



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 Influential 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

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?



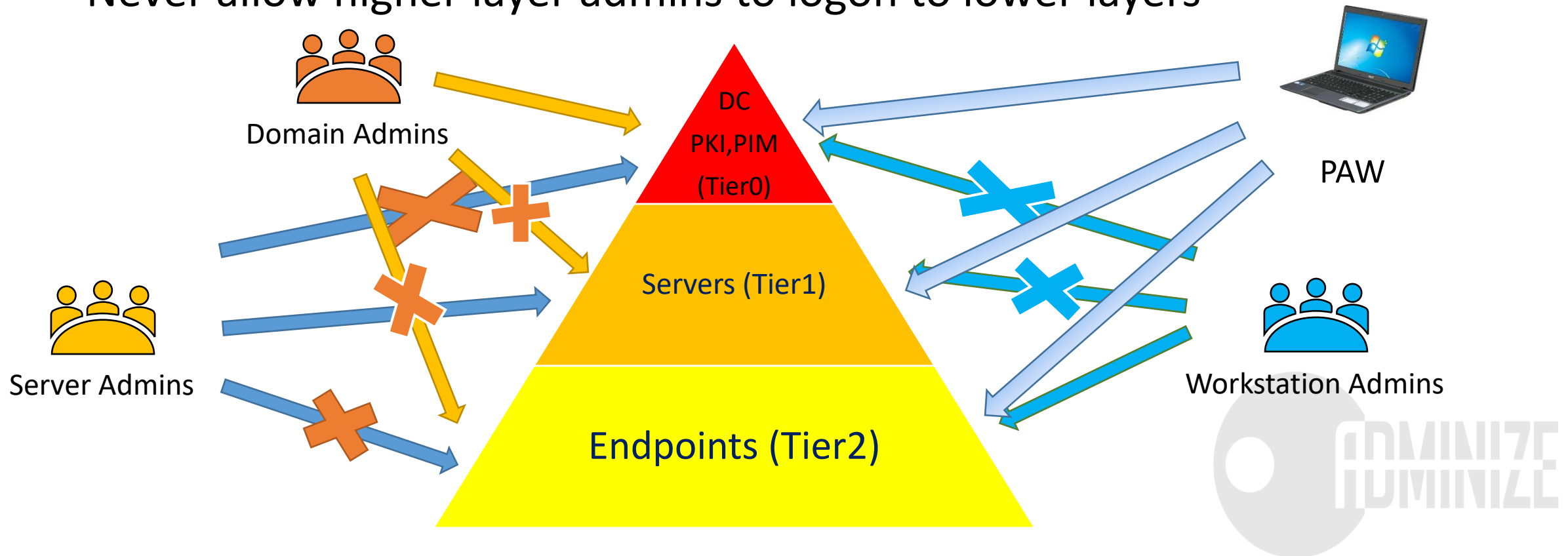
Tier Model AD/AAD

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!

The image shows the Group Policy Management console and the Group Policy Management Editor. In the console, the 'Computers' folder under 'concept.local' is highlighted with a red arrow. The 'Computers' folder is expanded, showing sub-policies like 'c_AppLocker_Hardening' and 'Tier0_Protection', with another red arrow pointing to 'Tier0_Protection'. The 'Computers' table in the console is as follows:

Link Order	GPO	Enforced	Link Enabled	GPO Status	W
1	c_AppLocker_Hard...	No	Yes	Enabled	Nc
2	Tier0_Protection	No	Yes	Enabled	Nc

The Group Policy Management Editor window shows the 'Tier0_Protection [CONDC1.CONCEPT.LOCAL] Policy' selected. The left pane shows the hierarchy: Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies. The right pane shows the list of policies, with 'Deny access to this computer from the network' selected and highlighted in blue. A red box highlights the following policies:

Policy	Policy Setting
Deny access to this computer from the network	CONCEPT\Domain Admins
Deny log on as a batch job	CONCEPT\Domain Admins
Deny log on as a service	CONCEPT\Domain Admins
Deny log on locally	CONCEPT\Domain Admins
Deny log on through Remote Desktop Services	CONCEPT\Domain Admins

