PAW

Sami Laiho

Chief Research Officer, Senior Technical Fellow, MVP

Adminize.com / Win-fu.com / samilaiho.com

Sami Laiho

Chief Research Officer / MVP

- IT Admin since 1995 / MCT since 2001
- MVP in Windows OS since 2011
- ”100 Most Influencial people in IT in Finland” – TiVi’2019→
- Specializes in and trains:
  - Troubleshooting
  - Windows Internals
  - Security, Social Engineering, Auditing
- Trophies:
  - Best Session at Advanced Threat Summit 2020
  - Best Speaker at NIC, Oslo 2016, 2017, 2019, 2020, 2022 and 2023
  - Ignite 2018 – Session #1 and #2 (out of 1708) !
  - TechEd Europe and North America 2014 - Best session, Best speaker
  - TechEd Australia 2013 - Best session, Best speaker


X (ex-Twitter): @samilaiho
Bluesky: @samilaiho.com
LinkedIn

Ransomware is still a 'when' more than an 'if'

For the third year in a row, at least three out of four organizations suffered one or more ransomware attacks in the preceding twelve months:

- 25% stated that they were not attacked, which should be noted with caution since many security firms warn that the attacker can be lurking in your environment for 60 to 200 days prior to incurring damage or asking for the ransom. If true, then a high percentage of those respondents may simply have not discovered the breach yet
- 26% stated that they were attacked four or more times in the past year.

66%

of organizations in EMEA suffered at least one attack in the previous year

* Veeam EMEA

USA – Ransomware Cases

	2021	2022	2023
Hospital systems*	27	25	46
K-12 school districts*	62	45	108
Post-secondary schools	26	44	72
Governments	77	106	95
Totals	**192**	**220**	**321**

**Hospital systems are compromised of multiple hospitals and school districts of multiple schools. The total number of hospitals and schools impacted is explained in the sector-specific sections below.*

Average Ransoms Paid in US

- 2018 = 5000$
- 2023 = 1.500.000$

Last week VmWare 0-day vulnerability

- Price: 1,7M$
- When Criminals get more money their budget for the next attacks increase → 0-Day attacks become more common
- Sadly, the enemy is also becoming more bold and cruel…

Immutable Laws of Security (v2)

- **Law #1:** If a bad actor can persuade you to run their program on your computer, it's not solely your computer anymore.
- **Law #2:** If a bad actor can alter the operating system on your computer, it's not your computer anymore.
- **Law #3:** If a bad actor has unrestricted physical access to your computer, it's not your computer anymore.
- **Law #4:** If you allow a bad actor to run active content in your website, it's not your website anymore.
- **Law #5:** Weak passwords trump strong security.
- **Law #6:** A computer is only as secure as the administrator is trustworthy.
- **Law #7:** Encrypted data is only as secure as its decryption key.
- **Law #8:** An out-of-date antimalware scanner is only marginally better than no scanner at all.
- **Law #9:** Absolute anonymity isn't practically achievable, either online or offline.
- **Law #10:** Technology isn't a panacea.

My Take

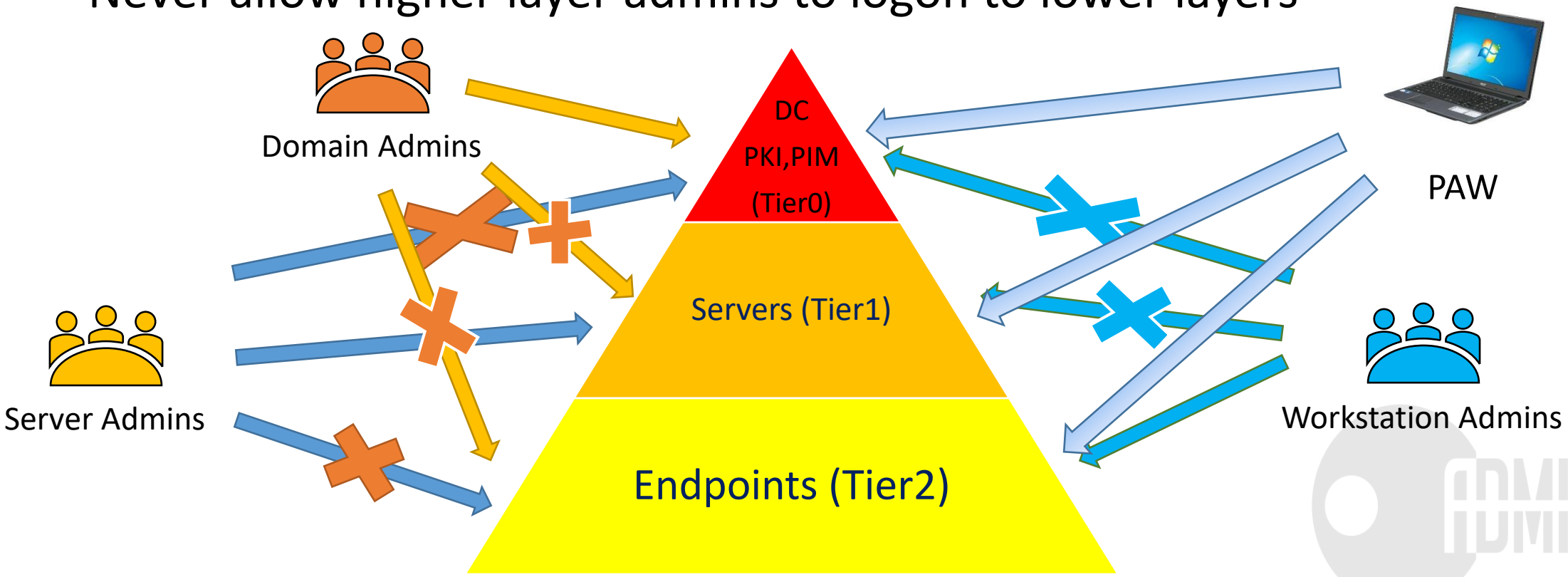
- Up to date hardware and software inventory
- BitLocker
- Principle of Least Privilege
- Tier Model for AD
- **Using PAW-model**
- Introduction of IPsec
- Allow-listing to some extent
- MFA, strong authentication
- USB-control?

