HACKTHEBOX

REDTEAMRD

Lateral Movements

Attacks & Defense

Helen Rodriguez
RedRioT

Julio Ureña
PlainText

Nov 2022

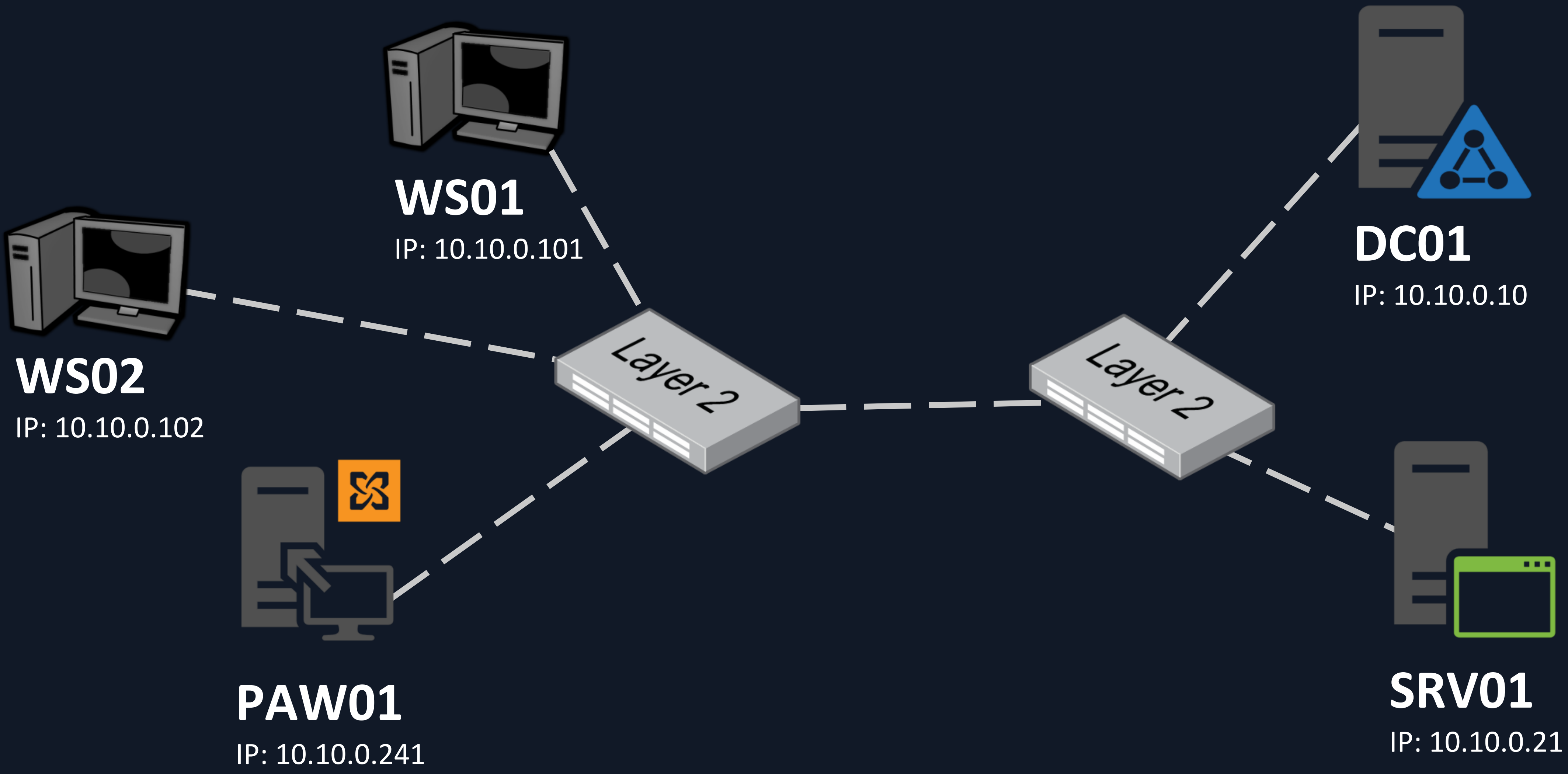
Agenda

- Lateral Movements * Attacks & Defense

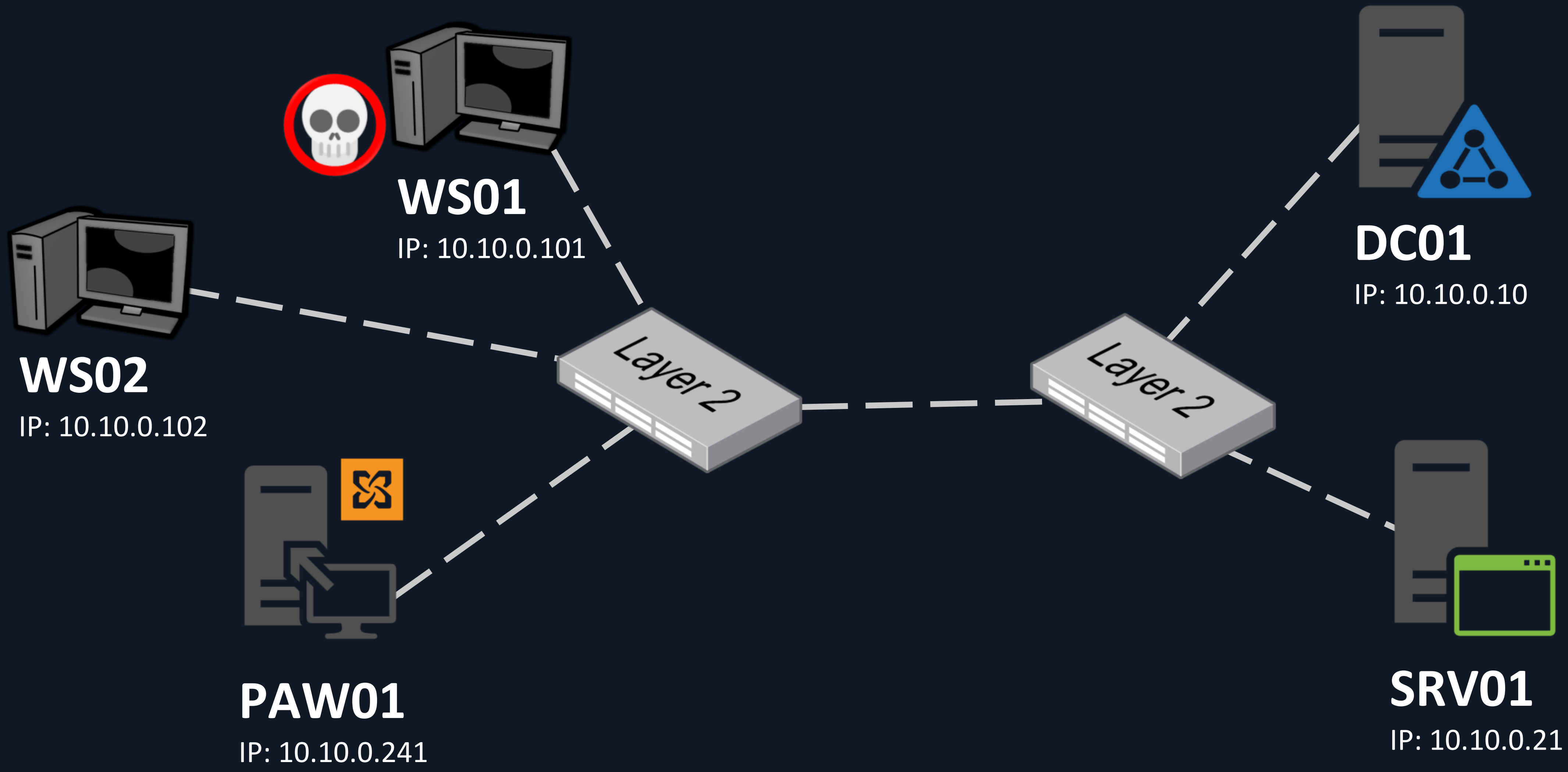
  Helen Rodriguez & Julio Ureña
- Anuncios
- Rifas & Premios
- Coffee Break

