Tier 1 Control Standards (State-Wide)

Firewall Architectural Standard: Traversal and Filtering

Standard ID
IOT-CS-ARC-004

Published Date
4/4/2017

Effective Date
7/3/2017

Last Updated
4/4/2017

Next Review Date
4/4/2018

Policy
06.0 Access Control (PR.AC)
06.5 PR.AC-5
06.5.1 Network Segmentation

Purpose
To protect against unauthorized horizontal and vertical movement throughout the State network.

Scope
All Devices that Connect to the State Network

Statement
IOT provides both the standard perimeter based firewall protection as well as the additional layers of security through multiple zones firewalled with different levels of security.

This Standard provides requirements to secure and protect the states computer network. By restricting, segmenting and encrypting the communication between networked based systems, IOT provides a comprehensive network security strategy.

IOT and its partnering agencies must use approved solutions such as stateful firewall, application firewall, proxy and router technologies, with access control entries or lists configured for this purpose to aide in insuring the overall integrity and security of the state’s IT network.

Authorized Zone Access and Communications

IOT is comprised of many interconnected networks within the state infrastructure called zones/enclaves. A zone is where networks are segmented from other interconnected networks by a physical firewall. Each zone shall have varying levels of security. IOT zones today are known as: Extranet, Intranet and Protected.

Each zone shall consist of different types of environments. Typical environments are Non-Production (e.g., Development, UAT) and Production. Environments shall contain information systems for the agencies where information systems are made up of servers, storage and peripheral devices that process common information.

Each zone is partitioned and isolated into virtual networks called Virtual Local Area Networks (VLANs). A VLAN can also be referred to as a segment or even tier. In the protected zone, VLANs shall provide agency and application segmentation in addition to implemented, controlled firewall rules.
Zone Access Matrix:

The following table works in conjunction with the Enterprise zone diagram listed above and is the high level template for approved device data flows throughout the various zones of the Enterprise:

<table>
<thead>
<tr>
<th>* Access via IOT’s approved proxy</th>
<th>** Specific services only (ex. MFT)</th>
<th>*** Specific applications only (ex. ETL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red – Not allowed</td>
<td>Yellow – Allowed with approval</td>
<td>Green – Allowed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Extranet</td>
</tr>
<tr>
<td>Extranet</td>
<td>*</td>
</tr>
<tr>
<td>Intranet</td>
<td>***</td>
</tr>
<tr>
<td>Shared DMZ</td>
<td>*</td>
</tr>
<tr>
<td>Shared Services</td>
<td>**</td>
</tr>
<tr>
<td>Agency DMZ/Pres</td>
<td>**</td>
</tr>
<tr>
<td>Agency Application</td>
<td>***</td>
</tr>
<tr>
<td>Agency Database</td>
<td>***</td>
</tr>
</tbody>
</table>

Authorized Zone Communication

- **Baseline for all Zones (Enclaves) including Extranet, Intranet and Protected**
  - Direct or delegated administrative access to any server or network devices within the environments shall use IOT’s sponsored Secure Access solution
  - Client data flows shall use IOT’s Web/Application Proxy solution to the presentation/demilitarized zone (DMZ) or approved application tier
  - Information systems shall use IOT’s Secure File Transfer and Storage solution
  - Communication between zones or communications containing confidential data shall be encrypted with approved cryptography modules as outlined in IOT’s Data Encryption Standard
  - Information Systems shall not span Zones
  - Interconnection between information systems that are in different zones shall go through an IOT application or web gateway
  - If an extranet/intranet/protected “hybrid” transition is required, an approved corrective action plan (CAP) shall be submitted and approved by IOT
  - Production and nonproduction environment rules are separate and shall not bridge the two environments

- **Intranet Zone**
  - Includes the Baseline for all Zones (Enclaves)

- **Extranet Zone**
  - Includes the Baseline for all Zones (Enclaves) section above and the following:
    - Untrusted vendor devices and firewalls shall be connected and pass through this zone only

- **Protected Zone**
  - Includes the Baseline for all Zones (Enclaves) section above and the following:
    - No layer two tunneling protocol, Client based or Site to Site VPN or Tunneling access to environments or devices shall be allowed
    - Agencies may use server to server IPSEC tunnels, via the published exception process, in order to secure transport of documented, unencrypted data in legacy applications only
      - Agencies may use server to server IPSEC tunnels, via the published exception process, in order to secure transport of documented, unencrypted data in legacy applications only
      - Agencies may use server to server IPSEC tunnels, via the published exception process, in order to secure transport of documented, unencrypted data in legacy applications only
      - Agencies may use server to server IPSEC tunnels, via the published exception process, in order to secure transport of documented, unencrypted data in legacy applications only
  - No wireless access shall be allowed
  - No file sharing access between zones shall be allowed
  - No direct end-user or application access in any tier in any zone shall be allowed

