Chapter 6

Hardening and Security

Tran Thanh Dien, PhD

October, 2020

CANTHO UNIVERSITY

Content

- Security is a top priority for IT
- Windows Firewall
- Windows Defender
- Protecting Data
- Encryption technologies
- Advanced Threat Analytics
- General security best practices

Why bother with security?

"the average number of days an attacker resides in your network before detection is 243!!!"

What are they typically doing during those 243 days? Siphoning all of your data, bit by bit out the back door

There are always new tools and technology coming out that can help you fight off the bad guys!!!

Security is a top priority for IT

CANTHO UNIVERSITY

Attacks ruin reputations

Before: Respected

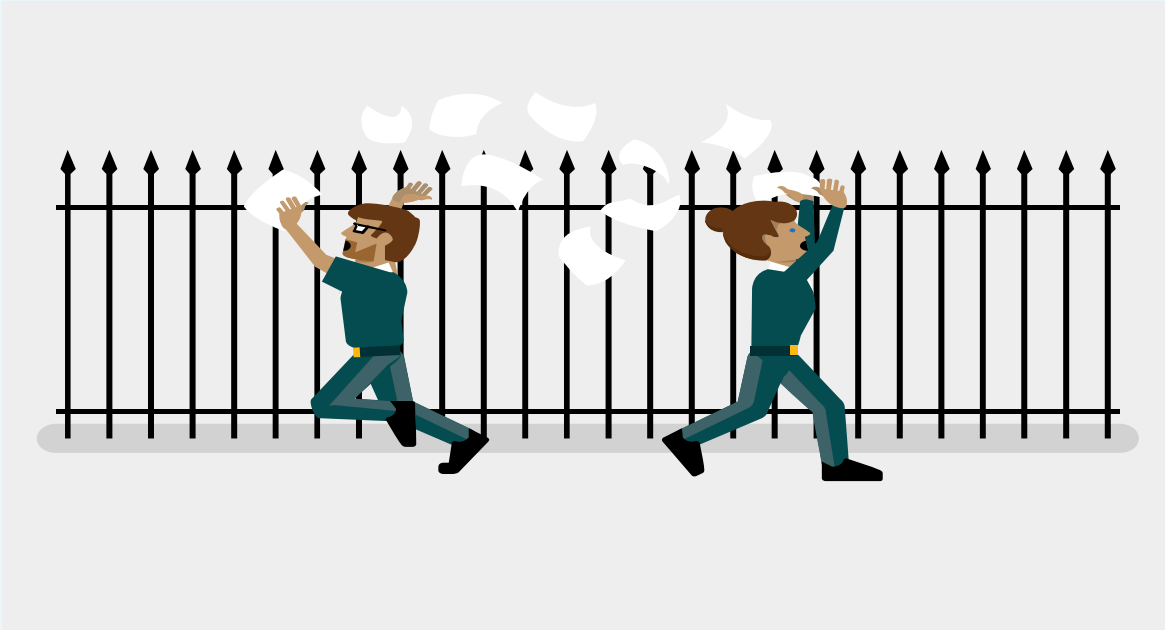
Industry credibility, positive reputation, customer confidence

After: Exposed

Loss of credibility, embarrassing information exposed, customer's lose faith

Attacks affect the IT security team

Before: Focused

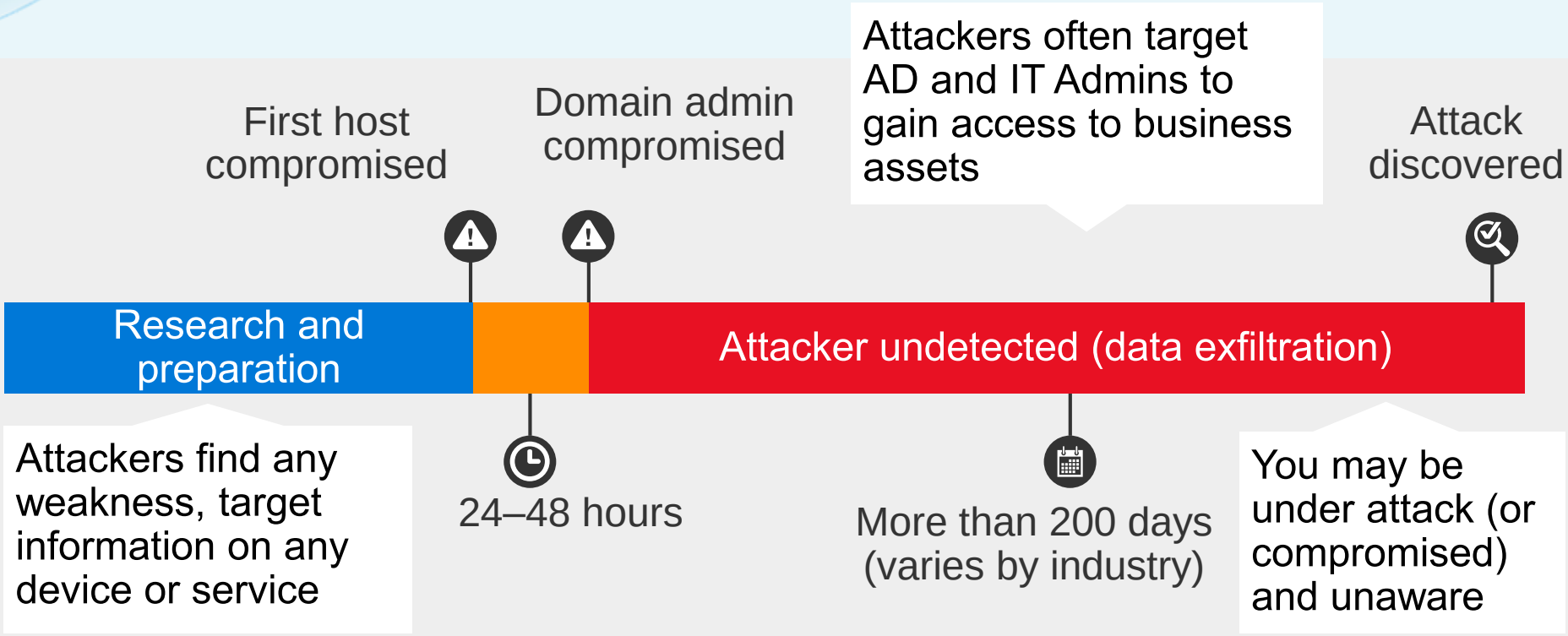


After: Overwhelmed

Well-chosen and dedicated: there was an appropriately sized and dedicated IT Security team

Overwhelmed, where to start? After a breach, the organization may spend more money at the security team, which increases in size.

Attack timeline

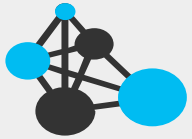


CANTHO UNIVERSITY

Different attack vectors

Attack the applications and infrastructure

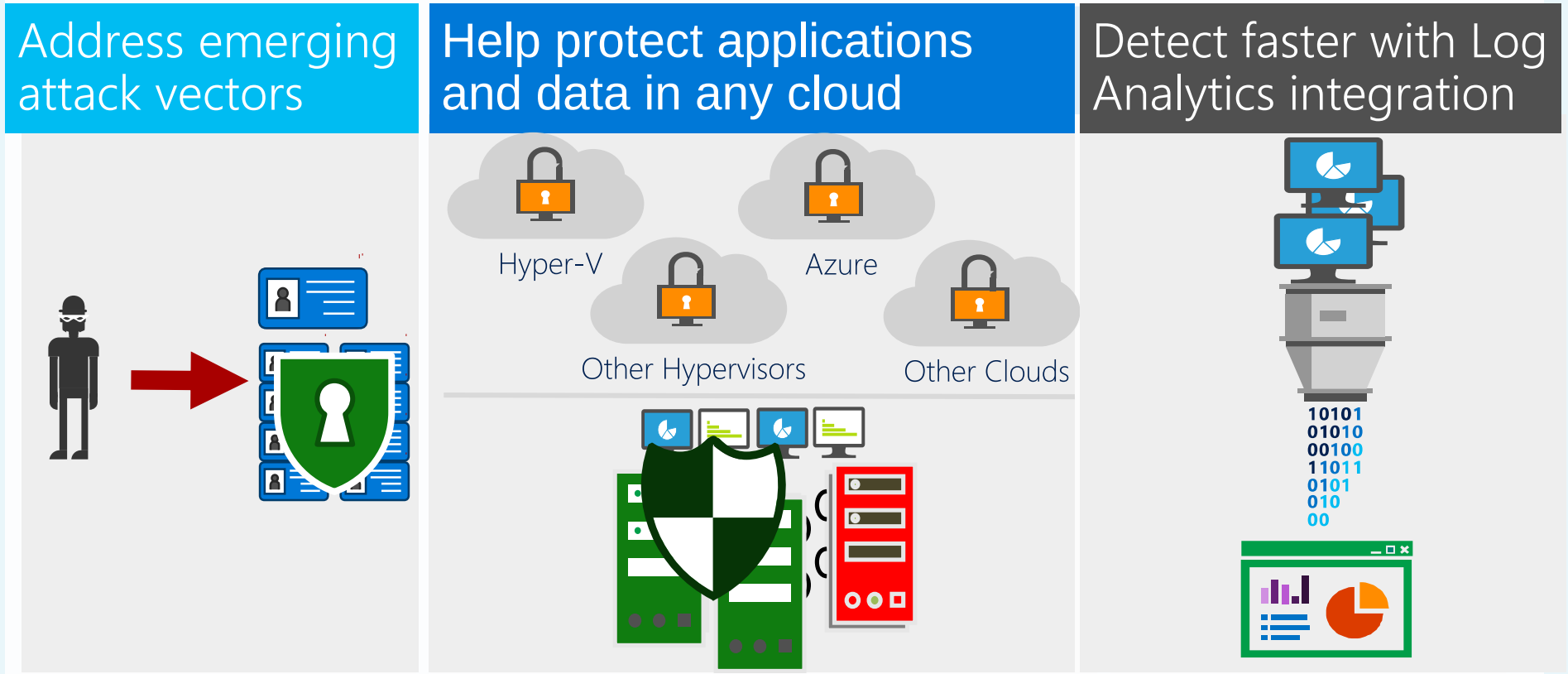
- Compromised privileged accounts
- Unpatched vulnerabilities
- Phishing attacks
- Malware infections



Attack the virtualization fabric

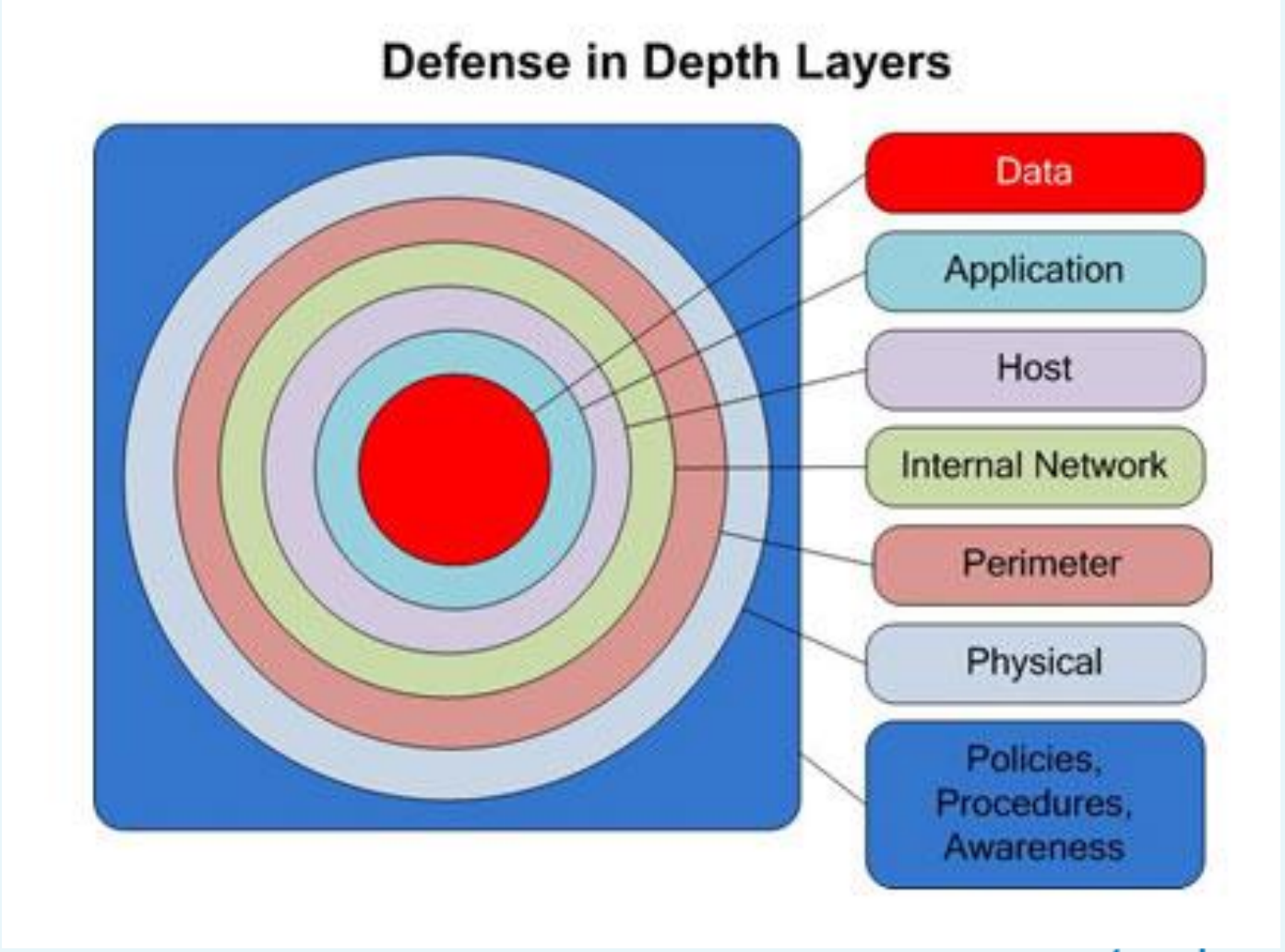
- Compromised fabric exposes guest VMs
- Easy to modify or copy VM without notice
- Can’t protect a VM with gates, walls, locks, etc.
- VMs can’t leverage hardware security (e.g., TPM)

Windows Server 2016: Layers of security

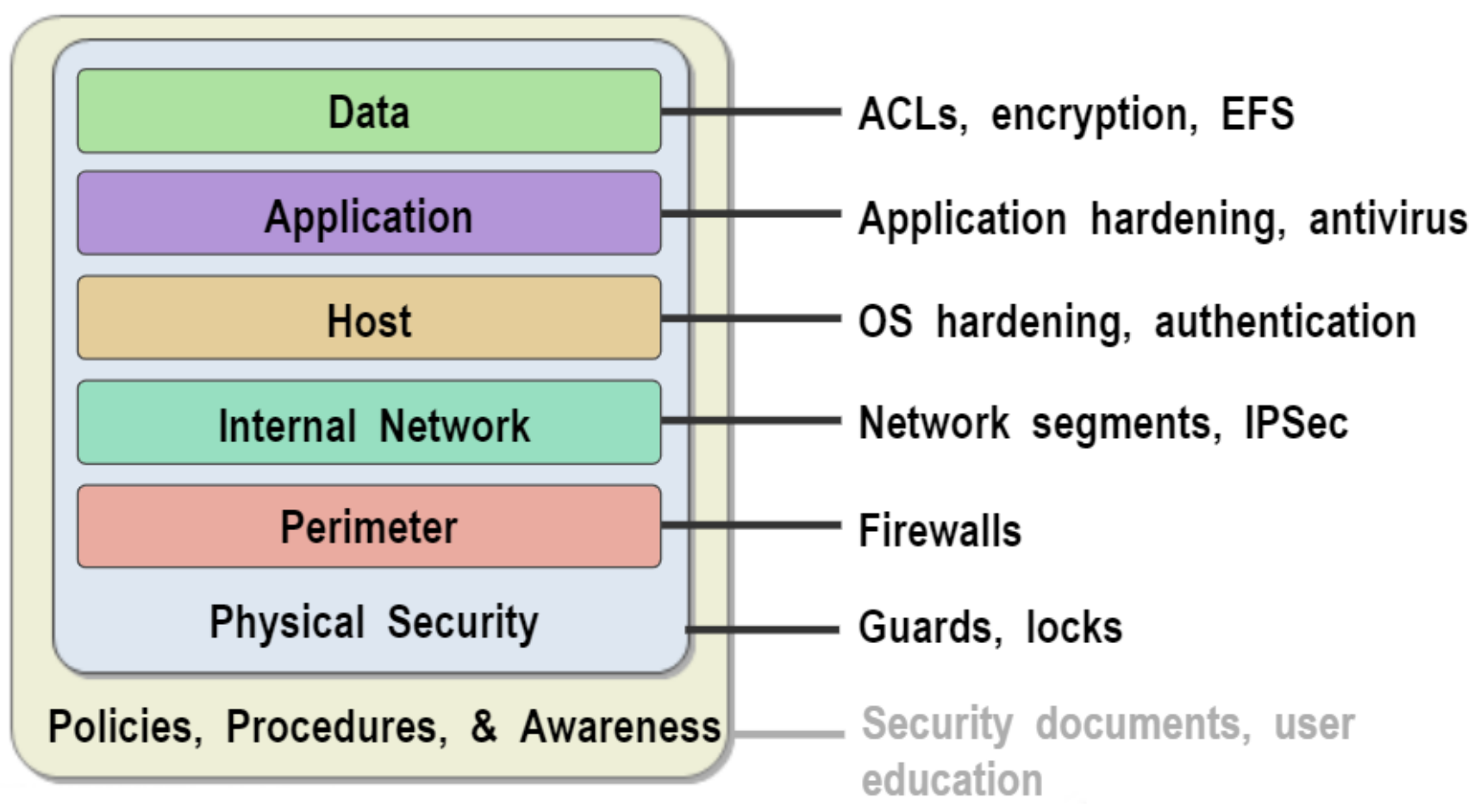


Protect: 1. privileged identity; 2. OS; 3. virtual machines

Defense-in-Depth Model



Defense-in-Depth Model



Defense-in-Depth Model

- **Data:** An attacker's ultimate target, including your databases, Active Directory service information, documents, and so on
- **Application:** The software that manipulates the data that is the ultimate target of attack
- **Host:** The computers that are running the applications
- **Internal Network:** The network in the corporate IT infrastructure

Defense-in-Depth Model

- **Perimeter:** The network that connects the corporate IT infrastructure to another network, such as to external users, partners, or the Internet
- **Physical:** The tangible aspects in computing: the server computers, hard disks, network switches, power, and so on.
- **Policies, Procedures, Awareness**: The overall governing principles of the security strategy of any organization.