Adding Groups

The screenshot displays the Group Policy Management Editor interface. On the left, the tree view shows the hierarchy: Tier0_Protection [CONDC1.CONCEPT.LOCA] > Computer Configuration > Policies > Windows Settings > Security Settings > Restricted Groups. The 'Restricted Groups' folder is highlighted with a red box. The main pane shows a table with the following content:

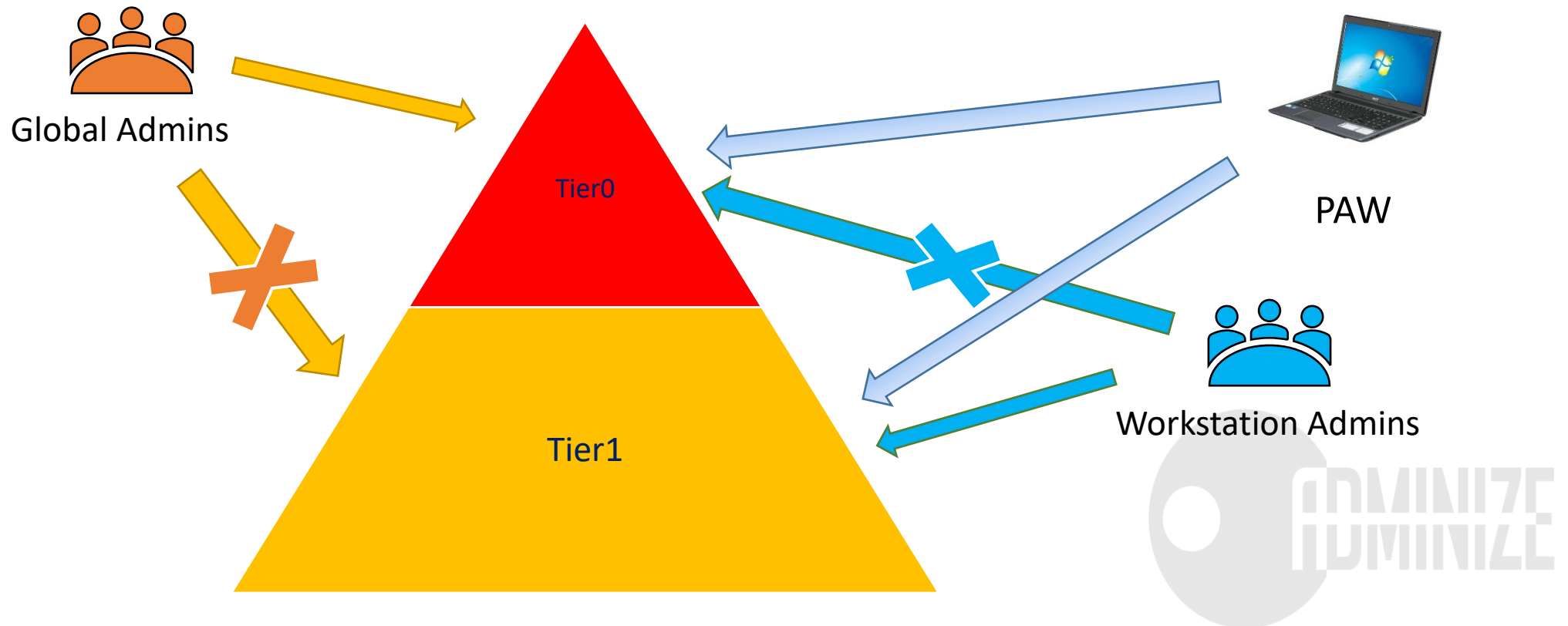
Group Name	Members	Member Of
CONCEPT\G_ComputerAdmins		Administrators

The 'CONCEPT\G_ComputerAdmins' group name is highlighted with a red box. Below the table, the 'CONCEPT\G_ComputerAdmins Properties' dialog box is open, showing the 'Configure Membership for CONCEPT\G_Compute...' section. The 'Members of this group:' list contains the text '<This group should contain no members>' and is highlighted with a red box. To the right of this list are 'Add...' and 'Remove' buttons. Below this, the 'This group is a member of:' list contains 'Administrators' and is also highlighted with a red box. To the right of this list are 'Add...' and 'Remove' buttons.



... 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!





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?

