**BẢNG THEO DÕI SỬA ĐỔI**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Trang** | **Nội dung sửa đổi** | **Ngày có hiệu lực** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Biên soạn** | **Kiểm tra** | **Phê duyệt** |
| **Chữ ký** | **Nguyễn Xuân Cảnh** | **Vũ Anh Tuấn** | **Ngô Vĩnh Quý** |

**1. Mục đích**

* Mô tả, định nghĩa các thành phần cơ bản của hệ thống CNTT.
* Giúp hiểu rõ hơn về chức năng nhiệm vụ của từng thành phần cơ bản của hệ thống Công nghệ thông tin

**2. Phạm vi áp dụng**

* Áp dụng toàn Trung tâm Giải pháp Công nghệ thông tin và Viễn thông.

**3. Tài liệu liên quan**

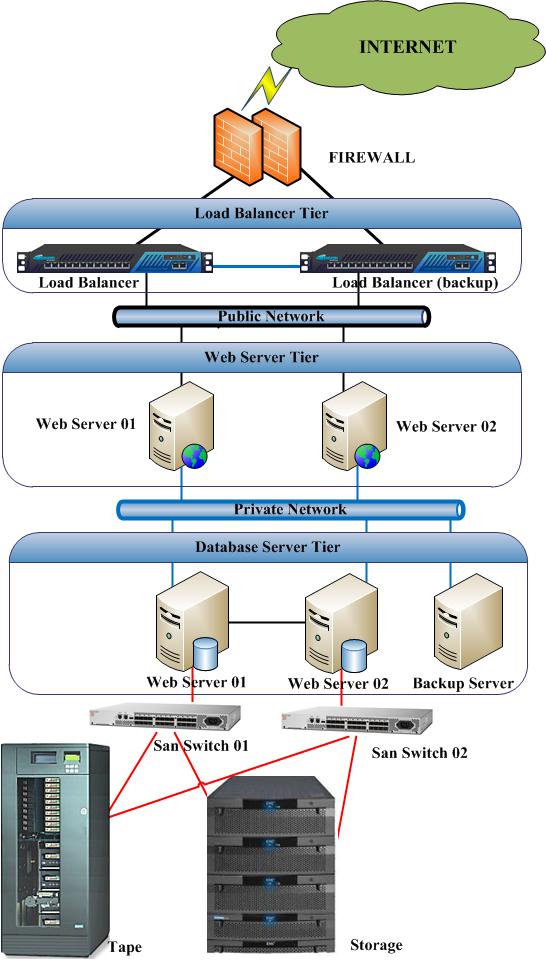
* Không có

**4. Định nghĩa và thuật ngữ**

|  |  |  |
| --- | --- | --- |
| **STT** | **Từ viết tắt** | **Giải thích** |
| 1 | Firewall | Thiết bị tường lửa |
| 2 | Load Balancer | Thiết bị cân bằng tải |
| 3 | Web Server | Máy chủ ứng dụng |
| 4 | Database Server | Máy chủ CSDL |
| 5 | San Switch | Thiết bị chuyển mạch quang |
| 6 | Storage | Thiết bị lưu trữ trên đĩa cứng |
| 7 | Tape | Thiết bị lưu trữ trên băng từ |
| 8 | Backup Server | Máy chủ sao lưu dự phòng |
| 9 | Network | Hệ thống mạng |
| 10 | FC | Kết nối quang |
| 11 | HBA | Card kết nối quang |

**5- Nội dung**

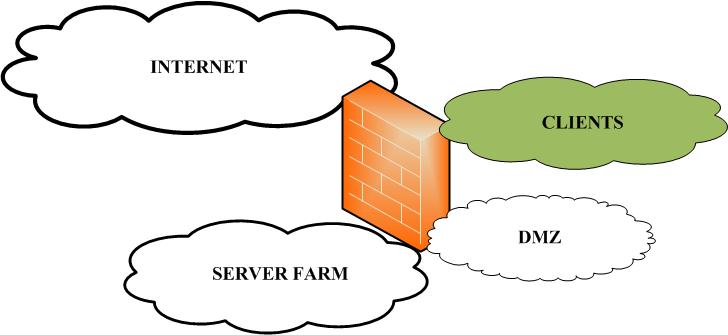
***5.1 Sơ đồ hệ thống CNTT cơ bản***

******

***5.2 Mô tả***

***5.2.1. Firewall***

* Thiết bị tường lừa được đặt ở ngoài cùng của hệ thống, làm nhiệm vụ kiểm soát các truy cập vào ra hệ thống, đảm bảo an toàn cho hệ thống may chủ triển khai ứng dụng
* Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet. Cụ thể là:
  + Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài (từ Intranet ra Internet).
  + Cho phép hoặc cấm những dịch vụ phép truy nhập vào trong (từ Internet vào Intranet).
  + Theo dõi luồng dữ liệu mạng giữa Internet và Intranet.
  + Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.
  + Kiểm soát người sử dụng và việc truy nhập của người sử dụng.
  + Kiểm soát nội dung thông tin thông tin lưu chuyển trên mạng.
* Các hãng cung cấp thiết bị tường lửa: Cisco, Fortinet, Checkpoint , F5 ...
* **Cách thức triển khai:**