Defense-in-Depth Model

Physical Security

- Physical access controls: Keep servers in locked room
- Maintain access logs to document who has had physical access to the servers
- Surveillance of the server room
- Read-Only Domain Controller (RODC)
- Windows BitLocker Drive Encryption and the Encrypting File System (EFS)

Defense-in-Depth Model

Perimeter Security

- VPN, Remote Desktop Protocol (RDP) over HTTPS, DirectAccess,…
- Firewall

Defense-in-Depth Model

Internal Network Security

- Windows Firewall with Advanced Security
- Network Access Protection (NAP)
- Virtual networks
- IPSec

Defense-in-Depth Model

Host Security

- Nano Server: Just enough OS
- OS Hardening
- Authentication

Defense-in-Depth Model

Application Security

- Application Hardening
- Anti-Virus

Defense-in-Depth Model

Data Security

- Encryption: EFS, BitLocker,...
- ACLs
- IPSec
- Active Directory Right Management Service (AD RMS)

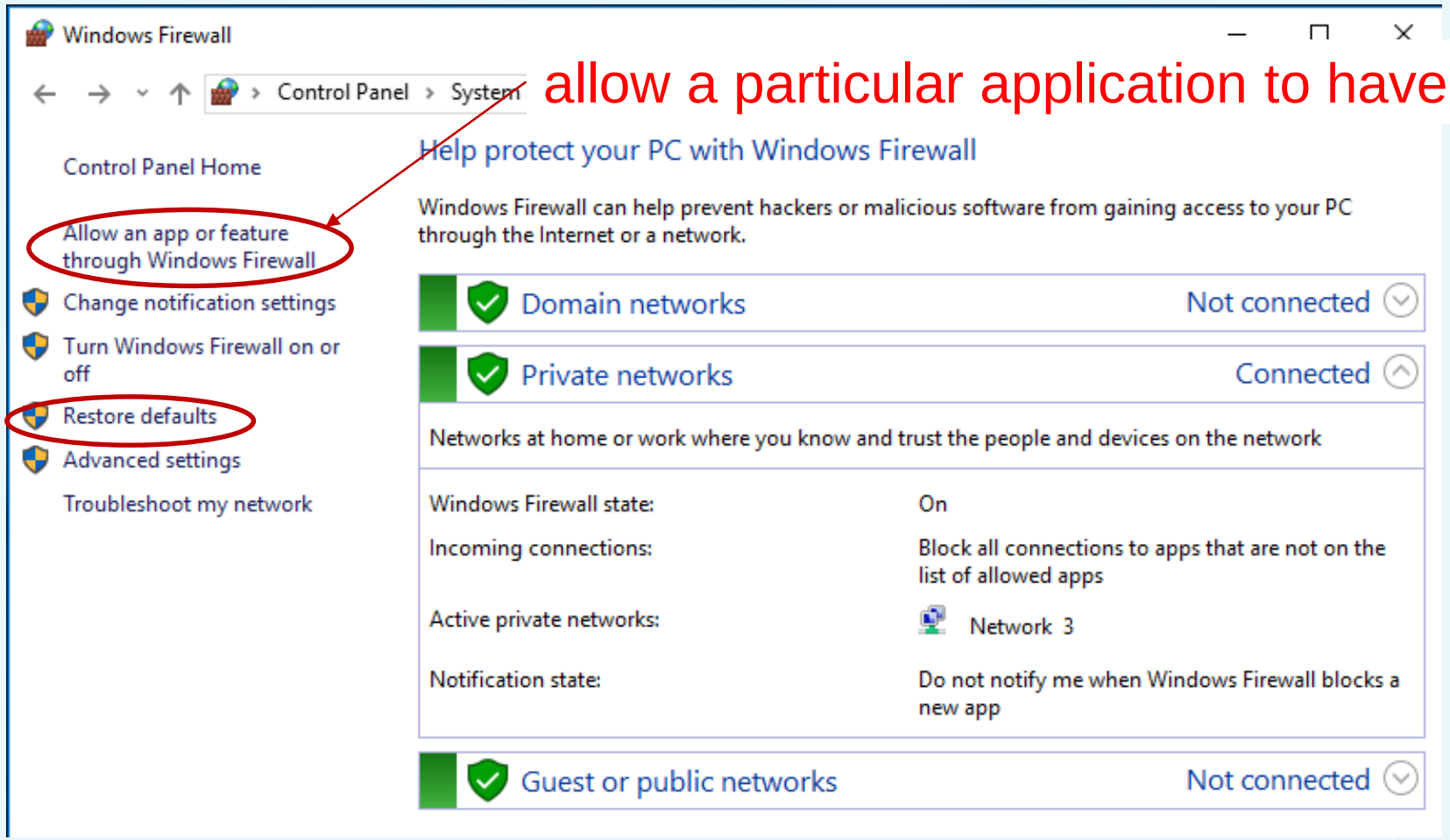
Windows Firewall

Windows Firewall with Advanced Security (WFAS)

- When think of securing devices at the network level, we think of perimeters: firewalls, mostly at a hardware level
- Another layer of firewalling that should be utilized is Windows Firewall!!!!
- Windows operating systems enhance the security architecture with Windows Firewall with Advanced Security (WFAS)

Windows Firewall settings

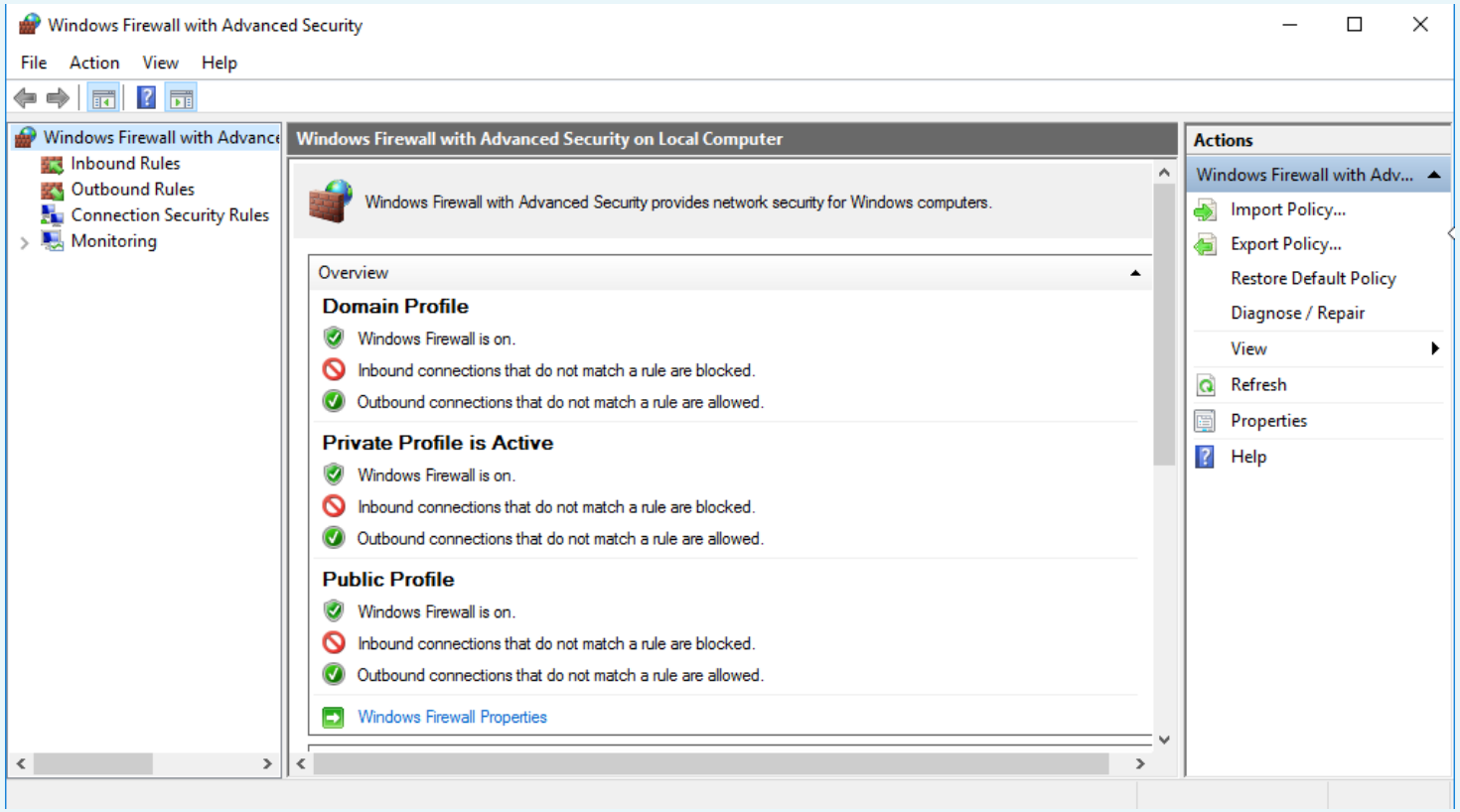
- Control Panel-> System and Security -> Windows Firewall



WFAS

Windows Firewall settings

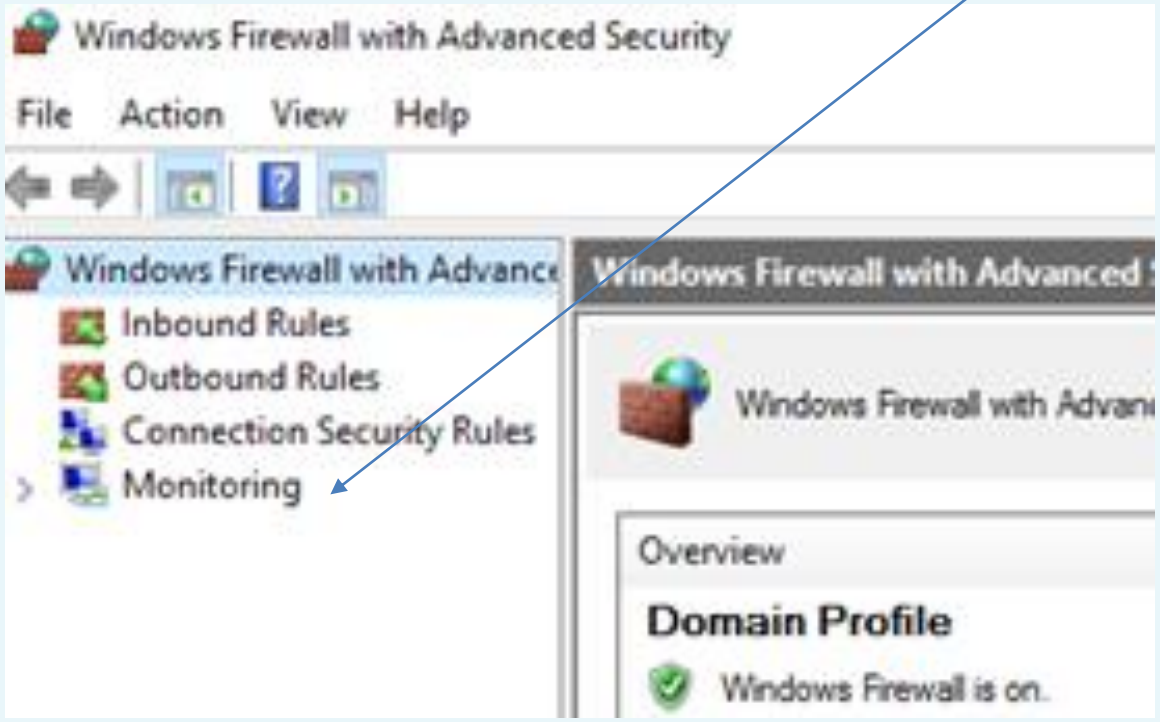
- Click on the Advanced settings link or Start -> Run and type wf.msc to launch WFAS administration console



WFAS

Windows Firewall settings

view actively engaged rules, including **Connection Security Rules**

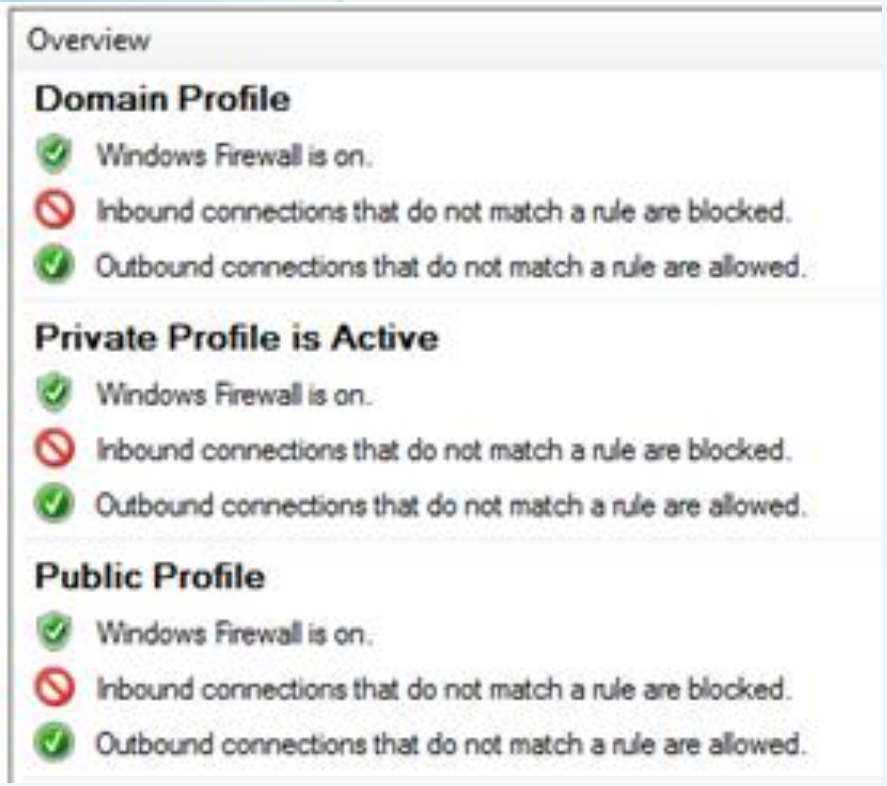


- WFAS does much more than block network traffic: it is also a connectivity platform

- If you plan to utilize IPsec for encryption of network traffic, rules in this section are the definitions of IPsec tunnels

WFAS

Windows Firewall settings: Profiles



Three different types of profiles:

- Domain Profile: only active for a domain-joined computer
- Private Profile: When connecting to a new network and prompted to choose where you are connected , if you choose either "Home" or "Work", that connection will be assigned the Private Profile.
- Public Profile: When prompted, if you choose "Public" then of course you are assigned the Public firewall profile.

WFAS

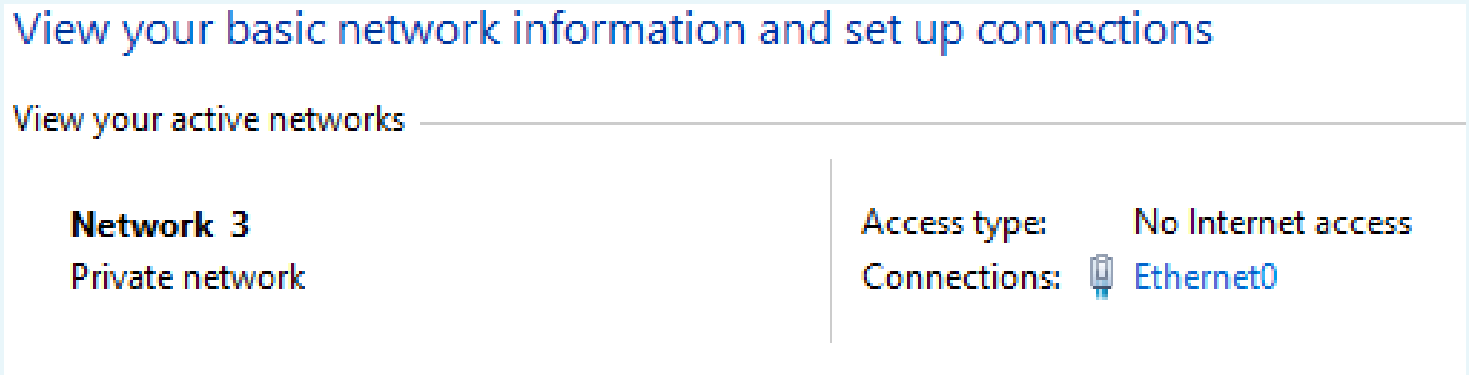
Windows Firewall settings: Profiles

- When any NIC on a server connected to a network, WF assign that connection one of the three different profiles
- Example: When connect your laptop to the Wi-Fi at your local coffee shop, Windows prompt and ask you if you were connecting to a home, work, or public network! i.e., WF asking you which profile to assign to the new network connection
- Assign NICs and network connections to different firewall profiles means that assign different access rules and criteria for what is or is not allowed over those different profiles.

WFAS

Windows Firewall settings: Profiles

- Each network connection assigned its own profile => more than one firewall profile active at the same time on the same system.
- For example, one server connected to both the corporate network and the public Internet. Inside WFAS, both the Domain Profile and the Public Profile are active
- To identify the profile of a NIC: Network and Sharing Center

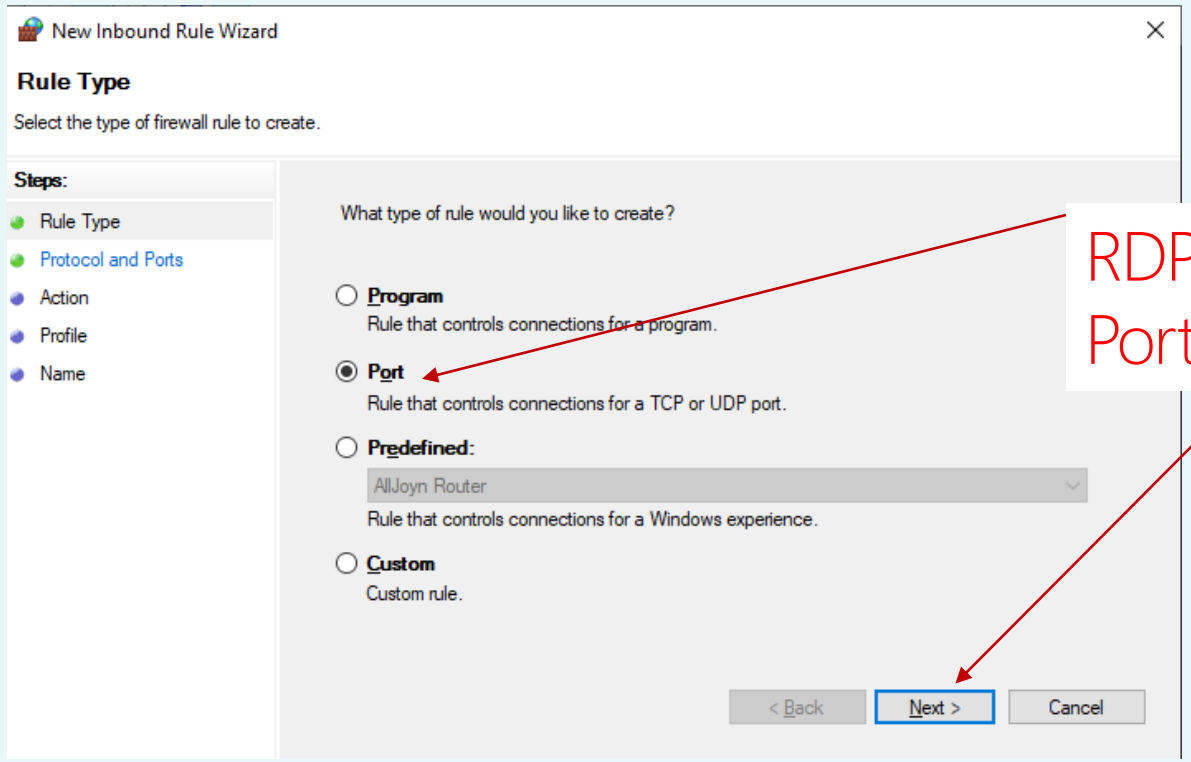


WFAS

Building a new Inbound Rule

To create a rule which blocks RDP access from the outside

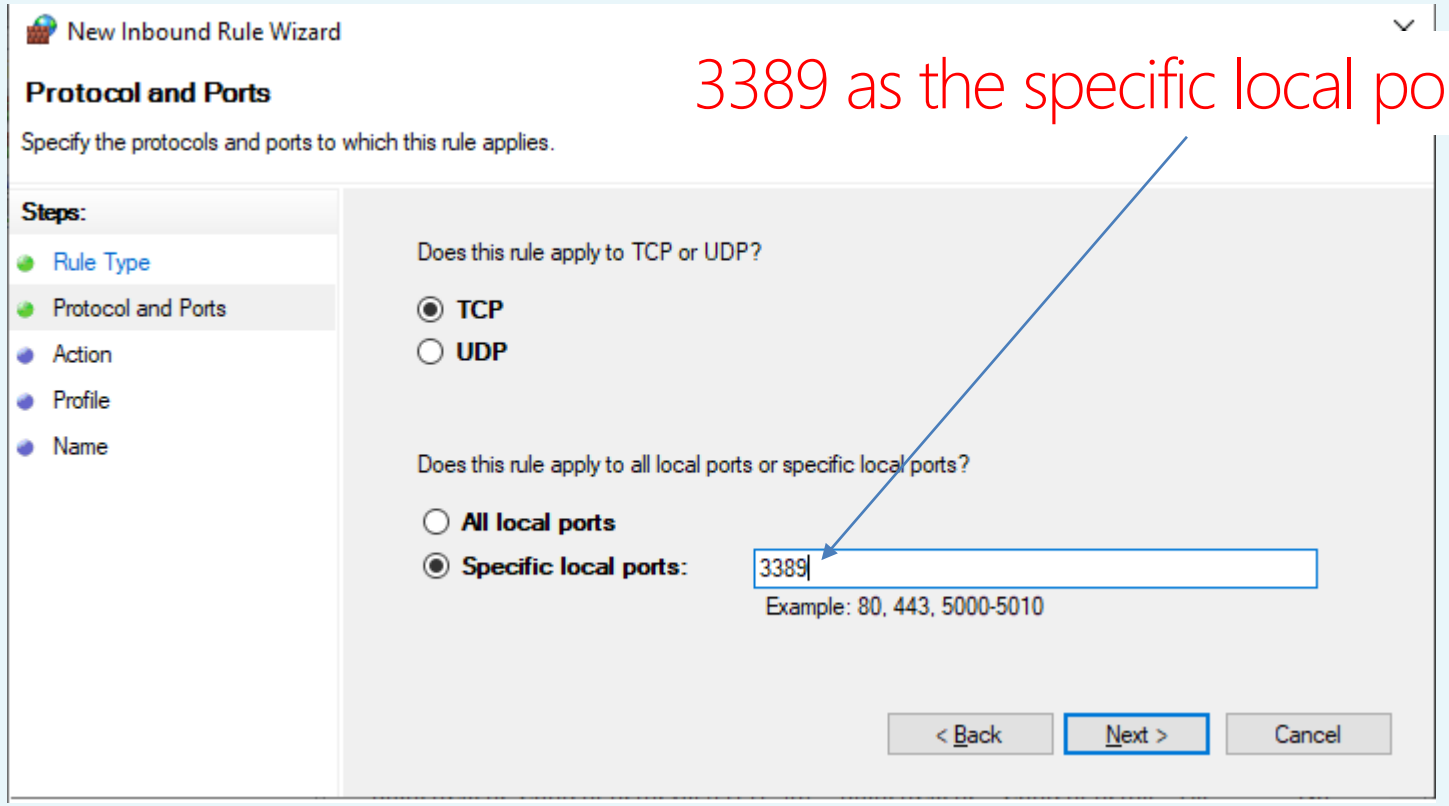
- Open up WFAS (wf.msc); Right-click on Inbound Rules, and choose New Rule…



