Communicating With Sam

Cost Effective Strategies for Network Security

Sam Johnston

Question:

Currently our company is based on a decentralized model for file and print serving with a centralized model for ERP on an iSeries at Head Office. Additionally, our network is a VPN network using Internet links and firewalls for VPN links to Head Office. Internet, which is an important service for about 50% of the user population, is served locally at each site. At the end of 2005 an audit suggested that we did not have the necessary levels of security for Internet access to meet guidelines and suggests a complex layered model for security for all Internet facing connections. Additionally, my CIO is interested in reducing the cost of support personnel at our remote offices supporting file and print serving and would like to migrate, as much as possible, applications to a centralized model. I am thinking that the best way to reduce cost on infrastructure is to centralize my services out of Head Office but I am concerned about the cost of my subsequent WAN and performance at the remote offices.

Answer:

Your company is coming to the realization that many companies are coming to today. In order to properly secure an Internet access site with local browsing there are a number of requirements for effective Internet security and they all come with a price tag.

Additionally, the complexity of supporting the infrastructure increases with the addition of dispersed systems. Since the costs for bandwidth on private networks is continually decreasing, an attractive option is to consider migrating off of VPN networks for reduced security risk and implement a carrier class network with SLAs, while providing Internet out of one or two offices for redundancy. This approach will reduce support expenses and security hardware deployment requirements.

An effective perimeter security model is to have 2 layers of firewalls to provide an internal and an external firewall with a DMZ in the middle. Often these firewalls will be provided by two different vendors for increased security. An additional security component recommended to enhance firewalls is Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) technology. This is typically deployed with an IDS or IPS appliance in the DMZ and the internal segment as a minimum. This will cover the network security component. Then there is a requirement for Web filtering, Email forwarding, anti-virus and anti-spam, mobile code detection, etc. and you have added some additional appliances or servers.

The end result is that in order to protect your enterprise network there is a significant investment required and a resulting complex infrastructure to manage. Therefore, the decision to move to a centralized Internet strategy makes sense much like having a Centralized iSeries for ERP makes a lot of sense.

So if the consideration is to move to a centralized model for Internet as well as file and print serving then there will be an additional load placed upon the WAN network and the network will need to be provisioned to assist in this. But there is another consideration. The end users at your organization have become accustomed to a certain response time and delivering this response time can add some additional cost to your future WAN.

However, there are technologies present that can assist you in reducing your operating cost on a WAN and providing the centralized type of model to support your business needs. There are 2 types of technologies from network vendors that could help in alleviating some of your challenges. These are presented under the category of Wide Area Application Services (WAAS). They are Application and Content Networking System (ACNS) and Wide Area File System (WAFS). At a high level, ACNS provides remote site caching and replication of pre-positioned content to remote appliances to reduce network bandwidth requirements and improve end user local performance. WAFS is designed to replace file and print services at the remote sites.

ACNS is a solution that combines the technologies of Web caching, Intelligent pre-positioning of static content and live and on demand streaming of applications, live events and video. How the solution works is that Content Engine Appliances (CEs) are distributed out to the remote sites to provide local support for these services thus providing improved performance to the end users and reduced bandwidth. For Web Caching the CEs are setup to cache Web requests in a traditional manner. This can be achieved using WCCP protocol to redirect Web requests to the CEs when there is local content for caching or bypassing the CE for new web content.

Pre-positioning of content can help the enterprise by enabling the Customer the ability to distribute static content to the remote sites. The solution will require a

Content Distribution Manager (CDM) as the brains to the solution which is typically located at Head Office next to the origin server (source of the content to be distributed). The CDM leverages a root Content Engine to extract source data and replicate to the remote Content Engines.

Typical applications replicated include software patches, Intranet shared files, file shares, stored video to name a few. The ACNS system can setup an intelligent replication of data from an origin server at Head Office and schedule replication of data to the remote sites taking into account bandwidth and schedules for access to network resources to optimize the use of the network and reduce the data transit required across the network. The result in less bandwidth required and improved performance to the end user.

