

WELCOME TO MODULE 8

# NETWORKING AND SYSTEM UPDATES

# SECTIONS

Section I- What is NIC?

Section II- Enable internet on the VM

Section III- NIC Teaming

Section IV- Network Configuration

Section v- Windows Updates

Section VI- NTP Configuration

Section VII- File Transfer Methods

Section VIII- FTP Server Installation and Configuration

Section IX- Sharing File System (Samba or NFS)

Section X- WSUS Server Installation and Configuration

Section XI- Windows Firewall

## Section I- What is NIC?

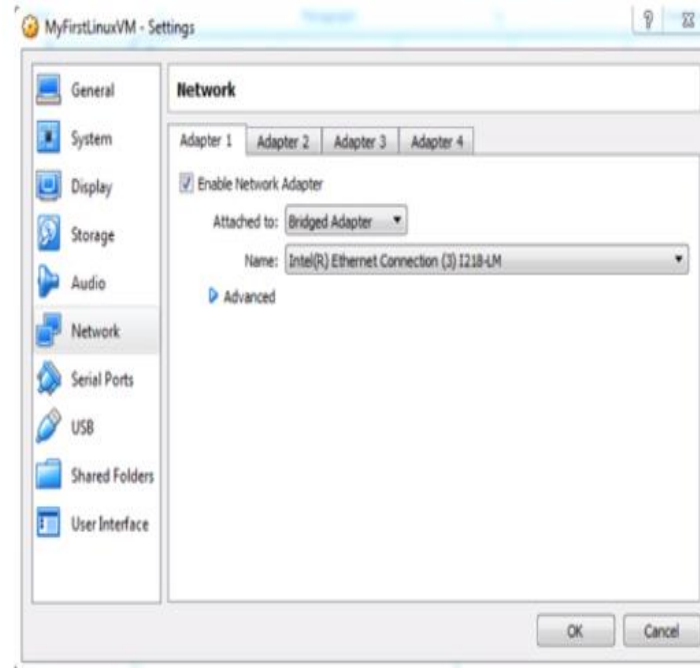
- NIC stands for Network Interface Card or sometimes controller. It is a network adapter hardware in the form of an add-in card that fits in an expansion slot on a computer's
- A NIC can have one or more ports



- All network communication flows through the NIC

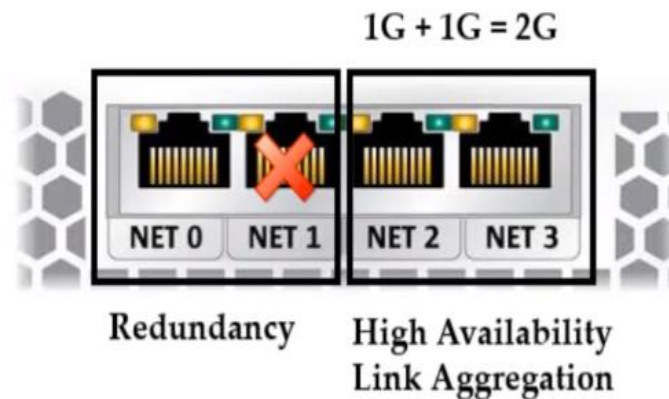
## ➤ Section II- Enable internet on the VM

- A VM network runs over its host network



## Section III- NIC Teaming

- NIC (Network Interface Card) teaming is also known as NIC bonding. It can be defined as the aggregation or combination of multiple NICs into a single team interface
- It's main purpose is to provide high network bandwidth or redundancy





## Difference between Bridged and Teaming:

- Bridged mode is a simplified version of teaming. In a nutshell all bridging does is allow the computer to see both network connections as 1, and use the bandwidth of both at the same time. It's also the only "teaming" type option available on non-server OS's.
- Teaming is more geared towards throttling and stability. Normally teaming is setup so that 1 line is in, and 1 line is out. This prevents the server from being over-run with too much incoming traffic such that the outgoing suffers, and vice-versa

# Teaming Mode

## Teaming Mode:

^ Additional properties

**Teaming mode:**

Switch Independent ▼

**Load balancing mode:**

Static Teaming

Switch Independent

**Standby adapter:**

LACP



You can configure your team for either Static Teaming, Switch Independent, or LACP (Link Aggregation Control Protocol).