Tier Model AD/AAD

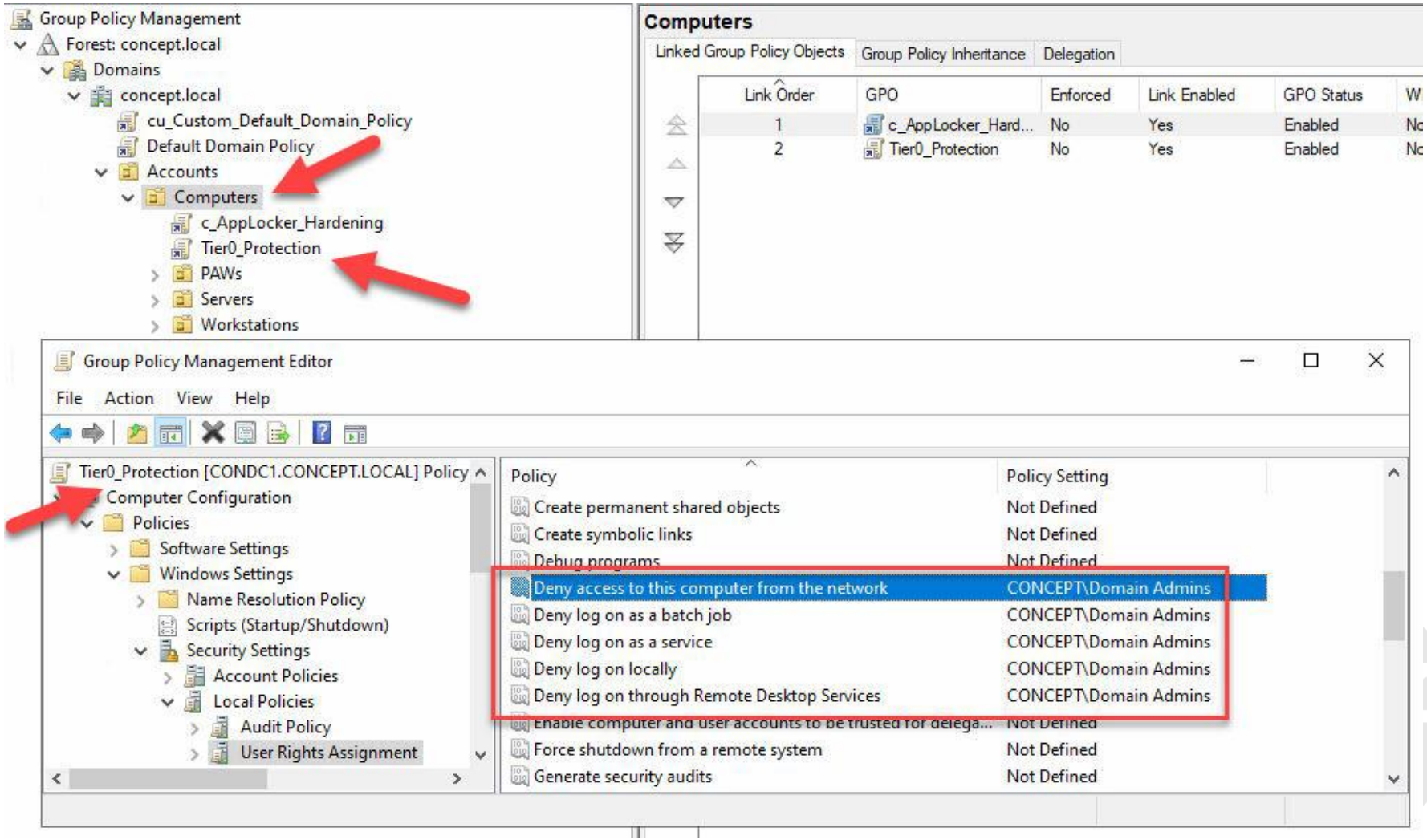
I know… – Entra ID (ME-ID)

Tier your Directories on-prem…

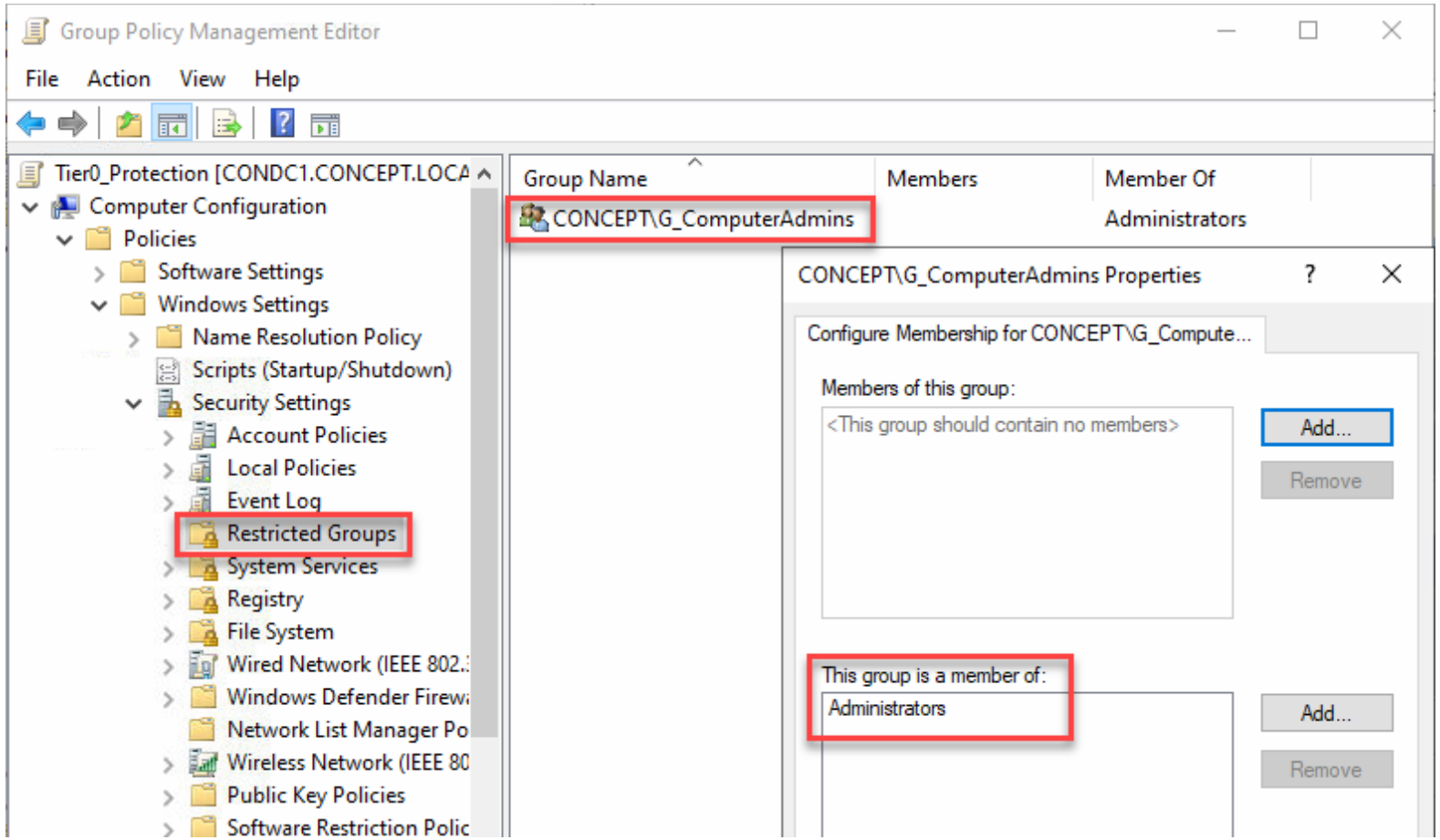
- Split your environment into three tiers
- Never allow higher layer admins to logon to lower layers



If Nothing Else, do This!