RDP runs over TCP port 3389. So we choose Port on this screen, and click on Next

WFAS

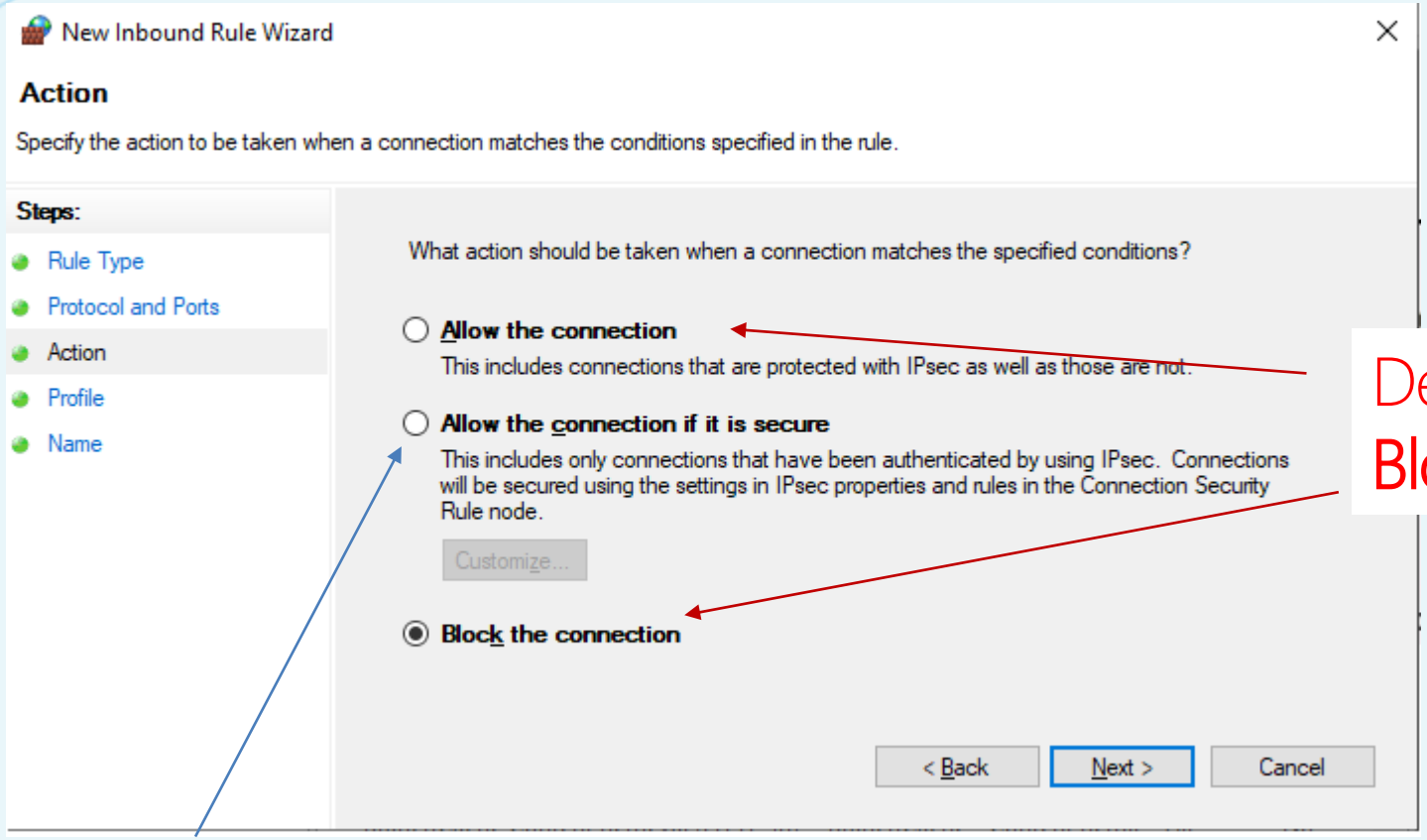
Building a new Inbound Rule



3389 as the specific local ports

WFAS

Building a new Inbound Rule



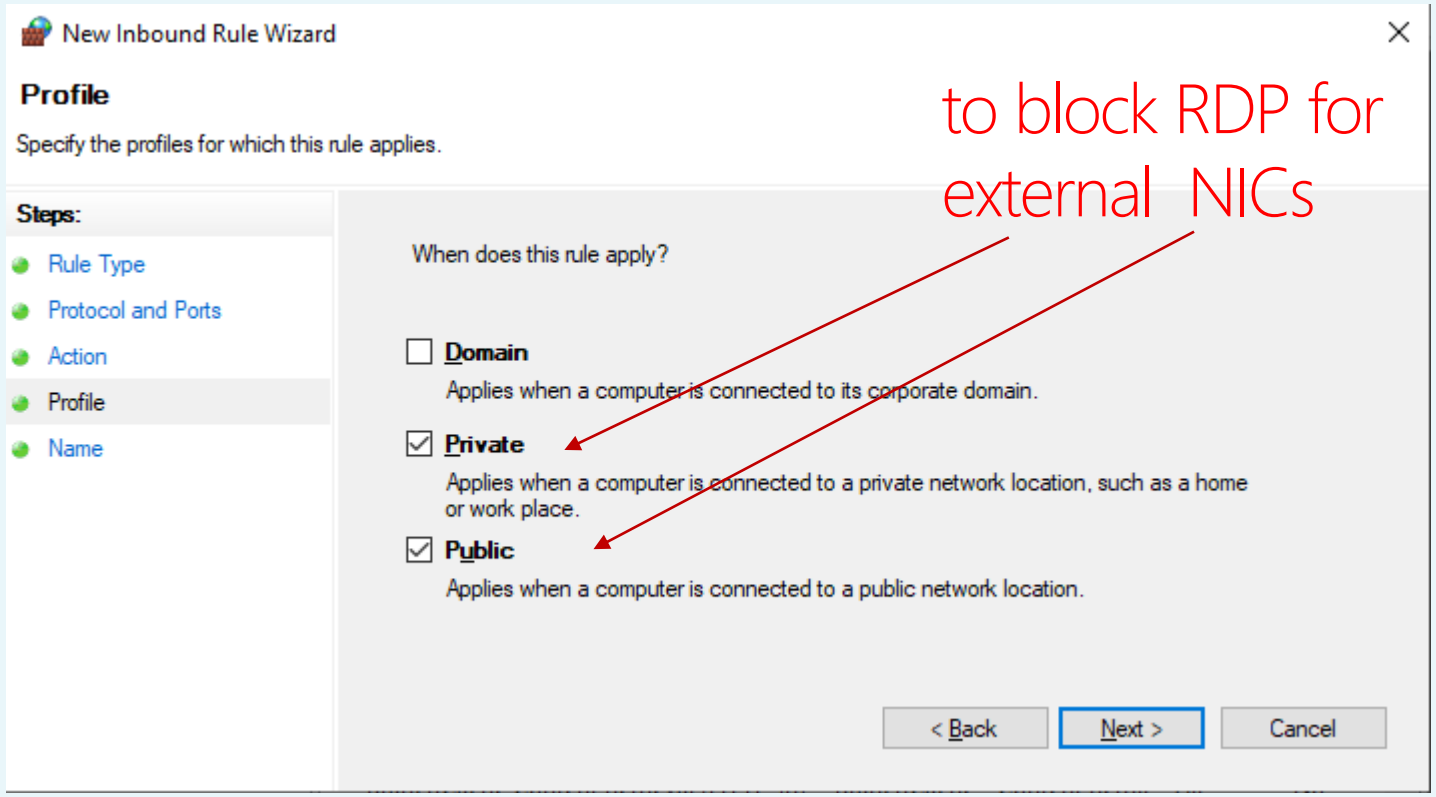
Decide whether to **Allow** or **Block** this particular port

Only allow the connection if it is authenticated by IPSec: IPsec already established in the network

WFAS

Building a new Inbound Rule

- The internal NICs connected to domain network will have the Domain profile assigned to them; other NICs have either Public or Private profiles active



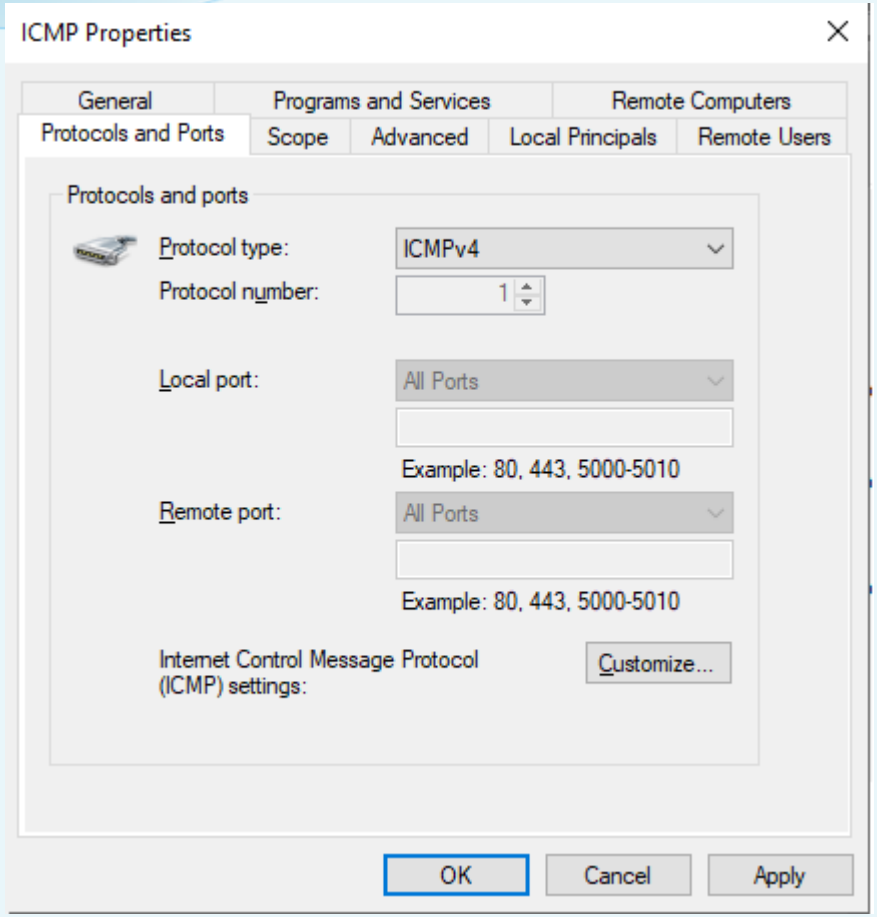
WFAS

Build a rule for ICMP

- New Windows Automatically block pings (ICMP)=> Need to create either an allow or a block rule for ICMP
- Create the new rule as previous example (Rule Type: **port**; Specific Local Port: **Any number**, e.g., 1234)
- Once your new rule is created, it presents in the **Inbound Rules** list. Right-click on it, and head into Properties.

WFAS

Build a rule for ICMP



- Navigate into the **Protocols and Ports** tab, and expand the drop-down menu for Protocol type.
- Choose ICMPv4 or ICMPv6.
- The new rule has now been changed to be an Allow rule for ICMPv4, and this server now respond to ping requests successfully

Managing WFAS with Group Policy

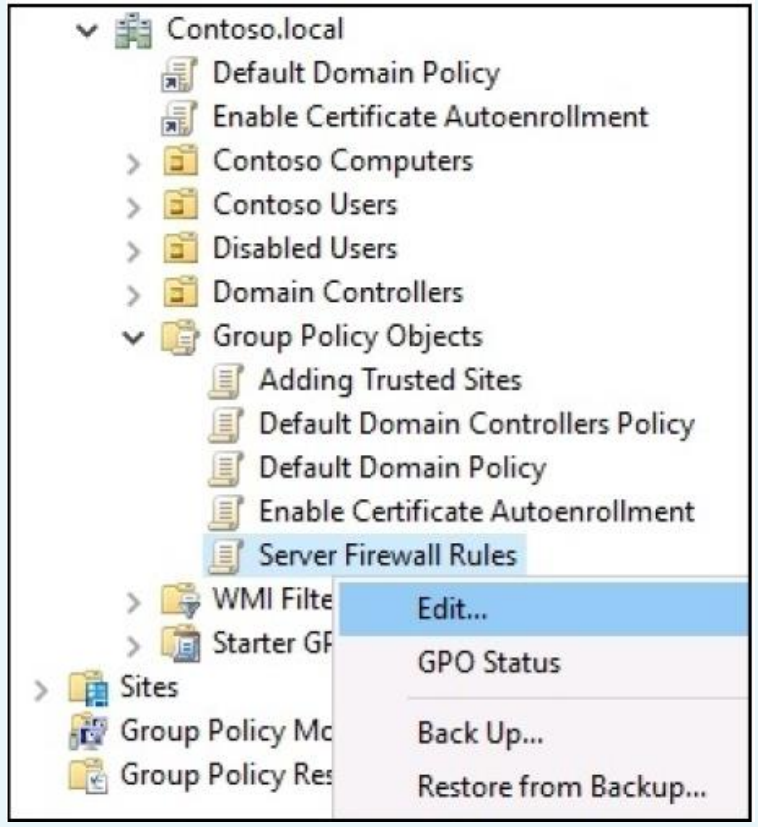
- Managing firewall rules on your servers, and clients, can be a huge step toward a more secure environment for your company
- If your company has 1000 computers and you are assigned to implement the entire list of allows and blocks on every machines, how do you solve this problem?
- Group Policy: setting up a firewall policy that applies to everyone is a breeze for your domain-joined machines

WFAS

Managing WFAS with Group Policy

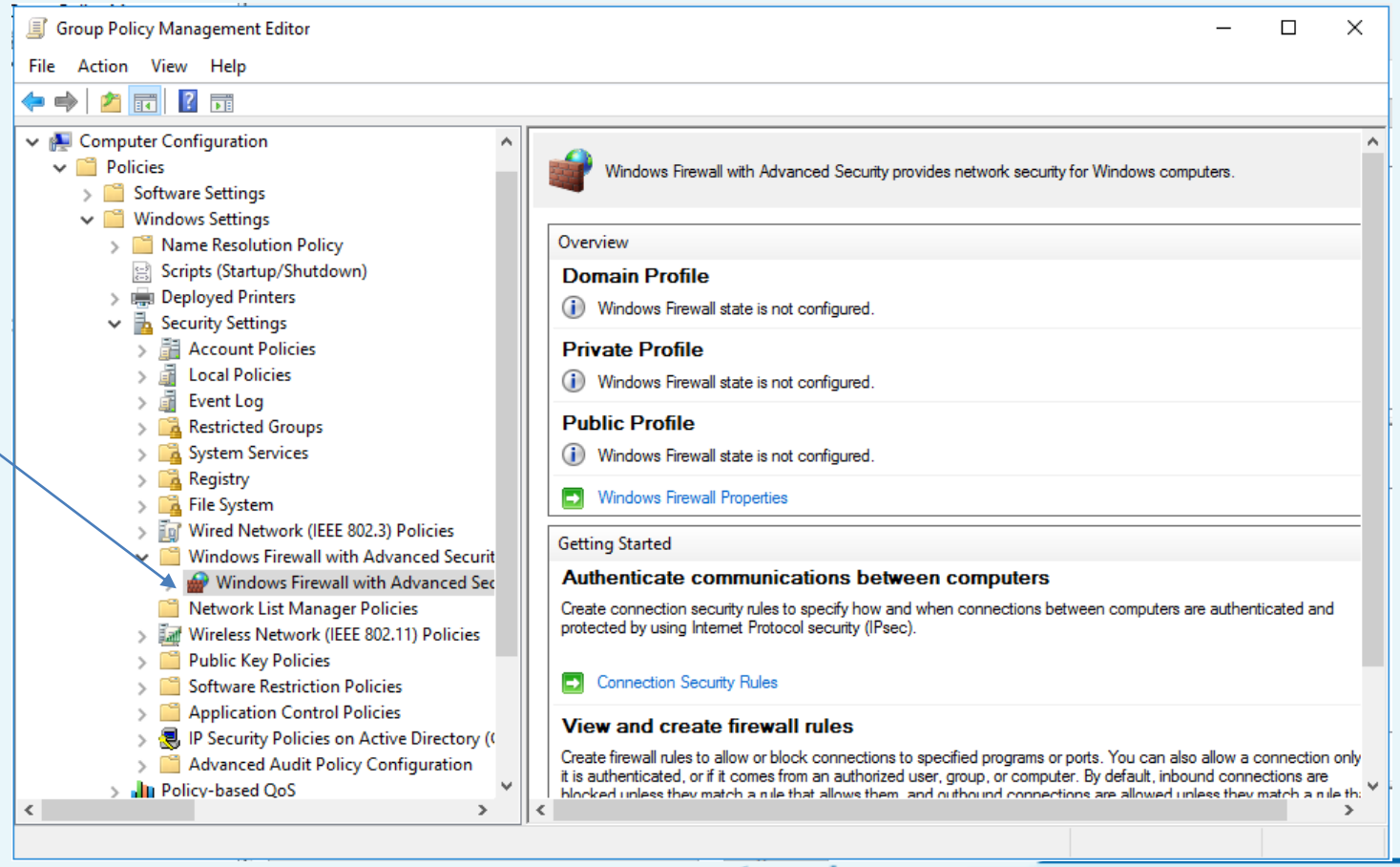
- For more granularity, You can have a GPO applies firewall rules to clients, and a separate GPO applies firewall rules to servers

- Creating a GPOs for firewall settings
- Once new GPO created, right-click on it from inside the Group Policy Management Console, and click on Edit….

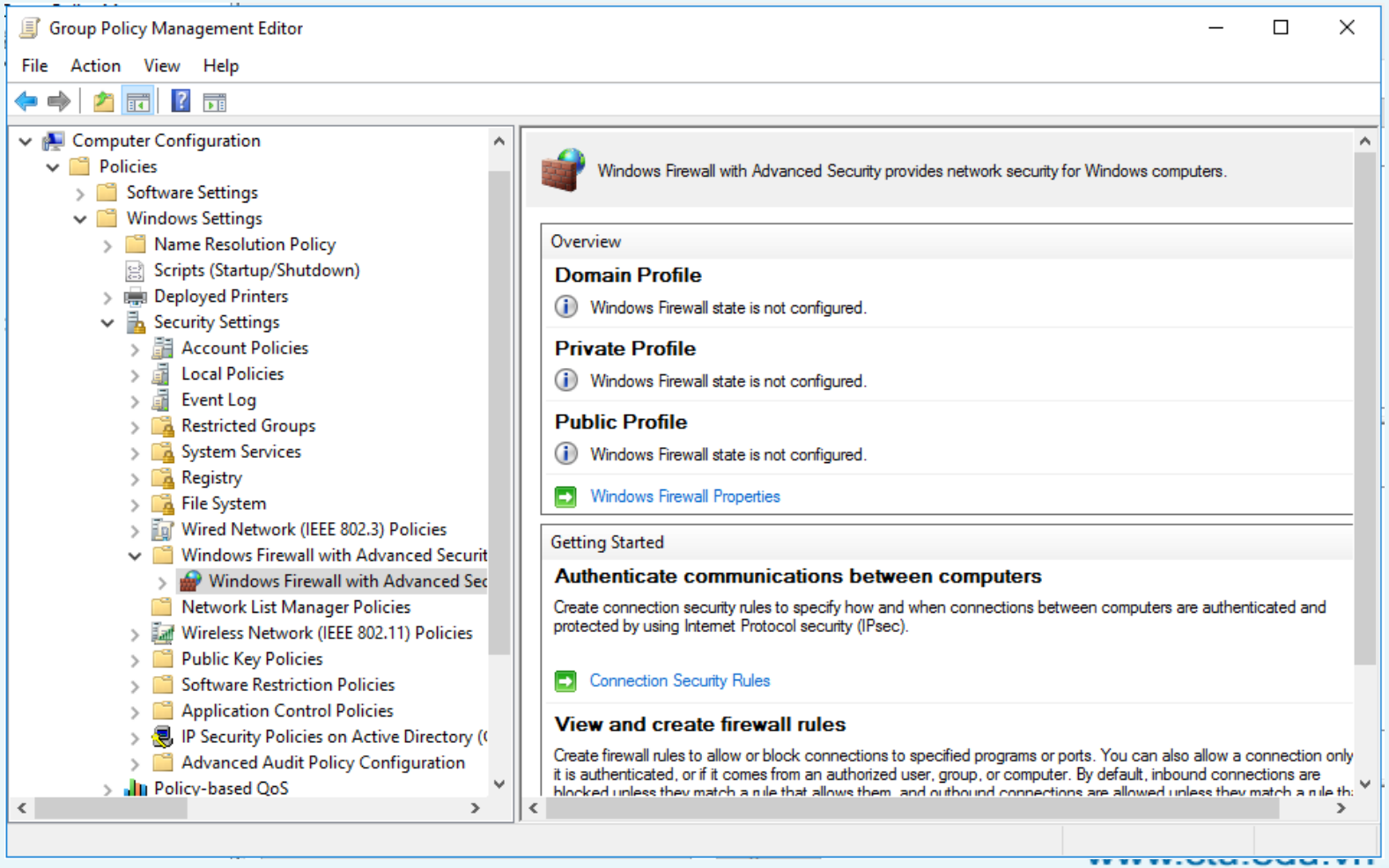


- Looking the insides of this new GPO to figure out the correct location to create some new firewall rules

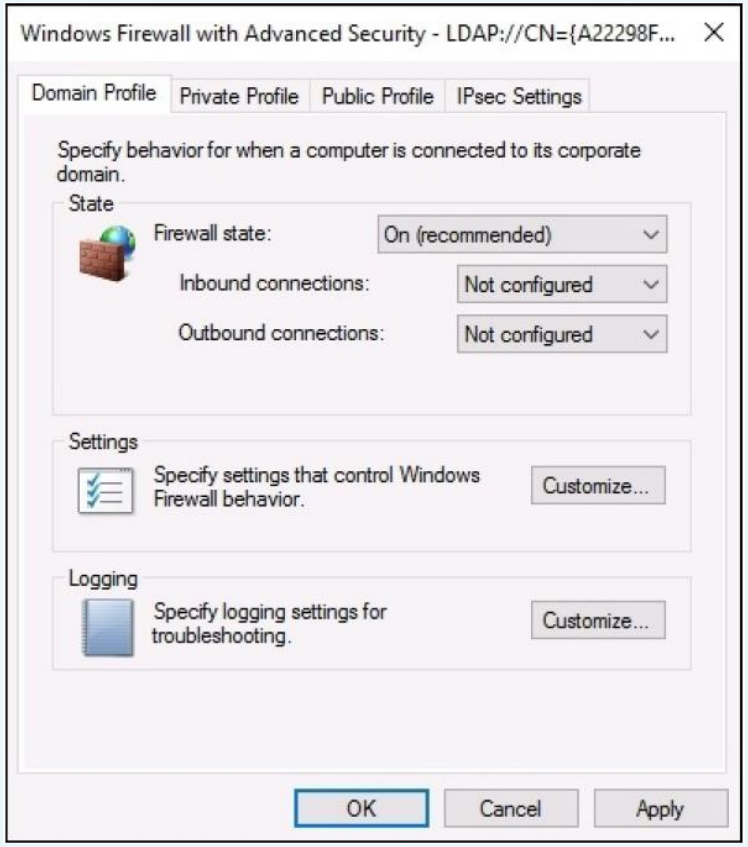
Windows Firewall with Advanced Security heading (Computer Configuration | Policies |Windows Settings | Security Settings)



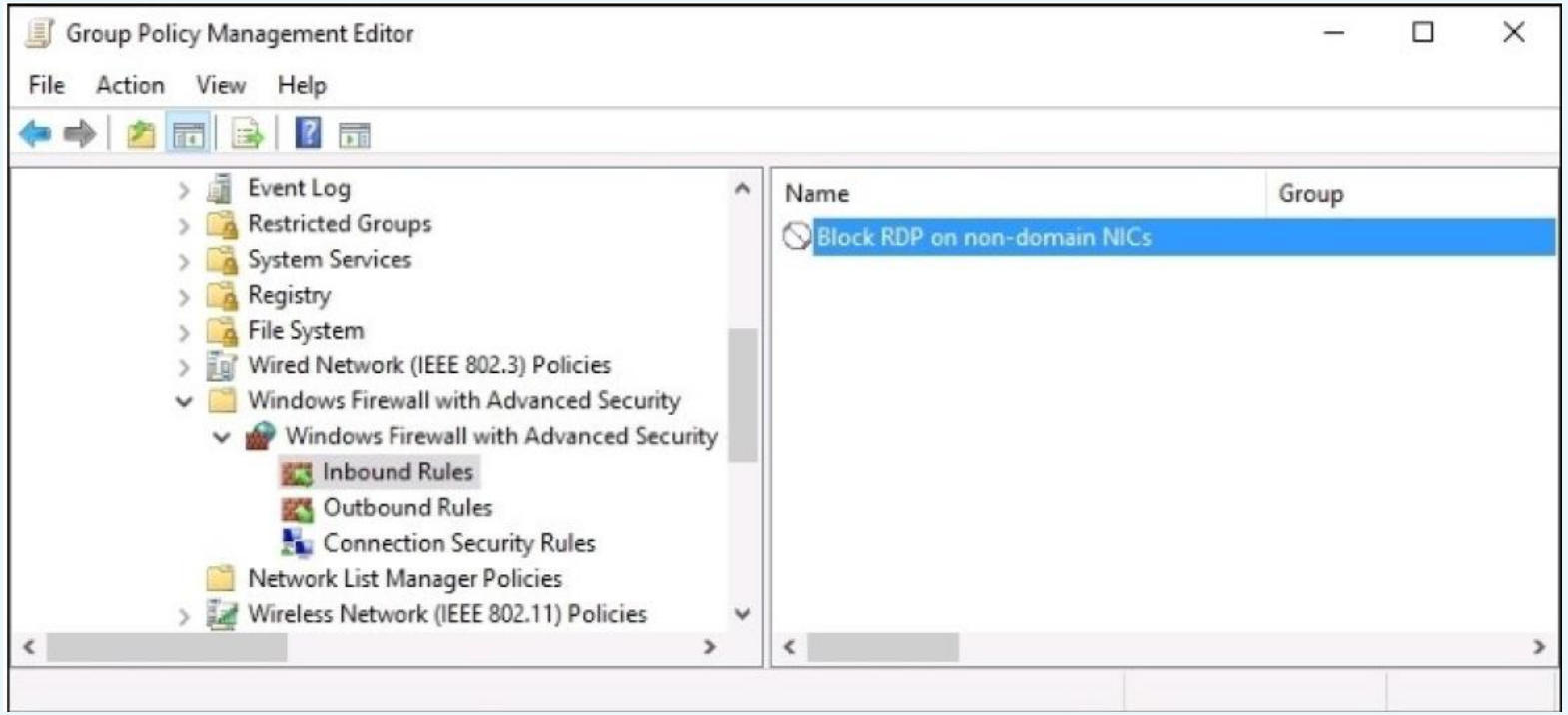
- Turned on or off firewall profiles, or the Windows Firewall



- Clicking on the Windows Firewall Properties to determine the status of each firewall profile individually



- Inside WFAS, we have categories for Inbound Rules and Outbound Rules to help building a rule into this GPO



Windows Defender

Windows Defender

Installation

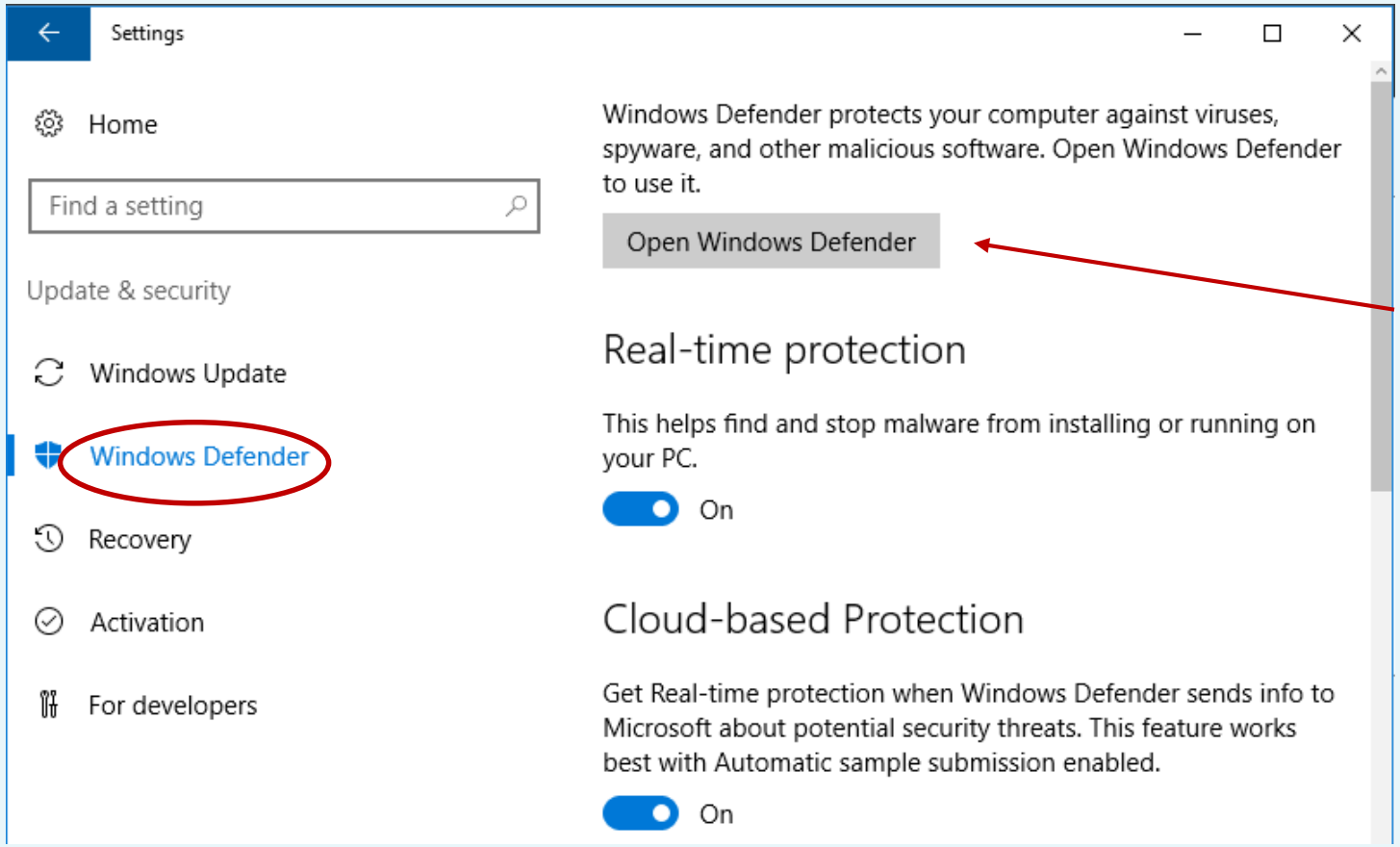
- Anti-malware software built into the Windows operating system (starting with Windows 8)
- Windows Defender installed by default in Windows Server 2016
- If it is not installed yet, we can easily add the Windows Defender feature either from the Add Roles and Features wizard, or by using PowerShell cmdlet:

Install-WindowsFeature –Name Windows-Defender-GUI

Windows Defender

User interface

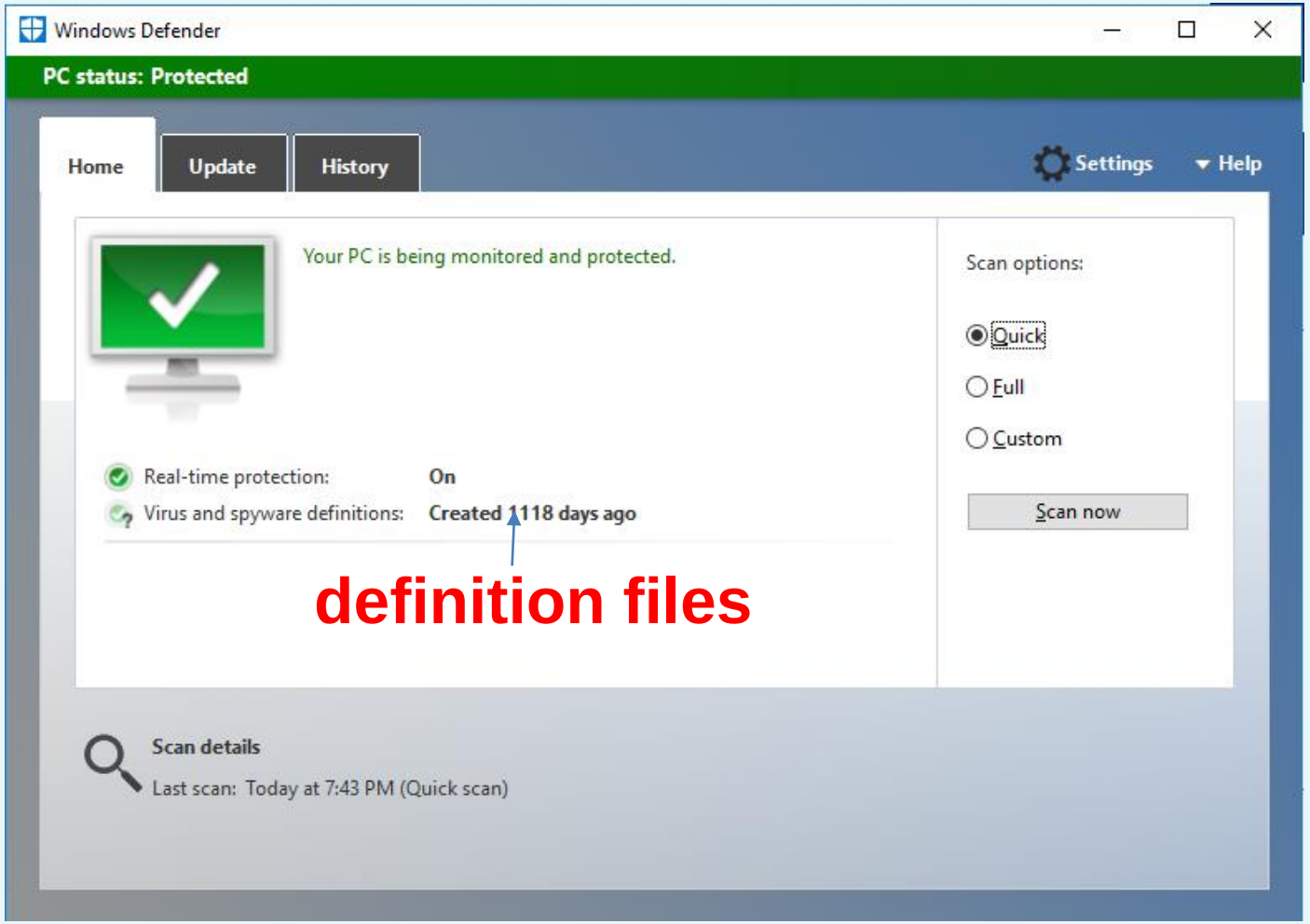
- Settings -> Update & Security



Open Windows Defender

Windows Defender

User interface

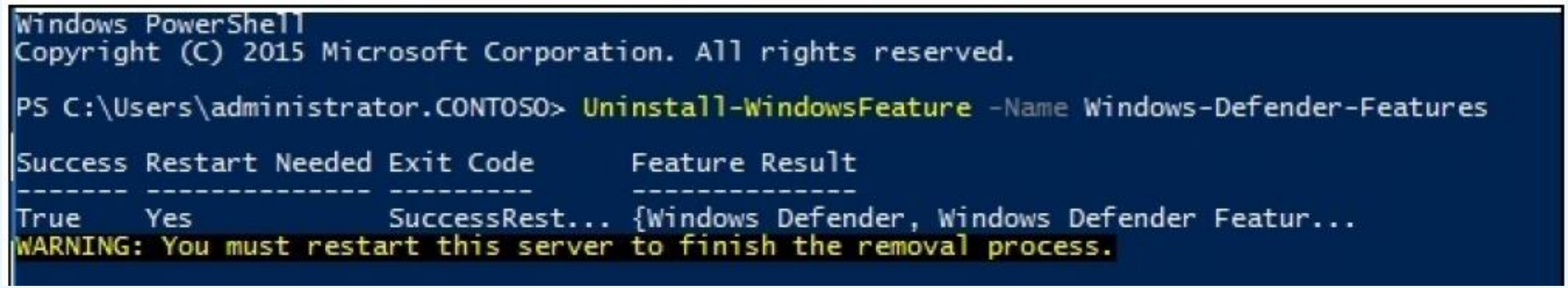


Windows Defender

Disabling

- If you want to disable Defender, you must remove the feature from Windows
- PowerShell:

