Office of Inspector General | United States Postal Service

Audit Report

Review of Perimeter Firewalls

Report Number IT-AR-18-003 | August 24, 2018

Table of Contents

Highlights

Objective

Our objective was to determine whether the network perimeter firewalls are properly configured and functioning to safeguard information technology (IT) according to Postal Service standards and industry best practices.

> *" Perimeter firewalls are the first line of defense of an organization's IT network."*

Perimeter firewalls are the first line of defense of an organization's IT network. They are essential components for detecting and protecting the network by blocking unnecessary incoming traffic to publicly available systems.

During fiscal year 2017, the Postal Service's [redacted] in revenue. Protecting systems connected to the Internet is critical to the security posture and financial well-being of the Postal Service. An accurate inventory of publicly available systems and associated ports helps an organization maintain visibility and control of network traffic using the firewalls.

What the OIG Found

The Postal Service network perimeter firewalls are [redacted]

We found the Postal Service [redacted] including subnets (a smaller network inside a larger network) and ports (a number used to uniquely identify a transaction by specifying network services). Additionally, administrators did [redacted]

[redacted]

These issues occurred because Postal Service procedures are not adequate to identify an inventory of all publicly available subnets and ports. In addition, the firewall review process does not adequately define procedures to identify and remove rules that could grant inappropriate access to the network. Rulesets were not reconciled when the firewalls were migrated from different vendors. Additionally, management did not prioritize [redacted]

The absence of an accurate inventory prevents an organization from maintaining visibility and control of network traffic with the firewalls. As a result, the firewalls [redacted]

When firewall security controls are not managed effectively:

- [redacted]
- [redacted]

When rulesets are not reconciled, overlapping rules occur. Overlapping rules could be obsolete, conflicting or redundant, which could negatively impact network performance. This could also introduce challenges to managing firewalls in an effective manner.

When firewalls are not configured to [redacted]

What the OIG Recommended

We recommended management:

1

ENHANCE PROCEDURES FOR IDENTIFYING ALL PUBLICLY AVAILABLE SYSTEMS AND ALL TCP PORTS.

2

IDENTIFY AND DOCUMENT ALL PUBLICLY AVAILABLE SYSTEMS AND ALL TCP PORTS.

3

ENHANCE PROCEDURES AND USE THE APPROPRIATE TOOLS FOR [redacted] TO THE POSTAL SERVICE NETWORK.

4

EVALUATE THE FIREWALL CONFIGURATIONS MONTHLY, AS REQUIRED BY POLICY, AND CONFIGURE PERIMETER FIREWALLS ACCORDING TO INTERNAL HARDENING STANDARDS.

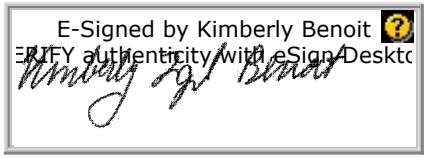
Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

August 24, 2018

MEMORANDUM FOR: JEFFREY C. JOHNSON
VICE PRESIDENT, INFORMATION TECHNOLOGY

GREGORY S. CRABB
VICE PRESIDENT, CHIEF INFORMATION SECURITY



FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology

SUBJECT: Audit Report – Review of Perimeter Firewalls
(Report Number IT-AR-18-003)

This report presents the results of our audit of U.S. Postal Service Perimeter Firewalls (Project Number 18TG004IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Jason Yovich, Director, Information Technology, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the U.S. Postal Service's Perimeter Firewalls (Project Number 18TG004IT000). Our objective was to determine whether the perimeter firewalls are properly configured and functioning to safeguard information technology (IT) operations according to Postal Service standards and industry best practices.

> *" The Postal Service is committed to creating and maintaining an information security environment to safeguard the confidentiality, integrity, and availability of its information. "*

Background

The Postal Service is committed to creating and maintaining an information security environment to safeguard the confidentiality, integrity, and availability of its information. Firewalls protect systems connected to the Internet and are critical to the security posture and financial well-being of the Postal Service. During fiscal year (FY) 2017, the Postal Service's [redacted] in revenue.

Firewalls are the first line of defense in an organization's IT network. They are essential components of detecting and protecting the network from potentially dangerous content and intrusion attempts. Firewalls block unnecessary incoming network traffic from accessing internal networks and hosts. For example, in 2017, Postal Service firewalls blocked 5,000 malware attempts. Firewalls also restrict outgoing network traffic from accessing undesirable external networks and hosts. It is critical for the Postal Service to safeguard its sensitive information and reduce the risk of unauthorized access to data and IT operations.

Finding #1: Inventory Management

The Postal Service does not maintain an accurate inventory of network information resources,[1] which includes subnets[2] and ports[3] that should be protected by firewalls. Management only provided a list of [redacted] Service policy states that management is responsible for maintaining an accurate inventory of Postal Service network information resources.[4]

This issue occurred because Postal Service procedures specify scanning a subset of available Transmission Control Protocol (TCP)[5] ports rather than the entire range of ports. Scanning only a subset prevents the identification of all publicly available systems.