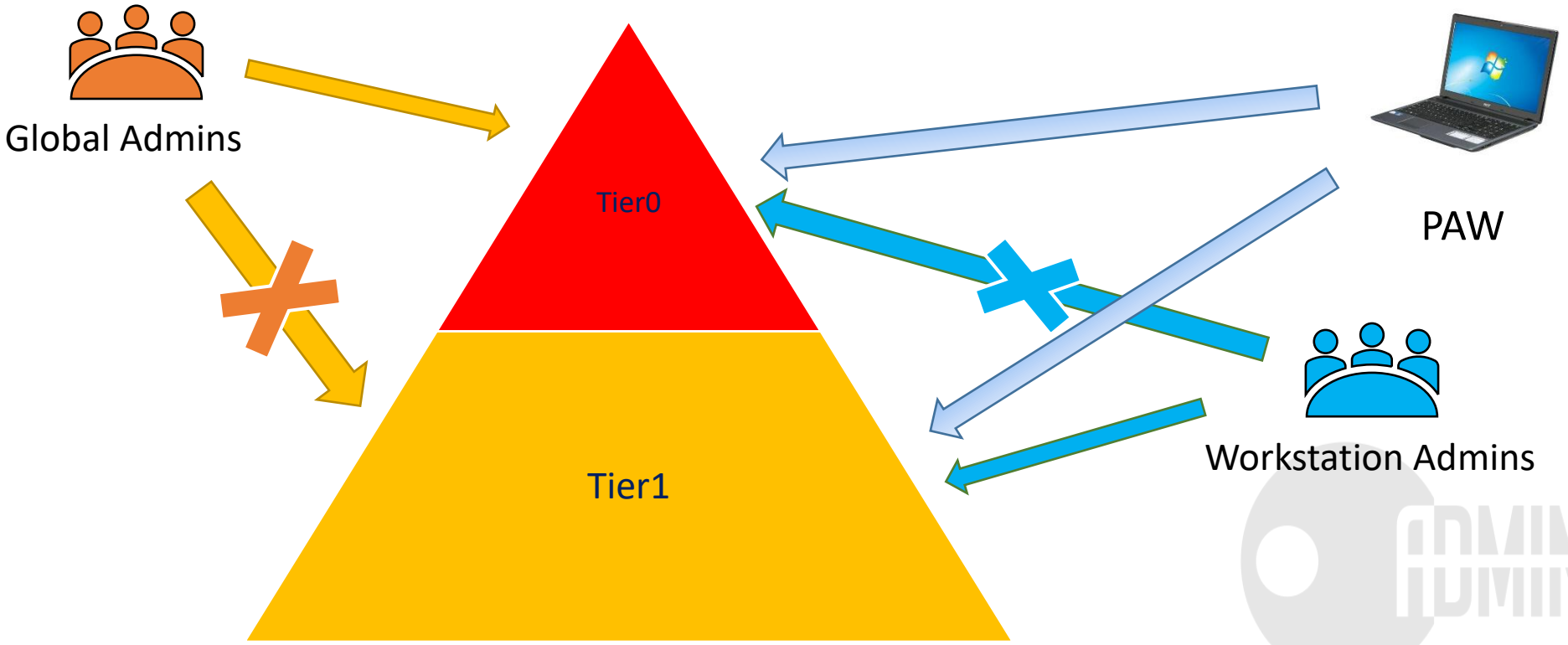


Adding Groups



… or in the Cloud

- Split your environment into two layers
- Never allow higher layer admins to logon to lower layers



Even More Important than AD-tiering!

PAW

(V)LAN1

Domain Admins

Domain

PAW

(V)LAN2

Fabric Admins

Fabric

PAW

(V)LAN3

Backup Admins

Backup

Privileged Access Workstation (PAW)

Limit the Attack Surface

If you can use a device to take down the company, you should not be able to Facebook on it…

Privileged Access Workstation (PAW)

Security is simple at the end…

Don’t let accounts that can take down your environment logon to devices with access to malware…

Don’t let computers that can take down your environment talk to Facebook…

Why?

Why?

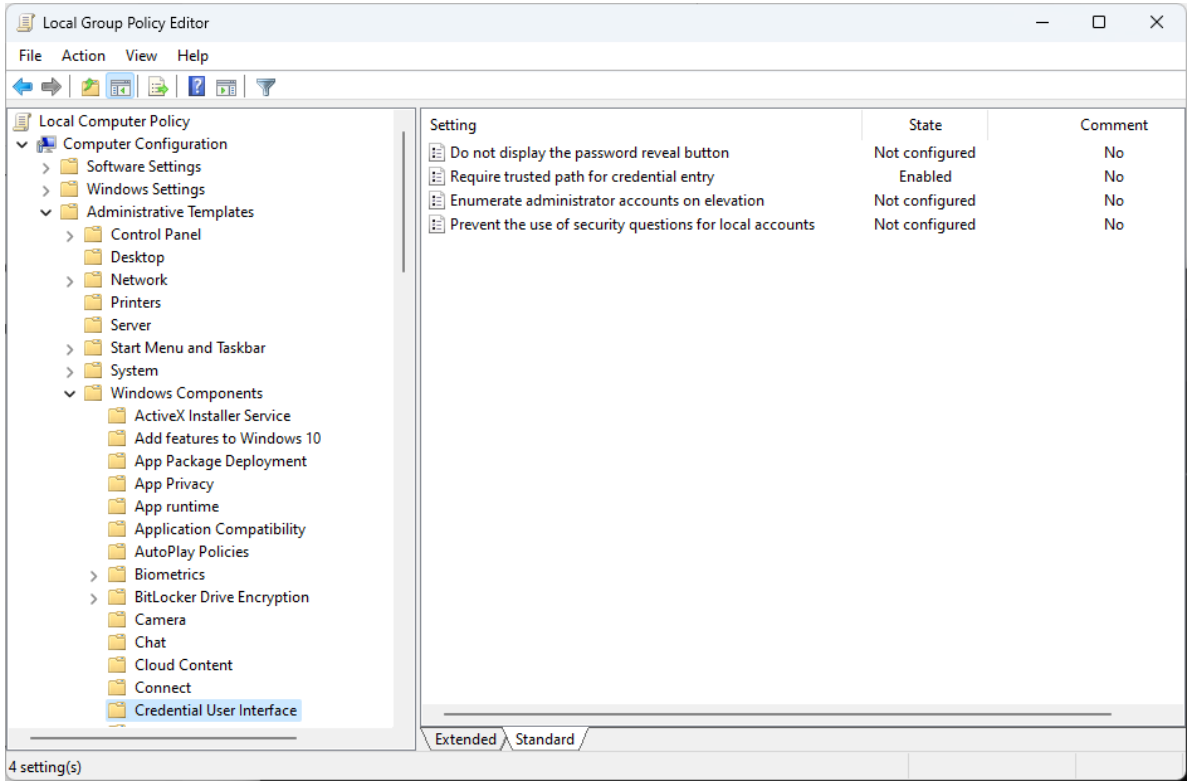
- Management tools just were not meant to work on servers
- RDP is an emergency console with two licenses
- No GUI
- High privileged user accounts can’t be used “where ever”

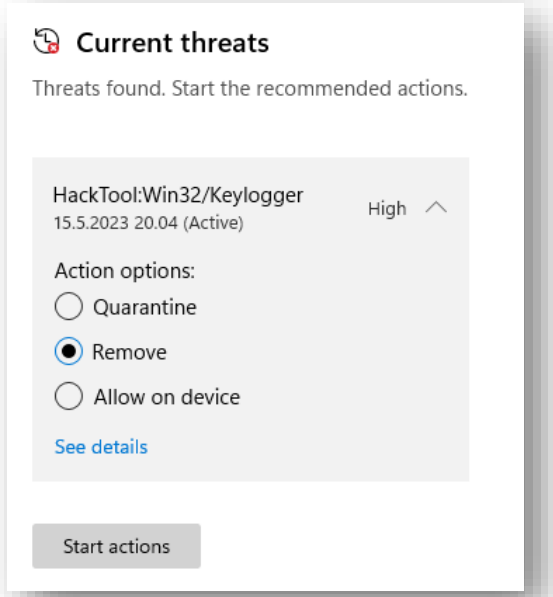
How?

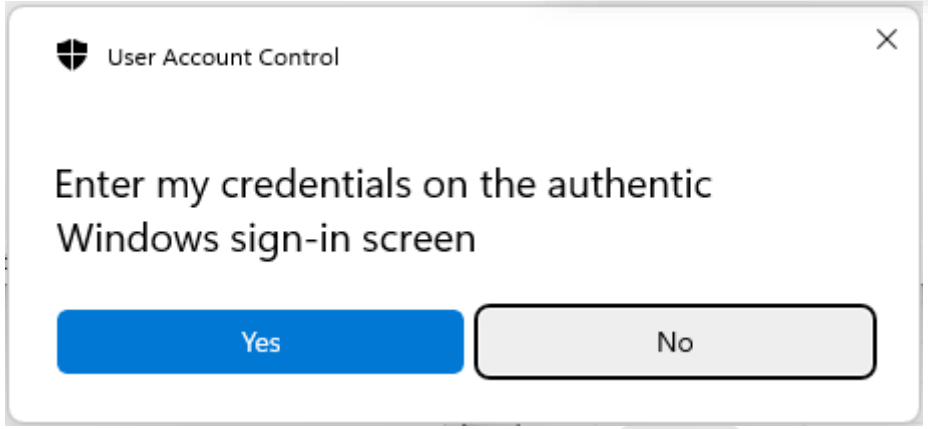
Platforms?

- Platform Level 1
  - A workstation is either a normal or a privileged one
- Platform Level 2
  - Admins have a VM
    - Running the admin stuff on the VM
    - Running the admin stuff on the Host
- Platform Level 3
  - Admins have separate computers for normal and privileged use

Credentials Protection







- And no Admin rights so you can’t install a Key Logger

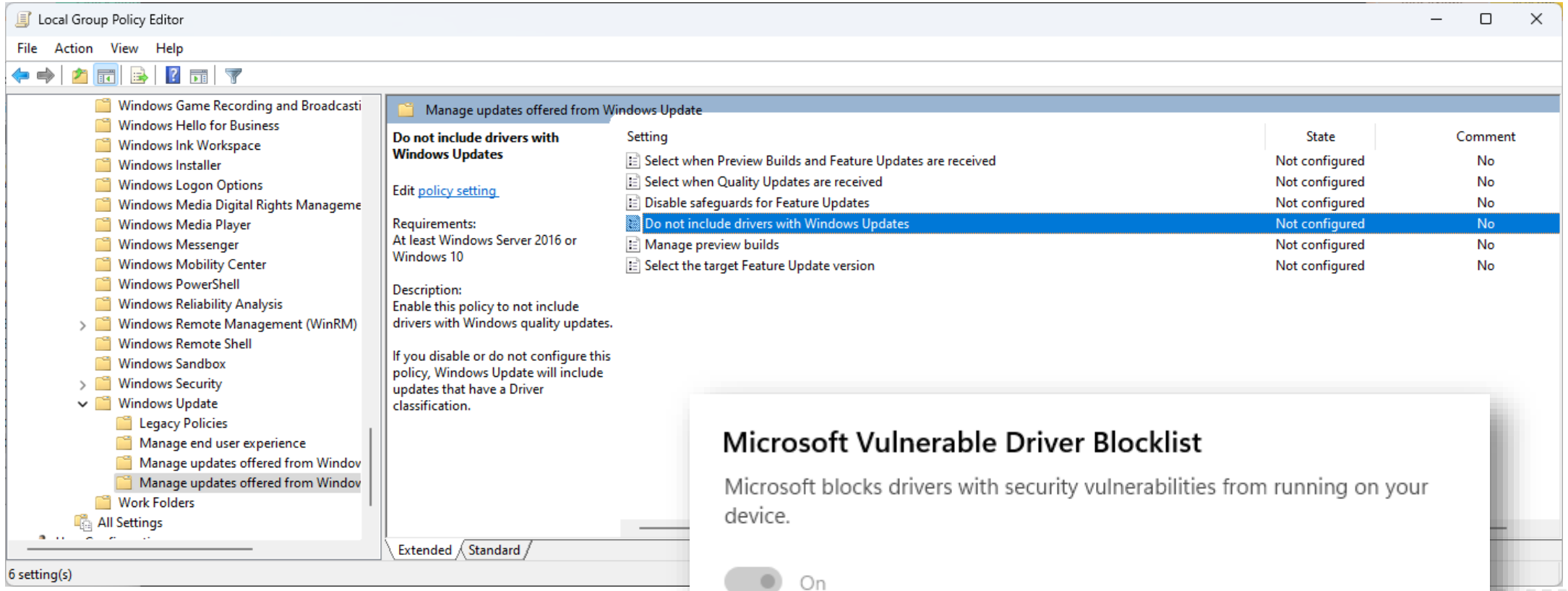
KeyLogger with PowerShell etc?

```
    # open logger file in Notepad
    notepad $Path
  }
}

# records all key presses until script is aborted by pressing CTRL+C
# will then open the file with collected key codes
Start-KeyLogger
At line:1 char:1
+ #requires -Version 2
+ ~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent


PS C:\Users\homer> |
```

Drivers


Local Group Policy Editor
File Action View Help
Windows Game Recording and Broadcasti
Windows Hello for Business
Windows Ink Workspace
Windows Installer
Windows Logon Options
Windows Media Digital Rights Manageme
Windows Media Player
Windows Messenger
Windows Mobility Center
Windows PowerShell
Windows Reliability Analysis
Windows Remote Management (WinRM)
Windows Remote Shell
Windows Sandbox
Windows Security
Windows Update
Legacy Policies
Manage end user experience
Manage updates offered from Windov
Manage updates offered from Windov
Work Folders
All Settings
Manage updates offered from Windows Update
Do not include drivers with Windows Updates
Edit policy setting
Requirements:
At least Windows Server 2016 or Windows 10
Description:
Enable this policy to not include drivers with Windows quality updates.
If you disable or do not configure this policy, Windows Update will include updates that have a Driver classification.
Setting
State
Comment
Select when Preview Builds and Feature Updates are received
Not configured
No
Select when Quality Updates are received
Not configured
No
Disable safeguards for Feature Updates
Not configured
No
Do not include drivers with Windows Updates
Not configured
No
Manage preview builds
Not configured
No
Select the target Feature Update version
Not configured
No
Extended
Standard
6 setting(s)
Microsoft Vulnerable Driver Blocklist
Microsoft blocks drivers with security vulnerabilities from running on your device.
On
Learn more

