Project Title: Security-Domain-Wide Controls

Microsoft Certified Solutions Associate

Author: Bhavesh Mayekar (linkedin.com/in/bhaveshmayekar)
Course: Microsoft Certified Solutions Associate
Date: 2025-09-17

Objective

*The goal of this project is to enforce **consistent endpoint security** across the domain using **Group Policy (GPO)**.*
This includes:

*Configuring **Windows Defender Firewall** policies*
*Applying **Microsoft Defender Antivirus** controls*
*Enforcing **Secure DNS Updates** for AD-integrated zones*

Why Security Matters

- ***Centralized Security*** *– Uniform GPO enforcement reduces misconfigurations.*
- ***Reduced Risk*** *– Protects against unauthorized access, malware, and lateral movement.*
- ***Auditability*** *– Logging provides visibility into firewall and DNS activity.*
- ***Resilience*** *– Domain-wide security baselines align with **enterprise best practices**.*

Technologies Used

- ***Group Policy Management Console (GPMC)***
- ***Windows Defender Firewall with Advanced Security***
- ***Microsoft Defender Antivirus (via GPO)***
- ***Active Directory–Integrated DNS*** *(Secure Dynamic Updates)*
- ***Windows Server 2016/2019/22***

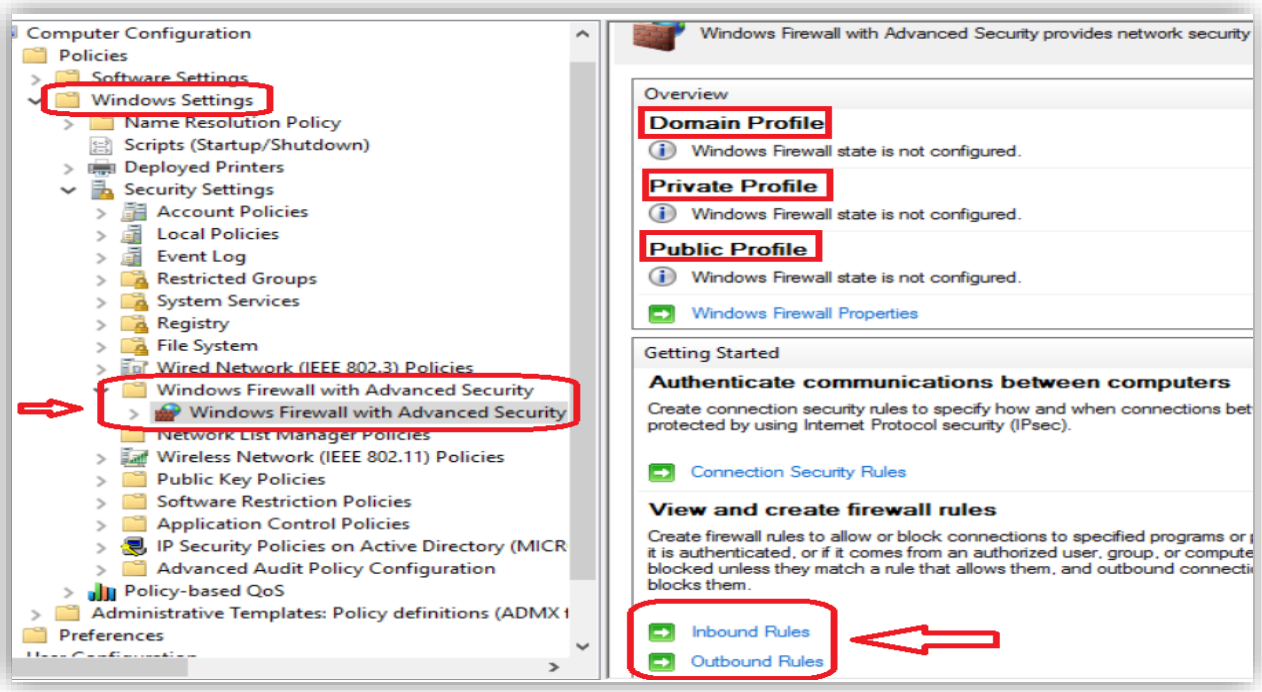
Lab Environment Setup

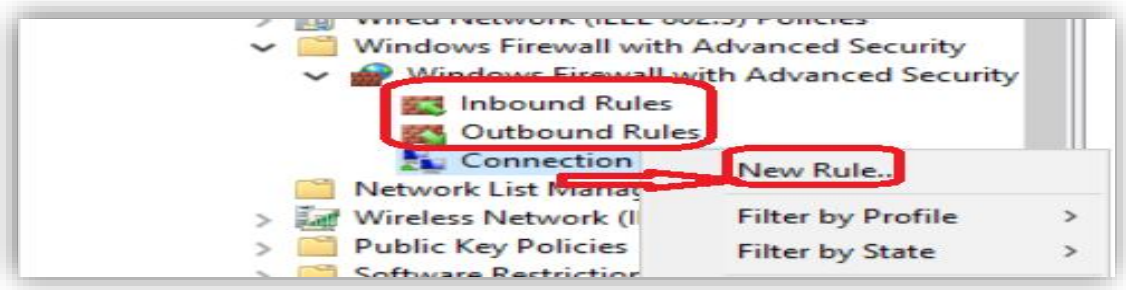
- ***Server 1 (DC)**: Domain Controller with **AD DS, DNS, DHCP, and GPOs***
- ***Server 2 (Member Server)**: Receives **security GPOs***
- ***Client Workstation**: Domain-joined PC for testing **Firewall, AV, and DNS security***

Step-by-Step Implementation

Step 1: Configure Windows Defender Firewall via GPO

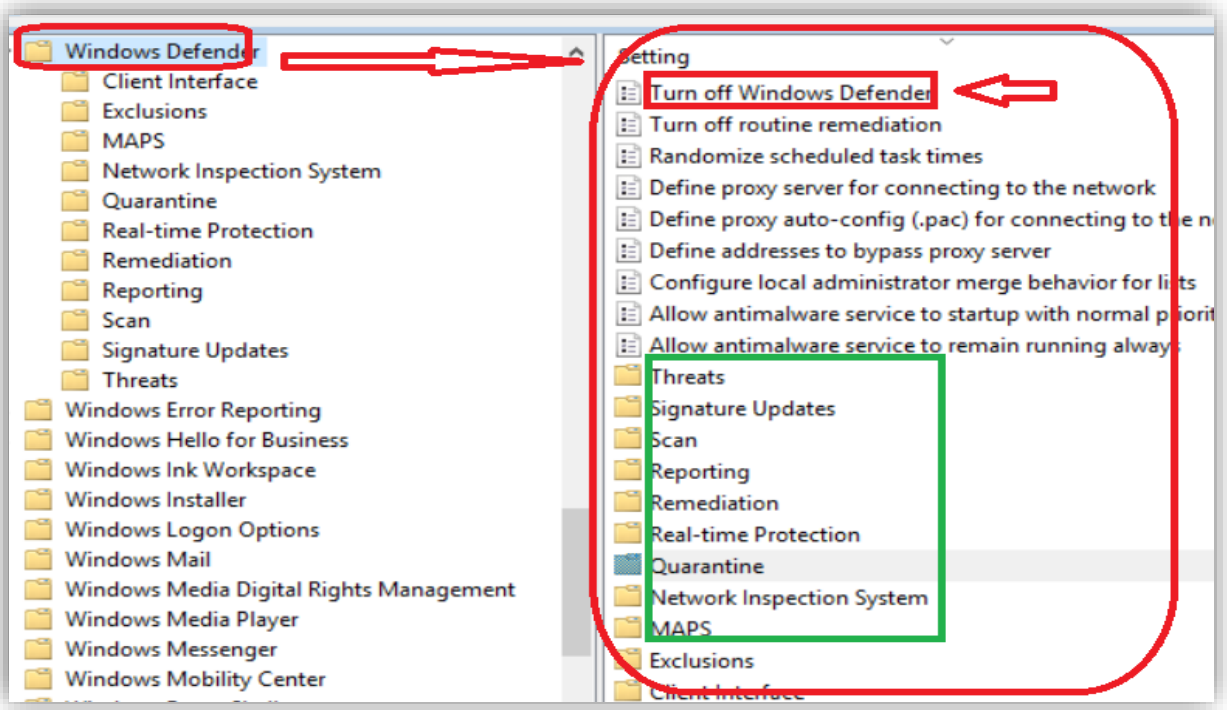
1. **On Server 1, open Group Policy Management Console (GPMC)**
2. **Right-click domain → Create a GPO in this domain, and Link it here (e.g., HR_Firewall)**
3. **Edit the GPO → Navigate to:**
   Computer Configuration > Policies > Windows Settings > Security Settings > Windows Defender Firewall with Advanced Security
4. **Configure Inbound/Outbound rules and profile settings (Domain, Private, Public)**
5. **Enable Firewall logging (set log path, size, and dropped/allowed connections)**

