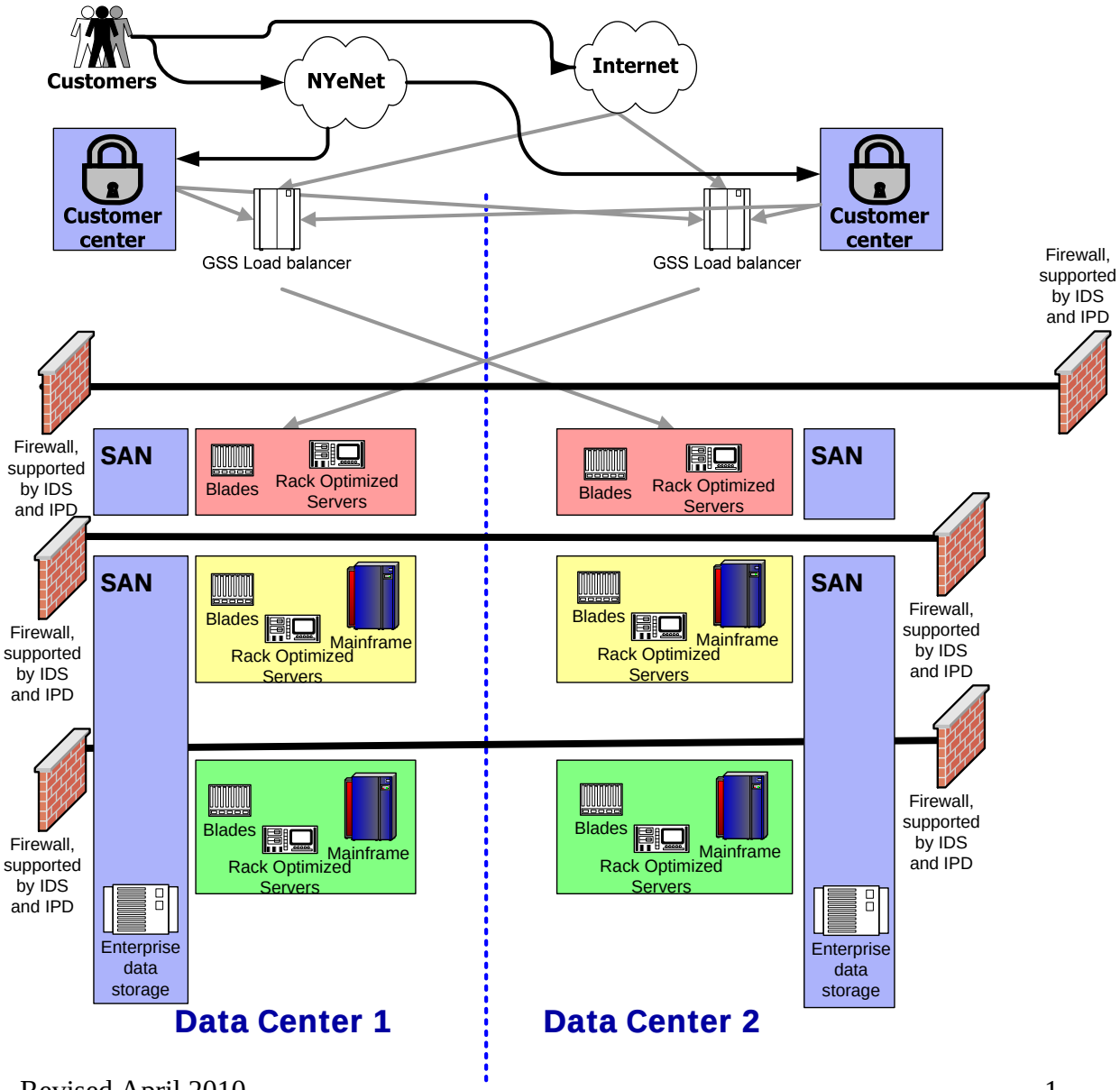
Enterprise Architecture Focus Item – Three Tiered Architecture

Introduction:
The Chief Information Officer/Office for Technology (CIO/OFT) is working with State Data Center (SDC) customers on deployment and migration strategies, in which the customer's applications can take full advantage of the benefits of the SDC infrastructure. A cornerstone piece of the infrastructure is the multi-data center three tiered architecture (TTA).

