STATE OF ALABAMA

INFORMATION TECHNOLOGY STANDARD

Standard 510S1: Zone Architecture		
Document/Version: 510S1-01	Version Date: 04/07/2021 (draft)	Effective Date: TBD

OBJECTIVE

The objective of his standard is to define the broad architectural requirements, basic components, and primary functions of a security zone architecture.

AUDIENCE

Information technology professionals responsible for the design and development of information systems, integration of systems onto the enterprise network, and management of systems throughout the system lifecycle,

REQUIREMENTS

To ensure the confidentiality and integrity of state data, the Alabama enterprise network (i.e., the network managed by the Office of Information Technology (OIT)) uses security zones to control and restrict access. A security zone is a portion of a network that has specific security requirements. Zones are typically separated using a firewall. The multi-zone network architecture depicted in Figure 1 is an approved state standard for a zoned architecture. The security zones defined for this architecture are as follows:

1. USER ZONE:

All users, whether internal and utilizing a client system on a state domain or external and connecting via the public Internet or virtual private network, are treated the same with regard to accessing systems and services in the next applicable zone.

2. FRONT END ZONE – SECURITY:

This zone provides the security services to the front-end zone. Using reverse proxy and web application firewall many common types of attacks made against websites and web servers can be identified and blocked.

3. FRONT END ZONE:

The front-end zone is the outward facing level of the architecture. The front-end zone is a sub-network (set of networks) that is used to provide services to the users without allowing the users direct access to data stores or other protected services or systems in the state network.

The following services/systems typically reside in the front-end zone:

- HTTP(S)
- FTP
- NTP
- SSH
- SharePoint Front End
- Public DNS

4. MIDDLE ZONE – SECURITY:

This zone provides the security services for the middle zone (when required). The SOA / XML Gateway provides protection between the front-end zone and the data zone.

5. MIDDLE ZONE:

The middle zone, sometimes referred to as the application or business logic layer, logically resides between the front-end zone and the data zone. This zone is responsible for accessing the data zone to retrieve, modify and/or delete data, apply various processing functions to that data, and send the results to the devices in the front-end zone.

The following services/systems typically reside in the Middle Zone:

- Web Services/Applications
- SharePoint Applications
- File Shares
- WINS
- Email
- Private DNS

The middle zone is not required for every application, but it is required when multiple front-end services will access the same database.

6. DATA ZONE:

The data zone hosts databases and database servers that store and retrieve information. This zone keeps data neutral and independent from application servers and business logic. Giving data its own zone improves scalability and performance in addition to minimizing the risk of unauthorized access attempts. The data zone may be segmented to isolate database systems from one another.

The following services and systems typically reside in the Data Zone:

- Active Directory
- SQL/Oracle
- SharePoint Database
- Mainframe

Access to the data zone is limited to authorized database administrators and applications.

7. LOGGING ZONE – SECURITY:

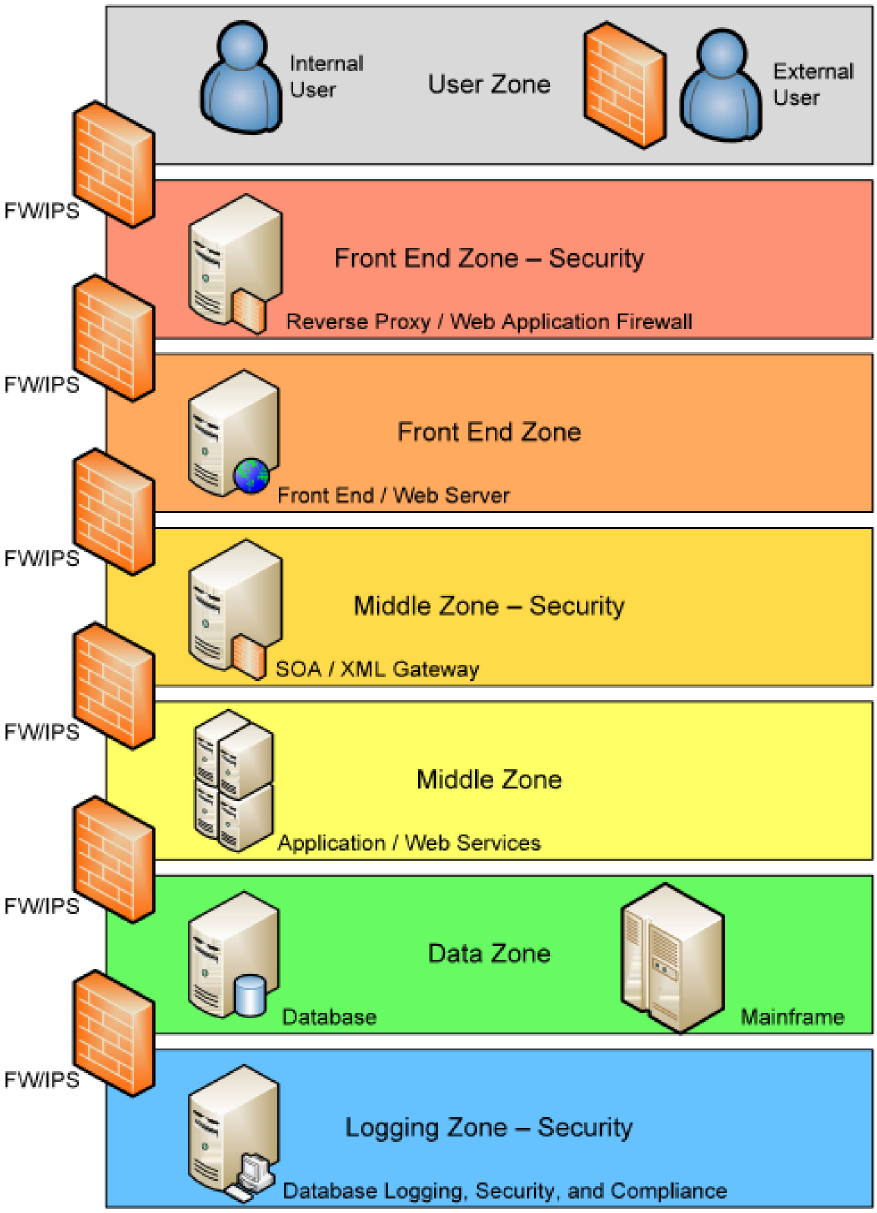
The logging zone will collect security event log information from any or all the other zones including, but not limited to, database transaction logs from the data zone and authentication data from the front-end zone. Centralized logging simplifies event correlation.

The following services and systems typically reside in the Logging Zone:

- Database transaction log duplication
- System logs
- Server Security logs
- SNMP Collation

Access to the logging zone is limited to authorized security administrators only.

Figure 1. Multi-Zone Network Architecture



SUPPORTING DOCUMENTS

This document is governed by:

- Policy 510: Security and Privacy Architectures

The following special publications (SP) of the National Institute of Standards and Technology (NIST) support this standard and may aid in its implementation:

- NIST SP 800-39: Managing Information Security Risk
- NIST SP 800-53R5: Security and Privacy Controls for Information Systems and Organizations

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
500S1-00	09/12/2012	Original document
510S1-01	DRAFT	Document number, title, and format changes