GSA IT

IT Security Procedural Guide:

Firewall and Proxy Change Request Process

CIO-IT Security-06-31

Revision 10

December 4, 2023

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – June 25, 2007		
1	Bo Berlas	Updated FW change request process.	Align with new IT Service Desk process.	Throughout
2	Bo Berlas	Updated IT security policy reference.	GSA Order CIO P 2100.1D was published on 06/21/2007	4
3	Bo Berlas	Updated FW change request form in Appendix A.	Change in process flow.	9
		Revision 2 – September 27, 2007		
1	Bo Berlas	Updated step 8 – destination email address for processing of firewall change requests.	Requested by GSA Firewall Team.	6
		Revision 3 – May 02, 2008		
1	Bo Berlas	Updated steps 3 and 8 in the firewall change request process to account for usage of CA Unicenter for ticket routing.	Processing tickets directly in CA Unicenter	5-6
2	Roy Iversen	Updated FW change request form in Appendix A	Change in required data. Clarification of process.	9
		Revision 4 – June 16, 2010		
1	Iversen	Updated “Firewall Change Process”. Emphasized that the request must be at least business 5 days prior to requested change. Changed web application scan from “OWASP Top 10” to “Standard” profile. Removed requirement to remediate all Medium Risk OS vulnerabilities, changed it to recommended. Specified that ISSMs can also submit FW requests. Clarification of verification or corrected vulnerabilities.	Clarifications and ease of process.	7
2	Iversen	Renamed “Emergency” requests to “Urgent” requests.	Name change	
3	Iversen	Clarified encryption requirements. Added “Scan Requirements” section. Included use of Core Impact for OS scanning. Changed web application scan from “OWASP Top 10” to “Standard” profile. Removed requirement to remediate all Medium Risk OS vulnerabilities, changed it to recommended.	Clarifications and ease of process.	
4	Iversen	Changed firewall form.	New form simplifies process	Appendix A
5	Iversen	Updated GSA Order Reference	New revision	6
6	Iversen	Updated cover	New cover sheet	1

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 5 – February 19, 2015		
1	Eriksen	Updated cover	New date and version	1
2	Eriksen	Updated Firewall Change Request process and add image showing Service Catalog	Change in process	6
3	Eriksen	All changes to the firewall access rules are processed as follows:	Change in process	6
4	Eriksen	Remove tool name from process	Removed reference to specific vulnerability scanning tool	7
5	Eriksen	Removed tool name from Operating System Vulnerability Scanning	Removed reference to specific vulnerability scanning tool	11
		Revision 6 – January 5, 2016		
1	Eriksen	Added image and information required to fill in the form	Added 2.0 Firewall Change Form	7 and 8
2	Eriksen	Removed quote from GSA Order CIO P 2100.1	Removed reference to avoid wrong information	6
3	Eriksen	Replaced Security Operations with Security Operations	Shorten the name	9-12
		Revision 7 – June 8, 2016		
1	Eriksen	Add language for Desktop firewalls	To cover Desktop Firewalls	7
2	Cozart-Amos/ Klemens	Converted to latest format and style	Conversion to latest format and style	All
		Revision 8 – June 6, 2018		
1	Feliksa/Eriksen	Updated format, structure, and style.	Biennial update.	Throughout
		Revision 9 - December 21, 2020		
1	Eriksen/ Quintananieves	Primary updates consisted of: • Clarified steps on requesting firewall changes • Added cybersecurity directives requirements • Established the proxy change request process/changed name of guide to include this process • Added a section on restricting privileged users to trusted sites	Biennial update.	Throughout

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 10 - December 4, 2023		
1	Peters	• Updated process for changes to firewall access rules.	Periodic update.	Throughout
2	McCormick	• Replaced images to reflect the current IT Service Desk images • Added tables describing information required for Firewall Change Request Forms. • Updated format to align with current GSA template for guides.		Throughout

Approval

IT Security Procedural Guide: Firewall and Proxy Change Request Process, CIO-IT Security 06-31, Revision 10, is hereby approved for distribution.

DocuSigned by:

Bo Berlas

FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Security Operations Division (ISO) at secops@gsa.gov.