* + Thông thường triển khai Firewall cho hệ thống CNTT thường chia làm 4 vùng để quản lý, giao dịch giữa các vùng với nhau sẽ được quản lý bằng các chính sách của Firewall
    - Vùng Client: là vùng người dùng hệ thống
    - Vùng DMZ: vùng chứa các máy chủ dùng chung cho hệ thống: AD, mail, antivirus server ...
    - Vùng Server: là vùng chứa các máy chủ triển khai hệ thống
    - Vùng Internet: vùng người dùng ngoài hệ thống
  + Firewall thường được triển khai 1 cặp, hỗ trợ cấu hình Active – Active hoặc Active – Standby

***5.2.2. Load Balancer***

* Thiết bị cân bằng tải làm nhiệm vụ chia tải truy cập vào hệ thống web server hoặc hệ thống ứng dụng đã được cấu hình nhiều máy chủ ứng dụng, giảm thời gian đáp ứng và tránh tình trạng quá tải trên máy chủ. Việc chia tải hoàn toàn trong suốt với người dùng, người dùng chỉ kết nối tới hệ thống qua 1 IP duy nhất.
* Lời ích khi sử dụng thiết bị cân bằng tải:
  + Tăng khả năng đáp ứng, tránh tình trạng quá tải trên máy chủ, đảm bảo tính linh hoạt và mở rộng cho hệ thống.
  + Tăng độ tin cậy và khả năng dự phòng cho hệ thống:Sử dụng cân bằng tải giúp tăng tính HA (High Availability) cho hệ thống, đồng thời đảm bảo cho người dùng không bị gián đoạn dịch vụ khi xảy ra lỗi sự cố lỗi tại một điểm cung cấp dịch vụ.
  + Tăng tính bảo mật cho hệ thống:Thông thường khi người dùng gửi yêu cầu dịch vụ đến hệ thống, yêu cầu đó sẽ được xử lý trên bộ cân bằng tải, sau đó thành phần cân bằng tải mới chuyển tiếp các yêu cầu cho các máy chủ bên trong. Quá trình trả lời cho khách hàng cũng thông qua thành phần cân bằng tải, vì vậy mà người dùng không thể biết được chính xác các máy chủ bên trong cũng như phương pháp phân tải được sử dụng. Bằng cách này có thể ngăn chặn người dùng giao tiếp trực tiếp với các máy chủ, ẩn các thông tin và cấu trúc mạng nội bộ, ngăn ngừa các cuộc tấn công trên mạng hoặc các dịch vụ không liên quan đang hoạt động trên các cổng khác.
* Các hãnh cung cấp thiết bị cân bằng tải: F5, Cisco
* **Cách thức triển khai:**
  + Thiết bị Loadbalancer nằm giữa Firewall và các vùng máy chủ cần cân bằng tải
  + Kết nối IP từ Client connect tới Firewall sau đó tới thiết bị cân bằng tải, thiết bị cân bằng tải sẽ làm nhiệm vụ phân chia các kết nối này tới từng server
  + Thiết bị Loadbalancer cần đảm bảo triển khai active-active hoặc active - standby

***5.2.3. Máy chủ***

* Máy chủ là một [máy tính](http://vi.wikipedia.org/wiki/M%C3%A1y_t%C3%ADnh) được [nối mạng](http://vi.wikipedia.org/wiki/M%E1%BA%A1ng_m%C3%A1y_t%C3%ADnh), có[IP](http://vi.wikipedia.org/wiki/IP) tĩnh, có năng lực xử lý cao và trên máy đó người ta cài đặt các [phần mềm](http://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m) để phục vụ cho các máy tính khác (máy trạm) truy cập để yêu cầu cung cấp các dịch vụ và tài nguyên.
* Máy chủ đước sử dụng để triển khai ứng dụng, cơ sở dữ liệu, các tiến trình ...
* Các hãng cung cấp máy chủ: Dell, IBM, HP ...
* **Cách thức triển khai:**
  + Đảm bảo hỗ trợ đầy đủ các kết nối FC, Ethernet ...
  + Hỗ trợ Raid 0, 1, 5, 6
  + Đối với máy chủ Database cài Oracle RAC hoặc SQL server cluster cần bổ sung thêm card FC để kết nối tới Storage
  + Có hỗ trợ quản trị từ xa quả port ethernet hoặc port manager
  + Với máy chủ, toàn bộ các thành phần quan trọng trên nó đều được thiết kế để dự phòng 1-1 cụ thể như sau:
    - Nguồn điện: dự phòng nóng 1-1, khi một nguồn nào đó hỏng, hệ thống vẫn hoạt động bình thường và có thể thay thế nóng khi hệ thống đang online.
    - Kết nối mạng: mỗi máy kết nối ra ngoài thông qua ít nhất 2 đường kết nối lên 2 switch riêng biệt và được cấu hình bonding với nhau để tăng băng thông, chia tải và dự phòng 1-1 cho nhau.
    - Ổ cứng: Toàn bộ dữ liệu người dùng được lưu ở mức dự phòng cao hơn trên tủ đĩa. Riêng ổ local của máy chủ được cấu hình RAID 1 đảm bảo dữ liệu trên ổ này được đồng bộ với ổ còn lại. Khi một trong hai ổ gặp sự cố, có thể rút và thay thế nóng.