Movimientos Laterales

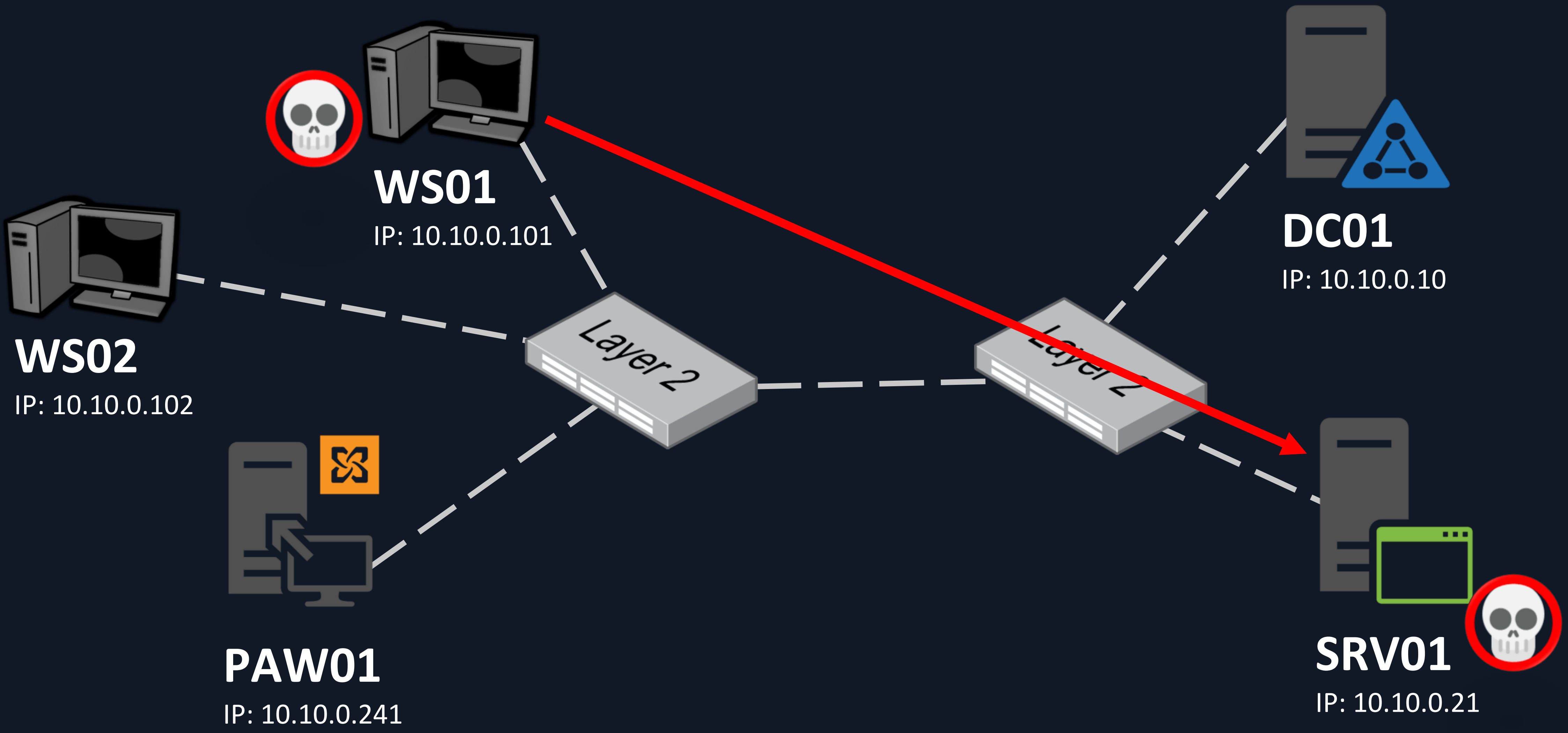
Diagrama de Red



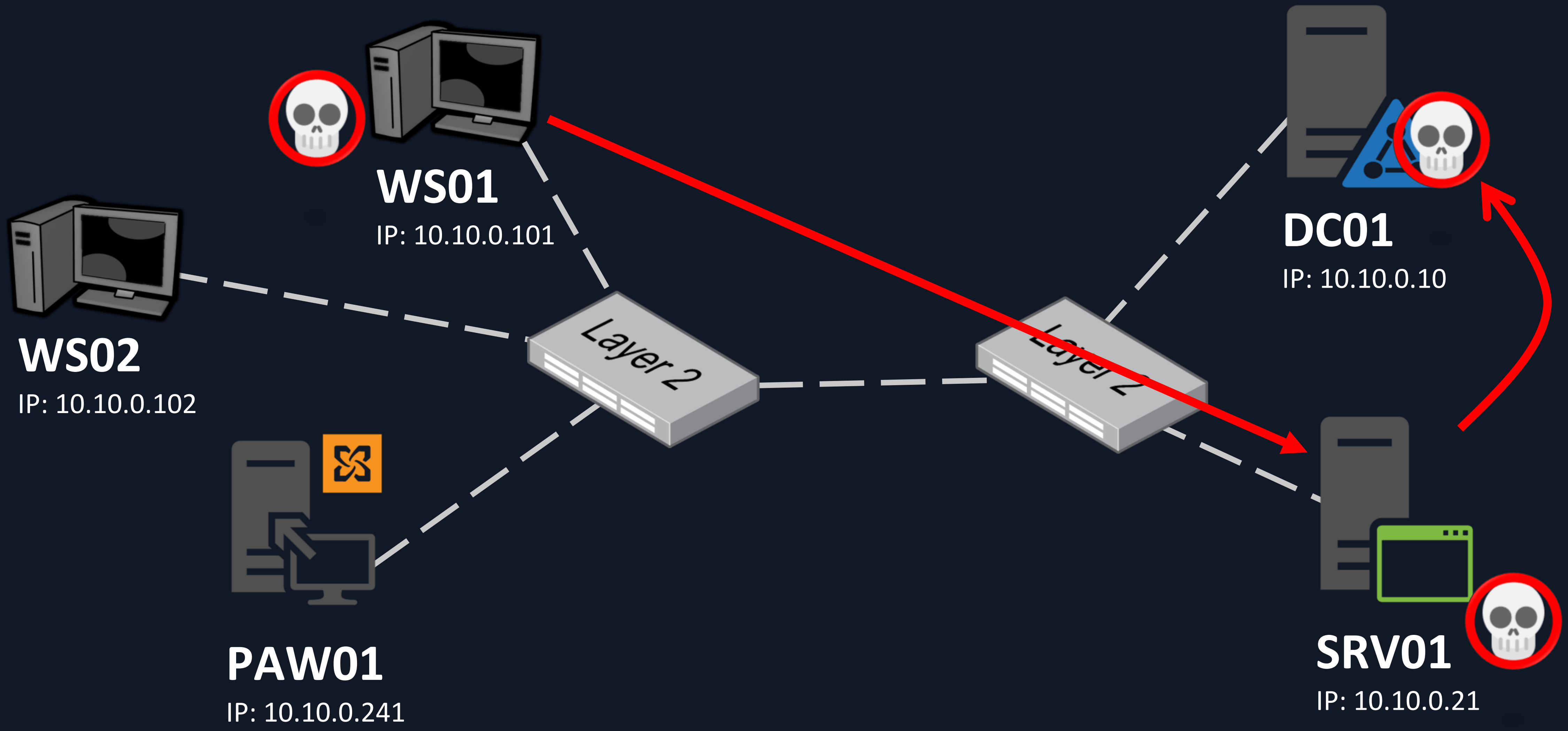
Ataque #1


WS01
IP: 10.10.0.101
WS02
IP: 10.10.0.102
PAW01
IP: 10.10.0.241
Layer 2
Layer 2
DC01
IP: 10.10.0.10
SRV01
IP: 10.10.0.21

Ataque #1


WS01
IP: 10.10.0.101
WS02
IP: 10.10.0.102
PAW01
IP: 10.10.0.241
Layer 2
Layer 2
DC01
IP: 10.10.0.10
SRV01
IP: 10.10.0.21

Ataque #1


WS01
IP: 10.10.0.101
WS02
IP: 10.10.0.102
PAW01
IP: 10.10.0.241
Layer 2
Layer 2
DC01
IP: 10.10.0.10
SRV01
IP: 10.10.0.21

Ataque #1

Acceso a **WS01** vía Phishing

WS01 -> Mimikatz: Extracción de Credenciales

- Password reutilizado en (WS02, SRV01)

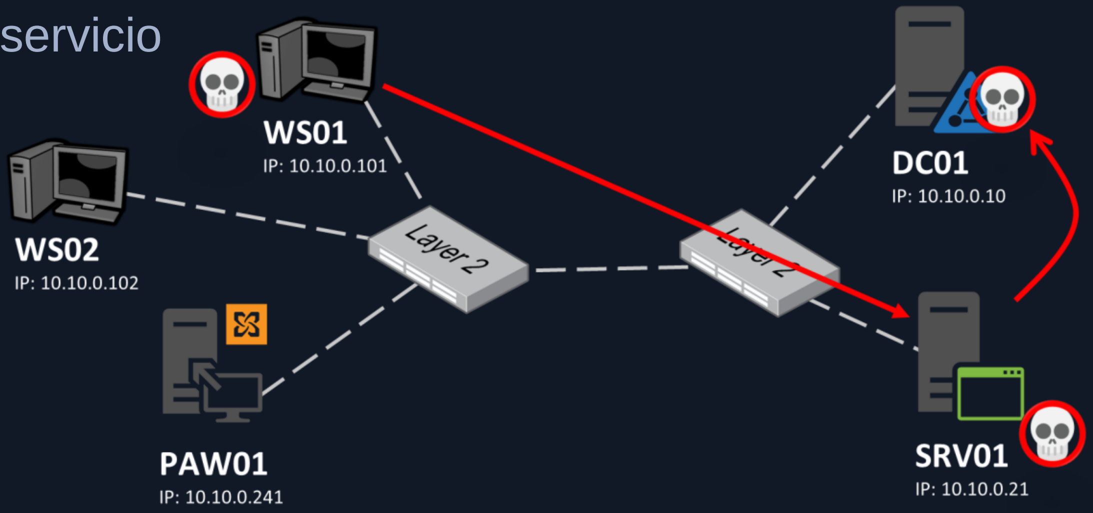
Movimiento Lateral a **SRV01** vía PowerShell Remoting

SRV01 -> Mimikatz: Extracción de Credenciales

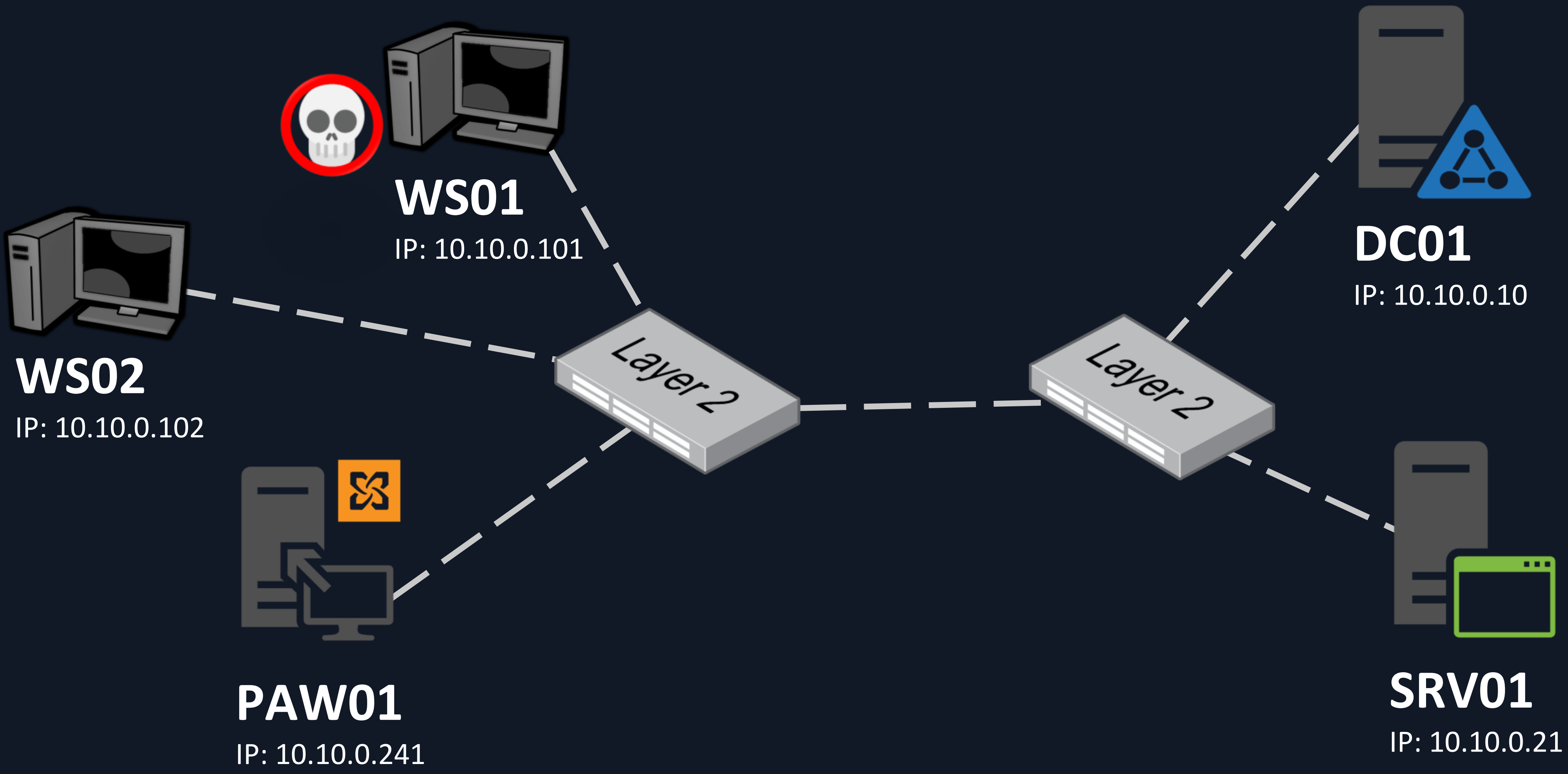
- Cuenta de Domain Admin en SRV01 registrada en un servicio

Movimiento Lateral a **DC01** vía RDP

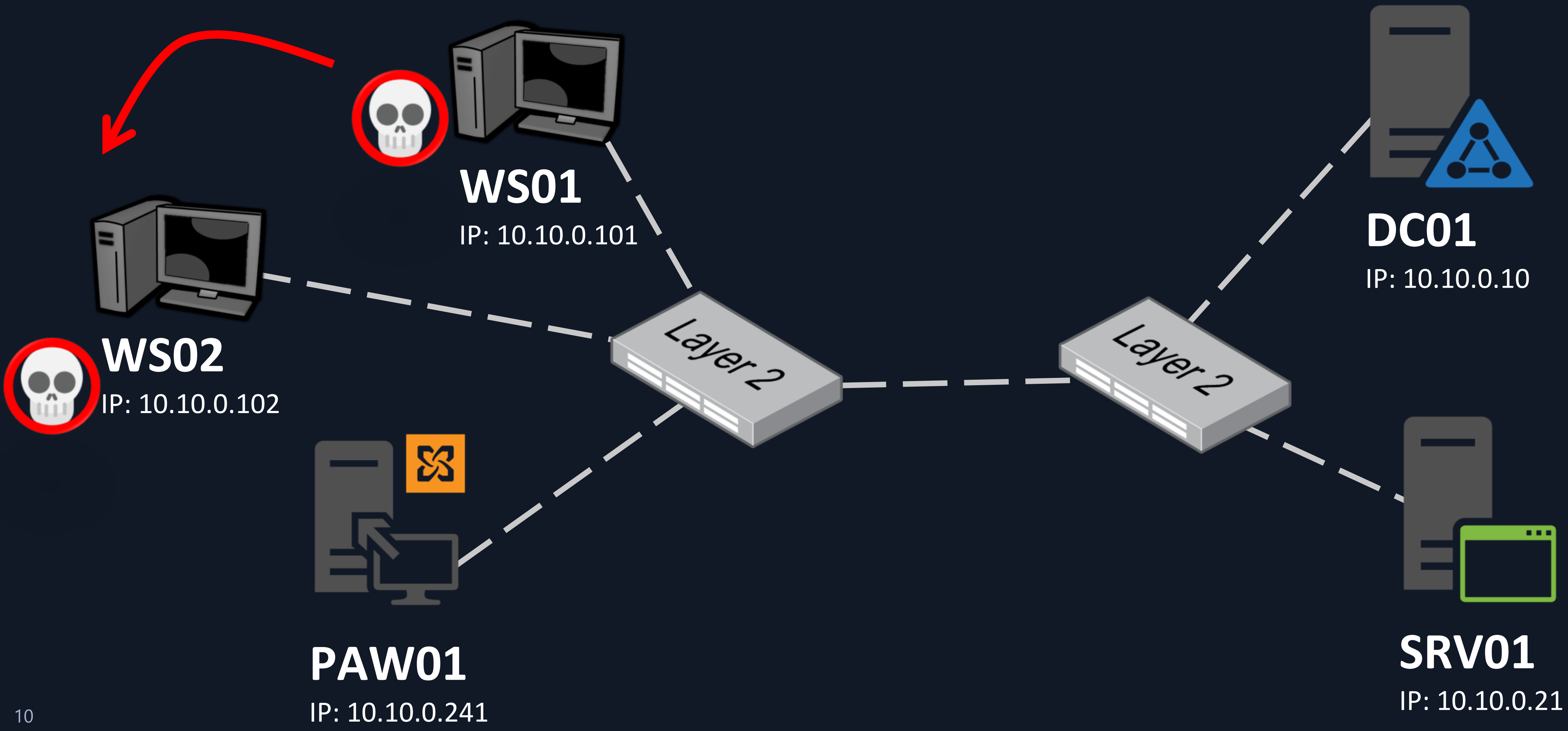
DC01 -> Mimikatz: DCSync Attack



Ataque #2


WS01
IP: 10.10.0.101
WS02
IP: 10.10.0.102
PAW01
IP: 10.10.0.241
Layer 2
Layer 2
DC01
IP: 10.10.0.10
SRV01
IP: 10.10.0.21

Ataque #2



WS01

IP: 10.10.0.101

WS02

IP: 10.10.0.102

PAW01

IP: 10.10.0.241

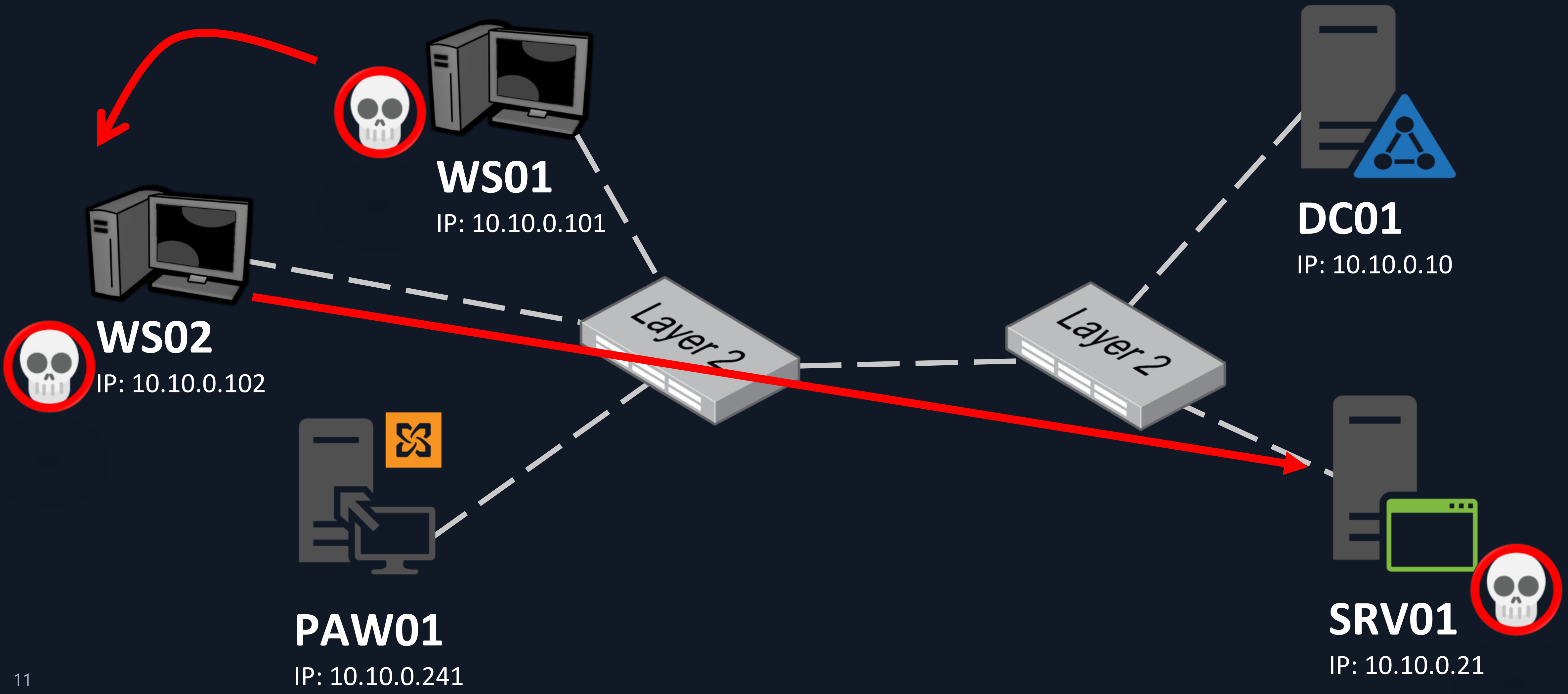
DC01

IP: 10.10.0.10

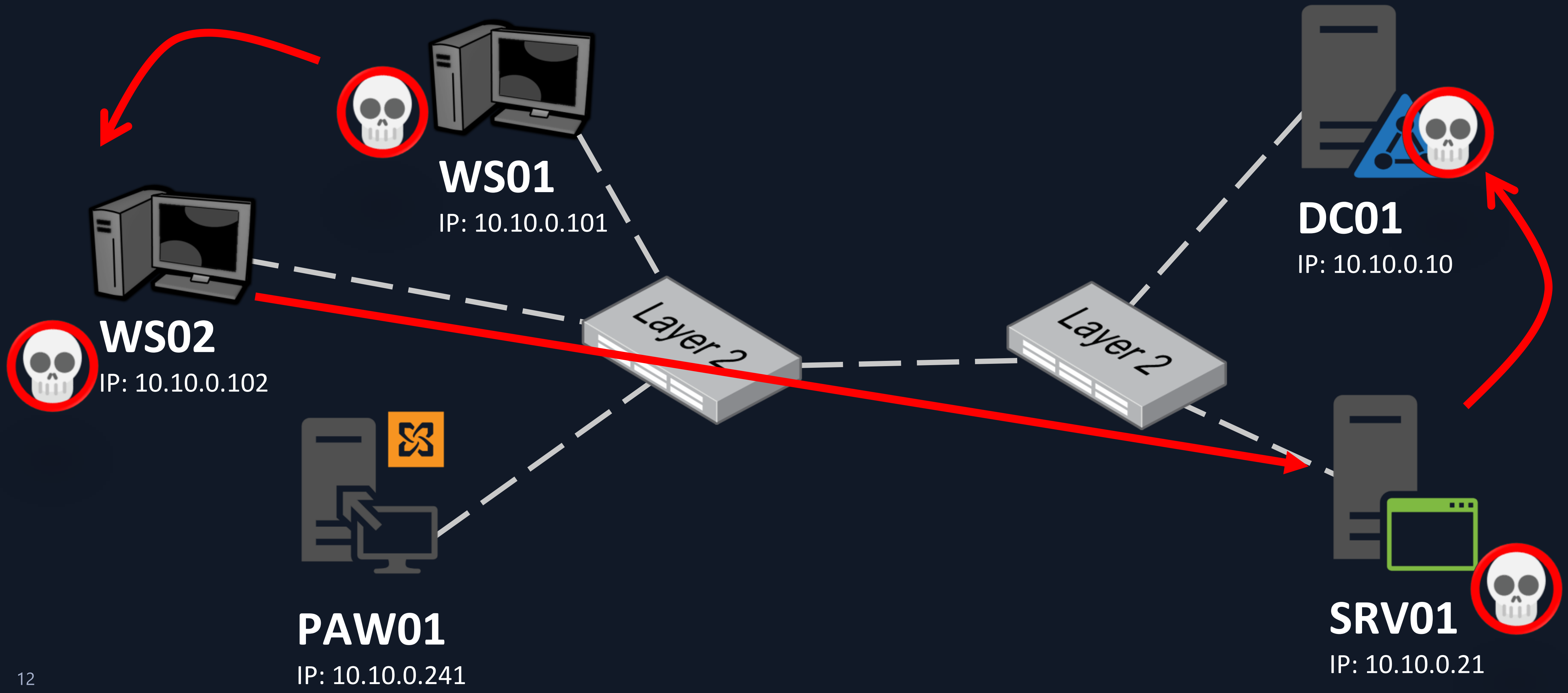
SRV01

IP: 10.10.0.21

Ataque #2


WS01
IP: 10.10.0.101
WS02
IP: 10.10.0.102
PAW01
IP: 10.10.0.241
Layer 2
Layer 2
DC01
IP: 10.10.0.10
SRV01
IP: 10.10.0.21

Ataque #2


WS01
IP: 10.10.0.101
WS02
IP: 10.10.0.102
Layer 2
Layer 2
DC01
IP: 10.10.0.10
PAW01
IP: 10.10.0.241
SRV01
IP: 10.10.0.21

Ataque #2

Acceso a **WS01** vía Phishing

WS01 -> Mimikatz: Extracción de Credenciales

- Encontramos las credenciales del **Workstation Admins**

Movimiento Lateral a **WS01** vía PowerShell Remoting

WS02 -> Mimikatz: Extracción de Credenciales

- Esta es la estación de trabajo de Alina, Server Admin.

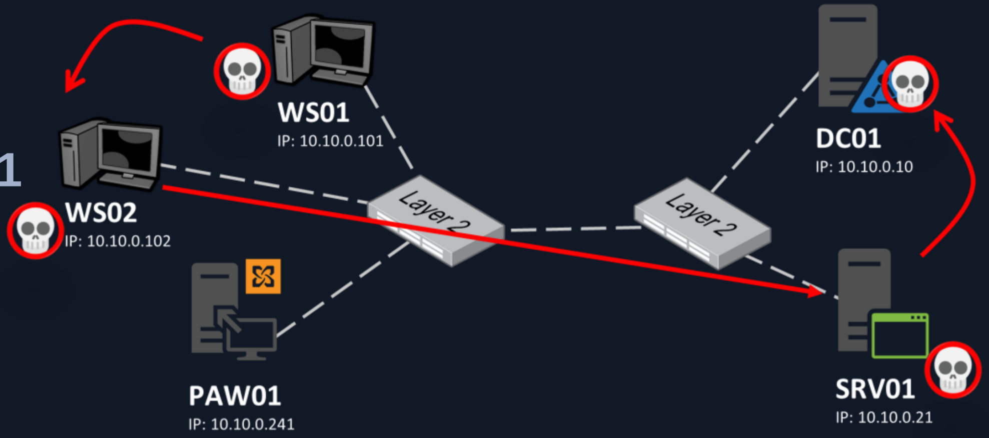
Movimiento Lateral a SRV01 via PSExec

SRV01 -> Mimikatz: Extracción de Credenciales

-   Cuenta de Domain Admin con una sección de RDP en **SRV01**

Movimiento Lateral a **DC01** vía RDP

DC01 -> Mimikatz: DCSync Attack



Defensa

RedRioT
Helen Rodriguez

Helen Rodríguez

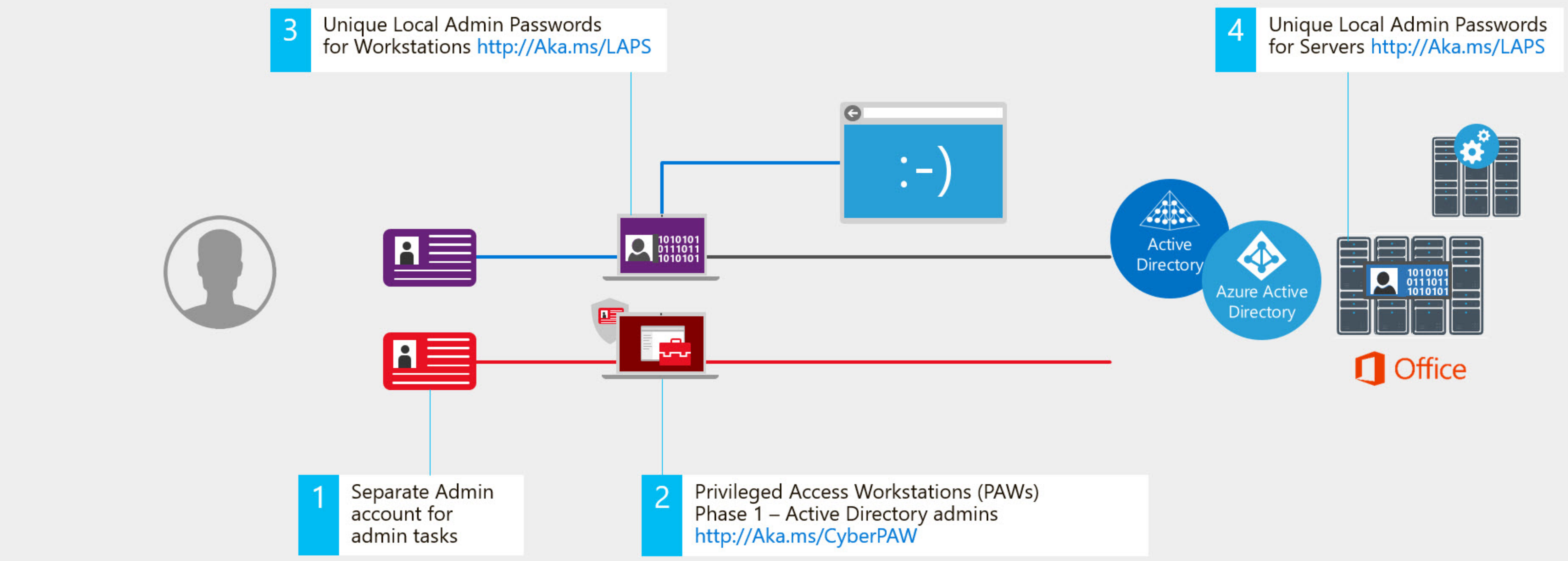
TECNÓLOGA DE SEGURIDAD INFORMÁTICA CON EXPERIENCIA EN CONSULTORÍA DE CIBERSEGURIDAD.