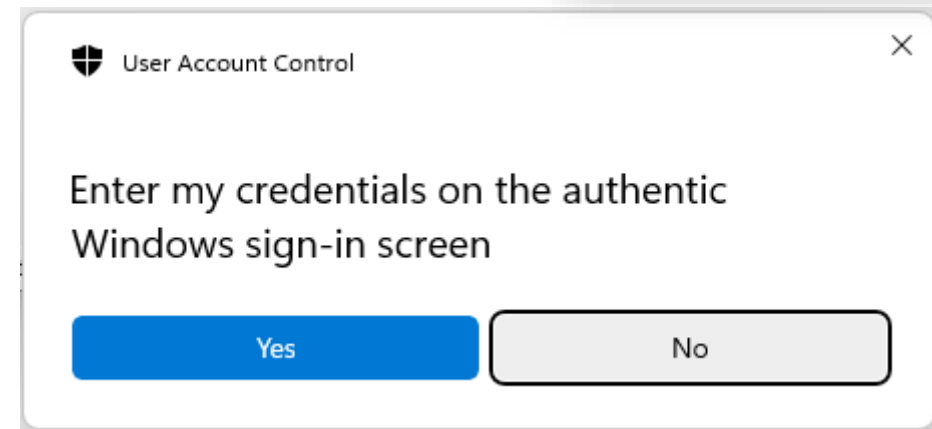
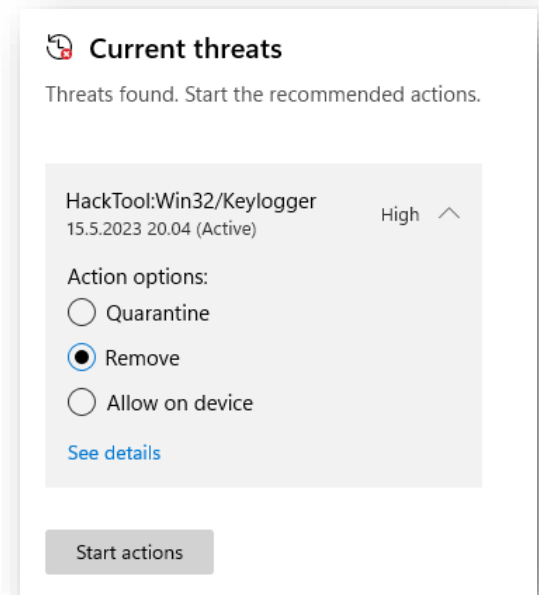
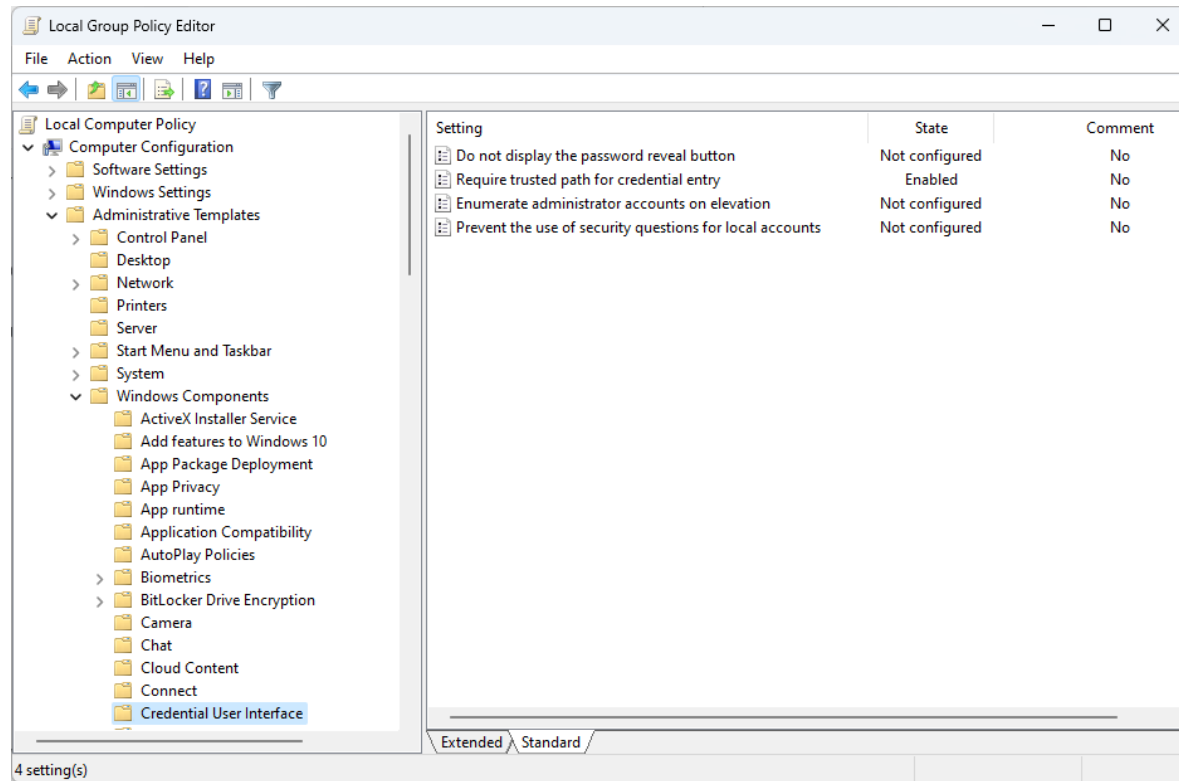