The absence of an accurate inventory of publicly available systems and associated ports prevents the Postal Service from maintaining visibility and control of network traffic using firewalls. It also prevents management from having [redacted]

Recommendation #1

Vice President, Information Technology, enhance procedures for identifying all publicly available systems and all Transmission Control Protocol ports.

Recommendation #2

Vice President, Information Technology, identify and document all publicly available systems and all Transmission Control Protocol ports.

1 Handbook AS-805, *Information Security*, Section 1-7, Information Resources, Exhibit 1-7, (network information resources include publicly available systems connected to the Internet), dated February 2018.
2 A smaller network inside a larger network. It is a logical grouping of connected network devices (hosts).
3 A number used to uniquely identify a transaction over a network by specifying both the host and the service.
4 Handbook AS-805, Section 2-2.19 (o), Security Roles and Responsibilities - Manager, Telecommunications Services.
5 A communication protocol commonly used to provide Internet services.

Finding #2: Firewall Rules Management

Firewall administrators did not adequately manage firewall security controls. According to Postal Service policy[6] and industry best practices,[7] firewall rules should deny all services not expressly permitted and restrict inbound Internet traffic. Policy also states that management must review firewall rules every six months.[8] During our review of the perimeter firewalls and remote scan[9] results we identified:

> *"Firewall administrators did not adequately manage firewall security controls."*

- [redacted]
- [redacted]
- [redacted]

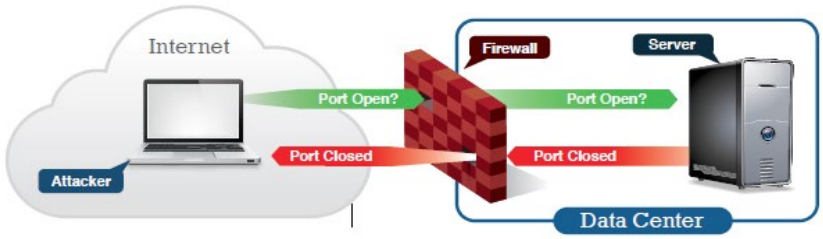
[redacted]

Table 1. Closed Ports

Port Number	[redacted]	Number of Closed Ports
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
Total		**3,483**

Source: [redacted]

Figure 1. Misconfigured Firewall Allowing Unnecessary Traffic to Host

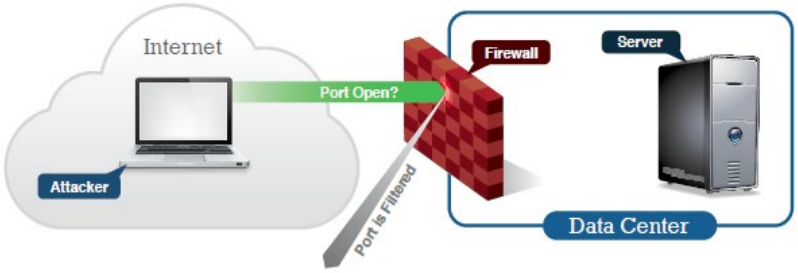


Source: U.S. Postal Office of Inspector General (OIG) illustration of firewall configuration based on analysis of enumeration data.

6 Handbook AS-805, Section 11-5.2.1 (a, b), Firewall Configurations.
7 National Institute of Standards and Technology Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, Section 4, Firewall Policy, dated September 2009.
8 Handbook AS-805, Section 11-5.2.4, Firewall System Integrity.

[redacted]

Figure 2. Properly Configured Firewall That Does Not Allow Traffic to Host with Closed Ports



Source: OIG illustration of firewall configuration based on analysis of enumeration data.

- [redacted]

  When rulesets are not reconciled, overlapping rules occur. Overlapping rules could be obsolete, conflicting or redundant, any of which could negatively impact network performance. This could also introduce challenges to managing firewalls in an effective manner.

These issues occurred because the [redacted]

During the audit period, management took corrective action to remove access to [redacted] and began the process of removing rules that prevent firewalls from filtering unnecessary traffic.

Recommendation #3

Vice President, Information Technology, enhance procedures and use the appropriate tools for [redacted]

Finding #3: Firewall Configuration

Firewall administrators did not implement required security settings[19] to the firewalls. During our review of [redacted]

"Firewall administrators did not implement required security settings to the firewalls."

[redacted]

[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Source: [redacted].

19 [redacted].
20 Handbook AS-805, Section 11-5.2, Implementing Firewalls.
21 [redacted].