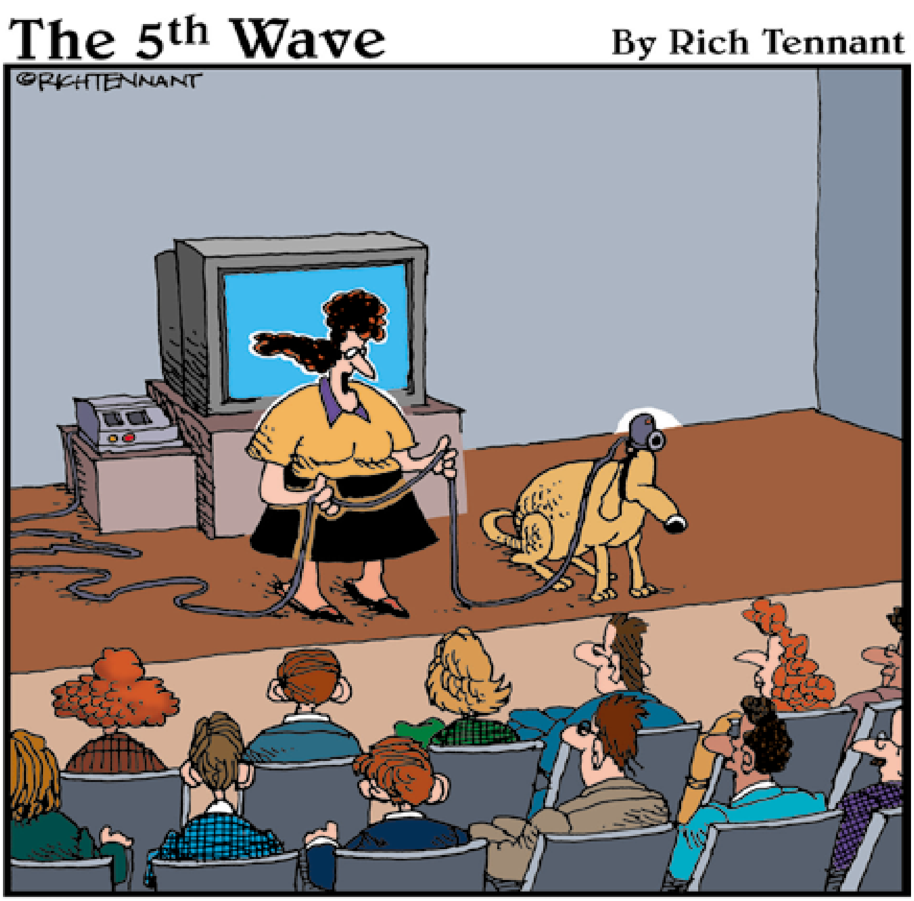
This solution can also support live streaming of Video assuming you also have an IP/TV solution. More commonly stored Video on Demand or corporate presentations can easily be added as static content for distribution. Since the playback is usually bandwidth intensive over the WAN, the ACNS solution provides for an enhanced level of learning opportunity to the remote sites through local playback.

As mentioned above, WAFS technology can also play a role in assisting in centralizing file and print services within your enterprise. The WAFS solution can replace file and print serving at the remote branch and enable the benefits of centralized management. One vendor defines the WAFS operation as using protocol specific optimizations such as latency mitigation, object caching, metadata caching, and WAN transport optimizations to ensure efficient operation of the standard file system protocols of Common Internet File System (CIFS) with Windows, and Network File System (NFS) with UNIX. This solution maintains file coherency, locking, security, and access policies.

In one vendor's implementation, the components that make up a WAFS solution are the WAFS Edge File Engine which is used at the remote branch to replace file and print servers. The WAFS Core File Engine is used in the data centre and is responsible for providing aggregation services for the remote Edge File Engines and termination of WAN optimized file requests. The WAFS Central Manager provides centralized, Web-based management and monitoring of all WAFS nodes.

These two solutions do require some management and deployment of hardware to the remote site. However, the solutions are appliance based and the majority of the administration can be done centrally out of the data centre. These solutions are designed to be managed by the centralized IT staff.

As with any design decision, each organization must weigh the costs of supporting and maintaining technology and look for efficient ways to manage and deliver resources to the end users. In many cases, simplifying a network by consolidating resources into locations where they can be readily managed will reduce the overall complexity of the operation and often result in reduced total cost to the business.



"I had a little trouble with the automatic video tracking camera, so during the video conference, before speaking, call Rollo here, and wait until his paws are on your knees and the camera is facing you before speaking."

Sam Johnston *is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to the iSeries community. He can be reached at (416) 438-0002 or via e-mail at sjohnston@intesys-ncl.com. Any TUG member wishing to submit a question to Sam can forward their typewritten material to the TUG office, or to Intesys. The deadline for our next issue is Friday April 14, 2006.*