- Consultor certificado de CyberArk (PAM, EPM Y cem) .
- Auditoria de Procesos.
- Auditor TI y Gestión de Riesgos.

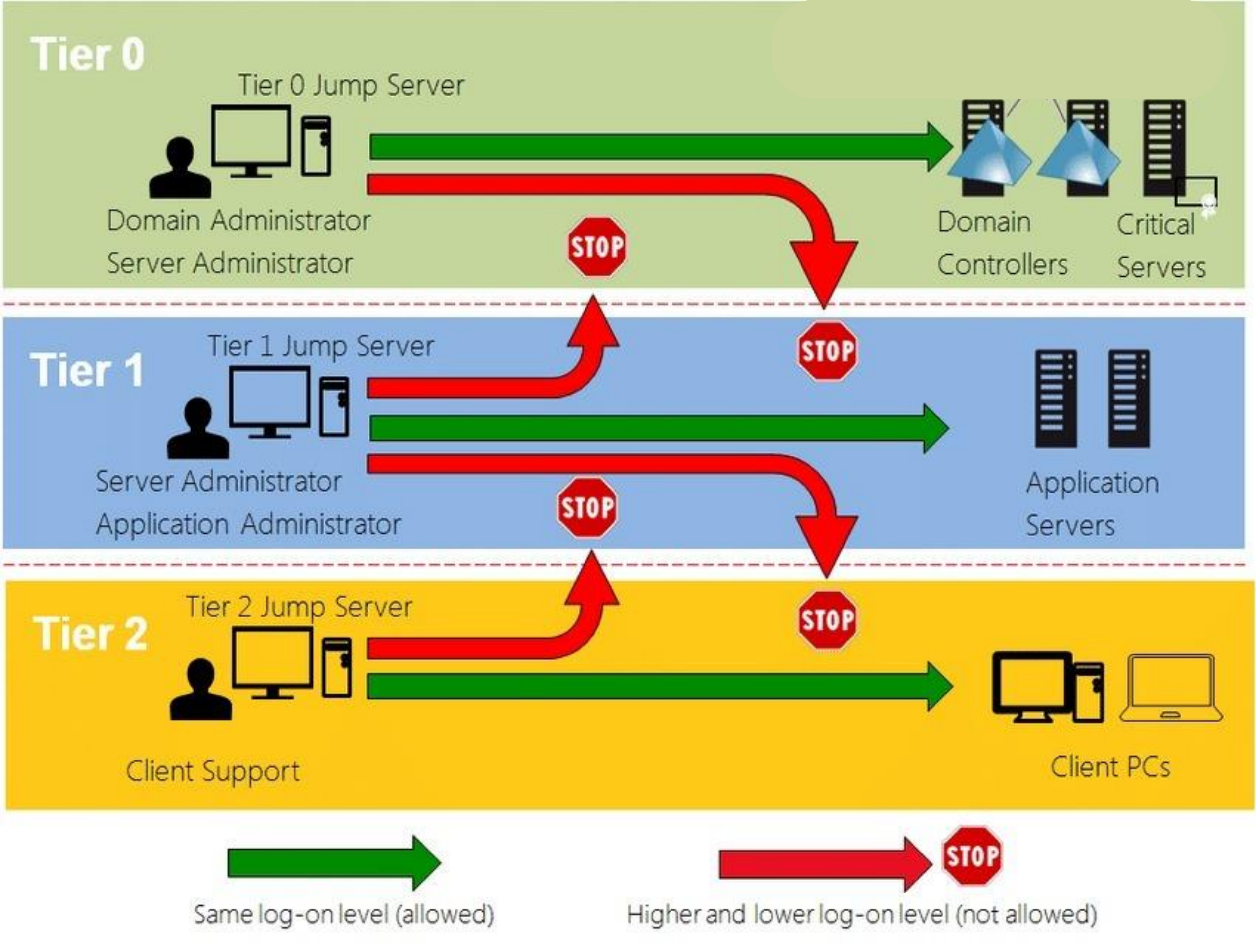
Encargada de auditar diversos sistemas, asegurando el correcto manejo de la información y de los usuarios que tienen acceso a ella.

YOU'RE AN ADMIN
2004
YOU'RE AN ADMIN
YOU'RE AN ADMIN
AND YOU'RE AN ADMIN
EVERYONE'S AN ADMIN!!
quickmeme.com

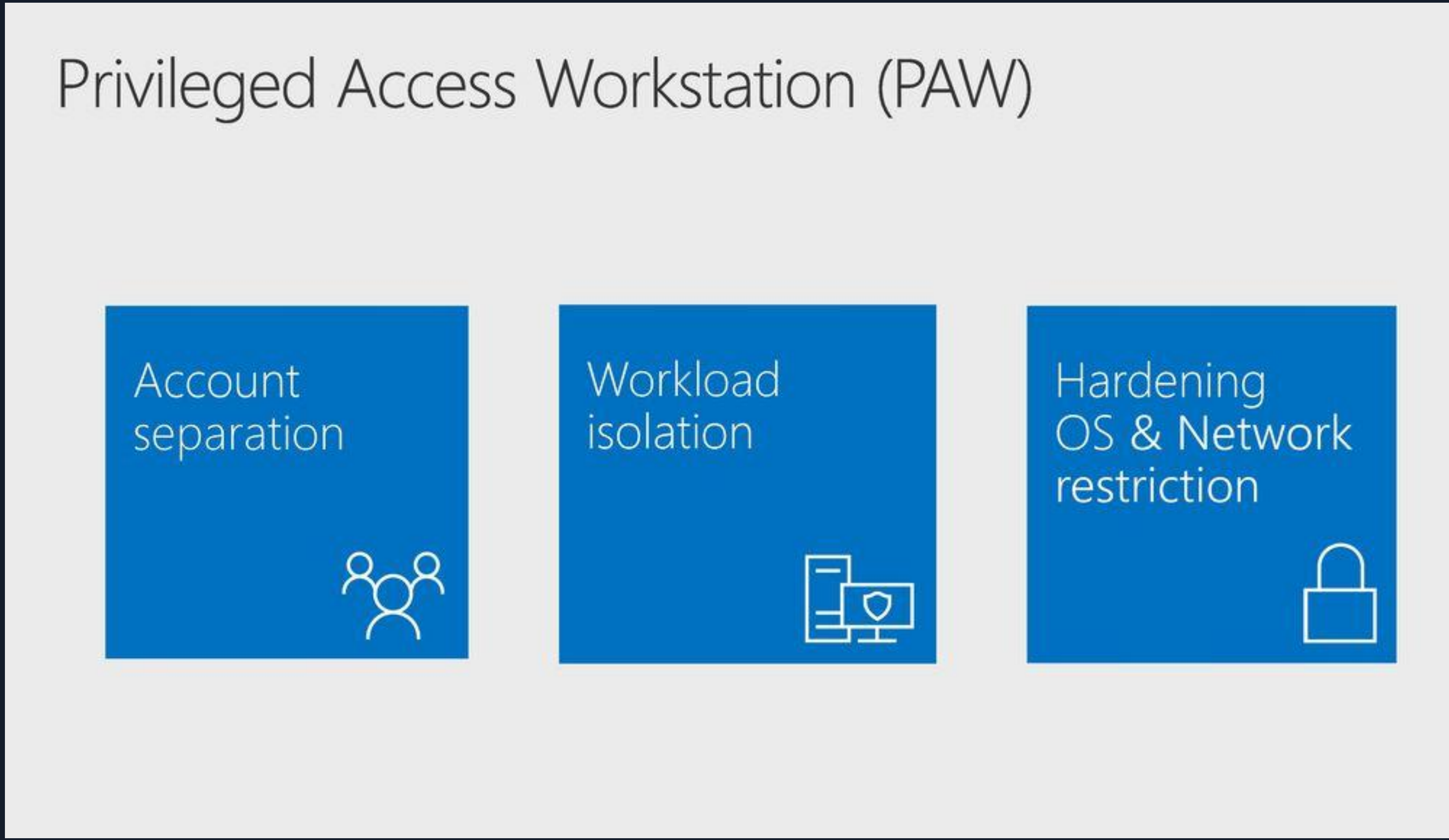
Admins . . .


3
Unique Local Admin Passwords for Workstations http://Aka.ms/LAPS
4
Unique Local Admin Passwords for Servers http://Aka.ms/LAPS
:-)
1010101
0111011
1010101
Active Directory
Azure Active Directory
Office
1
Separate Admin account for admin tasks
2
Privileged Access Workstations (PAWs) Phase 1 – Active Directory admins http://Aka.ms/CyberPAW

PARA SABER MAS SOBRE LAPS Y CÓMO CONFIGURARLO...


Tier 0
Tier 0 Jump Server
Domain Administrator
Server Administrator
STOP
Domain Controllers
Critical Servers
Tier 1
Tier 1 Jump Server
STOP
Server Administrator
Application Administrator
STOP
Application Servers
Tier 2
Tier 2 Jump Server
STOP
Client Support
Client PCs
STOP
Same log-on level (allowed)
Higher and lower log-on level (not allowed)

¿En qué consiste?



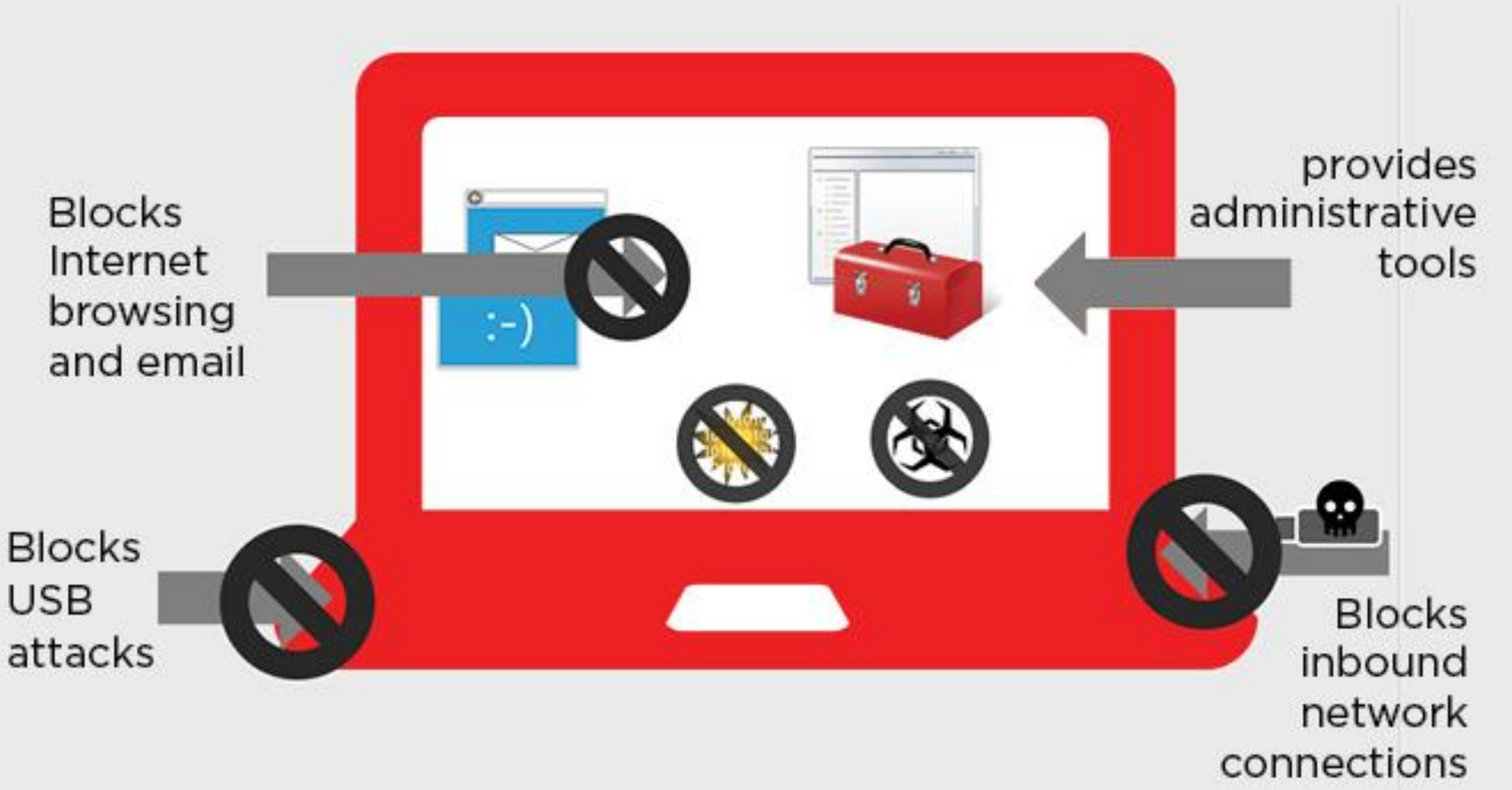
Privileged Access Workstation (PAW)

