

# CERT.LV vebinārs

## "Efektīva Windows ugunsmūra pārvaldība"

---

**Kristīne Kaula**, CERT.LV Drošības operāciju centra vadītāja

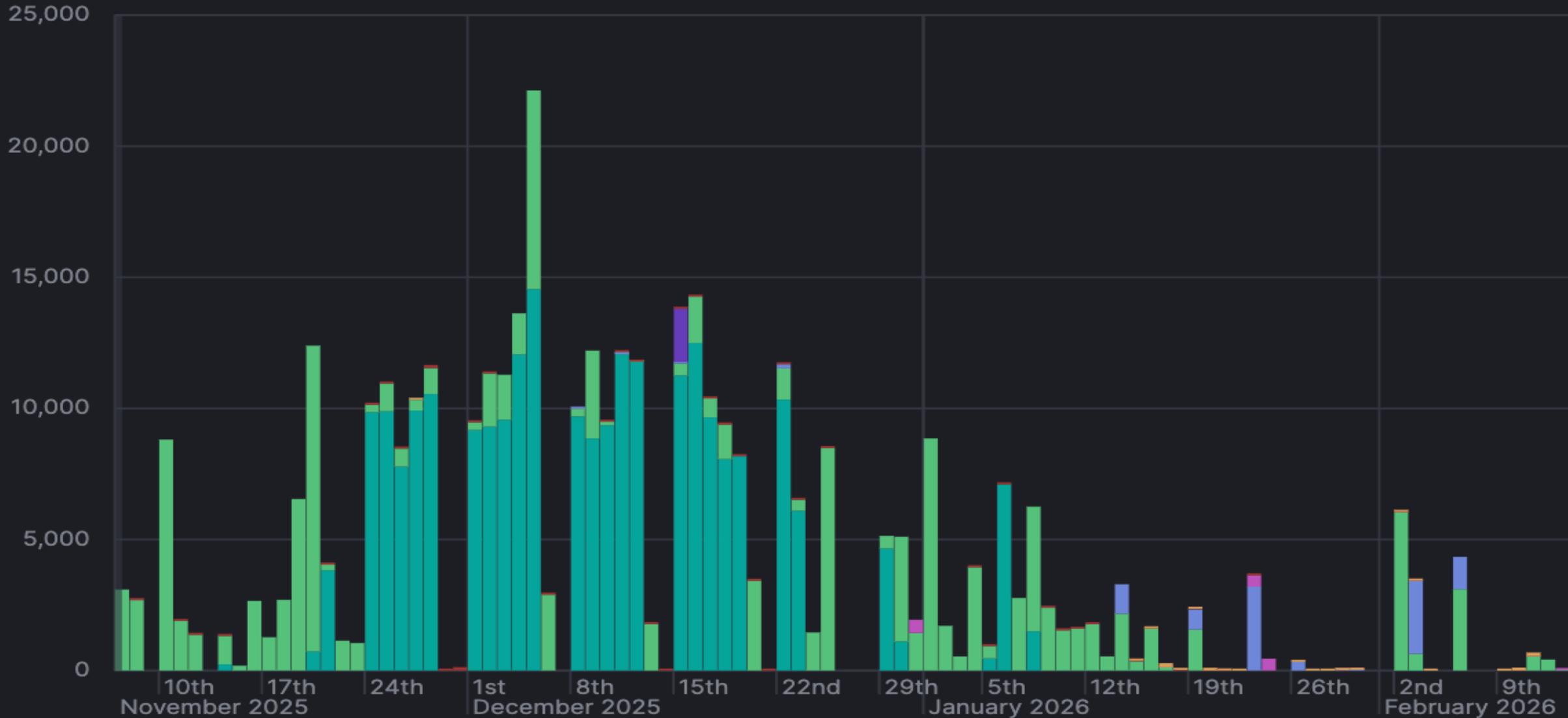
**Andris Medjānis**, CERT.LV kiberdrošības eksperts

**17.02.2026**





# Bruteforce from an External IP



# Mīti un patiesība

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

Windows Defender pasargā kā uguns mūris;

Uzstādīts VPN;

Antivīrusa programmatūra pasargā kā uguns mūris.

Internet piekļuve un bērni...

Konfigurācijas nianšes

Atļauta piekļuve LAN, nav ieslēgts obligāti

Konfigurācijas nianšes



# Tvērums

- Auditorijas priekšzināšanas: tīkli un pārvaldība – konceptuāli, Win. uguns mūris 0-10
- Fokusā Windows Uguns mūris
- 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**

**Inbound Rules**

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Authorized Computers	Authorized Local Policies
@(Microsoft.DesktopAppInstaller_12643...	@(Microsoft.DesktopAppInsta...	Domain...	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	Any
@(Microsoft.SecHealthUI_1000.27840.100...	@(Microsoft.SecHealthUI_1000.27840.100...	Domain...	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	Any
@(Microsoft.StorePurchaseApp_22507.144...	@(Microsoft.StorePurchaseA...	Domain...	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	Any
@(Microsoft.Windows.LKG.DesktopSpott...	@(Microsoft.Windows.LKG.D...	Domain...	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	Any
Alloyn Router (TCP-In)	Alloyn Router	Domain...	Yes	Allow	No	%System...	Any	Any	TCP	9955	Any	Any	Any	Any
Alloyn Router (UDP-In)	Alloyn Router	Domain...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any	Any	Any
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Ret...	All	No	Allow	No	SYSTEM	Any	Any	TCP	80	Any	Any	Any	Any
BranchCache Hosted Cache Server (HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP	80, 443	Any	Any	Any	Any
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discov...	All	No	Allow	No	%System...	Any	Local subnet	UDP	3702	Any	Any	Any	Any
Cast to Device functionality (Wave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	2177	Any	Any	Any	Any
Cast to Device functionality (Wave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	2177	Any	Any	Any	Any
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Dis...	UDP	Any	Any	Any	Any	Any
Cast to Device streaming server (HTTP-SL...	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayTo Renderers	TCP	10246	Any	Any	Any	Any
Cast to Device streaming server (HTTP-SL...	Cast to Device functionality	Private	Yes	Allow	No	System	Any	Local subnet	TCP	10246	Any	Any	Any	Any
Cast to Device streaming server (RTSP-SL...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	TCP	10246	Any	Any	Any	Any
Cast to Device streaming server (RTSP-SL...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	Any	Any	Any	Any	Any
Cast to Device streaming server (RTCP-S-Str...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP	Any	Any	Any	Any	Any
Cast to Device streaming server (RTCP-S-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any	Any	Any
Cast to Device streaming server (RTSP-S-Str...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	TCP	23554, 235...	Any	Any	Any	Any
Cast to Device streaming server (RTSP-S-Str...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	23554, 235...	Any	Any	Any	Any
Cast to Device UPnP Events (TCP-In)	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayTo Renderers	TCP	2869	Any	Any	Any	Any
Connected Devices Platform - WiFi Direc...	Connected Devices Platform	Public	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any	Any	Any	Any
Connected Devices Platform (TCP-In)	Connected Devices Platform	Domain...	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any	Any	Any	Any
Connected Devices Platform (UDP-In)	Connected Devices Platform	Domain...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any	Any	Any
Core Networking - Destination Unreachab...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any	Any
Core Networking - Destination Unreachab...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv4	Any	Any	Any	Any	Any
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	68, 67	Any	Any	Any	Any
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	546, 547	Any	Any	Any	Any
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP	Any	Any	Any	Any	Any
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	TCP	IPHTTPS	Any	Any	Any	Any
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPv6	Any	Any	Any	Any	Any
Core Networking - Multicast Listener Dis...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any	Any	Any
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any	Any	Any
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any	Any	Any
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any	Any	Any
Core Networking - Neighbour Discovery ...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any	Any
Core Networking - Neighbour Discovery ...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any	Any
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any	Any
Core Networking - Parameter Problem (L...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any	Any
Core Networking - Router Advertisement...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any	Any
Core Networking - Router Advertisement...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any	Any
Core Networking - Router Solicitation (I...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any	Any
Core Networking - Teledo (UDP-In)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	Edge Trave...	Any	Any	Any	Any
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any	Any
Core Networking Diagnostics - ICMP Ech...	Core Networking Diagnostics	Private...	No	Allow	No	System	Any	Local subnet	ICMPv4	Any	Any	Any	Any	Any
Core Networking Diagnostics - ICMP Ech...	Core Networking Diagnostics	Domain	No	Allow	No	System	Any	Any	ICMPv4	Any	Any	Any	Any	Any
Core Networking Diagnostics - ICMP Ech...	Core Networking Diagnostics	Private...	No	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any	Any	Any
Core Networking Diagnostics - ICMP Ech...	Core Networking Diagnostics	Domain	No	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any	Any
Cortex XDR Service P2P TCP In	Palo Alto Networks, Inc. Cor...	All	Yes	Allow	No	C:\Progr...	Any	Any	TCP	33200-33300	Any	Any	Any	Any
Cortex XDR Service P2P UDP In	Palo Alto Networks, Inc. Cor...	All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	33200-33300	Any	Any	Any	Any
Delivery Optimization (TCP-In)	Delivery Optimization	All	Yes	Allow	No	%System...	Any	Any	TCP	7800	Any	Any	Any	Any
Delivery Optimization (UDP-In)	Delivery Optimization	All	Yes	Allow	No	%System...	Any	Any	UDP	7800	Any	Any	Any	Any
Desktop App Web Viewer	Desktop App Web Viewer	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	Any
Desktop App Web Viewer	Desktop App Web Viewer	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	Any
Desktop App Web Viewer	Desktop App Web Viewer	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	Any
DIAL protocol server (HTTP-In)	DIAL protocol server	Domain	Yes	Allow	No	System	Any	Any	TCP	10247	Any	Any	Any	Any
DIAL protocol server (HTTP-In)	DIAL protocol server	Private	Yes	Allow	No	System	Any	Local subnet	TCP	10247	Any	Any	Any	Any
Distributed Transaction Co-ordinator (RPC)	Distributed Transaction Co-...	Domain	No	Allow	No	%System...	Any	Any	TCP	RPC Dyna...	Any	Any	Any	Any
Distributed Transaction Co-ordinator (RPC)	Distributed Transaction Co-...	Private...	No	Allow	No	%System...	Any	Local subnet	TCP	RPC Dyna...	Any	Any	Any	Any
Distributed Transaction Co-ordinator (RP...	Distributed Transaction Co-...	Private...	No	Allow	No	%System...	Any	Local subnet	TCP	RPC Endp...	Any	Any	Any	Any
Distributed Transaction Co-ordinator (RP...	Distributed Transaction Co-...	Domain	No	Allow	No	%System...	Any	Any	TCP	RPC Endp...	Any	Any	Any	Any
Distributed Transaction Co-ordinator (TC...	Distributed Transaction Co-...	Domain	No	Allow	No	%System...	Any	Any	TCP	Any	Any	Any	Any	Any
Distributed Transaction Co-ordinator (TC...	Distributed Transaction Co-...	Private...	No	Allow	No	%System...	Any	Local subnet	TCP	Any	Any	Any	Any	Any
Feedback Hub	Feedback Hub	Domain...	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	Any

