CERT.LV vebinārs

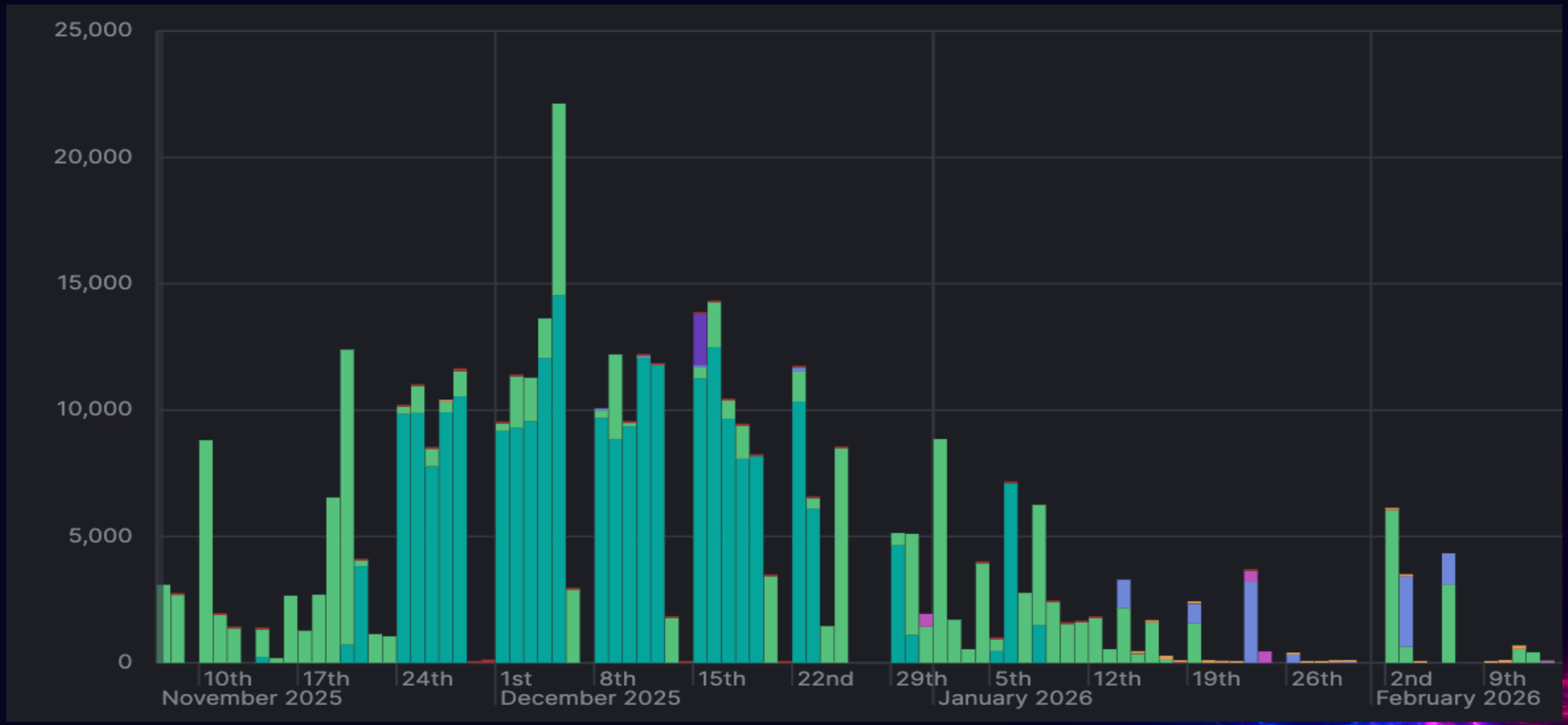
"Efektīva Windows ugunsmūra pārvaldība”

Kristīne Kaula, CERT.LV Drošības operāciju centra vadītāja

Andris Medjānis, CERT.LV kiberdrošības eksperts

17.02.2026

Bruteforce from an External IP



Mīti un patiesība

Dators ir pasargāts korporatīvā vidē aiz iestādes ugunsmūra, mājās netiek nests;

Internet piekļuve un bērni…

Windows Defender pasargā kā ugunsmūris;

Konfigurācijas nianses

Uzstādīts VPN;

Atļauta piekļuve LAN, nav ieslēgts obligāti

Antivīrusa programmatūra pasargā kā ugunsmūris.

Konfigurācijas nianses

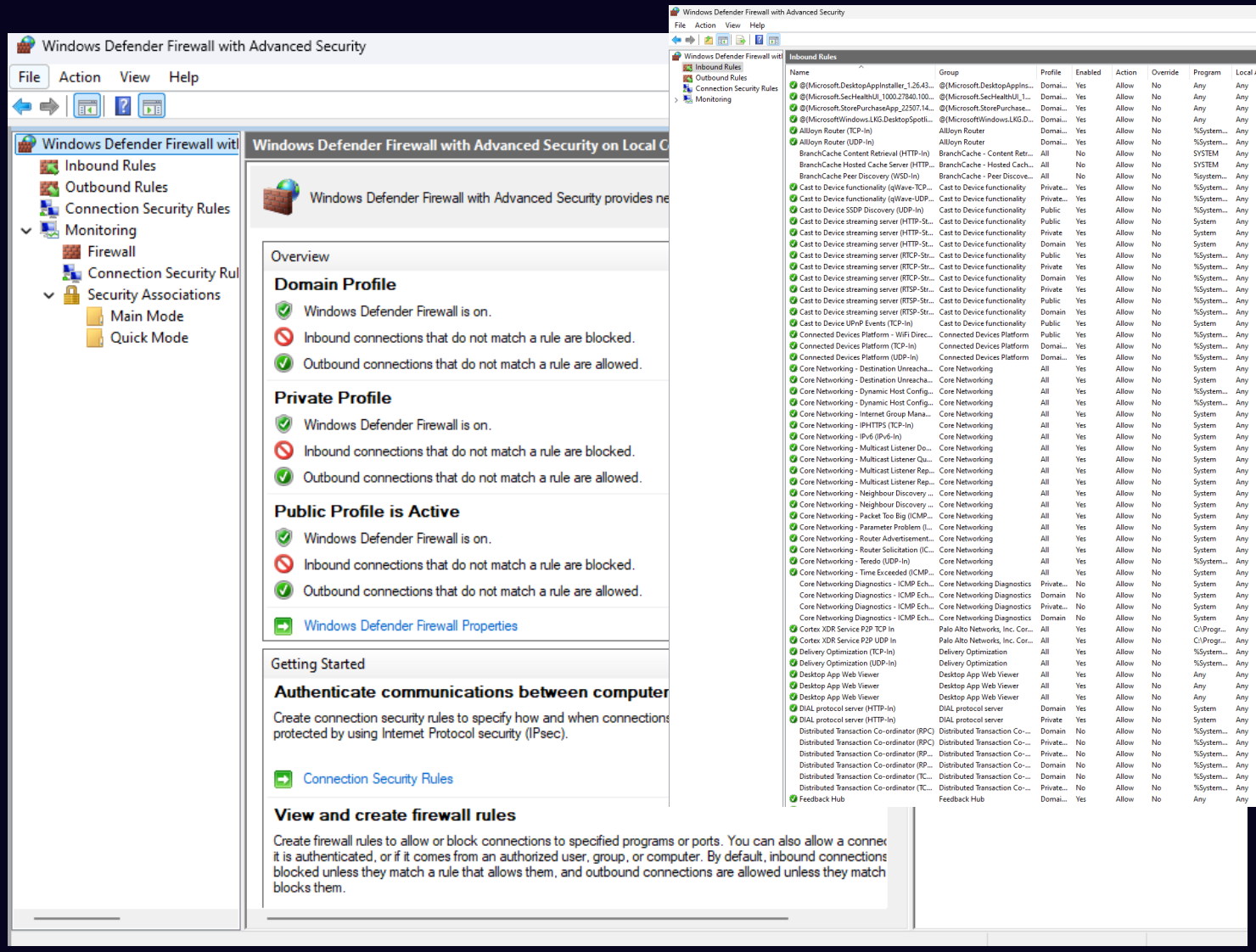
Tvērums

- Auditorijas priekšzināšanas: tīkli un pārvaldība – konceptuāli, Win. ugunsmūris 0-10
- Fokusā Windows Ugunsmūris
- IPSEC (īss ieskats)
- AD Grupu Politika – klasiskā pārvaldība (īss ieskats)
- InTune – mākoņpakalpojuma pārvaldība (īss ieskats)
- Mīti un patiesība
- Pievienotā praktiskā vērtība (nepārlasīt dokumentāciju)
- Semināra ilgums – 16:00 - ?

Plāns

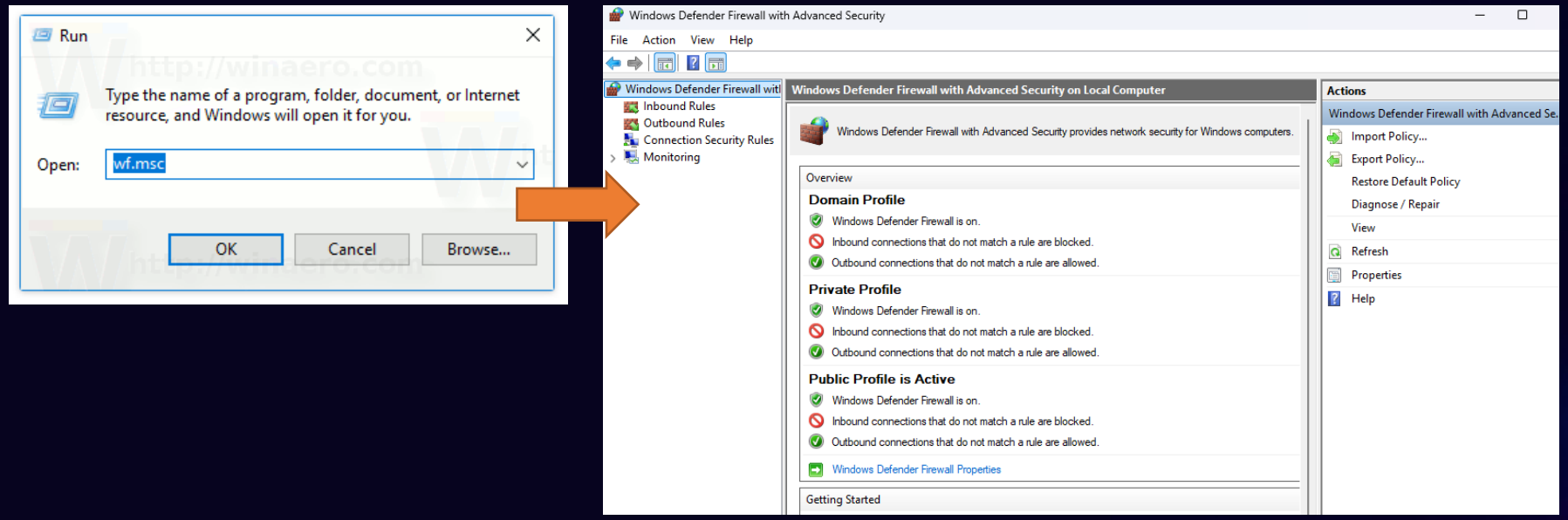
- Ugunsmūra pārvaldība
- Kā tas darbojas
- Galvenās kļūdas
- Iestatījumi (noklusējuma, ieteicamie)
- Žurnālfaili
- Tehniski padomi
- Mīti un patiesība
- Jautājumi, atbildes