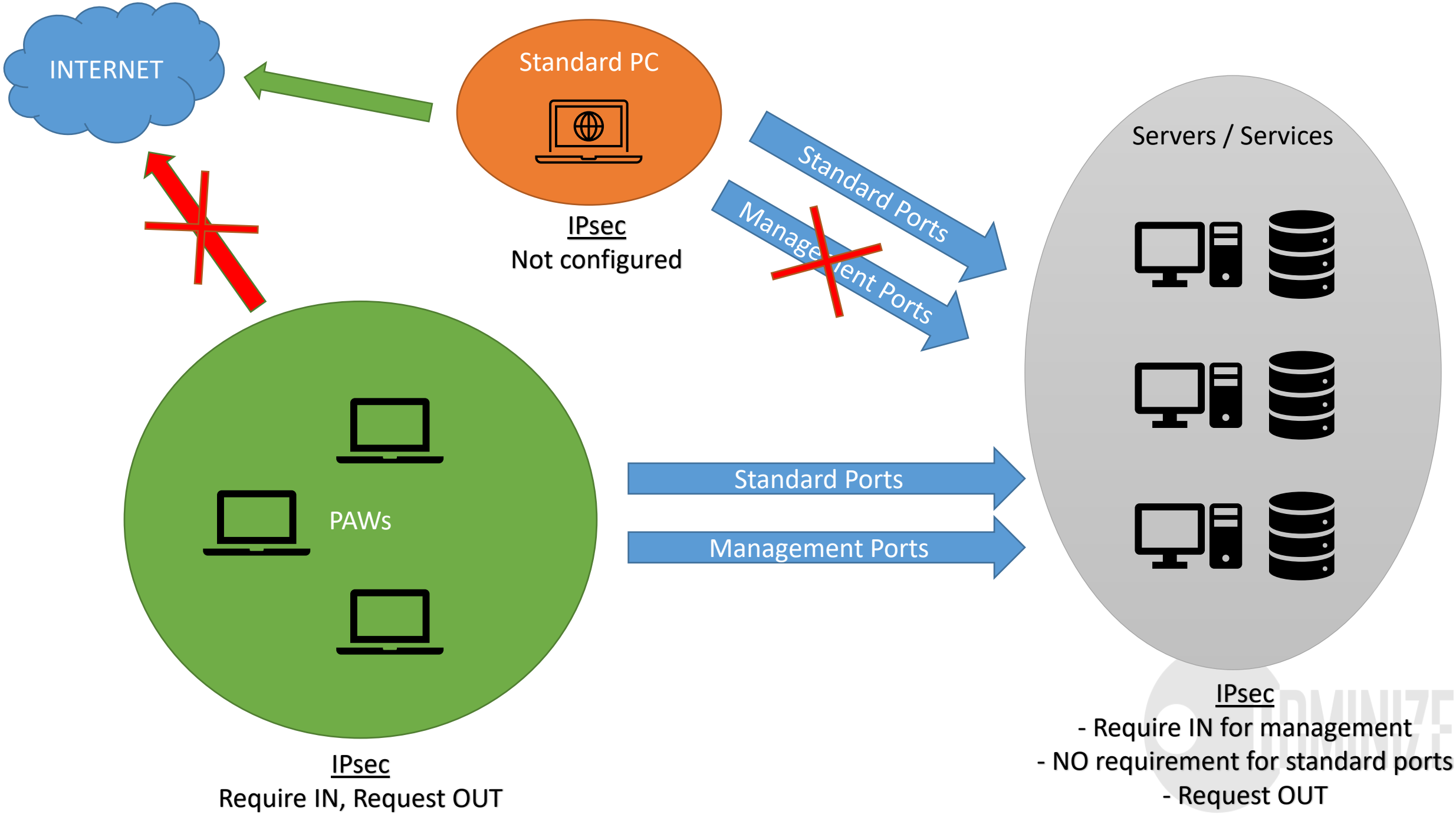
Owning a nested VM

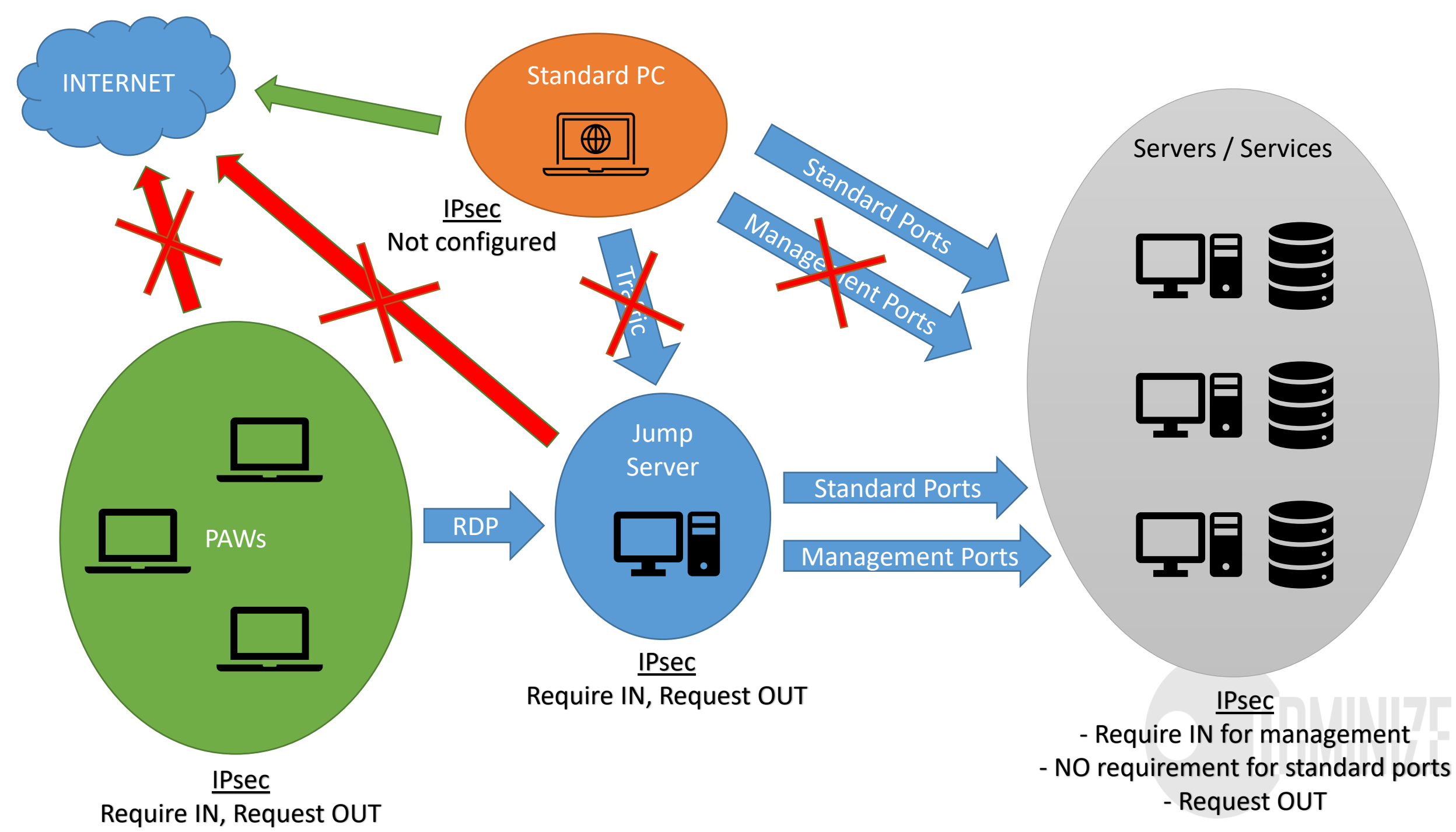
Why not on a shared Hypervisor?

What about Jump Servers?

Jump Servers

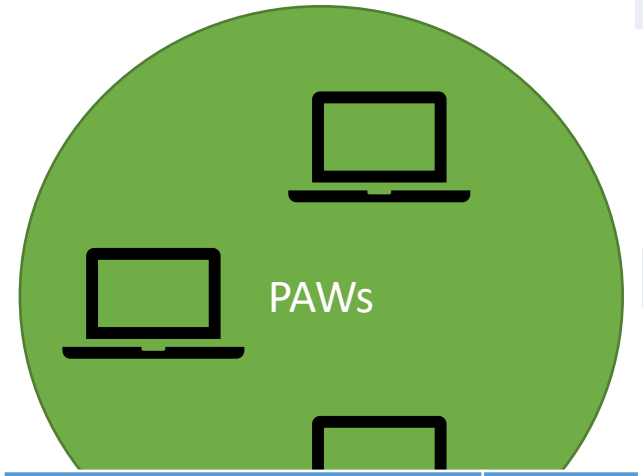
- This approach is frequently proposed to mitigate risk to administration and does provide some security assurances, but the jump server approach by itself is vulnerable to certain attacks because it violates the "clean source" principle. The clean source principle requires all security dependencies to be as trustworthy as the object being secured.


INTERNET
Standard PC
IPsec
Not configured
Standard Ports
Management Ports
Servers / Services
PAWs
Standard Ports
Management Ports
IPsec
Require IN, Request OUT
IPsec
- Require IN for management
- NO requirement for standard ports
- Request OUT


INTERNET
Standard PC
IPsec
Not configured
Traffic
Standard Ports
Management Ports
Servers / Services
PAWs
RDP
Jump
Server
Standard Ports
Management Ports
IPsec
Require IN, Request OUT
IPsec
Require IN, Request OUT
IPsec
- Require IN for management
- NO requirement for standard ports
- Request OUT

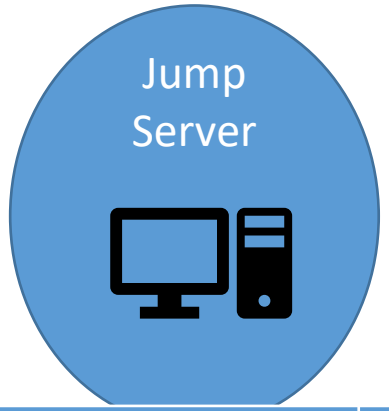
Administrators-group members

Administrators	
Domain Admins	YES
Workstations Admins	YES
Server Admins	NO
Builtin Administrator (used via LAPS)	YES