Description:
CIO/OFT's design for TTA is similar to the designs that are commonly described in white papers and best practices documents available from familiar industry sources. At its most basic level, the design calls for physical separation of the application delivery components into tiers. In this regard, the presentation layer resides in tier 1, the business logic and application serving components in tier 2, and the data and database components in tier 3.



As the diagram depicts, a "hard separation" exists between the tiers. Communication flows between the tiers are strictly controlled and protected. High performance and high availability firewall devices, along with intrusion prevention systems are in place to control and monitor the data as it crosses the tier boundaries.
The principles used in the creation of the design are:

- Business logic or non-public data will not reside on Tier 1

  The resources deployed in tier one, are classified as the most vulnerable. Any data that is resident on a tier one device, therefore is considered to be vulnerable to unauthorized access or alteration. For that reason, our design calls for data to be located in a more appropriate location, preferably tier 3, whenever possible.

- User does not access business logic or database directly

Speaking in terms of access from the perspective of communication flows, the design calls for all user sessions to terminate in tier 1. Sessions that do not originate from tier 1 servers will not pass the firewalls separating tier 1 from tier 2. By the same token, sessions that do not originate from tier 2 servers will not pass the firewalls separating tier 2 from tier 3. *Where non-OFT hosted servers are required to access tier 2 devices, Host Intrusion Prevention Devises (HIPS) are required*

- Separate and secured access for administration of servers

All the servers in the environment will be connected to a separate administrative network, in which all maintenance, administrative activity, and enterprise systems management and monitoring will occur.

- Intrusion prevention at both protocol and content levels

Active scanning will take place on all data flows traversing tiers, in OSI layers one through Seven.

- Each tier has increasingly stringent security filters

The firewall rules are strict. Communication between servers will only be enabled on very specific ports. A function that requires direct communication to workstations, without a proxy/reverse proxy in tier one is not acceptable. NetBIOS traffic will not be enabled.

- Simple and proven design decreases vulnerability

The design is built on industry standard concepts and best practices.

- Load Balancing at each tier

Load balancing at each tier will be provided by intelligent network load balancing devices.

- Load Balancing across Data Centers

Load sharing across data centers will be provided via network global site selection products at above tier 1. Applications requiring this level of availability and which are planned to be implemented in the TTA should be architected to accommodate this.

- Legacy Tier

For applications that cannot be architected to abide by the rules of the TTA, the SDC provides another network referred to as the Legacy Tier. The Legacy Tier allows all communications between servers within that tier. Although inherently less secure than the TTA, the Legacy Tier still provides greater redundancy and security than the old Legacy network the SDC is migrating servers out of.

Standards

Production network

1) All user communication sessions into three-Tier environment terminate on tier 1 NYeNET or tier 1 Internet
2) Tier 1 NYeNET or tier 1 Internet servers can communicate only through firewalls to: tier Application servers, Legacy servers and other tier 1 Presentation servers as needed
3) Tier 2 Application servers can communicate only through firewalls to: tier 3 Data Base servers, Legacy servers, and tier 2X Application servers, as needed
4) Tier 3 Data Base servers can communication only through firewalls to: tier 2 Application servers, tier 2X Application servers, and other tier 3 Data Base servers as needed.
5) NYeNET customer can access both NYeNET and Internet Tier 1. Internet customers can only access Internet Tier 1.
6) Outbound traffic to the Internet is only granted to from Internet Tier 1.
7) With the exception of the Legacy tier, security is implemented within each tier to block server to server traffic, except where required.
8) Network connectivity standards are two 100 megabit copper connections running IP protocols for production network, one 100 megabit copper for admin LAN and 1 Gigabit copper for IP backup. Some networks are trunked over the same physical network on servers hosting virtual guests.
9) Each tier will be protected via a combination of a firewall and intrusion prevention device that in combination provide inspection of protocol and application layers.
10) A separate network for administration of servers and network equipment will be provided at each data center. This LAN will be used by server and network administrators as well as by Enterprise Systems Management servers. User access for administrator access to tier 2 or tier 3 will be via client VPN or SSL VPN.
11) Capability to provide a private connection between servers on Data Base tier 3 for Data Base server writes synchronization between primary sites for high availability application requirements. The capability provided is via layer 3 connections as required.
12) Netegrity (NYSDS) is the preferred method for of application authentication and authorization for users.
13) Server Load balancing appliances will be provided in each tier except for tier 3. These load balancers will communicate with global load balances at each primary data center to allow for application load balancing between primary data centers and to provide options for disaster recovery.