==

CATEGORY: WindowsFirewall

==

Firewall operations directly affect system security, network exposure, application connectivity, and compliance posture. 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 Rules

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

1. Purpose

This script retrieves Windows Firewall rules, supporting troubleshooting, compliance, and security investigations.

2. Scope

- Windows servers and workstations
- Inbound and outbound rules
- All profiles (Domain, Private, Public)

3. Definitions

- **Firewall Rule:** A policy controlling network traffic.
- **Profile:** Network category applied to the rule.

4. Preconditions

- Operator must have permission to query firewall configuration.

5. Required Inputs

- Optional: Rule name filter
- Optional: Direction filter (Inbound/Outbound)

6. Procedure Steps

1. Input Collection
    - Wizard prompts for optional filters.
2. Rule Enumeration
    - Retrieve all firewall rules.
3. Filtering
    - Apply name or direction filters if provided.
4. Attribute Retrieval
    - Extract:
        - Rule name
        - Enabled state
        - Direction
        - Action (Allow/Block)
        - Program/path
        - Local/remote ports
        - Profile
5. Output Formatting
    - Present structured rule list.
6. Logging
    - Log filters, operator, timestamp.

7. Expected Output

- List of firewall rules with key attributes.

8. Post-Execution Validation

- Operator may verify via `wf.msc` or `Get-NetFirewallRule`.

9. Error Handling

- Access denied
- Invalid filter
- Firewall service unavailable

10. Security Considerations

- Rule data may reveal sensitive network exposure.

11. Audit Logging Requirements

- Operator ID
- Filters used
- Timestamp

12. Organizational Benefit Statement

This script provides a consistent, auditable method for enumerating firewall rules, supporting troubleshooting and compliance.

SOP 2 – Enable Firewall Rule

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

1. Purpose

This script enables a firewall rule, supporting application connectivity, troubleshooting, and configuration management.

2. Scope

- Windows servers and workstations
- Inbound and outbound rules

3. Definitions

- **Enable Rule:** Activate a firewall rule so it applies to traffic.

4. Preconditions

- Operator must have administrative rights.
- Rule must exist.
- Action must be authorized.

5. Required Inputs

- Rule name

6. Procedure Steps

1. Input Collection
    - Wizard prompts for rule name.
2. Rule Resolution
    - Identify matching rule.
3. Enable Operation
    - Set rule state to Enabled.
4. Post-Enable Verification
    - Confirm rule is active.
5. Logging
    - Log rule name, operator, timestamp.

7. Expected Output

- Confirmation that the rule was enabled.

8. Post-Execution Validation

- Operator may verify via `Get-NetFirewallRule`.

9. Error Handling

- Rule not found
- Access denied
- Firewall service unavailable

10. Security Considerations

- Enabling rules may expose services; ensure approvals.

11. Audit Logging Requirements

- Operator ID
- Rule name
- Timestamp

12. Organizational Benefit Statement

This script ensures firewall rule enablement is performed safely and consistently, supporting connectivity and configuration management.

SOP 3 – Disable Firewall Rule

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

1. Purpose

This script disables a firewall rule, supporting security hardening, troubleshooting, and configuration rollback.

2. Scope

- Windows servers and workstations
- Inbound and outbound rules

3. Definitions

- **Disable Rule:** Deactivate a firewall rule so it no longer applies.

4. Preconditions

- Operator must have administrative rights.
- Rule must exist.
- Action must be authorized.

5. Required Inputs

- Rule name

6. Procedure Steps

1. Input Collection
    - Wizard prompts for rule name.
2. Rule Resolution
    - Identify matching rule.
3. Disable Operation
    - Set rule state to Disabled.
4. Post-Disable Verification

    - Confirm rule is inactive.

5. Logging
    - Log rule name, operator, timestamp.

7. Expected Output

- Confirmation that the rule was disabled.

8. Post-Execution Validation

- Operator may verify via `Get-NetFirewallRule`.

9. Error Handling

- Rule not found
- Access denied
- Firewall service unavailable

10. Security Considerations

- Disabling rules may block required application traffic.

11. Audit Logging Requirements

- Operator ID
- Rule name
- Timestamp

12. Organizational Benefit Statement

This script ensures firewall rule disablement is performed safely and with full accountability, supporting security and troubleshooting.

SOP 4 – Create Firewall Rule

Script Name: Create Firewall Rule **Category:** WindowsFirewall

1. Purpose

This script creates a new firewall rule, supporting application deployment, troubleshooting, and network configuration.

2. Scope

- Windows servers and workstations

- Inbound and outbound rules

3. Definitions

- **Custom Rule:** A user-defined firewall policy.

4. Preconditions

- Operator must have administrative rights.
- Rule creation must be authorized.
- Ports and programs must be valid.

5. Required Inputs

- Rule name
- Direction (Inbound/Outbound)
- Action (Allow/Block)
- Protocol (TCP/UDP)
- Local/remote ports
- Optional: Program path
- Optional: Profile

6. Procedure Steps

1. Input Collection
    - Wizard prompts for rule parameters.
2. Validation
    - Confirm ports and protocol are valid.
    - Confirm rule name is unique.
3. Creation Operation
    - Create firewall rule with specified parameters.
4. Post-Creation Verification
    - Confirm rule exists and is enabled.
5. Logging
    - Log rule name, parameters, operator, timestamp.

7. Expected Output

- Confirmation of rule creation.

8. Post-Execution Validation

- Operator may verify via `Get-NetFirewallRule`.

9. Error Handling

- Invalid ports
- Access denied
- Rule already exists

10. Security Considerations

- Creating rules may expose services; ensure approvals.

11. Audit Logging Requirements

- Operator ID
- Rule name
- Parameters
- Timestamp

12. Organizational Benefit Statement

This script ensures firewall rule creation is performed safely and consistently, supporting application deployment and network configuration.

SOP 5 – Delete Firewall Rule

Script Name: Delete Firewall Rule **Category:** WindowsFirewall

1. Purpose

This script deletes a firewall rule, supporting cleanup, de-provisioning, and configuration rollback.

2. Scope

- Windows servers and workstations
- Inbound and outbound rules

3. Definitions

- **Rule Deletion:** Removing a firewall rule from configuration.

4. Preconditions

- Operator must have administrative rights.
- Rule must exist.
- Deletion must be authorized.

5. Required Inputs

- Rule name

6. Procedure Steps

1. Input Collection
    - Wizard prompts for rule name.
2. Rule Resolution
    - Identify matching rule.
3. Safety Check
    - Prevent deletion of critical system rules unless authorized.
4. Deletion Operation
    - Remove rule from firewall.
5. Post-Deletion Verification
    - Confirm rule no longer exists.
6. Logging
    - Log rule name, operator, timestamp.

7. Expected Output

- Confirmation of rule deletion.

8. Post-Execution Validation

- Operator may verify via `Get-NetFirewallRule`.

9. Error Handling

- Rule not found

- Access denied
- Deletion blocked by system

10. Security Considerations

- Removing rules may expose or block traffic; ensure approvals.

11. Audit Logging Requirements

- Operator ID
- Rule name
- Timestamp

12. Organizational Benefit Statement

This script ensures firewall rule removal is performed safely and with full accountability, supporting cleanup and configuration rollback.

SOP 6 – Get Firewall Profile Status

Script Name: Get Firewall Profile Status **Category:** WindowsFirewall

1. Purpose

This script retrieves the status of Windows Firewall profiles, supporting security monitoring, compliance, and troubleshooting.

2. Scope

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

3. Definitions

- **Profile:** Network category with independent firewall settings.

4. Preconditions

- Operator must have permission to query firewall configuration.

5. Required Inputs

- None

6. Procedure Steps

1. Profile Enumeration
    - Retrieve Domain, Private, and Public profile settings.
2. Attribute Retrieval
    - Extract:
        - Firewall enabled state
        - Default inbound/outbound action
        - Logging settings
        - Notification settings
3. Output Formatting
    - Present structured profile summary.
4. Logging
    - Log operator and timestamp.

7. Expected Output

- Firewall profile configuration summary.

8. Post-Execution Validation

- Operator may verify via Windows Security Center or PowerShell.

9. Error Handling

- Access denied
- Firewall service unavailable

10. Security Considerations

- Profile data reveals security posture; restrict access.

11. Audit Logging Requirements

- Operator ID
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for retrieving firewall profile status, supporting security monitoring and compliance.