SecureDirect Reference Implementation Demonstration

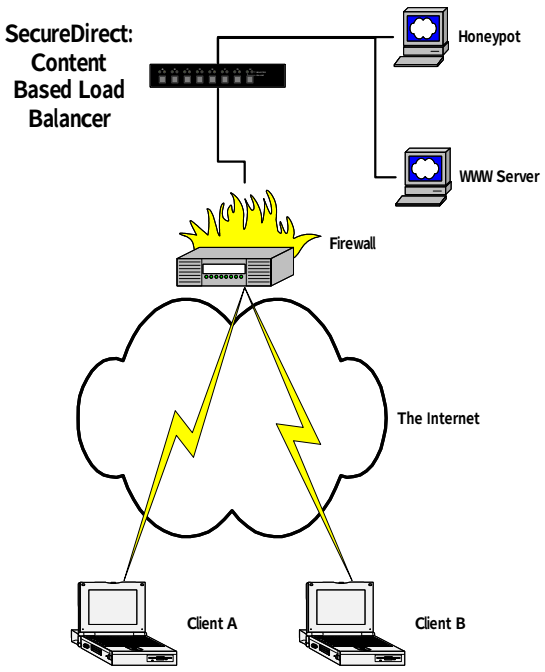
Internet Conference 2002

31 October 2002

Joe Stevens
j.stevens@jens.co.jp

Shadan Saniepour
s.shadan@jens.co.jp

The paper *Design and Implementation of Secure, Content Based Traffic Control* presented an overview of the design and the challenges faced in building the system we call *SecureDirect*. In order to better illustrate the functioning of this system, we will be demonstrating its core feature: the ability to direct internet traffic based on request content. The test network we will be using is diagramed below:



The server side of the demonstration will consist of 3 Sun Ultra 5 Workstations running Solaris 8 (The WWW Server, the Honeypot, and the SecureDirect Server) and a standard firewall appliance (Watchguard Technologies Firebox™ III Model 1000). Only the firewall appliance will be located on the public network. It will accept requests on port 80 to a public IP address (the "site IP"), and forward them to SecureDirect on the private network segment using standard Destination Network Address Translation (DNAT). This demonstration could have been accomplished without the firewall appliance, but would have required at least 3 public IP addresses. Both of the client machines are standard Windows-based notebook computers, and will be the only machines present at the Demonstration Site. The remainder will be located at JENS Corporation's Network Operations Center.

The demonstration itself will start by having participants use both client machines to browse to the site IP. Because neither machine has been identified as an attacker, both will see the "production" page on the WWW server. Next, a simple attack (directory traversal, etc) will be launched from one of the clients. Then, both clients will once again browse to the site IP. This time, however, one client will be identified as an attacker, and thus will see a special page served from the honeypot. The other client, however, will still see the page on the production WWW server, showing that the traffic from "good" clients remains unaffected.