

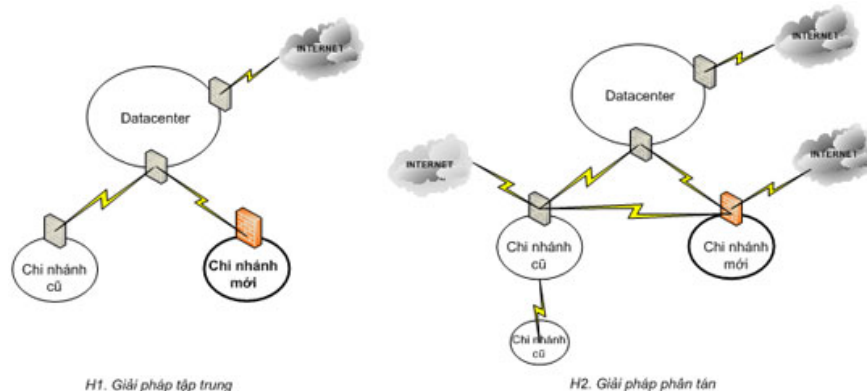
Network design for branches (Part 2)

This article will cover the process of designing firewall services for branch networks.

This article will cover the process of designing firewall services for branch networks. Problem: Company A opens a new branch. Requirements:

- The branch has about 50 employees and needs to be connected to the Internet. The branch needs to have a connection with the DataCenter.
- The branch provides information to customers and partners through the use of a Web Server containing websites. This Web Server must be separate from the branch's internal network with a firewall.
- Internet access requests from clients within the branch network must go through a firewall.
- Resources on the Web Server must be available for customers and counter partners
- At the branch, there should be 1 network administrator. The task of this person is to design a firewall service for the branch to ensure the security of information when accessing the Internet as well as to secure the branch network from unauthorized access from outside.

The first thing to consider is the concentration and dispersion of the service



- Data concentrated in DataCenter
- Branch must have connection to DataCenter
- Firewall and network infrastructure services in DataCenter must provide enough throughput to serve all branches
- The access from outside to the branch must be through DataCenter and subject to the management of DataCenter
- Low cost, easy to manage

- High probability of incidents (WAN lines) - Stored data according to decentralization on branches
- Branches can connect with other branches
- Branch firewall service must provide enough throughput to serve connections
- External access to the branch is not required through DataCenter.
- Flexible, high availability
- High cost, difficult to manage

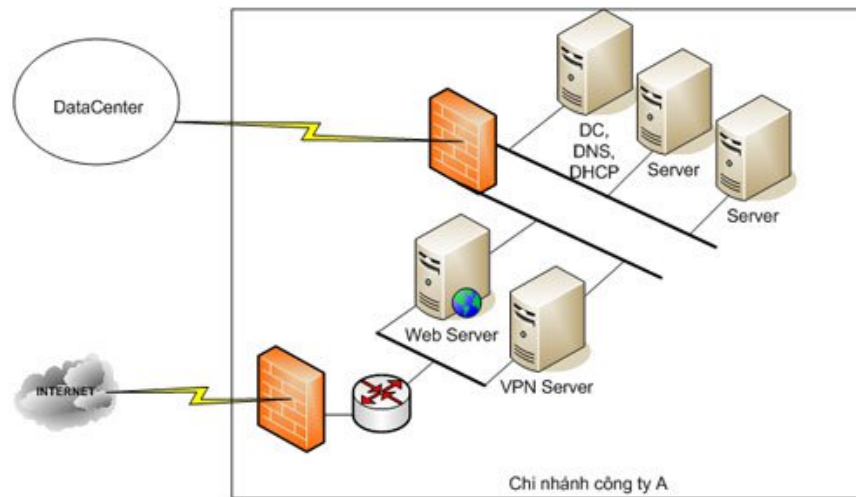
Consider access from inside out external resources

These access can be from branch network clients to DataCenter / other branch resources or to the Internet. Factors to consider:

- **Access scope** : allows only internal network clients to reach a limited group of external resources. Clients must be members of a domain and be authenticated on the firewall
- **Traffic type** : need to know the types of traffic transfer protocols that application programs run in the branch network to use. This supports the configuration of packet filtering / blocking services on the firewall.
- **Design access rules (access rules) and network rules** : use access rules to identify protocols, source networks, destination networks, access content, etc. to enforce external access. Use network rules to determine the blocking / enabling communication between networks. For example, allow Internet users to access Web Server located in the DMZ area of the branch.
- **Performance** : If you put resources at the branch, the data access speed and the availability of the service at the branch will be very high. However, a high-speed WAN connection is required to connect to the DataCenter to update, synchronize and back up data. If the branch only has a low speed WAN link, it is possible to use the firewall's caching technique to increase network performance.

Consider external access to internal resources

- **Traffic type** : need to specify how users from outside access to resources in the branch network. In some cases, the firewall may automatically block / filter packets of some common protocols. In addition to other protocols, it is necessary to monitor and configure the administrator.
- **Business function** : if the branch has the function of providing resources to external clients, it is necessary to configure the firewall service to manage access to these resources.



H3. Một cách tiếp cận của bài toán

User support design

The design of firewall services must also ensure functional requirements for clients. Detail:

- **Internet access** : if the client needs to access the Internet or Web applications, it is possible to configure a Web proxy for the branch network. After configuring the Web proxy, access requests are sent to the firewall and the firewall sends requests to the destination.
- **Accessing application programs** : If clients need access to application programs that use Winsock through the firewall, it is necessary to configure the clients appropriately for communication from clients through the firewall to the application. out smoothly.
- **User authentication** : if the branch has regulations on the classification of users to assign access to resources, the firewall needs to authenticate the user. In addition, this also allows access control to each resource object.

Designed for operation

When designing a firewall service, it is necessary to consider the operation of this service. The following factors must take into account:

- **Optimization** : the firewall service on launch must be optimized for performance. In order to do this, it is necessary to actively monitor the operation of the service through log files and warnings.
- **Support** : Need to consider the ability to support services. For example, for branches without a technical team, the firewall service needs to be configured for remote management.
- **Change** : firewall service when needed may have to change. For example, add a new second firewall to protect servers in the branch network. You may need to change the configuration of the first firewall accordingly.

You finished reading the article "**Network design for branches (Part 2)**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
