Version 2.0

# What is SOCKS?

## An explanation of the SOCKS protocol and application proxy gateway systems

B. Scott Wilson, CISSP

IBM Global Services, Network Services

# What is SOCKS?

- SOCKS is a generic proxy protocol for TCP/IP-based networking applications.
- The SOCKS protocol provides a flexible framework for developing secure communications by easily integrating other security technologies.

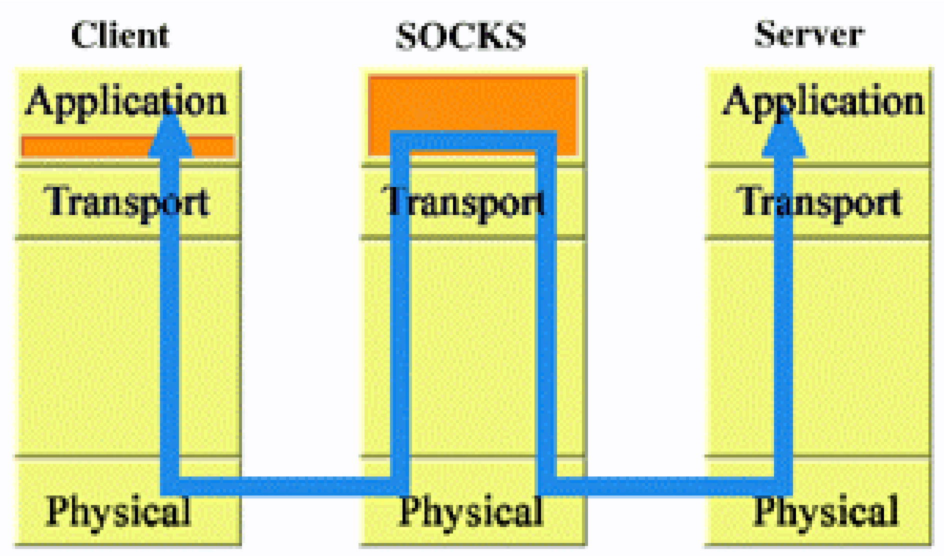
# How does it Work?

- When an application client needs to connect to an application server, the client machine connects to a SOCKS proxy server. The proxy server connects to the application server **on behalf of** the client, and relays data between the client and the application server.
- For the application server, the proxy server ***is*** the client.

# The SOCKS Protocol

- SOCKS version 5 is an IETF approved standard protocol implementation (RFC 1928).
- SOCKS includes two components, the SOCKS server and the SOCKS client. The SOCKS server is implemented at the application layer, while the SOCKS client is implemented between the application and transport layers *(see next slide).*
- The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS Server, without requiring direct “IP-reachability”.

# SOCKS and the OSI Layer Model

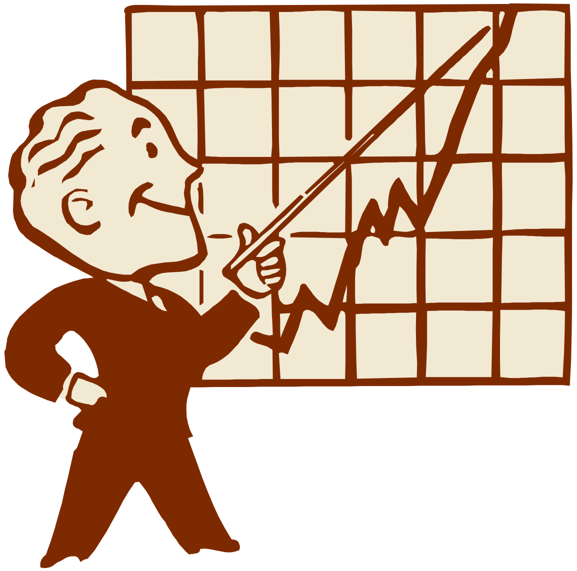


# Functions of SOCKS

- The SOCKS protocol performs four functions:
  - Making connection requests
  - Setting up proxy circuits
  - Relaying application data
  - Performing user authentication (optional)

# Features of SOCKS

- Transparent network access across multiple proxy servers
- Easy deployment of authentication and encryption methods
- Rapid deployment of new network applications
- Simple network security policy management



# Benefits of SOCKS

- A single communication protocol authenticates users and establishes the communication channel
- SOCKS is application independent
- Can be used with either UDP or TCP based protocols; even supports redirection of ICMP!
- Bi-directional support and intrinsic NAT, for added security and anti-spoofing.

# Summary

- SOCKS is based on IETF and industry **standards**
- SOCKS is **easy** to deploy and manage
- SOCKS is **transparent** to the user, while providing multiple layers of security