Title:	**Firewall Architectures for High-Speed Networks**
PI:	Errin W. Fulp
PI Institution:	Wake Forest University, Computer Science Department

Project Website: http://nsg.cs.wfu.edu

Abstract:

The **objective of this DOE project is to develop new firewall optimization techniques and architectures** that are suitable for the next generation of high-speed and Quality of Service (QoS)-enabled networks. Firewalls remain a key component for securing networks that are vital to government agencies and private industry. They enforce a security policy by inspecting and filtering traffic arriving or departing from a secure network. While performing these critical security operations, firewalls must act transparently to legitimate users, with little or no effect on the perceived network performance (QoS). Unfortunately, firewalls can easily become a bottleneck, given increasing traffic loads and network speeds. Packets must be inspected and compared against increasingly complex rule sets and tables, which is also a time-consuming process. As a result, current firewall systems can introduce significant delays and are unable to maintain QoS guarantees. Firewalls are also susceptible to Denial of Service (DoS) attacks that merely overload/saturate the firewall with illegitimate traffic. Unfortunately current firewall technology only offers a short-term solution that is not scalable.

The first objective of this project, firewall optimization, focused on decreasing the number of comparisons required per packet. This was accomplished by reorganizing policy rules via special sorting techniques that maintain the original policy integrity. This research is important since it applies to current and future firewall systems. Another method for increasing firewall performance is with new firewall designs. The architectures under investigation consist of multiple firewalls that collectively enforce a security policy. These distributed systems quickly divide traffic across different levels based on perceived threat, allowing traffic to be processed in parallel (beyond current load balancing technology). Traffic deemed safe is transmitted to the secure network, while remaining traffic is forwarded to lower levels for further examination. The result of this divide-and-conquer strategy is lower delays for legitimate traffic, higher throughput, and traffic differentiation (a key component for maintaining QoS). Furthermore, the distributed design is scalable to traffic loads and is less susceptible to DoS attacks. Important design issues include determining the firewall-node configuration (number of levels and number of nodes per level) as well as rule distribution. Simulation and analytical results show these new architectures can out-perform current firewall systems, providing higher throughput, lower delays, and predictable traffic differentiation.

Major Research Activities:

Significant progress has been made in the important areas of security policy optimization, parallel firewall system design, and policy distribution methods. The findings of this research

will benefit current and future firewall systems. Furthermore given these advancements, the project is on schedule to proceed with the third year.

- **Security Policy Optimization** - The order of firewall rules significantly impacts the security (integrity) and performance (processing time) of a security policy. Using the policy models developed in the first year, we have continued to develop algorithms that can optimize list and tree structured security policies. These heuristics can reduce the number of comparisons required with results of up to 80%.

- **Distributed Firewall Designs** - This year focused on the function-parallel firewall architecture that distributes rules over an array of firewalls. Simulation results and analytical models indicate this model can achieve a significant reduction in processing delay that is possible as compared to current data-parallel designs. This design will serve as the basis for the hierarchical firewall architecture that will be investigated this year.

- **Security Policy Distribution** - Given an array of firewall-nodes, rules must be distributed such that the integrity of the original policy is maintained. Using the policy Directed Acyclical Graph (DAG) model developed in the first year, we have established certain criteria that must be followed to maintain integrity in parallel-firewall architectures. The third year will combine these results with the policy profile to determine the optimal rule placement.

- **Implementation** - We are currently implementing the function-parallel firewall architecture using Linux PC's which can provide a low-cost, scalable, high-speed firewall system. This work has also resulted in two provisional patents for high-speed security devices. In addition a collaborative effort has been started between this project and DOE Pacific Northwest National Laboratories (PNNL) that will integrate high-speed security techniques into their infrastructure.

Synergistic Activities and Project Impact

As previously mentioned, the project has also started network security collaboration with Deborah Frincke and John McCoy from the DOE Pacific Northwest National Laboratories (PNNL). During this summer the PI worked at PNNL to further develop the optimization techniques and parallel designs with respect to the security infrastructure (PNNL currently utilizes a data-parallel design). This was a unique opportunity to apply our current parallel firewall research to an actual high-speed network environment.

Furthermore, a small start-up company has been formed based on this research. The company developed a business plan and seeks to market commercial versions of the optimization methods and distributed firewall architectures that are the subject of two patents pending (60/638,438 Function-Parallel Firewall and 60/665,664 Methods and Systems for Firewall Policy Optimization). During the summer of 2005 due diligence was conducted that indicates there are several opportunities in the high-speed network security device market. In this initial phase of operations, independent testing will be performed, by a noted third-party, on the firewall systems to validate the results of our internal tests.