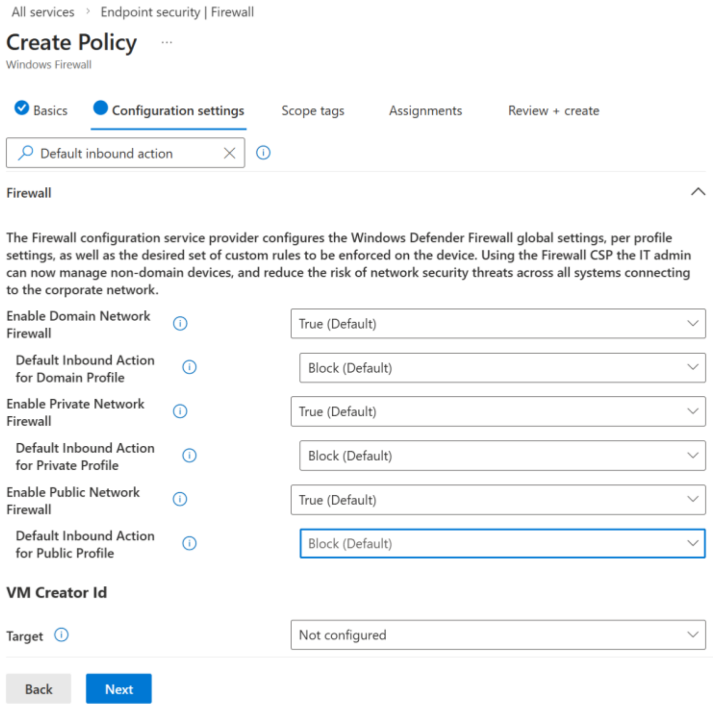
Lab 8 – Endpoint Security: Microsoft Defender Firewall

Lab 8 – In this lab, I configured an enterprise firewall baseline for Windows 10/11 devices using Microsoft Intune Endpoint Security. I created and deployed a Microsoft Defender Firewall policy to enable firewall protection across Domain, Private, and Public network profiles, enforcing a secure default posture with inbound traffic blocked and outbound traffic allowed. The policy was assigned at the device level to ensure protection regardless of user sign-in. Successful policy deployment and enforcement were checked on the endpoint using Windows Security.



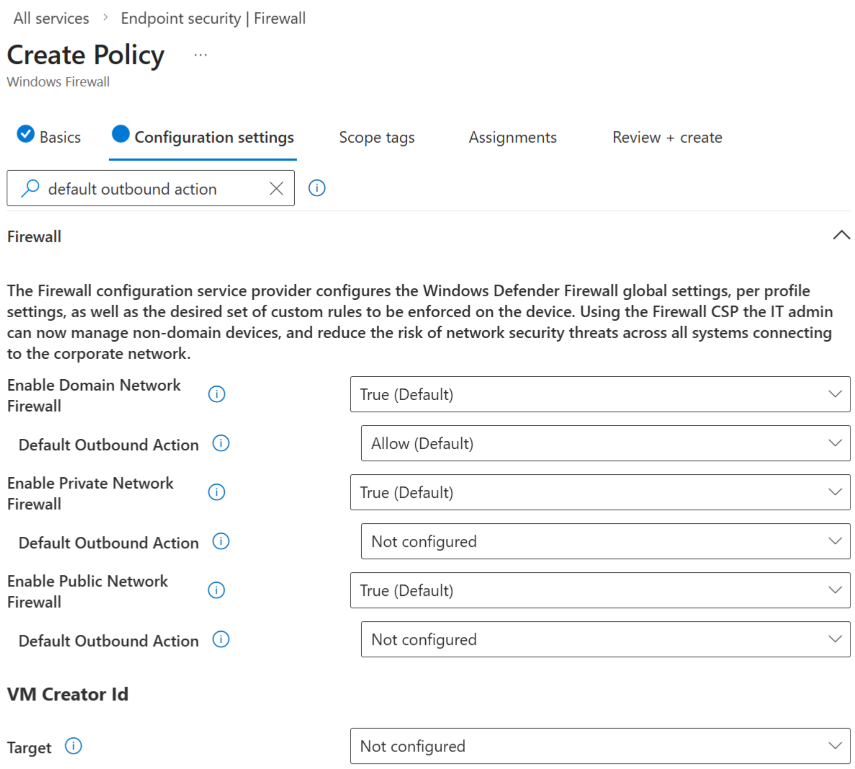
The Firewall configuration service provider configures the Windows Defender Firewall global settings, per profile settings, as well as the desired set of custom rules to be enforced on the device. Using the Firewall CSP the IT admin can now manage non-domain devices, and reduce the risk of network security threats across all systems connecting to the corporate network.