***5.2.4. Storage***

* **Storage Area Network ( SAN )** là một mạng riêng được thiết kế cho việc mở rộng các thiết bị lưu trữ một cách dễ dàng và các máy chủ khi kết nối với SAN sẽ hiểu như là một khối HDD đang chạy trên cục bộ .
* Việc truyền dữ liệu từ Server đến hệ thống lưu trữ SAN được sử dụng dựa trên các cổng quang để truyền dữ liệu : 1 GBb/s Fiber Channel , 2 GBb/s Fiber Channel , 4 GBb/s Fiber Channer , 8 GBb/s Fiber Channer , 1 GBb/s iSCSI ,.....
* Chi phí triển khai hệ thống SAN cực kỳ đắt , nó đòi hỏi phải dùng các thiết bị Fiber Chennel Networking, Fiber Channel Swich,...
* Các ổ đĩa chạy trong hệ thống lưu trữ SAN thường được dùng : FIBRE CHANNEL , SAS , SATA,....
* Tính năng :
  + Lưu trữ được truy cập theo Block qua SCSI, FC
  + Khả năng I/O với tốc độ cao
  + Tách biệt thiết bị lưu trữ và Server
* **Cách thức triển khai:**
  + Đầu tư Storage trong trường hợp cần lưu trữ nhiều dữ liệu, hoặc cần triển khai Oracle RAC hoặc SQL Cluster
  + Đối với tủ đĩa, các ổ cứng được nhóm thành nhiều RAID GROUP, với mỗi RAID GROUP được cấu hình raid 5 cho phép 1 ổ trong RAID GROUP lỗi hệ thống vẫn hoạt động bình thường. Mặt khác, để làm tăng khả năng sẵn sàng của tầng dữ liệu cực kỳ quan trọng này, trong giải pháp đề xuất có đầu tư thêm cho mỗi khay một ổ dự phòng (spare). Ổ dự phòng này có nhiệm vụ tự động được gán vào một trong các RAID GROUP có 1 ổ bị lỗi để thay thế cho ổ lỗi đó. Như vậy với giải pháp này cho phép có tối đa 2 ổ bị lỗi đồng thời trên 1 RAID GROUP hệ thống vẫn hoạt động bình thường. Khi ổ cứng bị lỗi, ta có thể thay thế nóng các ổ này một cách dễ dàng.
  + Ngoài ra, một trong các phần quan trọng nhất của tủ đĩa là Controller, đối với thành phần thiết bị này giải pháp dự phòng cho nó là có 2 Controller chạy Active-Active. Lưu lượng luồng dữ liệu sẽ được cấu hình phân tán, dàn trải đều trên các RAID GROUP và trên cả 2 Controller. Ví dụ: Tại một thời điểm, trong điều kiện hoạt động bình thường, dữ liệu trên mountpoint /u01 được ưu tiên đi qua Controller A và dữ liệu trên mountpoint /u02 được ưu tiên đi qua Controller B để share tải. Khi một Controller bị lỗi (ví dụ Controller A), hệ thống sẽ tự động chuyển lưu lượng trên mountpoint /u02 đi sang Controller B và ngược lại. Do đó đảm bảo tính sẵn sàng và giảm tải ở mức cao nhất cho việc phân luồng và dự phòng dữ liệu

***5.2.5. San Switch***

* Thiết bị chuyển mạch quang, làm nhiệm vụ chia sẻ tủ đĩa tới các máy chủ thông qua kênh truyền quang
* **Cách thức triển khai:**
  + Triển khai 2 san switch với hệ thống storage để đảm bảo dự phòng, 2 san switch cấu hình chạy active – active
  + Trên server sẽ có hai đường kết nối FC tương đương nhau tới 2 san switch

***5.2.6. Tape***

* Là thiết bị lưu trữ dữ liệu băng từ
* Dữ liệu sẽ được backup từ Disk - > Tape một cách tuần tự,
* Băng từ được lưu trữ tại một trung tâm lưu trữ cách xa với khu vực triển khai hệ thống,
* **Cách thức triển khai:**

**6. Phụ lục đính kèm**

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên phụ lục** | **Mã hiệu** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |