California Department of Technology	3117

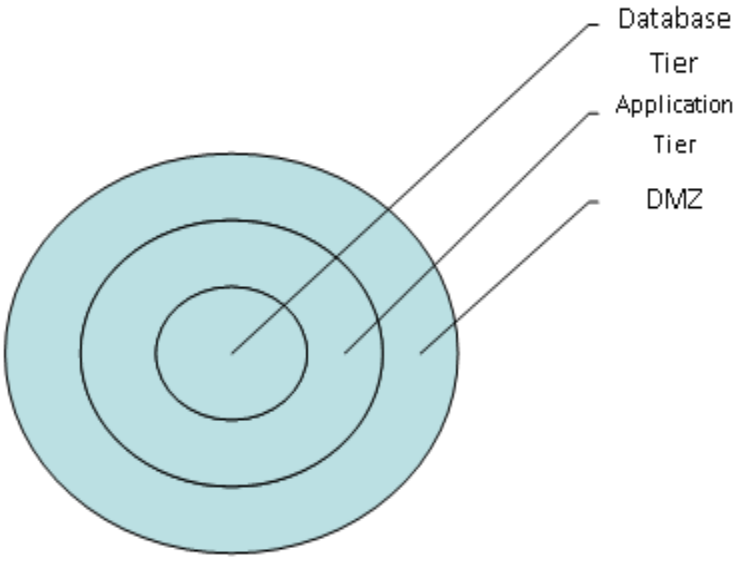
NETWORK ARCHITECTURE STANDARD			
OWNER:	Security Management Branch	**ISSUE DATE:**	
DISTRIBUTION:		**REVISED DATE:**	

This document was last reviewed/updated in December, 2015.

SECTION 1: INTRODUCTION

The California Department of Technology (CDT), Office of Technology Services (OTech), requires that OTech-hosted systems be designed to follow a "n-tiered" network architecture.

"N-tier architecture" is characterized by the functional decomposition of applications, service components, and their distributed deployment. A "tier" is a functionally-separated hardware and software component. Typically, n-tier architectural platforms place each service, or group of services, on a separate server, enabling systems to be divided into easily-scalable components. The most widespread use of "multi-tier architecture" refers to three-tier architecture with a public facing (DMZ) tier, an application tier, and a data/database tier as illustrated in the diagram below. This Standard defines the requirements surrounding the components of n-tiered architecture and the acceptable tiered architectural models.



IMPORTANT: System data in the hosted environment must be classified by the customer and disclosed to the OTech Account Management Branch. Hosted systems containing unclassified data will adopt the most restrictive security measures by default.

SECTION 2: STANDARD REQUIREMENTS

This section provides a high-level description of the web, application, and data tiers and the acceptable tiered network architecture designs.

Part I - Network Architecture Tiers

De-Militarized Zone (DMZ)

The De-Militarized Zone (DMZ), sometimes called the web tier or web layer, is the outward facing level of the application. The OTech will use a system of physical and logical firewalls to create a DMZ. A DMZ is a sub-network (or set of networks) that resides between a trusted internal network, such as the internal OTech network, and an untrusted external network, such as the public Internet. It is used to provide services to the outside world without allowing the outside world direct access into the internal network.

Listed below are system components that ***must*** reside in a DMZ:

- Public-facing web servers
- Publicly accessible File Transfer Protocol (FTP) servers. Note: FTP servers must use a secure file transfer (SFTP or FTPS) unless they are technologically unable to do so. In that case, a Security Exception Request must be filed (see Section 3B).
- Proxy servers
- Email gateways
- Streaming Video servers that only stream public information
- Incoming fax servers and incoming/outgoing fax servers
- Public-facing Domain Name System (DNS) servers
- Traffic management and security components that permit the above devices to function effectively and securely

Application Tier

The application tier, sometimes referred to as the logic/business logic layer, logically resides between the DMZ and the data tier. This tier is responsible for accessing the data tier to retrieve, modify and/or delete data, apply various processing functions to that data, and send the results to the devices in the DMZ (web tier). **No direct public access is allowed to the application tier**.

Listed below are system components that may reside in the application tier:

- Applications or application servers
- Authentication devices, such as active directory or domain controllers
- Systems “processing” information
- Non-public facing FTP servers
- Non-public facing web servers hosting Intranet (internal) applications
- Internal DNS servers
- Outgoing fax servers (isolated within this tier)
- Project specific traffic management and security components that permit the above devices to function effectively and securely

Data/Database Tier

The data or database tier is the inner-most tier of the n-tier architecture. This tier hosts databases and database servers that store and retrieve information. This tier keeps data neutral and independent from application servers and business logic. Giving data its own tier improves scalability and performance in addition to minimizing the risk of unauthorized access attempts. **No direct public access is allowed to the data tier.**

Listed below are system components that must reside in the data tier:

- Databases, database servers, and file servers
- Storage area networks and network attached storage
- Internal DNS servers
- Database archive and reporting servers
- Devices storing confidential or sensitive information

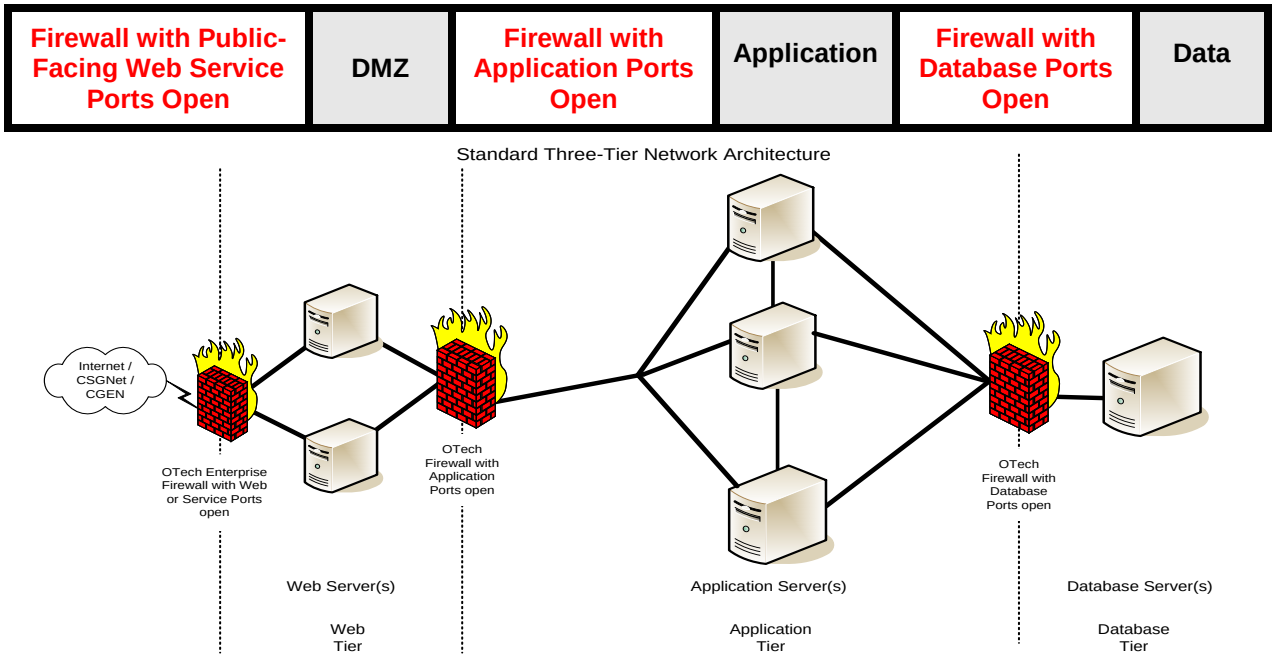
Part II - Standard Network Architectures

The Security Management Branch requires that systems be designed to one of the two network architectures (Three-Tier or zOS Architecture) listed below. If either of these designations cannot be applied, please refer to Section 3 of this Standard.

