Security Standard and Guidelines

1. Overview

Information Technology is committed to protecting the City Of Rockville (COR)'s employees, partners, citizens and the City from illegal or damaging actions by individuals, either knowingly or unknowingly.

Security becomes critical component to any organization. Any IT project requires involvement of security related aspect to protect from cyber attack. Firewalls also play important role in network securities that control the flow of network traffic between networks or hosts that employ differing security postures. COR uses firewalls, intrusion prevention system, and others to meet security requirements from mandates (i.e. FISMA, NIST Framework); some mandates, such as the Payment Card Industry (PCI) Data Security Standard specifically require firewalling.

However, security can be significantly ineffective in protecting organization if the requirements are not managed and clearly define correctly and effectively. It is very crucial to have standard management techniques and tools that users can use to examine, refine and verify the correctness of written firewall filtering rules and security standard and guidelines in order to increase the effectiveness cyber security.

2. Purpose

This document provides practical standard guidelines on developing standard requirements such as IT projects, policies and selecting, configuring, testing, deploying and managing security devices.

3. Scope

COR places a lot of security to protect systems within City network. Security standard and guidelines are developed to maintain the need of security and daily requirement. Cisco Adaptive Security Appliance (ASA) Next Generation firewalls to inspect, analyze, monitor and protect any threats, malware, and secure lower layers of network traffic to the application layer. Cisco FirePower Management Center (FMC) virtually builds on top of Cisco to perform in-depth inspection and perform advanced malware protection. To improve the effectiveness and security of the firewalls; COR firewall policy should implement the following recommendations:

a) Create a firewall policy that specifies how firewalls should handle inbound and outbound network traffic.
b) Identify all requirements that should be considered when determining which firewall to implement.

c) Create rulesets that implement the firewall policy while supporting firewall performance.
d) Manage firewall architectures, policies, software, and other components throughout the life of the firewall solutions.
e) Explicit deny the end of all the require policies.

4. Responsibilities

Preparation, execution, review and maintenance of this document related to the operation

- Information System Security and Compliance Manager
- Cyber Security Engineer

Review and approval of documents and procedures

- Director of Information Technology

5. COR Firewall Technologies

This section provides an overview of COR firewall technologies and basic information on the capabilities of several commonly used types. The major implementation part of Cisco ASA Next Generation includes network address translation (NAT), content filtering features and inline intrusion detection and prevention system (IDPs) which can react to attacks that they detect to prevent damage to systems protected by the firewalls.

5.1 Packet Filtering

The main feature of the firewall is the packet filter which is also known as stateless inspection. It is based on the ruleset on source ip address, destination ip address, network or transport protocol and the interface being traversed by the packet that employ access controls lists. Packet filter operates at the network layer that filter inbound (ingress filtering), outbound (egress filtering) or/and bidirectional traffic.

5.2 Stateful Inspection

Stateful inspection improves on the functions of packet filters by tracking the state of the connections (i.e. TCP or UDP communication) and blocking packets that deviate from the expected state. Three major states exist for TCP traffic-connection establishment, usage, and termination. Stateful inspection examines the TCP headers to monitor the state of each connection from the state table.

5.3 Application Firewalls

An application firewall is a form of firewall that controls an application or its service. The application firewall builds to control all network traffic on any OSI layer up the application layer. Because it acts on the application layer, it inspects the contents of traffic, blocking

specified content, such as certain websites, viruses, or attempt to exploit known logical flaws in client software.

5.4 Network Access Control

Cisco FMC is associated with Active Directory, and can perform client checks for incoming connections from remote users and allow or disallow access based on those particular roles and rules for any exception request which has been approved by IT Security Team.

6. Standard Firewall Rules

A firewall rule dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications and content types based on the information security policies. Before a firewall policy is created, some form of risk analysis should be performed to develop a list of the types of traffic needed and how they must be secured. This risk analysis should be based on an evaluation of threats; vulnerabilities; countermeasures in place to mitigate vulnerabilities; and the impact if the systems or data are compromised. Because of the dynamic nature of hosts, networks, protocols, and applications, deny by default approach will be implemented to decrease the risk of attack and can also reduce the volume of traffic carried on COR network.

