Configuring a Router to Support SDM
November 10, 2008
By Luke Foster

Cisco SDM (Security Device Manager) is a web based management tool that works with the Cisco IOS to aid in the configuration and management of Cisco routers. The GUI (Graphical User Interface) allows engineers with little experience to configure Cisco routers, and stage large deployments. SDM is also powerful enough to help experienced engineers efficiently implement advanced security measures such as an IPS (intrusion Prevention System).

There are two types of SDM, SDM and SDM Express. The express version is just a limited form of SDM for routers that do not have enough flash memory to support the full SDM (SDM requires 6MB of flash, SDM Express requires only 2MB of flash). SDM is factory installed on the 1800 series, 2800 series, and 3800 series routers. SDM is also factory installed on router platforms with the (K9) security bundle. If a router does not have SDM installed, the software can be downloaded for free from Cisco. When downloading the SDM software from Cisco, make sure to verify the IOS version of the router can support SDM.

SDM provides several wizards to walk an engineer through configuring a router. These wizards range from interface configurations, to VPN (Virtual Private Network), and even QoS (Quality of Service) configurations. The Security Device Manager also provides real time monitoring, logging, and security audit features. It will even notify an engineer if it notices conflicting configuration parameters and suggest resolutions.

Note - SDM can be enabled on deployed routers without affecting the network

To configure a router to support SDM:

First, enable the HTTP or HTTPS server on the router.

Router# **configure terminal**
Router(config)# **ip http server**
Router(config)# **ip http secure-server**
Router(config)# **ip http authentication local**
Router(config)# **ip http timeout-policy idle 600 life 86400 requests 10000**

Next, create a user who has enable privileges

Router(config)# **username** *username* **privilege 15 secret 0** *password*

Finally, configure the vty lines to support telnet / ssh local login and privileged level 15 users

Router(config)# **line vty 0 4**
Router(config-line)# **privilege level 15**
Router(config-line)# **login local**
Router(config-line)# **transport input telnet ssh**
Router(config-line)# **exit**

Note – If your router supports 16 vty lines, enter the commands above for vty line 5-15 as well

Article Source: http://www.ccbootcamp.com/support-resources/resources/articles-by-ccbootcamp.html