**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 computers**

Create connection security rules to specify how and when connections protected by using Internet Protocol security (IPsec).

[Connection Security Rules](#)

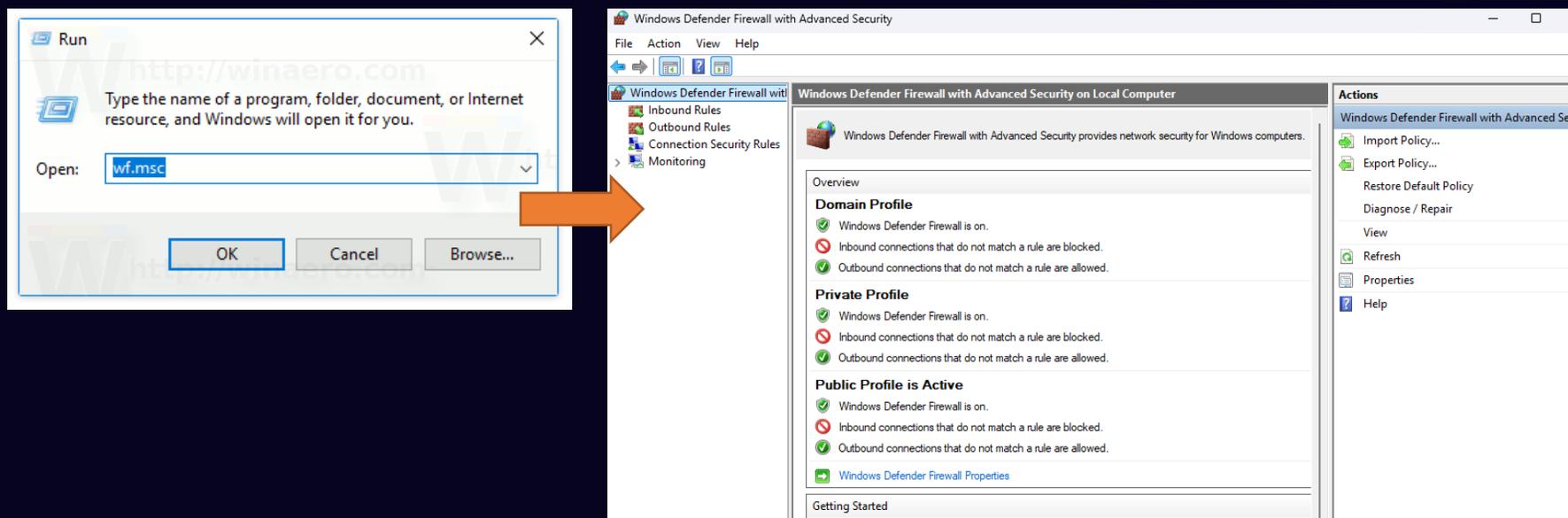
**View and create firewall rules**

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

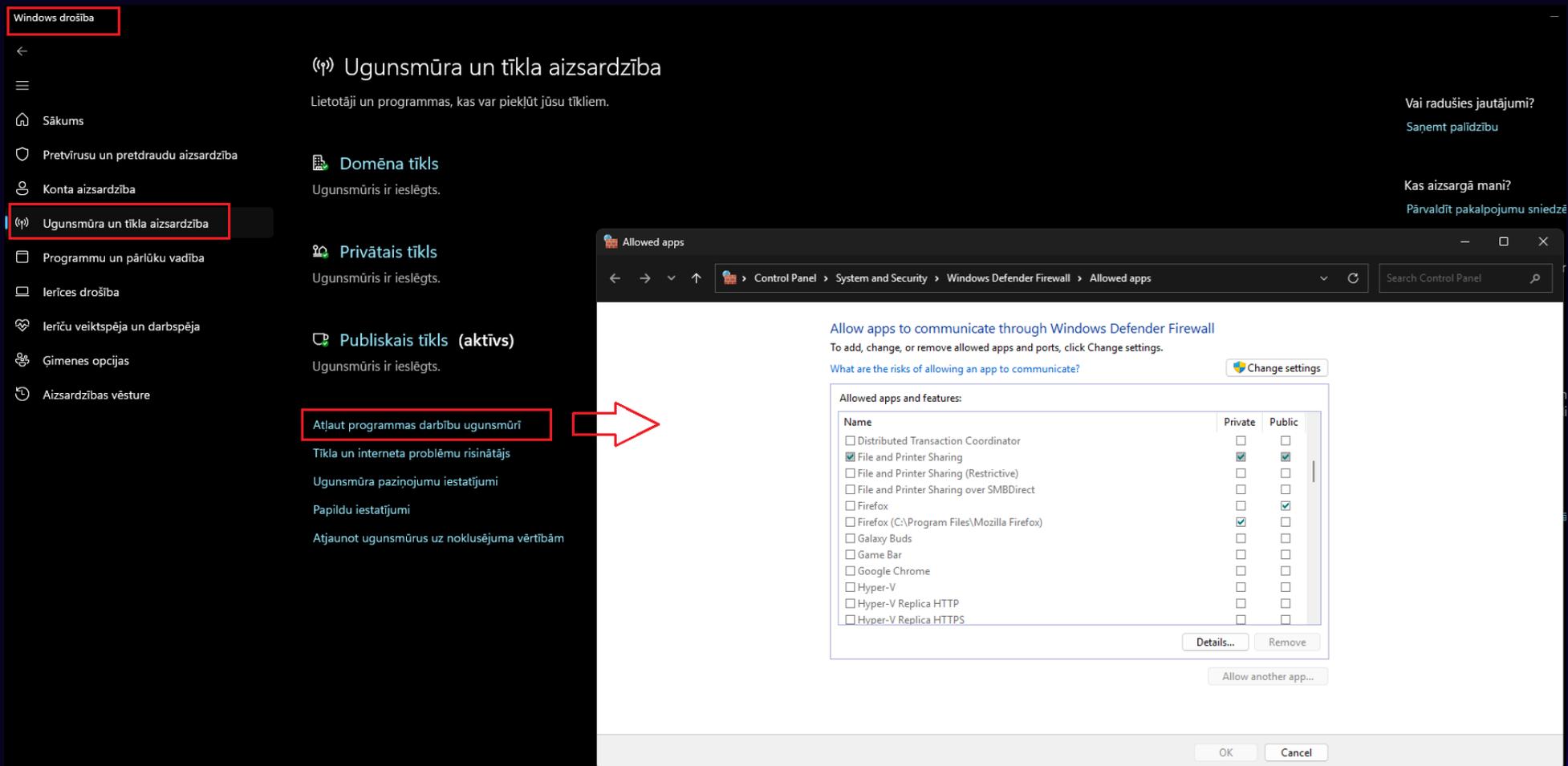


# Lokālā pārvaldība

- wf.msc (grafiskā saskarne)



# Lokālā pārvaldība (no kā izvairīties)



The image shows a Windows Security window with the left sidebar containing several options. Two options are highlighted with red boxes: "Windows drošība" at the top and "Ugunsdzēsība un tīkla aizsardzība" in the middle. A red arrow points from the "Atļaut programmas darbību ugunsdzēsībā" option in the main content area to the "Allowed apps" window.

The "Allowed apps" window is titled "Allowed apps" and shows the path: Control Panel > System and Security > Windows Defender Firewall > Allowed apps. The main heading is "Allow apps to communicate through Windows Defender Firewall". Below this, there is a table of allowed apps and features:

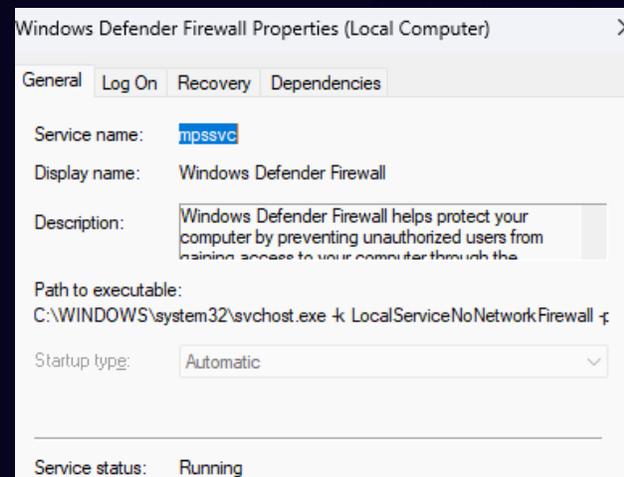
Name	Private	Public
<input type="checkbox"/> Distributed Transaction Coordinator	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> File and Printer Sharing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> File and Printer Sharing (Restrictive)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> File and Printer Sharing over SMBDirect	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Firefox	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Firefox (C:\Program Files\Mozilla Firefox)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Galaxy Buds	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Game Bar	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Google Chrome	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Hyper-V	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Hyper-V Replica HTTP	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Hyper-V Replica HTTPS	<input type="checkbox"/>	<input type="checkbox"/>

At the bottom of the window, there are "OK" and "Cancel" buttons.