Table of Contents

1 Introduction

The General Services Administration (GSA) enterprise firewalls are an integral facet of GSA's "defense-in-depth" strategy in securing agency information and systems. They centrally control access to systems and devices across GSA. It is imperative that strict guidelines be established and followed to ensure that only necessary and effective rules are applied to the firewall rule-base. The following sections detail the required process for all changes to the GSA firewall rule-base.

1.1 Purpose

This guide documents the firewall change request process at GSA. The guide describes the steps in the process including request initiation, vulnerability and application security scanning, and approvals.

1.2 Scope

The GSA firewall change request procedures apply to all individuals who request changes to a firewall rule-base.

1.3 Policy

GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," contains the following policy statements regarding firewall change requests.

Chapter 4: POLICY FOR PROTECT FUNCTION

1. Identity Management, Authentication and Access Control

pp. OCISO must approve all requests for access through the GSA Firewall. Firewall change requests must follow the process outlined in GSA CIO-IT Security-06- 31: Firewall Change Request. This includes changes to desktop firewall and intrusion prevention systems.

qq. OCISO will block access to all external sites deemed to be a security risk to GSA. Exceptions to this policy must be approved by the CISO.

1.4 References

Federal Laws, Standards, and Publications:

- Federal Information Processing Standard (FIPS) Publication (PUB) 140-3, "Security Requirements for Cryptographic Modules"
- Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Directives

GSA Policies, Procedures, and Guidance:

- GSA CIO Order 2100.1, "GSA Information Technology (IT) Security Policy"

The document below is available on the GSA IT Security Procedural Guides page.

- CIO-IT Security-09-43: Key Management
- CIO-IT Security-17-80: Vulnerability Management Process

The document below is available on the restricted GSA IT Security Technical Guides and Standards page.

- CIO-IT Security-14-69: SSL/TLS Implementation

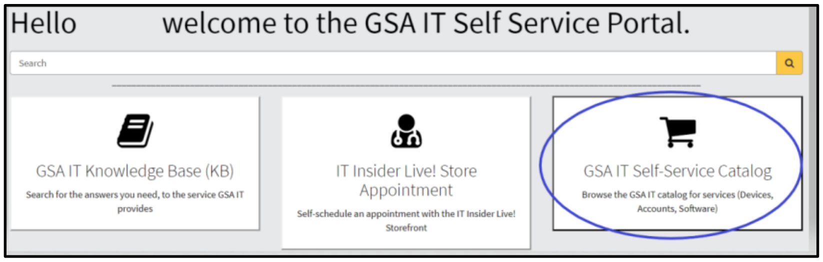
2 Firewall Change Request Process

The Firewall Change Request Form is available via the GSA IT Service Desk. This form is used for both desktop and network firewall changes. It is designed to assist in collecting the necessary information for the GSA IT Security Operations (SecOps) team to evaluate, approve, and implement firewall change requests. Users with an active gsa.gov account and a “business-need” may request firewall changes. Additionally, the following minimum requirements must be met:

- All updates, development and configuration for the components involved (hardware/servers/sites/etc.) must be complete and a code freeze enforced.
- All components involved must be available and ready for evaluation.

Follow these steps to access the Firewall Change Request Form:

1. Navigate to the GSA IT Self Service Portal.
2. Select **Self-Service Catalog**.



Hello welcome to the GSA IT Self Service Portal.

Search

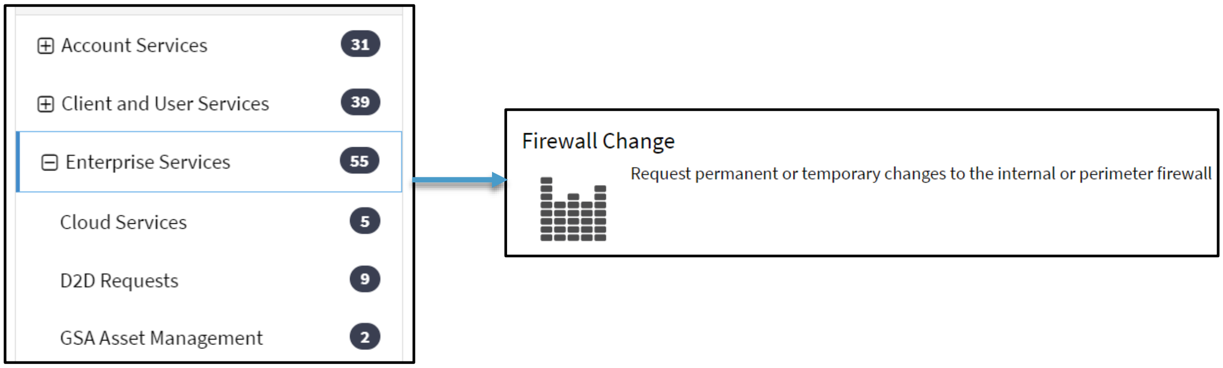
GSA IT Knowledge Base (KB)
Search for the answers you need, to the service GSA IT provides

