

SECURING THE SERVER

PREPARED BY



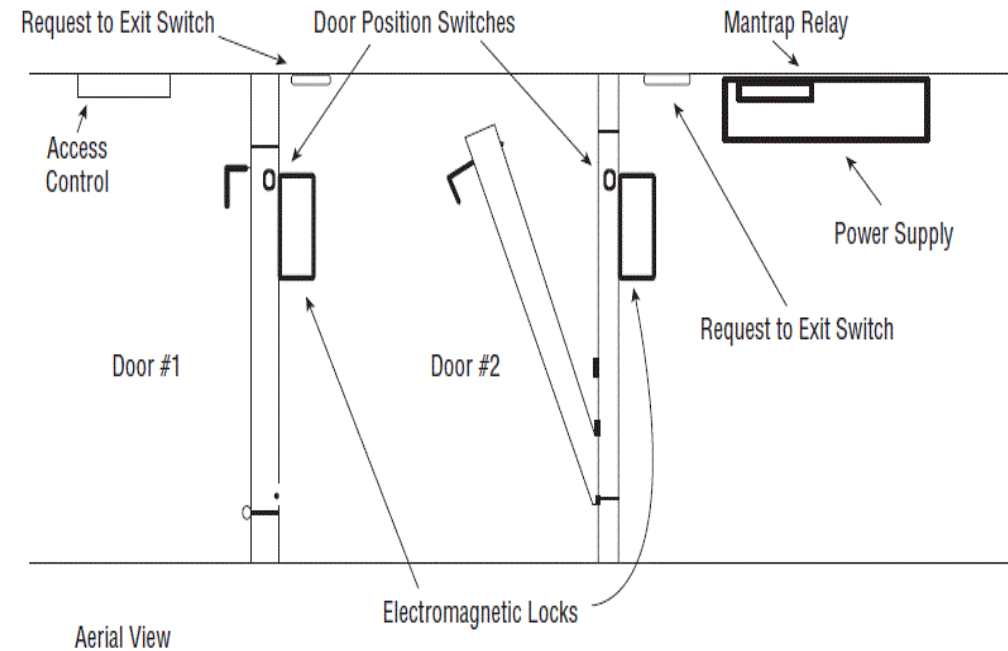
- Physical Security Methods and Concepts
- Server Hardening Techniques

PHYSICAL SECURITY METHODS AND CONCEPTS

- There are many logical security methods that can be used to protect the data on a server, if users can attain physical access to the server, the options available to them to compromise the server increase dramatically.
- **Multifactor Authentication:-** There are three factors of authentication. When more than one of these factors is required to authenticate, it is called multifactor authentication. It is *not* multifactor if it uses two forms of the same factor of authentication.
 - **Something You Have**
 - **Something You Know**
 - **Something You Are**(Prone to False Positive and False Negative)

Security Concepts

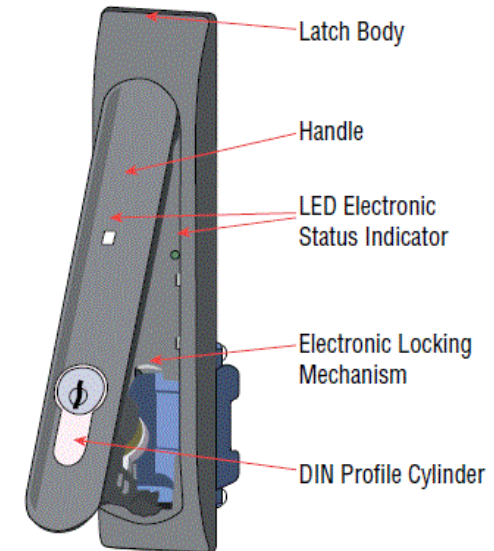
- A **Mantrap** is a series of two doors with a small room between them. The user is authenticated at the first door and then allowed into the room. At that point additional verification will occur (such as a guard visually identifying the person) and then the user is allowed through the second door. Mantraps also typically require that the first door is closed, prior to enabling the second door to open.



- An increasingly popular method of tracking physical assets is to tag them with **radio frequency identification (RFID) chips**. This allows for tracking the location of the asset at any time.
- The main components of this are
 - **RFID Reader** This device has an antenna and an interface to a computer.
 - **Transponder** This is the tag on the device that transmits its presence wirelessly.
- The tags can be one of two types: passive and active.
 - Active tags have batteries whereas
 - passive tags receive their energy from the reader when the reader interrogates the device.

- All users should possess and wear **Identification Cards**, but it becomes even more important when those users have access to the server room.
- Biometric
- Keypad
- Access List
- Security Guard
- Security Camera
- Key and Locks
- Cabinet

Cabinet lock with alarm



SERVER HARDENING TECHNIQUES

- It involves hardening the system **logically**
 - that is, hardening the operating system and applications
 - and hardening the server physically by ensuring the device cannot be tampered with by someone who can touch the server

OS Hardening

Involves a series of steps that should result in a server that offers a minimum of attack points to a hacker.

Stopping Unneeded Services/Closing Unneeded Ports

The easiest way to do this is to install a host firewall on the system and adopt a “disable by default” policy with respect to services. Then manually enable any you need

Installing Only Required Software

You should examine all installed applications and retain only those you need.

Installing Latest Operating System Patches

Always keep the server updated with all operating system patches and service packs.

- **Implementing Application Hardening**

- Applications can have many features and embedded programs that you may not make use of. Determine which of these you require.

- **Installing Latest Patches**

- Applications can have many features and embedded programs that you may not make use of. Determine which of these you require.

- **Disabling Unneeded Services/Roles/Features**

Endpoint Security

- Therefore, the process of providing endpoint security is the process of ensuring that every endpoint (including servers) has been secured in the same way in which you would secure the network gateway.
- There are two main issues to consider when providing endpoint security:
 - Identifying intrusions when they occur and preventing the spread of malware.

A host-based intrusion detection system (HIDS) is installed on the device (for the purpose of our discussion, a server) and the system focuses solely on identifying attacks on that device only.

These systems can use several methods of detecting intrusions.

- **Signature Based** Analyzes traffic and compares patterns, called *signatures*, that reside within the IDS database. This means it requires constant updating of the signature database.
- **Anomaly Based** Analyzes traffic and compares it to normal traffic to determine if the traffic is a threat. This means any traffic out of the ordinary will set off an alert.

There are drawbacks to these systems:

- A high number of false positives can cause a lax attitude on the part of the security team.
- Constant updating of signatures is needed.
- A lag time exists between the release of the attack and the release of the signature.
- An HIDS cannot address authentication issues.
- Encrypted packets cannot be analyzed.
- In some cases, IDS software is susceptible itself to attacks.