Three-Tier Architecture

Separation of the three functional tiers is the preferred architecture design. Separating the web server(s), application server(s), and database server(s) is the best way to isolate the most vulnerable devices from the more sensitive devices—creating the most layers of difficulty to compromise system data.

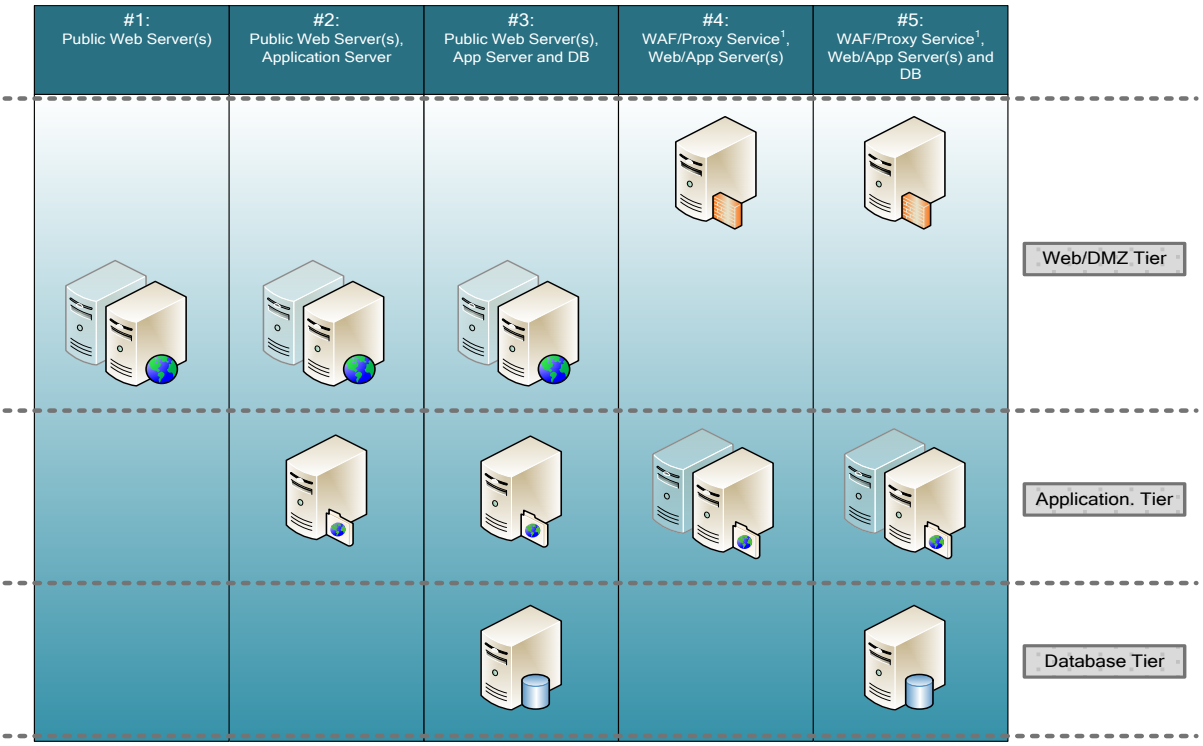
Provided below is a simplified **standard** three-tier network architecture diagram:



Regardless of the type of server implementation (physical or virtual), the above diagram represents the recommended segmentation of the information system into the shown three tiers: Web/DMZ Tier, Application Tier, and Data/Database Tier.

However, there are instances when a 'standard' three-tier architecture, as shown above, is not possible. These are when all of the above layers are not needed or when existing Commercial, Off-The-Shelf (COTS) or custom implementations must combine layers of the above tiers. The following diagram illustrates the approved n-tier variations for these instances.