Account separation

Workload isolation

Hardening OS & Network restriction

Privileged Account Workstation



Blocks Internet browsing and email

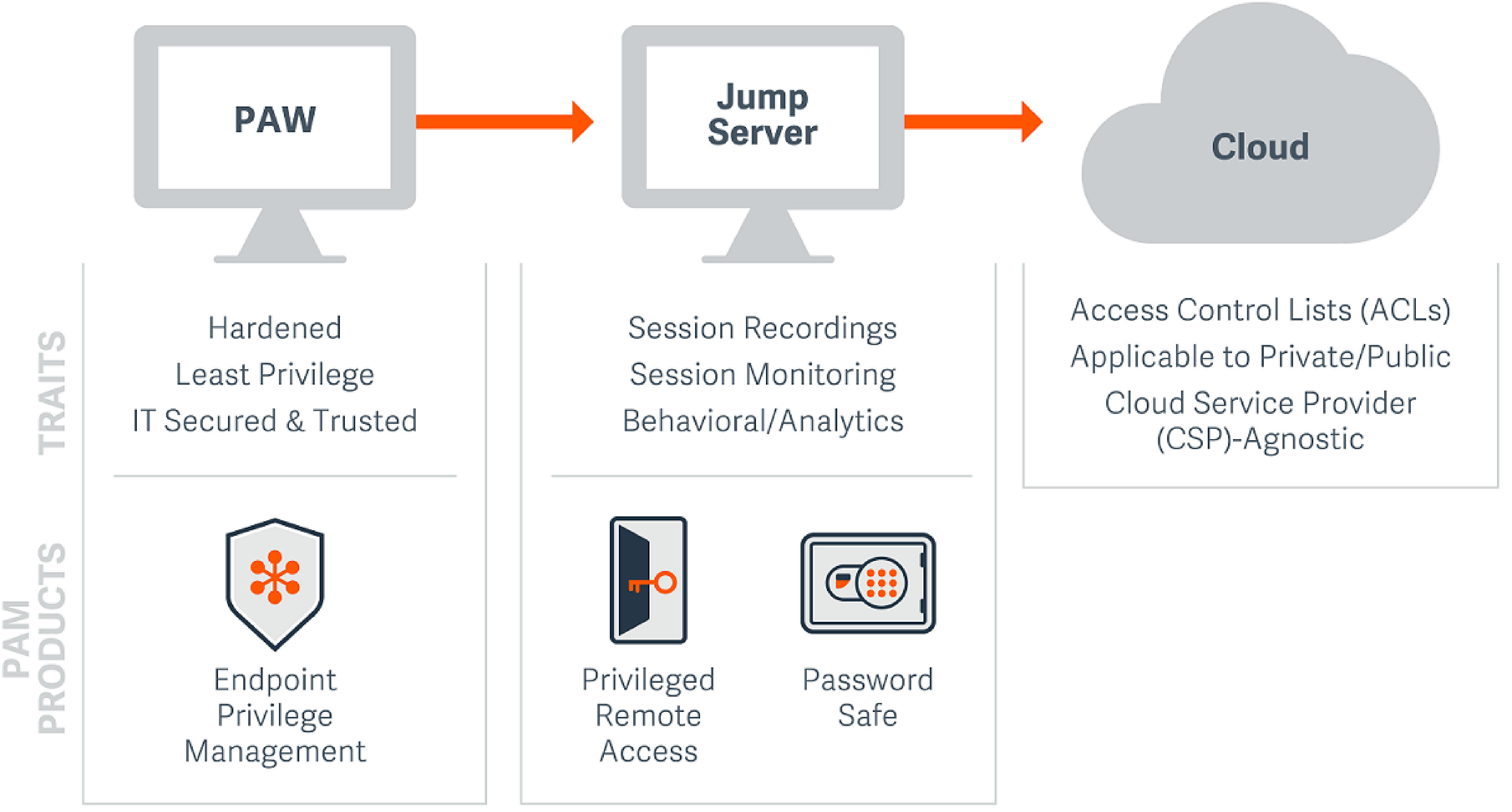
provides administrative tools

Blocks USB attacks

Blocks inbound network connections

CIS Benchmarks

Privileged Access Workstation (PAW) Diagram



PAW

Jump Server

Cloud

TRAITS

Hardened

Least Privilege

IT Secured & Trusted

Session Recordings

Session Monitoring

Behavioral/Analytics

Access Control Lists (ACLs)

Applicable to Private/Public

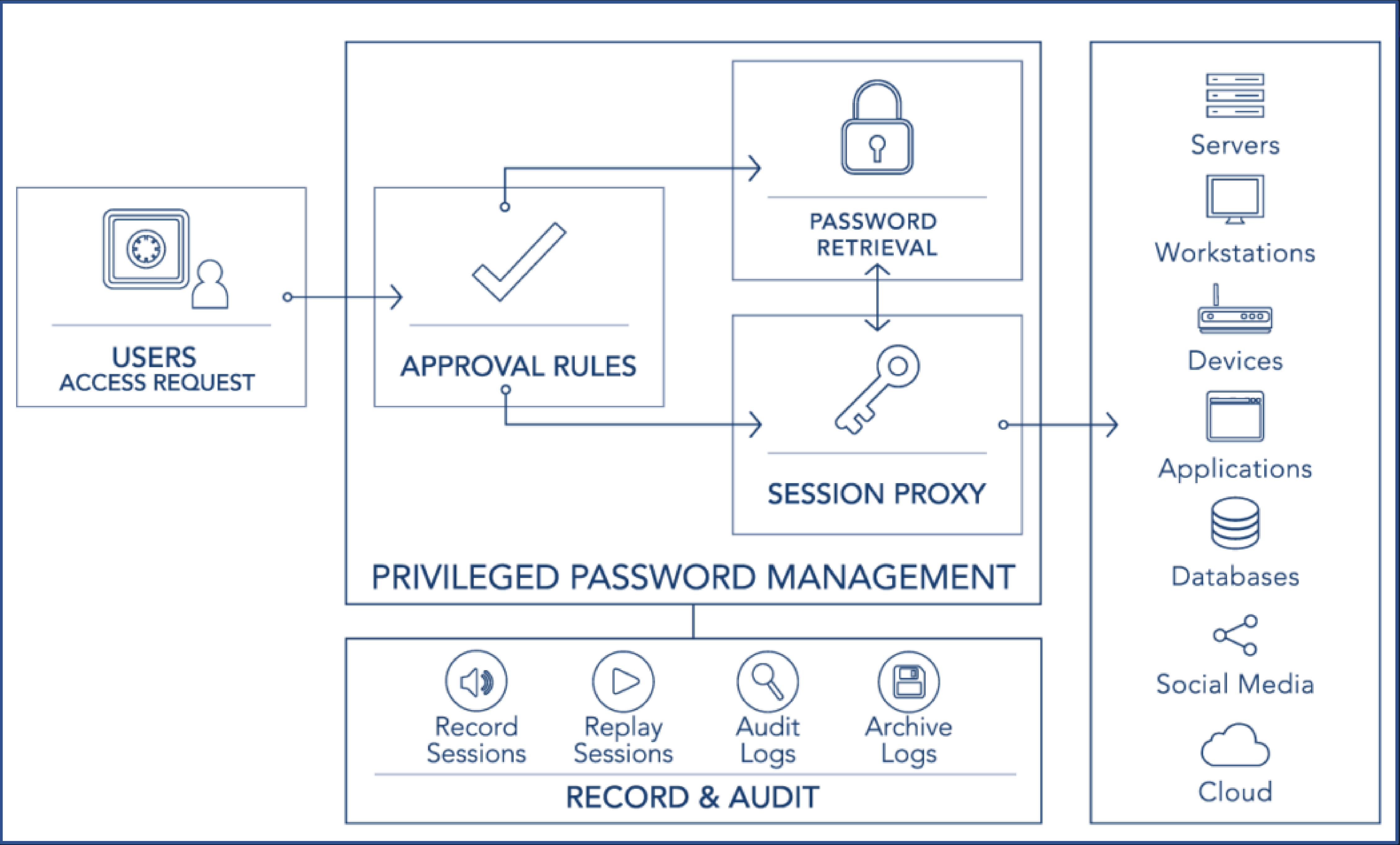
Cloud Service Provider (CSP)-Agnostic

PAM PRODUCTS

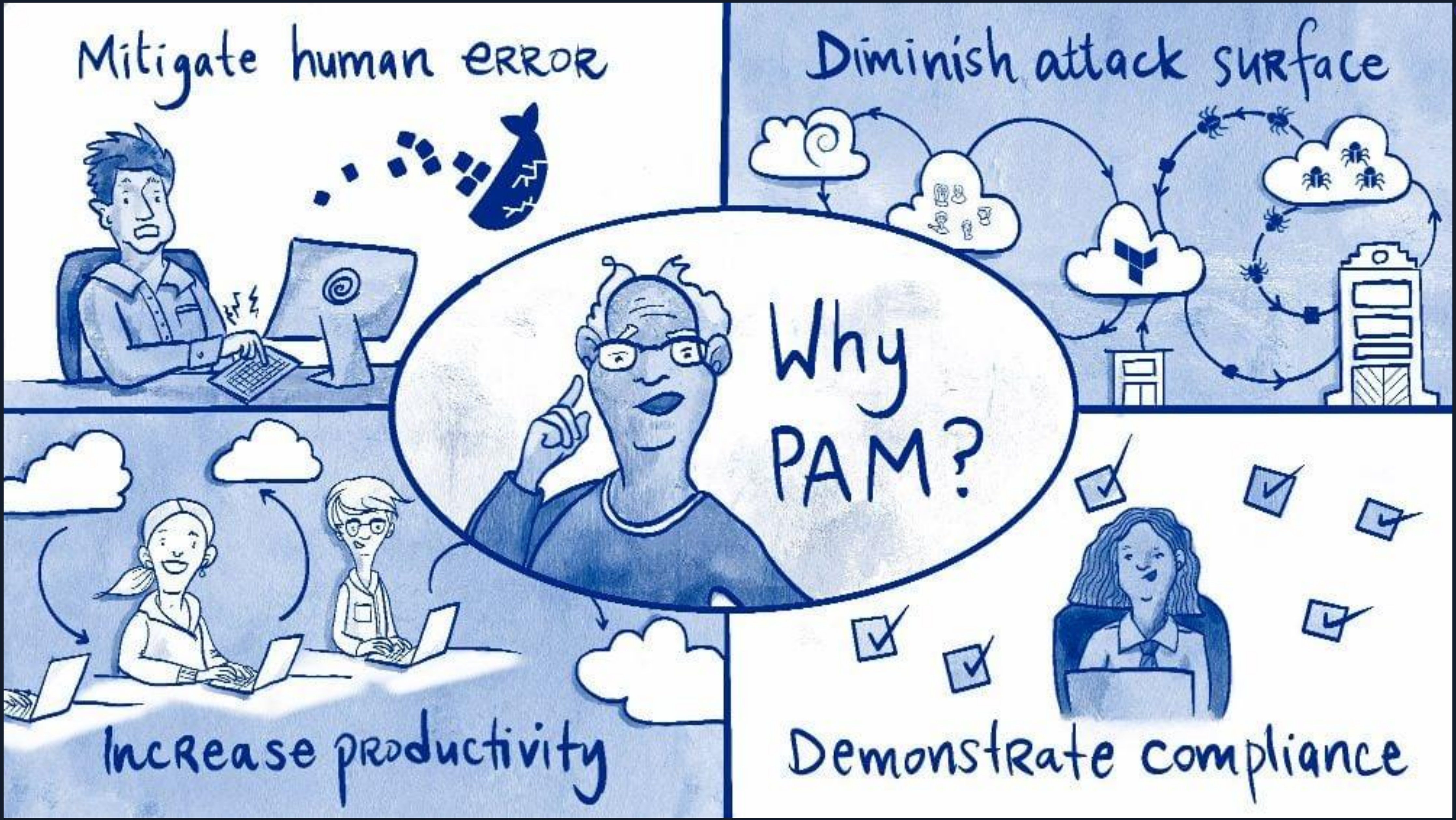
Endpoint Privilege Management

Privileged Remote Access

Password Safe


USERS
ACCESS REQUEST
APPROVAL RULES
PASSWORD RETRIEVAL
SESSION PROXY
PRIVILEGED PASSWORD MANAGEMENT
Record Sessions
Replay Sessions
Audit Logs
Archive Logs
RECORD & AUDIT
Servers
Workstations
Devices
Applications
Databases
Social Media
Cloud