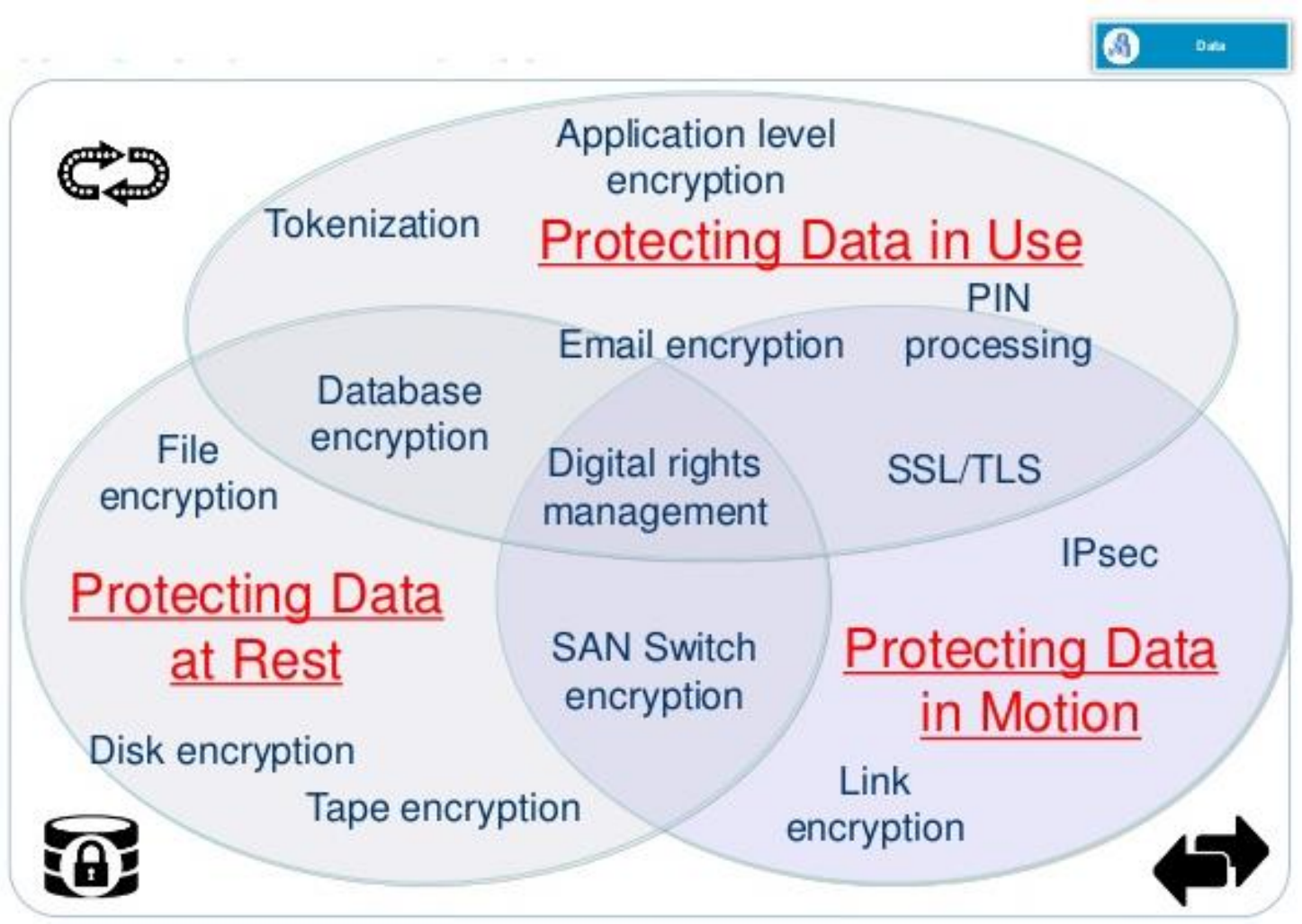
Uninstall-WindowsFeature –Name Windows-Defender-Features



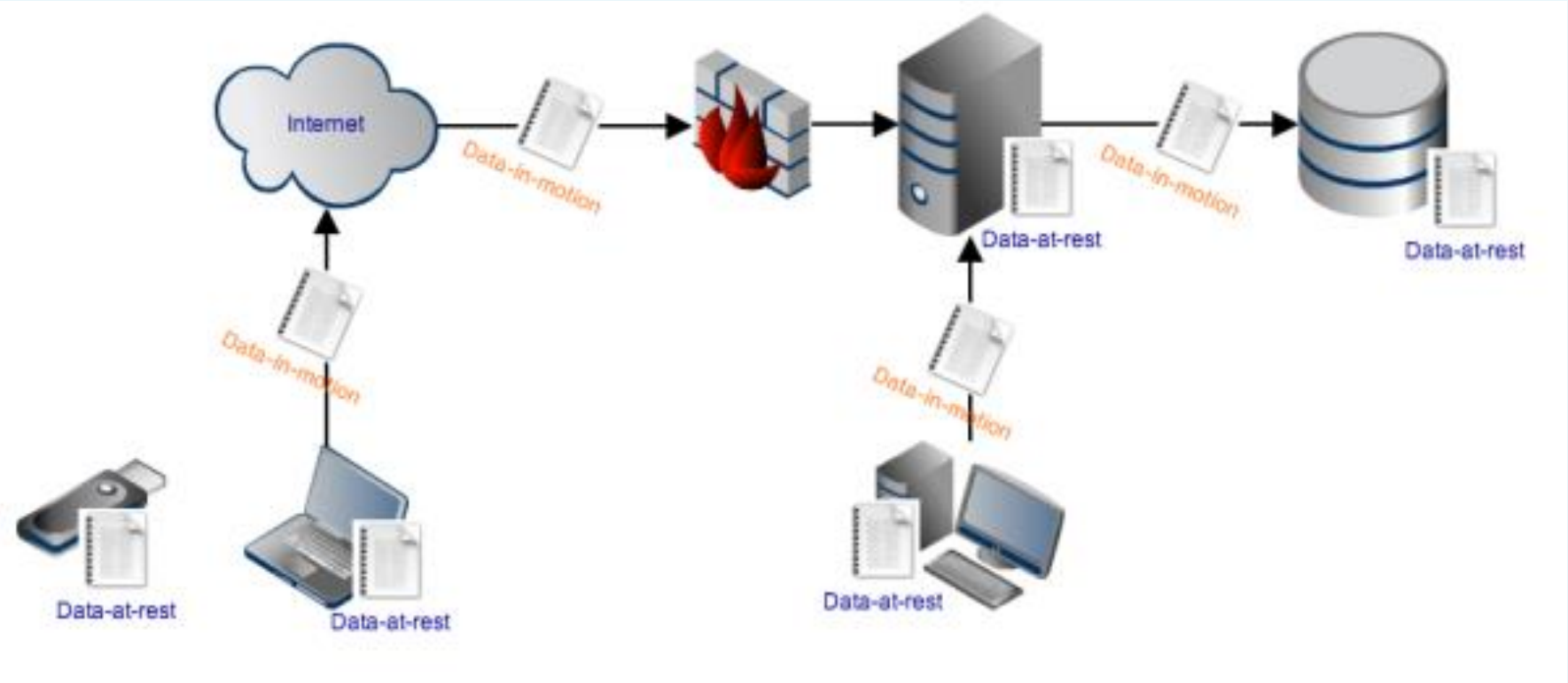
Protecting Data

Protecting Data

Protecting Data



Protect Data at Rest

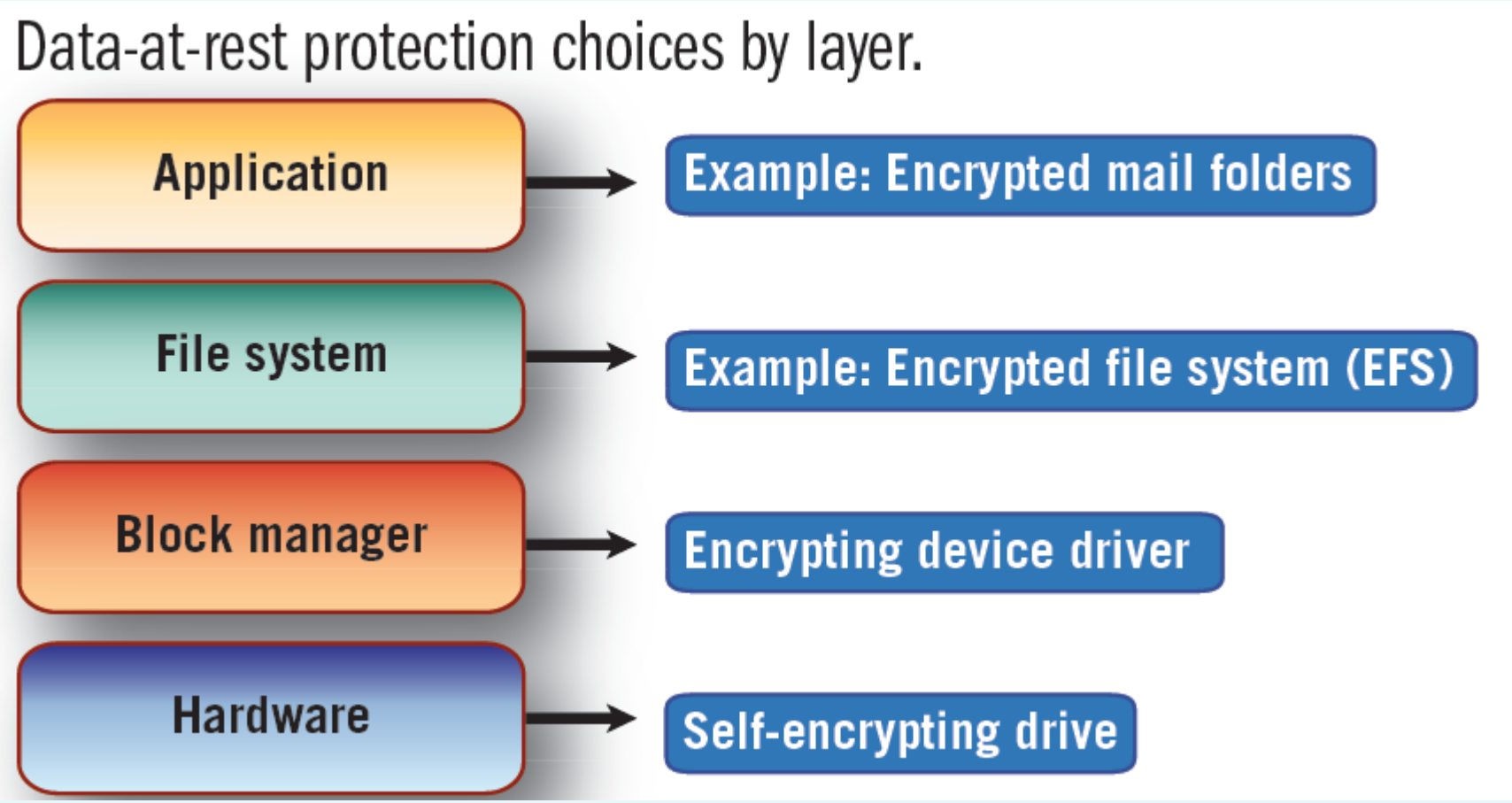


Data stored on client computers, servers, databases, or backup media.

Protecting Data at Rest

- A popular target for attackers: if successfully accessed, it can be copied, transferred, and then used for different types of illegal activities.
- Numerous examples of stolen personal user information and credit card numbers,.e.g.,
  - Yahoo: 500 million accounts were stolen in 2014;
  - Community Health Systems, Inc.: 4.5 million patient data stolen including social security numbers .
- All these examples show that protection of the data at rest should be taken very seriously.

Protect Data at Rest



Protecting Data at Rest

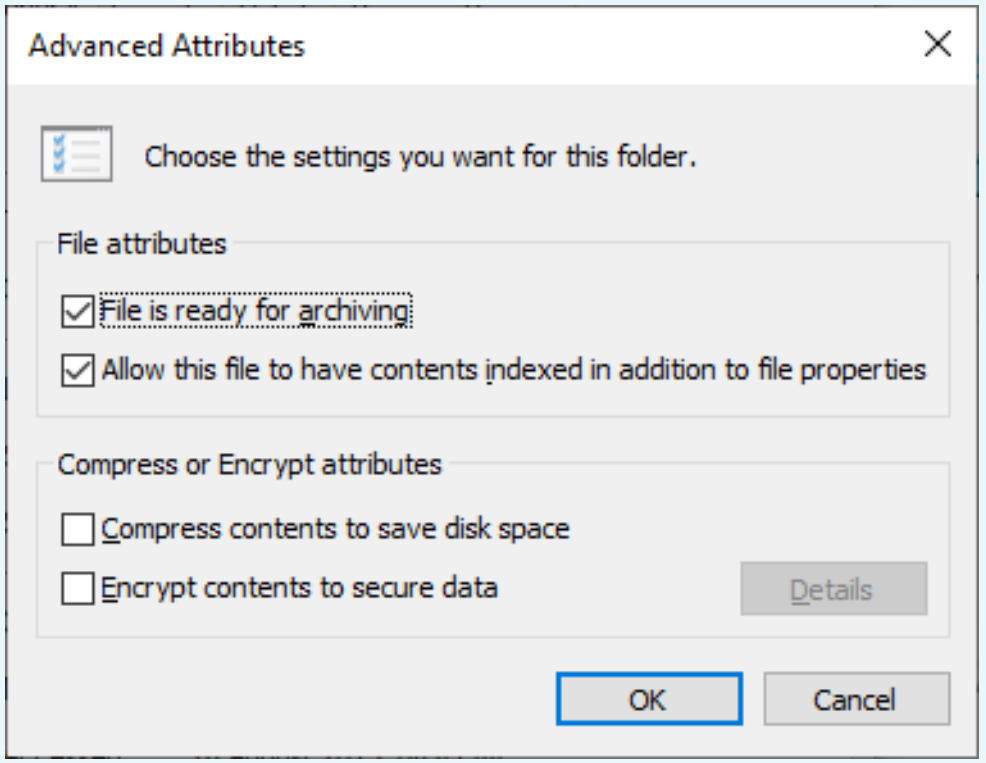
Encrypting File System

- Encrypting File System (EFS): existed on both client and server operating systems
- EFS encrypt only particular documents or folders
- Prevent unauthorized users from viewing its content, no matter of the type of permissions users have to a file
- The process of encryption and decryption is transparent to the user and applications.

Protect Data at Rest

Encrypting File System

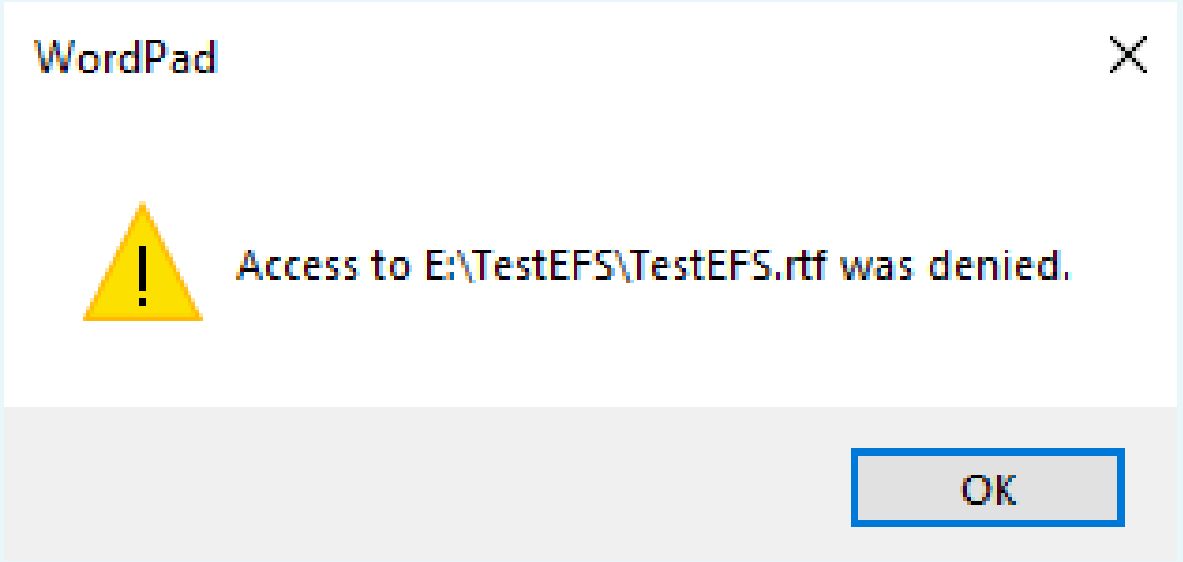
- When encrypting a file or folder, users just need to select a check box to encrypt the contents to secure data



Protecting Data at Rest

Encrypting File System

- When users access the encrypted files or encrypted folders, they open them the same way they would open a nonencrypted file.
- When unauthorized users attempt to open the file, they will receive a message stating that access is denied

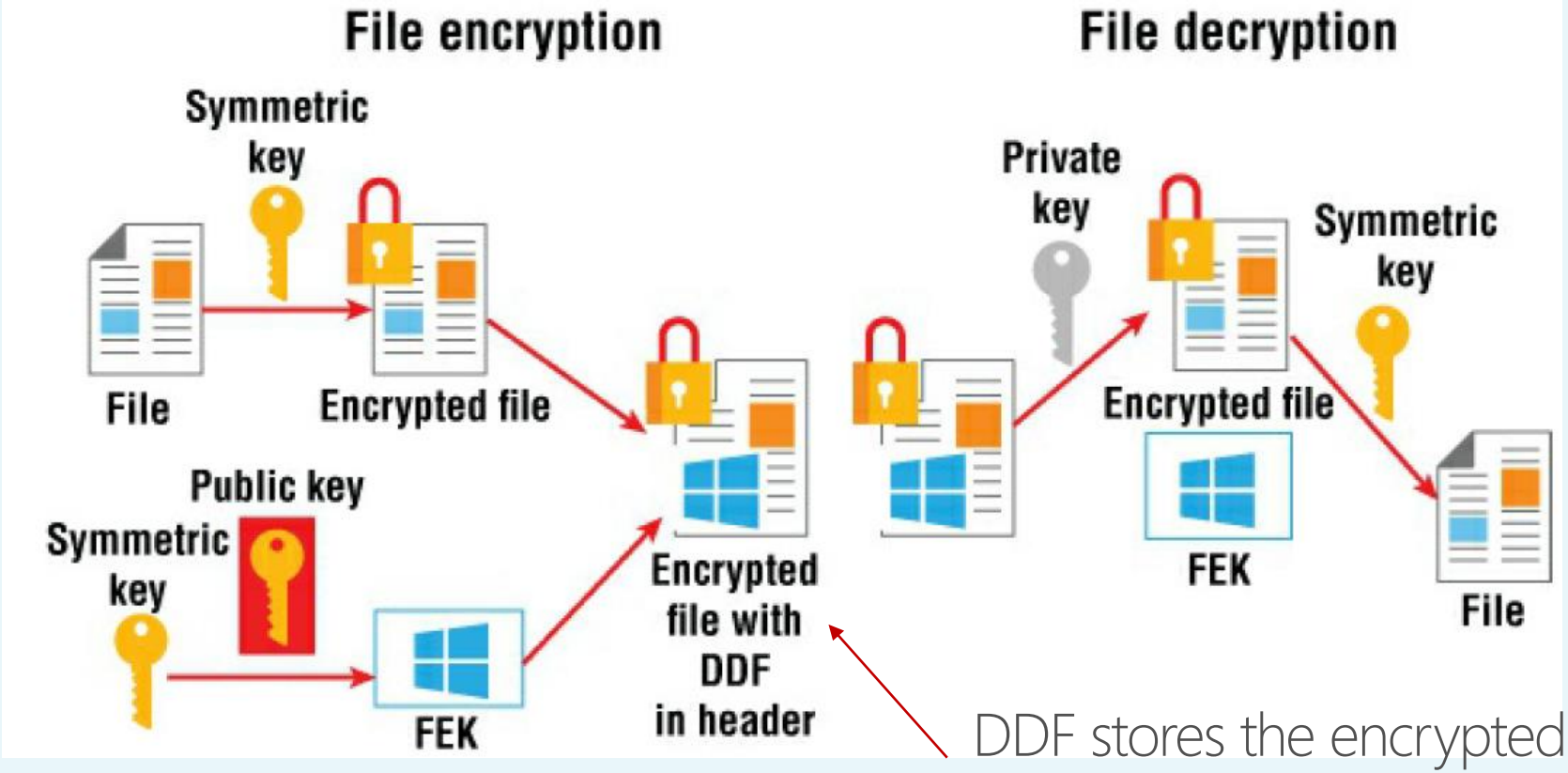


Protecting Data at Rest

Encrypting File System

2. EFS then encrypts the file with the generated FEK

3. Encrypts the FEK with the user's public key



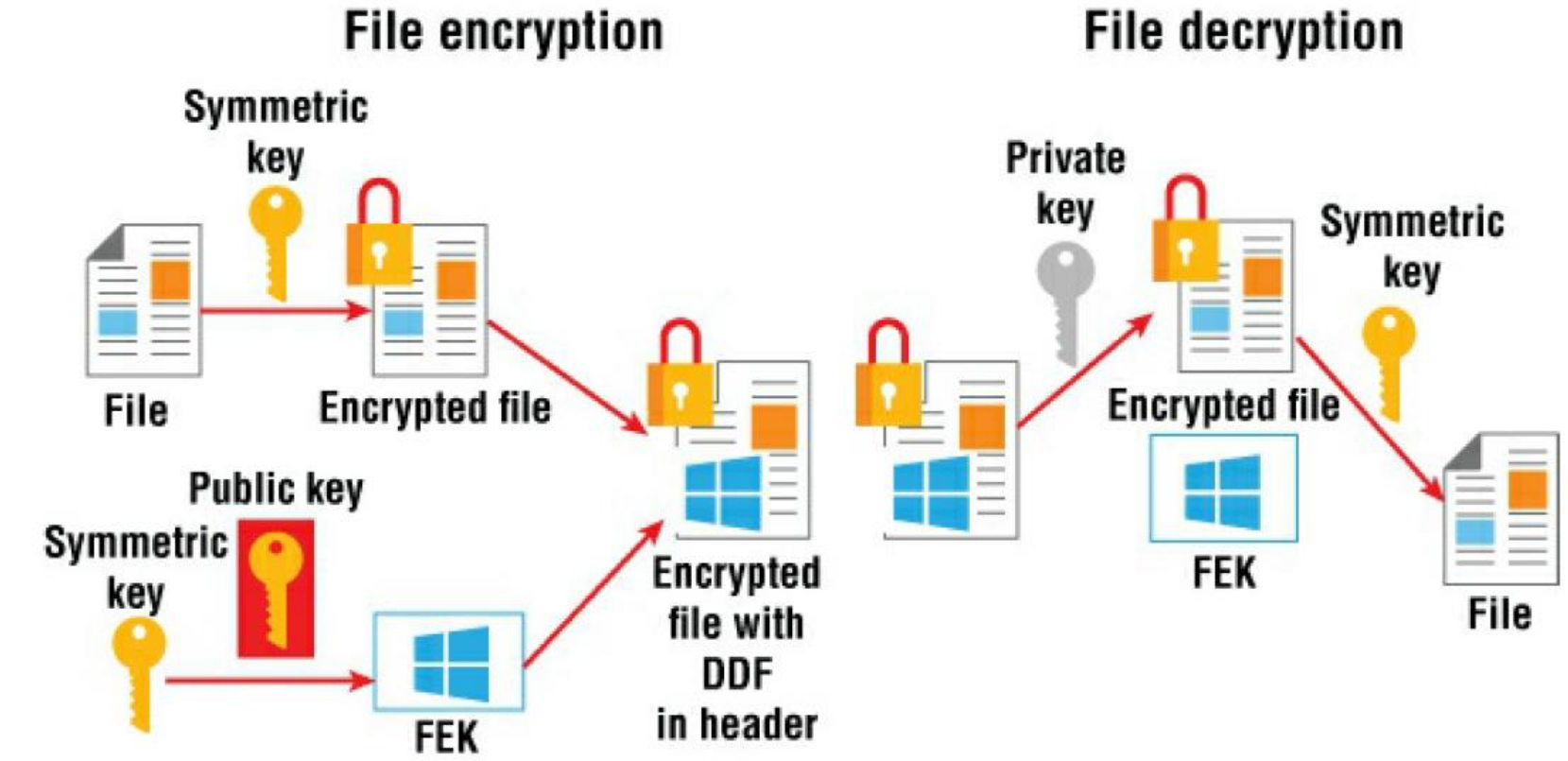
1. EFS first generates a random symmetric file encryption key (FEK) for each file

DDF stores the encrypted FEK with the user's public key

Protecting Data at Rest

Encrypting File System

1. EFS uses the user's private key to decrypt the FEK.



2. If EFS decrypts the FEK successfully, EFS uses it to decrypt the file content.

Protecting Data at Rest

BitLocker

- A volume-encryption technology that encrypts the whole volume to protect data from unauthorized access.
- Can encrypt an entire volume or only the used parts of a volume.
- BitLocker requires the hard drive is encrypted, i.e, OS can't boot without the encryption being unlocked.
- How do we unlock the hard drive so that our machine can boot?

Protecting Data at Rest

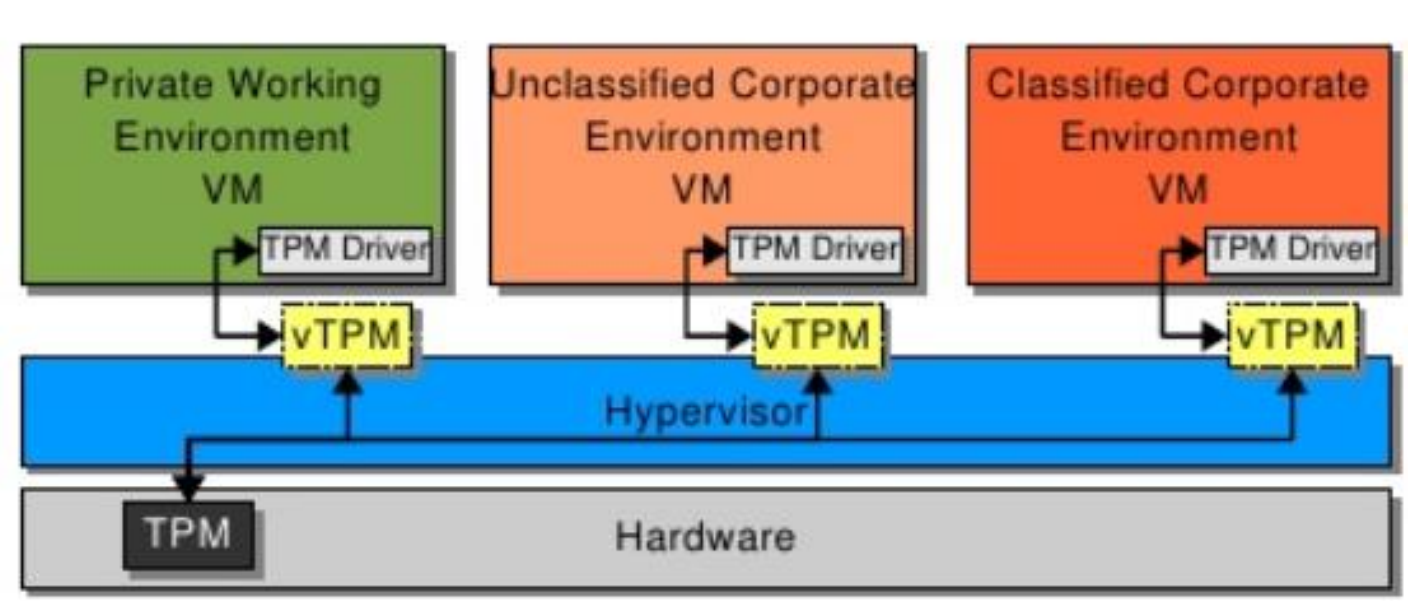
BitLocker

- The best method is to store the "unlock keys" inside a Trusted Platform Module (TPM):
  - A physical microchip built into a computer.
  - You simply enter a pin to gain access to the TPM in order to make it boot.
- If deploy BitLocker without the presence of a TPM, to unlock a BitLocker volume and make it bootable you need to plug in a physical USB stick that contains the BitLocker unlock keys.

Protecting Data at Rest

BitLocker and the Virtual TPM

- Can BitLocker apply to VMs?
  - VMs do not have a TPM, and you also have no way of plugging in a USB stick!
  - Virtual TPM: Brand new in Windows Server 2016 that can be used for storing these keys!

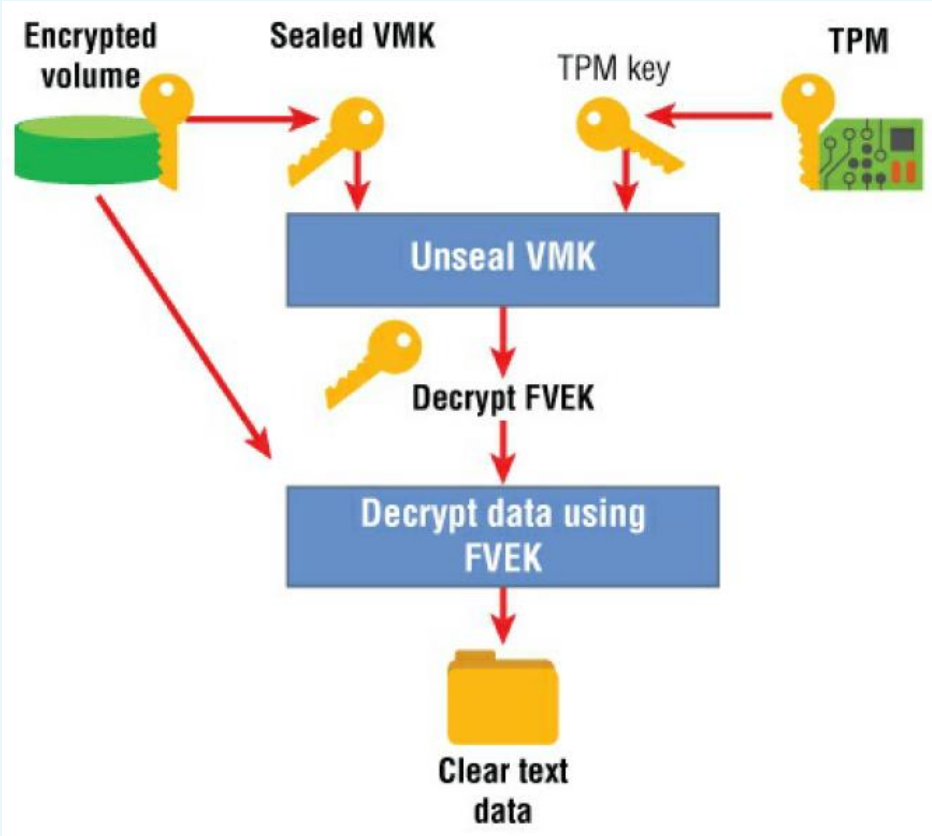


Protecting Data at Rest

BitLocker drive encryption architecture

- Sectors are encrypted by the full-volume encryption key (FVEK)

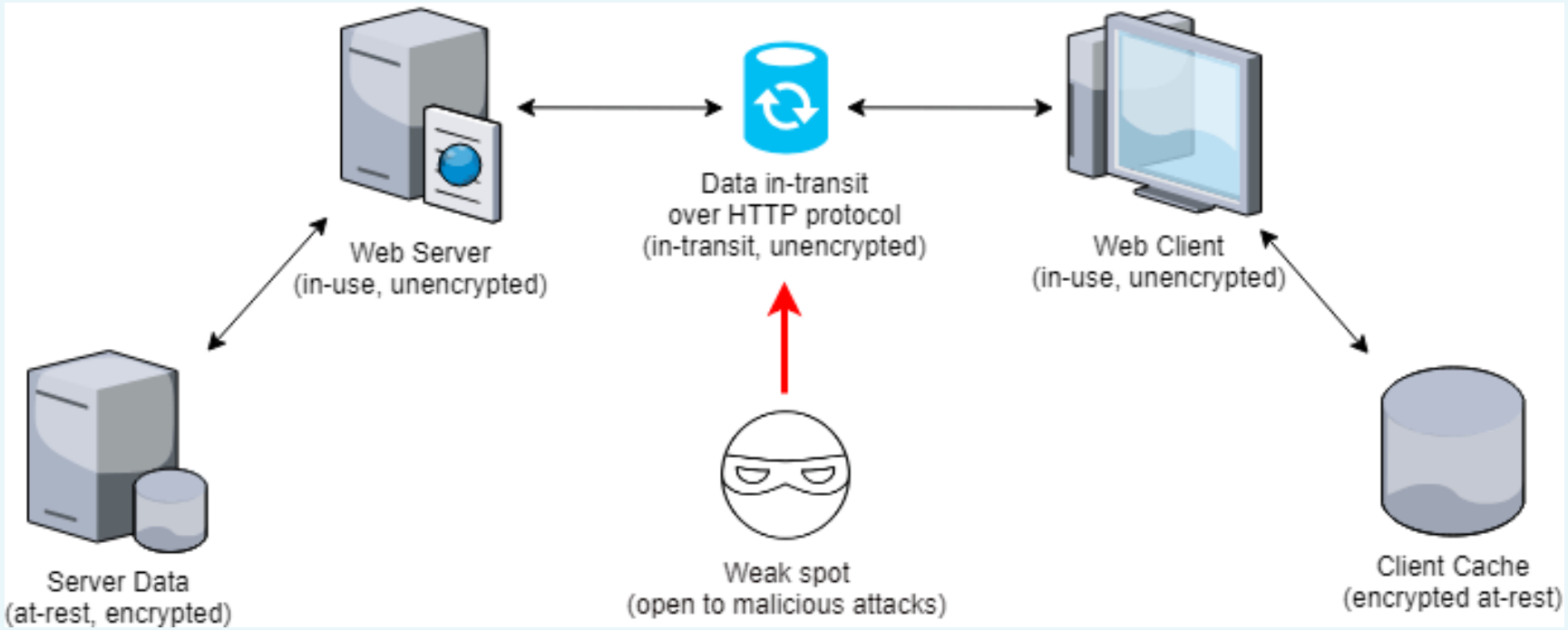
- FVEK is encrypted with the volume master key (VMK)
- The VMK is also encrypted by one or more key protectors.
- The default key protector is the TPM, but you can configure additional protectors, such as a PIN and a USB startup key.



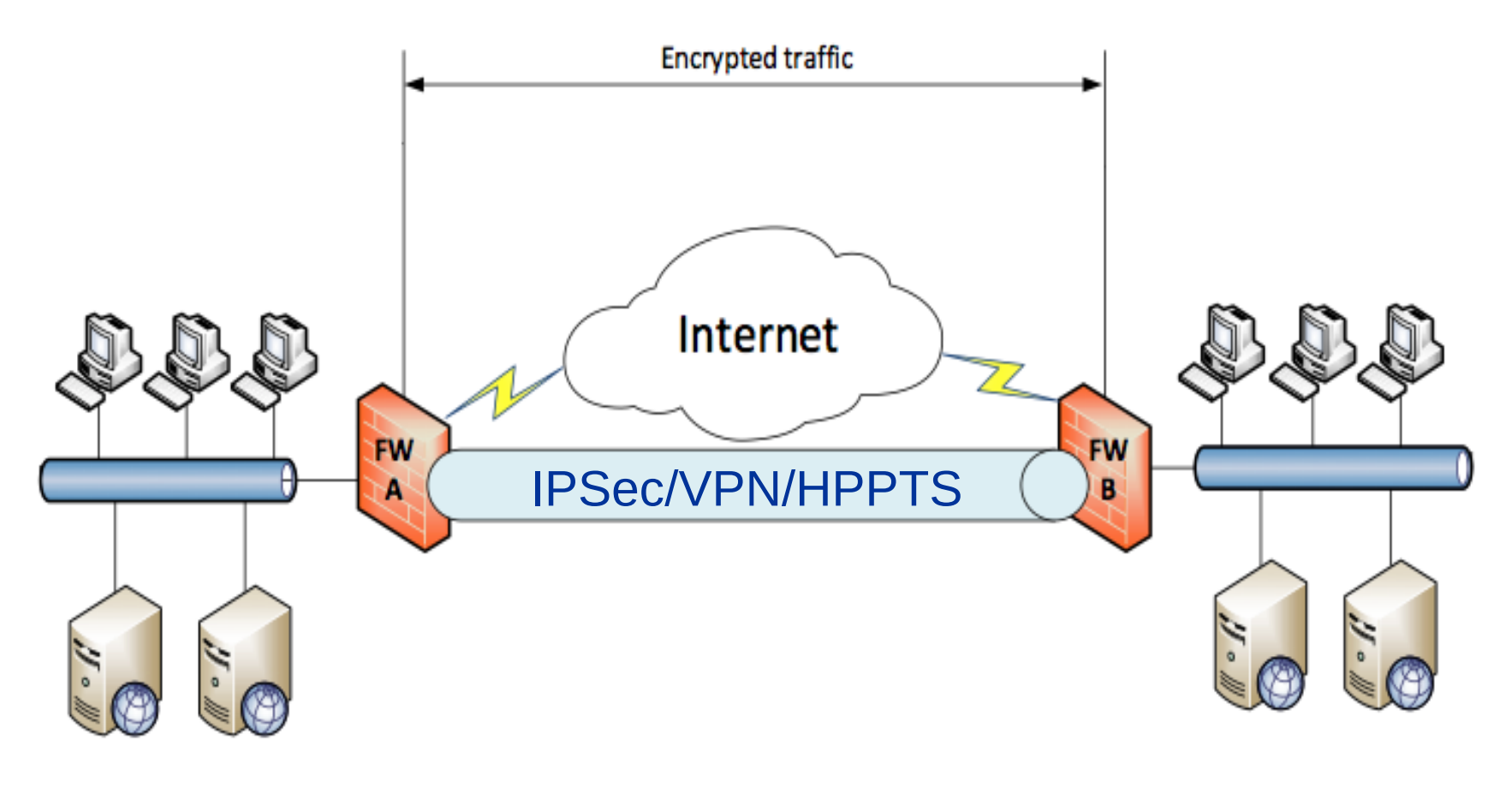
- FVEK encrypted with the VMK stored on the disk as part of the volume metadata.

Protecting Data in Transit

- Data in transit includes all the information that client computers and servers transfer during their communication



Protecting Data in Transit



Protecting Data in Transit

IPsec

- A suite of protocols that can help protect data in transit through a network by providing authentication, integrity checking, and encryption.
- Two IPSec security protocols used to provide these security services: Encapsulating Security Payload (ESP) and Authentication Header (AH)
- ESP: providing authentication, integrity and confidentially
- AH: provides a mechanism for authentication only

Protecting Data in Transit

IPsec

- IPsec has the following characteristics:
  - Offers mutual authentication before and during communications
  - Forces both parties to identify themselves during the communication process
  - Enables confidentiality through IP traffic encryption and digital packet authentication

Protecting Data in Transit

IPsec

- IPsec well suited for:
  - Securing host-to-host traffic on specific paths.
  - Securing traffic to servers, e.g., IPsec protection for all client computers that access a server.
  - Using L2TP/IPsec for VPN connections. You can use the combination of Layer Two Tunneling Protocol (L2TP) and IPsec (L2TP/IPsec) for all VPN scenarios.
  - Site-to-site (gateway-to-gateway) tunneling e.g., interoperability with third-party routers

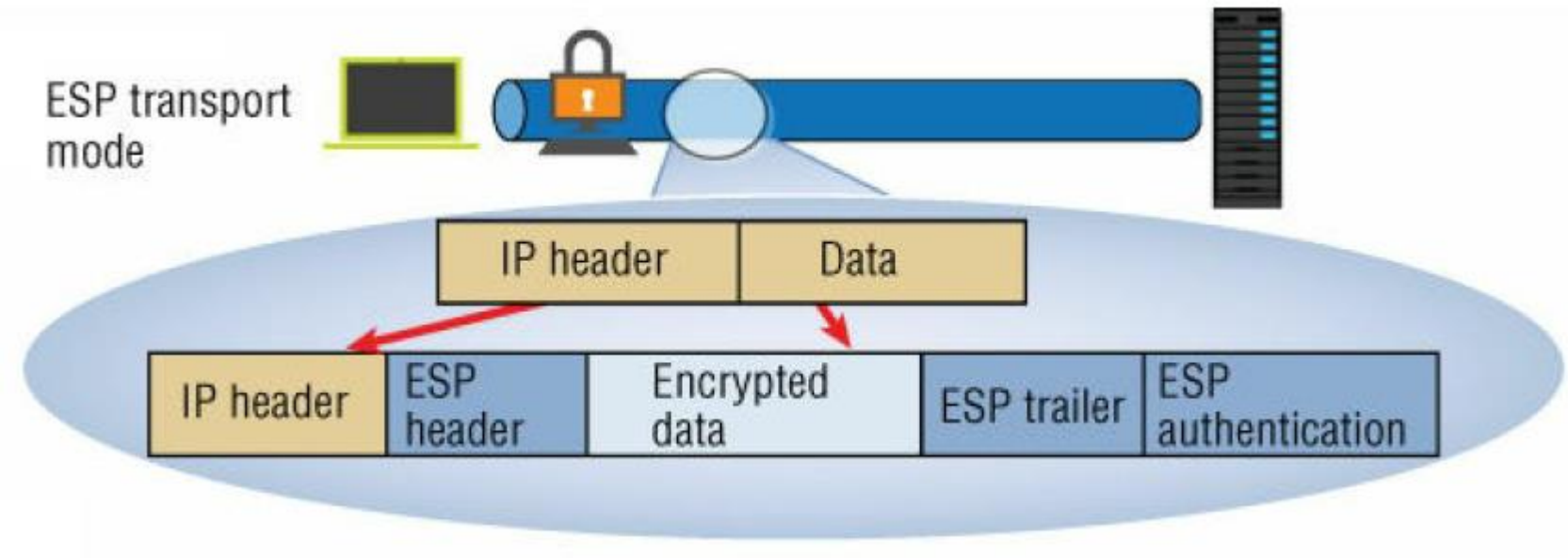
Protecting Data in Transit

IPsec

- When configuring VPN on RA server: one of the connection protocols the VPN clients can use to connect to the VPN server is IPsec (IKEv2) tunnels
- DirectAccess tunnel is also protected by IPsec.
- We can specify the traffic moving around inside our corporate networks to be encrypted using Ipsec by using IPsec policy settings.

Protecting Data in Transit

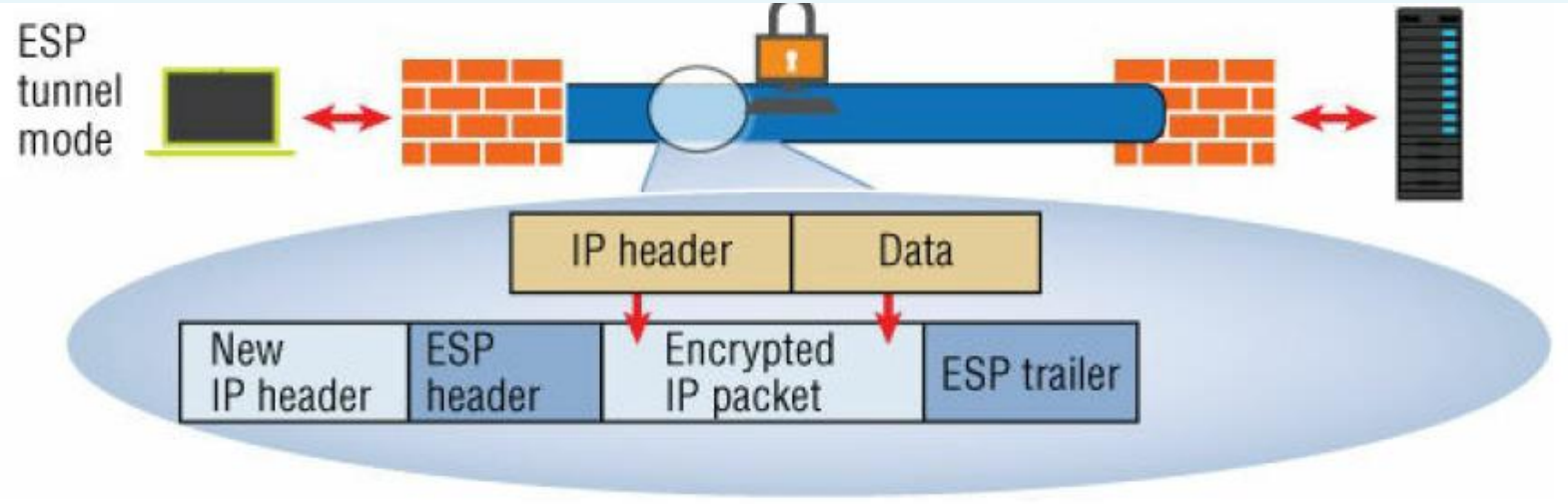
IPSec mode: Transport mode



- Enable end-to-end communications between two hosts.
- In this mode, the data payload is encrypted, but the header data remains unchanged.

Protecting Data in Transit

IPSec mode: Tunnel mode



- The entire original packet is encrypted and becomes the payload of a new packet
- IPSec-aware routers
  - to encapsulate and encrypt network traffic from hosts that are not IPsec aware,
  - and then decrypt it for use on the destination network by other hosts that are not IPSec aware.

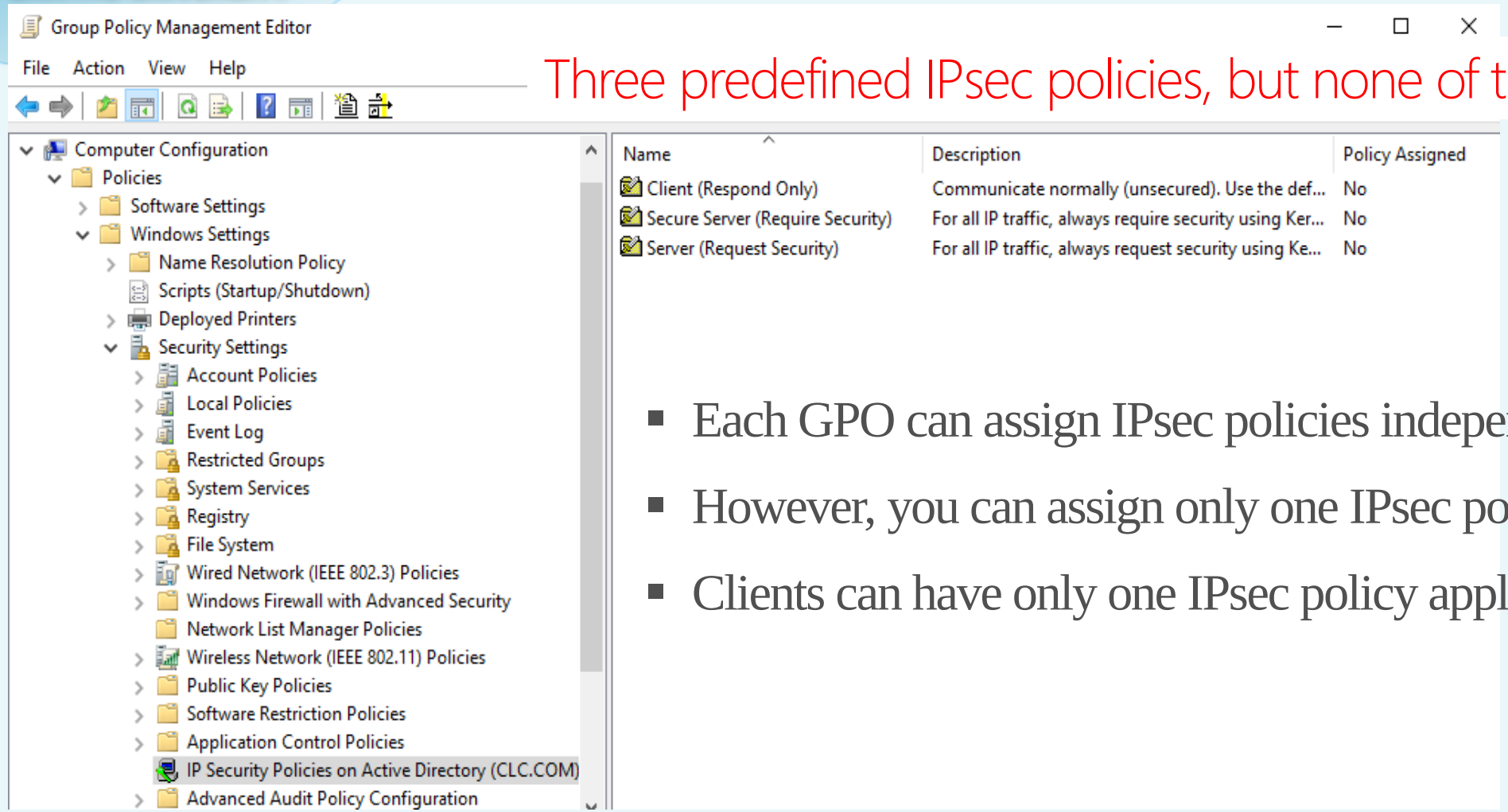
Protecting Data in Transit

Configuring IPsec

- Two different places that IPsec settings can be configured in a Microsoft Windows environment:
  - IPsec Security Policy snap-in.
  - Windows Firewall with Advanced Security

Protecting Data in Transit

Configuring Ipsec: Using a GPO



Three predefined IPsec policies, but none of them are assigned

- Each GPO can assign IPsec policies independently of other GPOs.
- However, you can assign only one IPsec policy within a single GPO.
- Clients can have only one IPsec policy applied to them at a time

Protecting Data in Transit

Configuring Ipsec: Using a GPO

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecured). Use the def...	No
Secure Server (Require Security)	For all IP traffic, always require security using Ker...	No
Server (Request Security)	For all IP traffic, always request security using Ke...	No

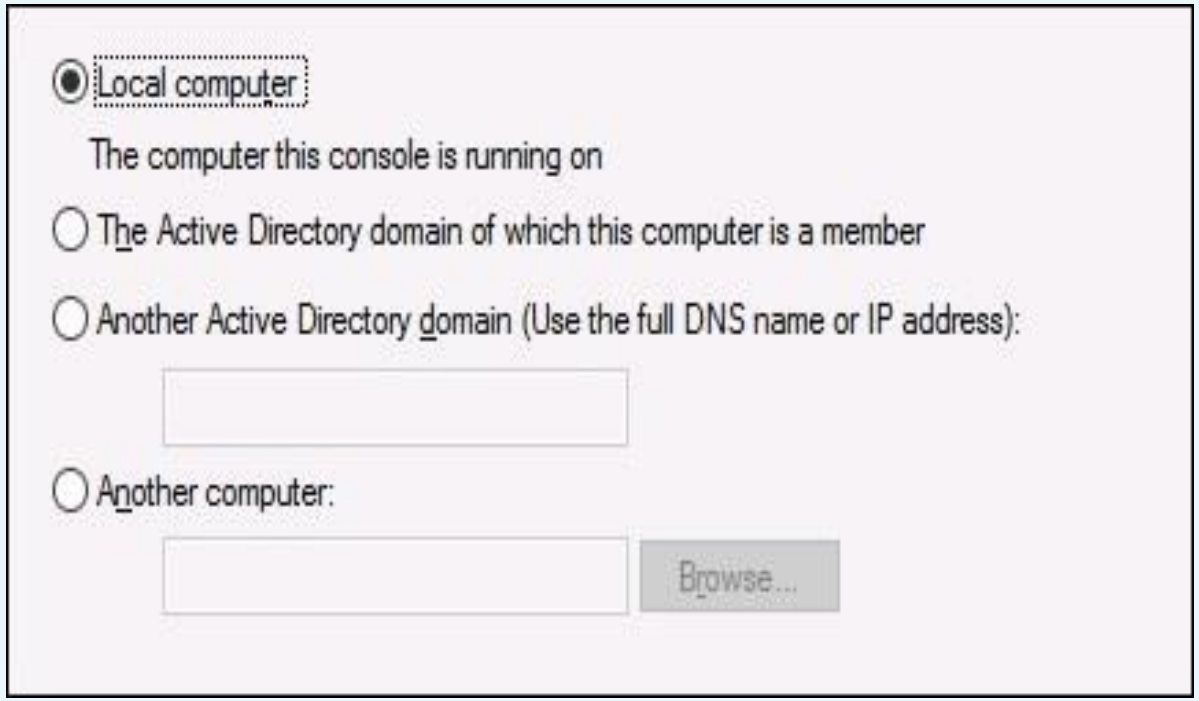
- **Client (Respond Only):** computers to negotiate security and authentication methods when requested.
- **Server (Request Security):** a computer to always request security by using the Kerberos V5 authentication protocol for all IP traffic, and allows unsecured communications with the clients that donot response to the request
- **Secure Server (Require Security)**: a computer to always require a secure connection for all IP traffic and to block untrusted computers.
  - Donot allow unsecured communication

Protecting Data in Transit

IPsec Security Policy snap-in

- The console for manipulating IPsec settings accessed via MMC

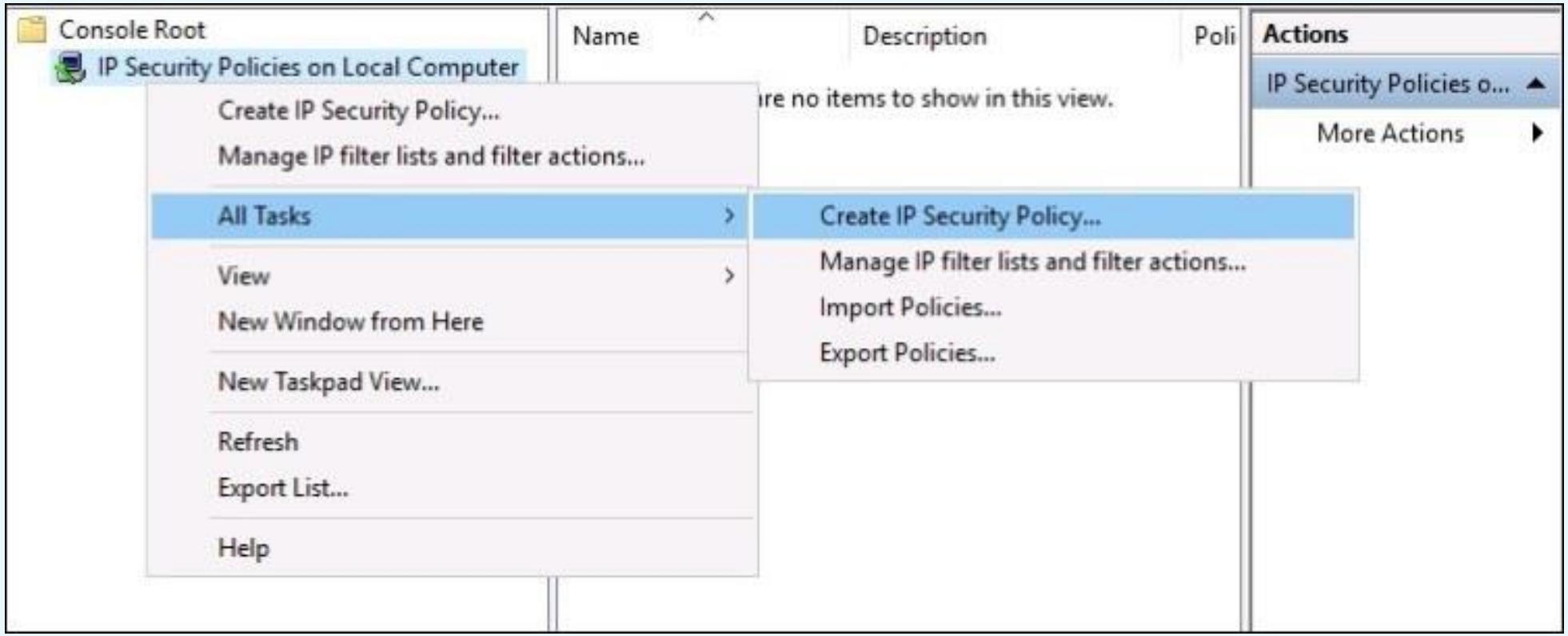
- Open MMC and add the IP Security Policy Management snap-in.
- You can view either the local IPsec policy of the machine or open the IPsec policy for the domain itself



Protecting Data in Transit

IPsec Security Policy snap-in

- Once inside, you can start creating your own by using the Create IP Security Policy… by right clicking on IP Security Policies.



Protecting Data in Transit

Configuring IPsec: Using WFAS

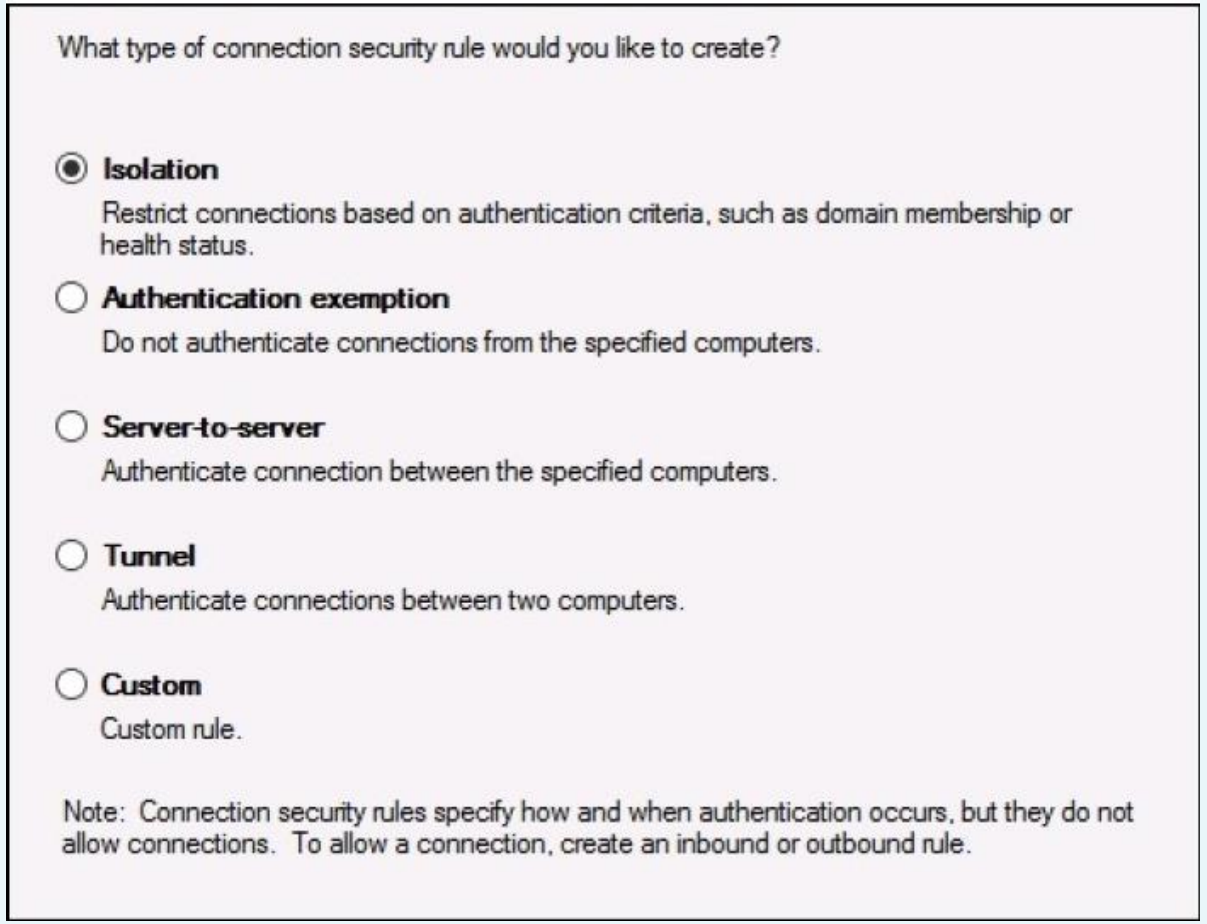
- The newer platform used for establishing IPsec connection rules is the Windows Firewall with Advanced Security

- Open WFAS
- Navigate to the **Connection Security Rules**, then right-click and choose **New Rule...**