IT Insider Live! Store Appointment
Self-schedule an appointment with the IT Insider Live! Storefront

GSA IT Self-Service Catalog
Browse the GSA IT catalog for services (Devices, Accounts, Software)

Figure 2-1. Self-Service Catalog

3. Select **Enterprise Services** from the navigation menu on the left, scroll down, and then on the right click on the **Firewall Change** card.

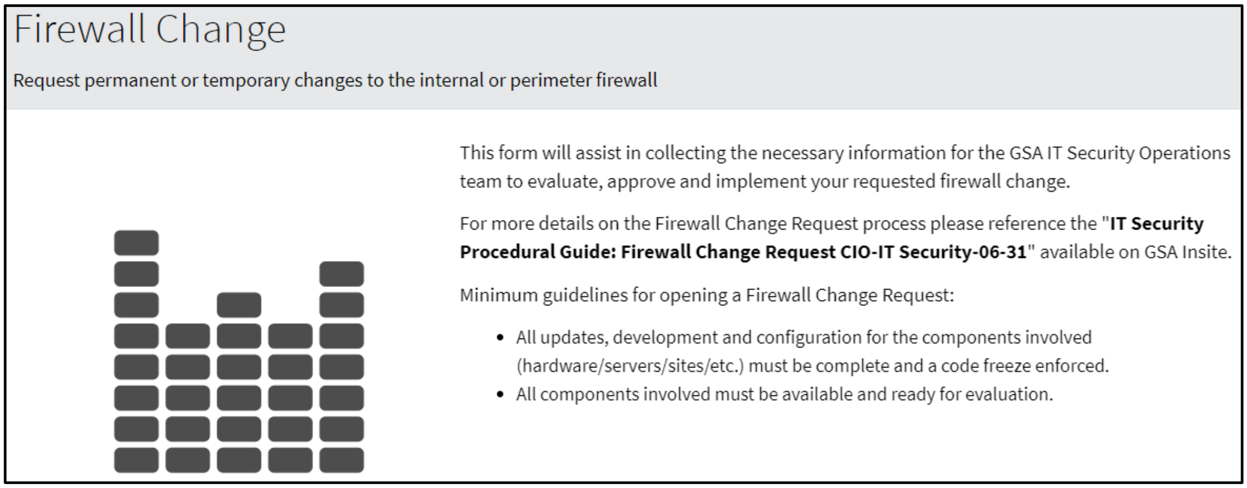


⊞ Account Services	31
⊞ Client and User Services	39
⊟ Enterprise Services	55
Cloud Services	5
D2D Requests	9
GSA Asset Management	2

Firewall Change
Request permanent or temporary changes to the internal or perimeter firewall

Figure 2-2. Enterprise Services and Firewall Change

The Firewall Change Request Form appears.



Firewall Change

Request permanent or temporary changes to the internal or perimeter firewall

This form will assist in collecting the necessary information for the GSA IT Security Operations team to evaluate, approve and implement your requested firewall change.

For more details on the Firewall Change Request process please reference the "**IT Security Procedural Guide: Firewall Change Request CIO-IT Security-06-31**" available on GSA Insite.

Minimum guidelines for opening a Firewall Change Request:

- All updates, development and configuration for the components involved (hardware/servers/sites/etc.) must be complete and a code freeze enforced.
- All components involved must be available and ready for evaluation.