Visa sākums

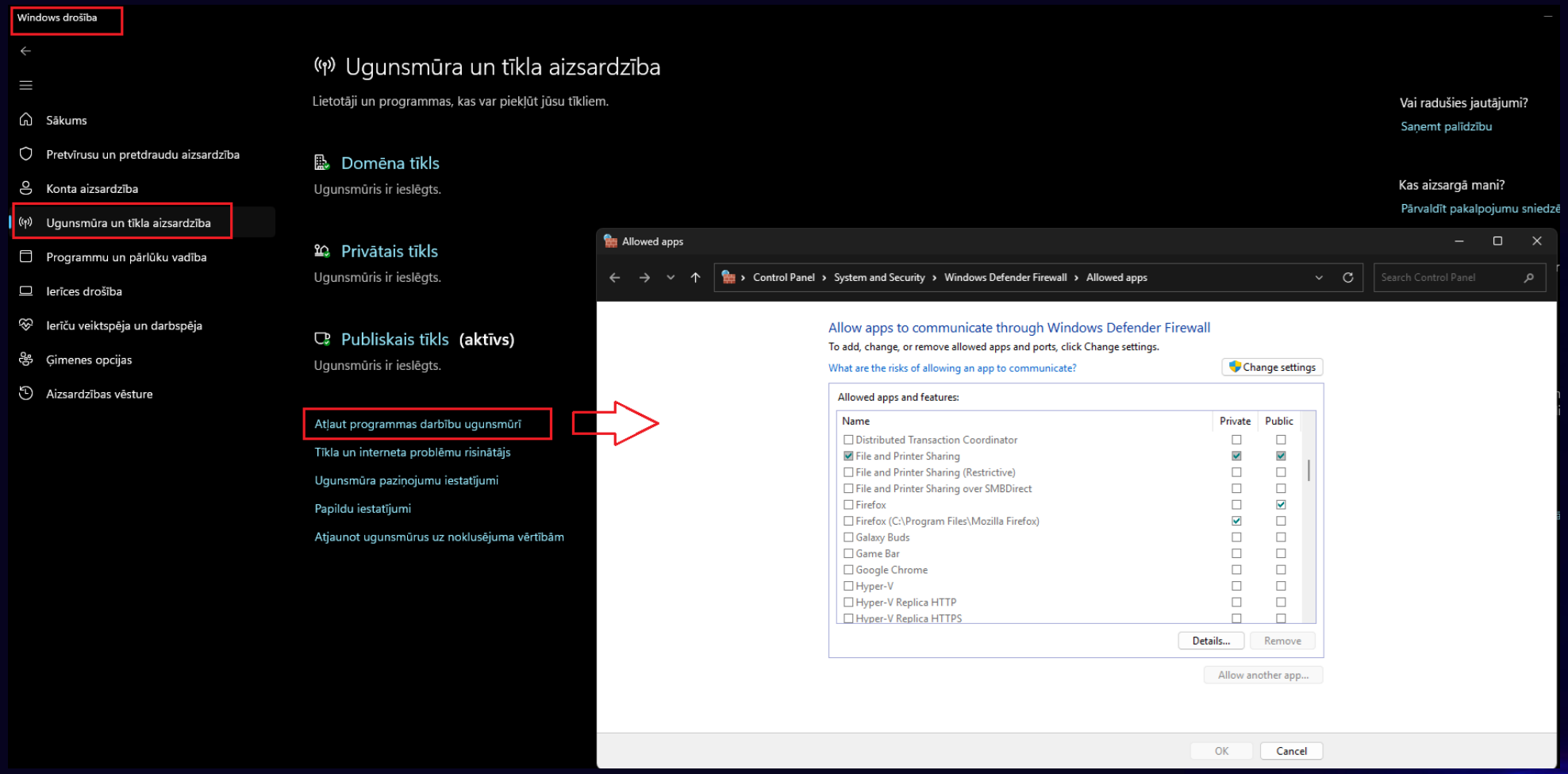

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with Advanced Security on Local C
Windows Defender Firewall with Advanced Security provides ne
Overview
Domain Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile is Active
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Defender Firewall Properties
Getting Started
Authenticate communications between computer
Create connection security rules to specify how and when connections
protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connec
it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections
blocked unless they match a rule that allows them, and outbound connections are allowed unless they match
blocks them.
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Security Associations
Main Mode
Quick Mode

Lokālā pārvaldība

- wf.msc (grafiskā saskarne)



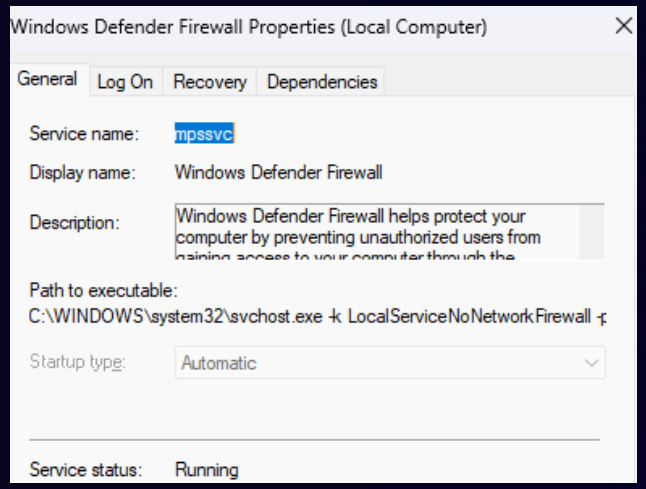
Lokālā pārvaldība (no kā izvairīties)



Lokālā pārvaldība

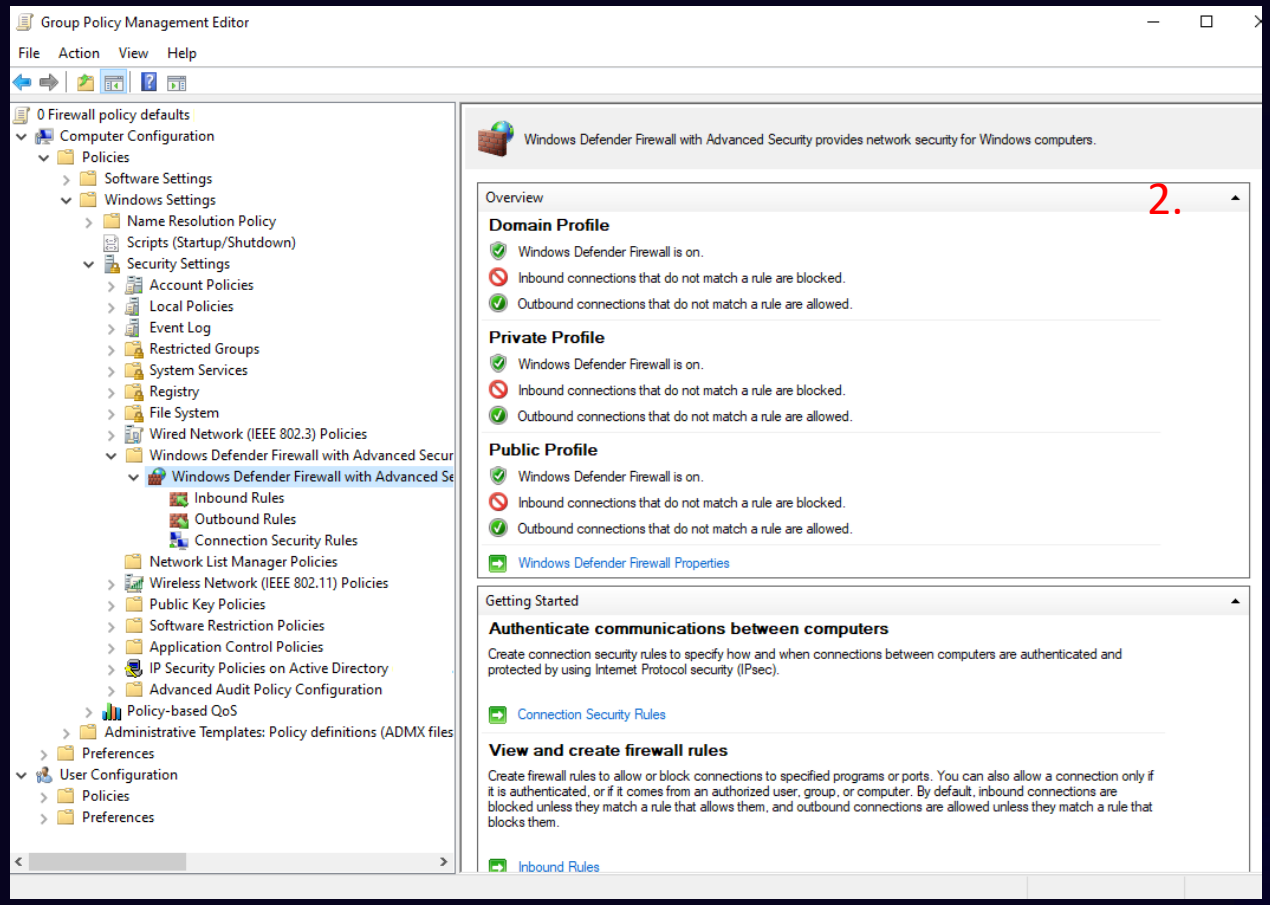
- (klasiski) Netsh Advfirewall
- (moderni PowerShell) Get-NetFirewallRule

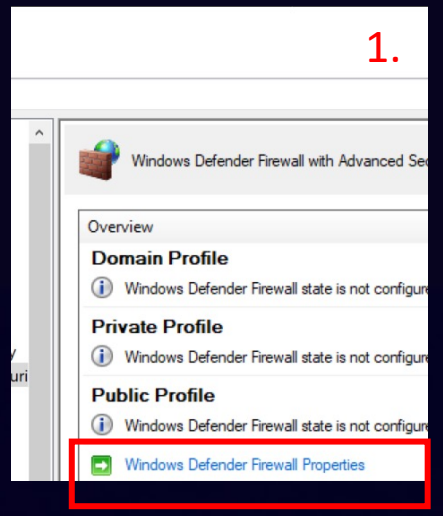
- Informācijai – atbildīgais Win. serviss – Mpssvc Windows Defender Firewall (Neizslēgt!)



*Grupu pārvaldība

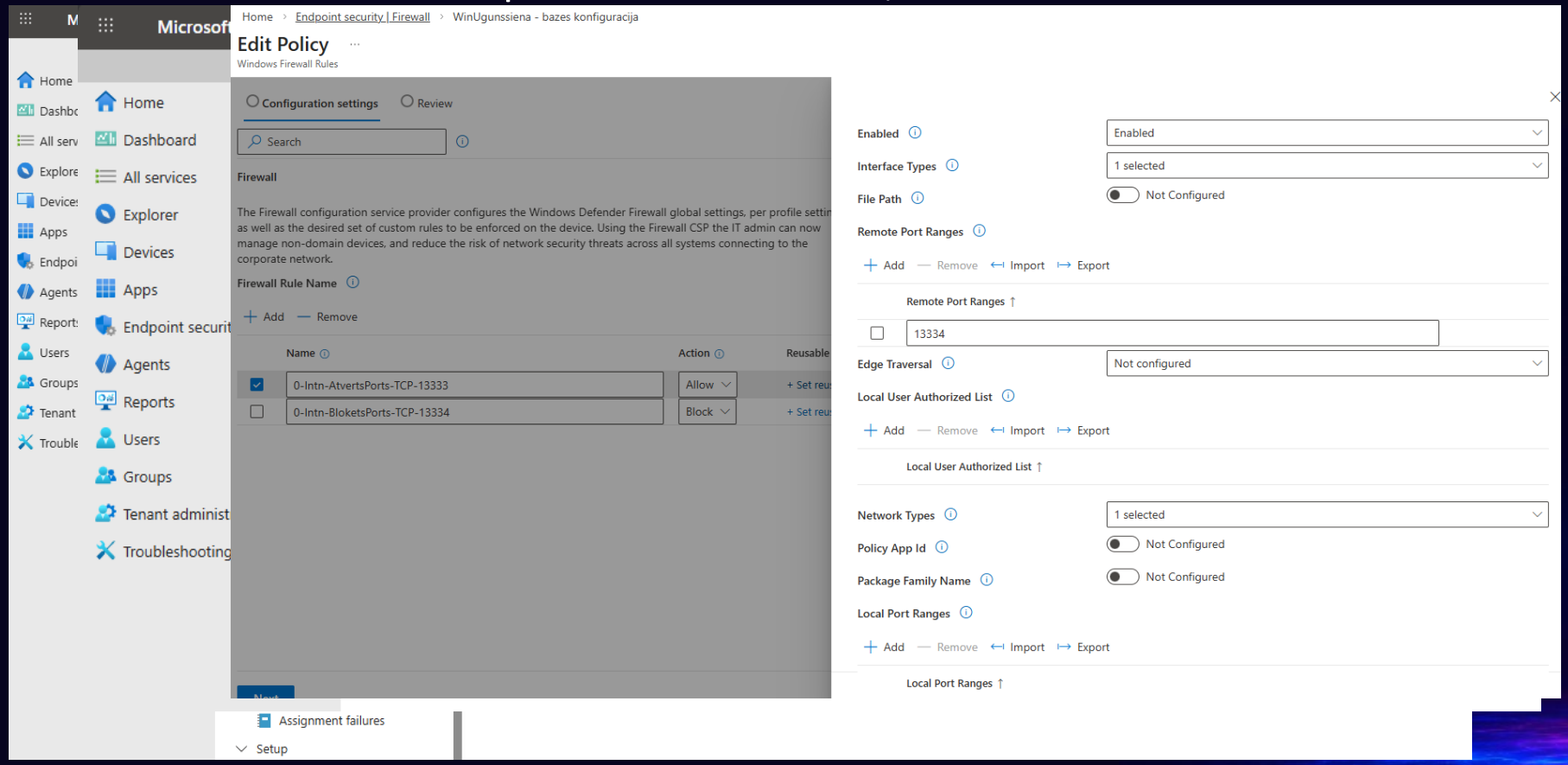
- Aktīvā Direktorija, grupu politika (GPO)
  - * Tēmas robeža – pārvaldība ar AD/GPO