**Static Teaming** requires configuration on the switch and the computer to identify which links form the team. Because this is a statically configured solution. This is a switch dependent mode of NIC teaming.

**Switch Independent mode** allows you to distribute the NICs in your team across numerous Network Switches in your environment.

**LACP** provides the Link Aggregation and allows for the expansion and reduction of the NIC team. This is a switch independent mode of NIC teaming.

### Load Balancing Mode:

#### ^ Additional properties

**Teaming mode:**

Switch Independent ▼

**Load balancing mode:**

Address Hash ▼

**Standby adapter:**

Address Hash

Hyper-V Port





**Address Hash** is how you configure your team to load balance network traffic between the NICs in the team.

**Hyper-V Port** load balancing will load balance your traffic by VM. With Hyper-V Port, the good news is that each VM will transact on a separate NIC, but the down side is that each VM will only transact over a single NIC.

If you have multiple virtual NICs in your VM and they are teamed, the Hyper-V Port may be the best choice. For most configurations, I expect that the Address Hash will be your best choice to allow your VM to still access the network in case the NIC the VM is utilizing fails. Remember that with Hyper-V Port the failure of the NIC the VM is utilizing disrupts communication between the VM and the network. Address Hash won't have this problem

## Section IV- Network Configuration

- A computer network, or data network, is a digital telecommunications network which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections between nodes



We will learn...

- IP (*192.168.1.x*)
- Subnet (*255.255.255.0 - The practice of dividing a network into two or more networks is called subnetting*)
- Gateway (*allows data to flow from one network to another*)
- MAC address (*A media access control address of a device is a unique identifier assigned to a NIC*)

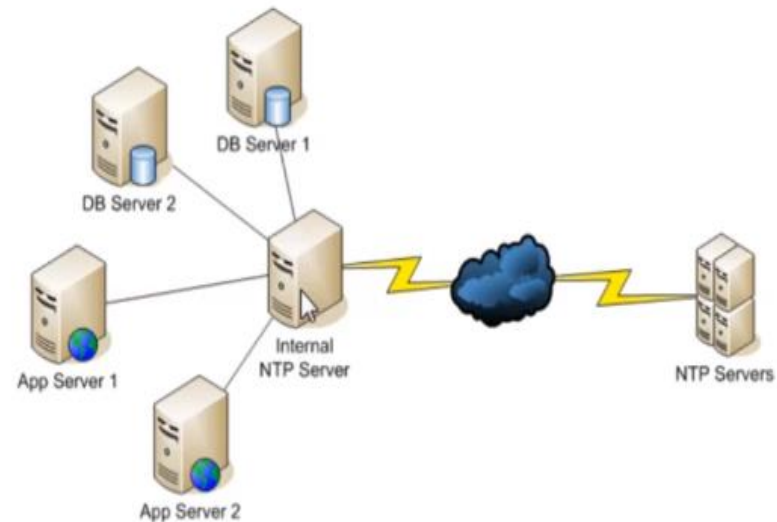
## Section v- Windows Updates

- Windows Update is a Microsoft service for the Windows families of operating system, which automates downloading and installing software updates over the Internet
- The service delivers software updates for Windows, as well as the various Microsoft antivirus products, including Windows Defender and Microsoft Security Essentials
- The main reasons for update are:
  - Address a specific bug or flaw
  - Improve an OS or application's general stability
  - Fix a security vulnerability
- To access Windows update menu
  - Type settings in the search bar and click "update and security"
- Service
  - Windows Update



## Section VI- NTP Configuration

- The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems
- Time protocols determine how closely two computers' clocks are synchronized. A time protocol is responsible for determining the best available time information and converging the clocks to ensure that a consistent time is maintained on separate systems
- Service name
  - Windows Time





# Commands to configure NTP on Windows 2016

- To configure Windows Time Service

Type the following command on powershell:

```
W32tm /config /manualpeerlist:pool.ntp.org /syncfromflags:MANUAL
```

- ❑ Use the command to stop the service:

```
Stop-service w32time
```

- ❑ Use the command to start the service:

```
Start-service w32time
```

Now the Windows Server 2016 is an NTP client of pool.ntp.org and its time/clock is synced with the NTP pool servers (The server is at the same time the NTP server for other domain client systems).

