Public Facing Architecture Standard

Travis County

Information Technology Services

Revision: 2.1

Abstract

The Public Facing Architecture Standard document's purpose is to facilitate the deployment and maintenance of externally facing web sites, web services and hosted applications for Travis County. Having this standard will increase the speed of implementation by both internal Travis County application development teams and outside vendors and partners as well as establish a relatable standard for this type of environment.

Travis County adopts the "n-Tiered" architecture approach to establish a set of standards to match simplified and complex system designs in current technology. This approach will allow for flexibility in deploying and administering the highly varied solution architectures that the Travis County Information Technology Services department encounters and reduce the effort required to force all solutions to conform to the same rigid standard.

This living document will be accompanied by a regularly meeting architectural review board to ensure the standard does not become dated and irrelevant. Regular review and revision will also allow the Architectural Review Board to understand trends and changes in the marketplace and react quickly to those variations.

Table of Contents

Purpose for an Architecture Standard

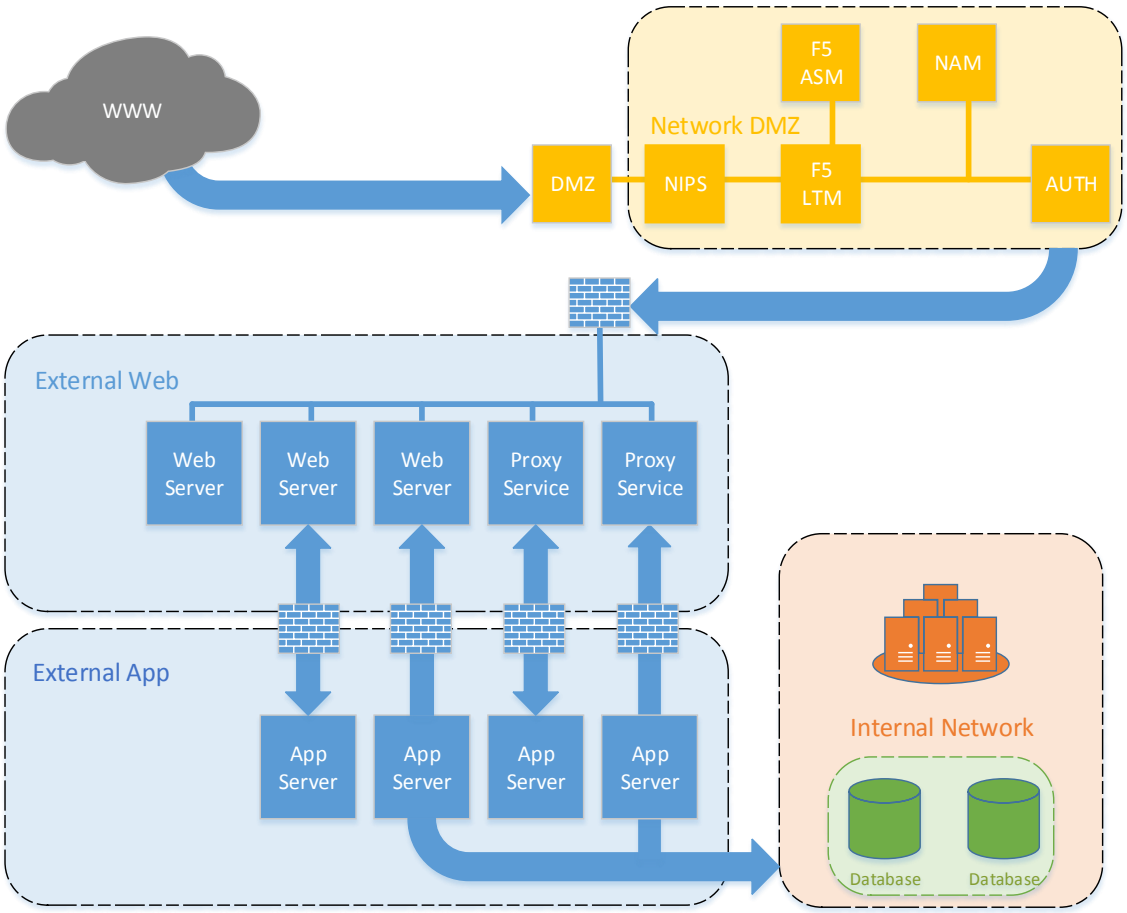
The Architecture Standard aides in ability of ITS to administer security and infrastructure controls to maintain an healthy and protected externally facing environment. The standard will allow the application development team, partners and vendors to have a reference architecture for implementing new solutions.