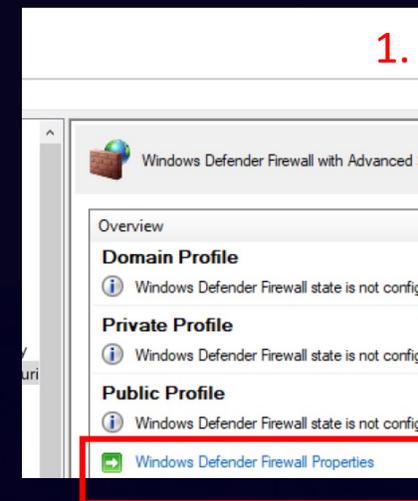
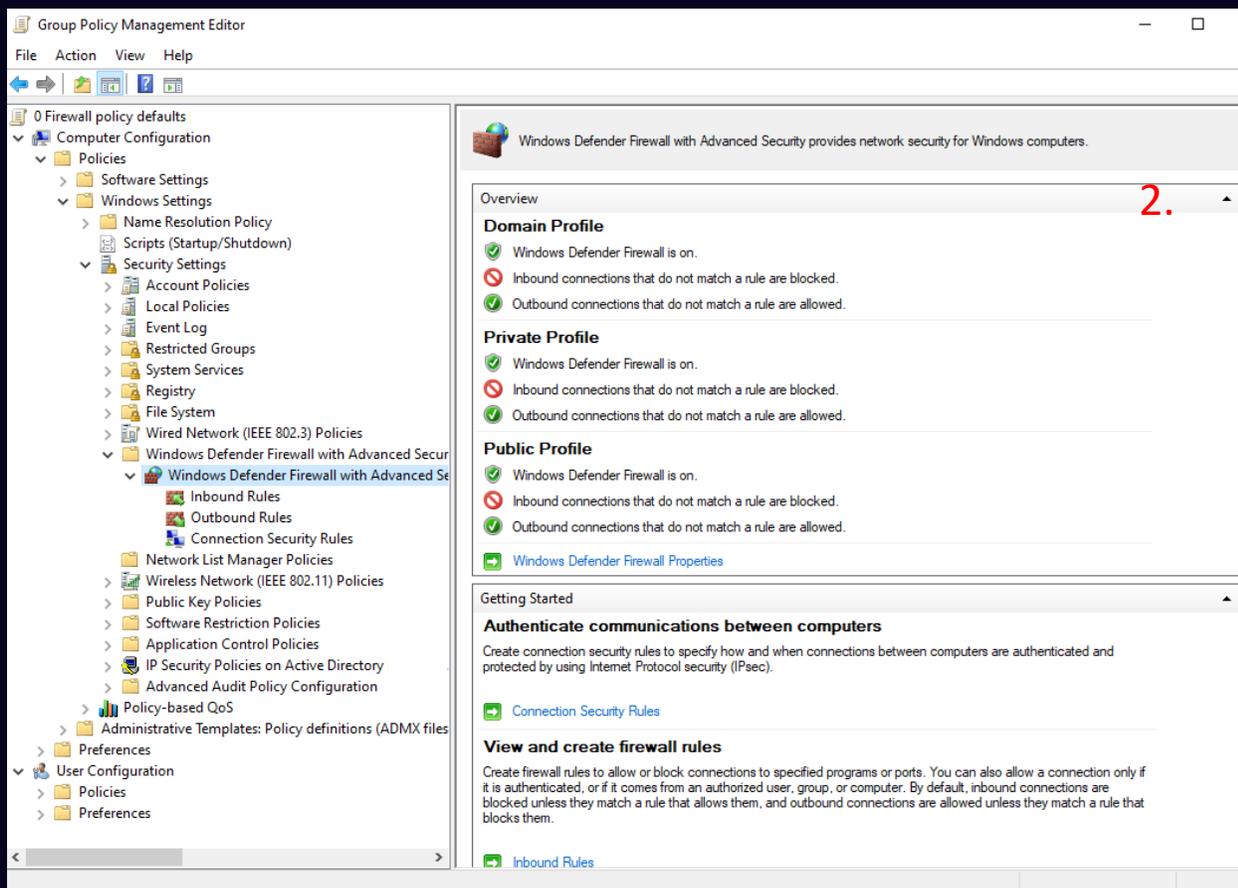
# Lokālā pārvaldība

- (klasiski) Netsh Advfirewall
- (moderni PowerShell) Get-NetFirewallRule
- Informācijai – atbildīgais Win. serviss – Mpssvc  
Windows Defender Firewall  
(Neizslēgt!)



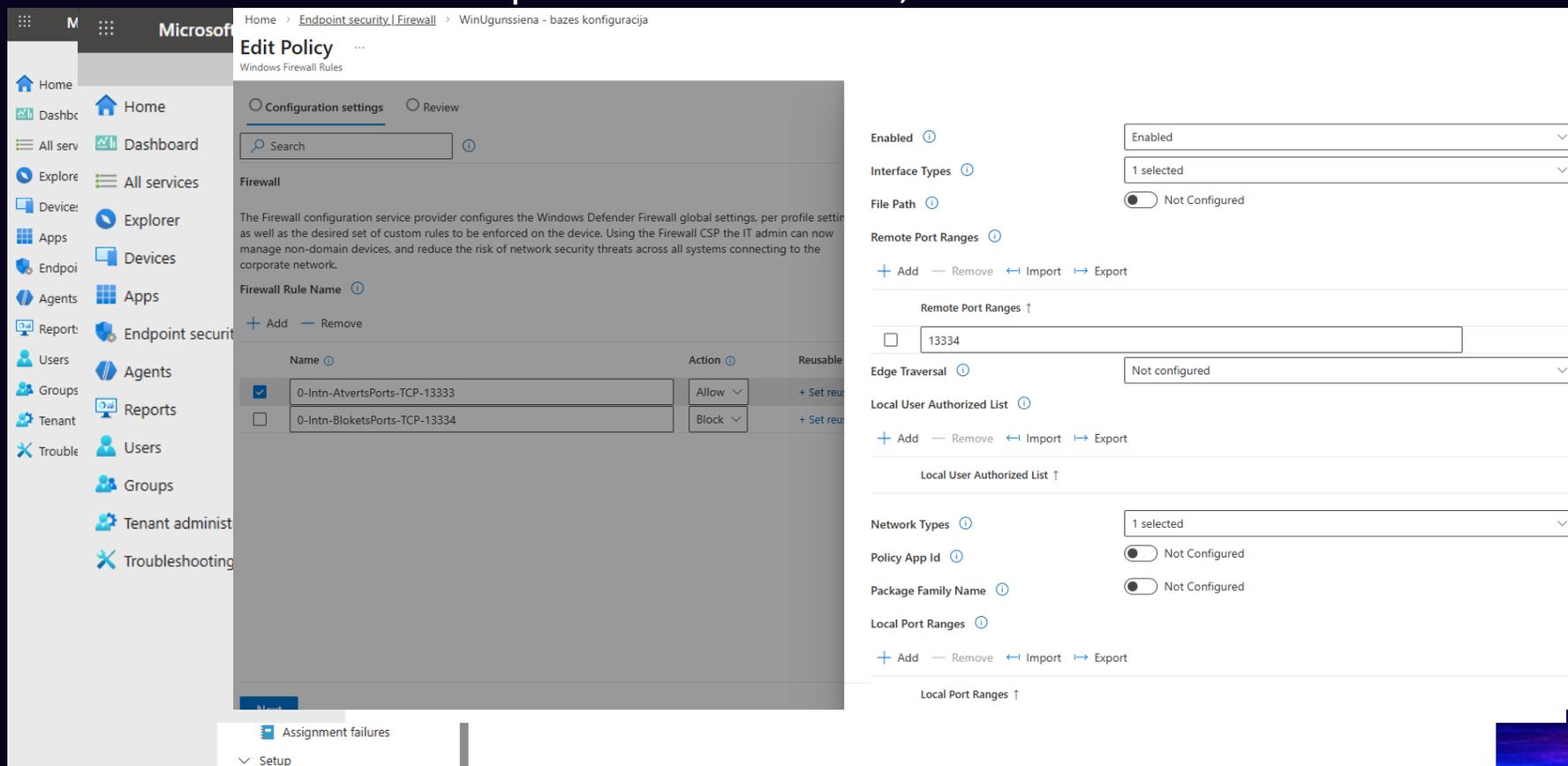
# \*Grupu pārvaldība

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



# \*Grupu pārvaldība

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



The screenshot displays the Windows Firewall configuration interface. On the left, a navigation pane shows the 'Endpoint security' section expanded, with 'Firewall' selected. The main area is titled 'Edit Policy' and shows the 'Configuration settings' tab. A table lists firewall rules:

Name	Action	Reusable
0-Intrn-AtvertsPorts-TCP-13333	Allow	+ Set reusable
0-Intrn-BloketsPorts-TCP-13334	Block	+ Set reusable

On the right, a configuration panel for the selected rule is shown, including settings for 'Enabled' (set to 'Enabled'), 'Interface Types' (1 selected), 'File Path' (Not Configured), 'Remote Port Ranges' (13334), 'Edge Traversal' (Not configured), 'Local User Authorized List', 'Network Types' (1 selected), 'Policy App Id' (Not Configured), and 'Package Family Name' (Not Configured).