Figure 2-3. Firewall Change Request Form Introduction

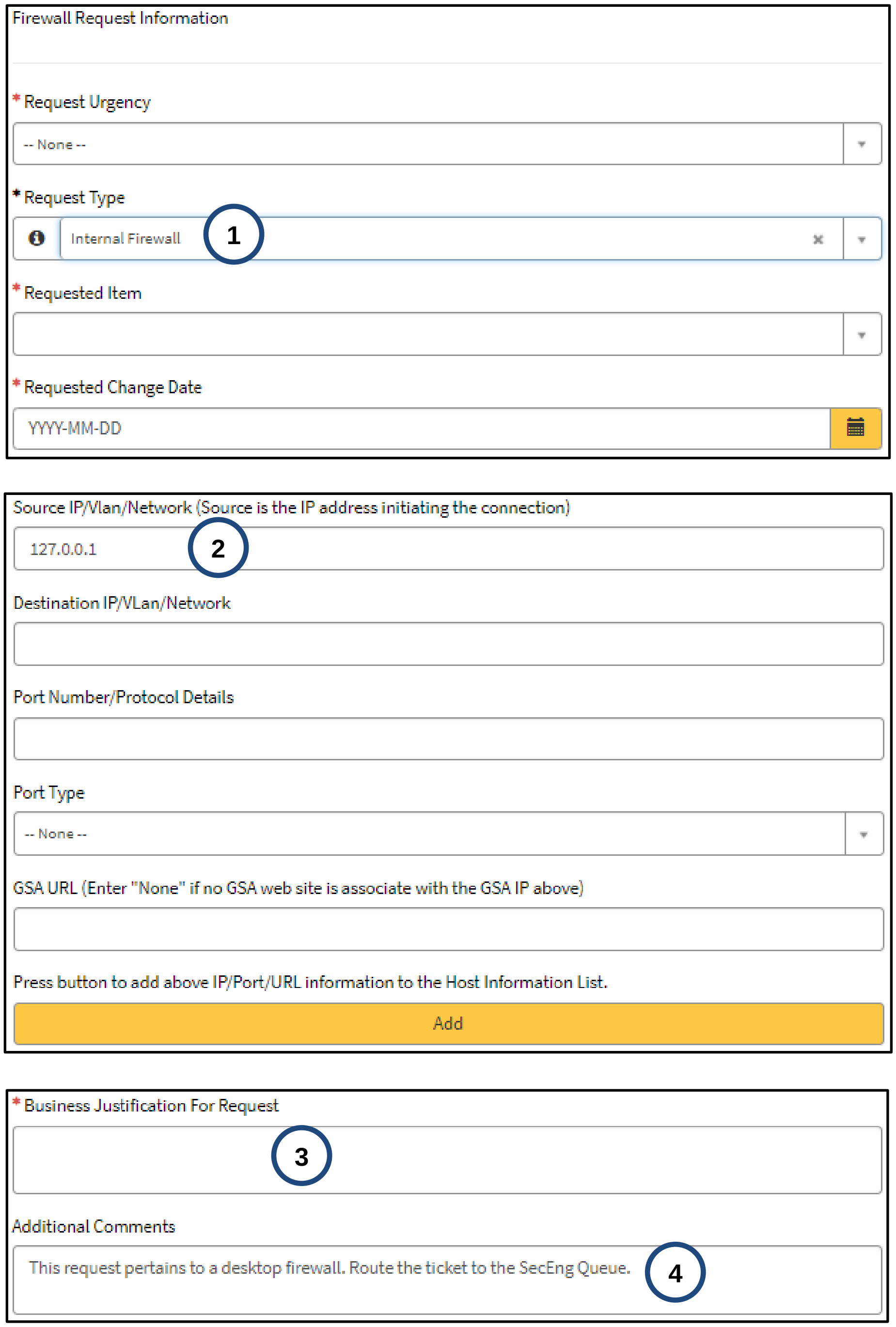
2.1 Desktop Firewall Changes

Changes to a user's Windows Firewall must be coordinated through the GSA Office of the Chief Information Security Officer (OCISO) Security Engineering Division (ISE).

The specific information required to identify the request as a Desktop Firewall Change is described in Table 2-1. Numbers in the Form Line column correlate to the numbered steps in Figure 2-4. All required fields in the ServiceNow ticket must be completed before requesting the change in.

