**Chapter 1**

**Understanding a network**

Network - a set of two or more endpoint devices that communicate with each other through a shared medium.

Protocol - means a strict code of etiquette and precedence.

What do devices that can be networked have in common?

* They all possess at least one network interface card (NIC), they are running a network operating system (NOS), and have been coded in a way that takes advantage of one or more of the networking protocols that are available.

Another definition of a network is that it's a shared medium. When referring to a network medium or to network media, we are talking about the channel that the data is being transferred across.

**Understanding internet**

When spelled with a lowercase i, internet is derived from inter-network and refers to the connectivity between different networks.

When capitalized, the Internet refers to the services that are publicly available outside of our own networks and the supporting infrastructure.

The difference between World Wide Web (WWW) and Internet:

* The Internet refers to services and infrastructure.
* In contrast, the WWW is only a portion of the services that the Internet provides and refers to servers that provide websites to end users.

**Understanding intranets**

The prefix intra- means on the inside.

An intranet relates to network communication within our network.

Access to intranet services will be controlled through user/device authentication to ensure that they remain private and inaccessible from the Internet.

Some organizations host internal web pages, such as the collaborative tool SharePoint from Microsoft, or a Human Resources self-service portal.

**Understanding extranets**

Exam tip: Do not confuse an extranet with a demilitarized zone (DMZ), otherwise known as a perimeter network,. For an extranet, the words to look for are trusted or authorized.

An extranet is when we allow access to our intranet to organizations other than our own.

For security reasons access is only permitted to trusted (or authorized) organizations such as our business partners or our larger customers. Furthermore, this access is limited only to the resources that they need for their normal interaction with us.

**Introduction to basic security features**

**1. Firewalls**

A firewall is designed to either allow or deny network traffic based upon a set of defined criteria. These criteria could be a predefined set of default rules or could be user-created, or even a combination of the two. These rules are often referred to as access control entries (ACEs), and a group of them form an access control list (ACL). These criteria could then be applied to outbound (or egress) traffic or inbound (or ingress) traffic. Understanding that a rule can be applied in each direction is important to know.

Several firewalls read through their rules in a sequential manner. They read the rules in order until they find one that matches, and then apply that rule and doesn't carry out any further processing.

Host-based firewall

* A host-based firewall is one that is either built into the OS or installed on the device (E.g. Windows Firewall).
* The limitation of this is that you need to configure the firewall on each device, and it only protects that device.
* One saving grace if you are in a domain environment is that you can deploy these settings to each machine using a group policy object.
* Leaves your network susceptible to an attack from outside.

Network-based firewall

* A network-based firewall, on the other hand, provides protection to all your networks and monitors traffic
* This may be through a dedicated hardware device or as a feature on another network device, such as a router.
* If one computer in the network is compromised, it can attack other computers in the network.

It is recommended that any network you run has both host-based and network-based firewalls to provide what is known as defence in depth.

Windows Defender Firewall

* Windows Defender Firewall is accessible via Control Panel | System and Security | Windows Defender Firewall.
* It details the configuration for private networks and public networks.
* When you connect to a new network, you are prompted to specify what sort of network location you are connecting to. Home or work networks are classed as private networks; Wi-Fi hotspots in bars, libraries, coffee shops, etc. would be classed as guest or public networks.
* To change the settings, we need to click on Turn Windows Defender Firewall on or off on the left-hand side of the page.
* We can go into the Advanced settings by clicking on that option on the left-hand side of the Windows Defender Firewall pop-up screen.
* Clicking on Inbound Rules takes you to a list of current inbound rules and clicking on Outbound Rules provides you with a list of current outbound rules. By double-clicking on an existing rule, you can see the properties of that rule and edit the configuration accordingly
* A new rule can be created by selecting the appropriate direction, that is, inbound or outbound, and then clicking on New Rule.
* Another rule type you can configure is Connection Security Rules, which allow or deny traffic based on what security mechanism is in place on the connection.
* On Windows devices firewall logs are stored at: %systemroot%\system32\LogFiles\Firewall\pfirewall.log.
* We need to enable logging in the properties of Windows Firewall with advanced security.

**2. DMZ**

A DMZ, or a perimeter network, is a means of allowing the public to access certain network services while still maintaining the security of your internal devices.

There are some similarities between extranets and DMZs, but an extranet provides access to those services to trusted organizations, whereas a DMZ allows access to the public.

Common services that would be placed in the DMZ include a web server and a Domain Name System (DNS) server.

Some organizations will purchase firewalls from two different manufacturers. If an organization used the same firewall throughout its infrastructure, and that firewall had a vulnerability, then the vulnerability would likely be reproduced across the network.