# 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

#	Action	Chain	Src. Address	In. Interface	Out. Interface	Bytes	Packets
0	✔ accept	input				254.3 KB	2 928
1	✔ accept	input	192.168.88.0/24			810.5 KB	8 722
2	✘ drop	input				12.5 KB	75
3	▶ Fast Track connection	forward				37.1 MB	253 955
4	✔ accept	forward				37.0 MB	253 166
5	✔ accept	forward	192.168.88.0/24		ether1-gateway	374.6 KB	3 901
6	✘ drop	forward			ether1-gateway	0 B	0
7	✘ drop	forward				21.7 KB	366

Windows Defender Firewall with Advanced Security on Local Computer

Overview

**Domain 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.

**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**

- 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 computers**

Create connection security rules to specify how and when connections between protected by using Internet Protocol security (IPsec).

Connection Security Rules

Windows Defender Firewall with Advanced Security on Local Com... X

Domain Profile Private Profile Public Profile IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

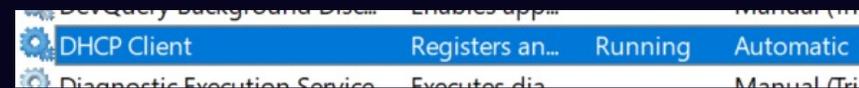
Specify logging settings for troubleshooting. Customize...

OK Cancel Apply



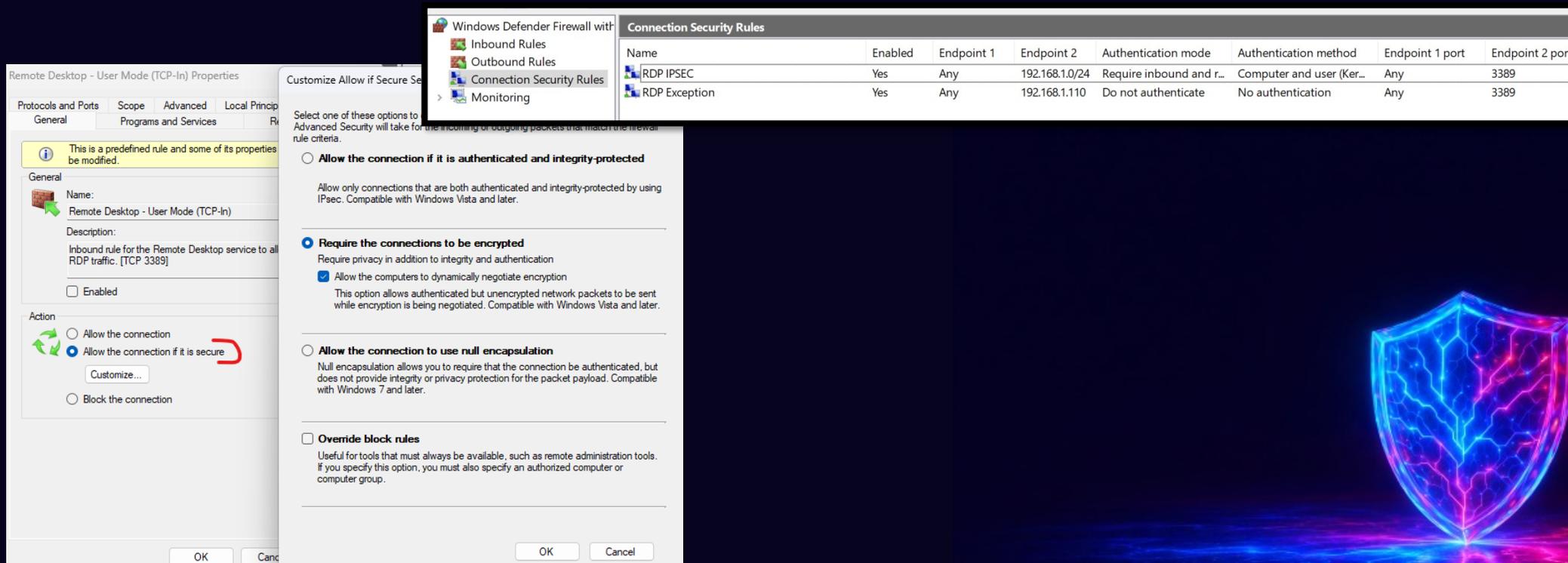
# Darbības pamatprincipi - prioritāte

1. Operētājsistēmas pamatelementi (piem., DHCP klients)



2. "Connection security rules" (IPSEC)

"Allow connection if it is secure" (IPSEC) – nākamais brieduma līmenis



Windows Defender Firewall with Advanced Security - Connection Security Rules

Name	Enabled	Endpoint 1	Endpoint 2	Authentication mode	Authentication method	Endpoint 1 port	Endpoint 2 port
RDP IPSEC	Yes	Any	192.168.1.0/24	Require inbound and r...	Computer and user (Ker...	Any	3389
RDP Exception	Yes	Any	192.168.1.110	Do not authenticate	No authentication	Any	3389

Remote Desktop - User Mode (TCP-In) Properties

General

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

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

Action

Allow the connection

Allow the connection if it is secure

Block the connection

Customize Allow if Secure...

Select one of these options to customize the rule. Advanced Security will take for the incoming or outgoing packets that match the 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.



## 3. Bloķēšana

<input checked="" type="checkbox"/>	0_tcp_web_80-443	All	Yes	Allow	No	Any	Any	Any	Any	Any
<input checked="" type="checkbox"/>	0_VNC-OUT	All	Yes	Block	No	%SystemDrive%\Users\XTR\Downloads\VNC-				
<input checked="" type="checkbox"/>	0_VNC-OUT	All	Yes	Block	No	C:\Users\XTR\Downloads\winbox64-				

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

Name	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> File and Printer Sharing (SMB-In)	Private...	Yes	Allow	No	System	Any	Local subnet	TCP	445	Any
<input checked="" type="checkbox"/> File and Printer Sharing (SMB-In)	All	Yes	Allow	No	System	Any	Any	TCP	445	Any

<input checked="" type="checkbox"/> Remote Desktop - Shadow (TCP-In)	Remote Desktop			All	Yes	Allow	No	%System...	Any	Local subnet,
<input checked="" type="checkbox"/> Remote Desktop - User Mode (TCP-In)	Remote Desktop			All	Yes	Allow	No	%System...	Any	Local subnet,
<input checked="" type="checkbox"/> Remote Desktop - User Mode (UDP-In)	Remote Desktop			All	Yes	Allow	No	%System...	Any	Local subnet,
<input checked="" type="checkbox"/> Remote Desktop - User Mode (TCP-WF-In)	Remote Desktop			All	No	Allow	No	%System...	Any	Local subnet,

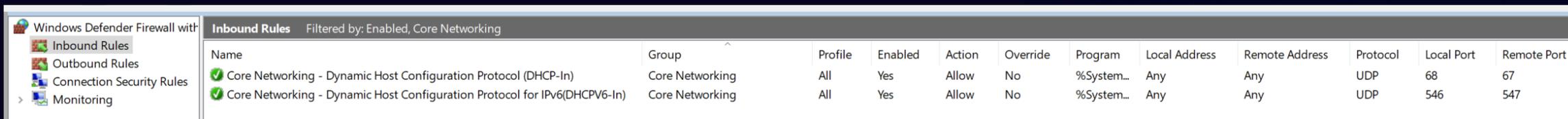
## Rezumējums (oficiāli)

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"



## Realitāte

1. Operētājsistēmas pamatelementi (DHCP klients, DNS klients u.c.)
  - Pilna kontrole, jāizveido visi nosacījumi!



Windows Defender Firewall with Inbound Rules Filtered by: Enabled, Core Networking

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)**



Laiks uzlabojumiem (pirms → pēc)

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security on Local Co...

Inbound Rules Filtered by: Enabled

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
1_tcp123-ntp-time		All	Yes	Allow	No	Any	Any	Any	TCP	Any	123
1_udp123-ntp-time		All	Yes	Allow	No	Any	Any	Any	UDP	Any	123
Core Networking - Dynamic Host Configur...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	68	67
Core Networking - Dynamic Host Configur...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	546	547

Security Associations

- Main Mode
- Quick Mode

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security on Local Co...