6.1 Policies Based on IP Addresses and Protocols

By default, firewall policies should allow commonly used IP protocols number like ICMP(1) except egress policies towards provider edges or outside network or DMZ network towards Internet connectivity. It is necessary to restrict whenever possible to the specific hosts and networks within COR with a need to use those protocols. By permitting only necessary protocols, all unnecessary IP protocols are denied by default.

6.1.1 IP Addresses and Other IP Characteristics

Firewall policies should only permit appropriate source and destination IP addresses to be used. Specific recommendation for IP addresses include:

- Traffic with invalid source or destination addresses should always be blocked, regardless of the firewall location. Examples of relatively common invalid IPv4 addresses are 127.0.0.0 to 127.255.255.255 (localhost) and 0.0.0.0 (localhost/broadcast). 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.
- Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic (an invalid “external” address) should be blocked at the network perimeter. This most common type of invalid external addresses is an IPv4 address within the ranges in RFC990, RFC1700, RFC1918, RFC2544, RFC3068, RFC3927, RFC5736, RFC5771, RFC6598, and RFC6890.

- Traffic with a private destination address for incoming traffic or source address for outgoing traffic (an "internal" address) should be blocked at the network perimeter.
- Outbound traffic with invalid source addresses should be blocked (egress filtering).
- Incoming traffic with a destination address of the firewall itself should be blocked unless the firewall is offering services for incoming traffic that require direct connections.

6.1.2 TCP and UDP

Application protocols can use TCP, UDP, or both, depending on the design of the protocol. This has to be provided by user in order for network administrator to apply policy for them.

6.2 Rules Based on Application

Application based approach provides an additional layer of security for incoming and outgoing traffic by validating some of the traffic before it reaches the desired server. The application approach is based on the URL as well as roles of the user requirement to access to those restriction applications externally.

7. Planning and Implementation

This section focuses on the planning and implementation of firewalls in COR. Firewall and policy planning and implementation should be addresses in a phased approach including:

- **Plan** – The first phase of the process involves identifying all requirements to build the firewalls. Basic principles user should follow include:
    a. **Create defense-in-depth**. Defense-in-depth involves creating multi-tiered architecture (multiple) layers of security. All systems **MUST** support this architecture. This allows risk to be better managed, because if one layer of defense becomes compromised, another layer is there to contain the attack. The City will **NO** longer support flat or single network architecture.
    b. **Pay attention to internal threats**. Focusing attention on both internal and external threats through packet inspection and ~~also~~ ~~separate~~ distinguish between internal and external firewalls.

- **Configure** – The second phase involves all facets of configuring the firewall platform. This includes installing hardware and software as well as setting up rules for the system. Each policy has to be logged and send to centralize syslog or SIEM server for further forensic analysis. Real-time alerts should also be set up to notify administrator when important events occur~~s~~ on the firewall.

- **Test** – The next phase involves implementing and testing the firewall rules of the designed solution environment. The primary goals of testing are to evaluate the

functionality, performance, scalability, and security of the solution, and to identify any issues – such as interoperability-with components.

- **Deploy** – Once testing is completed and all issues are resolved, the next phase focuses on deployment of the firewall and policy into the enterprise.

- **Manage** – After the firewall or policy has been deployed, it is managed throughout its lifecycle to include component maintenance and support for operational issues. This lifecycle process is repeated when enhancements of significant changes need to be incorporated into the solution. Below are the standard guidelines how user should submit the firewall rules request.

  Policy rules and standards need to be updated as new threats are identified and requirements change, such as when new applications or hosts are implemented within the network, and should review periodically, which is **every 3 to 6 months cycle** with the requester or policy owner to ensure they remain in compliance with security policy. **If there is no response from the owner/requester within a week, the policy will be terminated and removed.**

  Logs and alerts should also be monitored continuously to identify threats-successful and unsuccessful- that are made to the system. Another important task is to perform periodic testing to verify that firewall rules are functioning as expected. Also, firewall policies and rulesets should be backed up daily.

  Changes to firewall rulesets or policies impact security and should be managed as part of a formal configuration change management process. A log should be kept of all policy decisions and ruleset changes. Comments should contain the **ticket/case number, requester information, duration of the policy created and expired, and reason** that associate to the policies as part of the auditing process.

