

Preface

The Internet has come a long way over the past twenty years. In the beginning, it was a carefully designed product. Today, that careful design is still the foundation, but on top of it one finds a mixture of proprietary solutions, strange protocols and zealous networking components modifying every packet they see. The authors of this book take a network-focused approach to security, management and high availability in this evolving landscape. The Internet may not be as pretty as it could be, but no system in such wide use can avoid adaptation to the pressing needs of its users. The readers of this book can take solace in the simple fact that networking is still fundamentally predictable. The study of networking always rewards those who are willing to roll up their sleeves and watch the individual packets go by.

The most zealous of the networking components is, of course, the firewall. Born of necessity, the firewall is the most popular creature to ever touch a packet. It is also the most hateful and apt to block the traffic we so carefully direct from client to server. The first section of the book examines firewalls from simple packet filters to the fully configurable commercial firewall before moving on to more complex issues.

Simply put, today's firewalls do perverse things to traffic. They are not content to merely observe and drop packets, they insist on modifying them as they pass – they change IP addresses and port numbers; they snoop at the application layer; they stuff traffic into tunnels; they store detailed state about each connection and session. A packet exiting the firewall may look vastly different from what it looked like when entering it.

A networking element can change a packet so as to make it entirely unrecognizable. In fact, a whole new range of networking elements work at making it theoretically impossible for the unauthorized user to infer anything about the transformed packet. This is today's virtual private network. It is not possible to discuss firewalls without also addressing VPNs, as the firewall is frequently the most sensible place to terminate encrypted tunnels. The degree to which virtual private networking has increased the complexity of managing networks is quite surprising. Ironically, VPNs lead administrators to punch security holes in their once neat firewall border.

If anything highlights the unique approach of this book, it is the time spent discussing the management of network security on large-scale networks. Configuring and diagnosing problems with gateway-to-gateway VPNs can be very difficult when they are controlled by different administrators. Remote VPN users must be under the control of the firewall to prevent each remote endpoint from turning into a back door into the trusted private net-

work. Firewall policies must be flexible and reusable, so that they can be applied to a variety of network security enforcement points. Successfully managing such a system is the aim of some new products focusing on meta-management – stripping away the details of the systems to allow the administrator to deal efficiently with a multitude of related network objects. The firewall, which used to be the end-all in security, is becoming a commodity. It is no surprise, therefore, that security companies are manoeuvring to manage the security enforcement points. We are quite close to seeing each personal computer as a managed network entity that must be secured under centralised control.

If there is any aspect of this book that is dear to my heart, it is the section on high availability. The firewall, by definition, has historically been a choke point and single point of failure. That is the beauty and vulnerability of the firewall: it gives you a single point of security administration. Security always walks a fine line between blocking the undesirable, and permitting the desirable. Over time, network availability has come to be as important as security, and high available security has become the goal. High availability solutions are still not entirely mainstream. This book explores the state of the art in firewall load-balancing, while firewall and ISP link high availability helps bring the topic to the front. A topic is not accessible for study until it has been named and cataloged. I hope this book, by naming and cataloging the issues, will encourage others to take on the topic with a fresh perspective.

The future holds many more active networking elements – the firewall is just the beginning. The agile network architect will always be well served by remembering the network's humble beginnings and staying network-focused.

Paul LeMahieu

paul@rainfinity.com