"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.

Servers, firewalls and networks can be either physical or virtual with the assumption they provide the same level of logical separation to match the purpose of the division. Out-of-Band Management should be used to access any device within the Public Facing Architecture.

"n-Tiered" Network Architecture Diagram



Network DMZ Tier

All network devices should be configured with access control lists to only allow approved communication from a specific source device, range, or network to a specific destination. Unnecessary or unused ports, protocols, and application services should be disabled. Application layer firewalls should be configured with least privilege to allow only specific communication required for the web application to function properly. When performing administrative functions on devices in the Public Facing Architecture, the use of SSH should be used where feasible.

All communication, known as "data in transit", regardless of data classification, should be encrypted from the client to the external web tier. For data classified as private information, the use of secure communication encryption mechanisms must be used from the client to the database in all tiers. Private data at rest must be encrypted. The data classification standards will dictate which data is considered public or private by Travis County ITS.

The Public Facing Architecture should be protected utilizing Network Intrusion Prevention System, Behavioral Malware Detection Appliances and related firewall appliances.

- Publicly accessible File Transfer Protocol (FTP) servers using a secure file transfer
- Proxy servers
- Behavioral Malware Detection Appliance
- Email gateways
- Streaming Video servers
- Incoming fax servers and incoming/outgoing fax servers
- Public-facing Domain Name System (DNS) servers
- Edge Router
- Network Intrusion Prevention Servers

Authentication Component (as required)

Internet-exposed applications fronted by the reverse proxy solution have the option to be authenticated or unauthenticated. In the case of an authenticated application, the reverse proxy accelerator is configured with an authentication contract that requires a user provide a user name and password before being granted access to the application. When credentials are provided, verification of those credentials is performed against a synchronized LDAP repository and access is granted.

For additional security, authorization services requiring a user to meet a predefined set of criteria, for example, membership in a group, are also available. Active Directory domain controllers should not be exposed to the DMZ nor should Active Directory domain controllers be placed in the DMZ for authentication purposes. Other mechanism to consider should include certificate based (X.509) and local accounts.

Passwords should comply with the Travis County password policy. No password should be allowed to traverse the DMZ in "clear text". Local accounts should not be created on the device if possible – all efforts should be made to minimize local accounts, especially privileged accounts (administrator level accounts).

External Web Tier

The external web tier or web layer, is the outward facing level of the application. It is used to provide services to the outside world without allowing the outside world direct access into the internal network. Where applicable, HOST files should be used for mapping IP addresses to hostnames for devices in this tier and the external app tier.

Host Intrusion Prevention should be installed and configured on all devices that communicate with or are in the DMZ. All HIPS services including the local firewall should be enabled on all devices where HIPS is installed. All open system devices in the DMZ which can have third party software installed on them, such as Linux or Windows devices, should have anti-virus software installed on them.

All systems in the External Web Tier should have their operating systems hardened. System hardening consists of disabling unneeded or high-risk services/protocols on the local device. Devices should not have administrative backdoor access. Base system hardening should be configured using a standardized image or template by referencing the Travis County Server Hardening Standard document.

Listed below are system components that must reside in the External Web Tier:

- Public-facing web servers
- External web sites
- Web Services – SOAP over HTTPS

External Application Tier

The external application tier resides between the external web tier and the database/internal 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 external 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
- Systems "processing" information
- ESBs and Message Queueing
- Project specific traffic management and security components that permit the above devices to function effectively and securely

Database/Internal Tier

The database/internal 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 database tier.