*Grupu pārvaldība

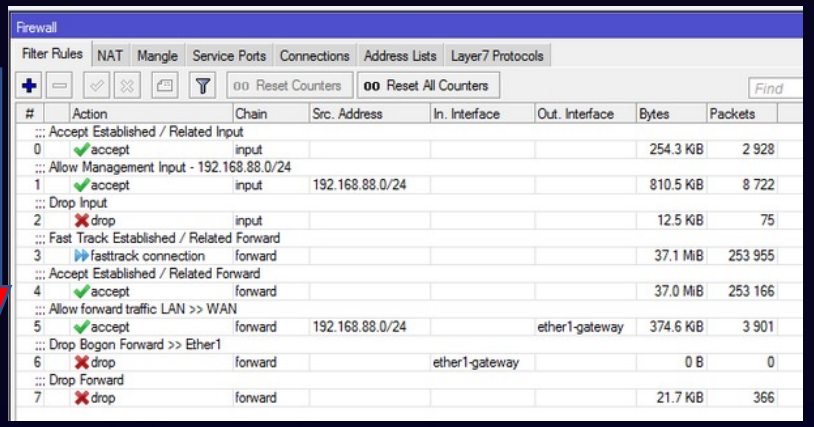
- InTune politika
  - * Tēmas robeža – pārvaldība ar InTune, M365



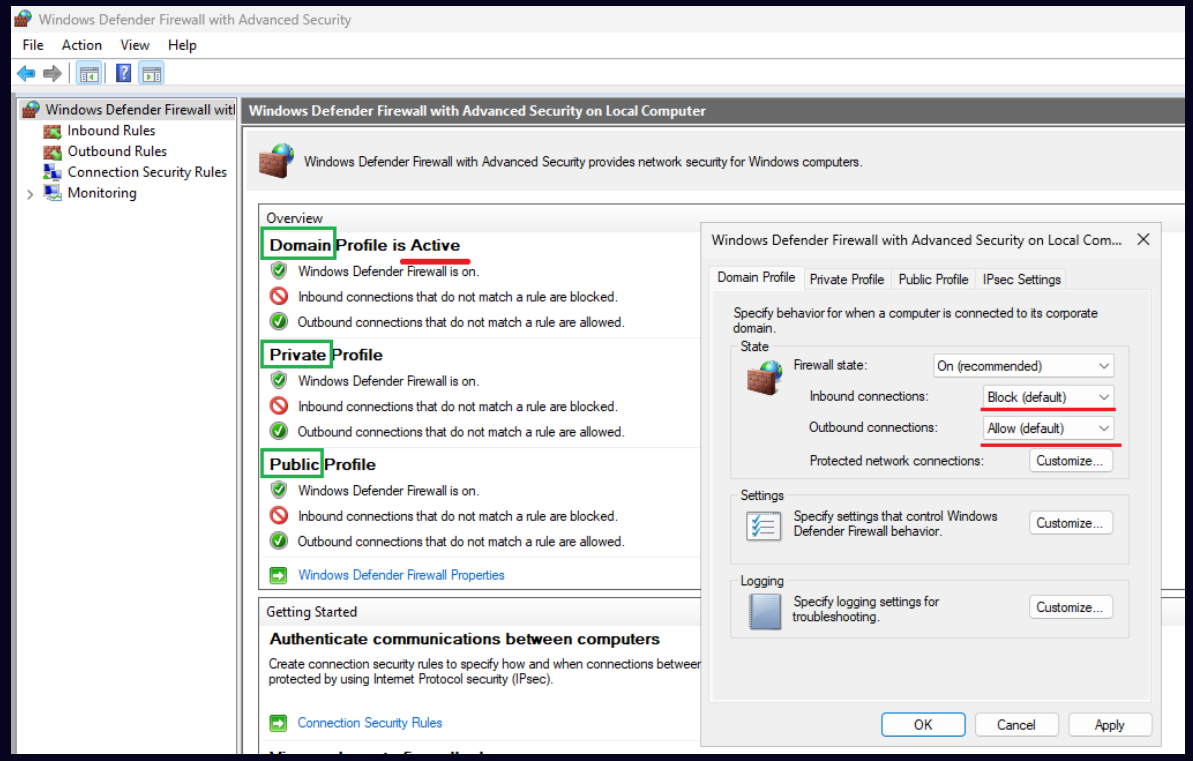
Darbības pamatprincipi

- Klasiski – secīgi, nosacījumi izpildīti rindas kārtībā

15		acce...	forward	192.168.1.10		6 (tcp)	443
16		drop	forward	192.168.1.0/24		6 (tcp)	443

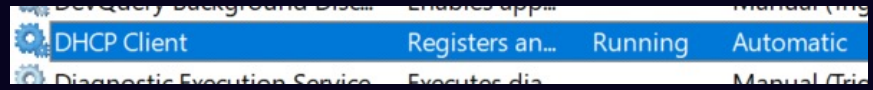


- Windows – profili un noklusējuma darbība

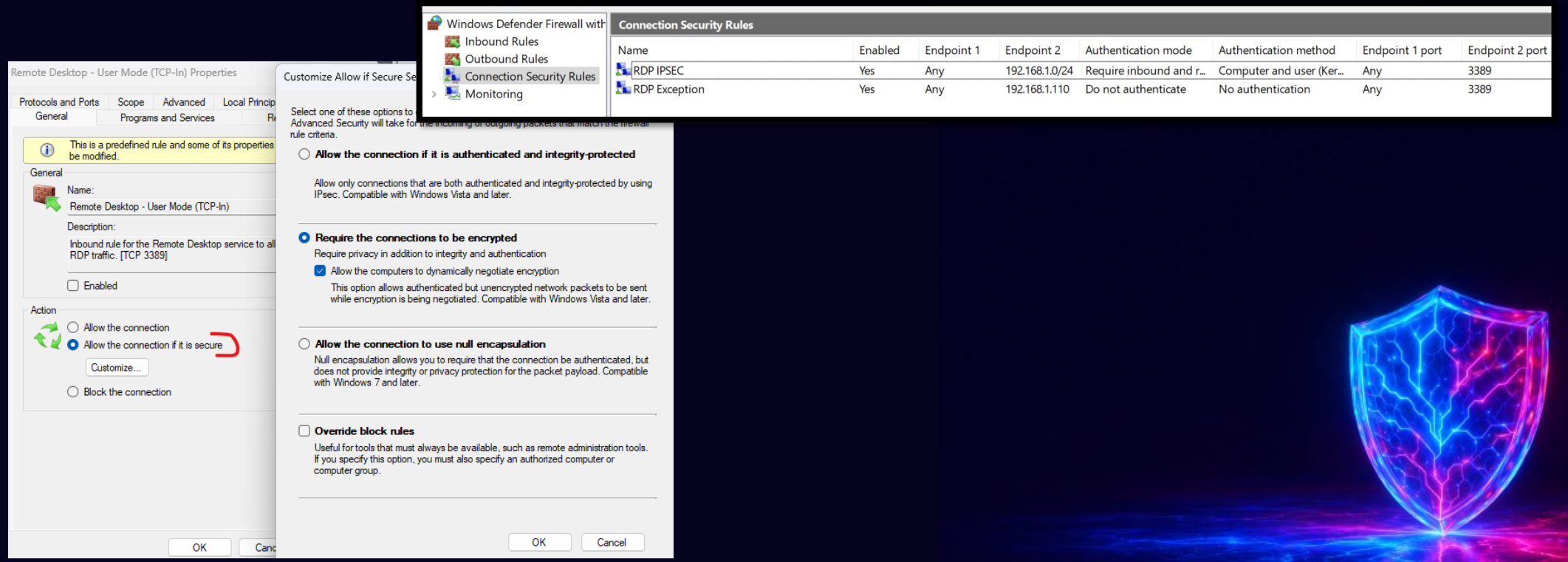


Darbības pamatprincipi - prioritāte

1. Operētājsistēmas pamatelementi (piem., DHCP klients)



2. "Connection security rules" (IPSEC)
   "Allow connection if it is secure" (IPSEC) – nākamais brieduma līmenis

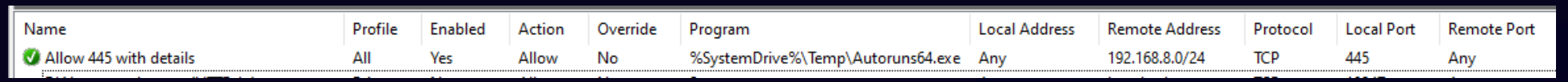
- 

Darbības pamatprincipi - prioritāte

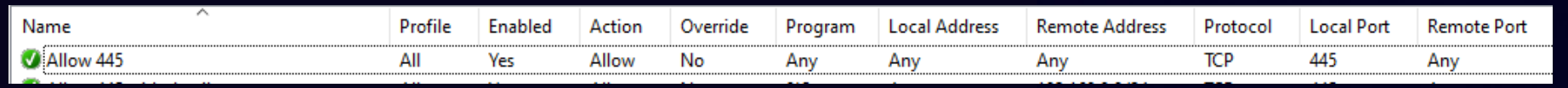
3. Bloķēšana

0_VNC-OUT	All	Yes	Block	No	%SystemDrive%\Users\XTR\Downloads\VNC-\

4. Detalizācija (jo specifiskāki nosacījumi, jo augstāka prioritāte)

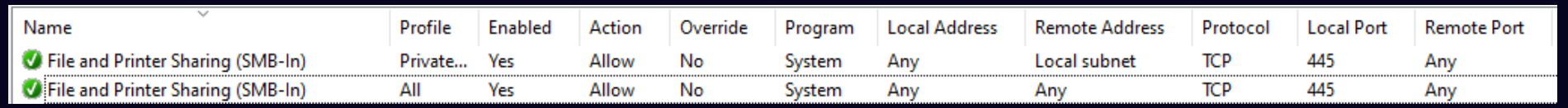


Name	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
Allow 445 with details	All	Yes	Allow	No	%SystemDrive%\Temp\Autoruns64.exe	Any	192.168.8.0/24	TCP	445	Any

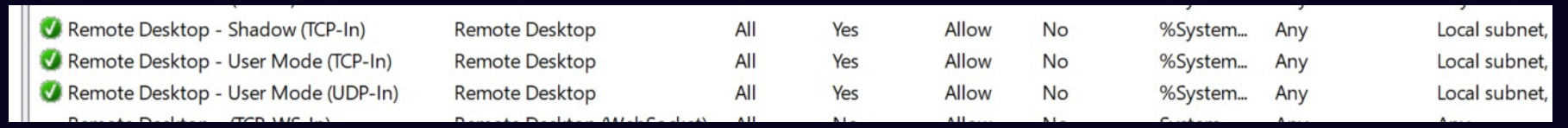


Name	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
Allow 445	All	Yes	Allow	No	Any	Any	Any	TCP	445	Any

