ASM Educational Center (ASM) *Est. 1992*

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

Firewall Penetration Testing

Most organizations have a perimeter firewall deployed between their internal systems and the Internet. This acts as the perimeter defense, filtering out unwanted inbound and outbound connections, as well as providing VPN, DLP, IPS and content checking capabilities for the organization. Firewalls have become much more intelligent than the stateful inspection firewalls of 5 years ago. SSL and IPSEC VPNs are terminated on them. They provide SMTP relay and HTTP proxying capabilities as well as providing comprehensive (DLP) Data Loss Prevention filtering. With these new capabilities comes increased risk, threat and potential exposures and therefore more advanced testing is required such as real validation of alerting when sensitive information is being removed from the organization, or ensuring when DDOS (Distributed Denial Of Service) are experienced the firewalls are able to deal with this traffic.

With multiple tiers of firewalls being deployed and constant changes in firewall rules, these devices need to be subject to stringent configuration and change management practices. This can help to ensure that potentially dangerous traffic is not allowed between systems in different network “trust zones” or “DMZ’s”. With our assessments taken from various points within your network, our consultants can assist you in understanding whether your firewall rules are an effective security measure and are only allowing necessary protocols. In conjunction with configuration audits performed in accordance with vendor standards, ASM can provide our clients with the assurance that they are not affected by risks such as excessive egress (outbound) access, hidden or undocumented firewall rules, and poor quality firewall log data being generated.