REDTEAMRD

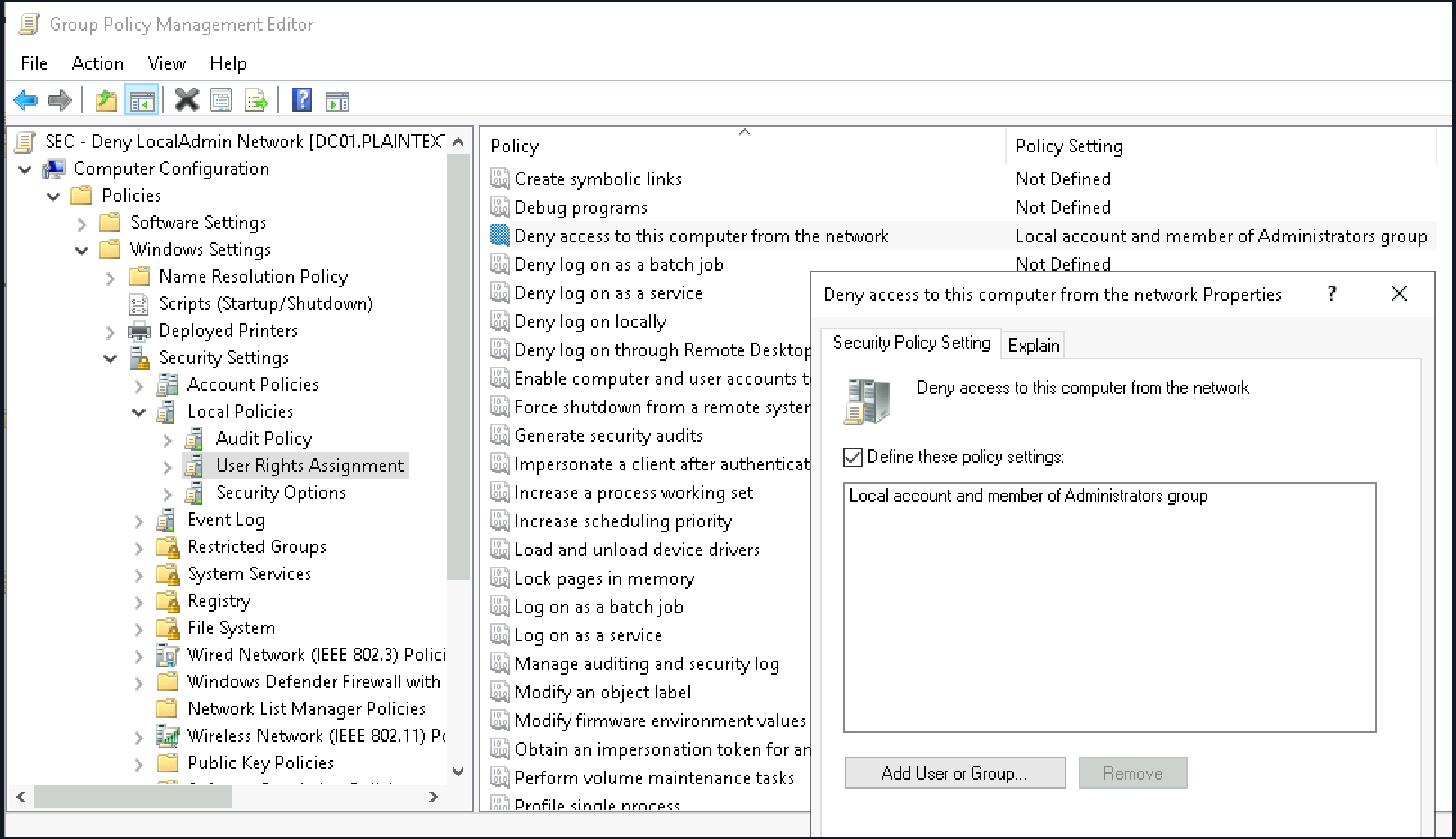

Mitigate human eRRoR
Diminish attack suRface
Why PAM?
Increase pRoductivity
DemonstRate compliance

¿ YA ESTAMOS SEGUROS?

Local Admin Protection

REDTEAMRD

Deny Local Administrator Network Logon



- SEC - Deny LocalAdmin Network [DC01.PLAINTEX
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Deployed Printers
        - Security Settings
          - Account Policies
          - Local Policies
            - Audit Policy
            - User Rights Assignment
            - Security Options
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Polici
          - Windows Defender Firewall with
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Pc
          - Public Key Policies

Policy	Policy Setting
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	Local account and member of Administrators group
Deny log on as a batch job	Not Defined
Deny log on as a service	
Deny log on locally	
Deny log on through Remote Desktop	
Enable computer and user accounts t	
Force shutdown from a remote syster	
Generate security audits	
Impersonate a client after authenticat	
Increase a process working set	
Increase scheduling priority	
Load and unload device drivers	
Lock pages in memory	
Log on as a batch job	
Log on as a service	
Manage auditing and security log	
Modify an object label	
Modify firmware environment values	
Obtain an impersonation token for an	
Perform volume maintenance tasks	
Profile single process	

Deny access to this computer from the network Properties

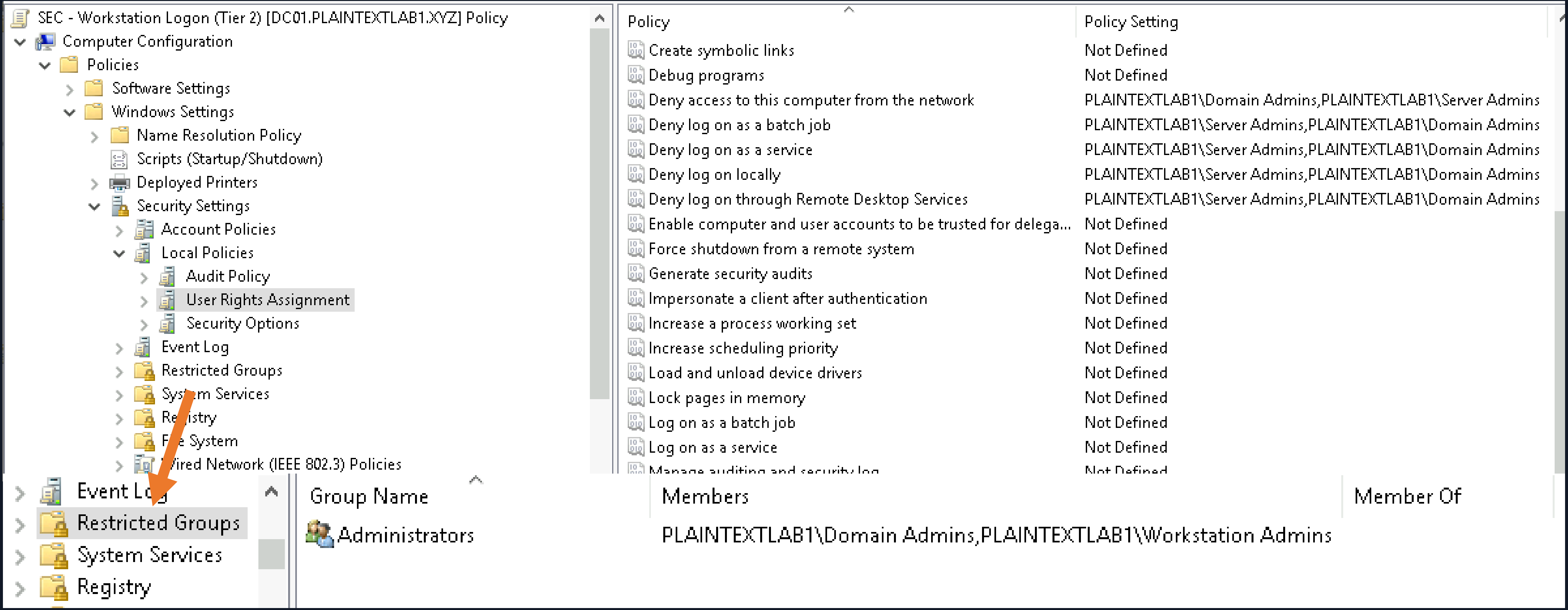
Deny access to this computer from the network

☑ Define these policy settings:

Local account and member of Administrators group

Tier Protection

Workstations (Tier 2) - Logon Policies



SEC - Workstation Logon (Tier 2) [DC01.PLAINTEXTLAB1.XYZ] Policy

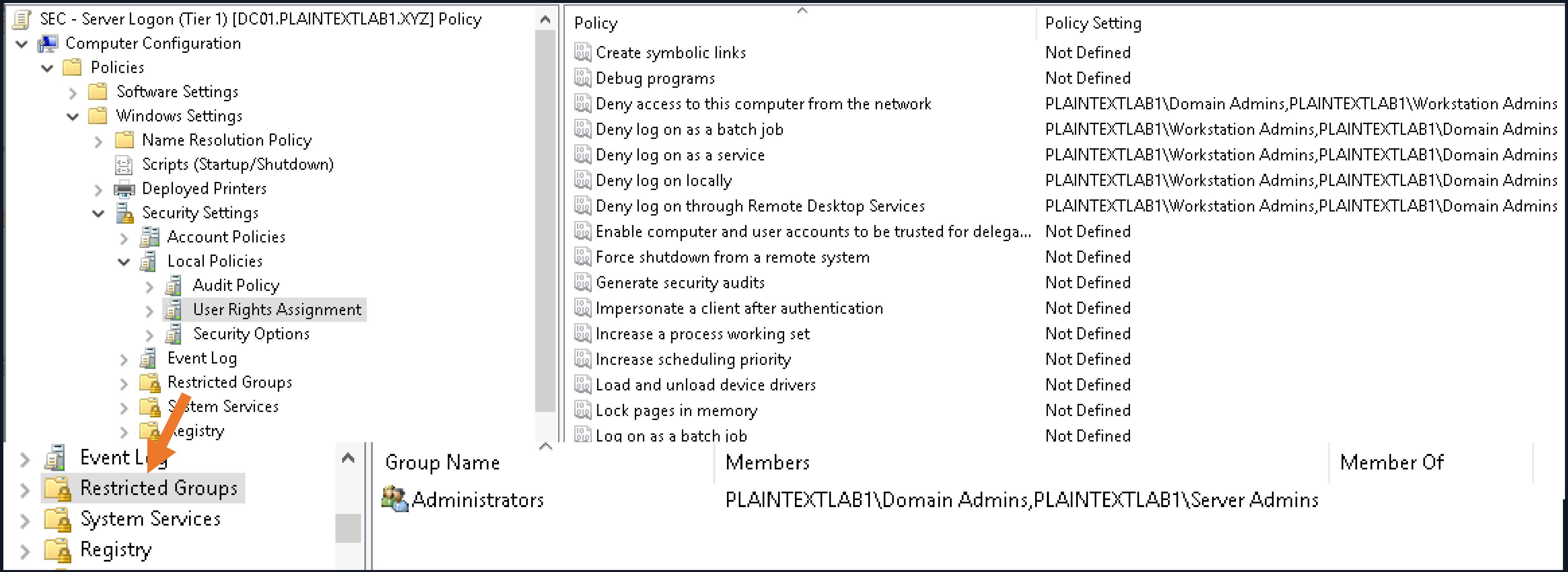
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policies

Policy	Policy Setting
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	PLAINTEXTLAB1\Domain Admins,PLAINTEXTLAB1\Server Admins
Deny log on as a batch job	PLAINTEXTLAB1\Server Admins,PLAINTEXTLAB1\Domain Admins
Deny log on as a service	PLAINTEXTLAB1\Server Admins,PLAINTEXTLAB1\Domain Admins
Deny log on locally	PLAINTEXTLAB1\Server Admins,PLAINTEXTLAB1\Domain Admins
Deny log on through Remote Desktop Services	PLAINTEXTLAB1\Server Admins,PLAINTEXTLAB1\Domain Admins
Enable computer and user accounts to be trusted for delega...	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Not Defined
Load and unload device drivers	Not Defined
Lock pages in memory	Not Defined
Log on as a batch job	Not Defined
Log on as a service	Not Defined
Manage auditing and security log	Not Defined

- Event Log
- Restricted Groups
- System Services
- Registry

Group Name	Members	Member Of
Administrators	PLAINTEXTLAB1\Domain Admins,PLAINTEXTLAB1\Workstation Admins	