5. Noklusējuma nosacījumi



Name	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
File and Printer Sharing (SMB-In)	Private...	Yes	Allow	No	System	Any	Local subnet	TCP	445	Any
File and Printer Sharing (SMB-In)	All	Yes	Allow	No	System	Any	Any	TCP	445	Any



Remote Desktop - Shadow (TCP-In)	Remote Desktop	All	Yes	Allow	No	%System...	Any	Local subnet,
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Allow	No	%System...	Any	Local subnet,
Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	Yes	Allow	No	%System...	Any	Local subnet,

Darbības pamatprincipi - prioritāte

Rezumējums (oficiāli)

1. Operētājsistēmas pamatelementi (piem., DHCP klients)
2. Paaugstinātas drošības nosacījumi (Conn. Sec. Rules), IPSEC
3. Bloķēšana
4. Detalizētākie pāri mazāk detalizētiem
5. Noklusējuma

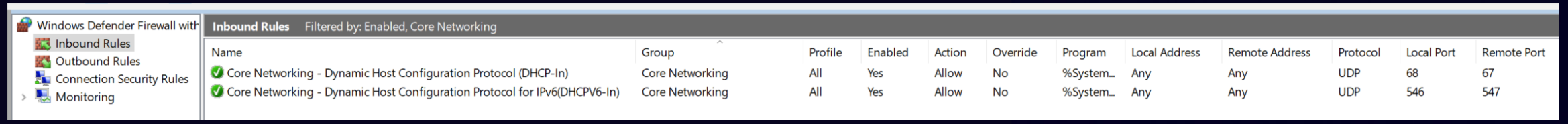
- "Favorītu sistēma"

Darbības pamatprincipi - prioritāte

Realitāte

1. Operētājsistēmas pamatelementi (DHCP klients, DNS klients u.c.)

- Pilna kontrole, jāizveido visi nosacījumi!



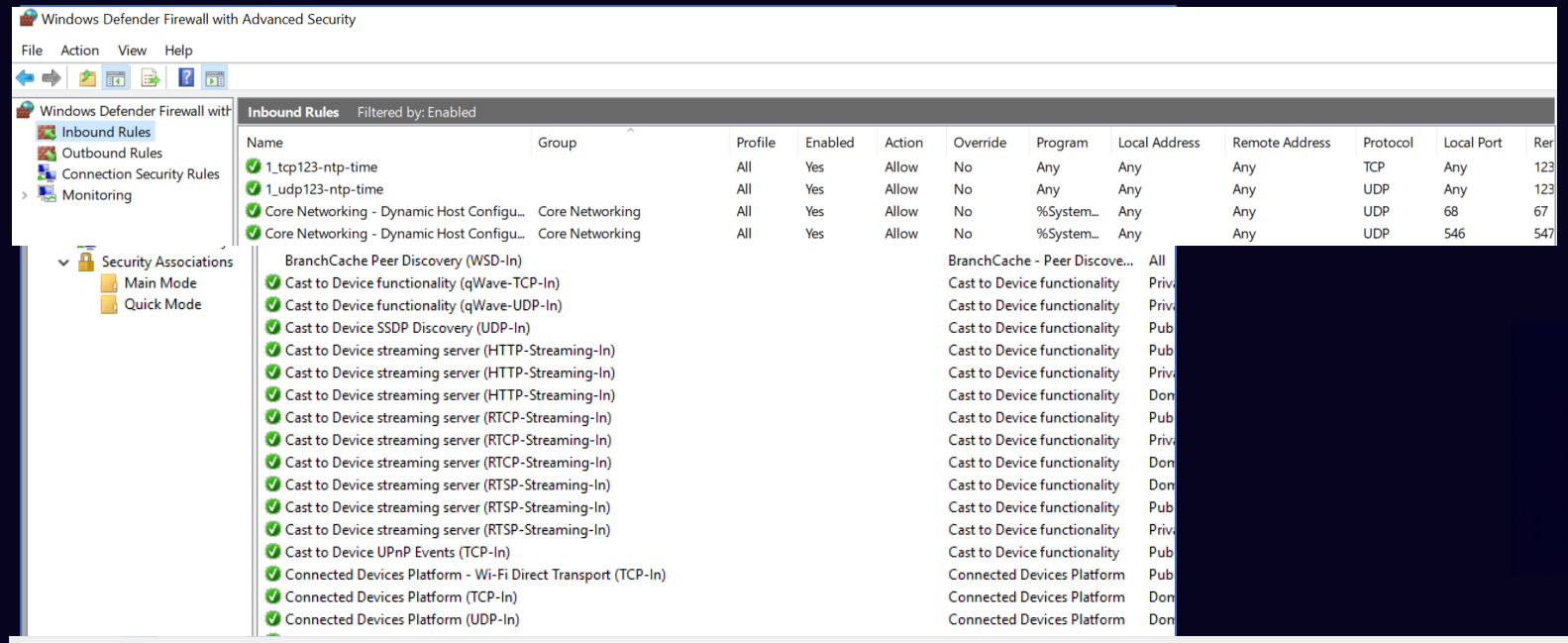
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
Core Networking - Dynamic Host Configuration Protocol (DHCP-In)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	68	67
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	546	547

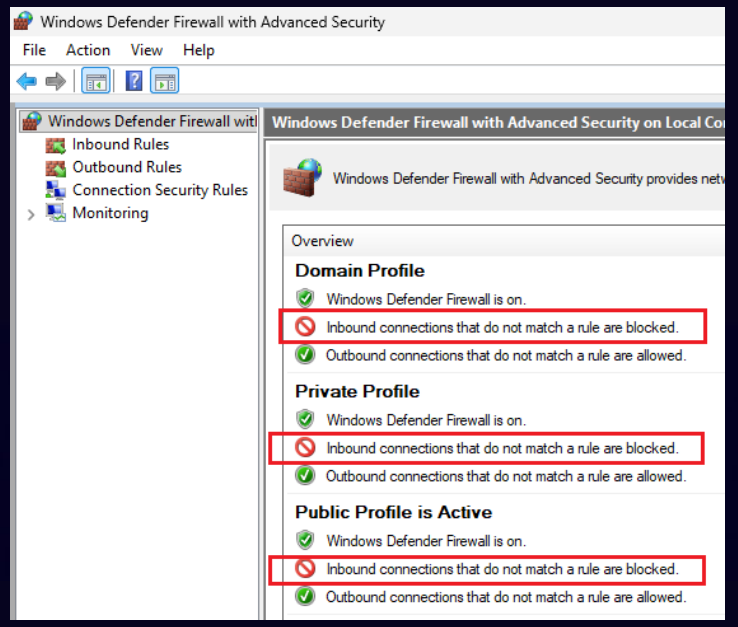
2. Nesarežģīt!

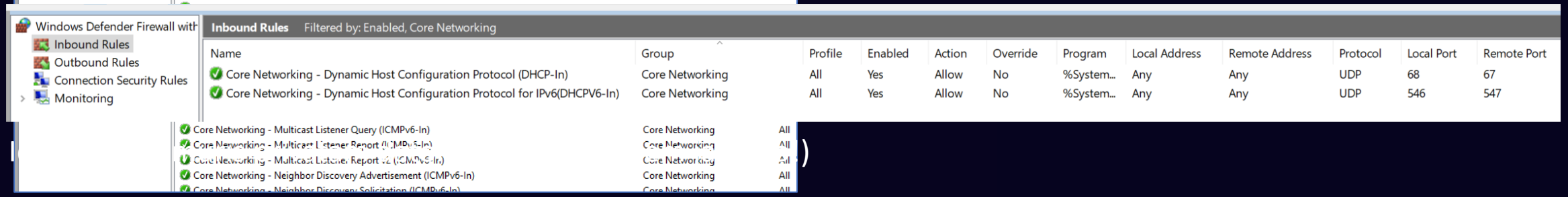
Profila bāze → bloķēšana → atļaušana
(vienkāršoti: profila bāze bloķē → atļauj izņēmumus)

Darbības pamatprincipi

Laiks uzlabojumiem (pirms → pēc)



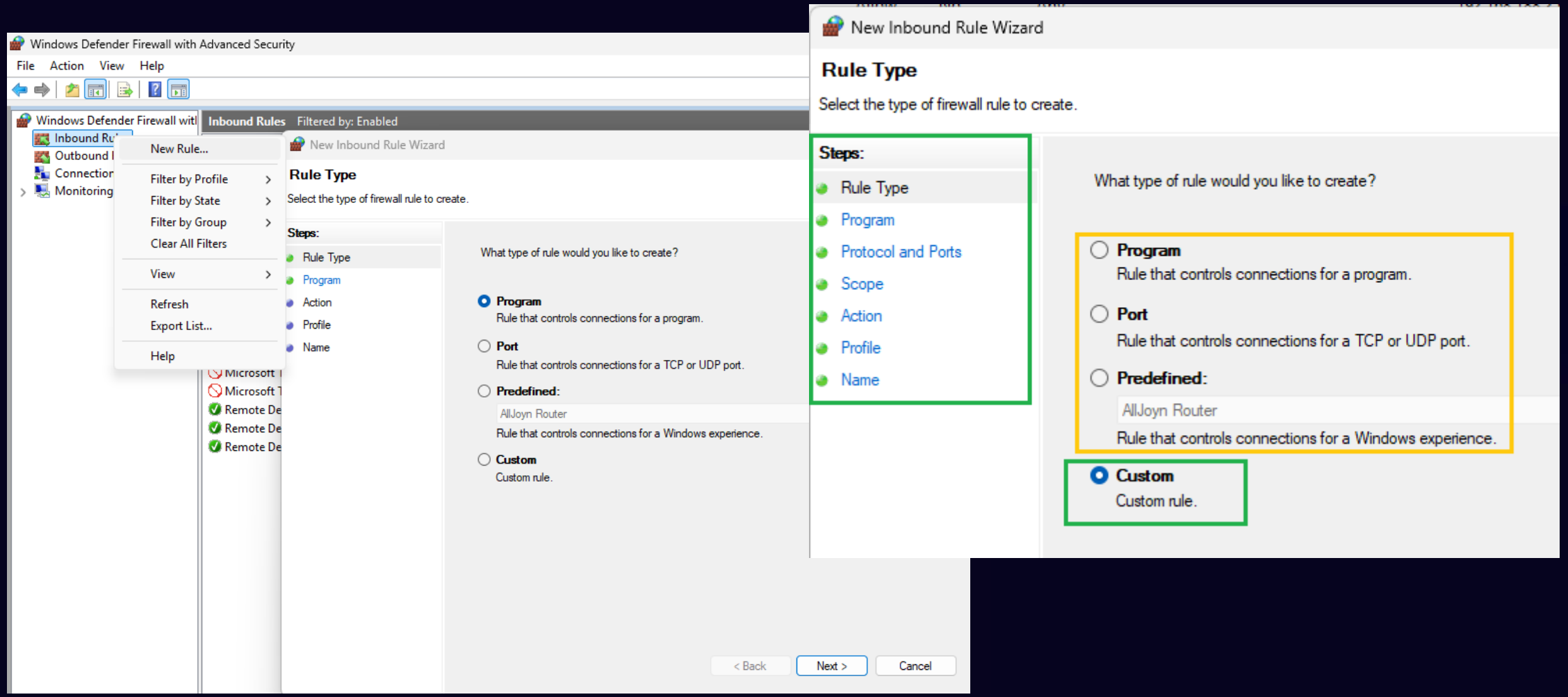




*

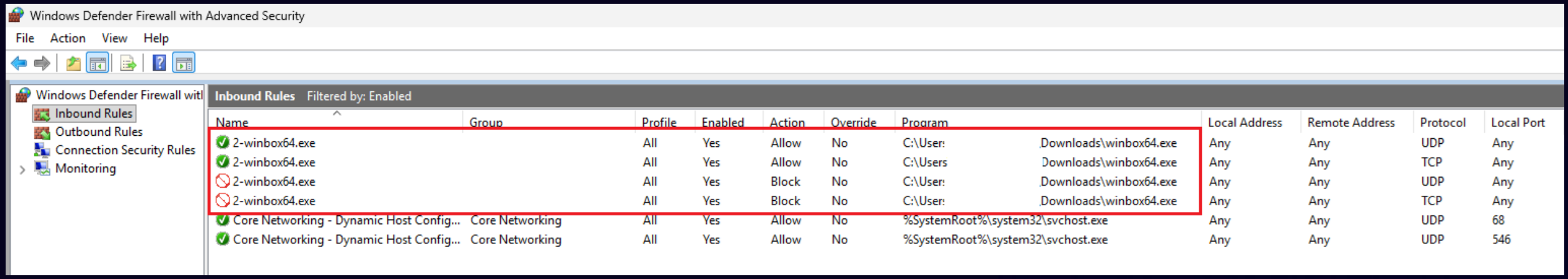
Tehnisks padoms

- Nosacījumu izveide



Tehnisks padoms

- Ugunsmūrī kontrolēt izpildāmos (exe) failus:

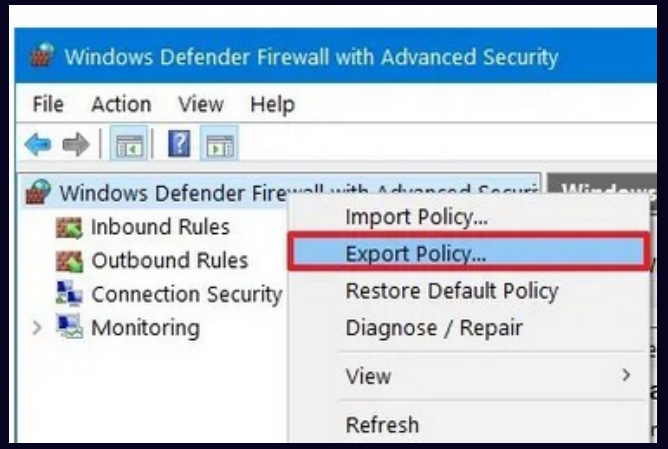


Tehnisks padoms

- Ugunsmūra profila saglabāšana (eksports un imports)

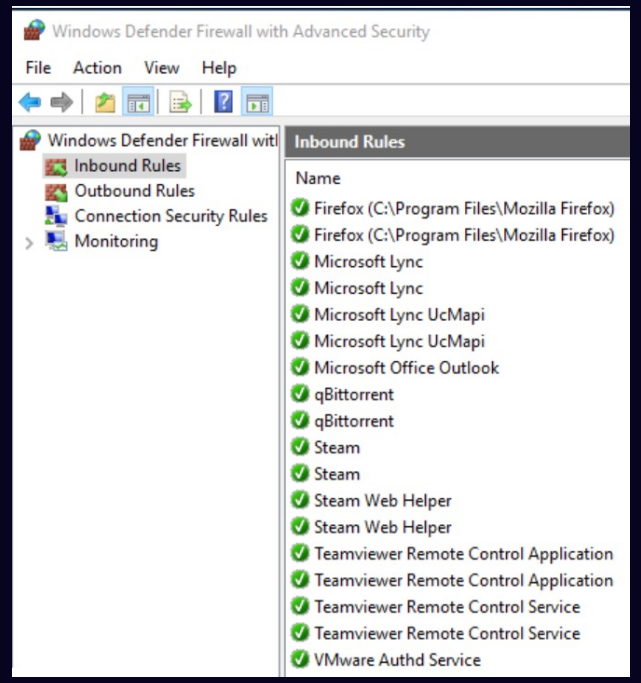
  netsh advfirewall export "C:\temp\firewall-rules.wfw"
  netsh advfirewall import "C:\temp\firewall-rules.wfw"

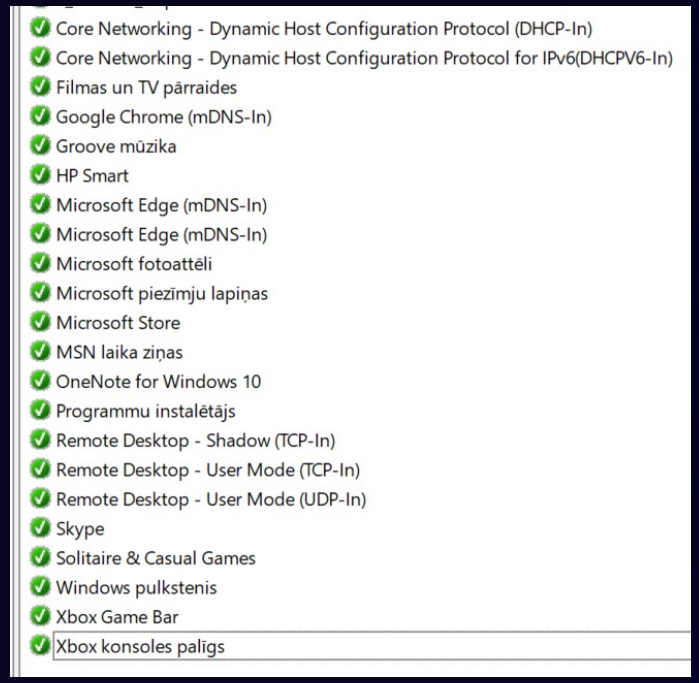
  Export-WindowsFirewallRules -FilePath "C:\temp\firewall-rules.wfw"
  Import-WindowsFirewallRules -FilePath "C:\temp\firewall-rules.wfw"



Ikdienas sarežģījumi

- Operētājsistēma, lietotnes, programmatūra izveido savus nosacījumus
  - Pārāk plaši atvērts (visi protokoli, porti, apakštīkli)
  - Dublikāti
  - Zudusi kontrole, pārskatāmība



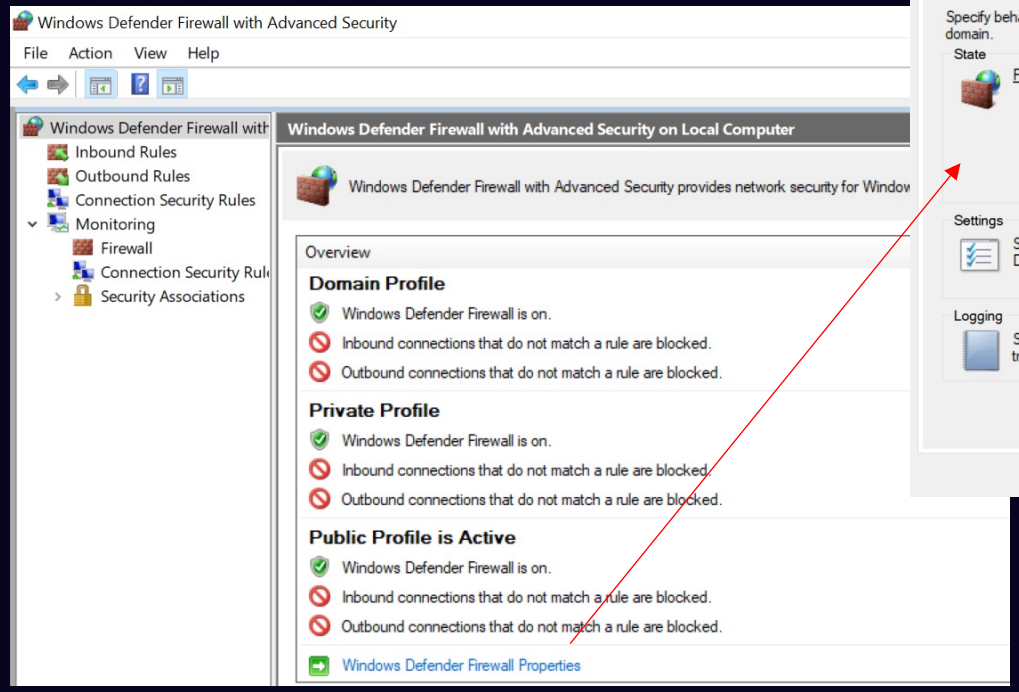


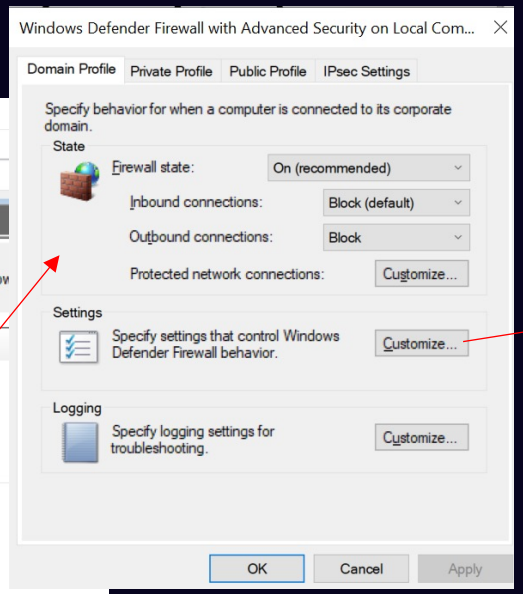
Ikdienas sarežģījumu risinājumi

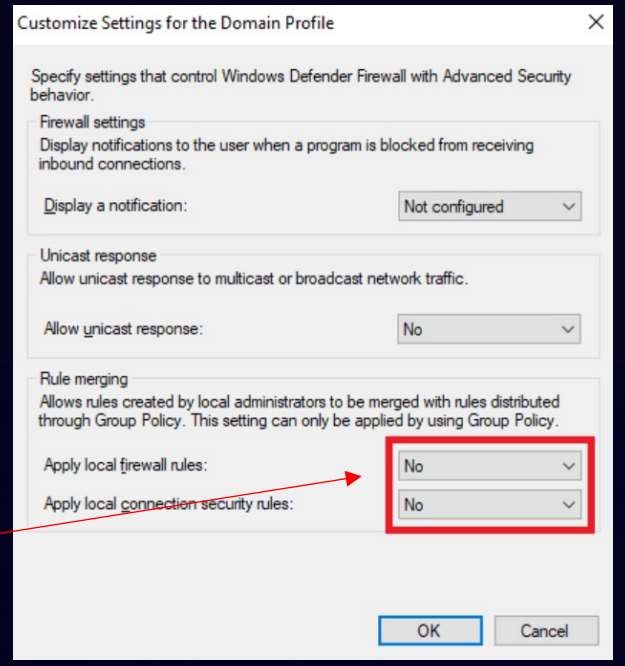
- Problēma: patvaļīgi izveidoti nosacījumi
  Objekts: Nepārvaldīts (privāts) dators
- Risinājums #1: uzdevumu pārvaldnieks (Scheduled Task), kas pēc grafika importē WFW konfigurācijas failu.
- Risinājums #2: reģistrā liegums mainīt ugunsmūri (nerekomendēts)

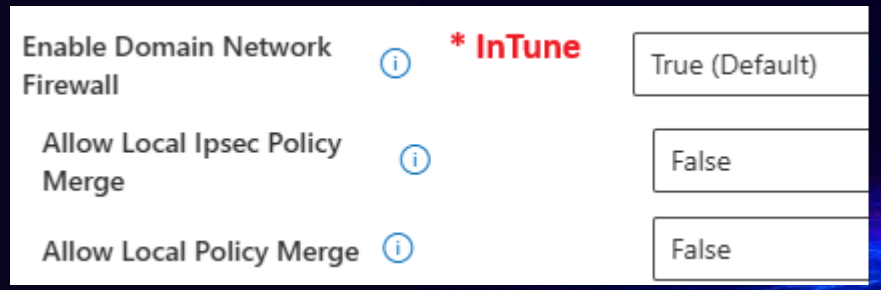
Ikdienas sarežģījumu risinājumi

- Objekts: gan pārvaldīts, gan privāts dators
- Ideālais risinājums #3: AD grupu politika (! Testēt !) (lokāli gpedit.msc)









Tehnisks padoms

- Ugunsmūra iestatījumi stājas spēkā uzreiz un nekavējoties
- Rezerves plāns B: komanda ar aizturi vai uzdevumu pārvaldnieks

