Security in a Virtual Office or "Office-in-a-Box"

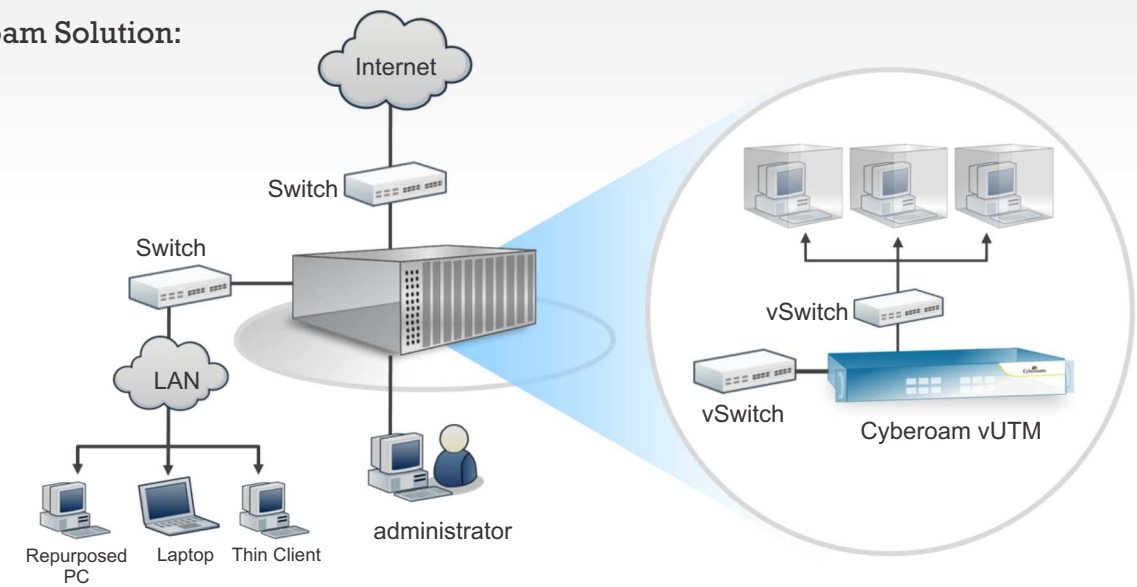
A virtual office or an 'Office-in-a-box' helps organizations handle the rise in number of devices in their network and helps employees connect to the network using their office PC and personal devices like home PC, iPad, android tablet, and more. This keeps the organization's intellectual property and other valuable data from leaving the network, while all data saved by employees is done on the organization's network. With the BYOD (Bring Your Own Device) trend catching up fast with most organizations, companies are finding themselves having to support multiple devices accessing their network resources across a range of operating systems and geographies. A virtual office allows them an easily scalable and rapid deployment scenario with minimal infrastructure costs involved.

Security Challenges of Virtualization

Users connecting to an 'Office-in-a-Box' network using multiple devices, specifically their personal devices that may lack security, increase the risk of security threat in the entire virtual network. User-based access controls become even more important in a virtual office set-up. For users connecting to the network while on the move or from home, a secure channel is important to ensure network and data security.

Virtual networks are also prone to attacks like hyperjacking; exploits attacking vulnerabilities in hypervisor management console, hypervisor & Guest OS; security risks arising out of loss of separation of duties between security/network security and operations and Zero Trust Networks.

The Cyberoam Solution:



Cyberoam virtual UTM provides multiple security features on a single appliance, protecting virtual office networks and assets with security features like firewall, IPS, Gateway Anti-Virus, Anti-Spam, Web Application Firewall, and much more. Cyberoam's Layer 8 Identity-based security policies over user authentication, service authorization and reporting (AAA) secure the Zero Trust virtual networks. Cyberoam's user-based controls enable controlled access to network resources. For users working from home, Cyberoam virtual UTM's VPN feature allows a threat-free tunnel for secure access to network resources.

Cyberoam virtual UTMs enable administrators to segment the management console in DMZ, route all traffic through Cyberoam virtual UTM appliances, and also enable separation of administrator duties with role-based administrator controls.