Platforms?

- 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

The screenshot shows the Local Group Policy Editor window. The left pane displays a tree view of policy categories, with 'Windows Update' expanded. The right pane shows the 'Manage updates offered from Windows Update' folder, with the 'Do not include drivers with Windows Updates' policy selected. The policy is currently set to 'Not configured'. A table below the policy lists other settings in the folder, all of which are also 'Not configured'. A description box explains that enabling this policy prevents Windows Update from installing drivers with security vulnerabilities.

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

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?

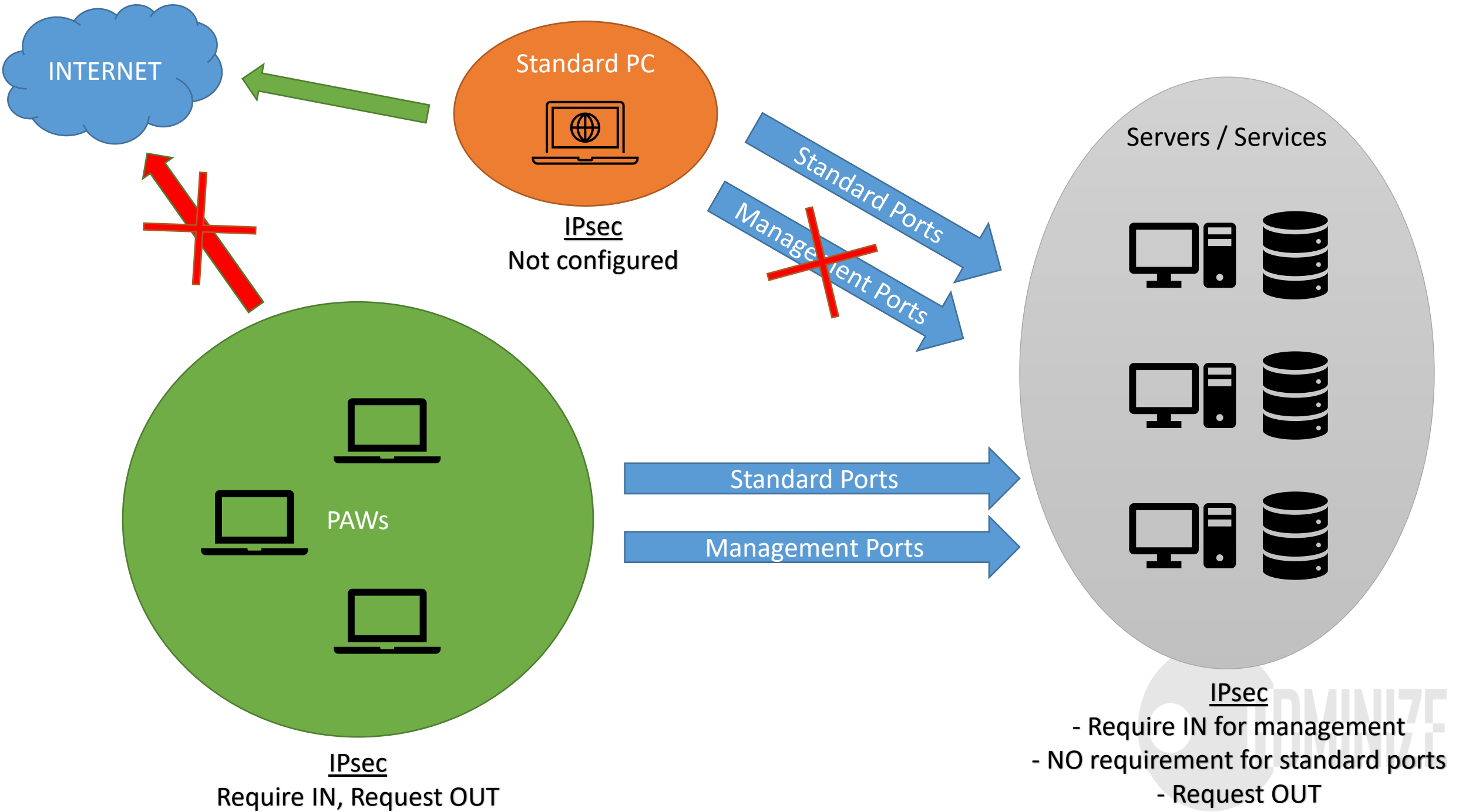
What about Jump Servers?

