==========

==========

CATEGORY: Firewall

==========

==========

Firewall configuration directly affects system security, network access, and compliance posture. These SOPs ensure every firewall action performed through RDAM Script Wizard is controlled, auditable, and aligned with enterprise security standards.

SOP 1 – Get Firewall Rules

Script Name: Get Firewall Rules **Category:** Firewall **Version:** 1.0 **Approved By:** IT Operations / Security

1. Purpose

This script retrieves Windows Firewall rules from the local system, supporting troubleshooting, compliance validation, and security audits.

2. Scope

- **Systems:** Windows servers and workstations
- **Firewall Profiles:** Domain, Private, Public
- **Authorized Personnel:**
    - Security engineers
    - System administrators
    - Network engineers
    - Incident response teams

3. Definitions

- **Firewall Rule:** A configuration entry controlling inbound/outbound traffic.
- **Profile:** Network category (Domain, Private, Public).
- **Direction:** Inbound or outbound.

4. Preconditions

- Operator must have read access to firewall configuration.
- System must support Windows Firewall with Advanced Security.
- RDAM must run under a context with local administrative privileges (recommended).

5. Required Inputs

- Optional:
    - Rule name filter
    - Direction filter
    - Profile filter

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for optional filters.
    - Validate filter formats.
2. **Firewall Module Initialization**
    - Load firewall management APIs.
    - If unavailable, abort and log.
3. **Rule Enumeration**
    - Retrieve all firewall rules.
    - Apply filters if provided.
4. **Data Extraction**
    - Extract:
        - Name
        - Enabled state
        - Direction
        - Action (Allow/Block)
        - Program/Service
        - Local/Remote ports
        - Profiles
        - Protocol

5. **Output Formatting**
    - Present results in structured table or JSON format.
    - Highlight disabled or blocking rules if applicable.
6. **Logging**
    - Log operator, filters used, timestamp.

7. Expected Output

- A list of firewall rules matching the filter criteria.

8. Post-Execution Validation

- Operator may cross-check with Windows Firewall GUI or `Get-NetFirewallRule`.

9. Error Handling

- Access denied
- Firewall service not running
- Invalid filter values

10. Security Considerations

- Firewall rules reveal system security posture; restrict access.
- Avoid exporting rule sets outside approved channels.

11. Audit Logging Requirements

- Operator ID
- Filters used
- Rule count
- Timestamp

12. Organizational Benefit Statement

This script provides a consistent, auditable method for reviewing firewall rules, supporting troubleshooting, compliance, and security posture assessments.

SOP 2 – Enable Firewall Rule

Script Name: Enable Firewall Rule **Category:** Firewall

1. Purpose

This script enables a specified Windows Firewall rule, restoring intended traffic control behavior. It supports troubleshooting, remediation, and security enforcement.

2. Scope

- Windows Firewall rules on servers and workstations
- Used by security, operations, and engineering teams

3. Definitions

- **Enable Rule:** Set rule state to active so it applies to traffic.

4. Preconditions

- Operator must have administrative privileges.
- Rule must exist.
- Enabling must align with approved change or remediation request.

5. Required Inputs

- Rule name (exact or partial match)

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for rule name.
    - Validate non-empty.
2. **Rule Resolution**
    - Query firewall rules for matching name.
    - If multiple matches, return list for operator selection (if supported).
    - If no match, abort.
3. **State Check**
    - If rule already enabled, return informational message.
4. **Enable Operation**
    - Set rule's `Enabled` property to `True`.
5. **Post-Change Verification**
    - Requery rule to confirm enabled state.

6. **Logging**
    - Log rule name, operator, timestamp.

7. Expected Output

- Confirmation that the rule was enabled.

8. Post-Execution Validation

- Operator may verify via GUI or PowerShell.
- Network team may validate connectivity.

9. Error Handling

- Rule not found
- Access denied
- Firewall service not running

10. Security Considerations

- Enabling rules may open network access; ensure approvals.
- Avoid enabling rules that weaken security posture.

11. Audit Logging Requirements

- Operator ID
- Rule name
- Previous state
- New state
- Timestamp

12. Organizational Benefit Statement

This script ensures firewall rule activation is performed safely and with full accountability, supporting secure and consistent system configuration.

SOP 3 – Disable Firewall Rule

Script Name: Disable Firewall Rule **Category:** Firewall

1. Purpose

This script disables a specified Windows Firewall rule, preventing it from applying to network traffic. It supports incident response, troubleshooting, and security hardening.

2. Scope

- Windows Firewall rules on servers and workstations
- Used by security, operations, and engineering teams

3. Definitions

- **Disable Rule:** Set rule state to inactive so it no longer applies.

4. Preconditions

- Operator must have administrative privileges.
- Rule must exist.
- Disabling must align with approved change or security directive.

5. Required Inputs

- Rule name (exact or partial match)

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for rule name.
2. **Rule Resolution**
    - Query firewall rules for matching name.
3. **State Check**
    - If rule already disabled, return informational message.
4. **Disable Operation**
    - Set rule's `Enabled` property to `False`.
5. **Post-Change Verification**
    - Requery rule to confirm disabled state.
6. **Logging**
    - Log rule name, operator, timestamp.

7. Expected Output

- Confirmation that the rule was disabled.

8. Post-Execution Validation

- Operator may verify via GUI or PowerShell.
- Security team may validate reduced exposure.

9. Error Handling

- Rule not found
- Access denied
- Firewall service not running

10. Security Considerations

- Disabling rules may block required traffic; ensure approvals.
- Disabling security-critical rules may violate policy.

11. Audit Logging Requirements

- Operator ID
- Rule name
- Previous state
- New state
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for disabling firewall rules, supporting incident response, troubleshooting, and security hardening.