Policy & Standard Background

Name: Firewall Standard

New

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

The 2017 version of OCIO 141.10 section 5.1.2 describes the minimum agency firewall configuration requirements. This new standard builds upon this by adding requirements from NIST 800-41, Guidelines on Firewalls and Firewall Policy.

What is the business case for the policy/standard?

- Ensure agency configure their firewalls to per the requirements in this standard.
- Ensure the restriction of firewall rule access to authorized personnel only.
- Manage firewall configuration in accordance with this standard.

What are the key objectives of the policy/standard?

The key objective of this standard is that agencies manage their firewall consistent with industry standards.

How does policy/standard promote or support alignment with strategies?

This policy ensures that agency environments, and those environments which interconnect agencies to the State Government Network, are protected from potentially threatening network traffic.

What are the implementation considerations?

Agencies will need to ensure implementation of:

- Configuration management system to manage firewall rules.
- A firewall review process to occur during firewall ruleset changes.
- Enforcement of authentication method for users with administrative access to firewall management console.

How will we know if the policy is successful?

Below are the success indicators for the Firewall Standard:

- Auditable records of firewall rule and configuration review meetings.
- Auditable logs showing that administrative users authenticated to the firewall management console using multifactor authentication.

State CIO Adopted:
TSB Approved:
Sunset Review:

WaTech
Washington Technology Solutions

FIREWALL STANDARD

Replaces:
IT Security Standard 141.10 (5.1.2)
December 11, 2017

See Also

RCW 43.105.450 Office of Cybersecurity
RCW 43.105.054 OCIO Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"

1. **Agencies must implement and annually review the baseline firewall security configuration requirements described below:**

    a. Change vendor-supplied default passwords and firewall configurations.

    b. Remove or disable all unnecessary default accounts before installing a firewall on the network.

    c. All firewall systems must fail in a closed state, allowing no traffic to pass.

    d. All firewalls must support inbound and outbound IPv4 and IPv6 traffic.

    e. All firewalls must generate event logs resulting from the creation of sessions and denial of traffic where appropriate.

    f. The firewall configuration must be reviewed at least annually, or more frequently based on agency business requirements.

2. **Agencies must institute network access and authorization controls to ensure that only authorized administrators have access to change firewall rules. The administrative interface to the firewall must support the following:**

    a. Identification and authentication of firewall administrators.

    b. Encryption of administrative traffic over a separate management network.

    c. Always use Multifactor Authentication (MFA) for Internet-facing firewall administrative interfaces.

    d. Agency-managed firewalls must utilize MFA to access the firewall management interface. This could be either through an isolated and secured management network or when the firewall is accessed directly.

    e. Local, physical console access does not require MFA. Configurations for local console access accounts to support emergency local access must be configured with recommended secure configurations based on vendor guidance or the CIS benchmarks per the Configuration Management Standard. Physical access to the firewall must be tightly controlled with locked cabinets or other datacenter environment access controls to prevent unauthorized access.

    f. Access to the administrative interfaces will generate an access audit log.

3. **Agencies must implement the following minimum technical security standards when configuring its firewall rulesets.**

   a. Block traffic originating from outside the agency network if it contains addresses within the agency network.

   b. Block services, protocols, and ports not specifically allowed by the agency security policy.,

   c. Allow only agency-approved out-going network traffic from the internal network to the DMZ or Internet. Approved out-going network traffic may include agency communications to other agencies, service providers, or authorized destinations.

   d. Allow only WaTech and agency-approved in-coming network traffic to the internal network from the DMZ, Internet, wireless networks and SGN. Approved in-coming network traffic may include communications from other agencies, service providers, or authorized sources.

   e. Block traffic with invalid incoming source or outgoing destination addresses. Examples of relatively common invalid IPv4 addresses are 127.0.0.0 to 127.255.255.255 (also known as the localhost addresses) and 0.0.0.0 (interpreted by some operating systems as a localhost or a broadcast address). These have no legitimate use on a network. Also, traffic using link-local addresses (169.254.0.0 to 169.254.255.255) should be blocked.

   f. Block traffic with private incoming source or outgoing destination addresses to or from the Internet. The most common type of invalid external addresses is an IPv4 address within the ranges in RFC 1918, Address Allocation for Private Internets, that are reserved for private networks. These ranges are 10.0.0.0 to 10.255.255.255 (10.0.0.0/8 in Classless Inter-Domain Routing [CIDR] notation), 172.16.0.0 to 172.31.255.255 (172.16.0.0/12), and 192.168.0.0 to 192.168.255.255 (192.168.0.0/16).

   g. Changes to the firewall ruleset must be reviewed when they are proposed. This review must align with the agency's change management policy. This review may require WaTech approval as appropriate.

REFERENCES

1. NIST 800-41 - Guidelines on Firewalls and Firewall Policy
2. Definitions of Terms Used in WaTech Policies and Reports
3. NIST Cybersecurity Framework Mapping:
   - Protection.Data Security-5: Protections against data leaks are implemented.
   - Protection.Access Control-5: Network integrity is protected (e.g., network segregation, network segmentation).
   - Protection.Protective Technology-4: Communications and control networks are protected.

CONTACT INFORMATION

- For questions about this policy, please contact the WaTech Policy Mailbox.
- To request a Security Design Review, please contact the Security Design Review Mailbox.