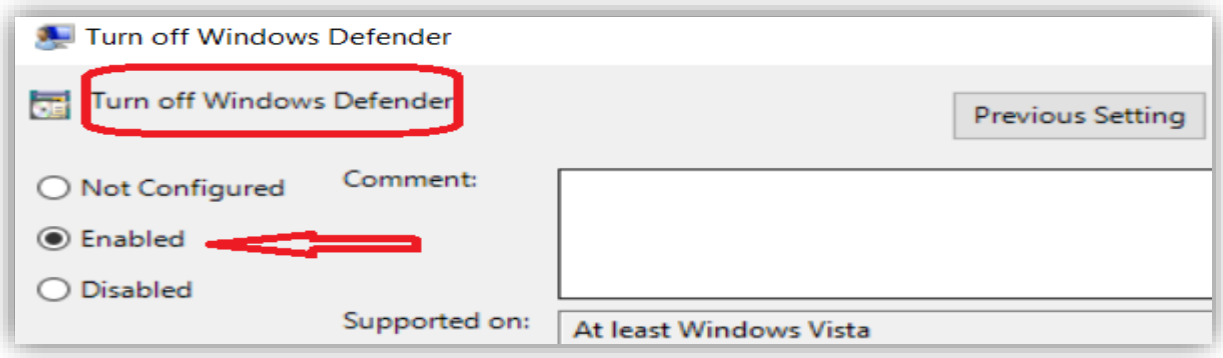




Step 2: Configure Microsoft Defender Antivirus via GPO

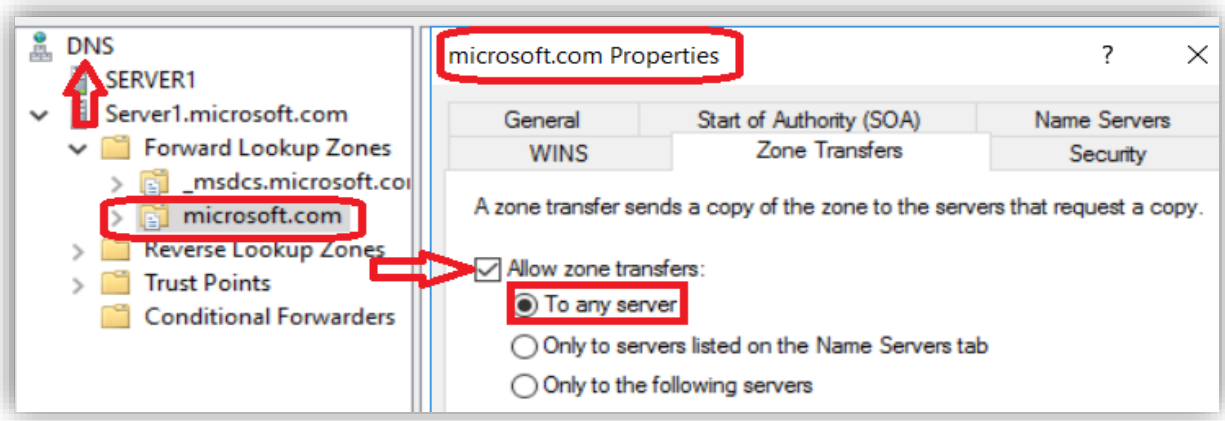
1. **Create/Edit GPO → Navigate to:**
   Computer Configuration > Policies > Administrative Templates > Windows Components > Microsoft Defender Antivirus
2. **Configure policies:**
   - **Real-time protection**
   - **Cloud-delivered protection**
   - **Exclusions**
   - **Scheduled scans**





