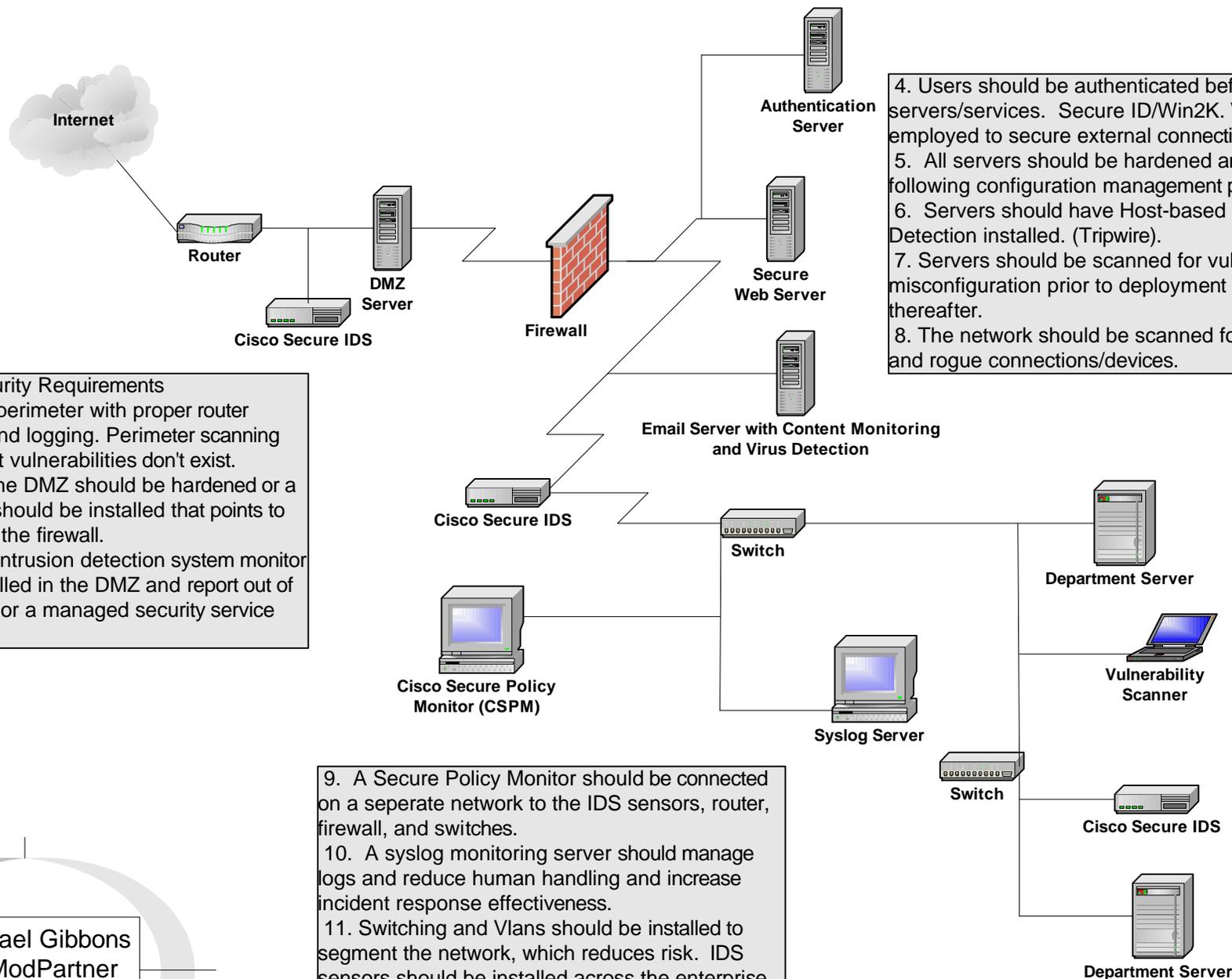


Network Security Tools and Services



Perimeter Security Requirements

1. Secure the perimeter with proper router configuration and logging. Perimeter scanning can ensure that vulnerabilities don't exist.
2. Servers in the DMZ should be hardened or a reverse proxy should be installed that points to servers behind the firewall.
3. A real time intrusion detection system monitor should be installed in the DMZ and report out of band to CSPM or a managed security service provider.

4. Users should be authenticated before accessing servers/services. Secure ID/Win2K. VPNs may be employed to secure external connections.
5. All servers should be hardened and patched following configuration management policy.
6. Servers should have Host-based Intrusion Detection installed. (Tripwire).
7. Servers should be scanned for vulnerabilities or misconfiguration prior to deployment and routinely thereafter.
8. The network should be scanned for vulnerabilities and rogue connections/devices.

9. A Secure Policy Monitor should be connected on a separate network to the IDS sensors, router, firewall, and switches.
10. A syslog monitoring server should manage logs and reduce human handling and increase incident response effectiveness.
11. Switching and Vlans should be installed to segment the network, which reduces risk. IDS sensors should be installed across the enterprise.

J. Michael Gibbons
SFA ModPartner
8/22/01