INT NETLINK's Past Projects

Data Centre Network Infrastructure Design Consultancy

Afghanistan

Government Department was planning to implement a New Data Centre based on the latest available technology with a strategic view for both Networking and Security Architectures.

INT Netlink consultancy provided detailed recommendations of both Network and Security architectures of Data Centre. In the following, we present the building blocks of the recommended Network and Security Design, covering the following areas or tiers:

- Data Centre Perimeter Network
- Data Centre Public Secure Zones Network
- Data Center InternalSecure Zones Network

INT Netlink Consultancy will address the security design attributes on each of these areas in compliance with Netlink Layered Security Architecture that enhances the security posture of best common practices and International standards security deployments.

Brief On Design Philosophy and Solution Architecture

INT Netlink consultancy for Govt Department will cater to design strategy which will build a carrier grade resilient network over none blocking topologies where all network elements are operating in active-active mode and responding to service requests simultaneously. Netlink vision of active-active mode of operation is not only reflected on network design but also on security design architecture.

This design philosophy maximizes the utilization of Data Centre resources and minimizes the cost of expensive equipment such as security devices etc…

The primary goal of this design architecture is to provide an environment capable of following the typical business model of dynamic change. This design model is capable of starting small and growing exponentially with changing demand by incrementally increasing the number of equipment that provide logical services to the appropriate client load.

This growth is built on a solid architectural foundation that supports high availability and a secure and manageable infrastructure.

Scalability. All components of the architecture support scaling to provide continuous growth to meet user demand and business requirements.

Availability. Components of the architecture provide redundancy or functional specialization to contain faults.

Security. The architecture provides an end-to-end security model that protects data and the infrastructure from malicious attacks or theft.

Manageability. Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment.

Scalability

The Data Centre architecture scales the number of unique users supported by cloning or replicating front-end systems. This scaling is coupled with a stateful load-balancing system to spread the load across the available clones. Partitioning the online content across multiple back-end systems allows it to scale as well. A stateful content-sensitive load-balancing system then routes requests to the correct back-end systems.

Availability

Front-end and Back-end systems on all layers are made highly available and scalable by using multiple cloned devices that are then load balanced using the Network Load Balancing service of Netlink Application Switches.

Security
To implement an appropriate security strategy, the architecture is broken into separate physical networks or network segments. This allows for the compartmentalization of the system so that a partial compromise of the system does not result in data loss.

The security architecture also maintains secure interfaces to external private networks such as disaster recovery sites, terminals' networks and customer partners' network that require access to Data Centre services.

The perimeter network includes Internet Gateway routers, Load balancing systems, SSL VPN gateway, Application switches and Threat Protection System.

The public network tier offers Government's public services to Internet clients and might include the following security zones:

Web-Service – eTicketing.
Internet Services Zone - Mail relay, DNS Service, SMTP etc.…
VPN Services Zone – provides IPSec and SSL-VPN service termination
Online Backend Services
Web Backend service
Collocation Space and Securities

Govt. Private Tier provides might include the following security zones:

Storage Network Zone
Database
Secure interfaces to Terminals and partners network
Manageability
Management and operations broadly refer to the infrastructure, technologies, and processes needed to maintain the health of an Internet application environment and its services. The goals of an overall management system are mapped into the following key areas:

Monitoring and alerting. Keeps track of key events happening in the system and helps to identify the bottlenecks in the system.
Content management. Allows the system to evolve in a controlled manner as requirements change.
Remote management. Allows the system to be managed from remote locations that help to improve system supportability.
Backup and restore. Allows the various systems to be comprehensively backed up. This will then allow any or all systems in the architecture to restore as required.

Perimeter Network Design
The perimeter network separates the outside network or public Internet network from an internal network of the organization. Perimeter network devices include border routers, caching servers, and firewalls. These devices provide connectivity, network security, and network availability.
To create a perimeter architecture that adequately protects the organization while letting people do their work, you need to make sure that the design reflects the way in which the services are used and configured and at the same time provide all necessary security measures against all possible threats. Perimeter security based on Layered Security architecture can help mitigate these threats by segregating Internal Govt network from the Internet.

Layered Security architecture as a concept goes beyond the protocol to an architecture and orientation of protecting information. This includes not just routers, firewalls, and VPNs, but policy, system hardening, intrusion detection, and software architecture.

Perimeter network composed of the following elements:
Hardened Internet Perimeter Router to provide access to Internet
Network Application Switches with Intelligent Traffic Management (ITM)
SSL accelerators and VPN Gateways
Intrusion Detection System

Internal Private Zones Network Design

The internal network behind the internal firewall consists of separate functional areas that are divided into network segments or VLANs. Implementing VLANs allows maximum isolation of different segments and increases security and management of data flow between application components.

The internal network for the DC architecture might consist of the following VLANs:
Database VLAN
Management VLAN
Back-end servers VLAN
purpose build applications VLAN

Disaster Recovery with Active-Active Data Centres

The primary objective of disaster recovery is to protect the organization in the event that all or parts of its operations and/or computer services are rendered unusable. Disaster recovery is the process of reacting to a disaster by being able to provide computing services from another location. In most cases, the countermeasures you employ to be able to recover from a disaster are entirely different from the solution you use to achieve continuous availability.

Data Centres Integration with Terminals Network

Integration of the Data Centres with terminals networks has been maintained with the consideration of the fact that the two terminals act as two separate business entities. Such consideration requires a design that assures the faults, which occur in one of the terminal networks or Data Centres, not to be reflected on other terminal or Data Centre. While maintaining all these requirements other features such as active-active mode of operation, quick failover convergence time and traffic load sharing have to be maintained at the same time.

Threat Protection System –TPS

Intrusion Detection/Prevention is quickly emerging from a niche market technology to core network infrastructure. Viruses, worms and other forms of attacks are proliferating against corporate networks at an increasing rate. The need to defend against these threats is driving the demand for technologies that would mitigate and prevent threats to networks.

Intrusion Sensors (IS): The sensors are placed at different locations on the network in an offline mode. Typically, sensors are connected to mirrored ports on a switch and monitor all the traffic traversing that port. Sensors are configured with the policy (rules) which determines the security policy that the sensor implements. The rules can be setup on the sensor directly using the sensor GUI or pushed down from the Defense Center.

Defense Center (DC) The Defense Center provides central management of up to one hundred (100) Network Sensors. The DC allows for

Group sensors by location, department, purpose etc
Develop policies per group
Update/distribute policies by group
Maintain group configurations

INT Netlink's strategy to address this reality is to provide a comprehensive portfolio embedded with all required features that when put all together provides the key attributes in building High Performance Data Center network and security solution that provides the following key attributes:

Disaster Recovery solution with Active-Active Data Centers

Product features to provide True Active-Active network infrastructure within the Data Center design

Multi-tier network Architecture, Layered Security Architecture based on Defense on Depth security guidelines, Vertical and horizontal scalability, Pay-As-You-Grow architecture , Unified Management Solution