



## Theories of Bulkhead Network Security

a white paper

copyright 2004 Simplir Inc.

# Bulkhead Network Security

The purpose of this paper is to describe a comprehensive implementation for securing wireless networks and evaluating the possible attack considerations under this security plan. Although the focus of this paper is wireless networks, the network structure provides a strong case for wired networks as well, given they face the same basic issues.

## Introduction

The goal of any network deployment is the fulfillment of services to end users. The network is a means to an end, and that end is user satisfaction. Therefore, the essence of the network is to provide reliable, consistent network service. Apart from mechanical failure, network security remains the most crucial element in networks meeting the expectations of network managers.

Networks are not secured by a single device. There is no magic bullet “firewall” that can protect the network. Networks are secured through the consistent application of principles. To build secure networks we introduce the phrase “Bulkhead Network Security”. The concept of a bulkhead was introduced in shipbuilding where shipmakers wished to compartmentalize the ship for the purpose of adding structure and to prevent the spread of disasters such as leakage and fire. Similarly, good network design recognizes that risks exist and that to minimize their impact on our network we wish to protect our network as we give it structure.

Bulkhead Network Security provides protection by securing the network against attack and the impact of attacks by integrating mechanisms of defense at every structural point in the network. Let us consider the types of security issues networks face and how Bulkhead Network Security solves them.

## Authentication and Theft of Service

The first layer of defense in wireless networking is authentication of the user. Before network traffic is carried across the network, it must be verified against a user or customer access list. In a wired network the physical barriers to the network devices and wires typically act as the sole authentication. In wireless topology additional considerations must be made.

The authentication mechanism embedded within most wireless access points is based upon MAC address. All network hardware interfaces (network cards, radios, etc.) are given a unique alphanumeric identification at the manufacturer. These unique keys are used in the routing of TCP/IP network traffic. This convenient identifier has been widely used for authentication in wireless access points as network packets are received; however, the MAC address can be forged by operating system software prior to submission to the wireless access point.. MAC based authentication can be circumvented

to gain network access.

The 802.11 standard includes a technology called Wired Equivalent Privacy (WEP). This feature includes a secret key shared between the wireless end user and wireless access point that is used to encrypt packets before they are transmitted. WEP has been implemented as an authentication mechanism solely and in combination with MAC based authentication schemes in many devices. It is widely accepted that the WEP protocol fails to provide the security it purports. There are software programs available for breaking the encryption algorithm and obtaining the secret key.

Virtual Private Networking (VPN) succeeds in providing a secure, encrypted means of authenticating users. It is recognized within the industry as the best means of authenticating wireless clients through its strong encryption and key exchange protocols.

The Simplir Firewall Router Blade (FRB) implements a tiered authentication scheme taking advantage of multiple layers of security mechanisms. Simplir matches MAC addresses with their associated IP address creating an IP/MAC combined pair. If the IP/MAC pair authenticates against the FRB authentication table, a VPN port is opened to the client for further authentication under the VPN protocol. If the VPN authentication succeeds, the end user is allowed to transmit.

By authenticating traffic at the network edge, the points of access into the network, Simplir FRBs insulate and protect the network from unauthorized users attempting to compromise resources.

## **DOS and QOS**

The network's resources are a commodity, and they are in limited supply. Once a user session is authenticated, the network must protect itself from being consumed by that session and creating denial of service (DOS) against other network users. An authenticated network user could block other users from network services by saturating a network segment's bandwidth resources.

Quality of Service (QOS) is an excellent method of preventing DOS issues on the network. QOS describes traffic patterns for prioritization and limitation. It creates a way of allocating fair usage of the network's resources to users according to their classification. Based upon this classification system, network traffic is shaped to prescribed bandwidth limitations and preference.

Most wireless access points make no provisioning for QOS or perform QOS at a centralized location. The network becomes vulnerable to saturation between links when QOS lacks distribution at every link in the network. If, as a user, my traffic is not shaped until it reaches the Network Operations Center (NOC), for example, I could saturate network segments between the access point and NOC.

All Simplir FRBs implement QOS allowing the network to prioritize traffic between every access point and backhaul link in the network's topology. Embedded rulesets ensure performance throughout the network allotting per customer/end user bandwidth limits while reserving resources for network management. This bulkhead implementation guarantees consistent service by preserving the quality of every network segment.

## **Intrusion**

As a network provider, your own equipment as well as that of your customers requires protection from would-be intruders. Best network administration practices requires that network services or ports open to the network be limited to the minimal necessary for required network services. Although auditing the hosts on your network and explicitly turning off unnecessary services is recommended, further protections are offered to you through the FRB's firewalling capabilities.

The FRB performs stateful packet filtering allowing you fine control over the flow of packets across every segment of your network. The FRB is preprogrammed with default rulesets optimized for providing wireless access to end users. These default rules only forward traffic that has been authenticated for network transport.

Customization of the firewall ruleset allows end users to be opened in the firewall allowing them their own control of their systems using their own firewall. Or, offer value added service to your customer by providing firewalling services for them. This selection is easily maintained using the FRB customer management interface.

Further customization of the firewall is provided through pinholes. These additional rules for specialized traffic may be configured through the encrypted management interface.

Again, deploying Simplir's Firewall Router Blades to build your network infrastructure creates granular control of your network segments giving you Bulkhead protection.

## **Interception**

Interception of network communications is a real threat in today's networked World. Both wired and wireless networks are vulnerable to man in the middle eavesdropping attacks, but the risk increases in wireless communications where mobility of the attacker increases and physical barriers are reduced. Best practices in security recommend Virtual Private Networking (VPN) to encrypt communication transmissions.

The Simplir FRB offers VPN connections to end users giving you the best in today's encryption technology. By encrypting communications from the end user to the access point and across wireless backhaul to the Network

Operations Center, all of your wireless transmissions can be trusted secure.

## **Conclusion**

The security issues facing network managers have been considered in the development of Simplir's Firewall Router Blade. By compartmentalizing each issue and offering protections throughout the network between each segment, the FRB minimizes security weaknesses and their implications across the network. Only the integration of MAC/IP authentication, VPN authentication and encryption, and QOS into FRB products can provide the Bulkhead Network Security required for carrier grade wireless networking.