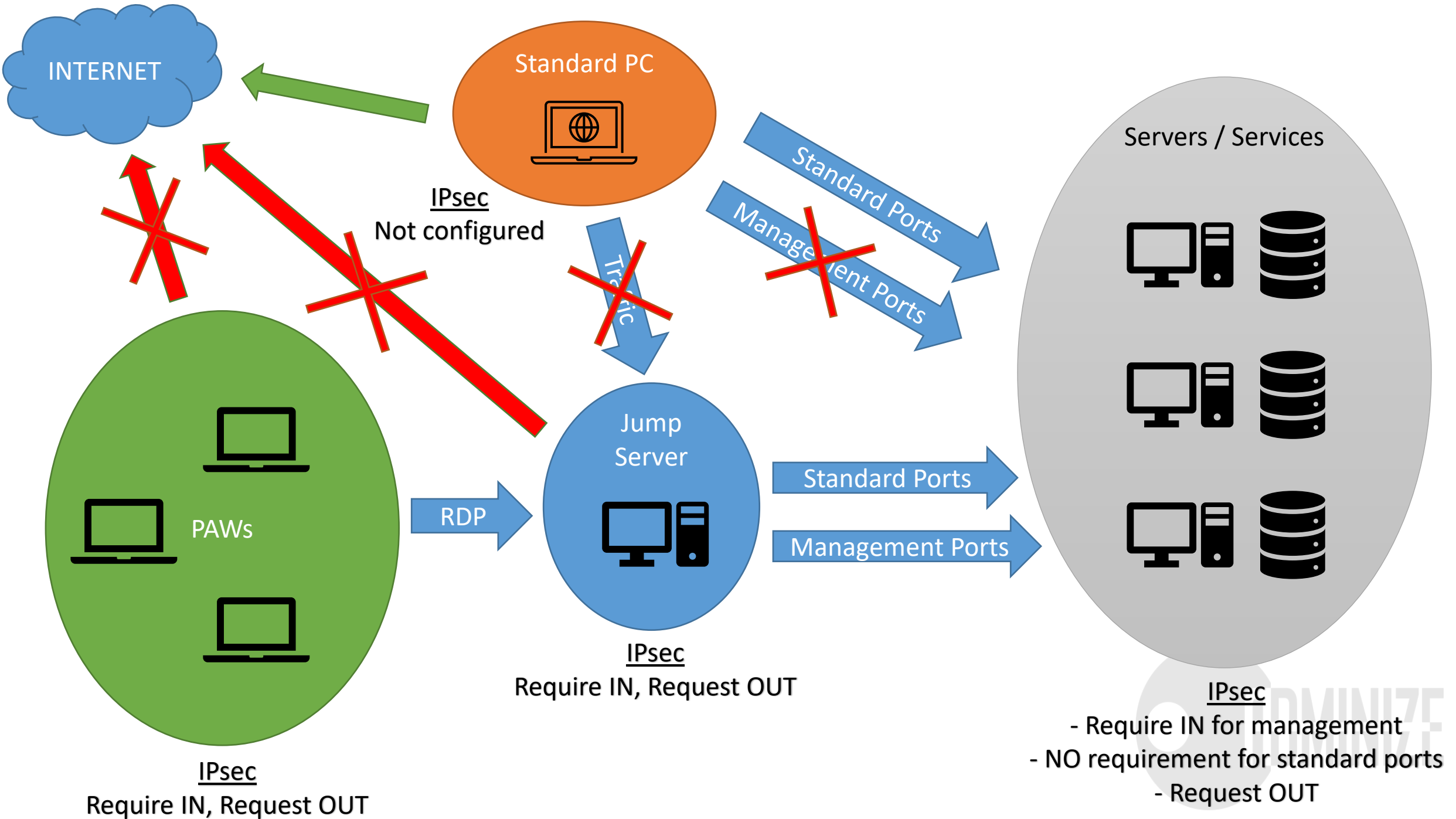


Jump Servers

- 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.



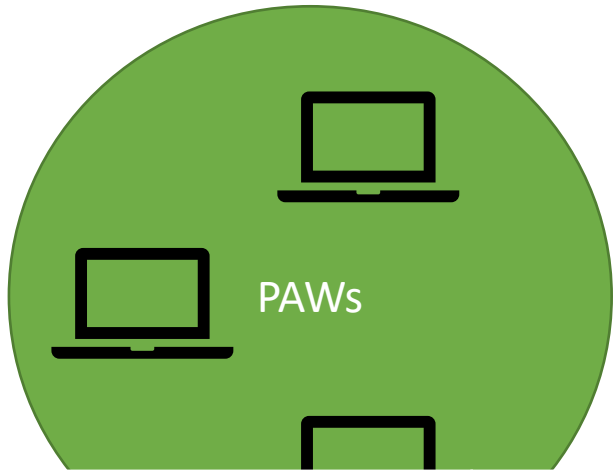




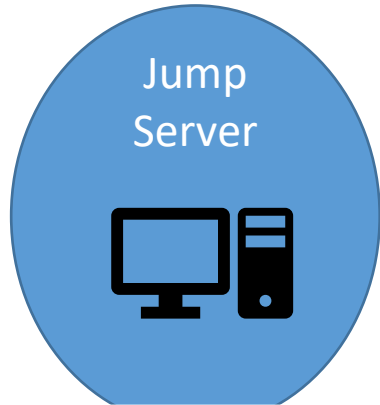