Then go to the client machines and run the following command on PowerShell to force them to sync their time/clock with the domain controller on the Windows Server 2016

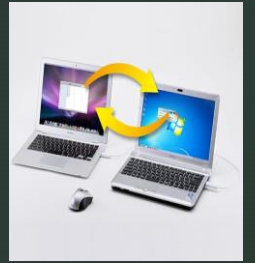
- ❑ `w32tm /resync`

You can check the time synchronization status using the following command.

- ❑ `w32tm /query /status`



## Section VII- File Transfer Methods




- There are so many ways to transfer files and most common ones are:

- ❖ USB attachment 

- ❖ External drives 

- ❖ CD / DVD 

- ❖ Email 

- ❖ Drop box 

In corporate environment file transfer occur through

- ✓ FTP (command available in dos and powershell)
- ✓ File Sharing (Samba, NFS, etc)
- ✓ 3rd party software (Filezilla, EaseUS, FlashGet etc.)

## Section VIII- FTP Server Installation and Configuration

### What is it?

FTP (File Transfer Protocol) is an abbreviation of File Transfer Protocol. As the name implies, FTP is used to transfer files between machines on a network. You can use FTP to share files between a local PC and a remote server and to access online software archives.

- FTP stands for File Transfer Protocol, it is a standard network protocol used for the transfer of computer files between a client and server on a computer network
- FTP is built on a client-server model architecture using separate control and data connections between the client and the server



We will learn...

- Installation of FTP server
- Configuration and Management of FTP server
- Test connection to the FTP server.

## Section IX- Sharing File System (Samba or NFS)

- File sharing is the practice of distributing or providing access to files and documents over the network
- The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
- The Common Internet File System (CIFS) Protocol is a dialect of SMB



We will learn...

- How to create a folder in C:\Simpson and share that folder
- Configure proper permissions for folder access
- Access the folder from a remote computer

# What's SAMBA

## What is Samba?

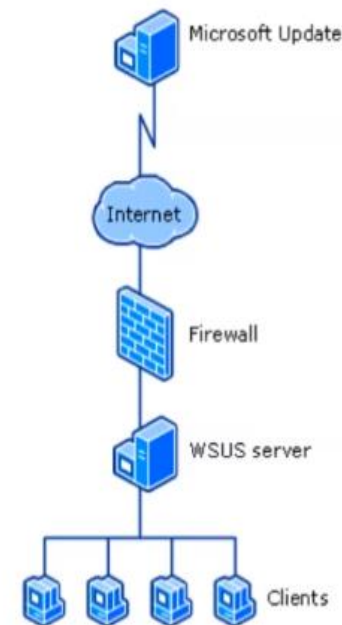
- Free suite of programs that enables flavors of UNIX to work with other operating systems such as OS/2 and Windows, as both a server and a client
- As a server, Samba shares Linux files and printers with Windows systems.
- As a client, Samba gives Linux users access to files on Windows systems

## Section X- WSUS Server Installation and Configuration

- Windows Server Update Services (WSUS), previously known as Software Update Services, is a computer program developed by Microsoft Corporation that enables administrators to manage the distribution of updates and hotfixes released for Microsoft products to computers in a corporate environment
- Purpose = Ease of management and security if clients do not have access to the internet