Enable Domain Network Firewall	True (Default)
Default Inbound Action for Domain Profile	Block (Default)
Enable Private Network Firewall	True (Default)
Default Inbound Action for Private Profile	Block (Default)
Enable Public Network Firewall	True (Default)
Default Inbound Action for Public Profile	Block (Default)

VM Creator Id

Target	Not configured

Notes: This screenshot shows the firewall policy configuration where the default inbound action is explicitly set to Block for Domain, Private, and Public network profiles. This ensures unsolicited inbound network traffic is denied across all network types, enforcing a secure firewall.



Create Policy

Windows Firewall

default outbound action

Firewall

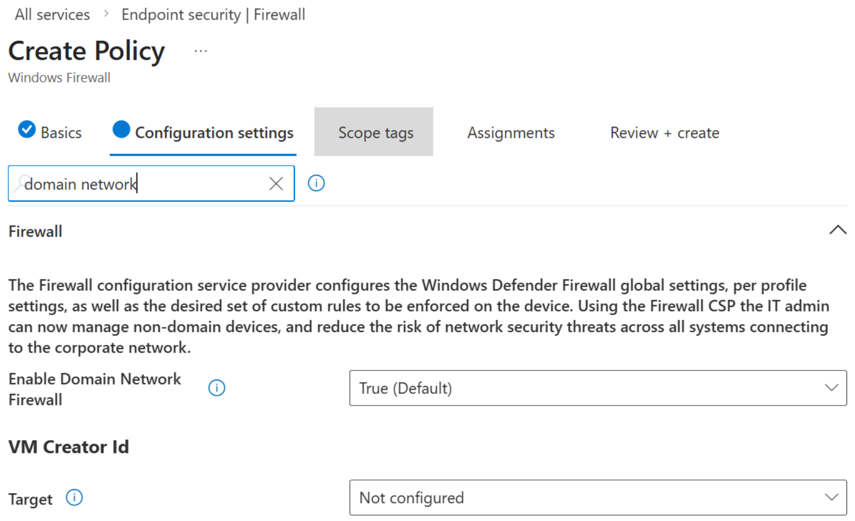
The Firewall configuration service provider configures the Windows Defender Firewall global settings, per profile settings, as well as the desired set of custom rules to be enforced on the device. Using the Firewall CSP the IT admin can now manage non-domain devices, and reduce the risk of network security threats across all systems connecting to the corporate network.

Enable Domain Network Firewall	True (Default)
Default Outbound Action	Allow (Default)
Enable Private Network Firewall	True (Default)
Default Outbound Action	Not configured
Enable Public Network Firewall	True (Default)
Default Outbound Action	Not configured

VM Creator Id

Target	Not configured

Notes: This screenshot shows the default outbound traffic configuration for the firewall policy. Outbound connections are allowed by default, aligning with good firewall practices while maintaining strong inbound traffic restrictions.



Create Policy

Windows Firewall

domain network

Firewall

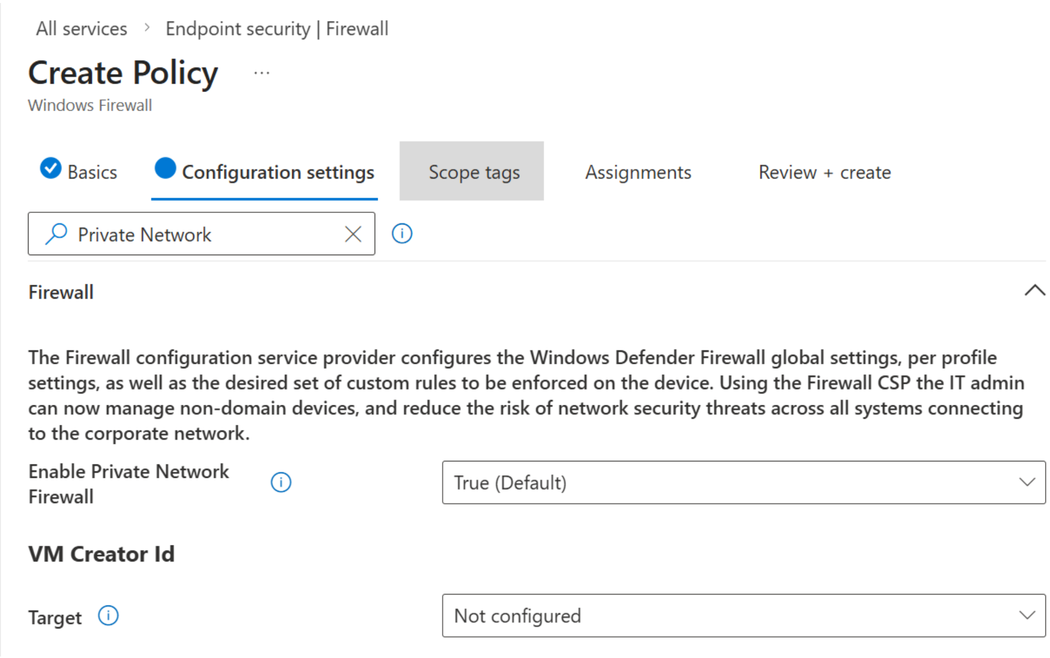
The Firewall configuration service provider configures the Windows Defender Firewall global settings, per profile settings, as well as the desired set of custom rules to be enforced on the device. Using the Firewall CSP the IT admin can now manage non-domain devices, and reduce the risk of network security threats across all systems connecting to the corporate network.