Administrators-group members



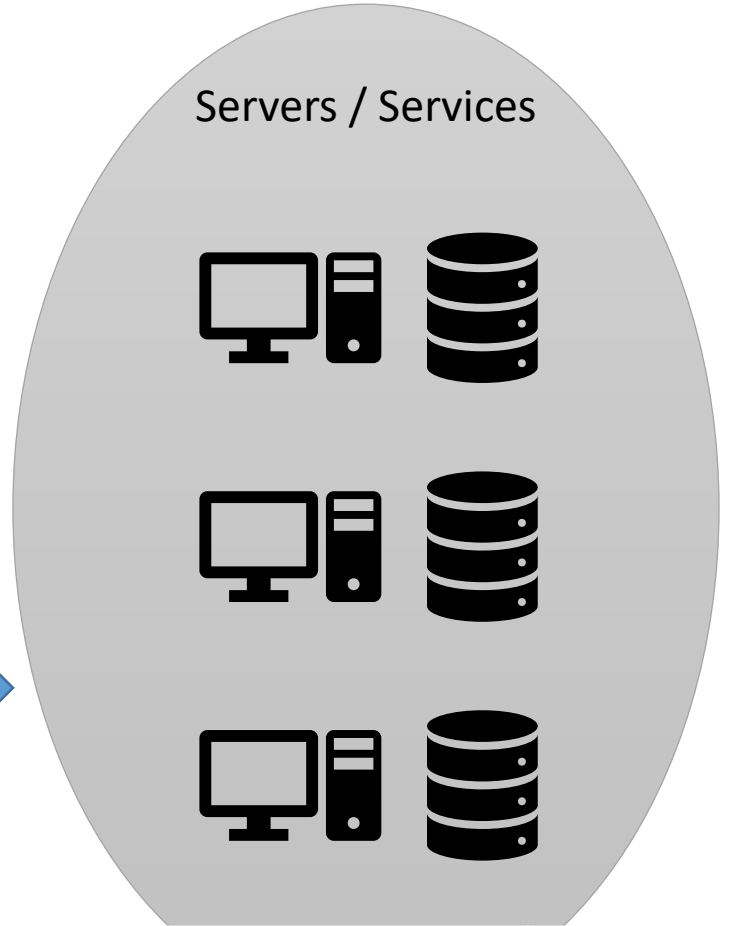
Administrators	
Domain Admins	YES
Workstations Admins	YES
Server Admins	NO
Builtin Administrator (used via LAPS)	YES



