

# MyVCO v2 Survival Guide



Page 1 of 2

*NetWolves network security services reduce the time and resources a business enterprise requires to maintain a protected network*

Unlike other network security products on the market that can be difficult to install and configure, NetWolves offers a comprehensive all-in-one solution with a common web-based interface that bridges the gap between protection and ease-of-use.

Depending on your company's particular network security policies, you may decide to implement some or all of the security services offered by NetWolves. All services are fully compatible, so you can decide to upgrade at any time to take advantage of additional features. These security services can also be managed from a central location using NetWolves' Secure Remote Monitoring & Management (SRM<sup>2</sup>) system.

**PCA and HIPPA-compliant Firewall** uses a combination of advanced security features for protecting systems on a company's network, while simultaneously allowing users to easily exchange information with others on the Internet. The firewall and network address translation (NAT) services offer total control over the creation of custom rules used to meet the stringent demands of nearly any IT security policy. Both the firewall and NAT also offer pre-defined rule sets, which provide for immediate security between the protected network systems and Internet.

**ASURERoute** is a unique dynamic alternate routing technology that determines when the required network service levels are not being met on your primary circuit. ASURERoute can determine, on a per application basis, if performance problems exist, and route traffic to an available secondary circuit that provides uninterrupted service, again on a per application basis. ASURERoute will continue to monitor network conditions, and when service levels can be met, it will permit traffic once again to utilize the primary circuit. ASURERoute can support any circuit technology serving as the primary and secondary means of network connectivity, including DSL, cable modem, satellite, frame relay, private line, ISDN, and IP.

**IPSec-Compliant VPN** is an extremely efficient and cost-effective alternative to frame relay lease line services. It is designed to provide users with transparent access to the VPN while also securing their communications activity. NetWolves' IPSec VPN is interoperable with VPN devices from vendors such as Check Point, Cisco, SonicWALL, and many others.

**MyVCO** v2  
virtual connected office



powered by **NetWolves**

## **IPSec host and client VPN**

### **SSL VPN**

### **ASURERoute**

### **Congestion management**

### **Advanced routing protocols**

### **Quality of service**

### **Intrusion detection**

### **Content filtering**

### **Email virus protection**

### **Internal and external (split) proxy services**

### **Mail server supports SMTP, IMAP4 and POP3**

### **Apache web server**

### **File sharing**

### **Log & report operating statistics and message logs**

### **Backup & restore email accounts, password files, web content and shared files**

### **Web-based administrative interface**

# Network Security



Client VPN, featuring SafeNet's HighAssurance™ Remote, includes FIPS technology, device authentication, and the Advanced Encryption Standard (AES) algorithm. HighAssurance Remote contains numerous high-level security features not currently found in other client VPN software products, and it is fully interoperable with NetWolves' Managed Network Security Services.

**SSL VPN** leverages the power and protection afforded by the Secure Socket Layer protocol, standard with today's popular web browsers, to access vital web-enabled resource applications on a company's protected network, including common email and file-share utilities. With NetWolves' SSL VPN, customers can provide authorized users with a simple key chain USB device and unique login password. The combination of these two security features provides formidable protection against unauthorized use resulting from password theft through such means as key logging or theft of the USB device itself.

**Congestion Management** monitors traffic congestion and bandwidth levels on two VPN tunnels between a WolfPac, located at a remote/branch site, and a hub device located at a main site. When traffic congestion is determined to be too high or bandwidth is too low on one tunnel, the WolfPac switches to a secondary VPN tunnel. Congestion and

bandwidth levels also are monitored on the second tunnel. Bandwidth threshold parameters can be specified to determine what conditions must exist in order for the second tunnel to be utilized.

**Advanced Routing** determines the appropriate path onto which data is forwarded between network devices, and how changes are reported and information is shared between these devices. The BGP, OSPF and RIP protocols are supported, as well as GRE tunneling.

**Quality of Service** offers a secure and reliable means of controlling, or shaping, the general intensity, direction and breakup of network traffic entering or leaving the WolfPac. QoS uses bandwidth capping, delays, and flow queues to perform this important function.

**Content Filtering** permits a business to effectively block or deny access to the Internet or specific web sites. Filtering irrelevant and unwanted Internet content is an effective tool for implementing and enforcing Internet usage policies, minimizing time-wasting and inappropriate Internet viewing habits, and substantially improving inter-networking bandwidth.

**Intrusion Detection** monitors the network's local host devices and network traffic for signs of attempted attacks and network security breaches. It is designed to detect and report unauthorized activity throughout a network, including port scans, network mapping, unauthorized access, failed access attempts, and abnormal network traffic patterns. NetWolves utilizes well-tested and proven network IDS technologies to accomplish its regimen. These technologies perform real-time traffic analysis and packet logging on IP networks, as well as host-based protection for the WolfPac security platform.

**Email Virus Protection** performs a number of functions to detect possible email viruses and prevent them from infecting network systems. The virus signature DAT file can be updated regularly in order to effectively detect the latest viruses.

Call today to learn more about  
NetWolves' A Single Source  
Managed Services Provider.