Hardware Hardening

- **Disabling Unneeded Hardware and Physical Ports/Devices**

The closing of any software ports that are not in use is part of digital hardening, but the disabling of any physical ports or connections on the server is a part of physical hardening.

Some of the items that should be considered for disabling are

USB ports

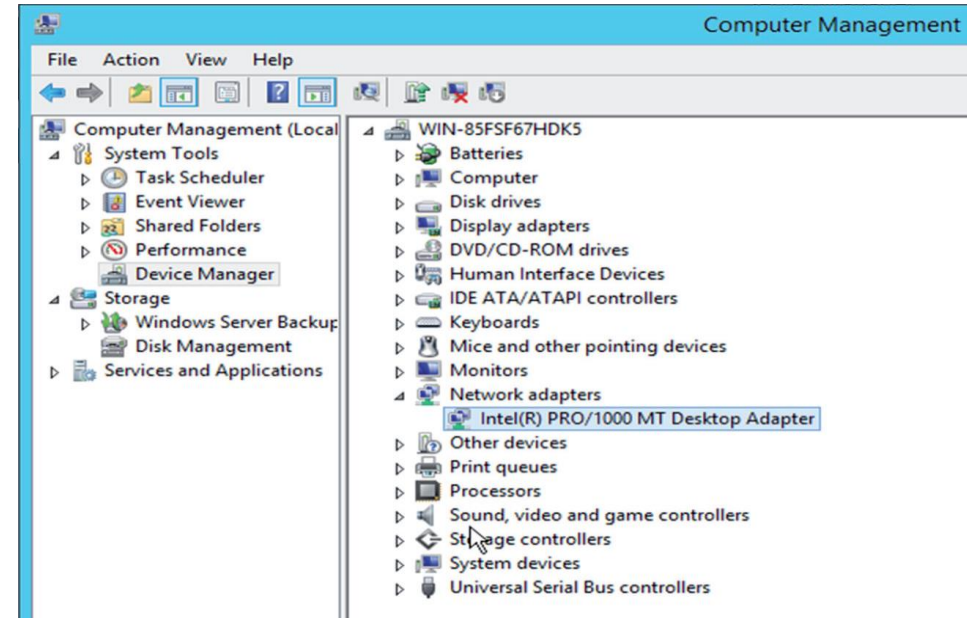
NICs

Serial ports

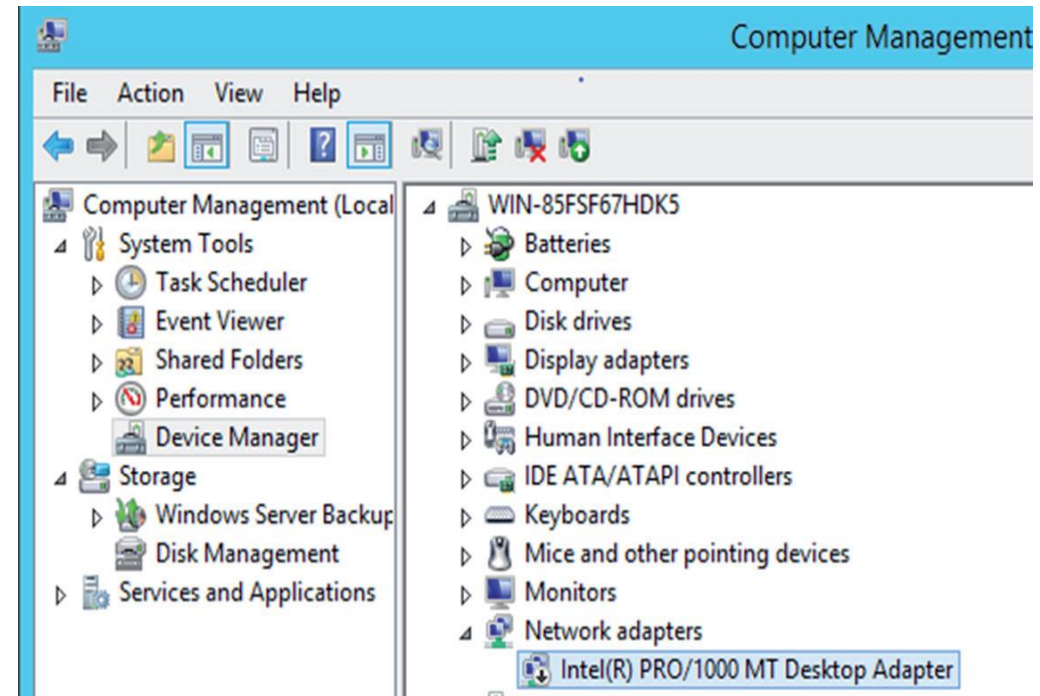
Firmware ports

Disabling the Network Adaptor in Windows Server 2012 R2

1. Open the Server Manager tool if it is not already open.
2. From the Tools menu select Computer Management.
3. In the Computer Management console select Device Manager.
4. Locate and expand the Network Adaptors device category as shown in fig

