Firewall Policy

Effective Date:
August 08, 2025

Category:
Security

Scheduled Review:
August 2026

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Document Control

This document replaces, in its entirety, the *Firewall Policy,* dated January 6, 2025.

3. Purpose

This Information Technology Policy (ITP) establishes an enterprise-wide security policy designed to augment privacy, authentication, and security via deployment of network firewalls.

4. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the commonwealth network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

5. Policy

For definitions found within this document, refer to the *IT Policy Glossary.*

5.1 Enterprise Policy for Agency Firewalls

With respect to agency network gateway firewalls:

- All agencies connected to the commonwealth MAN are required to implement a firewall at the gateway to their networks.
- At a minimum, agencies shall adhere to the baseline firewall policy rule set as identified in Section 5.2 below.
- Additional rules and permissible access may be added to the baseline firewall policy rule

set and implemented to provide network accessibility to meet the requirements of the agency.
- The agency's firewall will work in conjunction with the commonwealth enterprise firewalls, Network Intrusion Prevention Systems (NIPS), Network Intrusion Detection Systems (NIDS), and Host Intrusion Prevention System (HIPS) to provide the necessary security for the agency network.
- Existing non-standard and stand-alone, or Agency/Delivery Center specific firewalls may remain in place, but any new firewall shall comply with the firewall standards defined in this ITP.

The Office of Administration/Office for Information Technology (OA/IT) will function as the coordination point for all firewalls that agencies wish to establish between the agency's Local Area Networks (LANs) and the commonwealth MAN (including wide area connections). Agencies shall contact the OA, Enterprise Security Operations Section (oa-security@pa.gov) prior to purchasing and installing firewalls.

Agencies shall coordinate all firewall implementations with the Enterprise Security Operations section to ensure that the appropriate rule sets are in place to maintain the highest level of security and to support interoperability between multiple firewalls. This policy does not preclude any agency from utilizing router filters in conjunction with firewalls to enhance network security. Agencies shall refer to the *Firewall Product and Compliance Standard* for direction on product standards for Agency firewalls.

5.2 Enterprise Firewall Rule Set

The baseline firewall rule denies all services. *Enterprise Firewall Rule Set Standard* identifies those services that are permitted and provides information related to the Enterprise GeoIP blocking service. *Enterprise Firewall Rule Set Standard* identifies the most common services used for communications within the commonwealth's environment. These services are primarily agency to enterprise services and enterprise services to agency in nature.

Agencies shall perform an audit to identify all "Agency to Agency" and "Agency to Enterprise Service" application protocols to ensure those specific port requirements are documented and then applied to the agencies firewall(s). Agencies shall refer to the *Encryption Policy* for requirements on encrypting "Agency to Agency" communications.

5.3 Enterprise Web Application Firewall

Compliance rule sets will be invoked by the Enterprise Information Security Office (EISO) to automatically block attacks coming from the Internet.

All internet-facing web applications which contain **Sensitive Security, Protected, or Privileged Information**, as defined by the *Data Classification Policy,* are required to utilize a WAF.

All Internet-facing web applications which contain **Prerequisite-Required Information or Public Records**, as defined in the *Data Classification Policy,* are recommended to utilize a WAF. Agencies shall refer to the *Firewall Product and Compliance Standard* for a current listing of WAF standards.

Agencies shall use the Enterprise WAF offering unless there is a verified technical reason the

Enterprise offering will not work.

All existing Internet-facing web applications containing Sensitive Security, Protected, or Privileged Information, as defined in the *Data Classification Policy,* not currently secured by a WAF shall adhere to this guidance prior to the next scheduled annual review (12 months) of this ITP. Any applications not in compliance after 12 months will require an approved IT policy exception and Risk Assessment and Acknowledgement document (*IT Vendor Risk Management Reporting Procedure*).

5.4 Web Application Security Controls

Other WAF security control standards include, but are not limited to, the following:

- All WAF traffic shall be HTTPS capable of providing Distributed Denial of Service (DDoS) protection.
- The WAF may not disallow an authorized request from an Internet user and may not affect legitimate business traffic in the IT infrastructure while protecting web applications.
- The WAF default configuration must be able to monitor and prevent specific web application attacks until emergency patches and/or source-code changes can be made to the vulnerable web application.
- The default web application rule configuration must be able to monitor and immediately block types of Web attacks targeting the web application.
- An SSL certificate is required by the WAF to inspect data passed between the web servers.
- The WAF must be able to track, log, and inspect the following information relating to the web applications access by the end-user:
  - Application layer network traffic;
  - External and internal user sessions;
  - External and internal user-encrypted sessions;
  - Simulated attacks;
  - Blocked attacks; and
  - HTTPS, Proxy error logging to Security Information and Event Management (SIEM).
- WAF requires high availability architecture.
- WAF logs (including original source IPs) shall be sent to the enterprise SIEM.
- XFF header must be enabled from the original source to the backend application. This includes any load balancers in place.

5.5 Monitoring

All WAF implementations are subject to Enterprise audit on a random or as-needed basis.

5.6 Enterprise Content Filtering Standards

All internet traffic will be directed through the Commonwealth's Internet Access Control and Content Filtering (IACCF) implementation.

HTTPS inspection of outbound internet traffic is enabled for most content filtering service categories except for those IACCF categories identified in *Enterprise Content Filtering Standard*, which are not inspected due to the sensitivity of the internet content. The decryption of HTTPs traffic allows security tools to analyze traffic for threats and block them as necessary.

The Enterprise Information Security Office (EISO) shall maintain the *Enterprise Content Filtering Standard* with which agencies must comply. Agencies may implement more restrictive content filtering rules, provided they do not conflict with the requirements outlined in this Standard.

Agencies that have business requirements conflicting with the IACCF implementation minimum filtering policies as detailed in *Enterprise Content Filtering Standard* shall follow the IT Policy Exemption process as noted in section 7.

6. Contact

Questions or comments may be directed via email to OA, IT Policy.

7. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

8. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document
Revision	08/08/2025	Added document control section Removed non-essential content Added additional requirements for WAFs related to DDoS protection and sending logs to enterprise SIEM. Misc. clarifications