==========

==========

CATEGORY: WindowsFirewallAdvanced

==========

==========

Advanced Windows Firewall operations directly affect system security, network segmentation, application access, compliance, and threat mitigation. These SOPs ensure every firewall-related action performed through RDAM Script Wizard is **controlled**, **auditable**, and aligned with enterprise security standards.

SOP 1 – Get Firewall Status

1. Purpose

Retrieve the operational state of Windows Firewall across all profiles.

2. Scope

- **Domain, Private, and Public profiles**
- **Windows servers and workstations**

3. Preconditions

- **Operator must have permission to query firewall configuration**

4. Required Inputs

- **None**

5. Procedure Steps

- **Profile Enumeration** – Retrieve firewall state for all profiles.
- **Attribute Extraction** – Enabled/Disabled, inbound/outbound defaults.
- **Output Formatting** – Structured firewall status.
- **Logging** – Operator and timestamp.

6. Expected Output

- **Firewall status for all profiles**

7. Error Handling

- **Access denied**
- **Firewall service unavailable**

8. Security Considerations

- **Firewall state reveals security posture**

9. Audit Logging Requirements

- **Operator ID**
- **Timestamp**

10. Organizational Benefit Statement

This procedure provides visibility into firewall posture, supporting compliance, security audits, and operational readiness.

SOP 2 – Enable Firewall Profile

1. Purpose

Enable Windows Firewall for a specified profile.

2. Scope

- **Domain, Private, and Public profiles**

3. Preconditions

- **Operator must have administrative rights**

4. Required Inputs

- **Profile name**

5. Procedure Steps

- **Input Collection**
- **Profile Validation**
- **Enable Operation**

- **Post-Enable Verification**
- **Logging**

6. Expected Output

- **Firewall profile enabled**

7. Error Handling

- **Invalid profile**
- **Access denied**

8. Security Considerations

- **Enabling firewall may block existing connections**

9. Audit Logging Requirements

- **Operator ID**
- **Profile name**
- **Timestamp**

10. Organizational Benefit Statement

This procedure ensures firewall protection is applied consistently, strengthening system security and compliance.

SOP 3 – Disable Firewall Profile

1. Purpose

Disable Windows Firewall for a specified profile.

2. Scope

- **Domain, Private, and Public profiles**

3. Preconditions

- **Operator must have administrative rights**
- **Action must be authorized by security**

4. Required Inputs

- **Profile name**

5. Procedure Steps

- **Input Collection**
- **Profile Validation**
- **Disable Operation**
- **Post-Disable Verification**
- **Logging**

6. Expected Output

- **Firewall profile disabled**

7. Error Handling

- **Invalid profile**
- **Access denied**

8. Security Considerations

- **Disabling firewall increases attack surface**

9. Audit Logging Requirements

- **Operator ID**
- **Profile name**
- **Timestamp**

10. Organizational Benefit Statement

This procedure ensures firewall deactivation is controlled and auditable, supporting troubleshooting while maintaining accountability.

SOP 4 – List Firewall Rules

1. Purpose

Retrieve all firewall rules for inventory, troubleshooting, and compliance.

2. Scope

- **Inbound and outbound rules**
- **Enabled and disabled rules**

3. Preconditions

- **Operator must have permission to query firewall rules**

4. Required Inputs

- **Optional: Rule name filter**

5. Procedure Steps

- **Input Collection**
- **Rule Enumeration**
- **Attribute Extraction** – Name, direction, action, program, ports, profiles.
- **Output Formatting**
- **Logging**

6. Expected Output

- **List of firewall rules with metadata**

7. Error Handling

- **Access denied**
- **Invalid filter**

8. Security Considerations

- **Rules may reveal network architecture**

9. Audit Logging Requirements

- **Operator ID**
- **Filter used**
- **Timestamp**

10. Organizational Benefit Statement

This procedure provides a complete view of firewall configuration, supporting audits, troubleshooting, and security reviews.

SOP 5 – Create Firewall Rule

1. Purpose

Create a new inbound or outbound firewall rule.

2. Scope

- **Windows servers and workstations**

3. Preconditions

- **Operator must have administrative rights**
- **Rule must comply with security policy**

4. Required Inputs

- **Rule name**
- **Direction (Inbound/Outbound)**
- **Action (Allow/Block)**
- **Protocol**
- **Port(s)**
- **Optional: Program path**
- **Optional: Profile(s)**

5. Procedure Steps

- **Input Collection**
- **Validation**
- **Rule Creation**
- **Post-Creation Verification**
- **Logging**

6. Expected Output

- **Firewall rule created successfully**

7. Error Handling

- **Invalid parameters**

- **Access denied**

8. Security Considerations

- **Incorrect rules may expose services or block critical traffic**

9. Audit Logging Requirements

- **Operator ID**
- **Rule name**
- **Timestamp**

10. Organizational Benefit Statement

This procedure ensures firewall rules are created safely and consistently, supporting secure application access and network segmentation.

SOP 6 – Remove Firewall Rule

1. Purpose

Delete a firewall rule safely and with full audit accountability.

2. Scope

- **Inbound and outbound rules**

3. Preconditions

- **Operator must have administrative rights**
- **Rule must exist**

4. Required Inputs

- **Rule name**

5. Procedure Steps

- **Input Collection**
- **Rule Resolution**
- **Removal Operation**
- **Post-Removal Verification**
- **Logging**

6. Expected Output

- **Firewall rule removed successfully**

7. Error Handling

- **Rule not found**
- **Access denied**

8. Security Considerations

- **Removing rules may expose services or break connectivity**

9. Audit Logging Requirements

- **Operator ID**
- **Rule name**
- **Timestamp**

10. Organizational Benefit Statement

This procedure ensures firewall rules are removed cleanly and safely, preventing configuration drift and maintaining security posture.