

# Network Protection for Design Professionals

## Default Security Settings

### Background:

Firewalls, routers, VPN appliances, wireless access points and other network hardware have pre-defined “factory default” configurations. Similarly, security related software has default settings which are predetermined by the vendor. There are often inherent vulnerabilities in these default configurations if not adjusted to an operation’s specific security requirements. A common problem is that administrative passwords for these devices are not changed from the default. Administrative passwords allow device configuration changes that could be used to disable security. Factory default passwords are easy for attackers to guess and, in most cases, are readily obtainable from published lists for specific manufacturers and models.

### How to implement appropriate controls:

Formal policies should be implemented regarding the configuration of all network security devices and systems.

- Default configurations should be avoided and specific procedures should be put in place for the management of strong administrative passwords for these devices and systems.
- The policies should be updated as new vulnerabilities arise or network configurations change.
- Default policy for firewall handling inbound traffic should be to block all packets and connections unless the traffic type and connections have been specifically permitted.

Further information on firewall configuration and policy can be found in:

**The National Institute of Standards and Technology’s Guidelines on Firewalls and Firewall Policy,**

<http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf>



VICTOR O.  
SCHINNERER  
& COMPANY, INC.