8. Security Standard and Guidelines

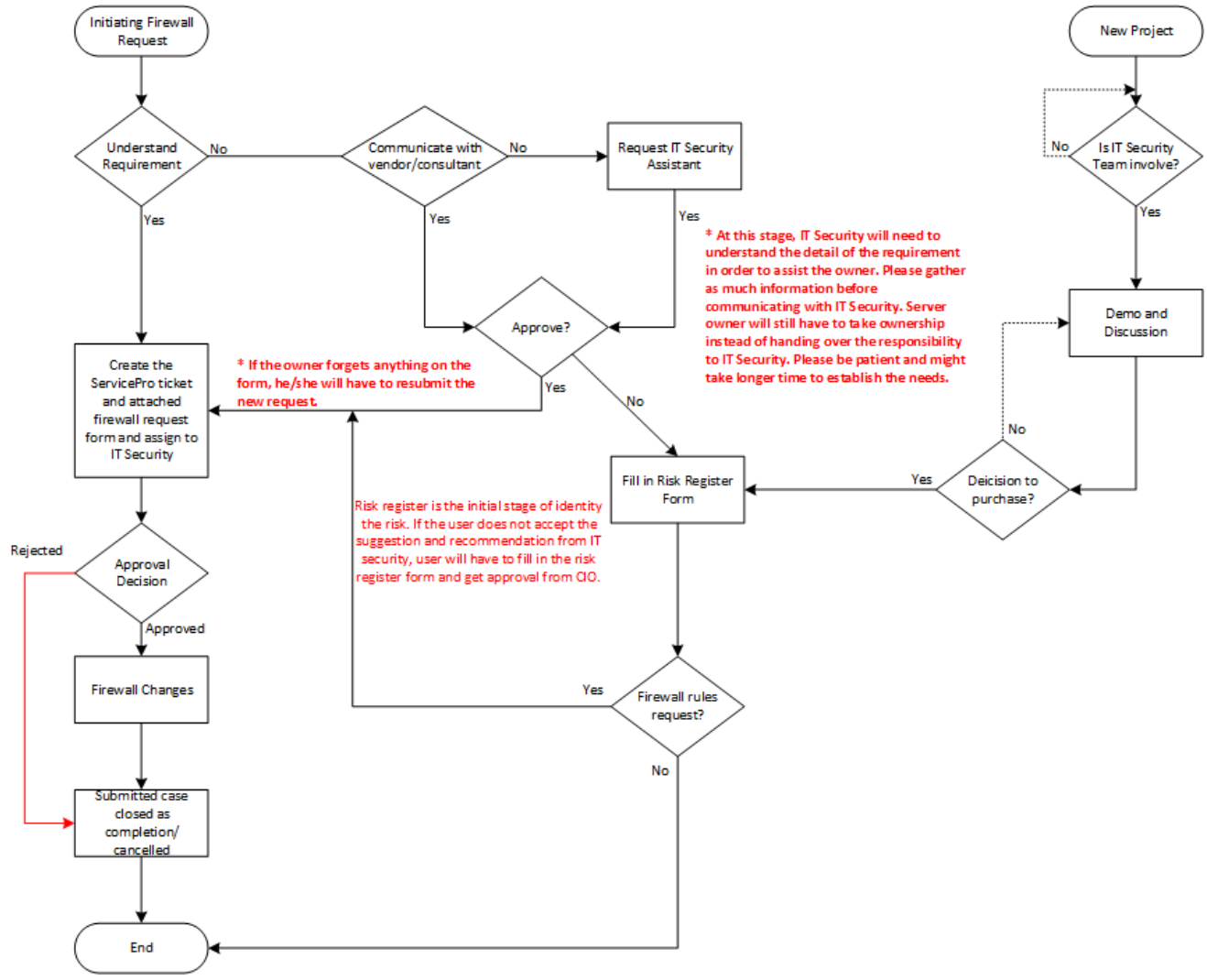
Security operation process is to allow user to understand the process during the initial request of involving IT security team until everything has been completed.