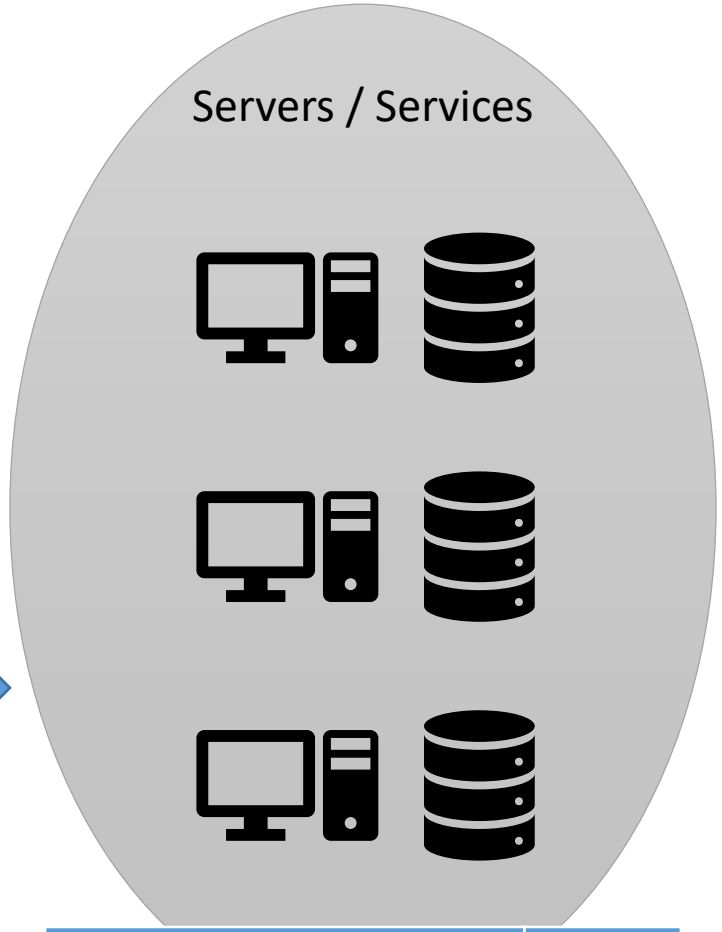


Administrators	
Domain Admins	NO
Workstations Admins	NO
Server Admins	NO
Builtin Administrator (used via LAPS)	YES

RDP



Administrators	
Domain Admins	NO
Workstations Admins	NO
Server Admins	NO
Builtin Administrator (used via LAPS)	YES



Administrators	
Domain Admins	YES
Workstations Admins	NO
Server Admins	YES
Builtin Administrator (used via LAPS)	YES

