

SECURITY DESIGN

Are You Ready?

That's the question posed by a popular technology manufacturer in its television ad campaign. Of course, most organizations reluctantly answer in the negative. The pace of change—both in networks and in computers—is accelerating beyond the wildest predictions. A few years the idea of security when connecting to the Internet was not a major concern to most organizations. More recently, installation of a firewall between the enterprise and the “cyberspace” was sufficient. Now, the boundary between the enterprise network and the Internet melts into a global, mobile, and virtual workplace. Do you know how to secure it? Questions such as - What are the roles of internal firewalls, PKI's, VPN's, and hardened operating systems? Where is the security perimeter and do the security procedures support the whole enterprise? Can the policy address all these technologies and make them work in concert? – plague the IT departments of many organizations.

Many people panic when faced with such a dramatic paradigm shift. Often, they are paralyzed with fear. Having just approved and committed the funds and resources to build a new, redundant firewall complex or implement an enterprise PKI, may create an environment where that outlay seems useless.

Rather than hindering business, security should enable it. The question is, how?.

Looking Back to Look Forward

The most effective way to face the future is to learn from the past. Often, organizations turn to technicians to design their infrastructure. These well-intentioned staffers do not have the background or experience to innovate. They can only develop solutions based upon the products and approaches in which they are trained.

Security, in particular, is a discipline learned the hard way. Only by understanding the original intent of a firewall, VPN, PKI, or other security technology enable the technologies to know the appropriate uses of that tool. Determining the right use of technology requires going back to first principles and working forward to prove the environment is secure.

Experience When You Need It

Network & Security Technologies has the security experience most organizations need. Our field-proven consultants possess years of experience. They can develop new solutions because they understand why the old ones work. They work from principles, not manuals.

Most importantly, Network & Security Technologies' security and networking expert consultants know the details, too.

Network & Security Technologies brings together network and security consultants from many different environments and disciplines. Rather than serving as a “body shop” for one or another vendor, we have staff trained across multiple vendors. Our people are as comfortable with configuring a Cisco PIX™ as they are with a Checkpoint Firewall-1™ or other industry standard security products. This in-depth expertise means that any new design will work. Moreover, familiarity with such a broad range of products results in a solution that will not be cost prohibitive.

The Design Process

Network & Security Technologies uses a standard process for all its Security Design engagements. This comprehensive approach can be applied to perimeter security, host based security, application security, phone switch based security or routers, and will meet our clients' requirements. The steps include:

- **Gather Data:** Network & Security Technologies will study the new and existing business drivers for the design.
- **Specify Requirements:** Network & Security Technologies will extract and document the technology requirements from the business drivers.
- **Develop Strategy:** Drawing upon its experience, Network & Security Technologies will identify the best strategy for meeting the business requirements.
- **Produce Design:** Network & Security Technologies will produce network maps, equipment lists, and device configurations. These deliverables, set within the context of a rational, actionable deployment may include estimates of resources and capital costs.

Throughout the engagement, Network & Security Technologies experts will collaborate with our clients' staff. This ensures that the final result addresses all concerns and constraints such as: existing infrastructure, budget, and culture. The Security Design document describes each component of the solution in specific detail to enable its immediate implementation. Network & Security Technologies' field proven consultants will present the design to executive management and staff to develop a consensus understanding of its objectives and logic. These same Network & Security Technologies experts will support you through the process of implementation and integration, or lead a Network & Security Technologies team to that end if required.

Our clients take advantage of the experience and know-how of Network & Security Technologies. They face the uncertain future with confidence and enable their organization to make use of the Internet, collaborate on-line with customers, and take their work to wherever in the world they need to go. Network and Security Technologies' clients do all of this with the safety and privacy that their business requires.

SECURITY SERVICES + SECURITY MECHANISMS = SECURITY CONTROLS