Security Approved N-Tier Architectures



[1] WAF/Proxy Services are provided by a Web Application Firewall and Proxy Service such as MS ISA 2006, MS Forefront TMG, or other equivalent devices/appliances.

DESCRIPTIONS FOR THE ABOVE DIAGRAM:

#1: Public Web Server(s). One or more simple web servers are needed to serve static pages.
#2: Public Web Server(s), Application Server. Application/business logic functions are needed in addition to web services, but no data/database functions are required.
#3: Public Web Server(s), App Server and DB. This is the same as the 'standard' case described previously.
#4: WAF Proxy Service, Web/App Server(s). This is similar to #2 but there are pre-existing requirements that combine both the web services and the applications services onto the same server(s). In this instance, a Web Application Firewall (WAF) / Proxy server/device is required in the DMZ to front the combined Web/App server(s) in the Application Tier.
#5: WAF Proxy Service, Web/App Server(s) and DB. This extends the #4 instance; where, data/databases services are also needed and are placed into the Database Tier.

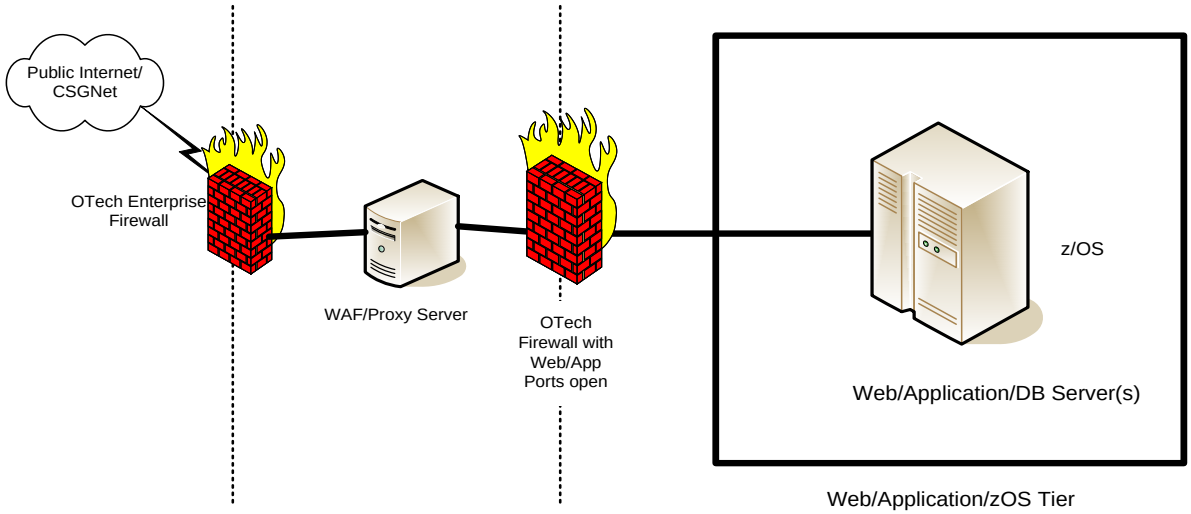
The WAF/Proxy server/device shown in #4 and #5 provide a connection target for traffic from untrusted networks, isolating the application/business logic function from traffic originating from those untrusted networks. Part III of this Standard describes the requirements of that WAF/Proxy server/device.

Z/OS Architecture

The combination of the web/application/data functions into one tier is approved **ONLY** if housed on z/OS system(s) and a WAF/Proxy server/device is used in the DMZ tier to front those combined functions. z/OS features and facilities provide a high level of security and system integrity specifically designed to protect one program from affecting another, either intentionally or accidentally. Facilities such as System Authorization Facility (SAF), Resource Access Control Facility (RACF), and Authorized Program Facility (APF), in addition to system integrity features such as storage protection and cross-memory communication controls, warrant this design.