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 with Advanced Security

File Action View Help

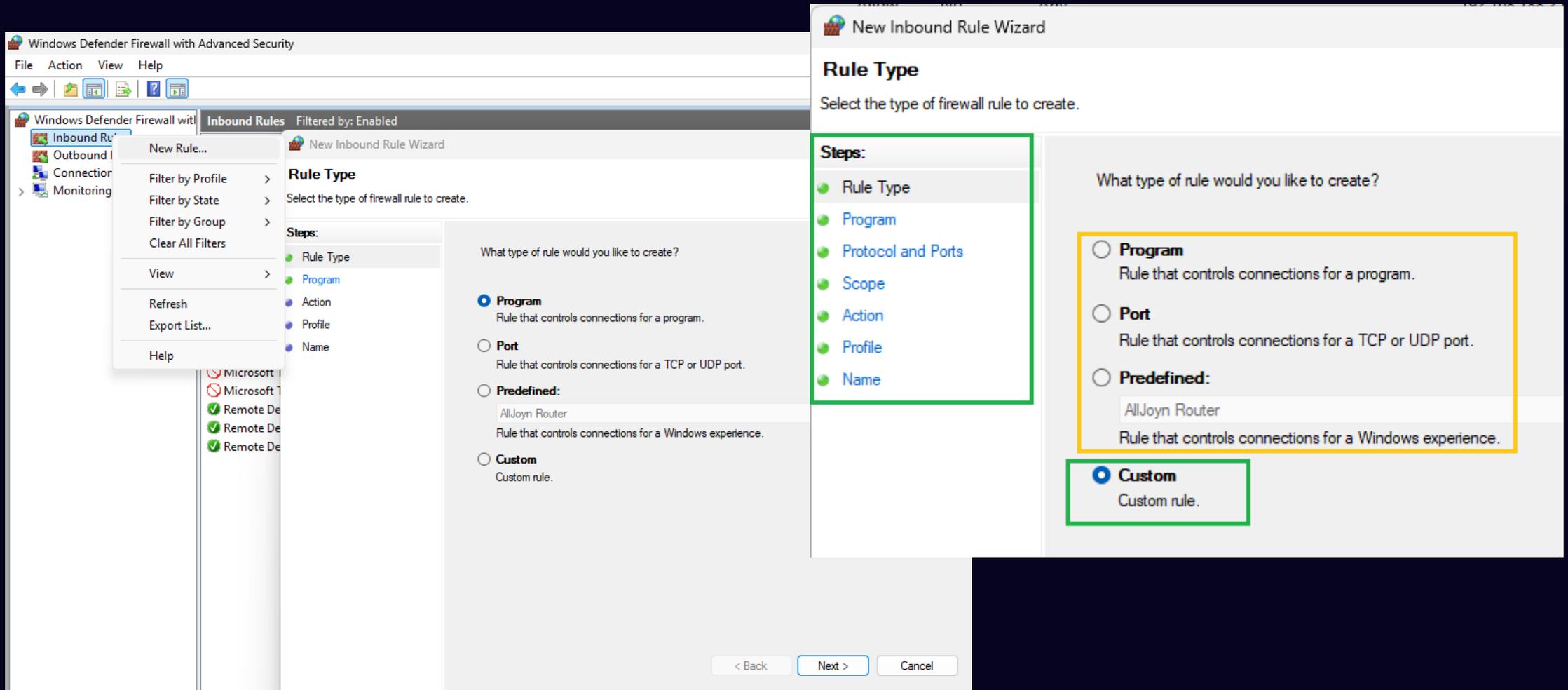
Windows Defender Firewall with Advanced Security on Local Co...

Inbound Rules Filtered by: Enabled, Core Networking

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

\* )

- Nosacījumu izveide



The screenshot displays the Windows Defender Firewall with Advanced Security interface. The 'Inbound Rules' tab is active, and a 'New Inbound Rule Wizard' dialog box is open. The wizard is at the 'Rule Type' step, which asks 'What type of rule would you like to create?'. The 'Program' option is selected. The 'Predefined' section is highlighted with a yellow box, and the 'Custom' option is highlighted with a green box. The 'Steps' list on the left is also highlighted with a green box.

**Rule Type**  
Select the type of firewall rule to create.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What type of rule would you like to create?

**Program**  
Rule that controls connections for a program.

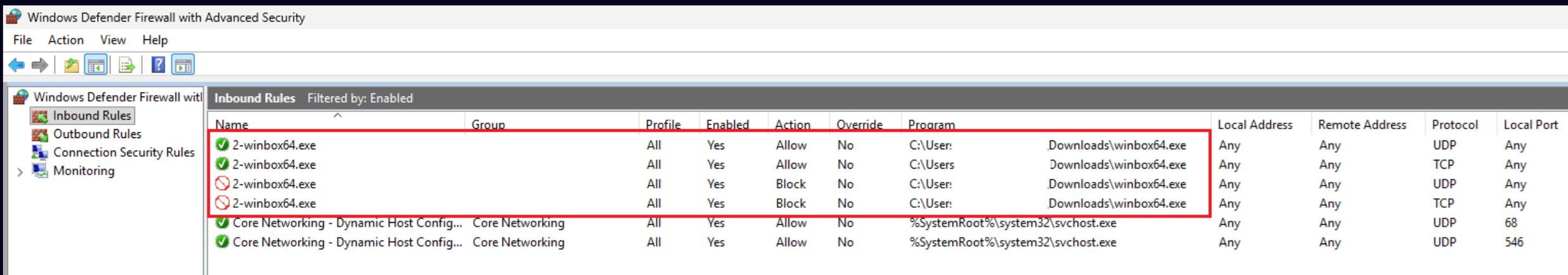
**Port**  
Rule that controls connections for a TCP or UDP port.

**Predefined:**  
AllJoyn Router  
Rule that controls connections for a Windows experience.

**Custom**  
Custom rule.

< Back Next > Cancel

- Ugunsmūrī kontrolēt izpildāmos (exe) failus:



The screenshot shows the Windows Defender Firewall with Advanced Security console. The 'Inbound Rules' tab is selected, and the rules are filtered by 'Enabled'. A red box highlights four rules related to '2-winbox64.exe'. The first two rules are 'Allow' rules, and the last two are 'Block' rules. The 'Program' column shows the path 'C:\Users\...Downloads\winbox64.exe' for the highlighted rules.

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port
2-winbox64.exe		All	Yes	Allow	No	C:\Users\...Downloads\winbox64.exe	Any	Any	UDP	Any
2-winbox64.exe		All	Yes	Allow	No	C:\Users\...Downloads\winbox64.exe	Any	Any	TCP	Any
2-winbox64.exe		All	Yes	Block	No	C:\Users\...Downloads\winbox64.exe	Any	Any	UDP	Any
2-winbox64.exe		All	Yes	Block	No	C:\Users\...Downloads\winbox64.exe	Any	Any	TCP	Any
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%SystemRoot%\system32\svchost.exe	Any	Any	UDP	68
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%SystemRoot%\system32\svchost.exe	Any	Any	UDP	546



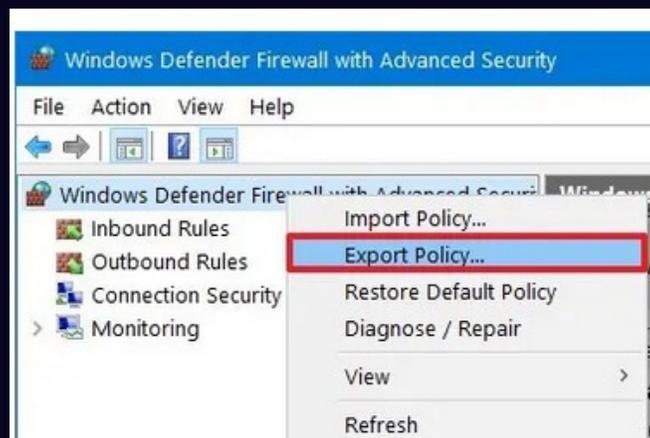
- Ugunsmūra profila saglabāšana (eksports un imports)

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

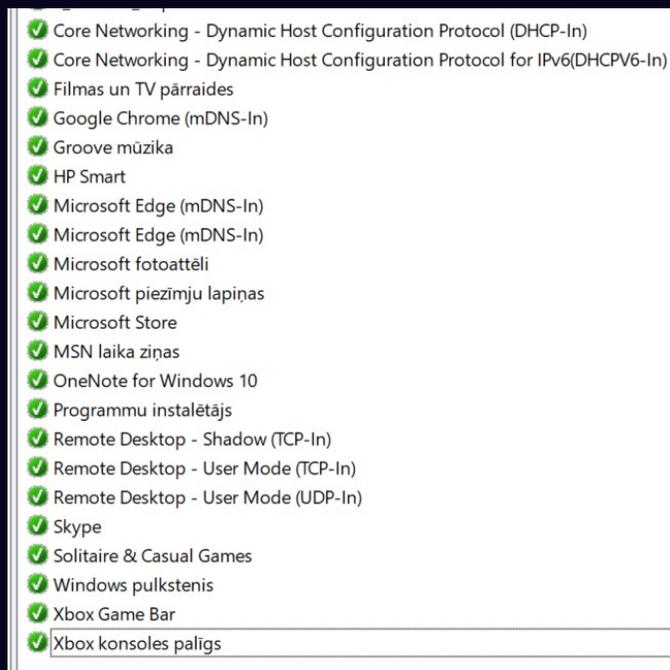
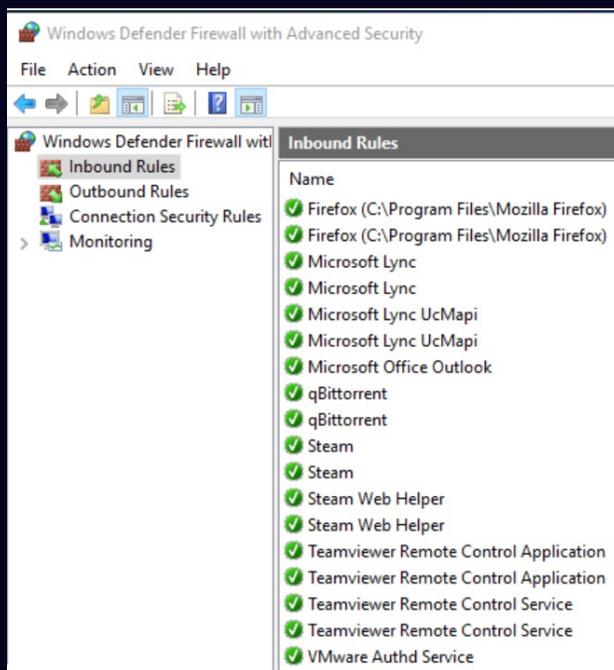
```
netsh advfirewall import "C:\temp\firewall-rules.wfw"
```