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



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>

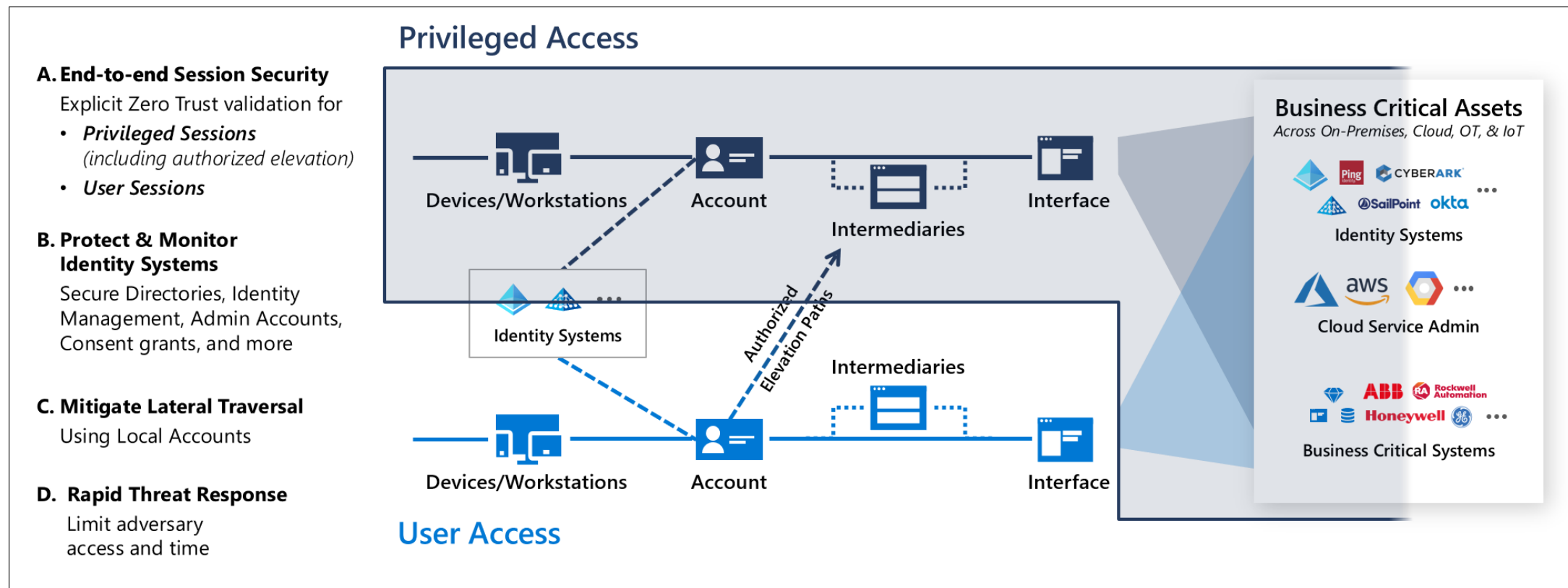


Azure PAW



Microsoft RAMP

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



DeviceID to identify PAWs

The screenshot shows the Microsoft Azure portal interface. At the top, there is a navigation bar with the Microsoft Azure logo, a search bar, and user information for 'admin@ac MATTI LAIHO OY'. Below the navigation bar, the breadcrumb trail reads 'Home > Matti Laiho Oy > Devices >'. The main content area displays the 'XENPAW01 | Properties' page for 'Matti Laiho Oy - Azure Active Directory'. A 'Manage' section contains buttons for 'Manage', 'Enable', 'Disable', and 'Delete'. A left-hand menu lists 'Properties', 'Roles and administrators (Preview)', and 'Administrative Units (Preview)'. The main content area shows a table of properties for the device:

Name	XENPAW01
<u>Device ID</u>	cc9a0baa-63fc-47b4-9d54-d159d41329de
Object ID	1c89153b-8cb9-4644-b93c-c6cfbedcab91
Enabled	Yes



Conditional Access to filter out PAWs

Microsoft Azure Search resources, services, and docs (G+/)

admin@adminize.com
MATTI LAIHO OY (ADMINIZE.CO...)