Enable Domain Network Firewall	True (Default)

VM Creator Id

Target	Not configured

Notes: This screenshot shows the Domain network firewall configuration. Microsoft Defender Firewall is enabled for the Domain profile, ensuring firewall protection is enforced when the device is connected to a corporate or domain-managed network.



Create Policy

Windows Firewall

Private Network

Firewall

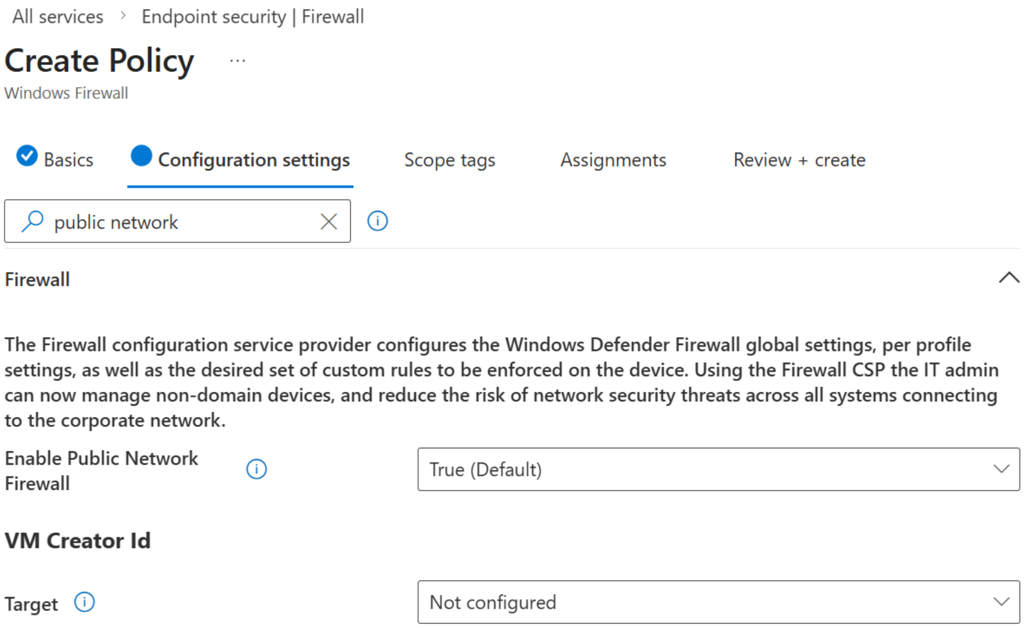
The Firewall configuration service provider configures the Windows Defender Firewall global settings, per profile settings, as well as the desired set of custom rules to be enforced on the device. Using the Firewall CSP the IT admin can now manage non-domain devices, and reduce the risk of network security threats across all systems connecting to the corporate network.

Enable Private Network Firewall: True (Default)

VM Creator Id

Target: Not configured

Notes: This screenshot shows the Private network firewall configuration. Microsoft Defender Firewall is enabled for the Private profile, providing protection when the device is connected to trusted private networks such as home or internal office networks.



Create Policy

Windows Firewall

public network

Firewall

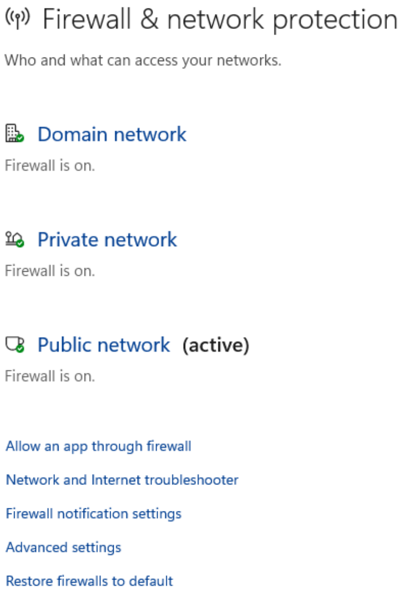
The Firewall configuration service provider configures the Windows Defender Firewall global settings, per profile settings, as well as the desired set of custom rules to be enforced on the device. Using the Firewall CSP the IT admin can now manage non-domain devices, and reduce the risk of network security threats across all systems connecting to the corporate network.