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

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



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



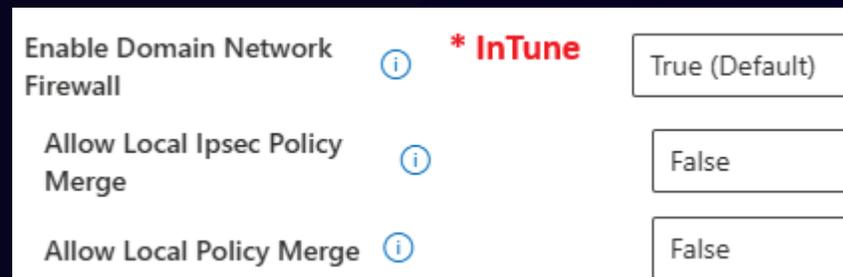
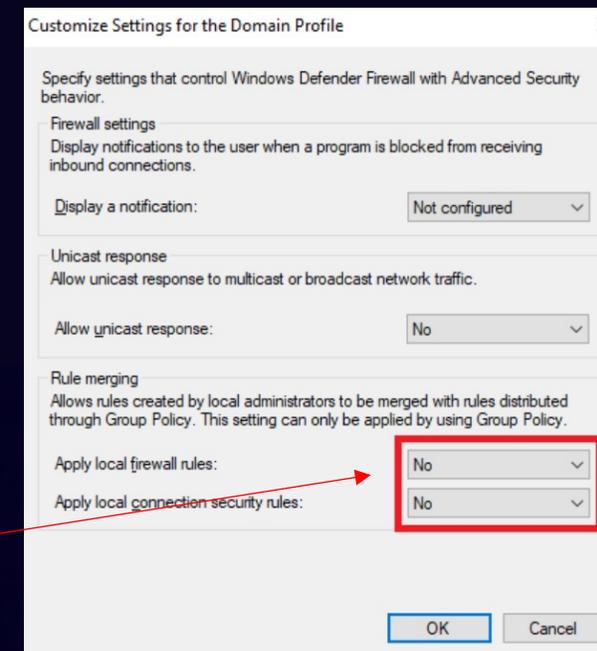
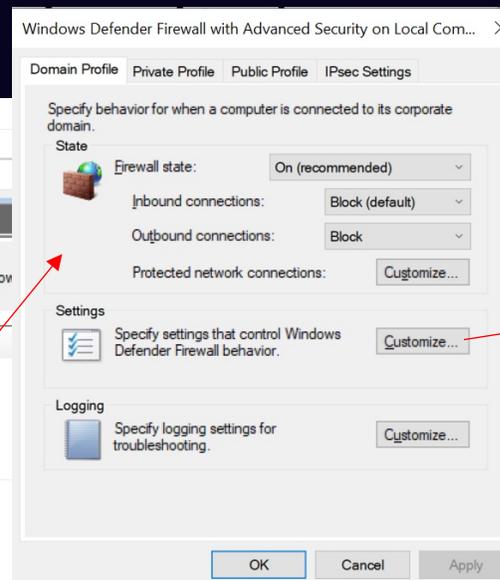
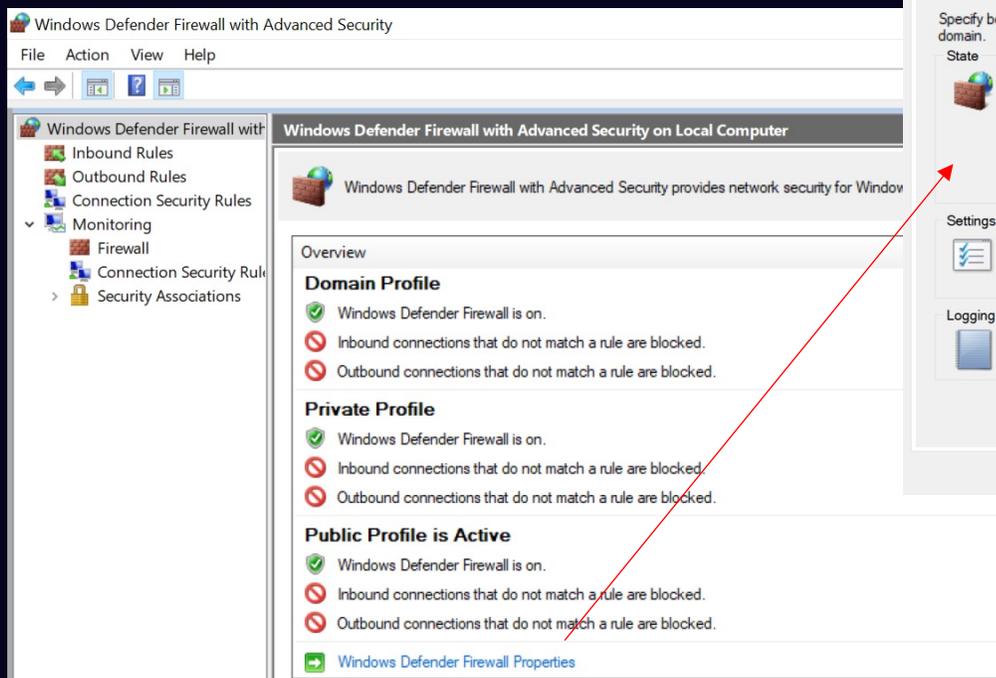
# Ikdienas sarežģījumu risinājumi

- 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 uguns smūri (nerekomendēts)



# Ikdienas sarežģījumu risinājumi

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



- 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:

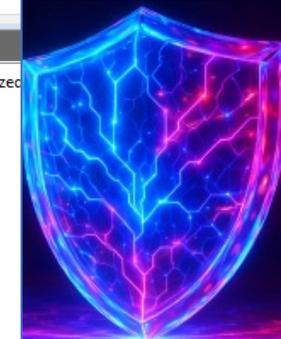
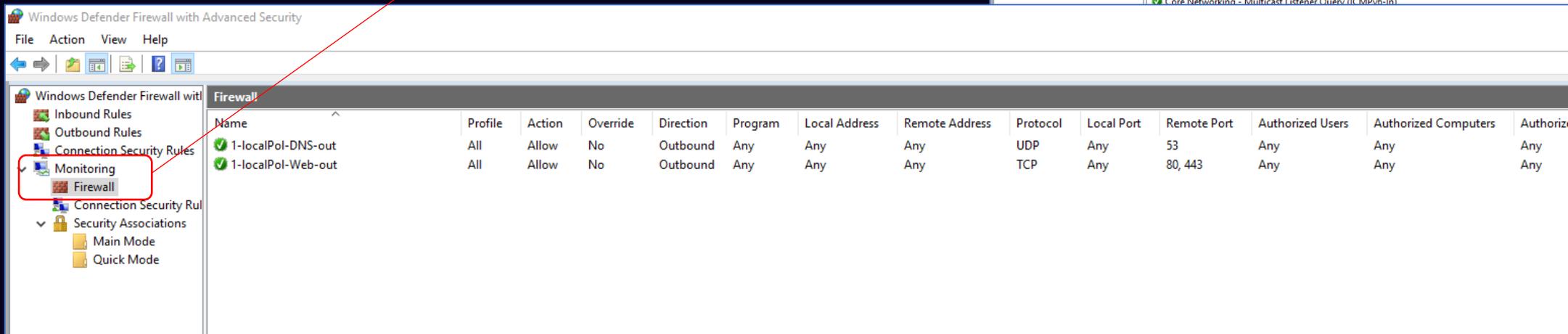
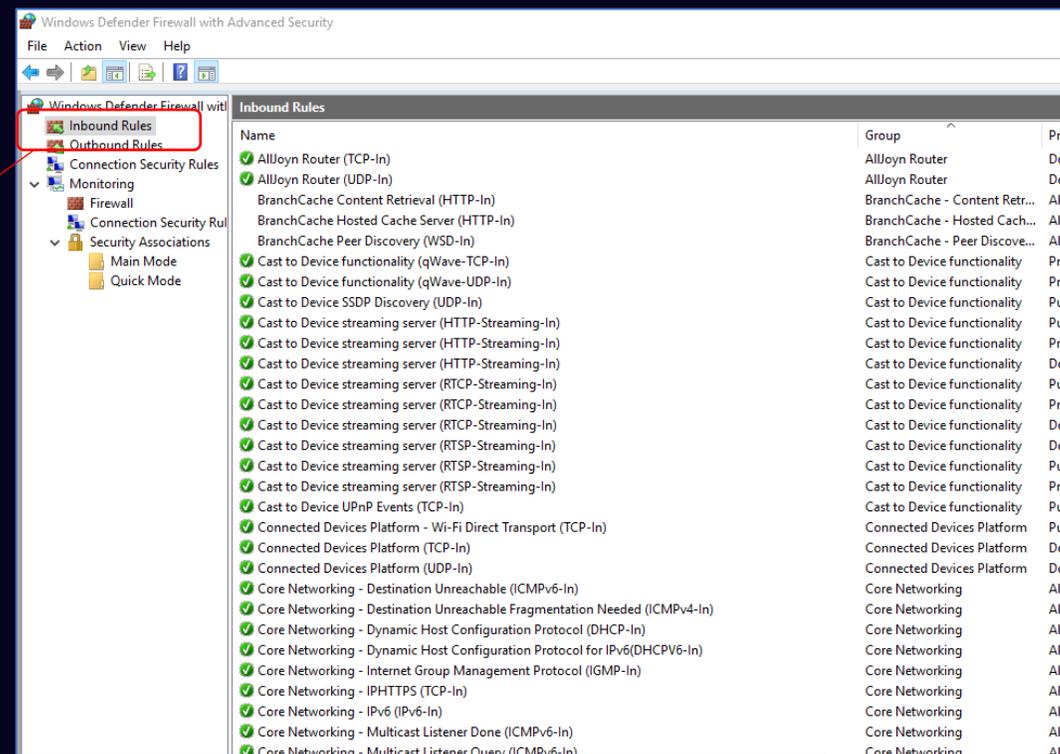
```
Start-Job -ScriptBlock {  
Start-Sleep -Minutes 15  
netsh advfirewall import "C:\temp\firewall-rules.wfw" }
```