Protecting Data in Transit

Configuring Ipsec: Using WFAS

- Once inside, you start to see that the options available



Protecting Administrative Access

Protecting Administrative Access

- Administrators are some of the most wanted targets
- Attackers might try to obtain access to an administrator's username, password, or even workstation or laptop
- Many types of techniques to steal user credentials and obtain access to data and services
- Grant users and administrators the lowest level of privilege needed to perform their everyday activities
- Administrators and developers need to have separate accounts for day-to-day activities

Protecting Administrative Access

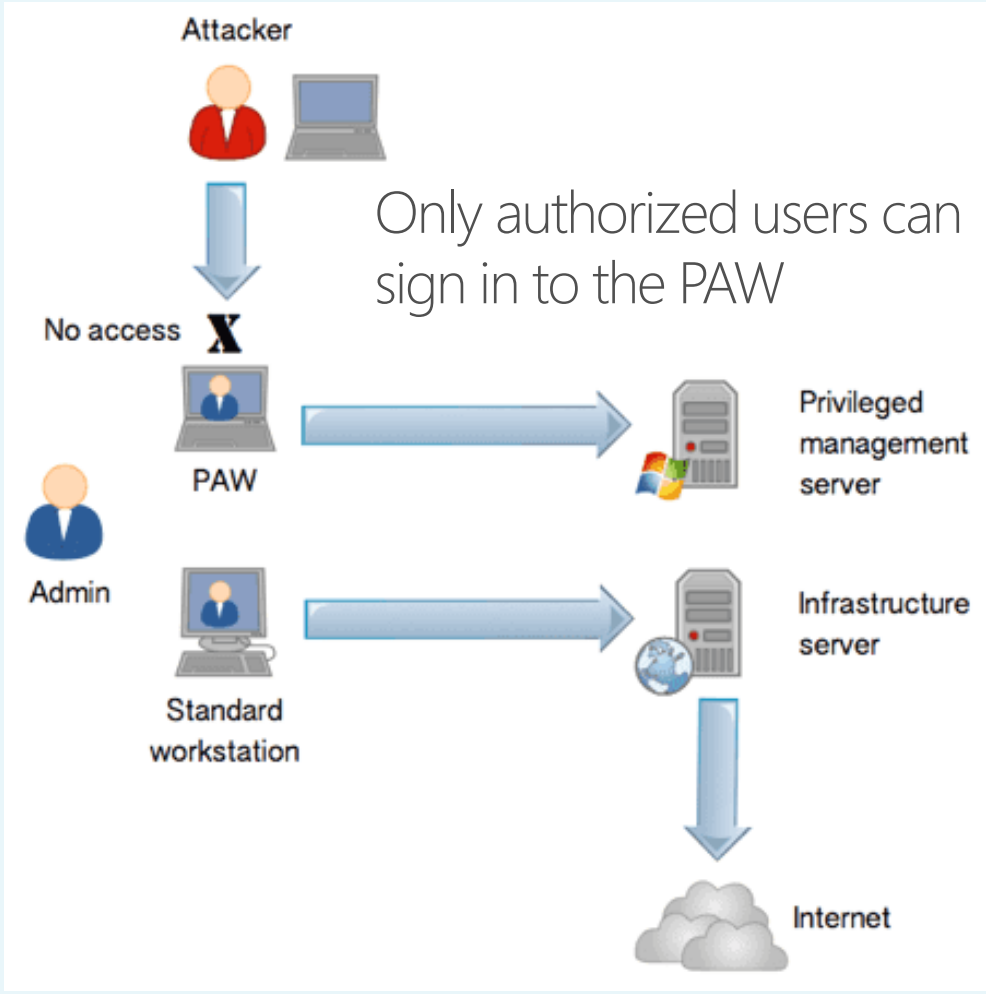
Privileged Access Workstations

- One way to mitigate the risk of an attack on an administrator's credentials is to use a Privileged Access Workstation (PAW)
  - secure administrative host: the computer that is used only for performing administrative tasks.

Protecting Administrative Access

Privileged Access Workstations

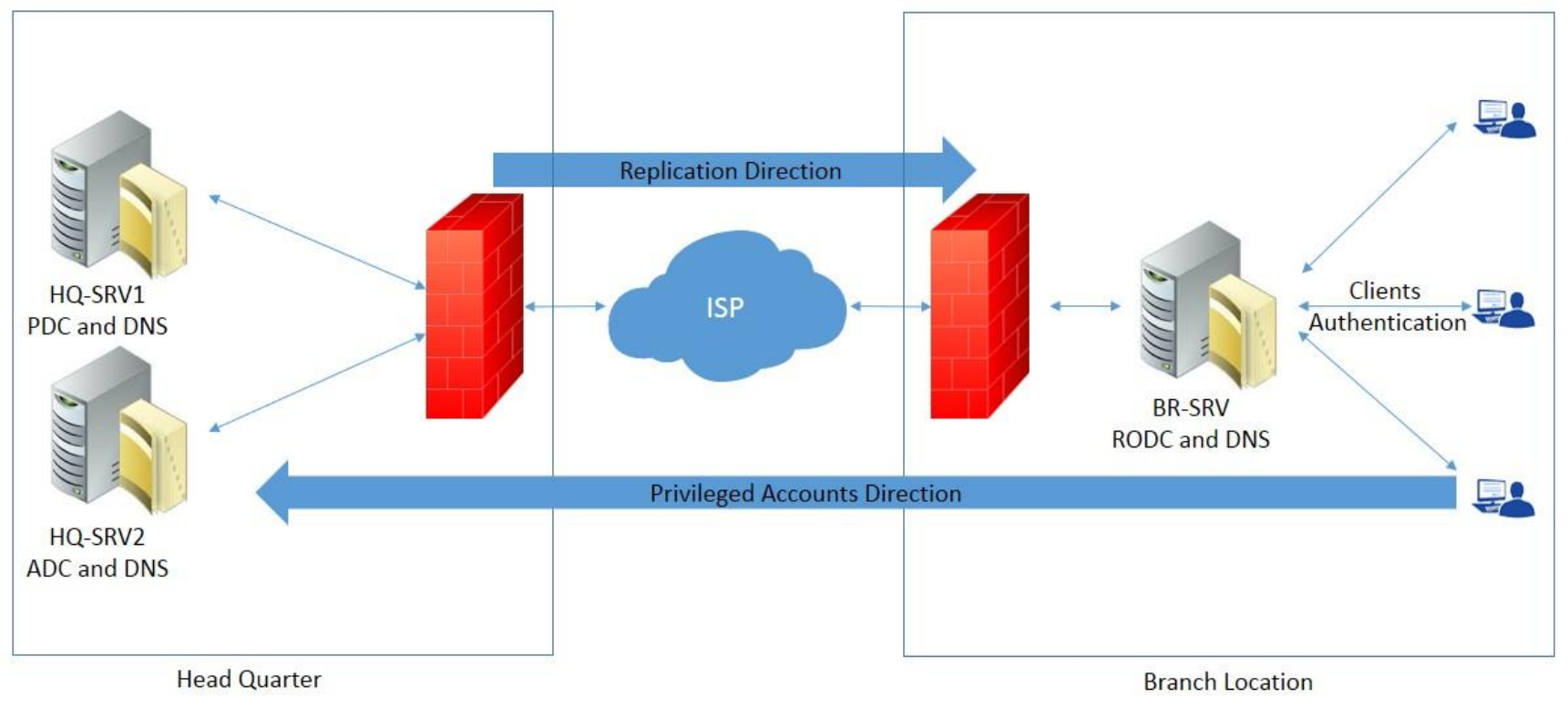
- Configured options:
  - Device Guard and AppLocker policies: to allow only authorized applications to run on PAW.
  - Credential Guard: protect the credentials.
  - BitLocker: protect the boot environment and the hard disk data.
  - Control access by using a firewall



Protecting Administrative Access

Securing Domain Controllers

- If an attacker gains access to domain controllers, the attacker will have access to all of the domain objects.



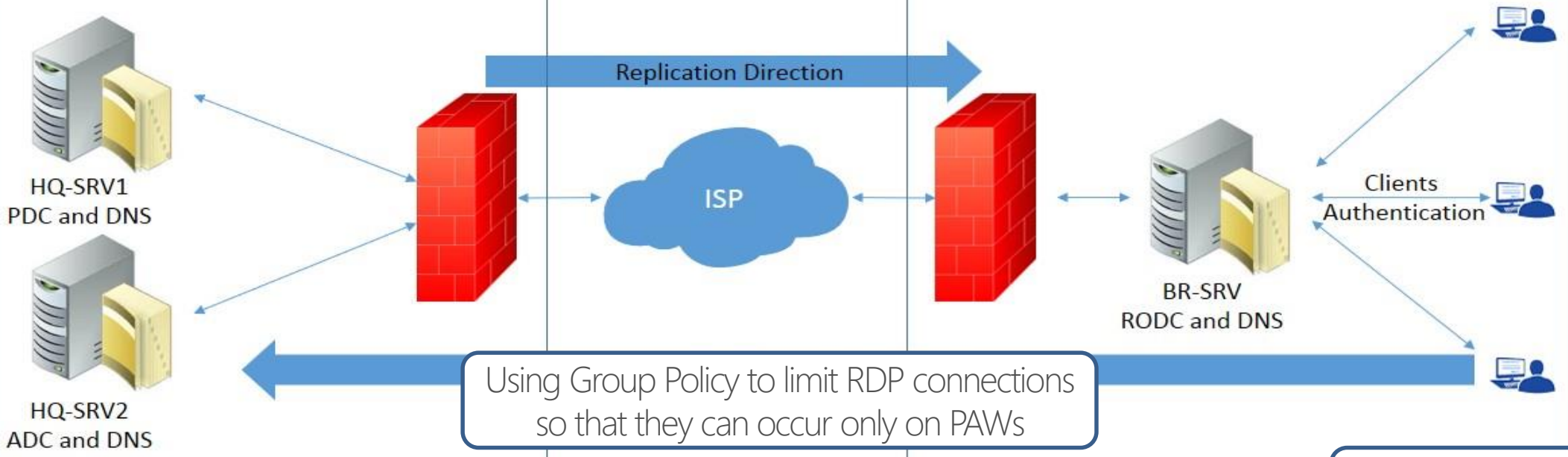
Protecting Administrative Access

Securing Domain Controllers

Regularly update domain controllers

Control the execution of executables and scripts on the DC with AppLocker and Device Guard

Configure Windows Firewall with Advanced Security



Using Group Policy to limit RDP connections so that they can occur only on PAWs

Deploy DCs on Server Core

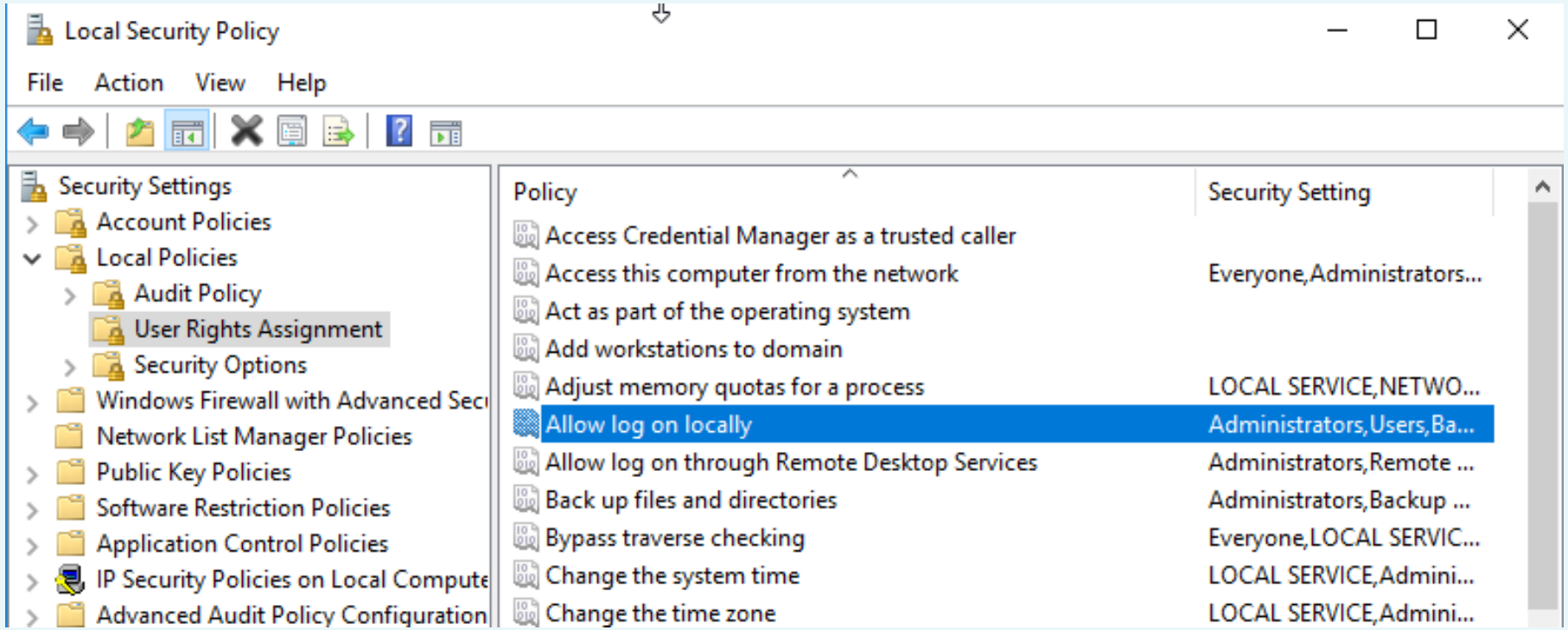
Deploy DCs on hardware that includes a Trusted Platform Module (TPM) chip, and configure all volumes with BitLocker Drive Encryption

Read-only domain controllers (RODC) in branch offices

Protecting Administrative Access

Restricting Logon Access

All servers should be configured to allow only administrators to physically log on to the console



General security best practices

General security best practices

Get rid of perpetual administrators

- Sometimes we need only to rely on ourselves to secure our systems.
- Get rid of perpetual administrators
  - Do all of your IT staff have domain admin rights the day they are hired?
  - Do any of your IT staff have access to the built-in domain administrator account password?
  - Do you have regular users whose logins have administrative privileges on their own computers?
- These are all terrible ideas!

General security best practices

Use a different computer to accomplish administrative tasks

- Utilizing a separate computer altogether when accomplishing administrative-level tasks.
- This would certainly help to keep your administrative system secure
- This way a compromise of the normal computer doesn't necessitate a compromise of the entire environment

=> never administer Active Directory from the same place that you browse Facebook

General security best practices

Using Administration-Only Accounts with Run As

- Run as Different User and Run as Administrator commands

CANTHO UNIVERSITY

General security best practices

Never browse the Internet from servers

- We spend all day working on servers, and very often have to reach out and check something from a web browser.
- It is so easy to pick up bad things from the Internet, especially on servers because if any machines in our network are running without antivirus protection
- Don't even do it for websites that you trust.
- A man-in-the-middle attack or a compromise of the website itself can easily corrupt your server. It's much easier to rebuild a client computer than it is a server.

General security best practices

Role-Based Access Controls

- Role-Based Access Control (RBAC) is an ideology all about separating job roles and duties
- When think about separating our employees' job roles from an IT perspective, we traditionally think in terms of Active Directory groups
- AD groups still empower administrators with full access to the groups themselves.
- RBAC technologies divide up roles at a different level: focuses more on employee job descriptions than access restrictions.

General security best practices

Just Enough Administration

- A great example of an RBAC technology included in Windows Server 2016 is Just Enough Administration (JEA), part of PowerShell 5.0.
- JEA provides a way to grant special privileged access for people, without needing to give them administrative rights
- Adding someone to the Administrators group on a server so that they can do their job is quite common, but JEA is a first step away from that necessity.
- JEA permits users to have access only to run particular PowerShell commands and cmdlets at an administrative level

General security best practices

Just Enough Administration

- If a user working within a JEA and try to invoke a cmdlet not part of the "allowed" cmdlets, PowerShell pretends like it doesn't even recognize that cmdlet.
- A DNS administrator occasionally need to restart the DNS services: Adopting the JEA/RBAC, not have administrative rights but have JEA-based rights within PowerShell
- Restarting the DNS service requires access to use the Restart-Service cmdlet
- JEA: provide the user the Restart-Service cmdlet, but only give permissions to restart DNS services. If the user tried to Restart-Service on winrm, they would be denied.

General security best practices

Device Guard

- A technology about limiting which applications allowed to run and install on your systems
- Have a white-list of allowed applications: enforce that only applications having a code signing certificate allowed to run
- Apps that are not trusted natively by Microsoft, or are not explicitly trusted by you, simply don't run.
- Device Guard is unique in that it manages both user and kernel mode processes.
- Even if an attacker gains access to the operating system of your server, if you have Device Guard policies in place, they will not be able to launch and run malicious software

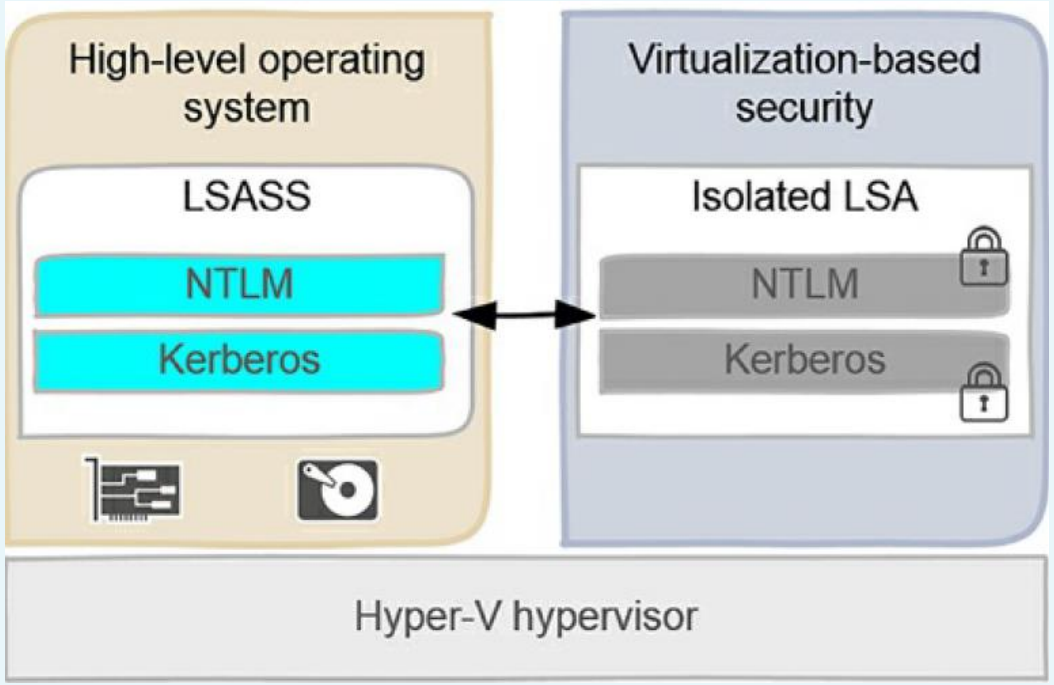
General security best practices

Credential Guard

- Prior to Windows 10 and Windows Server 2016, password hashes and tickets were stored on the hard drive of a machine, in the Local Security Authority (LSA).
- Those hashes were very easily stolen by using simple, free tools available on the Internet.
- Credentials Guard protects your domains credentials from being compromised.

General security best practices

Credential Guard



- NTLM and Kerberos secrets stored in user-mode memory in-side process
- Credentials accessible to attackers

- Credential Guard enabled
- NTLM and Kerberos secrets stored in an isolated protected LSA process

General security best practices

Improved detection

- Enhanced Logs: Log new audit events to better detect malicious behavior by providing more detailed information to security operation centers.
- Integration with systems management: Operations Management Suite (OMS) and other SIEM systems, can take advantage of this information to provide intelligence reports on potential breaches in the datacenter environment.

Summary

- Security for client machines, networks, cloud resources, and most importantly your data
- No single solution to secure your infrastructure, it requires many different technologies all working together to provide safety for your resources
- This chapter provides examples of security measures and technologies can be utilized
- Apps which transmit or store data unencrypted need to be modified or dumped
- Protection of information is essential to the longevity of our businesses