

Hardening Network Routing

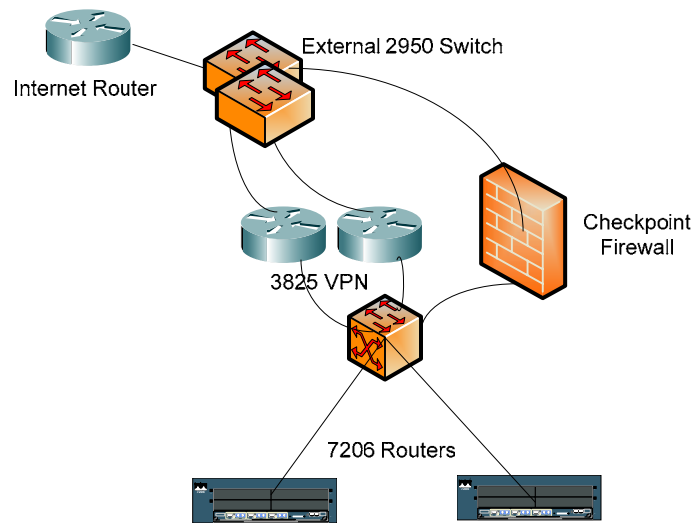
Kevin Brady

ICTN 4040

April, 2006

Realizing that the schematic you just saw looks like someone gave the crayons to a 5 yr old. Let's break it down into parts and see exactly what is being done to harden the network.

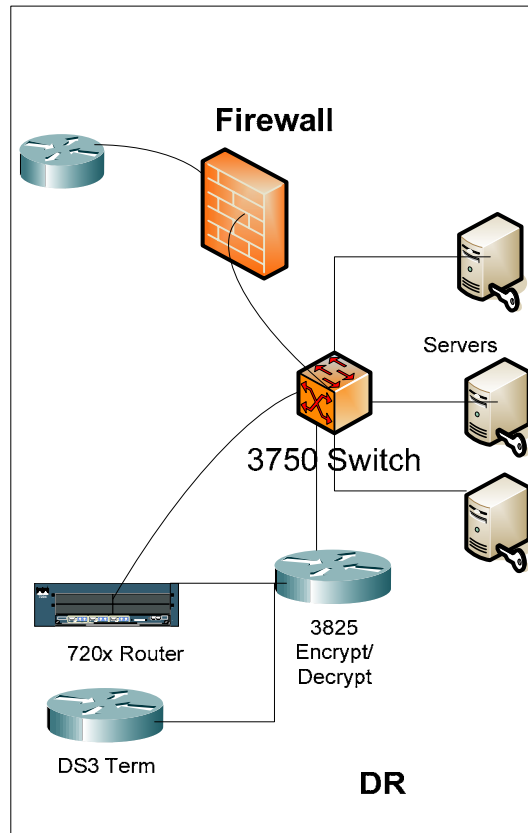
First we will look at the Core of the configuration:



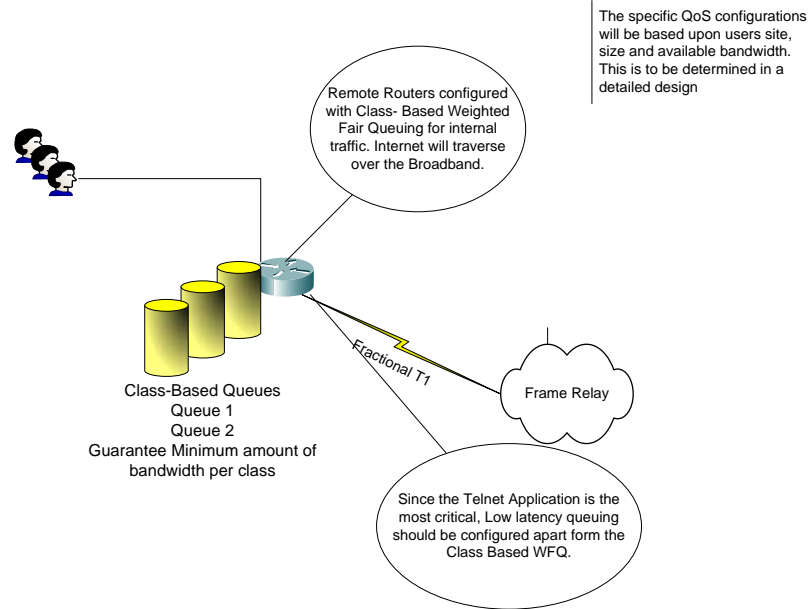
You should note that the actual data flow is from the Internet router through the External Switch to the firewall, once it is decrypted and screened it is then passed to the Core Switch, which allows it to gain access to the network by way of internal routers, you will also note that there is a second possible path. For the internal users that are using the network from external locations Virtual Private Networking (VPN) is used to authenticate their credentials before passing them to the Core Switch, and subsequently to the internal network. Each of the different stages provides an additional layer of security.