#3:

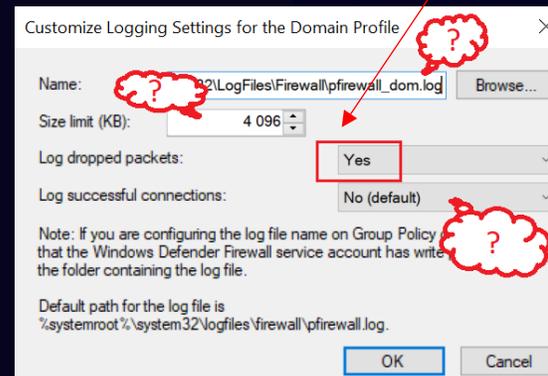
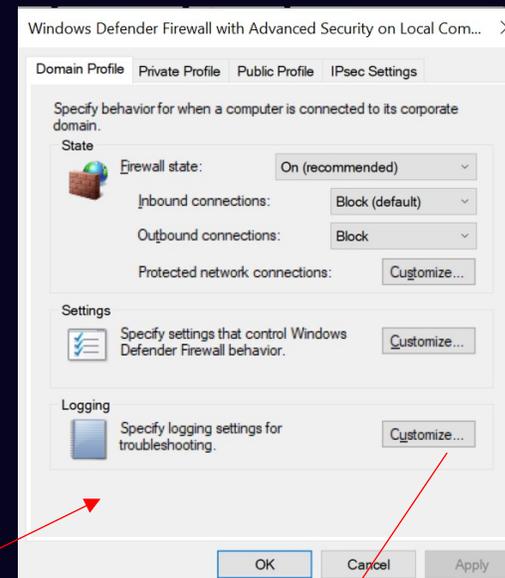
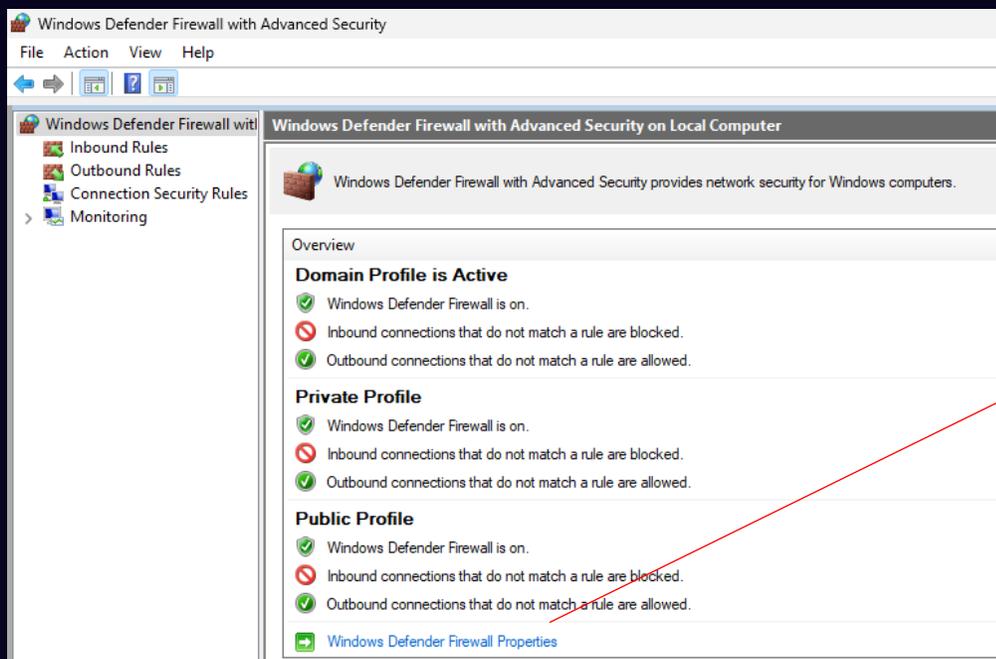
```
$time = (Get-Date).AddMinutes(15)  
schtasks /Create /SC ONCE /TN "FirewallRollback" /TR "netsh advfirewall import C:\temp\firewall-  
rules.wfw" /ST $time.ToString("HH:mm") /F
```



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



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







# Žurnālfaili

- Detalizētākas analīzes piemērs

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The 'Monitoring' tab is selected, displaying the status of the firewall. A red circle highlights the 'Monitoring' tab in the left-hand navigation pane. Another red circle highlights the log file path in the 'Logging Settings' section: `systemroot\system32\LogFiles\Firewall\pfirewall.log`.

Overlaid on the interface is a Notepad window showing the contents of the log file. The log entries are as follows:

#	date	time	action	protocol	src-ip	dst-ip	src-port	dst-port	size	path
175	09.02.2023	09:07:07	DROP		2 169.254.65.123	224.0.0.22	-	-	0	SEND
176	09.02.2023	09:07:07	DROP		2 169.254.65.123	224.0.0.22	-	-	0	SEND
185	09.02.2023	09:07:07	DROP		2 169.254.65.123	224.0.0.22	-	-	0	SEND
187	09.02.2023	09:07:07	DROP		2 169.254.65.123	224.0.0.22	-	-	0	SEND
190	09.02.2023	09:07:07	DROP	UDP	169.254.65.123	224.0.0.251	5353	5353	0	SEND
198	09.02.2023	09:07:07	DROP	UDP	169.254.65.123	224.0.0.251	5353	5353	0	SEND
213	09.02.2023	09:07:07	DROP	UDP	169.254.65.123	224.0.0.22	-	-	0	SEND
215	09.02.2023	09:07:07	DROP	UDP	169.254.65.123	169.254.255.255	137	137	0	SEND
216	09.02.2023	09:07:07	DROP	UDP	169.254.65.123	169.254.255.255	137	137	0	SEND
217	09.02.2023	09:07:07	DROP	UDP	169.254.65.123	169.254.255.255	137	137	0	SEND
223	09.02.2023	09:07:07	DROP		2 169.254.65.123	224.0.0.22	-	-	0	SEND
228	09.02.2023	09:07:08	DROP	UDP	169.254.65.123	169.254.255.255	137	137	0	SEND
229	09.02.2023	09:07:08	DROP	UDP	169.254.65.123	169.254.255.255	137	137	0	SEND
230	09.02.2023	09:07:08	DROP	UDP	169.254.65.123	169.254.255.255	137	137	0	SEND
233	09.02.2023	09:07:08	DROP	UDP	169.254.65.123	224.0.0.251	5353	5353	0	SEND
234	09.02.2023	09:07:08	DROP	UDP	169.254.65.123	224.0.0.251	5353	5353	0	SEND





# Žurnāļfaili – Windows (Event Log)

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

```
Administrator: Windows Powe...  
PS C:\> auditpol /set /subcategory:"{0CCE9226-69AE-11D9-BED3-505054503030}" /success:disable /failure:enable
```

The screenshot displays the Windows Event Viewer interface. The left pane shows the 'Security' log selected. The main pane shows 'Event 5157, Microsoft Windows security auditing.' The event details are as follows:

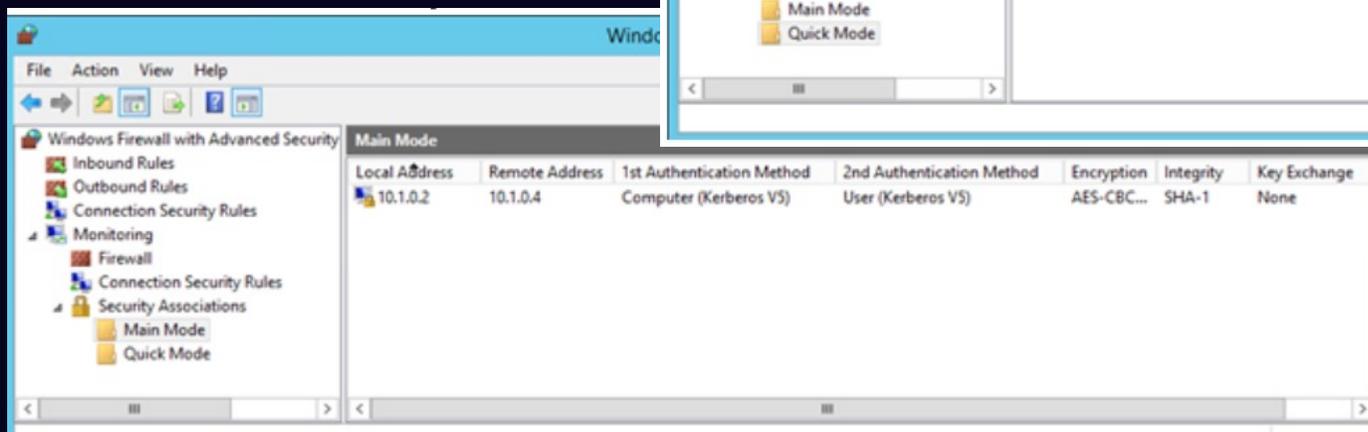
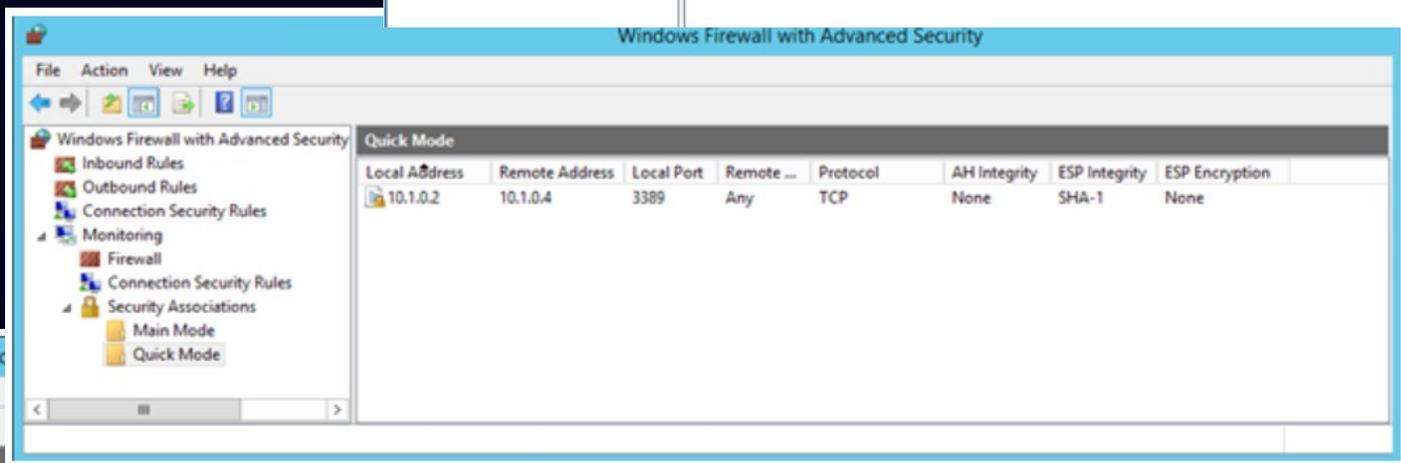
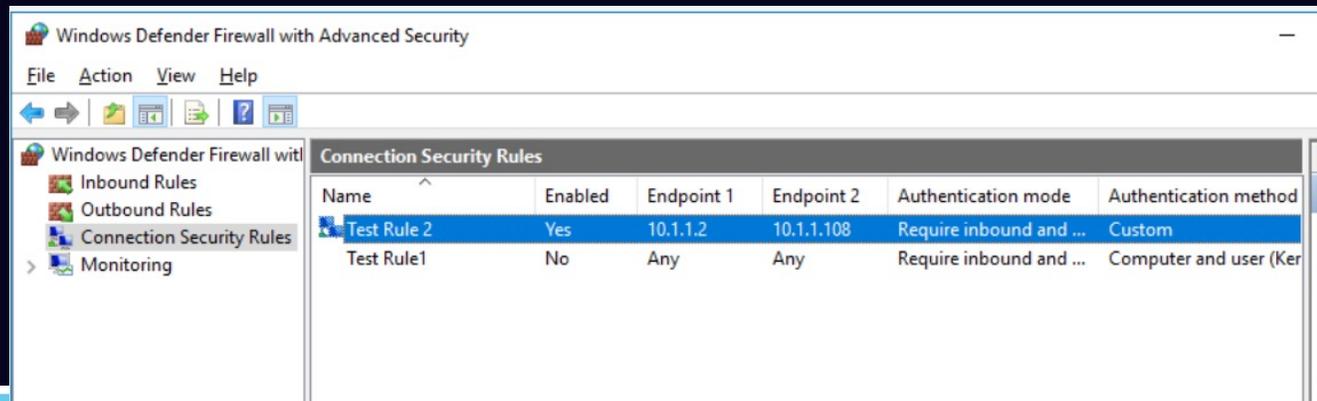
Section	Value
<b>General</b>	
The Windows Filtering Platform has blocked a connection.	
<b>Application Information:</b>	
Process ID:	9788
Application Name:	<u>\device\harddiskvolume3\program files (x86)\microsoft\edge\application\msedge.exe</u>
<b>Network Information:</b>	
Direction:	Inbound
Source Address:	192.168.188.104
Source Port:	5353
Destination Address:	224.0.0.251
Destination Port:	5353
Protocol:	17
Interface Index:	4

Log Name: Security  
Source: Microsoft Windows security  
Event ID: 5157  
Level: Information  
Task Category: Filtering Platform Connection  
Keywords: Audit Failure  
Logged: 17.02.2026 08:53:28

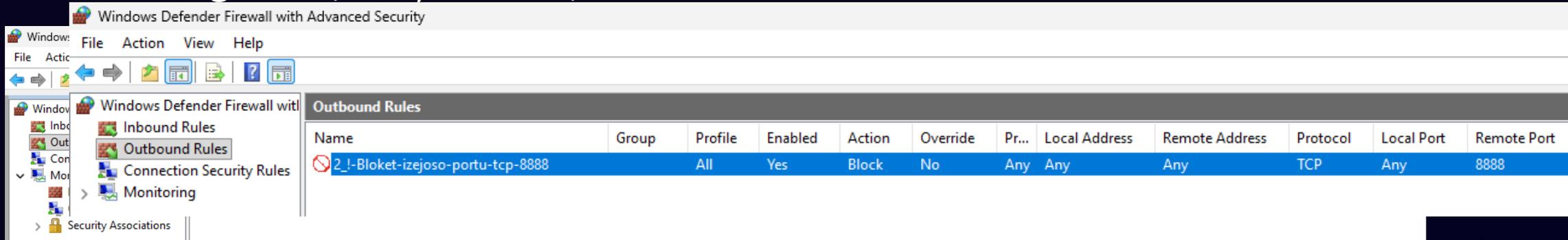


# Drošie nosacījumi (IPSEC)

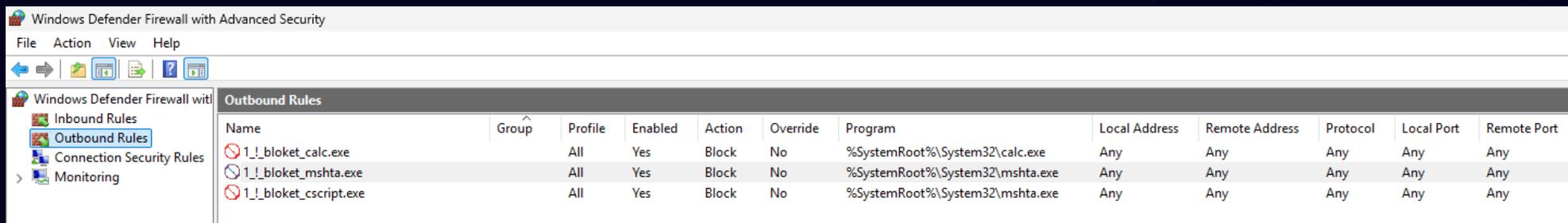
- IPSEC jebkuram savienojumam
- Autentifikācija x2 pirms savienojuma
- Izcils veids drošības uzlabošanai
- Tēma atsevišķam semināram
- Rūpīga testēšana!
- "Pro" līmenis!



- Ātrā reaģēšana, bloķēt sekas, kamēr meklē cēloni



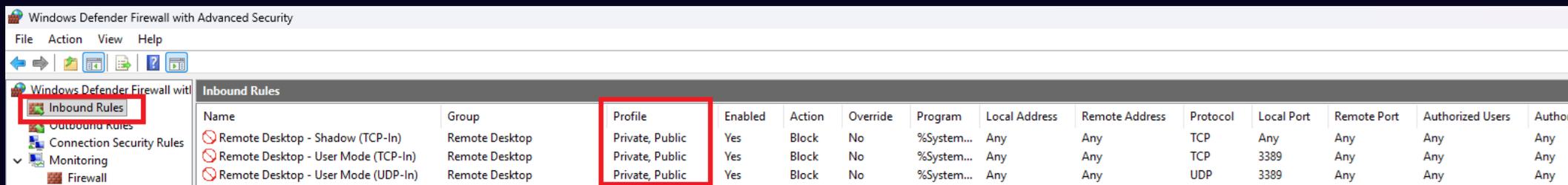
- Solis tālāk, bloķēt izpildfailus (exe), kam nav paredzēta pieeja tīmeklim



- 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!



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



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Author
Remote Desktop - Shadow (TCP-In)	Remote Desktop	Private, Public	Yes	Block	No	%System...	Any	Any	TCP	Any	Any	Any	Any
Remote Desktop - User Mode (TCP-In)	Remote Desktop	Private, Public	Yes	Block	No	%System...	Any	Any	TCP	3389	Any	Any	Any
Remote Desktop - User Mode (UDP-In)	Remote Desktop	Private, Public	Yes	Block	No	%System...	Any	Any	UDP	3389	Any	Any	Any

- Testēt!
- Info. Jaunums, uguns mūris 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



- 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



1. Dators ir pasargāts korporatīvā vidē aiz iestādes uguns mūra, mājās netiek nests  
Atb.: arī organizācijā gala iekārtām jābūt uguns mūrim, korp. risinājumi tiek kompromitēti, visu aizsardzību nebalstīt uz vienu risinājumu
2. Windows Defender pasargā kā uguns mūris  
Atb.: Defender ir aizsardzības komplekss ar dažādām komponentēm, uguns mūris ir tā būtiska un neatņemama sastāvdaļa, kura jākonfigurē
3. Uzstādīts VPN  
Atb.: VPN nav uguns mūris, uguns mūri nedrīkst aizstāt ar citas funkcijas pildošām alternatīvām
4. Antivīrusa programmatūra pasargā kā uguns mūris  
Atb.: AV ir cita misija un uzdevumi, tā nevar aizvietot uguns mūri
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), uguns mūris ir liels šķērslis vai bieži kā pēdējā aizsardzības līnija



# Paldies!