These issues occurred because management did not prioritize implementing the security standards to minimize the risk of vulnerabilities for all perimeter network firewalls. The firewall team consists of [redacted] During FY 2017, this team completed approximately 8,000 firewall change requests and more than 10,000 during FY 2018.[22]

When firewalls are not configured to hardening standards, the network is not adequately protected from unwanted traffic, potentially dangerous content, unauthorized access to sensitive data, and disruption of critical system operations. For example, [redacted]

Recommendation #4

Vice President, Information Technology, and Vice President, Corporate Information Security Office, evaluate the firewall configurations monthly, as required by policy and configure perimeter firewalls according to internal hardening standards.

Management's Comments

Management generally agreed with the findings and recommendations in the report, but disagreed with certain statements in the report. As part of their response, management described procedures in place for internal audits and reviews of current firewall rules.

Regarding recommendations 1 and 2, management agreed to develop a perimeter firewall configuration baseline document that will provide a single point of reference of all available subnets and TCP ports. The target implementation date is September 30, 2018.

Regarding recommendation 3, management agreed to improve the firewall rules review process and is in the process of remediation; however, management disagreed with the finding, noting that [redacted].

Additionally, management stated that the [redacted]. The target implementation date is September 30, 2018.

Regarding recommendation 4, management agreed to improve the review and documentation of exceptions to the hardening standards. [redacted]. Additionally, management stated that compensating controls existed. The target implementation date is September 30, 2018.

See Appendix D for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments generally responsive to recommendations 1, 2, 3, and 4.

Regarding management's comments on recommendation 3 that they identified [redacted] rules in a newly established monthly review of firewall rules in January 2018, the OIG identified these same [redacted] in March 2018. In response, management took corrective action to address the [redacted] identified. While we did not evaluate the effectiveness of the January 2018 review, it is the OIG's perspective that for a review process to be effective, [redacted] should be remediated shortly after identification.

Regarding recommendation 4, while compensating controls may exist, it is the OIG's position that management adhere to Postal Service policy regarding firewall configuration reviews. Firewalls are the first line of defense in an organization's IT network. They are essential components of detecting and protecting the network from potentially dangerous content and intrusion attempts.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

22 Fiscal year 2018 represents October 1, 2017 through June 30, 2018.

Appendices

Click on the appendix title below to navigate to the section content.

Appendix A: Additional Information

Scope and Methodology

Our objective was to determine whether Postal Service network perimeter firewalls are properly configured and functioning to safeguard IT according to Postal Service standards and industry best practices.

The scope of this audit was perimeter firewall configurations and rules used to support Postal Service IT operations and applicable hardening standards. Our review did not include reviewing firewalls that protect Postal Service mail processing equipment and mail handling equipment environments.

To accomplish our objective, we:

- Reviewed policies and standards related to the management of firewalls and interviewed key IT and CISO personnel to obtain an understanding of network security controls.
- Reviewed the Network Change Review Board change request process and tested samples of firewall related ServiceNow change requests.
- Obtained a perimeter firewall inventory from the Postal Service and compared implemented configurations against approved Postal Service firewall security standards and controls.
- Compared list of subnets provided by management to prior audits and open source documentation and performed Nmap scans on the routable subnets in Eagan, MN, to identify hosts protected by perimeter firewalls.
- Performed remote Nmap scans from Raleigh, NC, to identify hosts and services available to the Internet from the Postal Service network.

We conducted this performance audit from October 2017 through August 2018, in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on July 13, 2018, and included their comments where appropriate.

We assessed the reliability of perimeter firewall configurations and rules data by reviewing configuration change requests to firewalls in the change management system. We also performed a limited validation test by examining IP addresses and their associated ports. In addition, we interviewed agency officials knowledgeable about the data and process and reviewed required security controls. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact
Internet-Facing Devices	Identify internet-facing hosts connected to the Postal Service network and determine if a complete inventory exists.	IT-AR-17-001	11/4/16	None

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

Appendix D: Management's Comments

UNITED STATES POSTAL SERVICE

August 14, 2018

MONIQUE COLTER
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Review of Perimeter Firewalls (Report Number [IT-AR-18-DRAFT])

Management has reviewed the preliminary report regarding the audit of the perimeter firewalls. We are in disagreement with some of the findings. However, management does agree with the recommendations. Protecting US Postal Service digital assets has always been a primary goal of the Corporate Information Security Office (CISO) and Information Technology (IT). We are continuously working towards making the perimeter as secure and efficient as possible.

The OIG states "The Postal Service network perimeter firewalls are [redacted] The USPS disagrees with this statement; it does not put the findings into context. The firewalls have over [redacted]

There are always areas of improvement with any process area, and the Postal Service takes this matter seriously. We have been focusing resources on these improvements which the OIG may not have fully evaluated. The Postal Service has implemented a leading practice firewall management platform to aid in the maintenance of the rule sets across the perimeter and enterprise firewalls. The Postal Service currently has procedures in place that provides for the audits and reviews of current firewall rules.