The security used in this stage is tunneling, which uses the IP Security Protocol (IPSec) to encrypt the entire packet from its source to the destination. It is then decrypted, inspected and either forwarded or discarded.

The next segment looks like this:

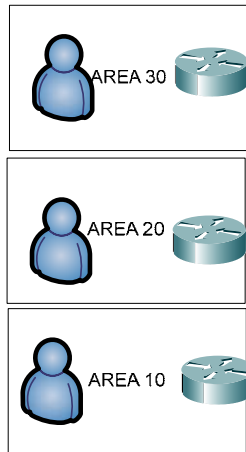


This portion of the diagram represents a Disaster Recovery site (DR), A critical element of any production network. In case of disaster all of the critical applications / data can be run from this location. It also uses the same method of authentication and decryption before allowing access to the servers. Due to the program / data backups required for a DR site to be effective, it must have the same amount of protection as the main network.



To further explain the bandwidth utilization process the diagram above shows that the data is processed on a percentage basis. Available bandwidth is allocated to a specific type of network traffic. A good example of this would be File Transfer Protocol (FTP), it would be allocated a minimal amount of bandwidth because speed is not as important. Other critical functions such as email, data processing, and applications would have a much higher portion allocated to them based on the business need. By limiting the bandwidth we are able to decide which tunnel the traffic passes through, thus allowing more control over the data and enhancing security.

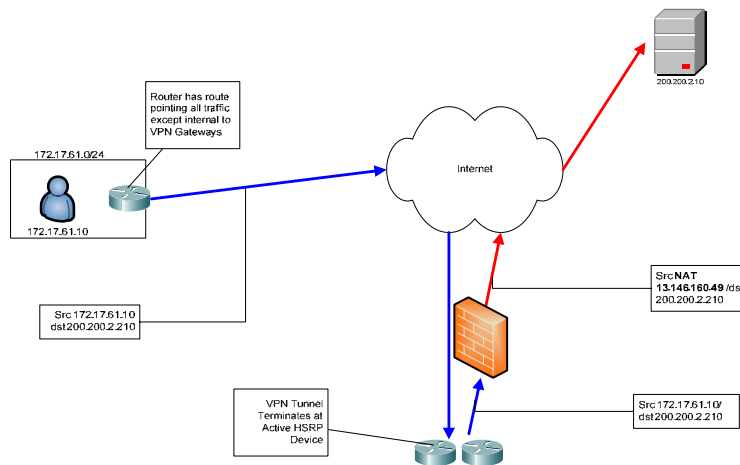
The final portion of the network diagram is the actual users.



The network is accessed through a series of two tunnels; the first takes the traffic that is business related and sends it directly to the network core using encryption to ensure the integrity of the data. The second tunnel is used for Internet traffic, it also provides a redundant link should the main tunnel fail. To minimize down-time of the network it is always a good practice to have redundant links. This allows for circuit / system failure without a devastating impact on the business.

As the world becomes more advanced in communication, the need for security increases exponentially. The use of the internet is becoming more of a necessity than a source of amusement, our children have no idea what the world was like years ago. As in all things the addition of technology has both good and bad in it.

The following diagram shows the actual path followed as the packets traverse the network toward their final destinations.



The data starts out with the user and all traffic that is not internal is pointed to a series of VPN Gateways. From the Internet the traffic travels through the tunnel and terminates at an active Host Standby Routing Protocol (HSRP) device. This provides backup to a router in the event of failure. Using HSRP, several routers are connected to the same segment of a network and present the appearance of a single Virtual Router. The process of transferring the routing process is transparent to the user. From there the data is passed to the firewall where it is inspected then encrypted before it is release to the internet. You will also note that the Internet Protocol (IP) address changes several times in the routing process. This enhances security by utilizing private addressing schemas to keep the traffic from reaching the Internet until it is ready.

In the previous pages and diagrams you have been given a general overview of a method used to increase security utilizing network hardware and routing protocols. With the rapid pace technology is changing we all need to be aware that the information we are passing is only as secure as the network it travels on.

References

Cisco Networking Academy Program. "Fundamentals of Network Security" Indianapolis, Indiana: Cisco Press 2004.

Whitman, Michael, and Mattord, Herbert. "Principles of Information Security" Canada: Thompson Course Technology 2005.

Ciampa, Mark. "Security Guide to Network Security Fundamentals" Canada: Thompson Course Technology 2005.