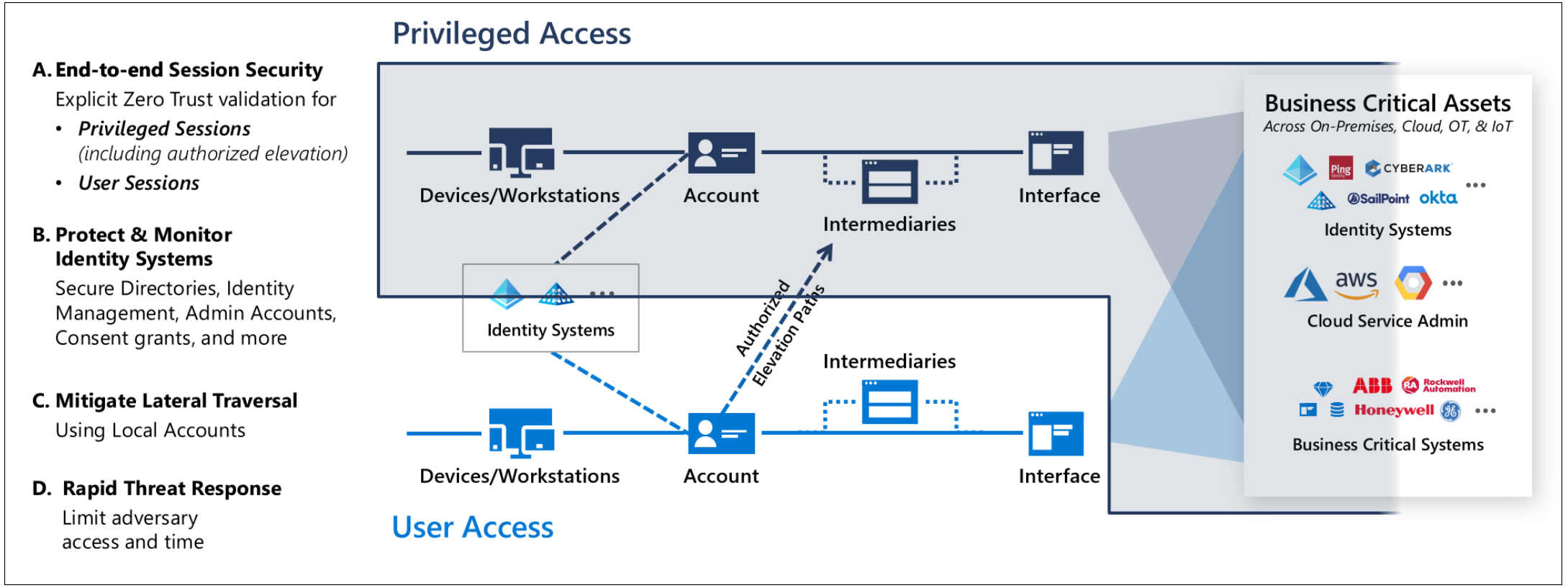
Good Run-through on IPsec for PAWs

- https://improsec.com/tech-blog/setup-rdp-dc-jumphost-paw-ipsec

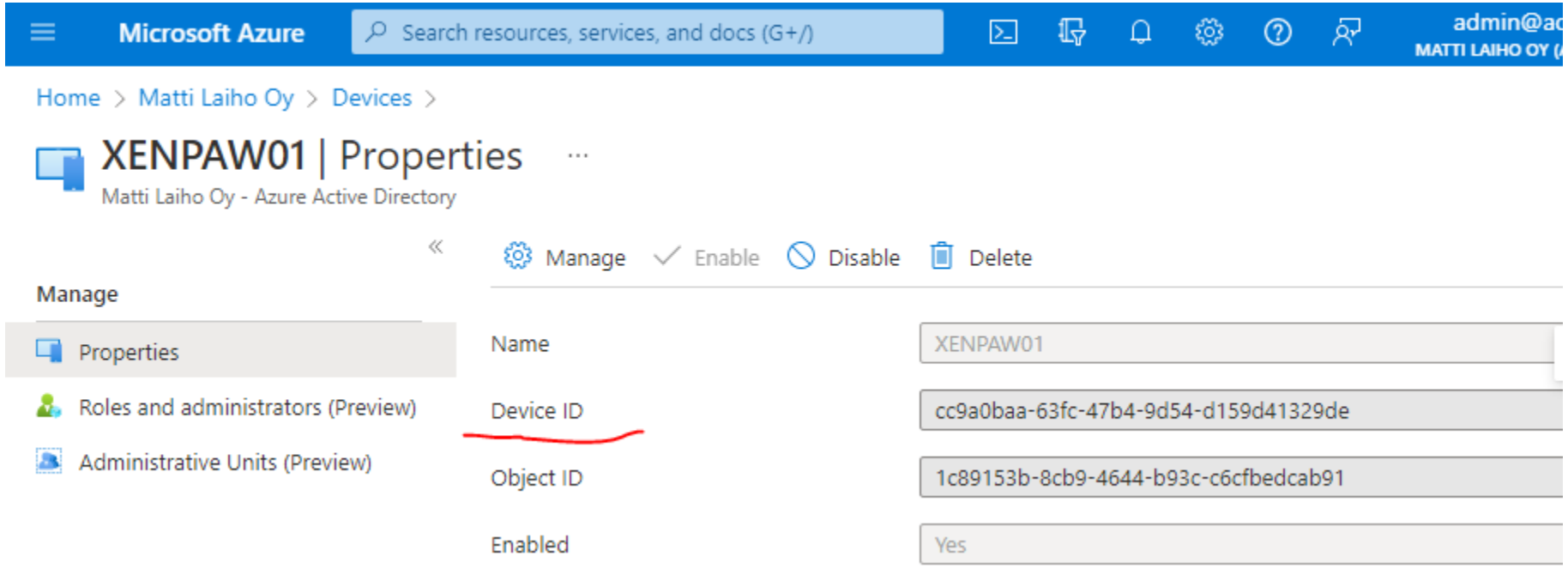
Azure PAW

Microsoft RAMP

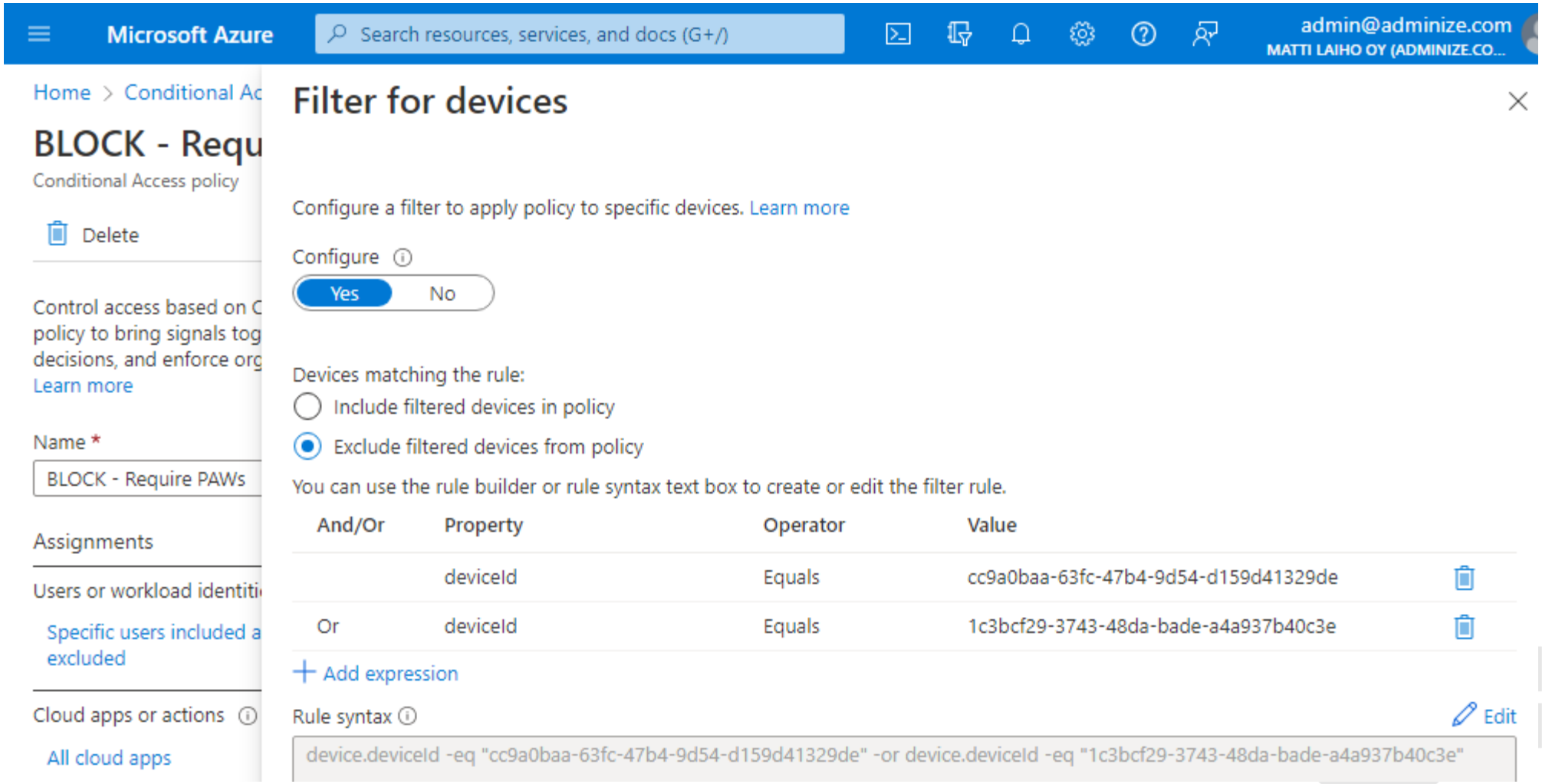
- https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan



DeviceID to identify PAWs



Conditional Access to filter out PAWs

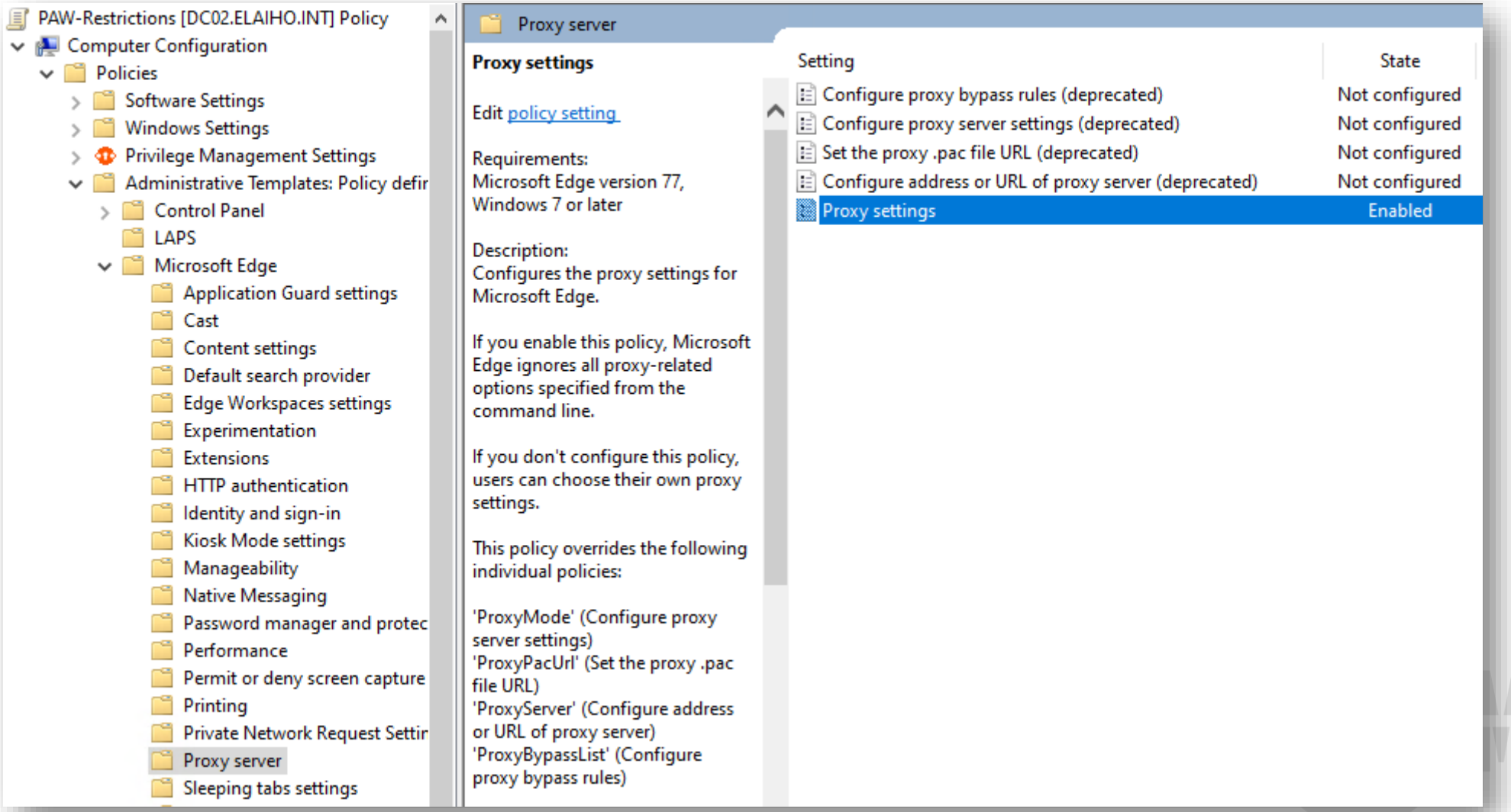


Recommended Reading

- Good run-through for AAD-environments
  - https://call4cloud.nl/2021/11/paw-love-and-thunder/