a. User will submit the request **only** through **ServicePro** ticketing system to IT Security team. The ticket will be assigned to one of the IT Security team members, the estimated time of response is within **5** business days. If there is any additional delay, IT Security will follow up with the user.
b. User can follow up with IT Security team through email. Users should consider the specific firewall to implement and any related IT project. If they do not know,

they can communicate with IT Security team member before creating the ticket. Any request that does not go to proper procedure will cause the delay of the process.

c. IT Security will assign an engineer to work on the ticket either related to the IT projects, needs or/and firewall related requests. IT Security will contact the user if they have any question related to the request before proceeding with any security requirement. IT Security will assist user to provide assistant and recommendation related to IT project needs and concern. IT Security has the right to reject any request related to firewall rules if they determine the rules are not relevant or do not meet the requirements above. There should not be any wide-open rules throughout the request (ex. Permit Any/Any).
d. IT Security will request the user to test the new firewall rules before closing the ticket.

The security work flow below will provide the overall security operation standard and guidelines.



8.1 Firewall Operation Guidelines

Below is the brief process of the request of firewall rules for the servers and devices.

- All the interfaces except end user computer are behind the firewall. This is to protect any malicious traffics passing through and attack the corporate servers and other critical components.
- The firewall allows any servers on SAN, SECURITY, PCI, DMZ and INT-APP interfaces to communicate with our Domain Controller (DC) to allow user login through Active Directory (AD) credential.
- Any servers on SAN, SECURITY, PCI, DMZ and INT-APP interfaces will allow accessing to internet through default web browsing protocols like http and https.
- Except the connections to DC and internet, all the servers that are not on the same interface will have implicit deny to any resources outside their own subnet. i.e, no default connection to file server.

- Any rule requires to use **secure** protocols. Any non-secure protocol will not be accepted such as using non-secure protocol for data transfer such as TCP port 445, FTP ports 20, 21 and etc. If user insists to use non-secure of protocol, user will have to fill in **risk register** form, so ~~that~~ the risk~~is~~ information is documented and identified beginning of the risk process.
- The owner of the server ~~should~~ shall gather the information from the vendor and/or consultant and provide IT Security the detail requirement of how they would like to communicate. Since it is the stateful firewall, IT security only requires the source that initiates~~al~~ the connection.
- For any internet facing Web Server ~~facing Internet~~, unsecure http port is no longer support.

Interfaces	Subnets	Description
WAN	Public Facing	Internet Connection
TRANSIT	10.2.0.0/16 and Enduser PCs	City of Rockville Enduser network and old Intranet servers
DMZ	192.168.1.0/24	City of Rockville Extranet Servers
County	172.29.69.0/24	Montgomery County network
INT-APP	10.200.10.0/24	City of Rockville Intranet Servers
EXT-DMZ	192.168.11.0/24	City of Rockville External Servers (not in City network)
PCI	10.200.26.0/24	City of Rockville PCI Compliance Servers/PCs
SECURITY	10.200.15.0/24	City of Rockville Security Tools network
DB	10.200.27.0/24	City of Rockville Database network
SAN	10.200.150.0/24	City of Rockville Storage network
AnyConnect	192.168.12.0/24	City of Rockville Remote Access network

Notes: There are more segmentation and VLAN on this network. If you are not sure where to place your system and device, please consult IT Infrastructure team.

8.2 IT project initiative

IT security must involve on any IT related project starting the beginning to assist user identifying the risk in the early stage. Risk register is the document use to identify the risk on the early stage

and include additional information about the risk, e.g. nature of the risk, reference and owner, mitigation measures.

9. Compliances

9.1 Compliance Measurement

The IT Security team will verify compliance to this standard guideline through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the server owner.

9.2 Exceptions

Any exception to this standard must be approved by the IT Security Team in advance.
Please email ITSecurity@rockvillemd.gov **for any question and concern.**

10.Definitions and Terms

The following definition and terms can be found in the Glossary located at:

- DMZ
- Firewall
- FISMA
- ICMP
- IDPS
- IP
- NAT
- PCI
- TCP
- UDP

11.Revision History

Date of Change	Responsible	Summary of Change
June 2015	IT Security	New
April 2018	IT Security	Add process and workflow
August 2020	IT Security	Update the process, standardization and guidelines