#1:

```
Start-Sleep -Minutes 15
netsh advfirewall import "C:\temp\firewall-rules.wfw"
```

#2:

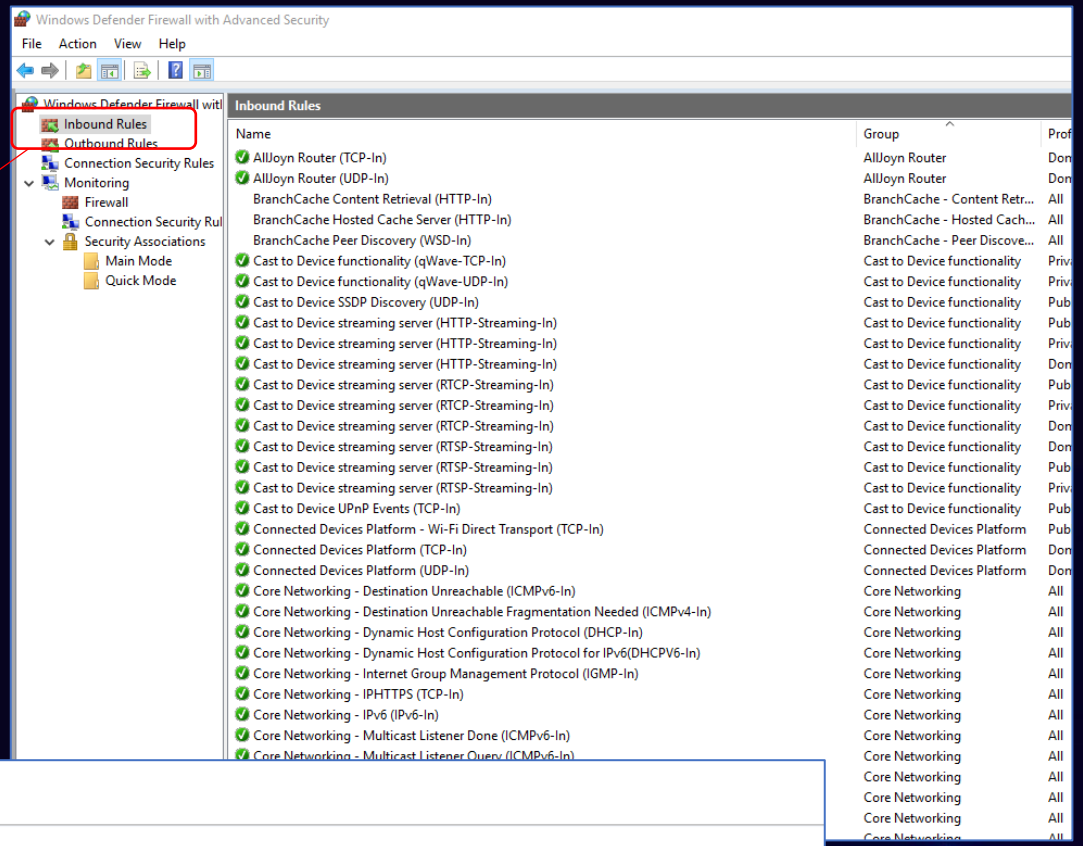
```
Start-Job -ScriptBlock {
Start-Sleep -Minutes 15
netsh advfirewall import "C:\temp\firewall-rules.wfw"  }
```

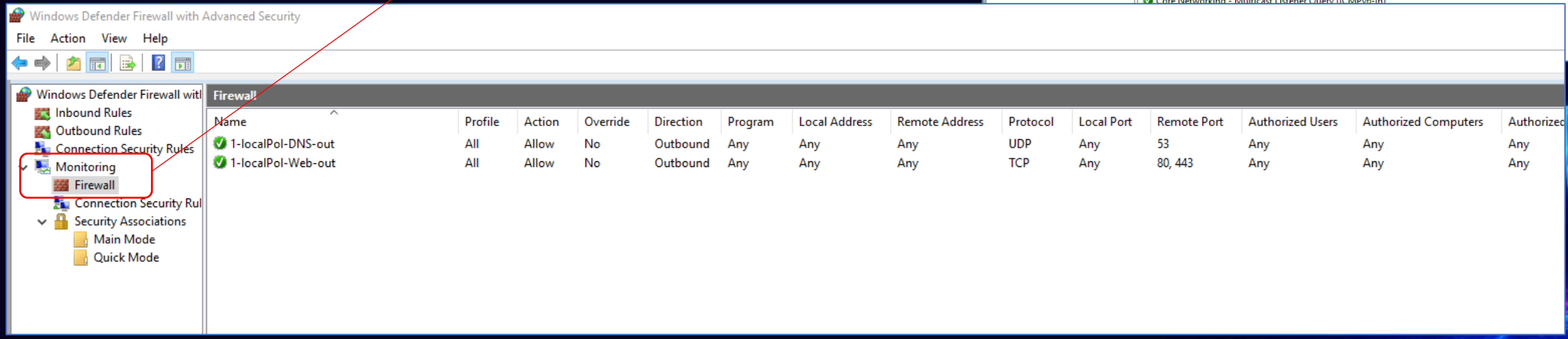
#3:

```
$time = (Get-Date).AddMinutes(15)
schtasks /Create /SC ONCE /TN "FirewallRollback" /TR "netsh advfirewall import C:\temp\firewall-rules.wfw" /ST $time.ToString("HH:mm") /F
```

Tehnisks padoms

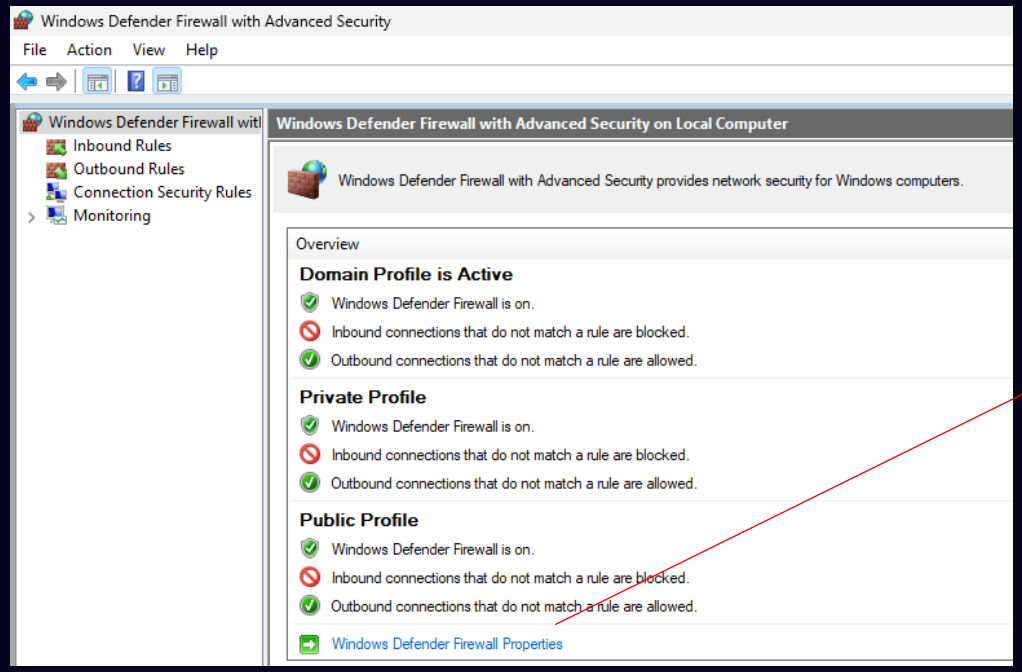
- Precīzai, aktuālai informācijai lietojiet "Monitoring" (īpaši, izmantojot AD, GPO)

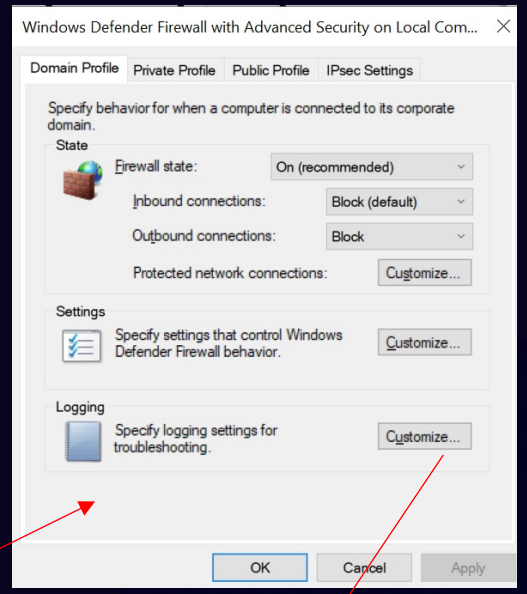


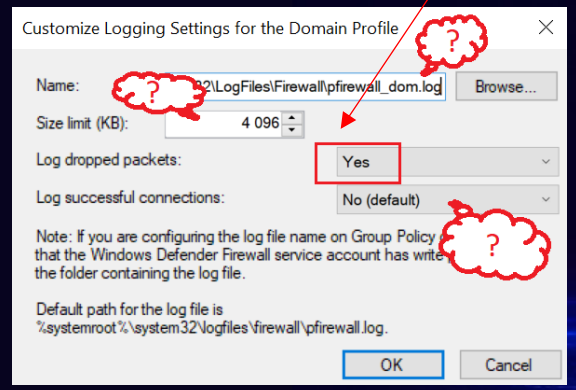


Žurnālfaili

- Ieslēgt atteiktos, bloķētos tīkla savienojumus
- Faila izmērs, nosaukums – pēc vajadzības
- Sekmīgi izveidotie savienojumi – pēc vajadzības

