locating DNS on the DMZ

Thank you