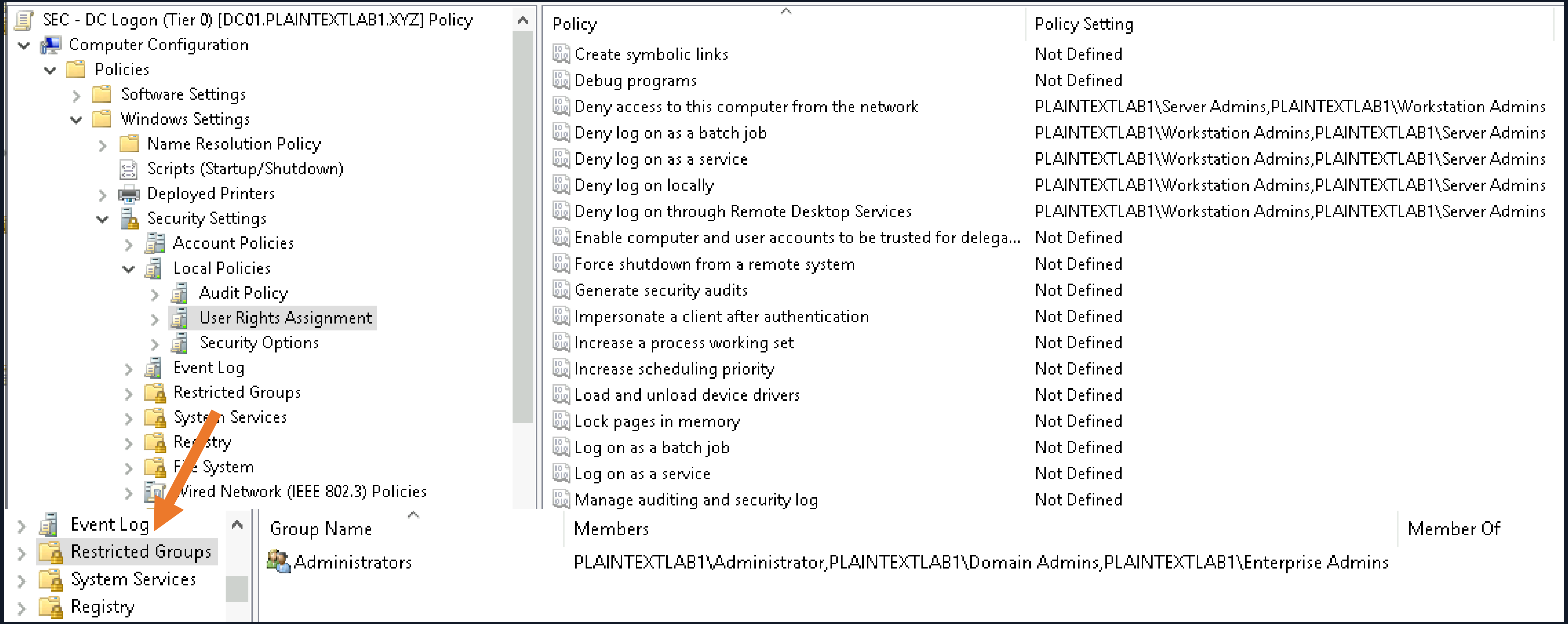
Servers (Tier 1) - Logon Policies



Policy	Policy Setting
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	PLAINTEXTLAB1\Domain Admins,PLAINTEXTLAB1\Workstation Admins
Deny log on as a batch job	PLAINTEXTLAB1\Workstation Admins,PLAINTEXTLAB1\Domain Admins
Deny log on as a service	PLAINTEXTLAB1\Workstation Admins,PLAINTEXTLAB1\Domain Admins
Deny log on locally	PLAINTEXTLAB1\Workstation Admins,PLAINTEXTLAB1\Domain Admins
Deny log on through Remote Desktop Services	PLAINTEXTLAB1\Workstation Admins,PLAINTEXTLAB1\Domain Admins
Enable computer and user accounts to be trusted for delega...	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Not Defined
Load and unload device drivers	Not Defined
Lock pages in memory	Not Defined
Log on as a batch job	Not Defined

Group Name	Members	Member Of
Administrators	PLAINTEXTLAB1\Domain Admins,PLAINTEXTLAB1\Server Admins	

DC (Tier 0) - Logon Policies

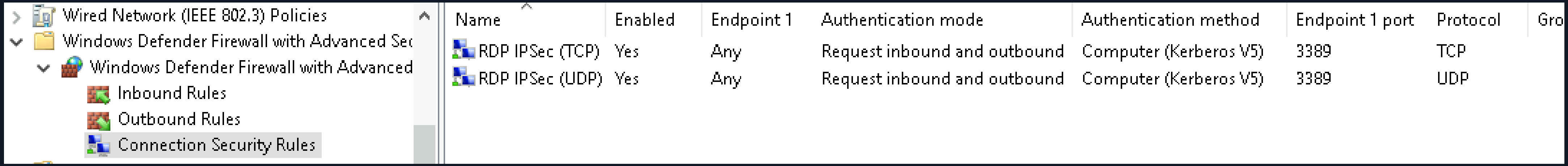


Policy	Policy Setting
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	PLAINTEXTLAB1\Server Admins,PLAINTEXTLAB1\Workstation Admins
Deny log on as a batch job	PLAINTEXTLAB1\Workstation Admins,PLAINTEXTLAB1\Server Admins
Deny log on as a service	PLAINTEXTLAB1\Workstation Admins,PLAINTEXTLAB1\Server Admins
Deny log on locally	PLAINTEXTLAB1\Workstation Admins,PLAINTEXTLAB1\Server Admins
Deny log on through Remote Desktop Services	PLAINTEXTLAB1\Workstation Admins,PLAINTEXTLAB1\Server Admins
Enable computer and user accounts to be trusted for delega...	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Not Defined
Load and unload device drivers	Not Defined
Lock pages in memory	Not Defined
Log on as a batch job	Not Defined
Log on as a service	Not Defined
Manage auditing and security log	Not Defined

Group Name	Members	Member Of
Administrators	PLAINTEXTLAB1\Administrator,PLAINTEXTLAB1\Domain Admins,PLAINTEXTLAB1\Enterprise Admins	

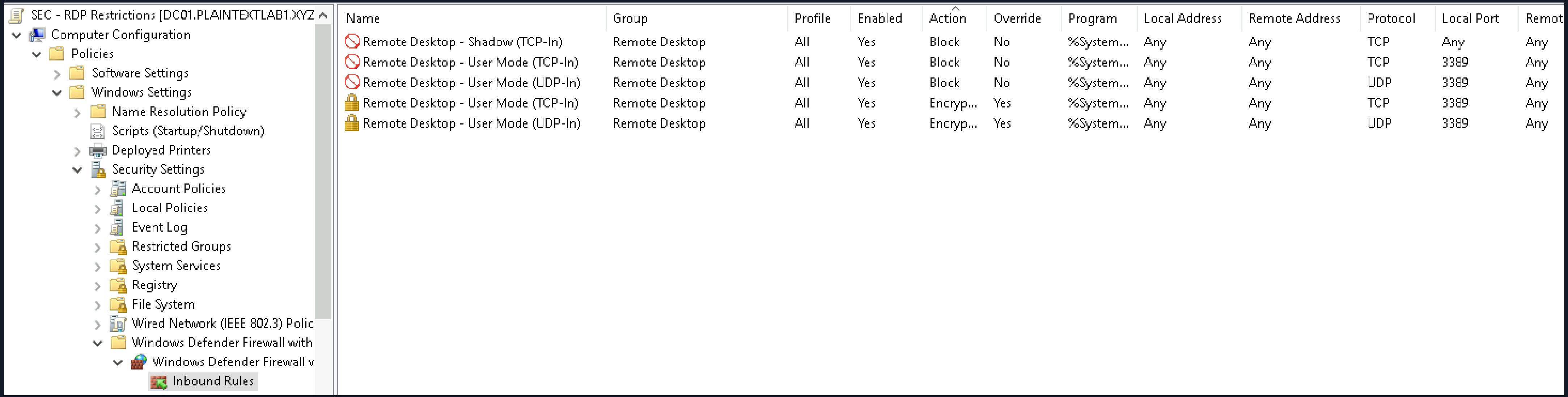
PAW Access

SEC – RDP IPSec (PAW & DC)


Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Sec
Windows Defender Firewall with Advanced
Inbound Rules
Outbound Rules
Connection Security Rules

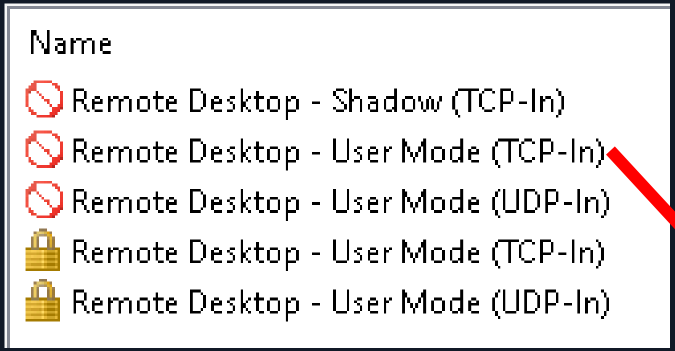
Name	Enabled	Endpoint 1	Authentication mode	Authentication method	Endpoint 1 port	Protocol	Gro
RDP IPSec (TCP)	Yes	Any	Request inbound and outbound	Computer (Kerberos V5)	3389	TCP	
RDP IPSec (UDP)	Yes	Any	Request inbound and outbound	Computer (Kerberos V5)	3389	UDP	

SEC – RDP Restrictions (DC Only)



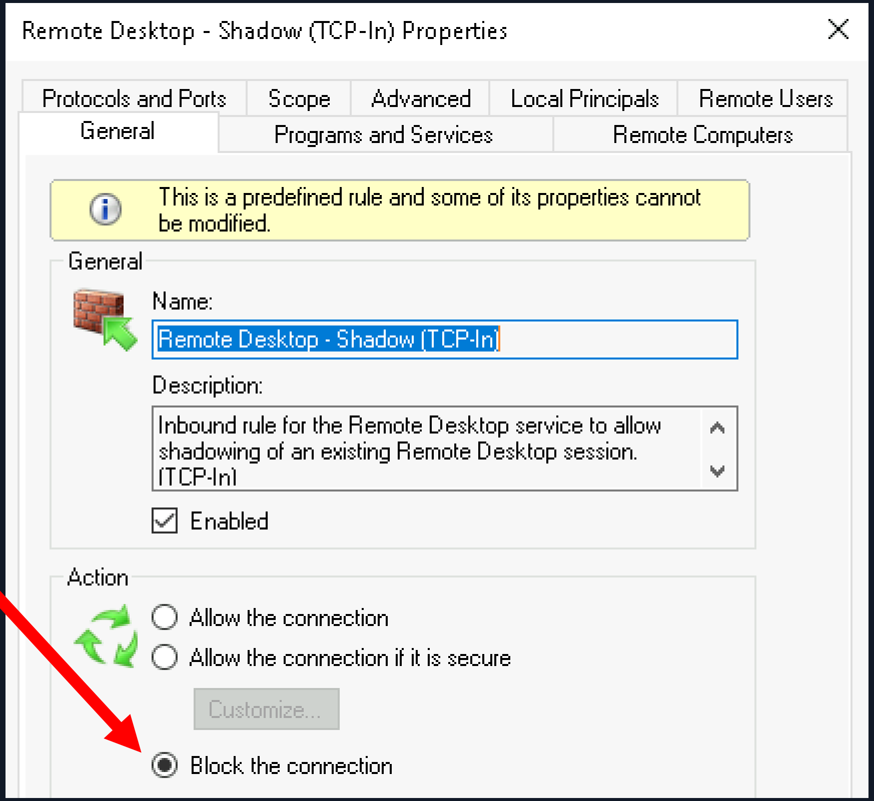
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remot
Remote Desktop - Shadow (TCP-In)	Remote Desktop	All	Yes	Block	No	%System...	Any	Any	TCP	Any	Any
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Block	No	%System...	Any	Any	TCP	3389	Any
Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	Yes	Block	No	%System...	Any	Any	UDP	3389	Any
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Encryp...	Yes	%System...	Any	Any	TCP	3389	Any
Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	Yes	Encryp...	Yes	%System...	Any	Any	UDP	3389	Any

SEC – RDP Restrictions (DC Only)



Name

- Remote Desktop - Shadow (TCP-In)
- Remote Desktop - User Mode (TCP-In)
- Remote Desktop - User Mode (UDP-In)
- Remote Desktop - User Mode (TCP-In)
- Remote Desktop - User Mode (UDP-In)



Remote Desktop - Shadow (TCP-In) Properties

This is a predefined rule and some of its properties cannot be modified.