- Conditional Access for Devices (more options)
  - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-condition-filters-for-devices

Restricting Internet Access



Restricting Internet Access

- {"ProxyMode": "fixed_servers","ProxyServer": "127.0.0.1:8080","ProxyBypassList": "*.azure.com;*.duosecurity.com;*.azure.net;*.microsoft.com;*.windowsupdate.com;*.microsoftonline.com;*.microsoftonline.cn;*.windows.net;*.windowsazure.com;*.windowsazure.cn;*.azure.cn;*.loganalytics.io;*.applicationinsights.io;*.vsassets.io;*.azure-automation.net;*.visualstudio.com;portal.office.com;*.aspnetcdn.com;*.sharepointonline.com;*.msecnd.net;*.msocdn.com;*.webtrends.com;*.msidentity.com;*.auth.microsoft.com;*.msftidentity.com;account.activedirectory.windowsazure.com;accounts.accesscontrol.windows.net;adminwebservice.microsoftonline.com;api.passwordreset.microsoftonline.com;autologon.microsoftazuread-sso.com;becws.microsoftonline.com;ccs.login.microsoftonline.com;clientconfig.microsoftonline-p.net;companymanager.microsoftonline.com;device.login.microsoftonline.com;graph.microsoft.com;graph.windows.net;login.microsoft.com;login.microsoftonline.com;login.microsoftonline-p.com;login.windows.net;logincert.microsoftonline.com;loginex.microsoftonline.com;login-us.microsoftonline.com;nexus.microsoftonline-p.com;passwordreset.microsoftonline.com;provisioningapi.microsoftonline.com;*.msftauth.net;*.live.com;*.msauth.net;*.cdn.office.net;*.akamaihd.net;*.office.com;*.res.office365.com;*.azureedge.net;arc.msn.com;outlook.office365.com;*.atmrum.net;*.azr.footprintdns.com;*.exchange.microsoft.com;shellprod.msocdn.com;*.akamaiedge.net;wildcard.msocdn.com.edgekey.net;*admin.sharepoint.com;*.msedge.net;*.asm.skype.com;*.config.office.net;cdn.botframework.com;*.omnichannelengagementhub.com;*.powerapps.com;*.dynamics.com;*.powerbi.com;*.microsoftstream.com;*.onestore.ms;*.assets-yammer.com;*.yammer.com;*.microsoft365.com;live.sysinternals.com;https://go.microsoft.com/;http://go.microsoft.com/;https://login.live.com;https://activation.sls.microsoft.com/;http://crl.microsoft.com/pki/crl/products/MicProSecSerCA_2007-12-04.crl;https://validation.sls.microsoft.com/;https://activation-v2.sls.microsoft.com/;https://validation-v2.sls.microsoft.com/;https://displaycatalog.mp.microsoft.com/;https://licensing.mp.microsoft.com/;https://purchase.mp.microsoft.com/;https://displaycatalog.md.mp.microsoft.com/;https://licensing.md.mp.microsoft.com/;https://purchase.md.mp.microsoft.com/"}

FQDN in Windows Firewall Rules

- Set-MpPreference -EnableNetworkProtection Enabled

- $domains = @('*.azure.com', '*.duosecurity.com', '*.azure.net', '*.microsoft.com', '*.windowsupdate.com', '*.microsoftonline.com', '*.microsoftonline.cn', '*.windows.net', '*.windowsazure.com', '*.windowsazure.cn', '*.azure.cn', '*.loganalytics.io', '*.applicationinsights.io', '*.vsassets.io', '*.azure-automation.net', '*.visualstudio.com', 'portal.office.com', '*.aspnetcdn.com', '*.sharepointonline.com', '*.msecnd.net', '*.msocdn.com', '*.webtrends.com', '*.msidentity.com', '*.auth.microsoft.com', '*.msftidentity.com', 'account.activedirectory.windowsazure.com', 'accounts.accesscontrol.windows.net', 'adminwebservice.microsoftonline.com', 'api.passwordreset.microsoftonline.com', 'autologon.microsoftazuread-sso.com', 'becws.microsoftonline.com', 'ccs.login.microsoftonline.com', 'clientconfig.microsoftonline-p.net', 'companymanager.microsoftonline.com', 'device.login.microsoftonline.com', 'graph.microsoft.com', 'graph.windows.net', 'login.microsoft.com', 'login.microsoftonline.com', 'login.microsoftonline-p.com', 'login.windows.net', 'logincert.microsoftonline.com', 'loginex.microsoftonline.com', 'login-us.microsoftonline.com', 'nexus.microsoftonline-p.com', 'passwordreset.microsoftonline.com', 'provisioningapi.microsoftonline.com', '*.msftauth.net', '*.live.com', '*.msauth.net', '*.cdn.office.net', '*.akamaihd.net', '*.office.com', '*.res.office365.com', '*.azureedge.net', 'arc.msn.com', 'outlook.office365.com', '*.atmrum.net', '*.azr.footprintdns.com', '*.exchange.microsoft.com', 'shellprod.msocdn.com', '*.akamaiedge.net', 'wildcard.msocdn.com.edgekey.net', '*admin.sharepoint.com', '*.msedge.net', '*.asm.skype.com', '*.config.office.net', 'cdn.botframework.com', '*.omnichannelengagementhub.com', '*.powerapps.com', '*.dynamics.com', '*.powerbi.com', '*.microsoftstream.com', '*.onestore.ms', '*.assets-yammer.com', '*.yammer.com', '*.microsoft365.com', 'live.sysinternals.com', 'https://go.microsoft.com/', 'http://go.microsoft.com/', 'https://login.live.com', 'https://activation.sls.microsoft.com/', 'http://crl.microsoft.com/pki/crl/products/MicProSecSerCA_2007-12-04.crl', 'https://validation.sls.microsoft.com/', 'https://activation-v2.sls.microsoft.com/', 'https://validation-v2.sls.microsoft.com/', 'https://displaycatalog.mp.microsoft.com/', 'https://licensing.mp.microsoft.com/', 'https://purchase.mp.microsoft.com/', 'https://displaycatalog.md.mp.microsoft.com/', 'https://licensing.md.mp.microsoft.com/', 'https://purchase.md.mp.microsoft.com/')

- foreach ($domain in $domains) {
- $id = '{' + (New-Guid).ToString() + '}'
- New-NetFirewallDynamicKeywordAddress -Id $id -Keyword $domain -AutoResolve $true
- New-NetFirewallRule -DisplayName "allow $domain" -Action Allow -Direction Outbound -RemoteDynamicKeywordAddresses $id }

Security Baselines for PAW

TPM, BitLocker, Ei-Admin, AppLocker, Baseline, Netin hallinta, inbound RDP blokattu.