

MSP Firewall Change Request SOP

Document no.	SOP-MSP-007
Revision	1.0
Owner	Network Engineering Lead
Effective date	October 15, 2026
Review cycle	Every 12 months

1. Purpose

To make every change to a managed client's firewall authorized, reviewed, reversible and documented, so rules never open more access than needed and anyone can see why each rule exists.

2. Scope

Applies to adding, changing or removing firewall rules, NAT, port forwards and VPN access on firewalls the MSP manages for clients. Firmware upgrades and full firewall replacements are handled as projects.

Definitions

Firewall change request	A ticket asking for a firewall rule to be added, changed or removed, with source, destination, ports, reason and duration.
Rule register	The documented list of a client's firewall rules, with the ticket, requester, reason and review or expiry date for each.
Temporary rule	A rule that is needed only for a set period, such as vendor access for a project, and must be removed when it expires.
Least privilege	Allowing only the specific sources, destinations and ports a business need requires, and nothing broader.

3. Responsibilities

Service Desk Technician	Logs the request, collects the required details and verifies the requester against the client's approver list.
Network Engineer	Designs the rule, backs up the configuration, implements and tests the change and updates the rule register.
Security Engineer	Reviews the security risk of each request and removes expired temporary rules.
Service Manager	Approves the change on the MSP side and decides when a request needs the client's risk acceptance.
Client Point of Contact	Requests or approves changes as an authorized approver and confirms the change works.

RACI matrix

Activity	Service Desk Technician	Network Engineer	Security Engineer	Service Manager	Client Point of Contact
Log and verify the request	R/A	I	-	-	C

Activity	Service Desk Technician	Network Engineer	Security Engineer	Service Manager	Client Point of Contact
Review security risk	-	C	R/A	I	I
Approve the change	I	C	C	R/A	R
Implement, test and document the rule	I	R/A	I	I	C
Remove expired temporary rules	-	R	A	I	I

R = Responsible, A = Accountable, C = Consulted, I = Informed

4. Materials and PPE

Materials, tools and systems

- PSA ticket with firewall change request form
- Client authorized approver list
- Firewall management console
- Configuration backup storage
- Client network documentation and rule register
- Rule naming convention

5. Procedure

Step	Task	Owner	Done
5.1	Log the firewall change request The Service Desk Technician logs the request in the PSA with source, destination, ports and protocol, business reason, requested date and whether the rule is temporary.	Service Desk Technician	☐
5.2	Verify the requester The Service Desk Technician checks that the requester is on the client's authorized approver list, or gets approval from someone who is. Warning: Never open inbound access on an unverified email request. Call the approver back on the number in the client documentation.	Service Desk Technician	☐
5.3	Translate the request into a rule The Network Engineer clarifies the details with the requester and writes the exact rule, using specific addresses and ports instead of broad ranges.	Network Engineer	☐
5.4	Review the security risk The Security Engineer reviews the proposed rule for inbound exposure, overly broad access and conflicts, and suggests safer options such as VPN access where they fit.	Security Engineer	☐
5.5	Approve the change The Service Manager approves the change for the MSP, and the Client Point of Contact approves it for the client, accepting any risk the security review raised. Checkpoint: Both the MSP and client approvals are recorded in the ticket before any change is made.	Service Manager	☐
5.6	Back up the firewall configuration The Network Engineer exports and stores the current firewall configuration so the change can be reversed quickly.	Network Engineer	☐

Step	Task	Owner	Done
5.7	Schedule the change window The Network Engineer schedules the change, inside the client's maintenance window if it could interrupt traffic, and tells the requester when it will happen.	Network Engineer	☐
5.8	Implement the rule The Network Engineer adds the rule using the naming convention, puts the ticket number in the rule comment and sets an expiry date for temporary rules.	Network Engineer	☐
5.9	Test and confirm the change The Network Engineer tests the intended traffic and checks that nothing else broke, then the requester confirms the change works as needed.	Network Engineer	☐
5.10	Roll back if the test fails If the change does not work or breaks other traffic, the Network Engineer restores the backed-up configuration and records what happened in the ticket.	Network Engineer	☐
5.11	Update the rule register The Network Engineer adds the rule to the client's rule register with the ticket, requester, reason and review or expiry date, and updates the network documentation. Checkpoint: Every rule on the firewall can be traced to a register entry and a ticket.	Network Engineer	☐
5.12	Remove expired temporary rules The Security Engineer reviews the rule register monthly and has temporary rules removed when they expire, unless the client approves an extension.	Security Engineer	☐

6. Quality checks

- Every change was requested or approved by an authorized client approver.
- A configuration backup exists from before every change.
- No any-to-any or broad inbound rules exist without documented client risk acceptance.
- Every rule has a ticket number in its comment and an entry in the rule register.
- No temporary rule remains past its expiry date.

7. Records

- Firewall change request tickets with approvals
- Configuration backups before each change
- Client firewall rule register
- Monthly temporary rule review

8. KPIs

- Percentage of firewall changes with complete approvals
- Number of rules without a ticket or register entry
- Number of expired temporary rules still active
- Percentage of changes rolled back

9. Common mistakes

- Opening a port because an unverified email asked for it.

- Writing broad rules to save time instead of specific ones.
- Changing the firewall without a configuration backup.
- Adding vendor access for a project and never removing it.

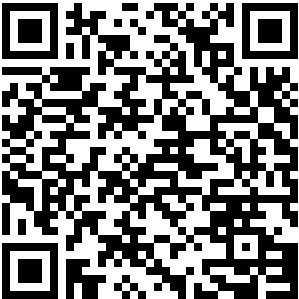
10. Revision history

Revision	Date	Description	Reviewed by
1.0	October 15, 2026	Initial release	Ilia Pirozhenko

Approval

Prepared by	Approved by	Date

This is a template. Adapt it to your organization, equipment and local regulations before use.



Scan for the latest version

Opens this template online, where you can download it again in Word, PDF, Excel or CSV — free, no sign-up.

Or [add it to Perfect Wiki](#) so your team can find it and ask questions about it in Microsoft Teams, Slack, kChat or Mattermost.