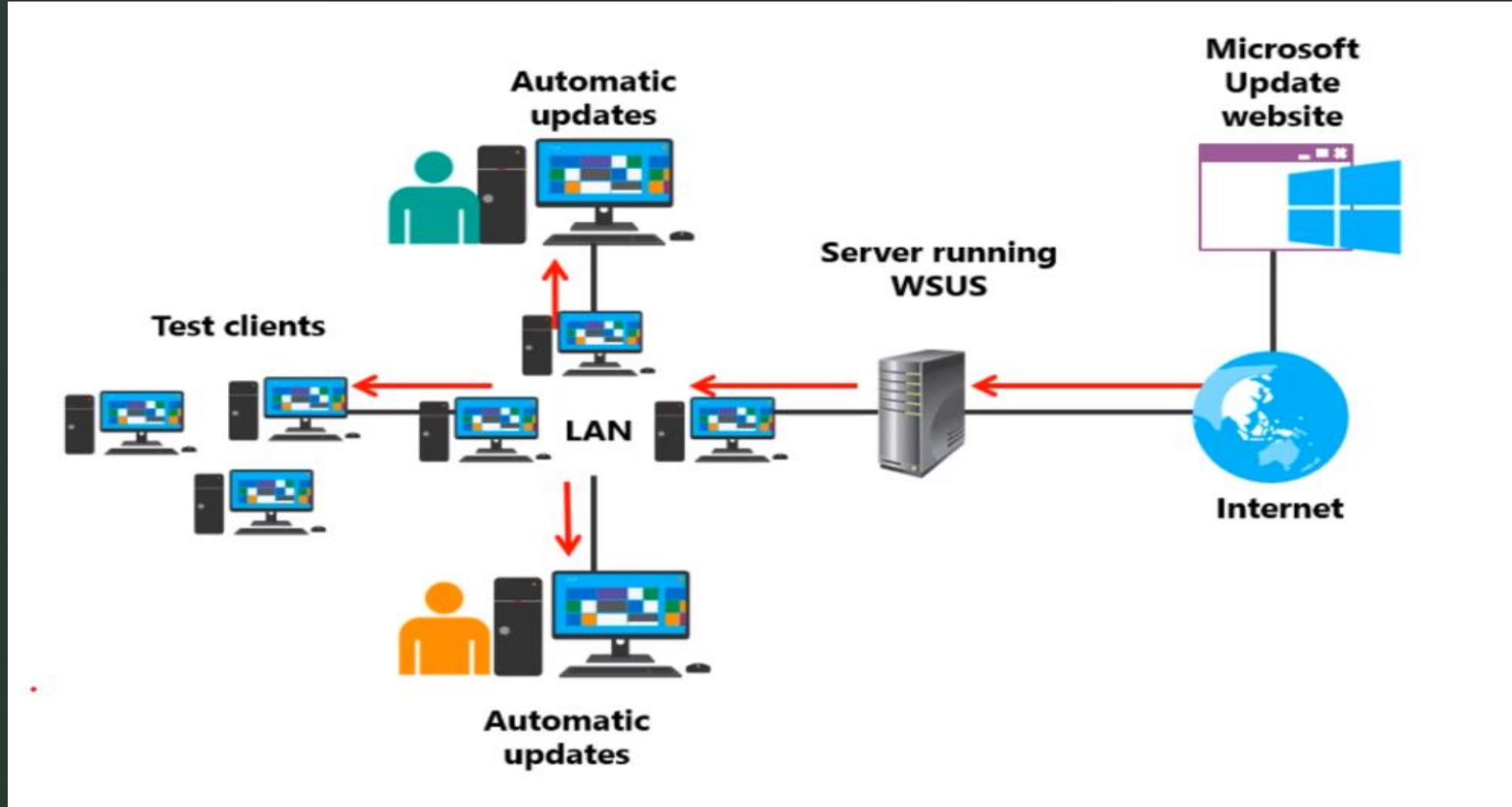
### We will learn...

- Installation of WSUS role and requires features
- Configuration and management of WSUS server