Table 2-1. Desktop Firewall Change Request Information

Form Line	Information Requested	Description
1	Request Type	Select **Internal Firewall** in the **Request Type** dropdown.
2	Source IP/VLAN/Network	Enter **127.0.0.1** as the IP address **Note**: Source is the IP Address initiating the connection.
3	Business Justification for Request	Within the **Business Justification for Request** field, explain why the change is required.
4	Additional Comments	Add the following note within the **Additional Comments** field: "This request pertains to a desktop firewall. Route the ticket to the SecEng Queue."



Firewall Request Information

* Request Urgency

-- None --

* Request Type

Internal Firewall

* Requested Item

* Requested Change Date

YYYY-MM-DD

Source IP/Vlan/Network (Source is the IP address initiating the connection)

127.0.0.1

Destination IP/VLan/Network

Port Number/Protocol Details

Port Type

-- None --

GSA URL (Enter "None" if no GSA web site is associate with the GSA IP above)

Press button to add above IP/Port/URL information to the Host Information List.

* Business Justification For Request

Additional Comments

This request pertains to a desktop firewall. Route the ticket to the SecEng Queue.

Figure 2-4. Desktop Firewall Request Form

2.1.1 Completing the Change Request

When the Change Request Form is complete, at the bottom of the request form click on **Order Now** to submit the ticket or **Add to Cart** to save the request for later submission.

Once the Service Desk ticket has been created and submitted, send an email to SecEng@gsa.gov, including the ticket number. Requests will normally be reviewed within five business days.