Firewall with Public-Facing Web Service Ports Open	WAF/Proxy	Firewall Application Ports Open	DMZ & Application & Data

Additional Security Approved z/OS **ONLY** Network Architecture



Additional Architecture Requirements

If multiple System Development Life Cycle (SDLC) environments exist within the Application Hosting services environment (e.g. development, test, pre-product, production, etc.), the architectural tiers for each of these SDLC environments must be on separate Virtual Local Area Networks (VLANs) and isolated by firewalls.

Part III - Web Application Firewall (WAF) / Proxy Requirements

A WAF/proxy server/device should:

- React appropriately (defined by active policy or rules) to threats against relevant vulnerabilities as identified, at a minimum, in the Open Web Application Security Project (OWASP) Top Ten.
- Inspect web application input and respond (allow, block, and/or alert) based on active policy or rules, logging all actions taken.
- Prevent data leakage - the ability to inspect web application output and respond (allow, block, mask and/or alert) based on the active policy or rules, logging all actions taken.
- Enforce both positive and negative security models. The positive model ("white list") defines acceptable, permitted behavior, input, data ranges, etc., and denies everything else. The negative model ("black list") defines what is NOT allowed; messages matching those signatures are blocked, and traffic not matching the signatures (not "black listed") is permitted.
- Inspect both web page content, such as Hypertext Markup Language (HTML), Dynamic HTML (DHTML), and Cascading Style Sheets (CSS), and the underlying protocols that deliver content, such as Hypertext Transport Protocol (HTTP) and Hypertext Transport Protocol over Secure Sockets Layer (SSL) (HTTPS). (In addition to SSL, HTTPS includes Hypertext Transport Protocol over Transport Security Layer [TLS].)
- Inspect web services messages, if web services are exposed to the public Internet. Typically this would include Simple Object Access Protocol (SOAP) and eXtensible Markup Language (XML), both document and RPC-oriented models, in addition to HTTP.
- Inspect any protocol (proprietary or standardized) or data construct (proprietary or standardized) that is used to transmit data to or from a web application, when such protocols or data is not otherwise inspected at another point in the message flow.
- Defend against threats that target the WAF itself.
- Support SSL and TLS termination, or be positioned such that encrypted transmissions are decrypted before being inspected by the WAF (encrypted data streams cannot be inspected unless SSL is terminated ahead of the inspection engine).

Examples of WAF/Proxy devices are MS ISA 2006, MS Forefront TMG, and various hardware appliances from multiple network vendors. A list of example products can be found at the OWASP website.

SECTION 3: APPLICABILITY AND EXCLUSIONS

Direct any questions regarding the applicability of this Standard to the Security Management Branch for clarification.

A. This Standard applies to applicable customer or OTech systems hosted within the Application Hosting services environment.

B. Intranet web service applications via CSGNet/CGEN are not always held to the above architectural requirements.

C. This Standard does ***not*** apply to Tenant Managed Services (TMS) Basic or Premium.

D. This Standard does not apply to development-only environments where no confidential, sensitive, and/or personally identifiable information is processed, stored, or transmitted and is not publicly accessible.

E. Exceptions to this Standard must be documented and will be considered on a case-by-case basis. Requests for an exception to this Standard must be submitted via the Security Policy/Standard Exception Request Form, TECH 358.

SECTION 4: AUDITING AND REPORTING

A. Auditing may be performed on a periodic or random basis by the Security Management Branch or its designees. In the event an audit determines this Standard is not being applied, notification will be sent to the appropriate person(s) for remediation.

B. Any known violations of this Standard must be reported to the CDT Chief Information Security Officer and the reporting employee's immediate supervisor.

SECTION 5: AUTHORITY/REFERENCE

Security Policy/Standard Exception Request Form, TECH 358
OWASP Top Ten

Please contact your OTech Customer Representative for the below document:
3100 - Acceptable Use Policy