STATE OF ALABAMA

Information Technology Standard

STANDARD 500S1-00: NETWORK ARCHITECTURE STANDARD

Statewide information technology (IT) architectural standards allow for the cost effective use of IT resources (systems and data) while maintaining maximum compatibility, interoperability, and interchange of data statewide.

The State of Alabama utilizes a multiple zone (or "n-tier") network architecture. A zoned architecture is characterized by the functional decomposition of applications, service components, and their distributed deployment. The multi-zone architecture provides a layered defense against attack/compromise by logically separating systems and services into zones. Each zone communicates with the adjacent zones and provides specific services to ensure data and system integrity, system interoperability, and transaction accountability.

OBJECTIVE:

Define the broad architectural requirements, basic components, and primary functions of State of Alabama IT networks.

SCOPE:

These requirements apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

REQUIREMENTS:

STATE-STANDARD ZONE ARCHITECTURE

The multi-zone network architecture depicted in Figure 1 (on page 3) is the approved standard for the State of Alabama. Zones are defined as follows:

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.

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.

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
- Telnet
- SharePoint Front End
- Public DNS

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.

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.

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/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.

Logging Zone – Security:

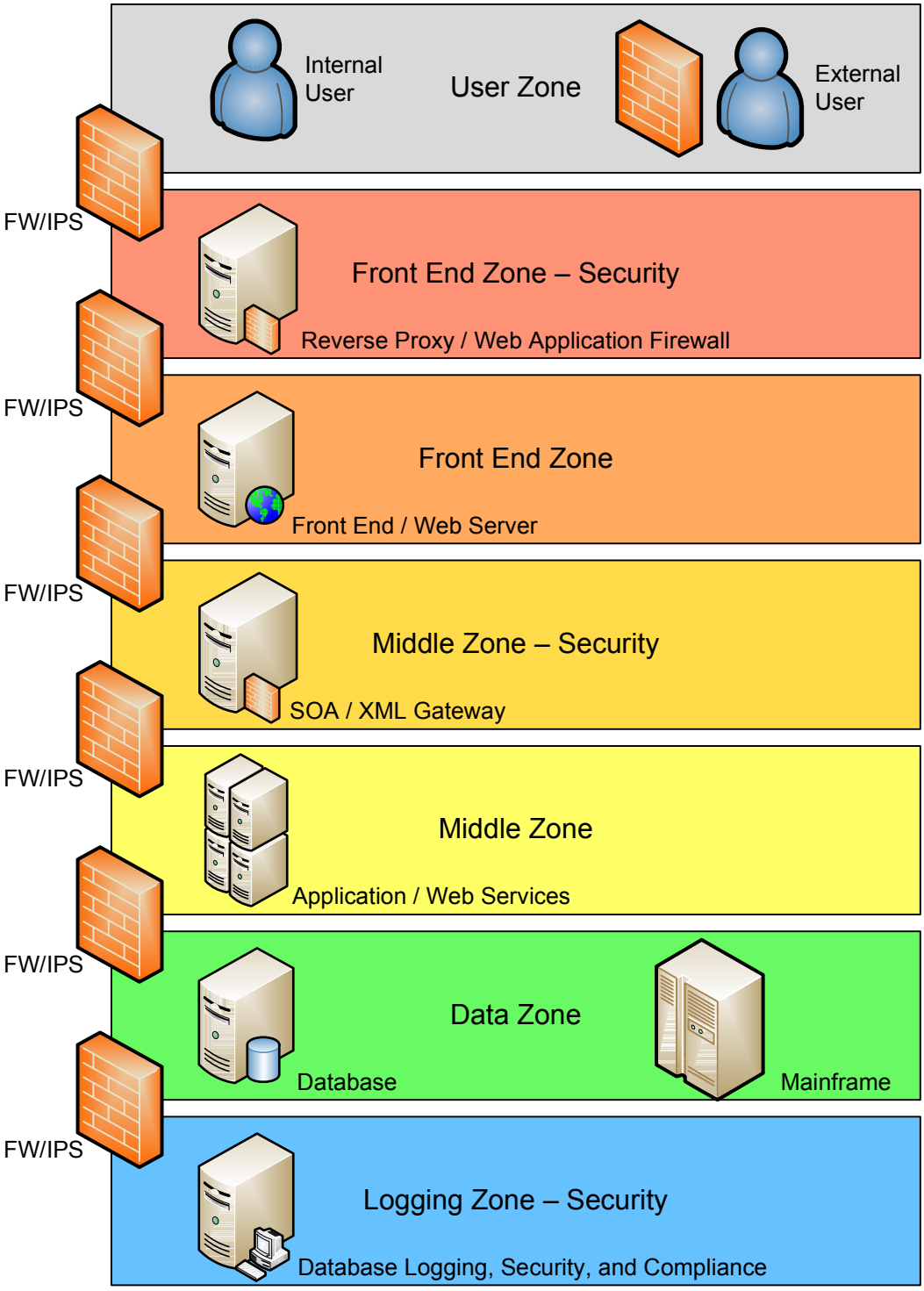
The logging zone will collect security event log information from any/all of the other zones including, but not limited to, database transaction logs from the data zone and authentication data from the front end zone. Centralized logging simplifies event correlation.

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

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

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

Figure 1: Multi-Zone Network Architecture



APPLICABILITY

The State standard architecture will be utilized whenever possible, however, there are instances when some zones are not required (e.g., a public web server with no applications or database functions) or when some zones must be combined (e.g., existing custom implementations or when required by commercial off the shelf software or systems).

When practical, agencies will be broken into separate zones (such as when the user base is sufficiently large) to isolate systems and provide more granular control. Agencies may also request multiple zones as they see fit (for example, to mirror the organizational structure).

EXCEPTIONS

Exceptions to this Standard must be documented and will be considered on a case-by-case basis by the State IT Security Council. Requests for an exception to this Standard must be submitted to the State CISO via the ISD Help Desk.

ADDITIONAL INFORMATION:

Information Technology Policy 500: Statewide Information Systems Architecture
http://cybersecurity.alabama.gov/documents/Policy_500_Statewide_Info_Systems_Architecture.pdf

Information Technology Policy 641: External Connections
http://cybersecurity.alabama.gov/documents/Policy_641_External_Connections.pdf

Information Technology Standard 641S1: Interconnecting IT Systems
http://cybersecurity.alabama.gov/documents/Standard_641S1_Interconnecting_IT_Systems.pdf

Information Technology Dictionary
http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
500S1-00	09/12/2012	Original document