Examples of firewall placement when implementing a DMZ:

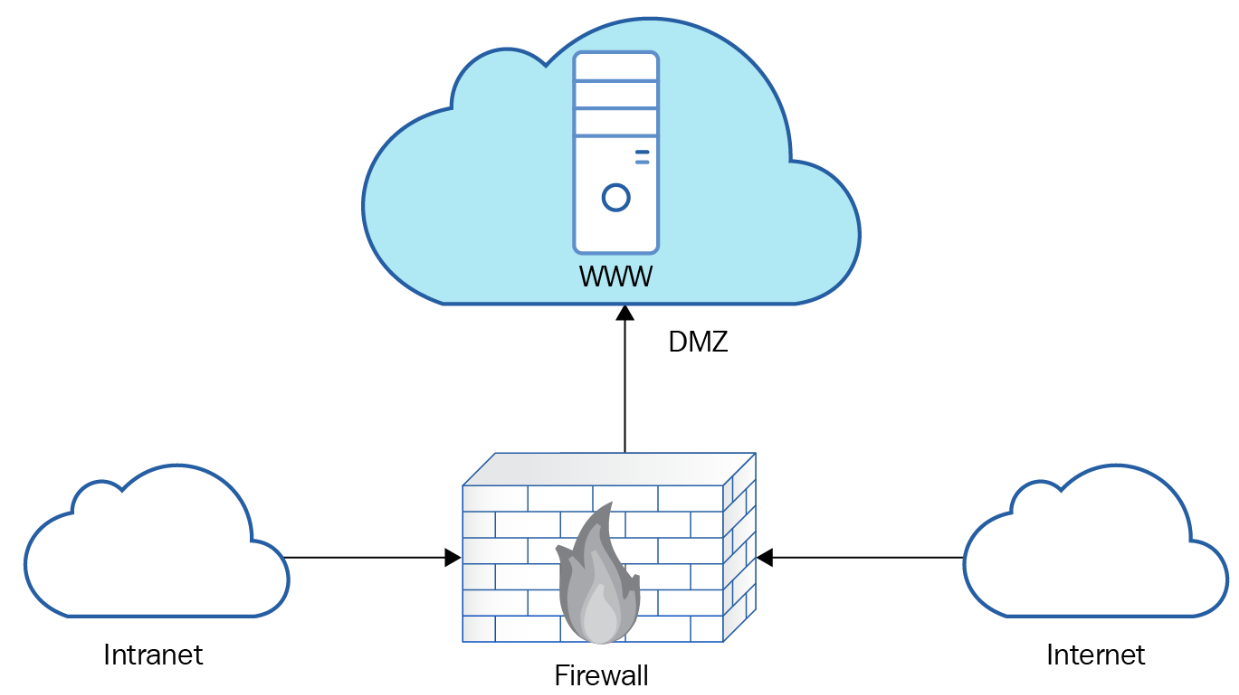
Figure 1 DMZ using 2 firewalls

A diagram of a cloud computing network

Description automatically generated

* Some organizations will purchase firewalls from two different manufacturers. If an organization used the same firewall throughout its infrastructure, and that firewall had a vulnerability, then the vulnerability would likely be reproduced across the network.

Figure 2 Three-homed firewall



* Also referred to as triple-homed or a screened subnet.
* While it saves the cost of only requiring one firewall, it increases the risk. If that one firewall is breached, then both the DMZ and the internal network could be compromised.

**3. VPNs**

A virtual private network can be defined as a means of transmitting private data securely from one network across an unsecured network to a third network. (Generally speaking, the unsecured network is the Internet)

We often refer to the use of VPNs as using a VPN tunnel.

Why would companies need to use a VPN

1. When an organization is located on multiple sites:

A diagram of a cloud computing system

Description automatically generated

* The organization has two sites: a head office and a branch site (sometimes referred to as satellite sites).
* All the traffic from the branch offices passes through a device known as a VPN concentrator.

2. Installation of a VPN client on each device (remote access VPN).

A diagram of a network

Description automatically generated

* Usually reserved for telecommuters or mobile users, such as sales staff or field engineers, or home-based users.
* When a user wants to connect to the head office, they need to open the VPN client application on their device and then authenticate via the application before they can gain access to the head office network.

3. VPN may also be used with an extranet to provide limited secure communication to our infrastructure for our trusted partners.

Three different VPN protocols Microsoft has in recent years:

* Point to Point Tunnelling Protocol (PPTP)
* Point to Point Protocol (PPP)
* Secure Socket Tunnelling Protocol (SSTP)