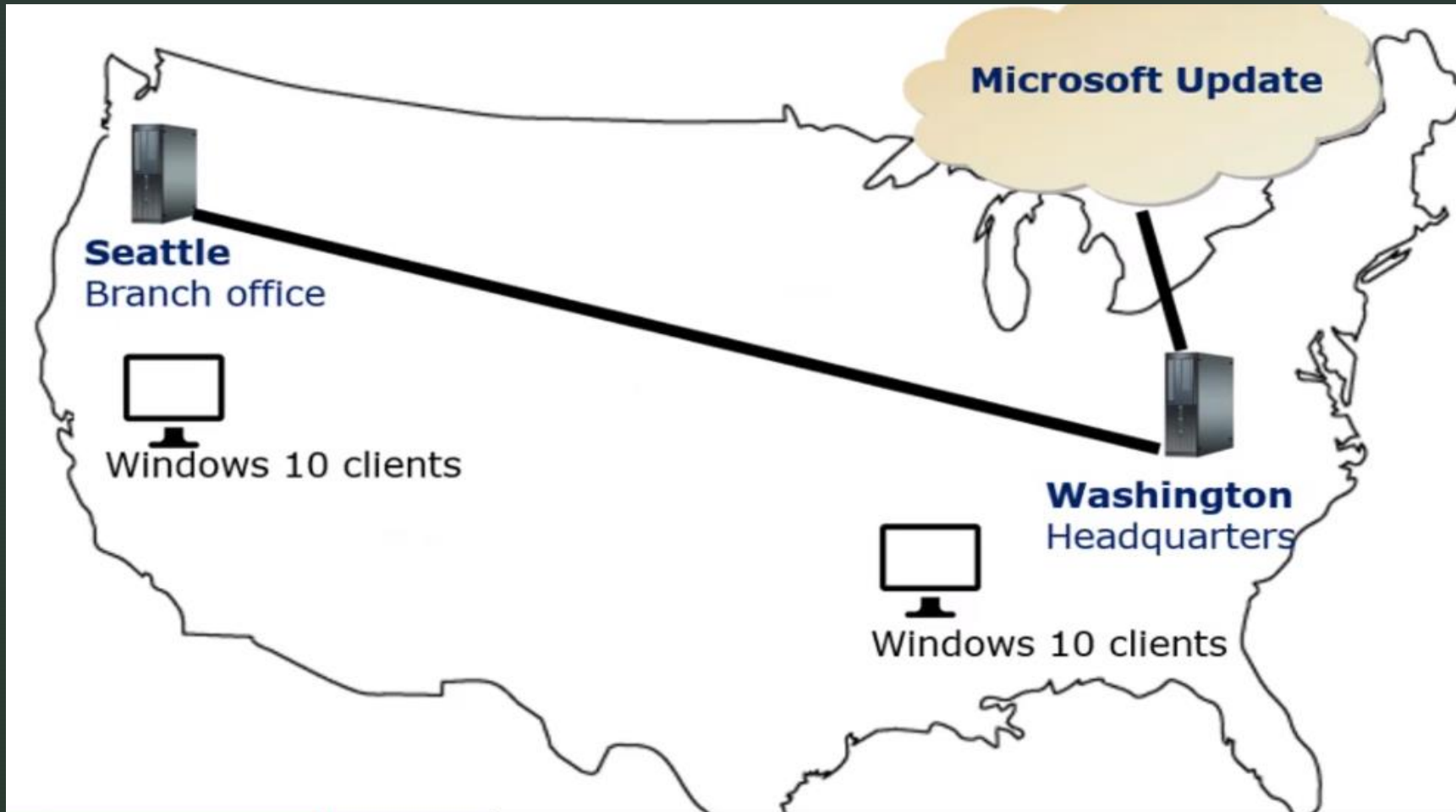




## The benefits of having a WSUS server



# UPSTREAM AND DOWNSTREAM



# WSUS MINIMUM REQUIREMENTS

## Minimum software requirements:

- IIS
- Microsoft .NET Framework 4.6
- Microsoft Report Viewer Redistributable 2008 or newer
- \*SQL Server 2008 R2 SP1 or newer, or Windows Internal Database (WID)

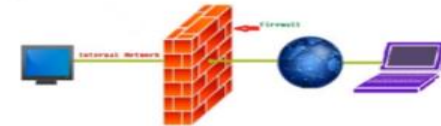
## Minimum hardware requirements:

- X64 1.4 GHz processor
- 2 GB of RAM
- 10 GB available disk space (40 GB recommended)

## Section XI- Windows Firewall

- The **Windows Firewall** is a security application created by **Microsoft** and built into **Windows**, designed to filter network data transmissions to and from your **Windows** system and block harmful communications and/or the programs that are initiating them.

- A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet



**We will learn...**

- How to access Windows Firewall
- How to enable or disable firewall
- How to configure firewall rules

# FIREWALL RULES

- Firewall rules are used to filter network traffic between the local computer and the network. To filter traffic means to allow or block traffic based on the filtering conditions specified in the rule.

Firewall rules in Windows Firewall with Advanced Security can be classified in various ways:

- **Inbound vs. outbound rules** Determines the direction of the rule; that is, whether the rule applies to traffic passing from the network to the local computer or vice versa.
- **Allow vs. block rules** Determines the action the rule takes; that is, whether the traffic specified by the rule will be permitted or not.
- **Allow if secure rules** Indicates another action that a rule can take; namely, that only traffic protected using IPsec will be permitted.
- **Authenticated bypass rules** Overrides blocking rules for properly authenticated traffic (an optional subtype of allow if secure rules).