Firewalls Are More Than Just Bandages

Peter Tasker, Chair
Executive Director
Information Systems Security Division
MITRE Corporation

Panelists:

Tom Haigh
Chief Technologist
Secure Computer Corporation

Tony Vincent
Director of Technical Services
Raptor Systems Inc

John Pescatore
Trusted Information Systems

TBD
.

Firewalls started as a relatively static first-line of defense, but they have become a central part of providing many protection services to an enterprise. This panel will look at the present roles played by firewalls and discuss important directions for the future. Can firewalls be effective against all of the emerging rich protocols associated with the World Wide Web? How should --or should-- firewalls respond to attacks? How do firewalls fit into the enterprise protection picture?

Questions the panel will address:

What services is it important for firewalls to provide besides traditional filtering? Are there some that should not be done at the firewall?

What kinds of attacks do firewalls respond to today and how do they respond? What are the pros and cons of dynamic response?

What can we expect firewalls to do against denial of service attacks?

What are the challenging applications for firewalls to support?

What are today's difficult security problems that firewalls do not address? What's hard about them? What's the hope of addressing them?

What's the role of desktop features in supporting the firewall's protection of the enterprise? With growing concerns about malicious Java applets and ActiveX controls, do firewall-like controls protecting the desktop make any sense to you?

How do firewalls limit damage to themselves when they're under attack?

What's important in the way of auditing and in tools for audit analysis?

Real-time alerts are becoming more important. Should customers want real-time alerts? What should they want? What should they expect (false positives versus false negatives)?

The security of a firewall is significantly influenced by the ease of configuring and maintaining the firewall. What's important in the administrative interface to a firewall?

There are lots of companies selling firewalls. What do you think are effective ways for testing and evaluating firewalls? Should firewalls be certified? If so, by whom?

There's talk about NT firewalls. Given the advertised security problems with NT, where do you stand on NT as the platform for a firewall? There are lots of tools for testing the features and configuration of Unix firewalls; what tools are available for testing NT firewalls?

What network security features do firewalls need to interact with?

What plans are there for remote authentication and administration in a VPN?

Do firewalls need to do anything different to address other network technologies (ATM, ISDN)? What different demands do these technologies place on a firewall?

What will be the next difficult security attacks for firewall vendors to worry about?