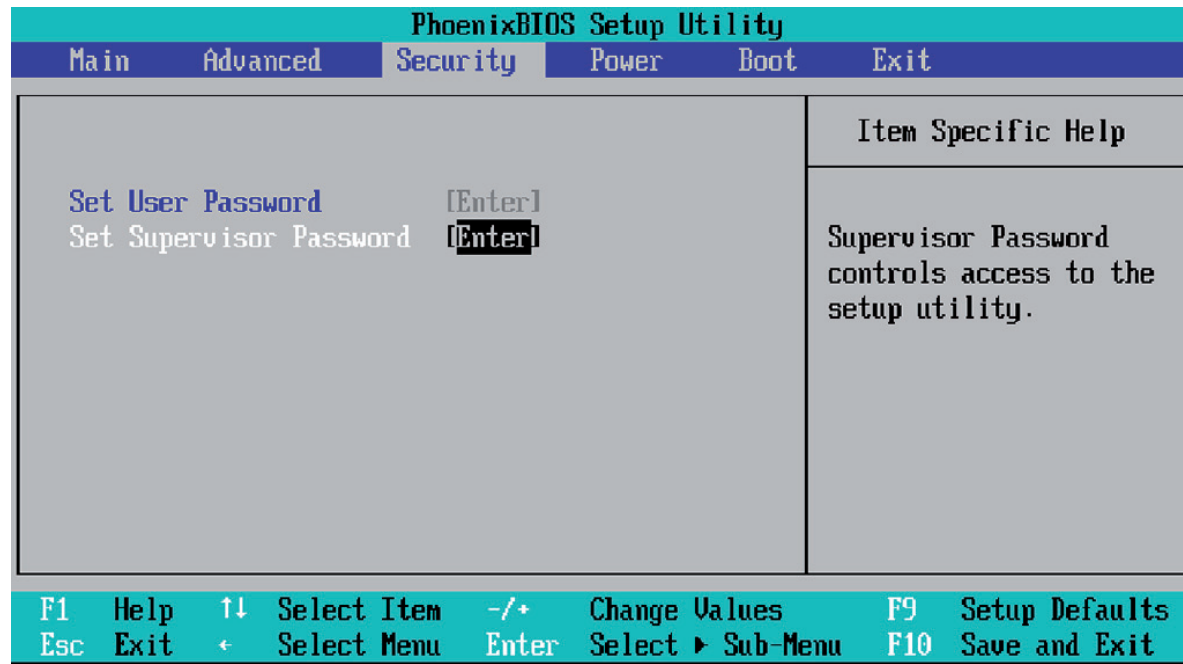


5. Right click the network adaptor you wish to disable (this server has only one, but your server may have more than one) and select Disable from the menu.
6. You can verify your work by looking for the black down arrow next to the adaptor as shown in Figure



BIOS Password

- This can prevent someone with physical access to the server from booting to the BIOS, changing the boot order, and enabling a boot device for the purpose of booting to an external OS that they can use to take data off the hard drive.



Which authentication mechanism is an example of something you have?

- A.** Password
- B.** Username
- C.** Smart card
- D.** Retina scan

Which authentication mechanism is an example of something you have?

- A. Password
- B. Username
- C. Smart card**
- D. Retina scan

Which of the following is *not* a drawback of using active RFID chips?

- A.** The tag signal can be read by any reader in range.
- B.** The tag signal can only go a few feet.
- C.** Multiple readers in an area can interfere with one another.
- D.** Multiple devices can interfere with one another when responding.

Which of the following is *not* a drawback of using active RFID chips?

- A. The tag signal can be read by any reader in range.
- B. The tag signal can only go a few feet.**
- C. Multiple readers in an area can interfere with one another.
- D. Multiple devices can interfere with one another when responding.

Which of the following is not true of an HIDS?

- A.** A high number of false positives can cause a lax attitude on the part of the security team.
- B.** An HIDS cannot address authentication issues.
- C.** Encrypted packets cannot be analyzed.
- D.** An HIDS monitors all traffic that goes through it looking for signs of attack on any machine in the network.

Which of the following is not true of an HIDS?

- A. A high number of false positives can cause a lax attitude on the part of the security team.
- B. An HIDS cannot address authentication issues.
- C. Encrypted packets cannot be analyzed.
- D. An HIDS monitors all traffic that goes through it looking for signs of attack on any machine in the network.**

Which of the following is *not* an example of physical hardening of the server?

- A.** Disabling USB ports
- B.** Implementing strong authentication to log into the server
- C.** Installing locks on server racks
- D.** Installing locks on the server room door

Which of the following is *not* an example of physical hardening of the server?

- A. Disabling USB ports
- B. Implementing strong authentication to log into the server**
- C. Installing locks on server racks
- D. Installing locks on the server room door

Basic Network Security Systems and Protocols

- **Firewall** are used to filter out unwanted traffic while allowing desired traffic.
- **Network-Based** firewalls are one of the first lines of defence in a network. There are different types of firewalls, and they can either be standalone systems or they can be included in other devices such as routers or servers.

Firewalls function as one or more of the following:

- ■ Packet filter
- ■ Proxy firewall
- ■ Stateful inspection firewall

- **Packet Filter Firewalls** A firewall operating as a *packet filter* passes or blocks traffic to specific addresses based on the type of application. The packet filter doesn't analyze the data of a packet; it decides whether to pass it based on the packet's addressing information.
- A **Proxy firewall** can be thought of as an intermediary between your network and any other network. Proxy firewalls are used to process requests from an outside network and those outbound from inside the network.(This Process includes hiding IP addresses).
- **Stateful inspection** is also referred to as stateful packet filtering. Most of the devices used in networks don't keep track of how information is routed or used.

How Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associated action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

Configure Security Protocols

Procedure

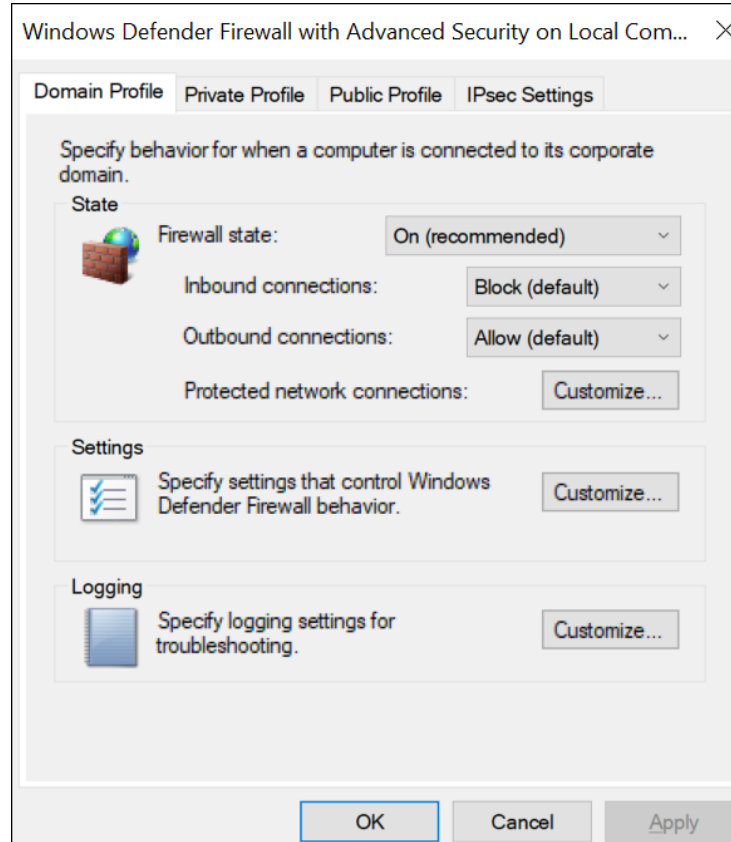
1.Run `wf.msc`.

The **Windows Defender Firewall with Advanced Security** window appears.

