

Network Security Optimization On a Business Driven Basis



Network Strategy Partners, LLC

MANAGEMENT CONSULTANTS TO THE NETWORKING INDUSTRY

www.nspllc.com

March, 2006

Network Strategy Partners, LLC (NSP) — management consultants to the networking industry — helps service providers, enterprises, and equipment vendors around the globe make strategic decisions, mitigate risk and affect change through custom consulting engagements. NSP's consulting includes business case and ROI analysis, go-to-market strategies, development of new service offers, pricing and bundling as well as infrastructure consulting. NSP's consultants are respected thought-leaders in the networking industry and influence its direction through confidential engagements for industry leaders and through public appearances, whitepapers, and trade magazine articles. Contact NSP at www.nspllc.com.

Contents

EXECUTIVE SUMMARY	1
REQUIREMENTS DEFINITION	2
ARCHITECTURE OPTIMIZATION	4
MIGRATION PLANNING.....	6
CONCLUSION	7

Executive Summary

Network security threats have emerged as a top concern for enterprise executives as networks have become an essential element of enterprise infrastructure. Enterprise intranets support the lifeblood of mission critical information systems, the Internet is increasingly used for

electronic commerce between corporate suppliers and customers, and most employees use Email and the World Wide Web as frequently as they use the telephone. The level and severity of network security threats, unfortunately, has grown also at an exponential rate and this trend does not appear to be slowing.

Network Threats

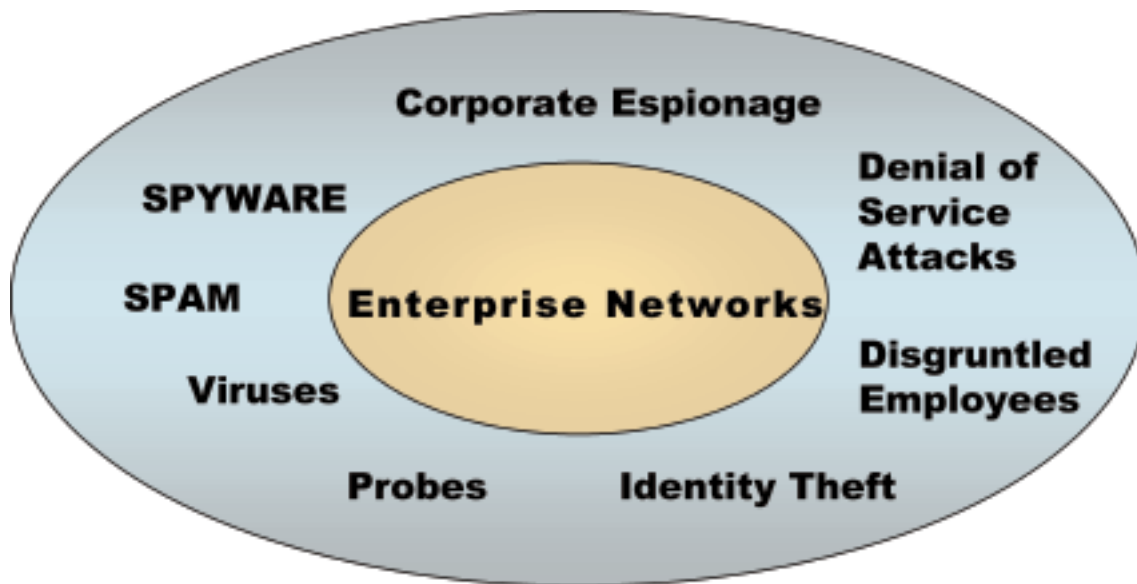


FIGURE 1

As security has emerged as a top concern for companies, so too has an entire industry focused on solving these problems. Multiple hardware and software components are used in the network to ensure security:

- Firewalls
- Intrusion Detection and Prevention Systems
- Identity Access Gateways
- Security Management Systems
- Self-Protecting Routers and Switches
- DMZ architectures

While it is clear that there is an urgent need for companies to make investments in security, it is also clear that this can be a bottomless pit. Network security risks are growing exponentially — no amount of money will fully eliminate these risks. For this reason, it is essential that

enterprises optimize network security. The optimization concept explicitly recognizes that security risks can never be fully eliminated because that would require infinite resources. Optimization, instead, restates the problem as one of spending the right amount of money on minimizing network security risks.

Optimization involves Operations Research techniques that have been used for years in designing networks, transportation systems, and manufacturing systems also can be applied to optimizing network security. The objective of this problem is to minimize the Total Cost of Ownership (TCO) of network security while satisfying corporate security requirements. Total Cost of Ownership is the sum of capital and operating expenses (CAPEX and OPEX) over the life of the network security assets.

While this is an easy problem to state, it is an extremely complex problem to solve. Clearly a formal process is required to identify and categorize the importance levels of information and systems in the network that need to be protected, develop an optimal architecture, and plan for a

successful migration. This process is depicted at a high level in the diagram below.

The body of this paper will define this process and the challenges of optimizing network security in enterprise networks.

Process

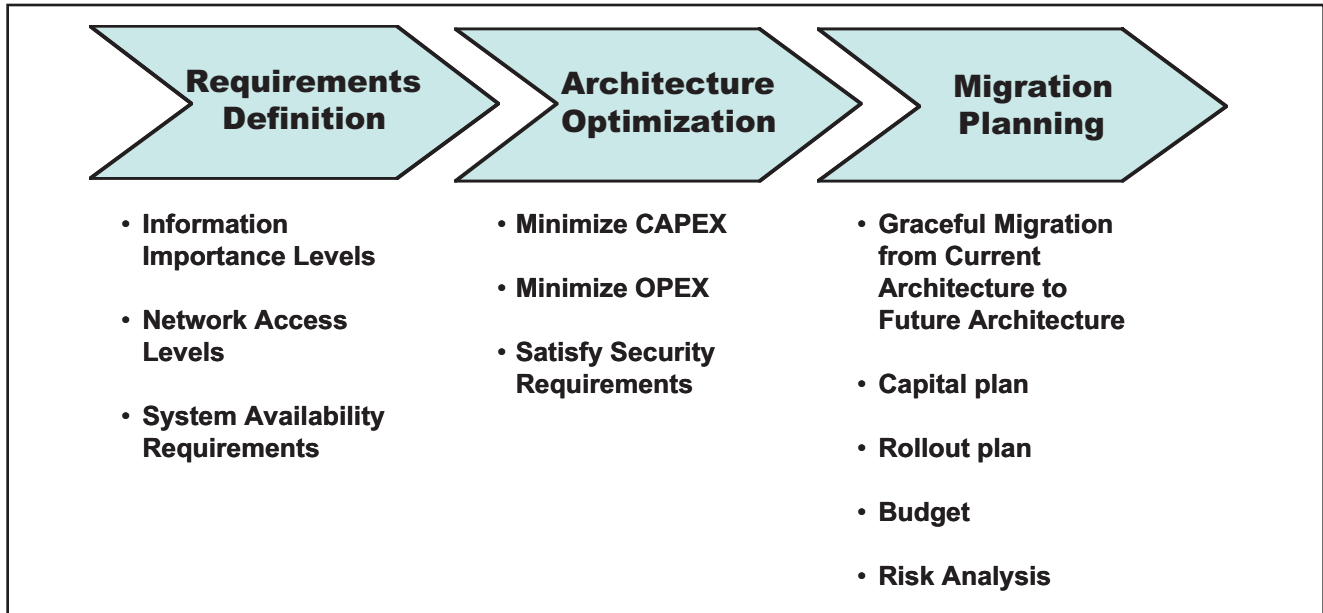


FIGURE 2

Requirements Definition

The first and most critical step in the process for optimizing network security is clearly defining the requirements for security. While this can be a complex task, it can be simplified by breaking down security requirements into several categories:

- Information Importance Levels
- Network Access Levels
- Network and System Availability Requirements

Information Importance Levels categorize the level of security that is necessary for various types of information (Databases, etc.) in the network. Four levels of importance are defined:

Information Importance

Information Importance Level	Definition
Critical	This information must be kept secure regardless of cost
High	Security is extremely important, however, cost is a consideration
Medium	Security is important, however, cost is a major driver
Low	Cost is the major driver and security is a secondary consideration

Network Access Levels define how information is shared on both the internal corporate network and the Internet.

