

## CTA INFORMATION SECURITY CASE STUDY:

### ENTERPRISE FIREWALL CONFIGURATION ASSESSMENT SERVICES

#### CLIENT DESCRIPTION:

The client is a major government agency with management responsibility over securing a national information network system. As with several other clients, the perimeter defenses implemented by this large organization evolved over time without the benefit of a comprehensive, consistent body of rules and practices used to protect information assets from threats via local area and wide area backbone networks.

#### CTA PROJECT DESCRIPTION:

Perform an end-to-end perimeter defense audit and develop and implement a complete firewall security policy, starting with a top-level enterprise policy, to network specific policies to be implemented on the agency's firewalls, and finally refine the firewalls' specific rule base.

#### PROJECT REQUIREMENTS:

The focus of the program is to provide consistent network perimeter protection, to ensure the authorized availability, integrity, and confidentiality of network services and automated information system (AIS) resources.

#### SYSTEM ARCHITECTURE:

The client's architecture is a large, complex, heterogeneous network consisting of thousands of workstations and hundreds of midrange servers and mainframe systems.

#### WORK ACCOMPLISHED:

CTA performed technical work in a number of areas as discussed below:

##### **Enterprise Security Policy Analysis**

We analyzed the enterprise security policy to determine the accesses, services, and activities that management wanted to allow and restrict to its users. The process included determining whether a firewall or another object should enforce the policy statement. We developed **the Information Systems Firewall Security Policy** statements which identified standard service and session configurations as well as any customized services. Customized services could include permitting certain services from a particular external network object such as a host. This list is the guide for analyzing Check Point security policy rule base and policy properties. Part of the analysis required identifying documentation and the rules that supports a user's request for customizations as well as other user unique accesses and restrictions.

##### **Network Object Identification**

In order to assess the firewall policies we identified network objects and their connectivity. This step was performed concurrently with the Enterprise Security Policy Analysis. During this step we collected the list of objects that the agency has implemented on its firewalls. We also determined the internal standards that the agency had used to define these objects in its firewalls. Standards include color schemes, groupings, etc. Object identification includes identifying firewalls, routers, major applications, general support systems, and other system components. We attempted to determine the network protection strategy and design and where the firewalls fit within this strategy.

## Firewall Security Policy and Property Analysis

Each firewall was analyzed to validate that it properly implemented the agency's policies and was properly configured. We used the policy statements from the **Information Systems Firewall Security Policy** document and the Agency Baseline Security Requirements to help analyze firewall policies implemented on each firewall.

### **BENEFITS TO CLIENT:**

The benefits to the customer are numerous. First, having a solid policy upon which to guide their agency-wide security program provided a basis for all program decisions balancing system usability against required security, and generally increased the cost effectiveness of their security program. Second, having a well-defined structure for implementing the security program, and trained personnel who know where to go for what types of information and decisions, did much to focus and increase the overall security posture of the organization.