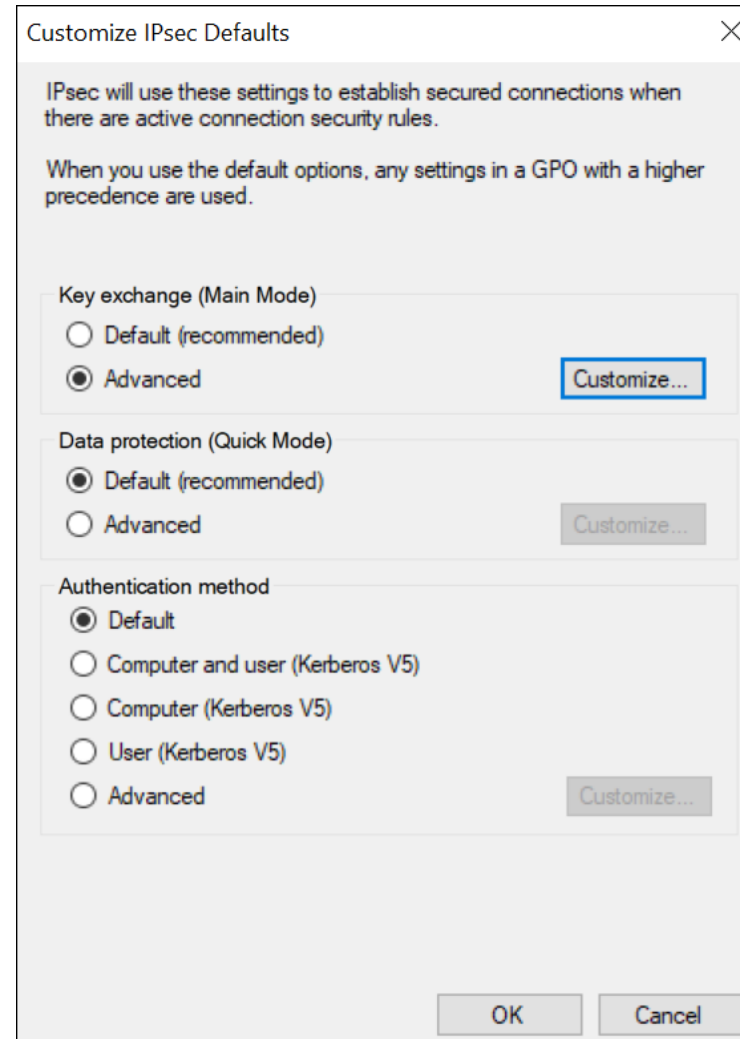
2.Create a security method:

a.Select **Actions > Properties**.

The **Windows Defender Firewall with Advanced Security on Local Computer** window appears.



b. Select **IPsec Settings > Customize**.
The **IPsec Defaults** window appears.



c. Under **Key exchange (Main Mode)**, select **Advanced > Customize**.
The **Customize Advanced Key Exchange Settings** window appears.

The screenshot shows a Windows-style dialog box titled "Customize Advanced Key Exchange Settings". It contains three main sections: "Security methods", "Key lifetimes", and "Key exchange options".

Security methods

Use the following security methods for key exchange.
Those higher in the list are tried first.

Security methods:

Integrity	Encryption	Key exchange algorithm
SHA-1	AES-CBC 128	Diffie-Hellman Group 2 (default)
SHA-1	3DES	Diffie-Hellman Group 2

Below the table are three buttons: "Add..." (highlighted with a blue border), "Edit...", and "Remove".

Key lifetimes

Specify when a new key is generated. If you select both options, a new key is generated when the first threshold is reached.

Minutes: 480

Sessions: 0

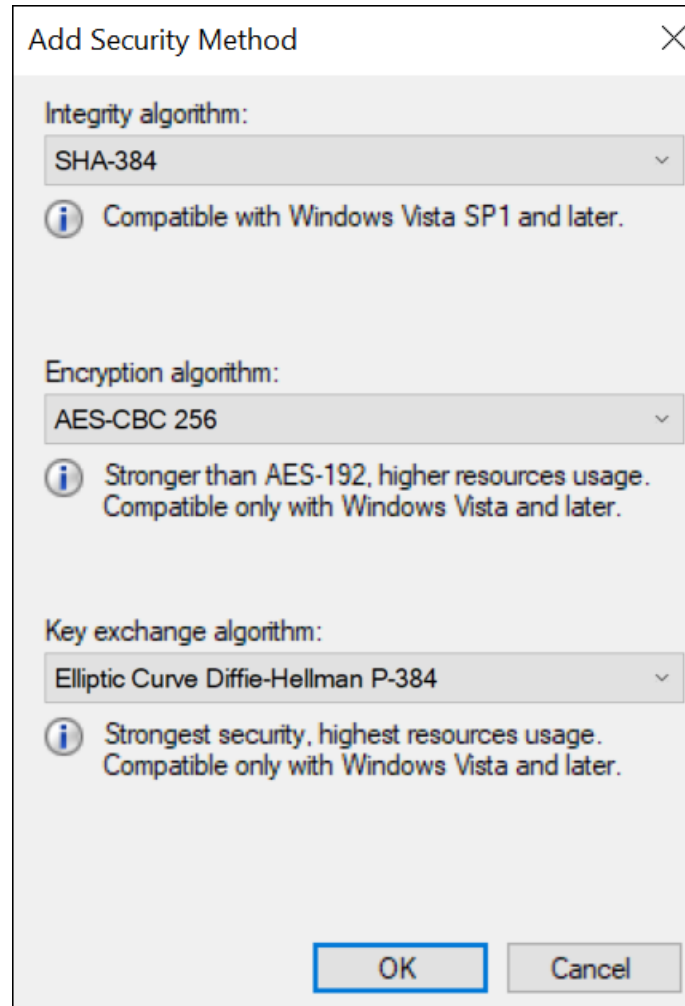
Key exchange options

☐ Use Diffie-Hellman for enhanced security.

Compatible with Windows Vista and later.

At the bottom right are "OK" and "Cancel" buttons.

- d. Select **Add**. The **Add Security Method** window appears.
- e. Select the algorithms that you want to use for each purpose. The following image shows an example.



The security method that you have added appears in the list.

Customize Advanced Key Exchange Settings

Security methods

Use the following security methods for key exchange.
Those higher in the list are tried first.

Security methods:

Integrity	Encryption	Key exchange algorithm
SHA-1	AES-CBC 128	Diffie-Hellman Group 2 (default)
SHA-1	3DES	Diffie-Hellman Group 2
SHA-384	AES-CBC 256	Elliptic Curve Diffie-Hellman P-384

Add... Edit... Remove

Key lifetimes

Specify when a new key is generated. If you select both options, a new key is generated when the first threshold is reached.

Minutes: 480

Sessions: 0

Key exchange options

☐ Use Diffie-Hellman for enhanced security.

Compatible with Windows Vista and later.

OK Cancel

- f. Move the security method that you have added to the top of the list. We recommend that you remove the other methods.
- g. Select **OK**.
- 3. Add integrity and encryption algorithms:
 - a. In the **Customize IPsec Defaults** window, under **Data protection (Quick Mode)**, select **Advanced > Customize**. The **Customize Data Protection Settings** window appears.

Customize Data Protection Settings

Data protection settings are used by connection security rules to protect network traffic.

☐ Require encryption for all connection security rules that use these settings

Data integrity

Protect data from modification on the network with these integrity algorithms. Those higher in the list are tried first.

Data integrity algorithms:

Protocol	Integrity	Key Lifetime (minutes/KB)
ESP	SHA-1	60/100,000
AH	SHA-1	60/100,000

Add... **Edit...** **Remove**

Data integrity and encryption

Protect data from modification and preserve confidentiality on the network with these integrity and encryption algorithms. Those higher in the list are tried first.

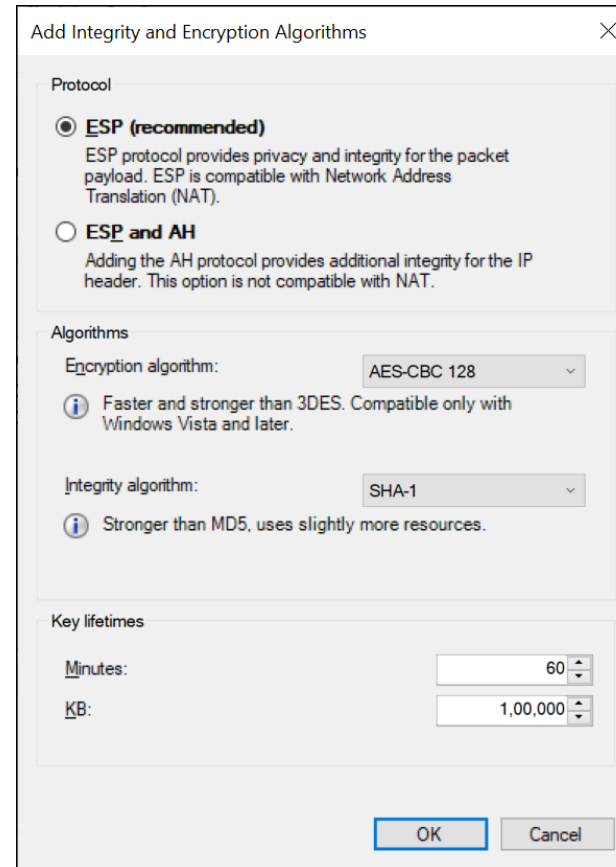
Data integrity and encryption algorithms:

Protocol	Integrity	Encryption	Key Lifetime (mi...
ESP	SHA-1	AES-CBC...	60/100,000
ESP	SHA-1	3DES	60/100,000

Add... **Edit...** **Remove**

OK **Cancel**

-
- b. Select the **Require encryption for all connection and security rules that use these settings** check box.
- c. Under **Data integrity and encryption**, select **Add**. The **Add Integrity and Encryption Algorithms** window appears.



The screenshot shows a dialog box titled "Add Integrity and Encryption Algorithms" with a close button (X) in the top right corner. The dialog is divided into three sections: "Protocol", "Algorithms", and "Key lifetimes".

Protocol: This section contains two radio button options. The first option, "ESP (recommended)", is selected and includes a description: "ESP protocol provides privacy and integrity for the packet payload. ESP is compatible with Network Address Translation (NAT)." The second option, "ESP and AH", is unselected and includes a description: "Adding the AH protocol provides additional integrity for the IP header. This option is not compatible with NAT."

Algorithms: This section contains two dropdown menus. The "Encryption algorithm:" dropdown is set to "AES-CBC 128" and has an information icon (i) next to it with the text: "Faster and stronger than 3DES. Compatible only with Windows Vista and later." The "Integrity algorithm:" dropdown is set to "SHA-1" and also has an information icon (i) next to it with the text: "Stronger than MD5, uses slightly more resources."

Key lifetimes: This section contains two input fields. The "Minutes:" field is set to "60" and the "KB:" field is set to "1,00,000". Both fields have up and down arrows for adjustment.

At the bottom right of the dialog are two buttons: "OK" and "Cancel".

- d. Under **Protocol**, ensure that **ESP** is selected.
 - e. Select the algorithms that you want to use for each purpose, and then select **OK**.
- The algorithms that you have selected appear in the list.
- f. Move the algorithms to the top of the list. We recommend that you remove the remaining items in the list.
 - g. Select **OK**.
4. Create a first authentication method:
- a. In the **Customize IPsec Defaults** window, under **Authentication Method**, select **Advanced > Customize**.
- The **Customize Advanced Authentication Methods** window appears.

Customize Advanced Authentication Methods

First authentication
Specify computer authentication methods to use during IPsec negotiations. Those higher in the list are tried first.

First authentication methods:

Method	Additional Information
Computer (Kerberos ...	

Add... Edit... Remove

☐ First authentication is optional

Second authentication
Specify user authentication methods or a health certificate to use during IPsec negotiations. Those higher in the list are tried first.

Second authentication methods:

Method	Additional Information
--------	------------------------

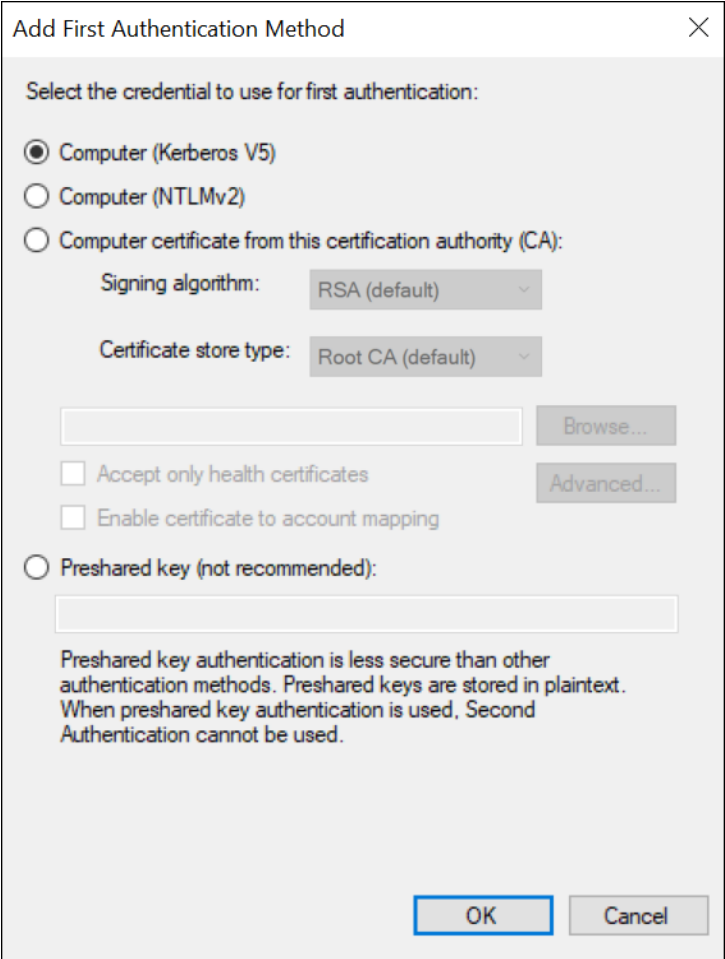
Add... Edit... Remove

☐ Second authentication is optional

A second authentication cannot be specified when a preshared key is in the first authentication methods list.

OK Cancel

b. Under **First authentication methods**, select **Add**.The **Add First Authentication Method** window appears.



The image shows a Windows dialog box titled "Add First Authentication Method". It contains three radio button options for selecting a credential. The first option, "Computer (Kerberos V5)", is selected. The second option is "Computer (NTLMv2)". The third option is "Computer certificate from this certification authority (CA):", which is expanded to show a "Signing algorithm" dropdown set to "RSA (default)", a "Certificate store type" dropdown set to "Root CA (default)", a text box with a "Browse..." button, and two checkboxes: "Accept only health certificates" and "Enable certificate to account mapping", both of which are unchecked. There is also an "Advanced..." button. The fourth option is "Preshared key (not recommended):", which is expanded to show a text box and a warning message: "Preshared key authentication is less secure than other authentication methods. Preshared keys are stored in plaintext. When preshared key authentication is used, Second Authentication cannot be used." At the bottom right are "OK" and "Cancel" buttons.

Add First Authentication Method

Select the credential to use for first authentication:

☒ Computer (Kerberos V5)

☐ Computer (NTLMv2)

☐ Computer certificate from this certification authority (CA):

Signing algorithm: RSA (default)

Certificate store type: Root CA (default)

Browse...

☐ Accept only health certificates Advanced...

☐ Enable certificate to account mapping

☐ Preshared key (not recommended):

Preshared key authentication is less secure than other authentication methods. Preshared keys are stored in plaintext. When preshared key authentication is used, Second Authentication cannot be used.

OK Cancel

-
- c. Provide the CA certificate that you want to use, and then select **OK**. The certificate that you have provided appears in the list.
 - d. Move the certificate to the top of the list. We recommend that you remove the remaining items in the list.
 - e. Select **OK**.

5. Create a connection security rule:

For Windows x86, run the following set of commands to create a rule:

```
netsh advfirewall
```

```
consec
```

```
add rule name=""<rule name>"" endpoint1=any endpoint2=any protocol=tcp port1=any port2=2010
```

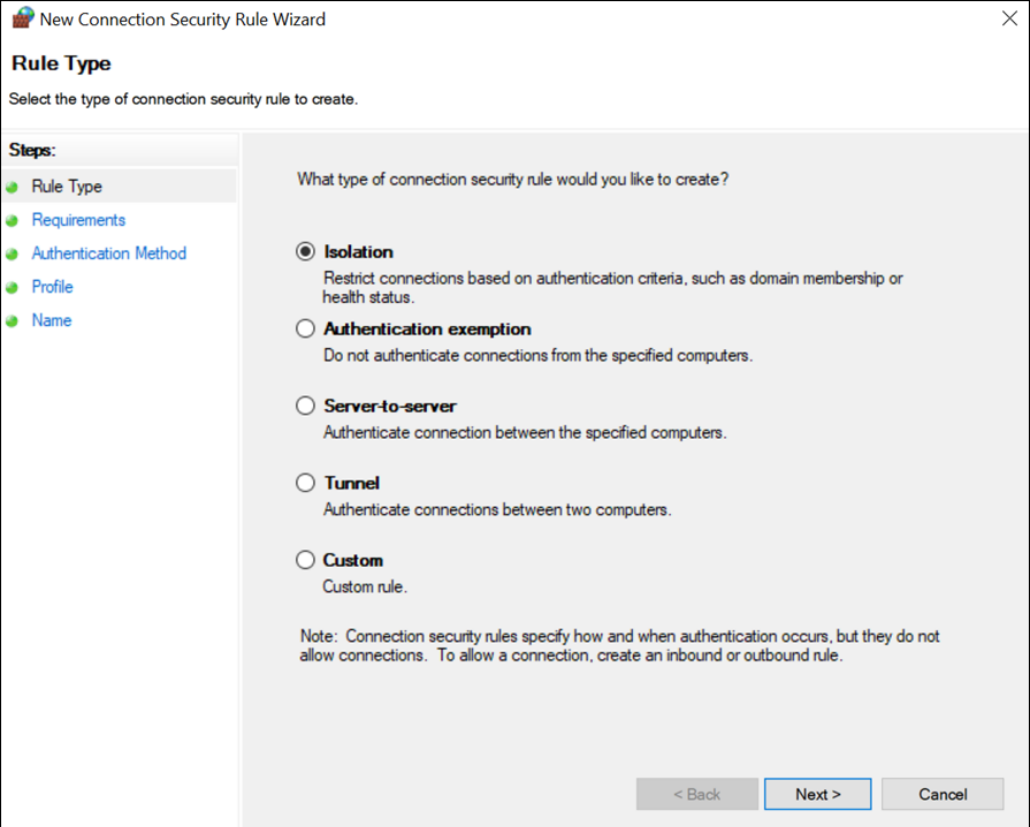
```
action=requestinrequestout
```

For other versions, perform the following steps:

a. In the **Windows Defender Firewall with Advanced Security** window, select **Connection Security Rules**.

b. Select **Actions > New Rule**.

The **New Connection Security Rule Wizard** window appears.



The screenshot shows the 'New Connection Security Rule Wizard' window. The title bar reads 'New Connection Security Rule Wizard'. The main heading is 'Rule Type' with the instruction 'Select the type of connection security rule to create.' Below this, a 'Steps:' pane on the left lists five steps: 'Rule Type' (selected with a green dot), 'Requirements', 'Authentication Method', 'Profile', and 'Name'. The main area asks 'What type of connection security rule would you like to create?' and lists five options with radio buttons: 'Isolation' (selected), 'Authentication exemption', 'Server-to-server', 'Tunnel', and 'Custom'. Each option has a brief description. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A note at the bottom states: 'Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.'