Below is a current list of the internal audits with their frequencies.

- Perimeter Transmission Control Protocol (TCP) Port Scans [redacted]
- Perimeter Firewall Rules [redacted]
- Perimeter Firewall Allow Any Rules [redacted]

The steps above are currently part of the Standard Operating Procedures (SOP) maintained by the CISO organization.

The USPS has implemented enhanced technologies and procedures during 2017 and 2018 to address ongoing improvements to the firewall rules and closed ports. We routinely review and refine the procedures and documentation for continuous improvement to manage the size and scale of the USPS network.

475 L'Enfant Plaza SW
Washington, DC 20260

WWW.USPS.COM

Recommendation 1:
Enhance procedures for identifying all publicly available systems and all Transmission Control Protocol ports.

Management Response/Action Plan:
Management has reviewed finding #1 and recommendations #1 and #2. the Postal Service disagrees with the statement that we do not maintain an accurate inventory of network information resources to include subnets and ports. The Postal Service is [redacted] While there were some discrepancies in the initial reporting to the OIG of the available subnets at the beginning of the audit, once the initial request was clarified, the Postal Service provided the accurate information to the OIG audit team. To avoid any future confusion, the Postal Service's IT and CISO teams are finalizing a perimeter firewall configuration baseline document that will provide a single point of reference of all available subnets and TCP ports. This will be a controlled document where any changes must be approved by designated IT and CISO personnel only.

Target Implementation Date: September 30, 2018

Responsible Official: Vice President, Information Technology

Recommendation 2:
Identify and document all publicly available systems and all Transmission Control Protocol ports.

Management Response/Action Plan:
Management has reviewed finding #1 and recommendations #1 and #2, the Postal Service disagrees with the statement that we do not maintain an accurate inventory of network information resources to include subnets and ports. The Postal Service is [redacted] While there were some discrepancies in the initial reporting to the OIG of the available subnets at the beginning of the audit, once the initial request was clarified, the Postal Service provided the accurate information to the OIG audit team. To avoid any future confusion, the Postal Service's IT and CISO teams are finalizing a perimeter firewall configuration baseline document that will provide a single point of reference of all available subnets and TCP ports. This will be a controlled document where any changes must be approved by designated IT and CISO personnel only.

Target Implementation Date: September 30, 2018

Responsible Official: Vice President, Information Technology

Recommendation 3:
Enhance procedures and use the appropriate tools for [redacted] to the Postal Service network.

Management Response/Action Plan:
Management has reviewed finding #2 and recommendation #3. The Postal Service disagrees with item one of this finding. The Postal service maintains a very complex network

and the [redacted] that were identified out of [redacted], amounts to only [redacted] in place. The OIG stated [redacted] of the [redacted] gave [redacted] external hosts access to the entire Postal Service network on all ports. [redacted] were stated [redacted] when they were actually limited to the Postal Service's [redacted] zone only, not the entire Postal Service network as stated in the report. [redacted]

Additionally, these [redacted] rules were part of a past business partner relationship, and the rules were under review for elimination following replacement of the service. These [redacted] rules were also identified in the newly established monthly review of firewall rules that Information Technology and Corporate Information Security started performing in January 2018. These [redacted] rules were remediated by the USPS as of April 2018.

The remaining [redacted]

Target Implementation Date: September 30, 2018

Responsible Official: Vice President, Information Technology

Recommendation 4:
Evaluate the firewall configurations monthly, as required by policy and configure perimeter firewalls according to internal hardening standards.

Management Response/Action Plan:
Management has reviewed finding #3 and recommendation #4, the Postal Service disagrees with the statement that firewall administrators did [redacted] The vulnerability risk was mitigated due to other compensating controls. This audit did not evaluate these compensating controls.

At the time of this OIG audit (March 2018), the hardening standards were [redacted] implemented. The [redacted] received final management approval in December 2017, and CISO has implemented a procedure to effectively evaluate the firewall configurations. For the external firewalls, the Postal Service will continue to validate the configurations against the Hardening Standards on a monthly basis. The Postal Service agrees to improve the review and documentation of any exceptions to the hardening standards as part of this recommendation. [redacted]

Target Implementation Date: September 30, 2018

Responsible Official:
Vice President, Information Technology, and Vice President, Chief Information Security Officer

William Koetz Digitally signed by William Koetz DN: cn=William Koetz, o=Information Technology, ou=Computer Operations, email=william.e.koetz@usps.gov, c=US Date: 2018.08.14 16:06:23 -05'00'

For
Jeffery C. Johnson
Vice President, Information Technology

Concurrence:

Gregory Crabb
Vice President, Chief Information Security Officer

cc: Manager, Corporate Audit & Response Management

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms.
Follow us on social networks.
Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100