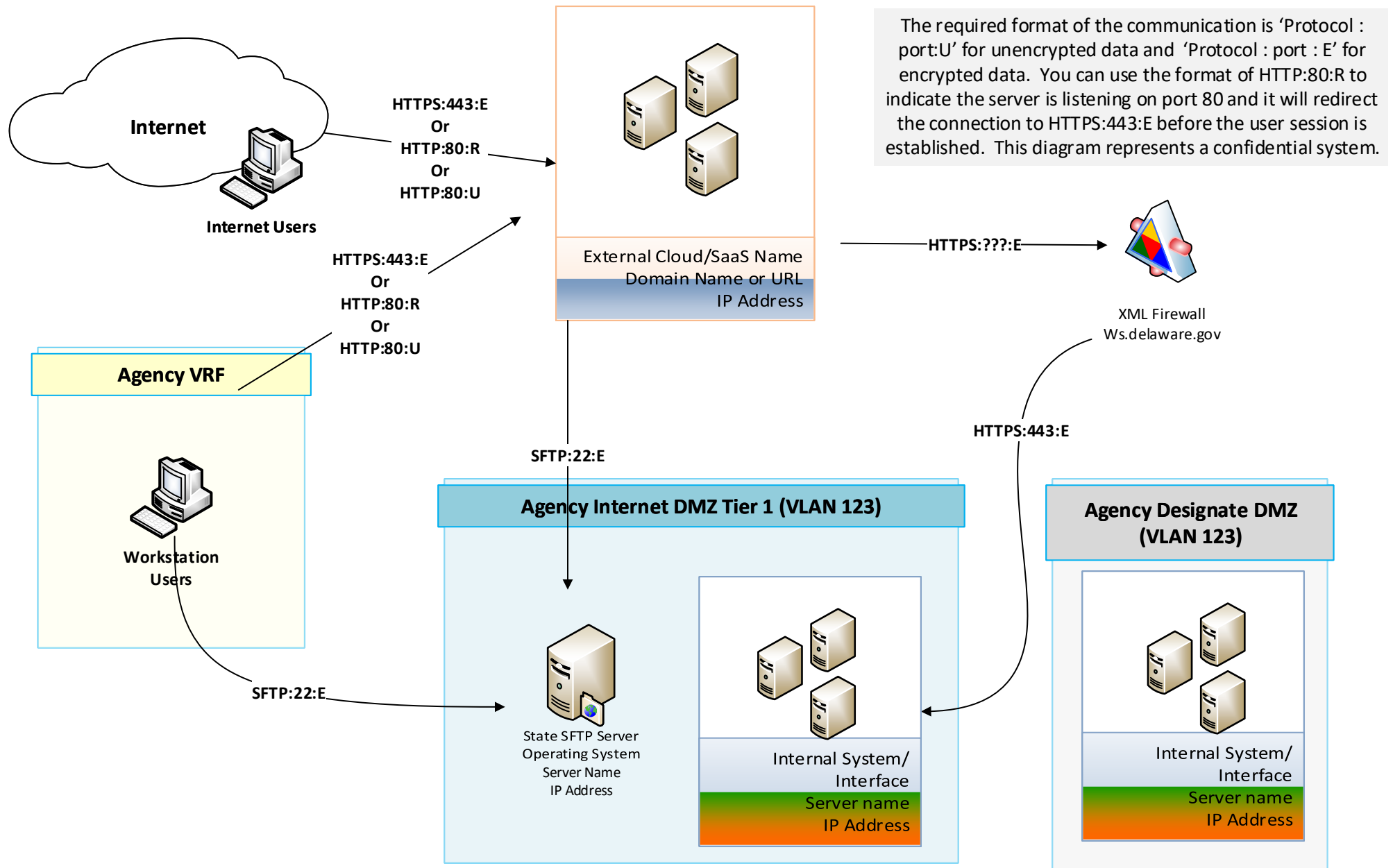
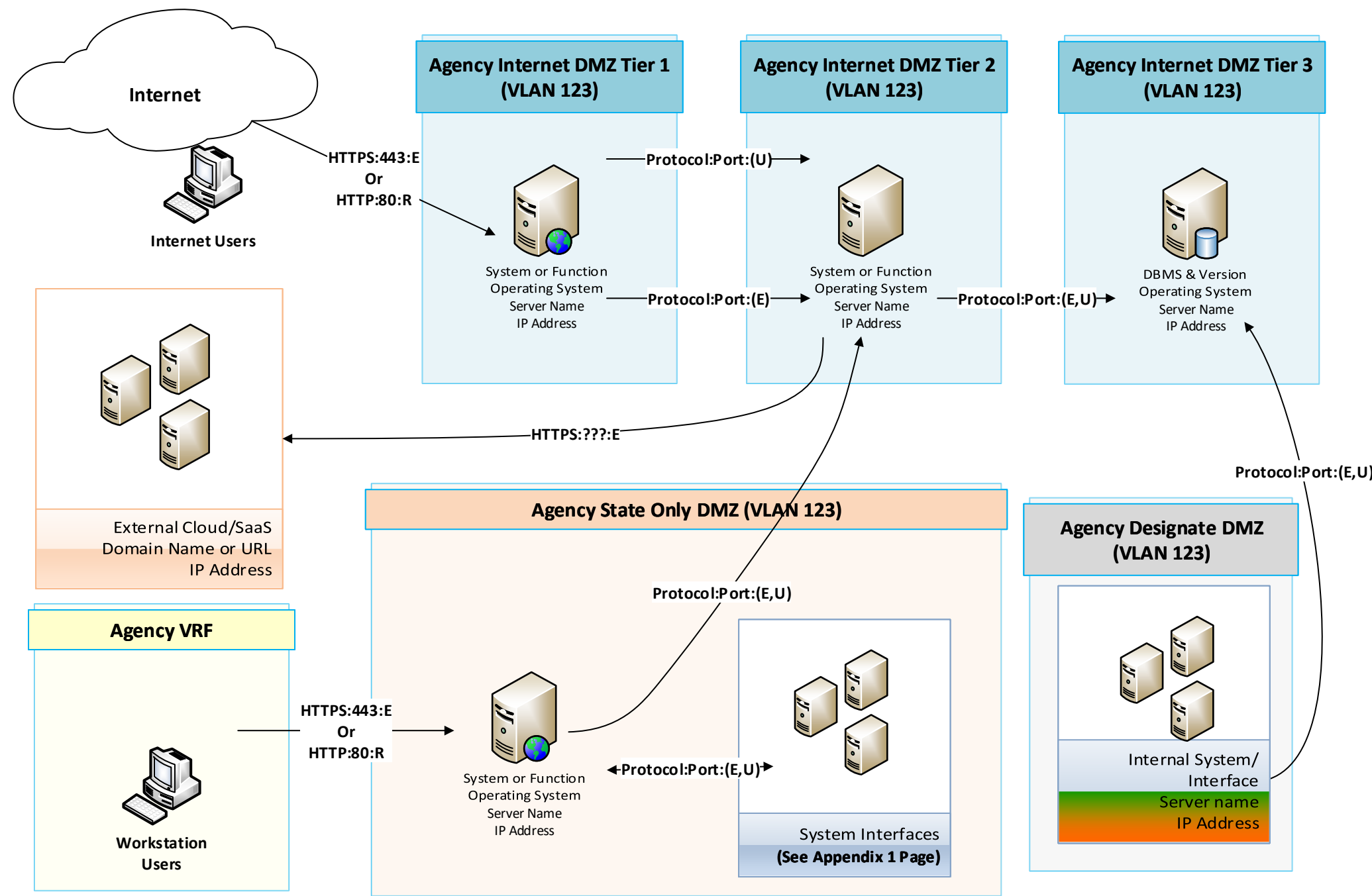
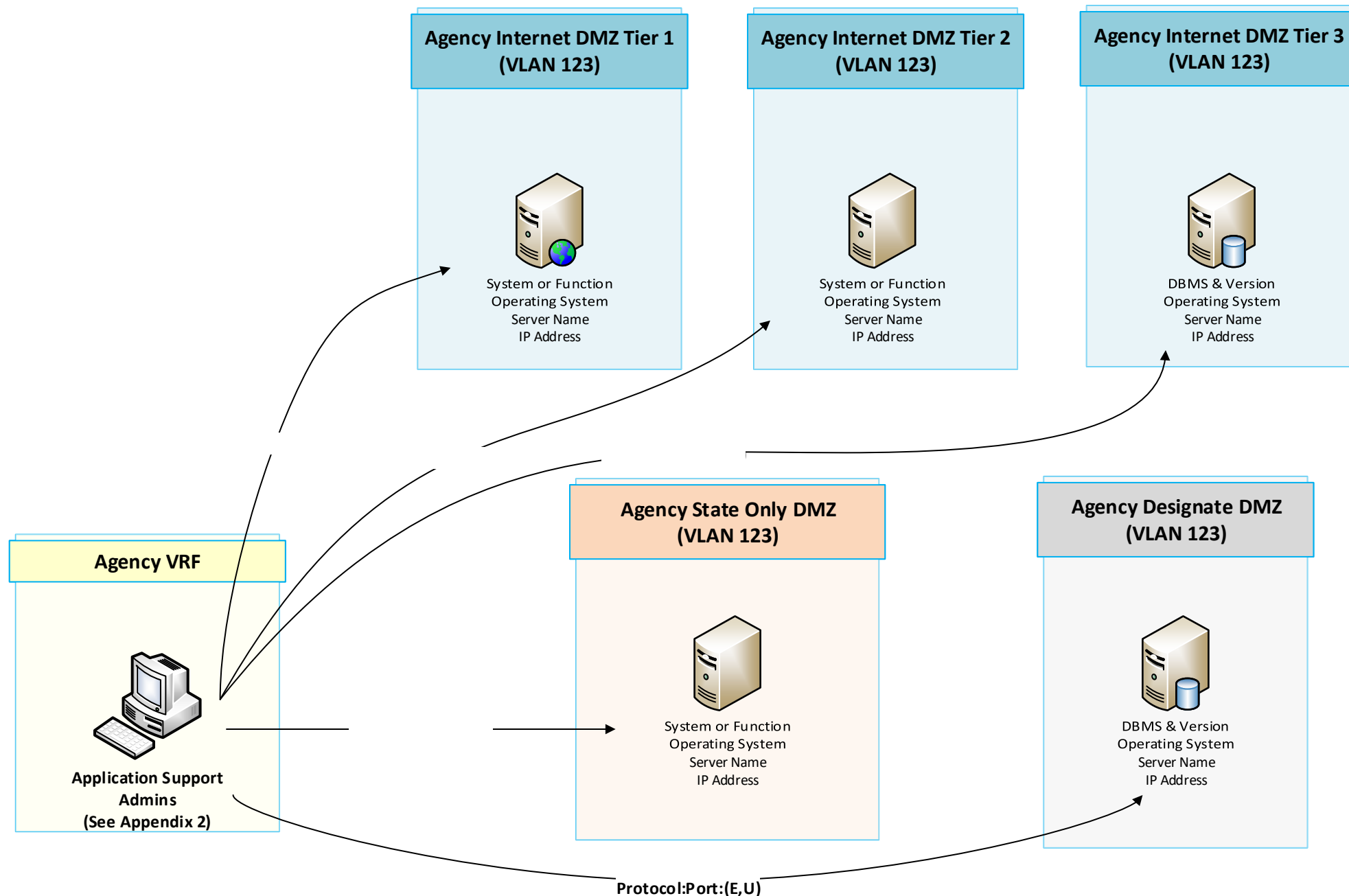


[illegible]



Drawing Name: Name of Application or System	Description: Brief Description of Application or System	Agency Logo	Agency Name
Creation Date: Date of original diagram			
Data Classification:			
Page: 2 of 9			
	Revision Date: May 6, 2019		
	Revision Engineer: Last person to revise diagram		





Drawing Name: Name of Application or System	Description: Brief Description of Application or System	Agency Logo Agency Name Confidential Information
Creation Date: Date of original diagram		
Data Classification::		
Page: 4 of 9		
	Revision Date: September 10, 2026	
	Revision Engineer: Last person to revise diagram	

[illegible]

Overview

The purpose of this document is to explain how to construct a proper network diagram that can be submitted to the Application Review Board (ARB). By adhering to these instructions, the ARB can more quickly review and recommend the network design. This document is accompanied by a reference diagram with examples of how Production, Test, Development and Support diagrams. The ARB requires at a minimum the Revision and Production tabs to be completed in order to perform a system design review. A Visio stencil has been created that will accompany the Network template defining the required object information that can be used to build your own network diagram.

Network Diagram Objects

A network diagram defines the users and objects that make up a complete system. All objects that make up a network diagram are provided in the Visio stencil set that accompanies this document. Please define all required information that is associated with the stencil objects. The basic system diagram objects are:

- User Workstation – This object represents a PC that sits on the state network (or is connected to the state network via a SSL/VPN connection) and will be accessing an object within the application. This is considered a secured workstation.
- Internet Users – This object is a cloud and PC and represents any workstation anywhere on the Internet that may access this application. This is considered an unsecured workstation.
- Extranet segments – Network segments – There are 4 unique network segments identified in the template: **Level 1 (Commonly referred to as Internet tiers 1, 2, 3), Level 2 (Built as needed), Level 3 (Commonly referred to as the State only DMZ), Level 4 (Commonly referred to as the agency Intranet)**. These are network segments on the state network that will hold servers that make up the application. The network segments are color coded based on the audience. The DMZ and VRF designated are required, VLANS assignments are optional.
- Load Balancer – This is a generic icon that represents a load balancer appliance (hardware or software). A load balancer icon should identify at a minimum the Virtual IP (VIP) assigned to the device and the DNS name assigned to that IP.
- Proxy Server – This is a generic icon that represents a proxy server appliance (hardware or software).
- Server – (Application, Database, SFTP and Web) – These are the basic object of a system. A server is a physical or virtual compute device that is providing some type of service that is being consumed. A server can be, and typically is, a Windows server or a Linux server, but could also be a hardware appliance. Servers must identify at a minimum the IP address and DNS name assigned to that IP. The OS and version must also be identified on the server object. Database Server must also identify the software and version of the database management system (DBMS). Servers must exist inside a network segment.
- Internal System Interface – Occasionally, systems will need to interface with other State systems. In this case, please use the internal system interface object to reference the “other” State system that talks to this system (or that this system talks to). Do not attempt to diagram a second system on this system diagram. The internal system interface must identify the name of the other system, IP address and DNS name assigned to that IP address. (Note: Visio Stencil Object will have to be Ungrouped in order to modify the text information.)
- External Cloud or SaaS – Occasionally, systems will need to interface with other external Cloud or SaaS solutions. In this case, please use the external Cloud and SaaS object to reference the “other” external solution that talks to this system (or that this system talks to). The external Cloud or SaaS must identify the name of contracted solution provider, the registered domain name or web uniform resource locator (URL), and the IP address. (Note: Visio Stencil Object will have to be Ungrouped in order to modify the text information.)

Connecting System Diagram Objects with Connectors

Connectors represent network communications between two objects. A diagram must contain **ALL** connectors between objects for the application to function. Connecting two objects in the same network segment are required.

Connector Directionality

Connectors must always have a single arrowhead indicating the direction that communication between two objects is **INITIATED**. Bi-directional communication (object A will initiate a connection to object B and object B will initiate a connection to object A) is only allowed between network segments in very special circumstances and should be considered “disallowed”. Bi-directional communication within a single network segment is permitted, however.

Connector Description

A connector must identify the protocol, port and whether encryption is used in communication between source and destination objects. The required format of the communication is ‘Protocol : port:U’ for public data and ‘Protocol : port : E’ for non-public data. You can use the format of HTTP:80:R to indicate the server is listening on port 80 and it will redirect the connection to HTTPS:443:E before the user session is established. The term ‘AD group’ may be used on the connector description to represent all of the DTI telecom approved ports/protocols required to talk with Active Directory and Domain Controllers.

Connector Source & Destinations

Connectors show communication from a source object to a destination object. Different objects imply different meanings. This is a list of what connections from and to different objects means:

- Server – Connections to (or from) a specific server means that **ONLY** that source (or destination) are permitted to use the communication specified on the connector. This is the most typical type of communication. Communication between network segments that is not identified should not be assumed permitted. It **IS** mandatory to document all server to server communications.
- Network segment – Connections to (or from) a network segment means that **EVERY** machine in that network segment can initiate (or receive) communications identified on the connector. This is not a normal situation and will need justification.