Secure Your Home Router

Stephanie Obodda - 2021-12-04 - Comments (0) - Home Wireless

Recommended Features

- NAT & SPI (Stateful Packet Inspection)
- WPA2 Wireless Security
- Ability to Adjust Signal Strength

Optional "Power User" Features

- Segment Traffic (Vlans)
- Ability to Use 3rd Party Firmware (e.g. OpenWRT)

Securing the Router

- Enable Admin over Secure Protocols (HTTPS & SSH)
- Change the Admin Password
- Update the Firmware
- Disable Remote Administration
- Disable Universal Plug & Play (UPnP)
- Enable Logging
- Disable DMZ
- Configure WPA2-AES for Wi-Fi
- Use a Strong Pre-Shared Key (PSK)
- Adjust Signal Strength if Available
- Use Static IP Addresses or DHCP Reserved Addresses
- Customize WiFi SSID & Hide It

Additional Features

- Utilize Vlans and AP Isolation
- Use Port Mapping for Local Servers
- Set Schedules for Mapped Ports
- Power Off Router When Not in Use

Summary

- Keep Firmware Updated
- Change your PSK & Admin Passwords Regularly
- Shutdown Any Unnecessary Features

Relayed Resources

- Nov. 11, 2009 presentation: Slides | Audio + Slides
- http://openwrt.org/ (Linux distribution for embedded devices)
- http://wigle.net/ (Wireless Geographic Logging Engine)
- http://www.netstumbler.com/ (Windows tool for detecting wireless LANs)
- http://www.kismetwireless.net/ (software used to analyze wireless network traffic; packet sniffer)