These levels are defined as follows:

Network Access

Network Access Levels	Definition
Internet	This information is shared across the Internet. Anyone with Internet access can share this information
VPN	This is information that is used by employees or trusted vendors. Access to this information can be either over the corporate Intranet or over a trusted VPN on the Internet
Intranet	This information is used only by employees and is accessed over the corporate Intranet
Workgroup	This information is accessed by a small geographically confined group and is accessed over a corporate LAN segment or VLAN

A major driver in defining and optimizing a network security architecture is to determine what information is critical and how widely it needs to be accessed. A simple way of doing this is to hold a workshop with key management in both IT groups and business units in the

company. One of the outputs of such a workshop is a matrix categorizing information by both Information Importance Levels and Network Access Levels. An example of such a matrix is provided below:

Information Importance vs. Network Access

Network Access Levels	Network Importance Levels			
	Critical	High	Medium	Low
Internet			Marketing Documents	
VPN	Medical Records SSN's Credit card	Proprietary Documents Email		
Intranet	Medical Records			
Working Group				

In the workshop corporate information is defined and categorized at a high level. Information in databases and file systems such as:

- Medical Records
- Social Security Numbers,
- Credit Card Information
- Email
- Proprietary Documents
- Marketing Documents
- Etc.

After this information is defined, the group then decides how to place this information in the matrix. When completed, the matrix provides a roadmap of how a network security architecture should be designed and optimized to minimize cost, while satisfying key security requirements.

Network and system availability levels are also important to the security requirements definition because they can be compromised by denial of service attacks, viruses, and worms. These levels are defined in the table below:

Availability Levels

Network and System Availability Levels	Definition
High	It is critical that these components of the network are available 24 X 7
Medium	Availability is important, however, 24X7 operation is not required
Low	Availability is not important

These requirements also are crafted in a workshop with IT and business group management teams.

The following sections of this paper define how networks are optimized for security such that CAPEX and OPEX are minimized while satisfying network security requirements.

Architecture Optimization

Once network security requirements and priorities are identified and prioritized within the business context the network architecture can be redesigned to optimize network security. Figure 3 outlines the process.

The process of optimizing the network architecture to minimize Total Cost of Ownership while satisfying the network security requirements consists of five steps. First the current network infrastructure is assessed. The assessment examines the network's functional, economic and physical capabilities. The functional capabilities include the security and availability requirements discussed in the preceding section. The economic assessment determines whether there are alternative network technologies or services that can meet existing requirements at lower cost while the physical assessment

simply determines whether the current equipment continues to meet its original performance specifications—is the facility in working order? This assessment creates a baseline used to determine if new infrastructure investments are required.

The second step in network security optimization is to translate the functional and business requirements for network security into technical terms. This includes projecting bandwidth and traffic requirements so that network elements of appropriate capacity are used and characterizing network traffic to assure that performance standards are met during peak usage periods. (This process is essential to achieving a financially efficient design as many network managers tend to “throw bandwidth” at the problem to assure that they are never caught short of network capacity.) Most importantly, this step involves translating business requirements such as network security is “critical” or “medium” into technical specifications such as the type of encryption to be used, Access Control Lists, protocols, and specification of VLANs.

The third step is to prepare a gap analysis. The gap analysis compares the technical requirements that were

identified in Step 2 with capabilities assessed in Step 1 and identifies any gaps between the required and existing network capabilities. This step also determines the hard and soft dollar impacts of the identified gaps so as to assure that a financial rationale exists for new investment. This analysis must necessarily involve assessments of such soft dollar items as legal and regulatory requirements, image, reputation and trust.