No DMZ device should store data classified as sensitive. All sensitive data should reside on internal network servers and that are encrypted. Data presented to the DMZ should have appropriate authentication mechanisms over a secure communication channel.

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

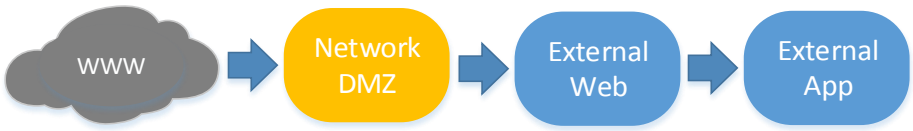
- Databases, database servers, and file servers
- Storage area networks and network attached storage
- Internal DNS servers
- Database archive and reporting servers
- Devices storing confidential or sensitive information
- Internal application servers

Standard "n-Tiered" Architectures

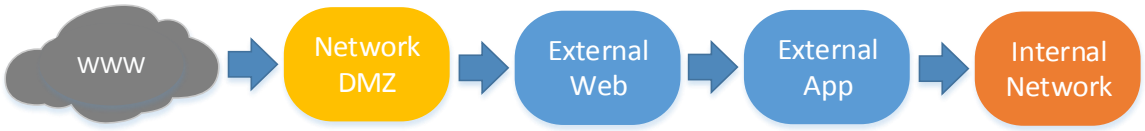
Descriptions for the "n-Tiered" Architecture Diagram

1. Public Web Server(s). One or more simple web servers are needed to serve static pages.

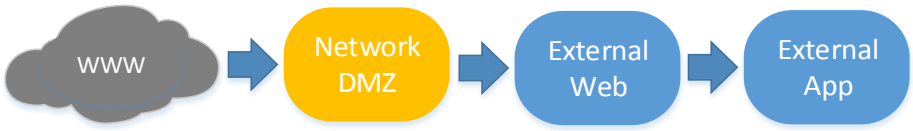
2. Public Web Server(s), Application Server. Application/business logic functions are needed in addition to web services, but no data/database functions are required.



3. Public Web Server(s), App Server and DB. This extends the #2 instance; where, data/databases services are also needed and are placed into the Database Tier.



4. WAF Proxy Service, Web/App Server(s). This is similar to #2 but there are preexisting 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.

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).

Architecture Review Board

The Travis County ITS Architecture Review Board will consist of representatives from each of the following groups: Application Development, IT Security, Systems Administration and LAN/WAN (Network Operations). This group will be responsible to agreeing on a standard architecture and the processes that surround this document.

Regular Review Intervals

The Architecture Review Board will meet semi-annually to address any changes in technology or process so that this document is maintained and relevant.

Architecture Exception

Travis County ITS will require that any proposed implementation that cannot conform to the established "n-Tier architecture" approach must present justification to the Architecture Review Board for consideration and approval. These requests should be rare, as compelling evidence will be required to gain the exception. Travis County will prefer that where feasible, implementations of new solutions make reasonable effort to adhere to the "n-Tier architecture". A granted exception will only be valid for the solution it is granted against and may not convey to a similar or expanded solution or deployment. If a high number of exceptions are being requested to take advantage of a new technology or changes in technology, the Architectural Review Board will consider revising the standards to include this new development.

Current running solutions that fall outside the approved architectures will be individually evaluated to determine their level of risk and requirement to be altered to adhere to the standards. Solutions that are unable to adhere to the standard and possess an unacceptable level of risk to be granted an exception may not be allowed to exist on the Travis

County network. This effort will reduce the risk of this solution to compromise other solutions or the environment.

Auditing and Enforcement

All devices in the DMZ should be actively and passively scanned for vulnerabilities on a regular basis. All vulnerabilities should be reviewed for their level of risk posed to the system and patching/remediation can be adjusted based on that risk. This applies to embedded devices, applications, and operating systems.

Appendix

Revision History

Date	Description	Revision
6/25/14	Initial Draft Document	1.0
8/25/14	Initial Release Document	2.1