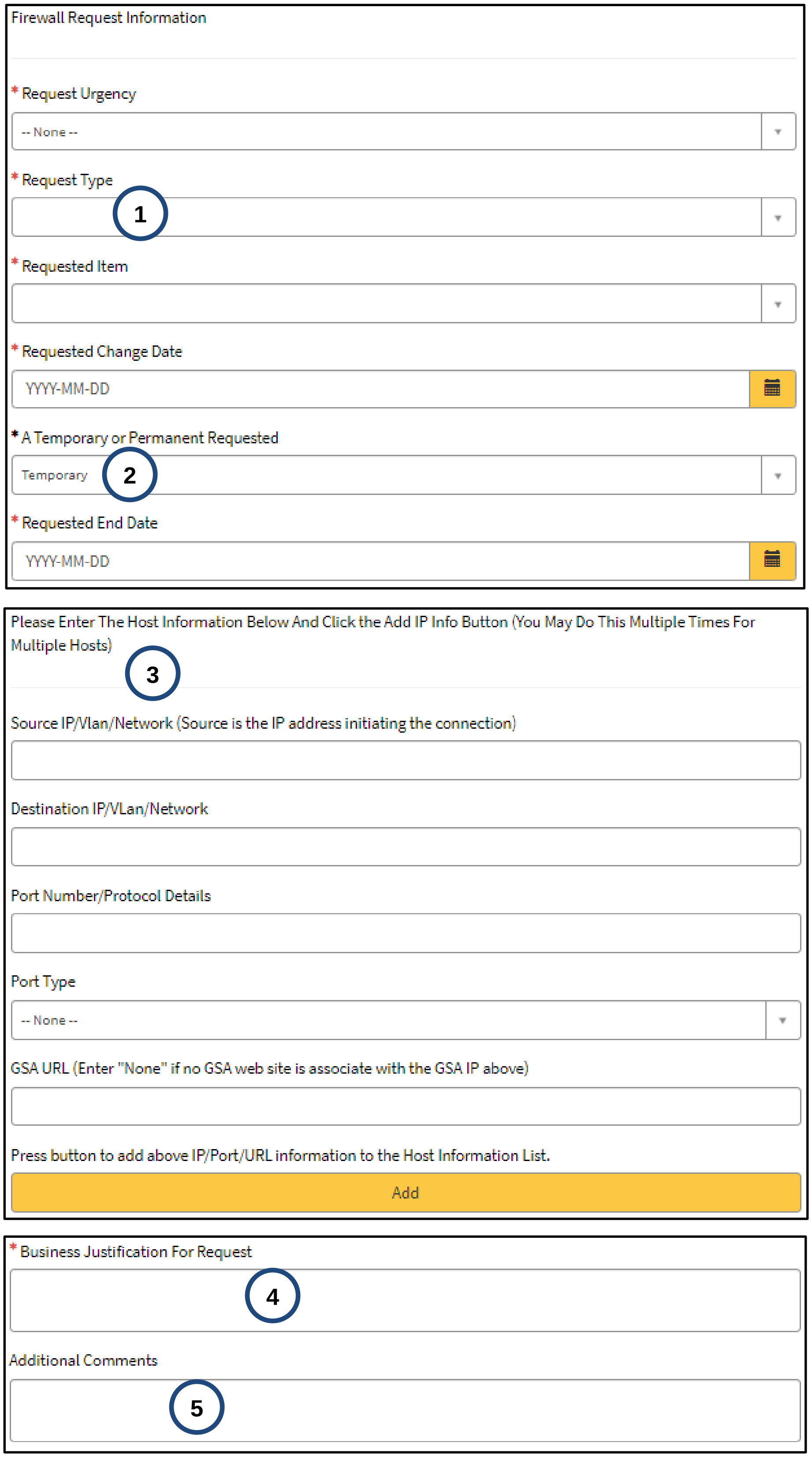
2.2 Network Firewall Changes

When a change to GSA's external (perimeter) or internal firewall(s) is required, a Service Catalog Request must be completed. For external requests, the Information System Security Officer (ISSO) or Information System Security Manager (ISSM) must submit the request **at least 5 business days ahead of the required change date**.

The specific information required to complete the request is describe in Table 4-1. Numbers in the Form Line column correlate to the highlighted steps in Figure 4-1.

Table 2-2. Network Firewall Change Request Information

Form Line	Requested Information	Description
1	Request Type	In the Request Type dropdown select the type of **Internal** or **Perimeter** Firewall request.
2	A Temporary or Permanent Requested	If the change is **Temporary**, provide the **Requested End Date**.
3	Enter the Host Information Add IP Info	**NOTE**: You may complete this process multiple times for multiple hosts. Click on the yellow **Add** bar to add the previously entered IP/Port/URL information to the Host Information List.
4	Business Justification for Request	Within the **Business Justification for Request** field, explain why the change is required.
5	Additional Comments	Add the following note within the **Additional Comments** field: "This request pertains to a network firewall. Route the ticket to the SecEng Queue.



Firewall Request Information

* Request Urgency

-- None --

* Request Type

* Requested Item

* Requested Change Date

YYYY-MM-DD

* A Temporary or Permanent Requested

Temporary

* Requested End Date

YYYY-MM-DD

Please Enter The Host Information Below And Click the Add IP Info Button (You May Do This Multiple Times For Multiple Hosts)

Source IP/Vlan/Network (Source is the IP address initiating the connection)

Destination IP/VLan/Network

Port Number/Protocol Details

Port Type

-- None --

GSA URL (Enter "None" if no GSA web site is associate with the GSA IP above)

Press button to add above IP/Port/URL information to the Host Information List.

* Business Justification For Request

Additional Comments

Figure 2-5. Network Firewall Request Form

2.2.1 Completing the Change Request

When the Change Request Form is complete, at the bottom of the request form click on **Order Now** to submit the ticket or **Add to Cart** to save the request for later submission.

Once the Service Desk ticket has been created and submitted, send an email to SecEng@gsa.gov, including the ticket number. Requests will normally be reviewed within five business days.

2.3 Processing the Change Request

- For **external firewall requests**, steps 1 to 8 apply.
- **Internal firewall requests** typically only include steps 1, 2, 7, and 8 (e.g., Creation of the request -> Approval by ISSO or ISSM -> Firewall Team makes the change -> Ticket update).

Changes to the firewall access rules are processed as follows:

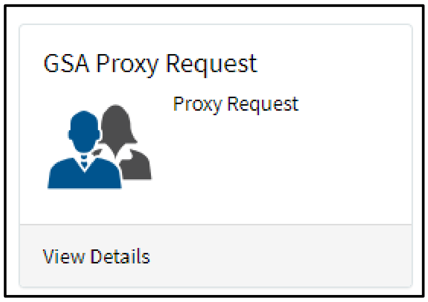
1. Individuals requiring a change to a firewall rule-base must submit a request via the GSA IT Self-Service Catalog as described in Section 2. The associated system ISSOs or ISSMs must approve the change request.
2. After the ISSM or ISSO approves the request, it is routed to the appropriate team’s queue, which depends on whether the request is Perimeter or Internal.
3. If the request is Perimeter/External:
    a. Tickets are generated with the CISO.OSScanTeam and CISO.WebScanTeam for vulnerability scanning.
    b. OS Vulnerability and Web Scans (as needed) are then conducted against the GSA hosts or devices as necessary with authenticated scanning. (**Note**: It is the requestor’s responsibility to provide credentials if required during the scans.)
4. Any required system scanning will be available within the applicable vulnerability and compliance scanning tool used by SecOps. Upon completion of scans, SecOps will forward the results of the scanning activities to the ISSO for remediation and copy the ISSM if remediation is required. The system should be free of High and Critical risk vulnerabilities prior to SecOps approval. See Section 4.2 for details.
5. Upon correction of the identified operating system (OS) and application vulnerabilities, SecOps will verify the corrective action, either manually or by rescanning.
6. Upon successful mitigation of identified vulnerabilities and ISSM approval, SecOps will close the scan tickets as complete and the Firewall Request will be generated within the **CISO.Firewall** queue with approval to process the request or deny the request.
7. Upon receipt of the approved Firewall Change Request from SecOps, the Firewall Team will make the requested change at the appropriate time and mark the IT Service Desk Ticket as Resolved.
8. SecOps will update the ticket to document the Service Catalog request details, approval, and the implemented firewall change.

2.4 Proxy Change Requests

GSA has internal proxy servers that may require special firewall requests to allow access to internal/external resources. The information required to complete the Proxy Change Request is described below.

Navigate to the GSA IT Self Service Portal

1. Select **Self-Service Catalog** as shown in Figure 3-1.
2. Select **Enterprise Services** from the navigation menu on the left and then click on the **GSA Proxy Request** card as shown in Figure 2-6.

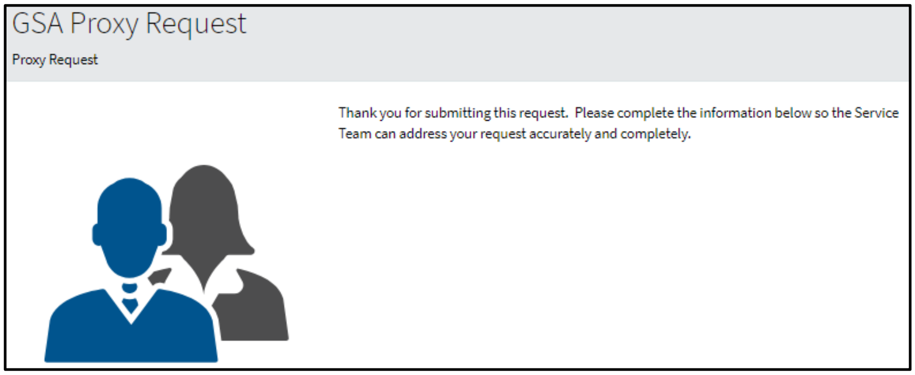


GSA Proxy Request

Proxy Request

Figure 2-6. Proxy Request Card

The Proxy Request Form appears as depicted in Figure 2-7. The information required by the form is similar to the information required in the Firewall Change Request form.



GSA Proxy Request

Proxy Request

Thank you for submitting this request. Please complete the information below so the Service Team can address your request accurately and completely.

Figure 2-7. Proxy Request Form Introduction

After completing the form, at the bottom of the request form click on **Order Now** to submit the ticket or **Add to Cart** to save the request for later submission.

2.5 Restricting Privileged Users to Trusted Sites

To approve a new domain for privileged users to access a trusted site, employees and contractors with privileged accounts (i.e., Short Name Accounts (SNAs)) must submit a GSA Proxy Request through the GSA Self-Service Catalog. This process applies if privileged users are working with a vendor or new application that requires access to a specific domain from an SNA account and the domain has not already been approved and requires approval by the ISSO/ISSM and the Director of Security Operations or CISO. Before submitting this request, refer to the full list of approved Proxy Whitelisted Domains. If the requested site is already approved, then a new Service Catalog request is not required.

3 Prioritization of Firewall Change Requests

The Firewall Change Request form and the Proxy Request form offer two alternatives in the **Request Urgency** dropdown: normal and emergency.

3.1 Normal Change Requests

Normal or routine firewall change requests require **at least 5 business days advance notice prior to the requested change date**. During this period, SecOps will conduct required OS and application testing, with retesting following vulnerability mitigation (if any). SecOps will coordinate any necessary approvals

Firewall change requests may exceed 5 business days if coordination with the ISSM, ISSO, and/or applicable system points of contact (POCs) becomes an issue and/or it takes a long time to mitigate vulnerabilities.

3.2 Urgent/Emergency Change Requests

In urgent situations, firewall change requests supporting key business functions may be communicated verbally with the OCISO Security Operations (ISO) Director. These requests must be pre-approved by the System Owner, Program Manager, or ISSM and followed up with appropriate documentation. SecOps will put forth a best effort to facilitate the completion of urgent change requests. Such requests must undergo OS and application security testing and have all High and Critical Risk vulnerabilities mitigated.

4 Reviewing the Firewall Change Request

4.1 Technical Review of the Firewall Change Request

Upon receipt of the completed Firewall Change Request Form, SecOps will review the request to ensure that only the required minimum access is requested and that insecure ports and/or services are not opened to the Internet.

As a rule, services such as file transfer protocol (FTP), Telnet, and other protocols that send sensitive data (e.g., log-in/authentication data) in the clear are generally not approved for perimeter changes.

Encryption must use FIPS 140-3/140-2[1] certified encryption modules. This implies applicability to transport layer security (TLS), as secure sockets layer (SSL) encryption is not FIPS certified. For more information, download the following GSA IT procedural guides.

- CIO-IT Security-09-43: Key Management
- CIO-IT Security-14-69: SSL/TLS Implementation

[1] NIST has issued FIPS 140-3 and no longer accepts FIPS 140-2 modules for validation. However, previously validated 140-2 modules will be accepted through September 22, 2026. For additional information see the NIST Cryptographic Module Validation Program website.

4.2 System Scan Requirements

OS vulnerability scans are normally required for all perimeter requests, and web application scanning is normally required for any request for HTTP or HTTPS protocols.

4.2.1 Operating System Vulnerability Scanning

OS vulnerability scans will be conducted with authentication where applicable. The credentials used typically require administrator-level privileges to run successful scans.

SecOps has preconfigured credentials that should be used for this. Contact the SecOps Scan Team for details.

All of the following conditions should be satisfied prior to SecOps approval:

1. The system is included in a Federal Information Security Modernization Act (FISMA) inventory as listed in the GSA Enterprise Architecture Analytics and Reporting (GEAR) FISMA inventory and scanned as part of the enterprise vulnerability management program (see CIO-IT Security-17-80), AND
2. There are no outstanding Critical risk vulnerabilities with Common Vulnerability Scoring System (CVSS) base score 9.0, AND
3. There are no active High risk vulnerabilities with CVSS base score 7.0 older than 14 days.

Each request is evaluated individually, and approval is at the discretion of the SecOps team.

4.2.2 Web Application Scanning

If applicable, change requests involving HTTP and/or HTTPS access will be scanned using GSA's vulnerability scanning tool.

4.2.3 Cybersecurity Directives Compliance Scanning

All Firewall Requests that will open a system to the public Internet must be scanned for compliance with all Cybersecurity and Infrastructure Security Agency (CISA) Directives.

4.3 Exceptions to Scanning

Scanning may be waived at the discretion of the CISO or Director of SecOps or their delegated staff. Typically, one of the following two criteria options must be satisfied in order for scanning to be waived:

Criteria #1

1. The request is to change or add a single Internet IP or a limited Internet IP range to an existing firewall rule, AND
2. The system is included in GSA's FISMA inventory and scanned as part of the enterprise vulnerability management program, AND
3. There are no Critical risk vulnerabilities (i.e., CVSS base score 9.0 or above), AND
4. There are no High risk vulnerabilities (i.e., CVSS base score 7.0 or above) older than 14 days.

OR

Criteria #2

The request is to make a minor change to an existing firewall rule that was put in place within the last 45 days and the system does not have any known outstanding vulnerabilities