New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Requirements
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

☒ **Isolation**
Restrict connections based on authentication criteria, such as domain membership or health status.

☐ **Authentication exemption**
Do not authenticate connections from the specified computers.

☐ **Server-to-server**
Authenticate connection between the specified computers.

☐ **Tunnel**
Authenticate connections between two computers.

☐ **Custom**
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

< Back Next > Cancel

-
- c. Select **Custom**, and then select **Next**.
 - d. Both for Endpoint 1 and Endpoint 2, select **Any IP Address**, and then select **Next**.
 - e. Select **Require authentication for inbound and outbound connections**, and then select **Next**.
 - f. Select **Default**, and then select **Next**.
 - g. Enter values as described in the following table, and then select **Next**.

Field	Description
Protocol type	Select TCP .
Endpoint 1 port	Select All Ports .
Endpoint 2 port	Select Specific Ports , and then enter 2010.

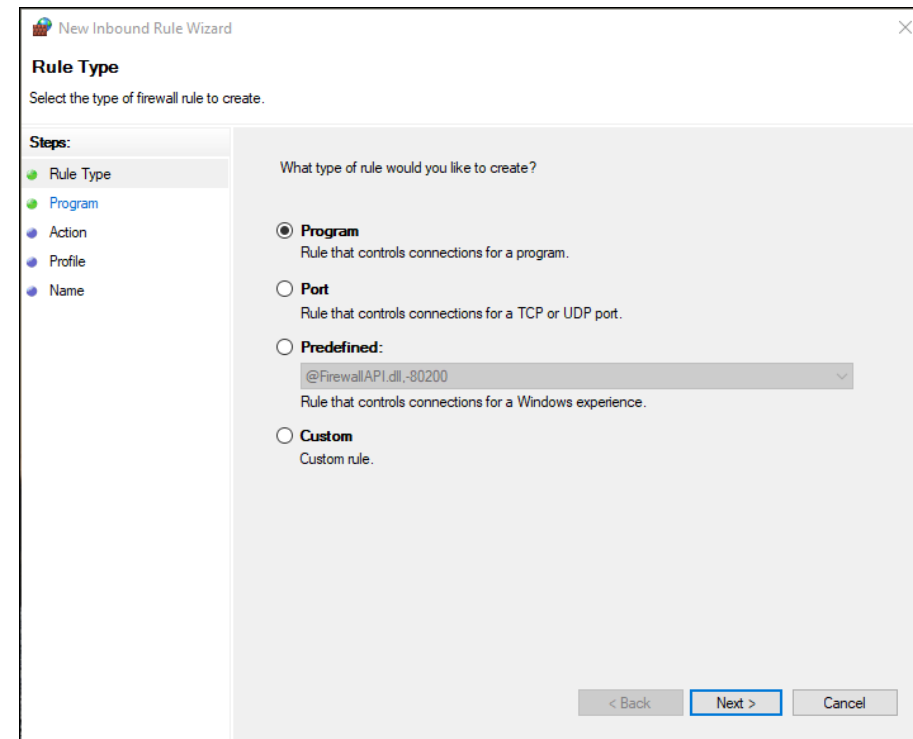
- h. Select when to apply the rule, and then select **Next**.
- i. Enter a name and description for the rule, and then select **Finish**.The rule appears in the **Connection Security Rules** window.
- j. Ensure that the rule is enabled.

6. If using Microsoft Windows Server 2019, 2016, 2012 R2 and/or Windows 8, 8.1, open up port number 5000:

a. In the **Windows Defender Firewall with Advanced Security** window, select **Inbound Rules**.

b. Select **Actions > New Rule**.

The **New Inbound Rule Wizard** window appears.



-
- c. Select **Custom**, and then select **Next**.
 - d. Select **All programs**, and then select **Next**.
 - e. Enter values as described in the following table, and then select **Next**.

Field	Description
Protocol type	Select UDP .
Protocol number	Leave the default value as is.
Local port	Select Specific Ports , and then enter 5000.
Remote port	Leave the default value as is.

- f. Both for the local and remote IP addresses, set the scope to **Any IP address**, and then select **Next**.
 - g. Select **Allow the connection**, and then select **Next**.
 - h. Select when to apply the rule, and then select **Next**.
 - i. Enter a name and description for the rule, and then select **Finish**. The rule appears in the **Inbound Rules** window.
 - j. Ensure that the rule is enabled.
- IPSEC is now configured on the machine.

7. Repeat all the steps above on all the machines that host the Historian server and/or its components/clients.

8. To verify that the IPSEC cryptography is used:

a. Ensure that the Historian server is running.

b. Ensure that the collectors are connected to the Historian server, and that the collectors are running.

c. Specify the tags for data collection. You can do so using [Configuration Hub](#) or [Historian Administrator](#).

d. Verify that the collector is collected data.

e. On each machine on which you configured IPSEC, run `wf.msc`.

The **Windows Defender Firewall with Advanced Security** window appears.

f. Select **Monitoring > Security Associations > Main Mode**.

The **Main Mode** section displays the connection that you have created.

Router Access List

- firewalls can be used to keep unwanted and perhaps malicious traffic types out of the network, and port security and NAC can help keep intruders out of the network, within the network there will be occasions when you don't want to allow communication between certain devices.

In these scenarios, you can use access control lists (ACLs) on the router.

The inherent limitation of ACLs is their inability to detect whether IP spoofing is occurring.

NIDS

- A network-based IDS (NIDS) monitors network traffic on a local network segment. This is in contrast to a host-based IDS (HIDS) that monitors a single machine.
- One of the disadvantages of an NIDS (which is an advantage of an HIDS) is that it cannot monitor any internal activity that occurs within a system, such as an attack against a system that is carried out by logging on to the system's local terminal.

Network Access Control

- Access of users to the network both locally and remotely should be strictly controlled. This can be done at a number of levels of the OSI model, and it can be accomplished in a decentralized or centralized manner:-
 - Port Security
 - 802.1x
 - NAC

Port Security

- Port security applies to ports on a switch, and since it relies on monitoring the MAC addresses of the devices attached to the switch ports, we call it Layer 2 security.

There are several things you can accomplish with port security. It can be used to

- Set the maximum number of MAC addresses that can be seen on a port.
- Define exactly which MAC addresses are allowed on the port.
- Take a specific action when a port violation occurs.