Enable Public Network Firewall: True (Default)

VM Creator Id

Target: Not configured

Notes: This screenshot shows the Public network firewall configuration. The firewall is enabled for the Public profile, enforcing a strict security posture when the device is connected to public or untrusted networks.



(ꟷ) Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network

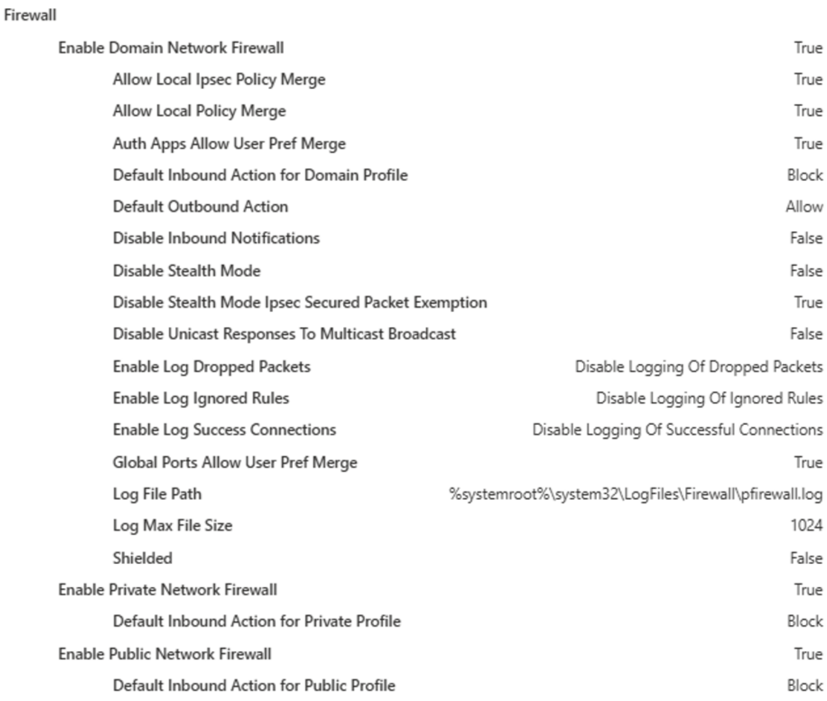
Firewall is on.

Public network (active)

Firewall is on.

Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default

Notes: This screenshot shows the Windows Security Firewall & network protection page on the managed endpoint. It confirms that Microsoft Defender Firewall is active and enforced across Domain, Private, and Public network profiles following policy deployment from Microsoft Intune.



```
Firewall
        Enable Domain Network Firewall                                                  True
                Allow Local Ipsec Policy Merge                                          True
                Allow Local Policy Merge                                                True
                Auth Apps Allow User Pref Merge                                         True
                Default Inbound Action for Domain Profile                               Block
                Default Outbound Action                                                 Allow
                Disable Inbound Notifications                                           False
                Disable Stealth Mode                                                    False
                Disable Stealth Mode Ipsec Secured Packet Exemption                     True
                Disable Unicast Responses To Multicast Broadcast                        False
                Enable Log Dropped Packets                        Disable Logging Of Dropped Packets
                Enable Log Ignored Rules                            Disable Logging Of Ignored Rules
                Enable Log Success Connections              Disable Logging Of Successful Connections
                Global Ports Allow User Pref Merge                                      True
                Log File Path                 %systemroot%\system32\LogFiles\Firewall\pfirewall.log
                Log Max File Size                                                       1024
                Shielded                                                                False
        Enable Private Network Firewall                                                 True
                Default Inbound Action for Private Profile                              Block
        Enable Public Network Firewall                                                  True
                Default Inbound Action for Public Profile                               Block
```

Notes: This screenshot shows the final review and summary of the Microsoft Defender Firewall policy in Intune. It confirms that firewall protection is enabled across all network profiles, inbound traffic is blocked by default, outbound traffic is allowed, and the policy is assigned to all managed devices.

Lab 8 – Summary

In this lab, I implemented centralized firewall enforcement for Windows 10/11 devices using Microsoft Intune Endpoint Security. A Microsoft Defender Firewall policy was configured to enable firewall protection across all network profiles and enforce secure inbound and outbound traffic behaviour.

The policy was assigned at the device level to ensure consistent protection across all managed endpoints. Deployment was verified using Microsoft Intune configuration status and confirmed on the endpoint through Windows Security, demonstrating successful policy application and enforcement.

This lab demonstrates how Microsoft Intune can be used to centrally manage endpoint firewall security and how administrators can validate policy enforcement through both management and endpoint-level controls.