The fourth step is to develop a recommended network design. The design process begins with developing at least three feasible alternatives for closing the gaps identified in

Step 3. Evaluation metrics and criteria are defined as a vehicle for choosing among the feasible alternatives. The criteria are determined using the business requirements (discussed in preceding section) as guidelines. The criteria then are used to create a design evaluation matrix that is used to provide an objective side-by-side comparison of each design alternative. The filled-in matrix makes selection of an optimal solution straightforward and easy to support as it breaks down sometimes-controversial decisions into simpler components so that areas of differing opinion are isolated and can be discussed (usually) on a more business-like and less emotional basis.

Architectural Optimizations Process

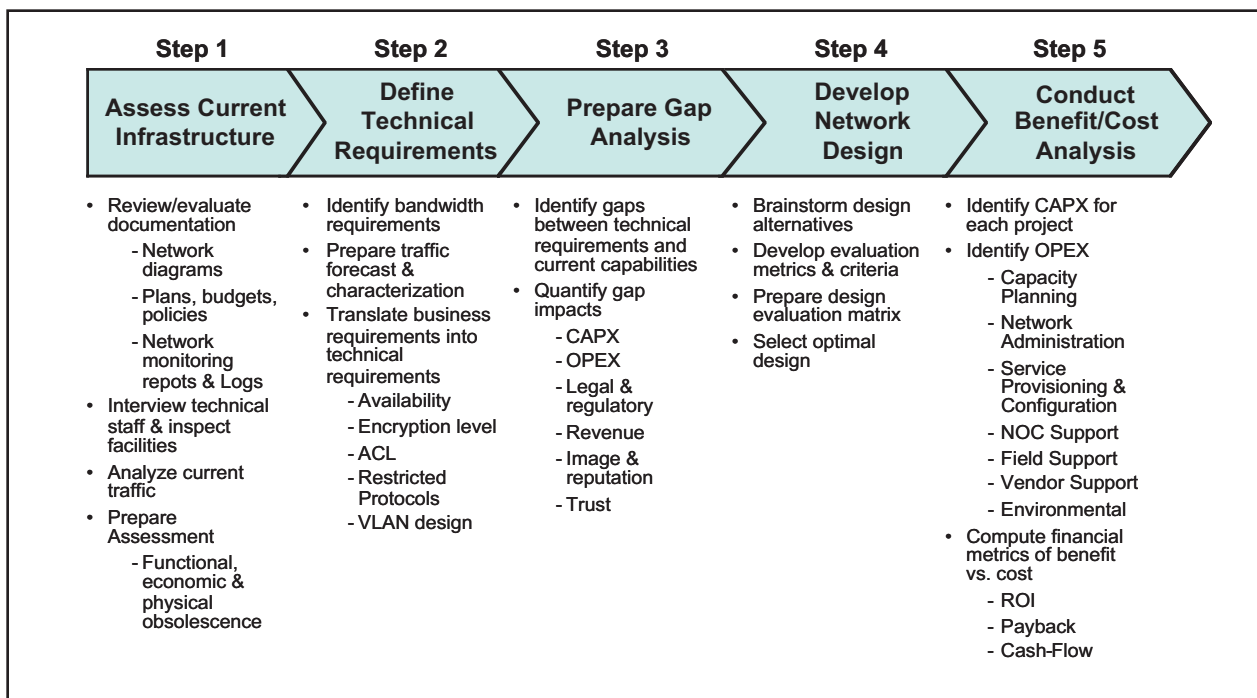


FIGURE 3

The final step is to conduct a benefit/cost analysis of the recommended design(s). The capital expense (CAPEX) of each project is identified along with its operating expense (OPEX). Whereas CAPX is easily quantified because purchase orders must be written to acquire new equipment, OPEX is both harder to quantify and more important to Total Cost of Ownership. OPEX includes network operations expenses such as capacity planning, network administration, service provisioning and configuration, NOC support, and field support; vendor support expense—often a percentage of the equipment purchase price; and environmental expense including

floor-space, cooling, power, battery and re-generation cost.

Decisions to proceed with implementation should be guided by financial metrics such as ROI and payback that balance the project benefits identified by the Gap Analysis (Step 3) versus the Total Cost of Ownership over the project life discussed above. This puts the decision to improve network security on a sound business driven basis independent of the self-serving fear mongering that has become unfortunately so common in our industry today.