802.1x

- The IEEE 802.1x security standard describes a method of centralizing the authentication, authorization, and accounting of users that connect either locally or remotely to the network.
- It is sometimes called port-based access control because in an 802.1x architecture, the user's port to the network is not opened until the process is complete.
- The 802.1x architecture can be applied to both wireless and wired networks and uses three components:
 1. **Supplicant** The user or device requesting access to the network
 2. **Authenticator** The device through which the supplicant is attempting to access the network
 3. **Authentication Server** The centralized device that performs authentication

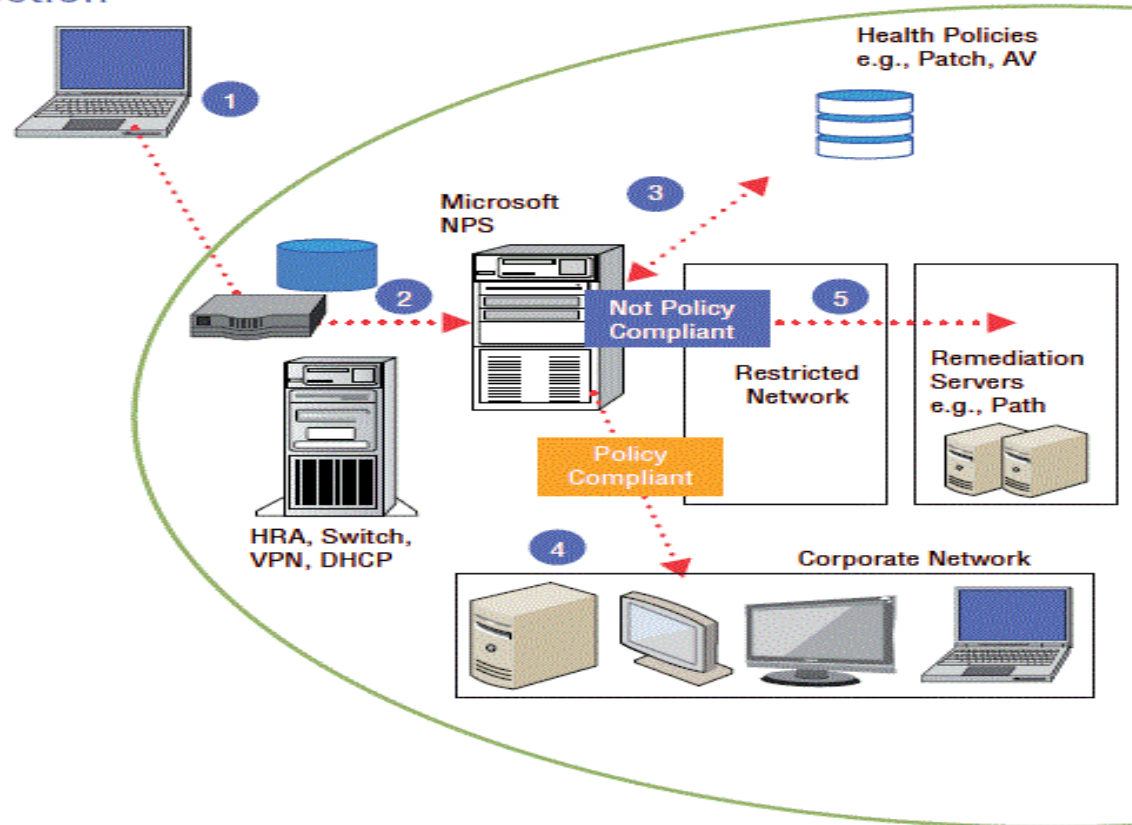
NAC

- Network Access Control (NAC) is a service that goes beyond authentication of the user. NAC includes an examination of the state of the computer the user is introducing to the network when making a remote access or VPN connection to the network.
- These services are called Network Access Protection(NAP) in Microsoft world. The goal to examine all the devices requesting network access for malware, missing security updates any other security issues the device could potentially introduce to network.
- The health state of the device requesting access is collected and sent to the Network Policy Server (NPS), where the state is compared to requirements. If requirements are met, access is granted and if requirements are not met access is usually limited or denied.

Network Access Protection

How it works:

- 1 Access requested.
- 2 Health state sent to NPS (RADIUS).
- 3 NPS evaluates against local health policies.
- 4 If compliant, access granted.
- 5 If not compliant, restricted network access and remediation.



Router Access List

- If you want to prevent users in the Sales subnet from accessing data in the Finance subnet. In these scenarios, you can use access control lists (ACLs) on the router.
- The inherent limitation of ACLs is their inability to detect whether is occurring. **IP spoofing**
- The hacker alters the IP address as it appears in the packet. This can sometimes allow the packet to get through an ACL that is based on IP addresses.
- It also can be used to make a connection to a system that only trusts certain IP addresses or ranges of IP addresses.

NIDS

- A network-based IDS (NIDS) monitors network traffic on a local network segment. This is in contrast to a host-based IDS (HIDS) that monitors a single machine.
- One of the disadvantages of an NIDS (which is an advantage of an HIDS) is that it cannot monitor any internal activity that occurs within a system, such as an attack against a system that is carried out by logging on to the system's local terminal.

PKI

- A public key infrastructure (PKI) includes systems, software, and communication protocols that distribute, manage, and control public key cryptography.
- Users and devices are issued public/private key pairs that are bound to a digital document called a digital certificate. This certificate (more specifically, the keys to which it is bound) can be used for a variety of things, including:-
 - Encrypting Data
 - Authenticating Users and Devices
 - Encrypting Email
 - Digitally Signing Softwares

VPN

- Virtual private network (VPN) connections are remote access connections that allow users to securely connect to the enterprise network and work as if they were in the office.
- These connections use special tunneling protocols that encrypt the information being transferred between the user and the corporate network.
 - Point-to-Point Tunneling Protocol (PPTP)
 - Layer 2 Tunneling Protocol (L2TP)

VLAN

- Virtual local area networks (VLANs) are logical subdivisions of a switch that segregate ports from one another as if they were in different LANs.
- For example, if only one device should be able to connect to the Finance server, the device and the Finance server could be placed in a VLAN separate from the other VLANs.

TABLE 7.1 Advantages of VLANs

Advantages	Disadvantages
Cost: Switched networks with VLANs are less costly than routed networks because routers cost more than switches.	Managerial overhead securing VLANs
Performance: By creating smaller broadcast domains (each VLAN is a broadcast domain), performance improves.	
Flexibility: Removes the requirement that devices in the same LAN (or in this case, VLAN) be in the same location.	
Security: Provides one more layer of separation at Layers 2 and 3.	

Thank you