General Filters

- The following shall be followed for authorized use of protocols:
  - IPv4 Only
  - IPv6 – Explicitly DENIED
ICMP is restricted to only type 8 and type 0 (echo request/echo reply)

Filtering of network traffic to control and restrict access across the State of Indiana’s network zones and its perimeter shall be utilized

Only traffic that is authorized per policy is permitted, and all other traffic is denied by default

Explicit logging option shall be added to each Access Control Entry (ACE) to enforce and ensure both “allowed” and “denied” flows are seen in event logs

All ACE’s shall be set to a level for Information based logging

Explicit “Deny All” statement shall be added at the end of each Access Control List (ACL) to log all remaining traffic being denied

Well-known Ports and specific protocols

- Allowed ports and Protocols shall follow its specific Remote Functional Call (RFC)
  - i.e. Allowing TCP for NTP is invalid
- Any port changed from the default well-known shall be recorded in the Information System documentation and approved by IOT Security
  - i.e. Changing HTTPS from TCP port 443 to 8443 or 4330 shall be documented in the firewall access control list description text

ACL’s or ACE’s shall not allow traffic to bypass other security defenses

All unnecessary network services on firewalls and routers that filter traffic shall be blocked and disabled

Egress and ingress filtering shall be configured to block spoofed packets

Traffic from unassigned IP address ranges, known as bogon lists shall be blocked

Border routers and firewalls shall be configured to not forward directed broadcasts

Outgoing connections to common Internet Relay Chat (IRC), peer-to-peer service and instant messaging ports if the usage of such services shall be blocked

External routing information protocols like Open Shortest Path First (OSPF) or Routing Information Protocol (RIP) shall be blocked

Packet filters

- More specific rules shall be configured and triggered before general rules
  - i.e. – Permit TCP Port 443 from 1.1.1.1 to 2.2.2.2 shall be implemented prior to the Deny IP from 1.1.1.1 to 2.2.2.2
- All rules shall follow least privilege
  - No rules utilizing host to subnet or subnet to host communication
  - No ACLs using ANY as Source or Destination and shall utilize a defined host list
- Communication between tiers/VLANs shall be encrypted with approved cryptography modules
- ACL’s shall show communication flows and be defined per vendor/agency documentation
- No nested group objects within an access control list (ACL) shall be permitted
- All privileged ports, with the exception of explicitly required ports, shall be closed
- Firewalls shall be configured to deny and log suspicious packets (e.g. packets that have suspicious source and destination ports)
  - All incoming traffic to non-privileged ports, except for acknowledgement packets, shall be rejected
  - External packets with an internal source IP address shall be identified and rejected, and an attacker alarm shall be triggered
  - Internal packets with an external source IP address shall be identified and rejected, and an attacker alarm shall be triggered

Content filters

- ACL’s and ACE’s shall strictly define and limit the types of files that can be transferred based on business requirements
- ACL’s and ACE’s shall block all executables and active content from being communicated though gateways
- ACL’s and ACE’s shall employ filtering techniques involving Anti-Virus scan, Date format check, Date range check, Data type check, File extension check, Keyword search, Metadata check, Protective Marking check and Manual inspection
- ACL’s and ACE’s shall block or drop any data identified by a data filter as suspicious until reviewed and approved for transfer by a trusted source other than the originator
- Spam protection mechanisms shall be implemented with a learning capability to more effectively identify legitimate communications traffic
Roles
IOT Personnel
Information Asset Owners/System Owners

Responsibilities
All IOT personnel and Information Asset Owners/System Owners that have the ability to approve, design, deploy and configure any firewall devices or appliances and/or associated filtering shall be required to follow all requirements outlined within the standard.

Management Commitment
Management shall ensure all outlined firewall requirements are enforced.

Coordination Among Organizational Entities
Agencies shall coordinate the validated Information System flows with the proper IOT personnel.

Compliance
Firewall rules will be reviewed periodically to determine least privilege and corresponding updates shall be made.

Exceptions
Exceptions will be handled on a case by case basis through the Director of Risk & Compliance, State CISO and the IOT Architecture team.

Related Tier 2 Standards (Agency Specific)
Firewall Standard-Administration and Management

Associated Documents
Firewall - Definitions

Attachments
Firewall Architectural Standard - terms and definitions.docx