

PROJECT PROFILE

Advanced Security Proxies

Objective

The goal of the Advanced Security Proxies (ASP) effort is to develop an approach for using firewall security proxies in conjunction with high-speed networks. The fundamental limitation of proxies has been their impact on overall network performance. By integrating technical innovations, centered on the use of highly-tuned networking protocol stacks, into a proxy firewall architecture, this research project will demonstrate the high-security benefits of proxy technology without impacting network performance. Moreover, the implementation will demonstrate the flexible use of the approach to provide for policy controlled tradeoffs between performance, security, and functionality.

Approach

Develop and prototype new high-speed firewall techniques that allow security proxies to selectively review protocol traffic. This capability is essential to avoid the proxy bottleneck that limits the applicability of firewall technology to high-speed networks. At the same time, the implementation will address the limitations of current firewalls (based on commodity operating systems running on general purpose hardware) that impact network performance. These limitations include the impact of excessive copying of network traffic between device, kernel and user protection domains, and the lack of any specialized support for proxy control operations applied to the network traffic flows. The proxying techniques employ a common subsystem that provides two key facilities: efficient protocol implementations, and selective control of reassembly of higher-level protocol messages from lower-level protocol packets. Proxy software uses this control to reassemble only when needed for security functions, otherwise allowing traffic to flow on a fast path from network interface to network interface.

In addition, an important part of the research effort is investigation of adaptive proxy behavior, where control of an application data stream can be changed from one technique to another in response to content or system load. As a result, each application data stream can be handled with security techniques that are appropriate to the risk of that stream, allowing system resources to be expended only in pursuit of site specific security goals. The reduction of unnecessary use of system resources (as compared with current proxy firewalls) allows correspondingly greater utilization of system resources to meet performance requirements so as to minimally impact network users. The basis for the mainline prototype of the proxy network subsystem is the Scout OS, developed by DARPA researchers at the University of Arizona. Scout provides a framework for optimized network protocol stacks, as well as providing a proxy execution environment with much lower overhead than conventional operating systems. Recent work in Scout also provides a basis for dynamic proxy behavior to reduce system resource usage: TCP connection splicing. Prototyping work with Scout is currently focused on proxy software execution, usage of TCP splicing and unsplicing, and performance measurements of the impact of each of these steps. This also includes implementing custom Scout device driver support for a high-speed OC-12 ATM interface, as well as integrating specialized OC-12 firewall hardware into the architecture. These components facilitate performance measurements on actual high-speed network infrastructure. In addition, they allow the system to avoid performance degradation that would otherwise occur at the lowest layer of the network.

Research Focus

High Performance Network Solutions

The demand for firewalls which can protect high-speed networks without reducing overall network throughput is continuing to increase over time. As the performance of network switches and media increases, fundamental advances are needed in the architecture of security devices placed at network boundary points, that allow proxy firewalls to enforce strong security policies while leveraging the capabilities of the latest generation of networking hardware. The ASP project is exploring one architectural approach to realizing this capability, utilizing customizable operating systems, high-performance hardware, and a quantitative approach to evaluating the engineering tradeoffs that lead to high performance solutions.

- Roger Knobbe
Principal Investigator,
Security Infrastructure Group

Recent Accomplishments

Implemented a prototype of the Advanced Security Proxies firewall architecture, demonstrating the performance and functionality of application proxies utilizing network stack control operations including connection splicing, and in-parallel traffic inspection and delivery. The prototype operates on 100 Mb/s FastEthernet, and is complemented by a set of firewall workload generation and data collection tools that is used for performing rigorous, repeatable loading and performance measurement experiments on the prototype firewall.

Implemented a new, restructured Scout TCP protocol stack. Based upon actual operational limitations encountered during firewall performance testing and loading, the new protocol stack uses a more robust internal architecture, geared toward providing consistent behavior under heavy network load. In addition, the new TCP stack includes support for RFC 2140 common control blocks that provide additional opportunities for proxy and system-wide optimization and control of network traffic.

Reached a major milestone in the effort to provide a customized Scout device driver for high-speed OC-12 ATM network interfaces by successfully building the core device driver sources within the Scout OS build environment. While additional work is required before the system will operate over the ATM network, the completion of the compile-time portion of the porting effort allows the project to move forward to the more significant runtime and performance tuning activities. Over 50% of the execution time in the highly-tuned prototype ASP firewall is spent in the Scout device drivers. Reaching our performance objectives requires careful implementation and integration with this layer of the system.

Additional Information

Contact Roger Knobbe (rknobbe@nai.com) at 310-737-1661 or visit our Web page at: <http://www.pgp.com/research/nailabs/distributed/advanced-security.asp>.

1/5/01



Who's watching your network

For more information on NAI Labs, contact your authorized NAI Sales Representative, or visit <http://www.nailabs.com>.

CORPORATE Headquarters

3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (800) 764-3337*
Fax (888) 203-9258

**Call for additional Worldwide Sales Offices*