General

Name: Remote Desktop - Shadow (TCP-In)

Description: Inbound rule for the Remote Desktop service to allow shadowing of an existing Remote Desktop session. (TCP-In)

☑ Enabled

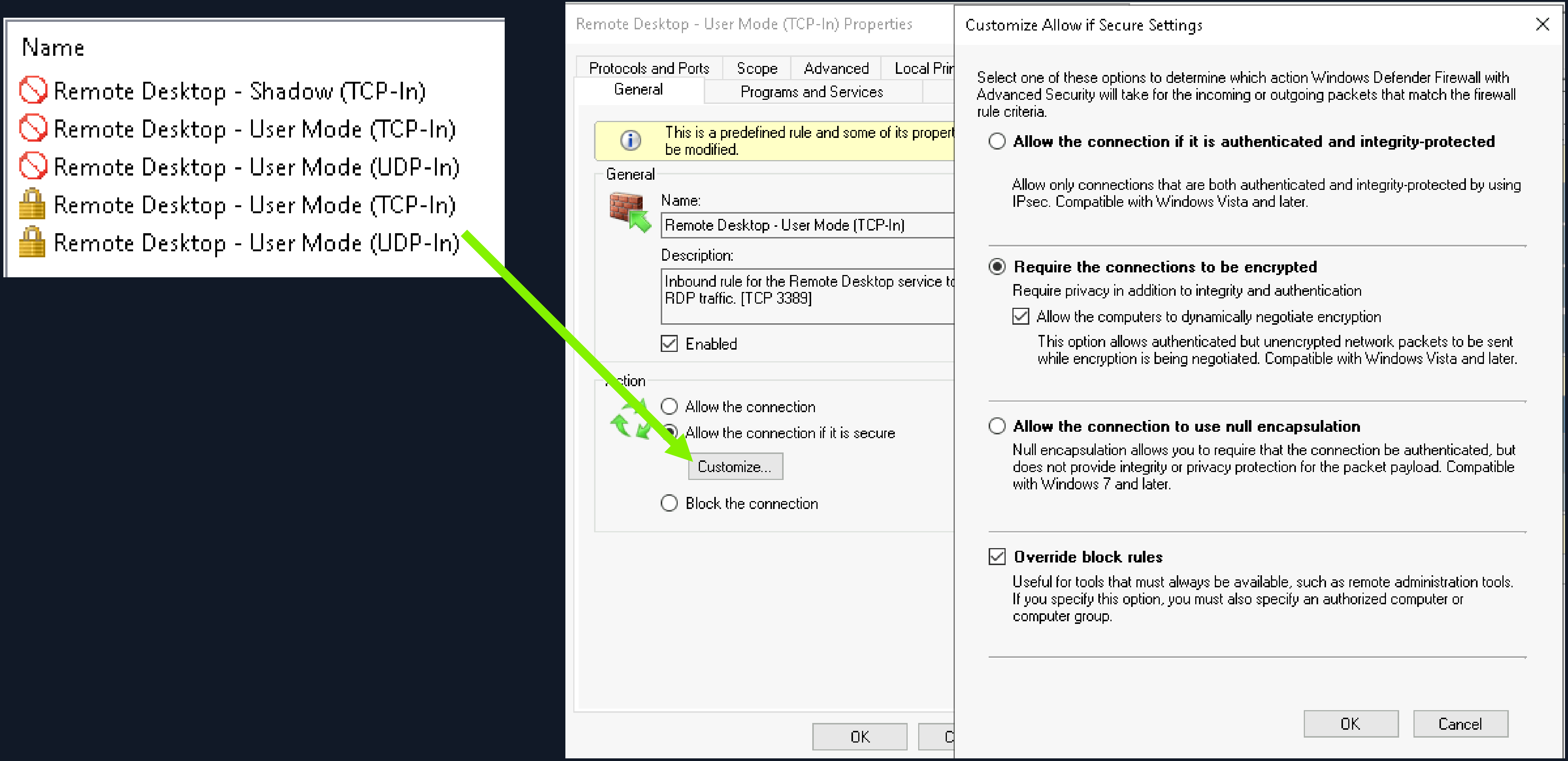
Action

○ Allow the connection

○ Allow the connection if it is secure

● Block the connection

SEC – RDP Restrictions (DC Only)



Name
- 🚫 Remote Desktop - Shadow (TCP-In)
- 🚫 Remote Desktop - User Mode (TCP-In)
- 🚫 Remote Desktop - User Mode (UDP-In)
- 🔒 Remote Desktop - User Mode (TCP-In)
- 🔒 Remote Desktop - User Mode (UDP-In)

Remote Desktop - User Mode (TCP-In) Properties

This is a predefined rule and some of its propert
be modified.

General

Name: Remote Desktop - User Mode (TCP-In)

Description: Inbound rule for the Remote Desktop service to
RDP traffic. [TCP 3389]

☑ Enabled

Action

○ Allow the connection

● Allow the connection if it is secure

○ Block the connection

Customize Allow if Secure Settings

Select one of these options to determine which action Windows Defender Firewall with Advanced Security will take for the incoming or outgoing packets that match the firewall rule criteria.

○ **Allow the connection if it is authenticated and integrity-protected**

Allow only connections that are both authenticated and integrity-protected by using IPsec. Compatible with Windows Vista and later.

● **Require the connections to be encrypted**

Require privacy in addition to integrity and authentication

☑ Allow the computers to dynamically negotiate encryption

This option allows authenticated but unencrypted network packets to be sent while encryption is being negotiated. Compatible with Windows Vista and later.

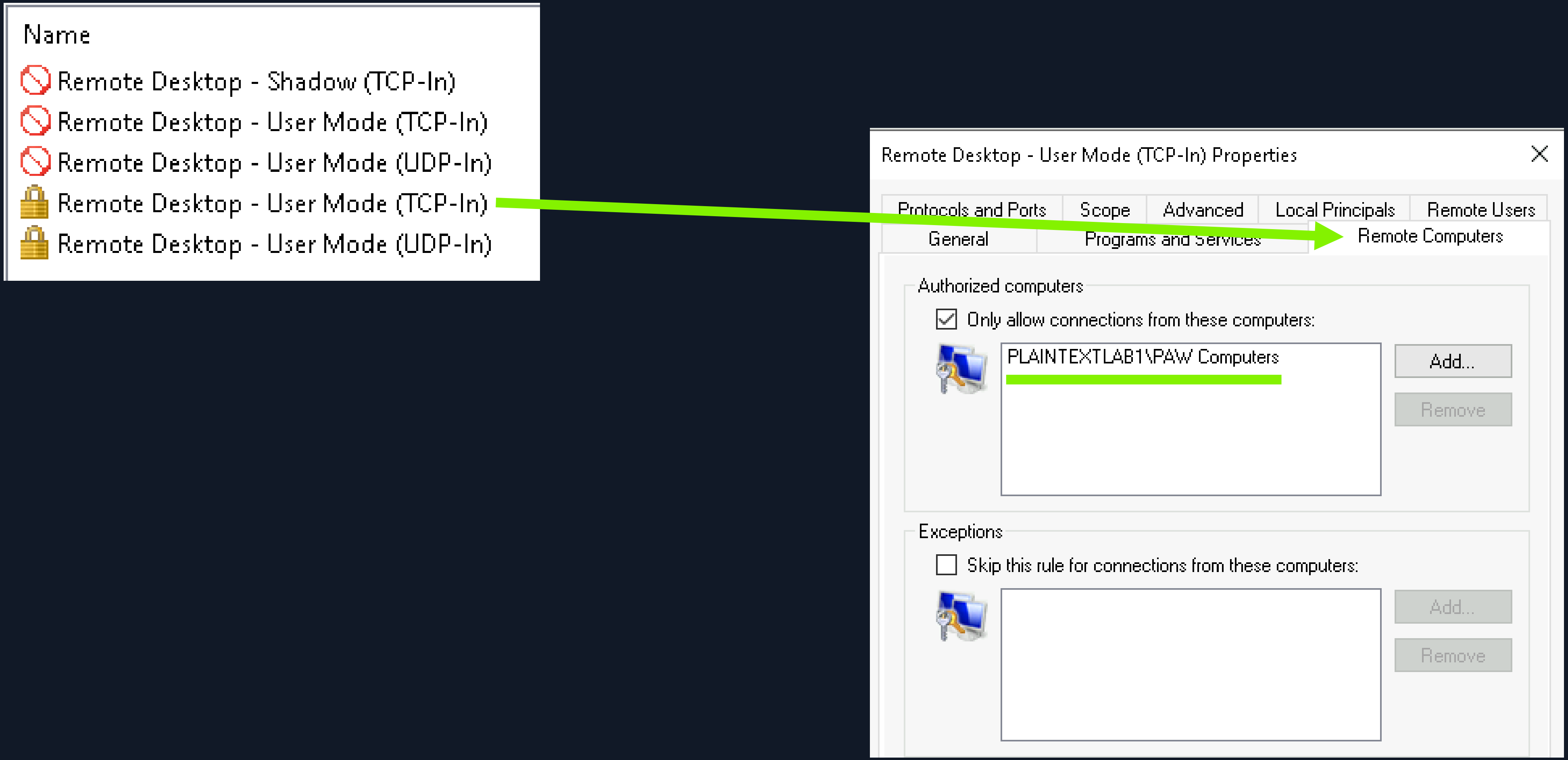
○ **Allow the connection to use null encapsulation**

Null encapsulation allows you to require that the connection be authenticated, but does not provide integrity or privacy protection for the packet payload. Compatible with Windows 7 and later.

☑ **Override block rules**

Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.

SEC – RDP Restrictions (DC Only)



Name

- 🚫 Remote Desktop - Shadow (TCP-In)
- 🚫 Remote Desktop - User Mode (TCP-In)
- 🚫 Remote Desktop - User Mode (UDP-In)
- 🔒 Remote Desktop - User Mode (TCP-In)
- 🔒 Remote Desktop - User Mode (UDP-In)

Remote Desktop - User Mode (TCP-In) Properties

Authorized computers

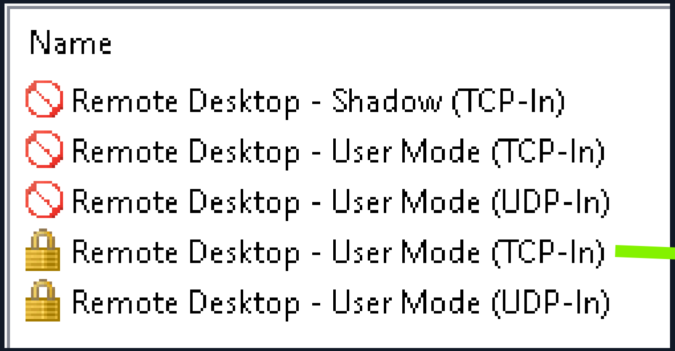
☑ Only allow connections from these computers:

PLAINTEXTLAB1\PAW Computers

Exceptions

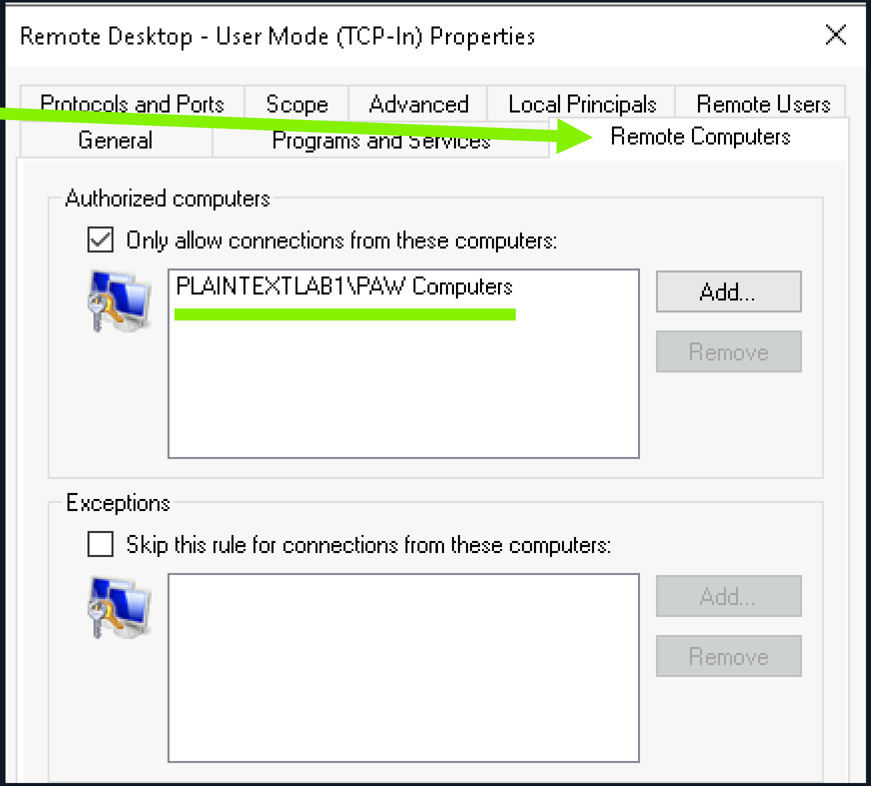
☐ Skip this rule for connections from these computers:

SEC – RDP Restrictions (DC Only)



Name

- 🚫 Remote Desktop - Shadow (TCP-In)
- 🚫 Remote Desktop - User Mode (TCP-In)
- 🚫 Remote Desktop - User Mode (UDP-In)
- 🔒 Remote Desktop - User Mode (TCP-In)
- 🔒 Remote Desktop - User Mode (UDP-In)



Remote Desktop - User Mode (TCP-In) Properties

Authorized computers

☑ Only allow connections from these computers:

PLAINTEXTLAB1\PAW Computers

Exceptions

☐ Skip this rule for connections from these computers:

¿Preguntas?

REDTEAMRD

Gracias!

REDTEAMRD