Home > Conditional Access

BLOCK - Require PAWs

Conditional Access policy

Delete

Control access based on Conditional Access policy to bring signals together for access decisions, and enforce organizational policies. [Learn more](#)

Name *

BLOCK - Require PAWs

Assignments

Users or workload identities

Specific users included and excluded

Cloud apps or actions ⓘ

All cloud apps

Filter for devices

Configure a filter to apply policy to specific devices. [Learn more](#)

Configure ⓘ

Yes No

Devices matching the rule:

Include filtered devices in policy

Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value	
	deviceid	Equals	cc9a0baa-63fc-47b4-9d54-d159d41329de	
Or	deviceid	Equals	1c3bcf29-3743-48da-bade-a4a937b40c3e	

+ Add expression

Rule syntax ⓘ

```
device.deviceid -eq "cc9a0baa-63fc-47b4-9d54-d159d41329de" -or device.deviceid -eq "1c3bcf29-3743-48da-bade-a4a937b40c3e"
```

Edit

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

The screenshot displays the Windows Group Policy Editor interface. The left-hand pane shows the navigation tree under 'PAW-Restrictions [DC02.ELAIHO.INT] Policy', with 'Proxy server' selected under 'Administrative Templates: Policy definitions' > 'Microsoft Edge'. The main pane shows the 'Proxy server' policy details, including requirements, description, and a list of overridden settings.

Proxy server

Proxy settings

Edit [policy setting](#).

Requirements:
Microsoft Edge version 77,
Windows 7 or later

Description:
Configures the proxy settings for Microsoft Edge.

If you enable this policy, Microsoft Edge ignores all proxy-related options specified from the command line.

If you don't configure this policy, users can choose their own proxy settings.

This policy overrides the following individual policies:

- 'ProxyMode' (Configure proxy server settings)
- 'ProxyPacUrl' (Set the proxy .pac file URL)
- 'ProxyServer' (Configure address or URL of proxy server)
- 'ProxyBypassList' (Configure proxy bypass rules)

Setting	State
Configure proxy bypass rules (deprecated)	Not configured
Configure proxy server settings (deprecated)	Not configured
Set the proxy .pac file URL (deprecated)	Not configured
Configure address or URL of proxy server (deprecated)	Not configured
Proxy settings	Enabled

MINI7C
MINI4C

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;*.we
btrends.com;*.msidentity.com;*.auth.microsoft.com;*.msftidentity.com;account.activedirectory.windowsazure.com;accounts.acce
sscontrol.windows.net;adminwebservice.microsoftonline.com;api.passwordreset.microsoftonline.com;autologon.microsoftazurea
d-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.mic
rosoft.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.offi
ce.net;*.akamaihd.net;*.office.com;*.res.office365.com;*.azureedge.net;arc.msn.com;outlook.office365.com;*.atmrum.net;*.azr.f
ootprintdns.com;*.exchange.microsoft.com;shellprod.msocdn.com;*.akamaiedge.net;wildcard.msocdn.com.edgekey.net;*.admin.s
harepoint.com;*.msedge.net;*.asm.skype.com;*.config.office.net;cdn.botframework.com;*.omnichannelengagementhub.com;*.p
owerapps.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.microso
ft.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) {
```
- ```
$sid = '{' + (New-Guid).ToString() + '}'
```
- ```
New-NetFirewallDynamicKeywordAddress -Id $sid -Keyword $domain -AutoResolve $true
```
- ```
New-NetFirewallRule -DisplayName "allow $domain" -Action Allow -Direction Outbound -RemoteDynamicKeywordAddresses $sid }
```



# Security Baselines for PAW

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