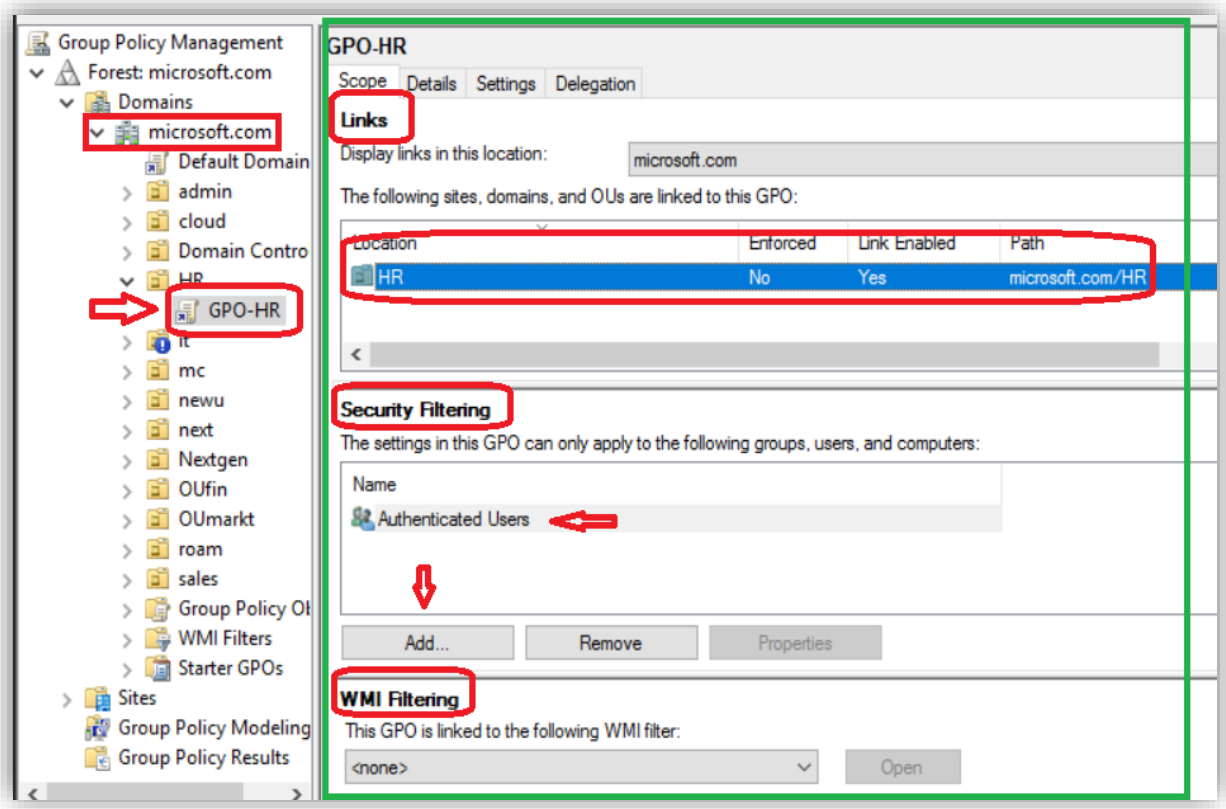
Step 3: Secure DNS Updates

1. **On Server 1, open DNS Manager**
2. **Right-click domain zone → Properties**
3. **Ensure:**
    - **Zone is AD-integrated**
    - **Dynamic updates = Secure only**



Step 4: Apply and Scope Policies

1. **Link GPOs at Domain/OU level**
2. **Use Security Filtering for specific groups**
3. **Use WMI Filters for OS/device targeting**



Validation Checks :

On Client machine:

- **Confirm GPO-applied Firewall profiles & rules in *Windows Defender Firewall with Advanced Security***
- **Verify Microsoft Defender settings and scheduled scans in *Windows Security***

On Server 1:

- **Confirm DNS Zone is AD-integrated with *Secure Only* updates**

Troubleshooting Tips :

- **Firewall rules not applying → Check GPO link order, inheritance, and security filtering**
- **Antivirus conflicts → Ensure only one authority configures Defender (GPO/Intune/SCCM)**
- **DNS updates failing → Verify client permissions and DNS zone "Secure only" setting**

Conclusion

This project successfully enforced domain-wide security controls using Group Policy. With Windows Defender Firewall, Microsoft Defender Antivirus, and Secure DNS updates in place, all endpoints now inherit a consistent, secure, and auditable baseline.

This strengthens the organization's defense against malware, unauthorized access, and misconfigurations, while aligning with enterprise security best practices.

It also lays a foundation for scalable, policy-driven endpoint management in hybrid environments.

Author: Bhavesh Mayekar (linkedin.com/in/bhaveshmayekar)
Course: Microsoft Certified Solutions Associate
Date: 2025-09-17