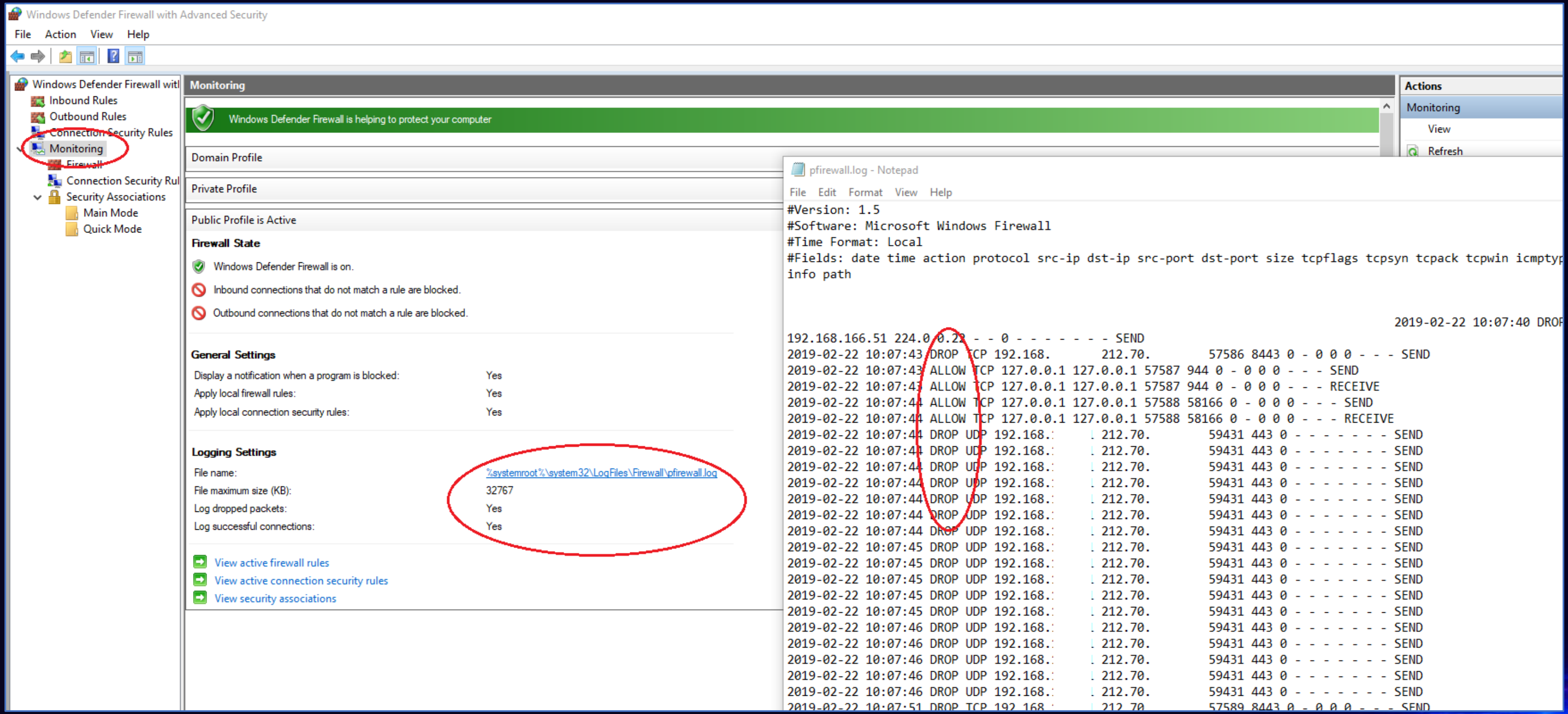






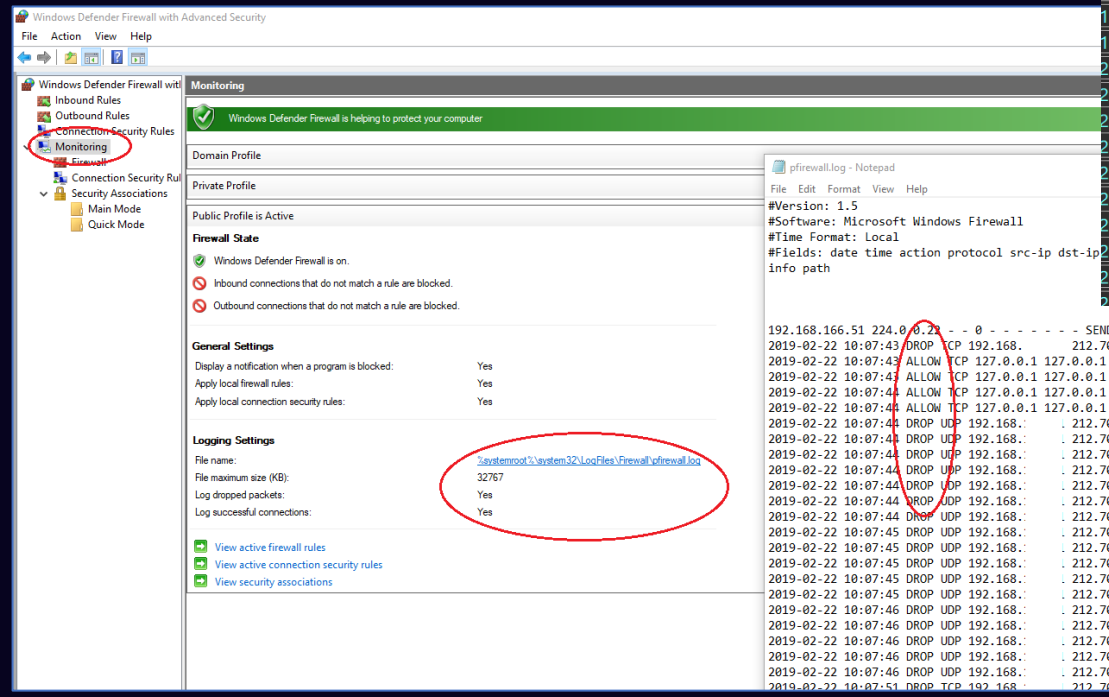
Žurnālfaili

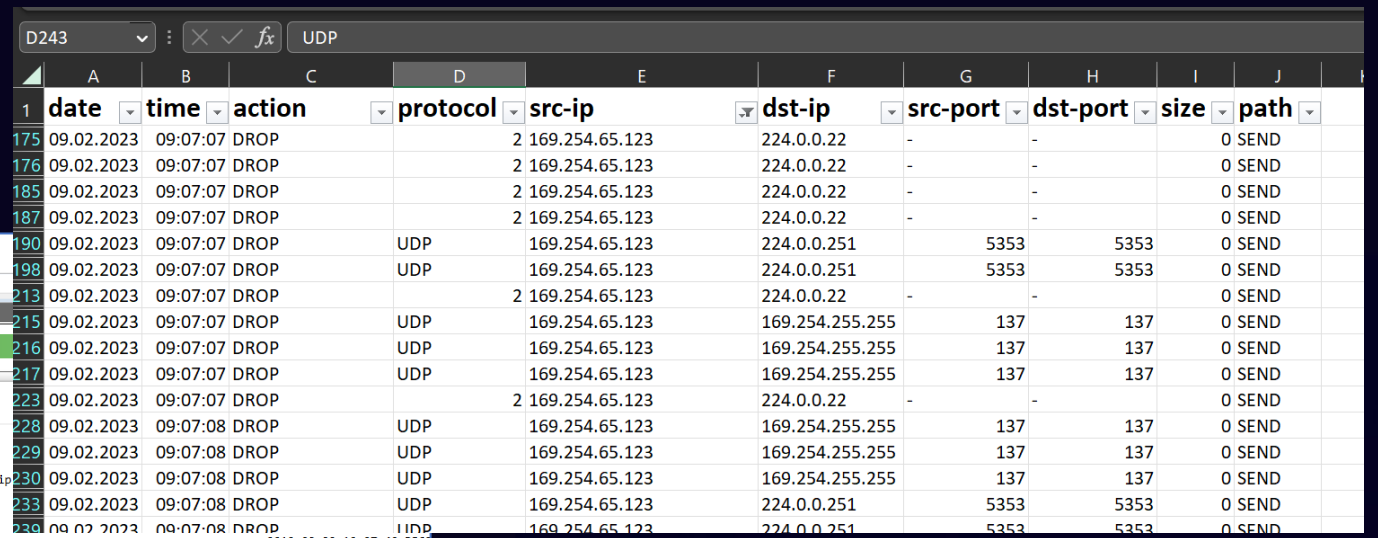
- Ātrā pārskatīšana



Žurnālfaili

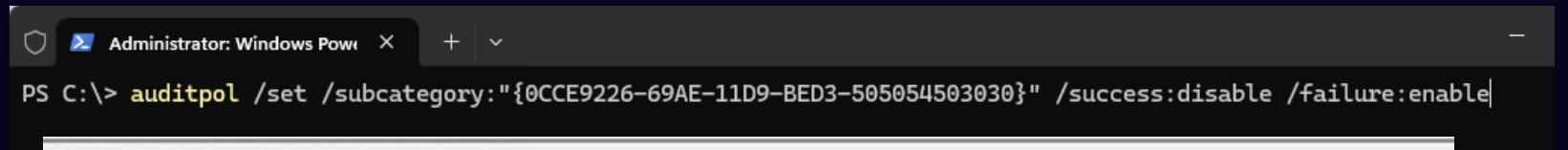
- Detalizētākas analīzes piemērs

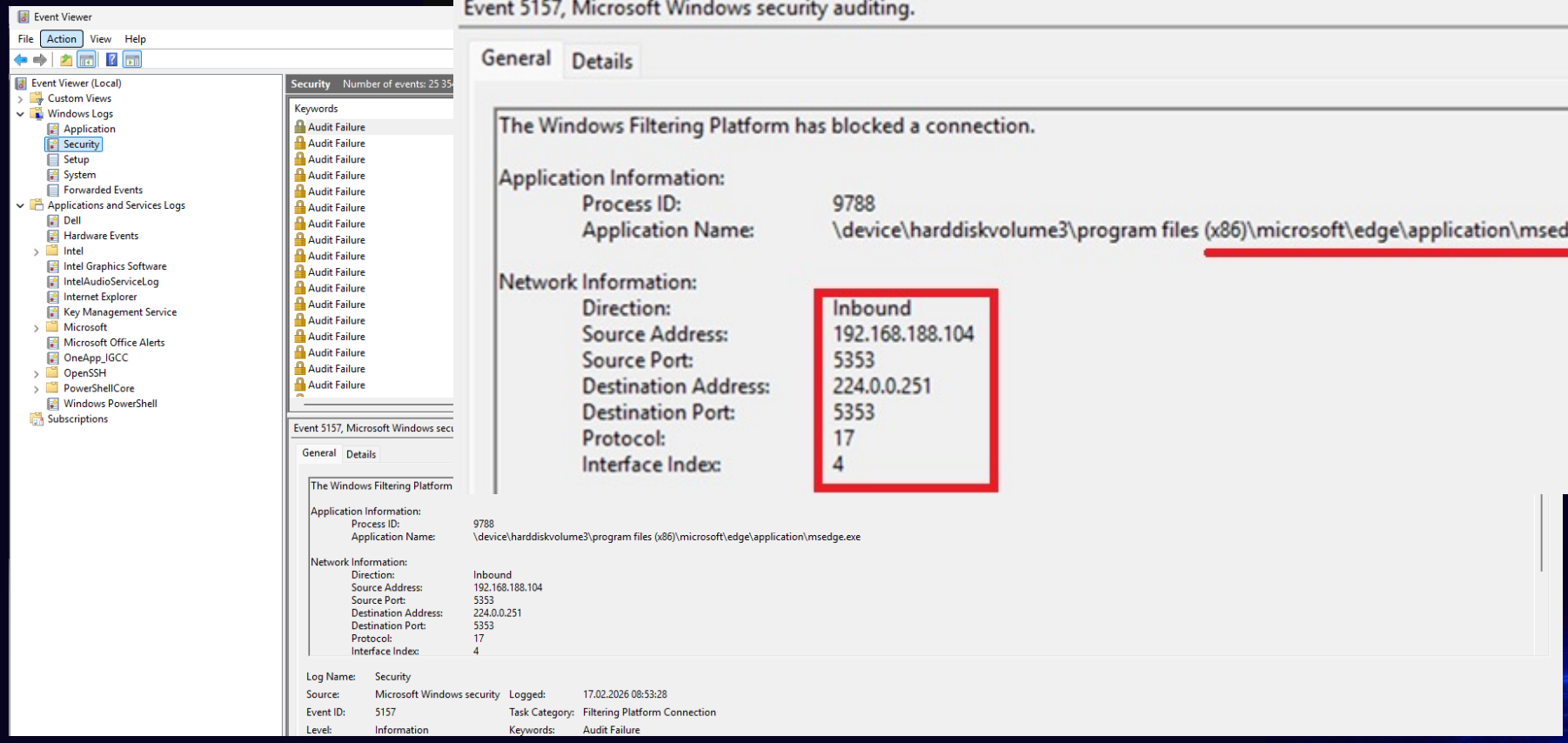




Žurnālfaili – Windows (Event Log)

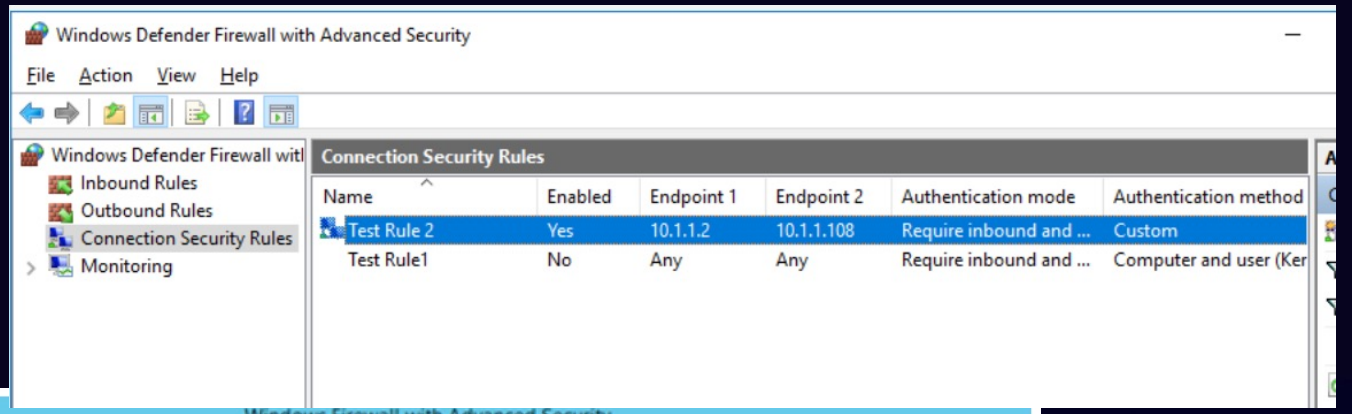
- Ērti atrast bloķēto izpildfailu (exe)
- auditpol /set /subcategory:"{0CCE9226-69AE-11D9-BED3-505054503030}" /success:disable /failure:enable

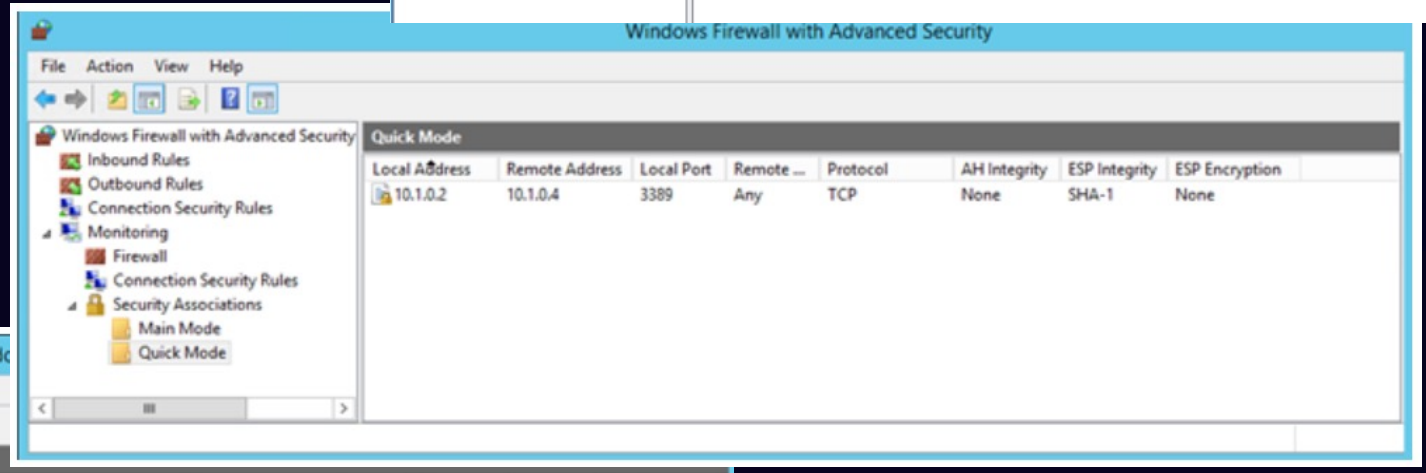


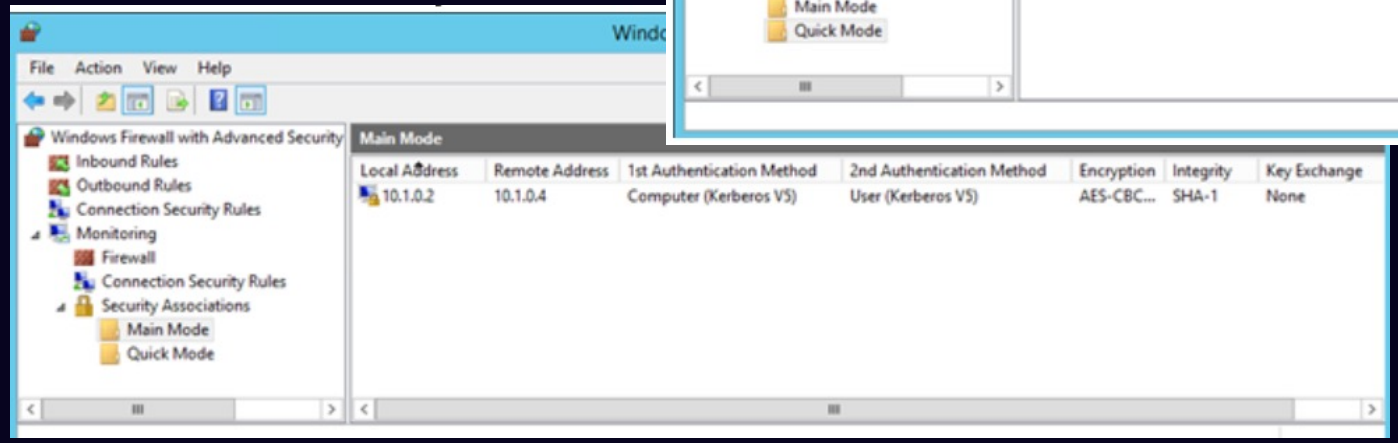


Drošie nosacījumi (IPSEC)

- IPSEC jebkuram savienojumam
- Autentifikācija x2 pirms savienojuma
- Izcils veids drošības uzlabošanai
- Tēma atsevišķam seminārам
- Rūpīga testēšana!
- "Pro" līmenis!

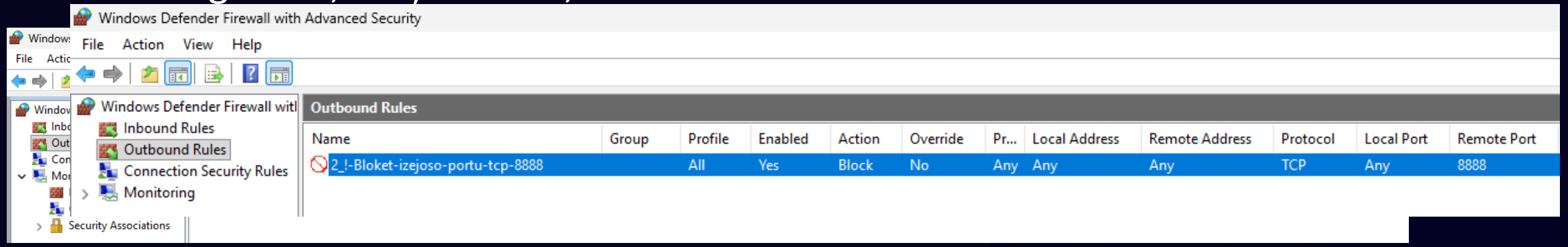




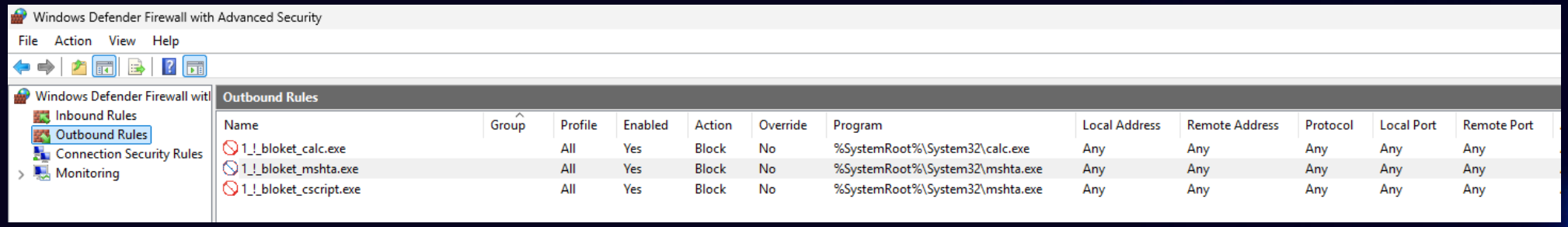


Tehnisks padoms

- Ātrā reaģēšana, bloķēt sekas, kamēr meklē cēloni



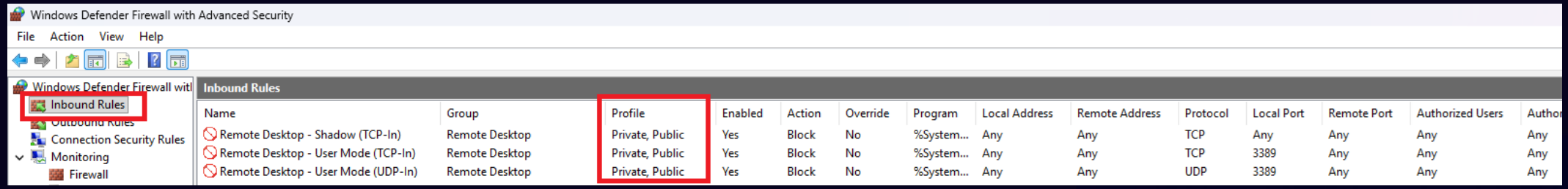
- Solis tālāk, bloķēt izpildfailus (exe), kam nav paredzēta pieeja tīmeklim



- powershell.exe; pwsh.exe; cmd.exe; wscript.exe; cscript.exe; mshta.exe; rundll32.exe; regsvr32.exe; installutil.exe; msbuild.exe; csc.exe; wmic.exe u.c.
- TESTĒT!

Tehnisks padoms

- Publiskā profilā bloķēt ienākošos attālinātās kontroli (rdp)
- Pārvaldības portus (WinRM)



- Testēt!

- Info. Jaunums, ugunsmūris atbalsta domēna vārdus:
  https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/dynamic-keywords#fqdn-feature-requirements

Tehnisks padoms

- Ideālais mērķis (rezultātu var sasniegt dažādos veidos)

- Atļaut tikai nepieciešamos ienākošos portus
- Publiskiem profiliem papildus liegumi
- Atļaut tikai nepieciešamos izejošos portus
- Saziņa ar serveri (AD, FS u.c.), bloķēt saziņu ar blakus iekārtām
- Pārbaudīt, testēt, izmēģināt!

- Drošie nosacījumi (conn.security rules) labākai pārvaldībai
- Drošie nosacījumi atsevišķiem datoriem un lietotājiem

Tehnisks padoms

- Biežāk uzdotie jautājumi

1. Kad GPO nosacījumi tiek apvienoti ar lokālajiem, kuriem priekšroka?
   Atbilde: spēkā favorītu sistēma, GPO papildina nosacījumus
2. Kā vairākas GPO rezultējas ugunsmūra nosacījumos?
   Atbilde: nosacījumu pulks papildinās, ieteicams neveidot daudz gpo
3. Vai ir "established, related" nosacījumi?
   Atbilde: nav
4. Trešo pušu alternatīvie risinājumi?
   Atbilde: jā, bet jāņem vērā:
   - bieži fonā darbojas tas pats Win.ugunsmūris
   - ir atkarība no specifiska produkta pārvaldības veida un tehniskā atbalsta
   - Win.ugunsmūrim ir plaša zināšanu bāze, komūna, pārvaldība integrēta OS ietvaros

Mīti un patiesība

1. Dators ir pasargāts korporatīvā vidē aiz iestādes ugunsmūra, mājās netiek nests
   Atb.: arī organizācijā gala iekārtām jābūt ugunsmūrim, korp. risinājumi tiek kompromitēti, visu aizsardzību nebalstīt uz vienu risinājumu
2. Windows Defender pasargā kā ugunsmūris
   Atb.: Defender ir aizsardzības komplekss ar dažādām komponentēm, ugunsmūris ir tā būtiska un neatņemama sastāvdaļa, kura jākonfigurē
3. Uzstādīts VPN
   Atb.: VPN nav ugunsmūris, ugunsmūri nedrīkst aizstāt ar citas funkcijas pildošām alternatīvām
4. Antivīrusa programmatūra pasargā kā ugunsmūris
   Atb.: AV ir cita misija un uzdevumi, tā nevar aizvietot ugunsmūri
5. Tīmekļa piekļuve un bērni…
   Atb.: rotaļām – rotaļu laukumi, izglītībai – skolas
6. Datoram atļauta piekļuve lokālajam tīklam, ieslēgt nav obligāti
   Atb.: uzbrucēji atrod veidus, kā pārvietoties starp datoriem (kādai iekārta būs pieeja tīmeklim), ugunsmūris ir liels šķērslis vai bieži kā pēdējā aizsardzības līnija

CERT.LV

Paldies!