Migration Planning

To minimize Total Cost of Ownership while satisfying the security requirements requires that the technical architecture be separated from vendor selection. This is true because the network security market is rapidly evolving, there are many new entrants, and no incumbent vendor has a complete solution. One consequence of the chaotic state of the market is that many new security functions appear first as security appliances—servers with tightly integrated proprietary software—rather than as security enhancements to well established products such as routers, switches or firewalls. The large number of vendor solutions, consequently, requires that the security

architecture decisions be made prior to a second round vendor selection process. Vendor viability and product support capabilities are key to this second round decision. Startup vendors must make product feature decisions more than a year in advance so there is a constant risk that they will guess wrong and go out of business. On the other hand, large established vendors tend to lag well behind in their security offerings and while their corporate viability is not at risk there is a very real risk that they will drop products or even product lines in order to remain competitive.

Figure 4 illustrates an implementation process designed to mitigate these risks.

Implementation Process

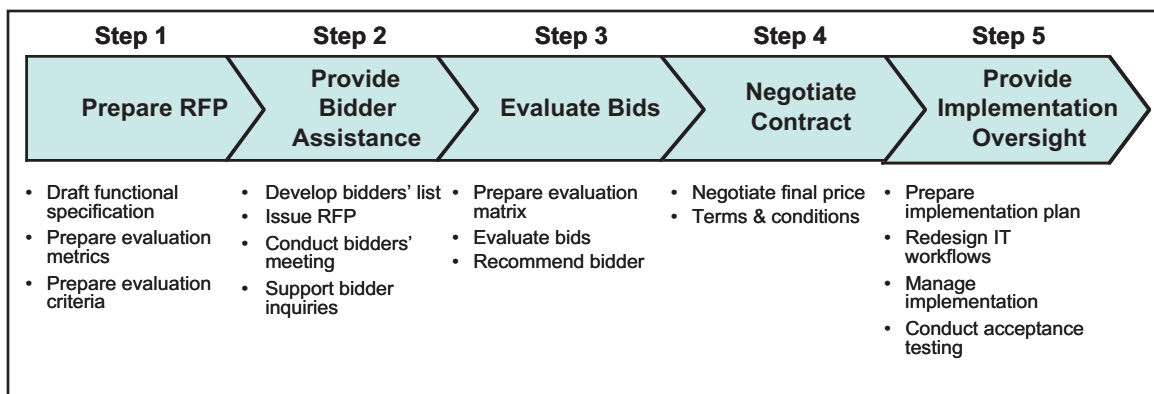


FIGURE 4

The implementation process consists of five steps. The first step involves developing a functional specification that is derived from the Network Architecture selection process described in the last section. The results of this work also guide development of evaluation criteria; however, these criteria differ from those used for architecture selection by emphasizing price, vendor viability and support.

The second step is designed to support the prospective bidders to assure that their best thinking and creativity is directed toward designing a solution meeting your specific needs. Bid evaluation uses the device of a vendor evaluation matrix to assure an objective evaluation. Commercial considerations are addressed in Step 4 while

Step 5 is designed to assure full compliance with the contract.

Implementation of a secure network, however, involves much more than a good technical design and selection of a reliable vendor. Network security also depends upon establishing and communicating good security policies and redesigning the work of the networking function to best utilize the new architecture. This often involves restructuring the network organization's work processes and re-training staff to create a service-oriented operation. An enterprise-wide training program may also be required to re-educate users on company security policies and procedures.

Conclusion

Network Security today is a hot button in corporate America. Networks are essential elements in business operations and the Internet is an integral component of electronic commerce. Hackers, thieves, viruses, worms, and other threats have generated fear in executive offices across the world and vendors have capitalized on this fear by developing an entire industry around network security.

Network Strategy Partners, LLC believes that the fear is well founded, however, we do not believe that the problem can be solved by blindly throwing money and human resources at the problem. A structured approach to optimizing network security is required to ensure that security requirements are adequately addressed while capital and operating expenses are minimized.