Zyxel ZyWall USG100 Brings Unified Threat Management

DATE: 2008-09-08
By Frank Ohlhorst

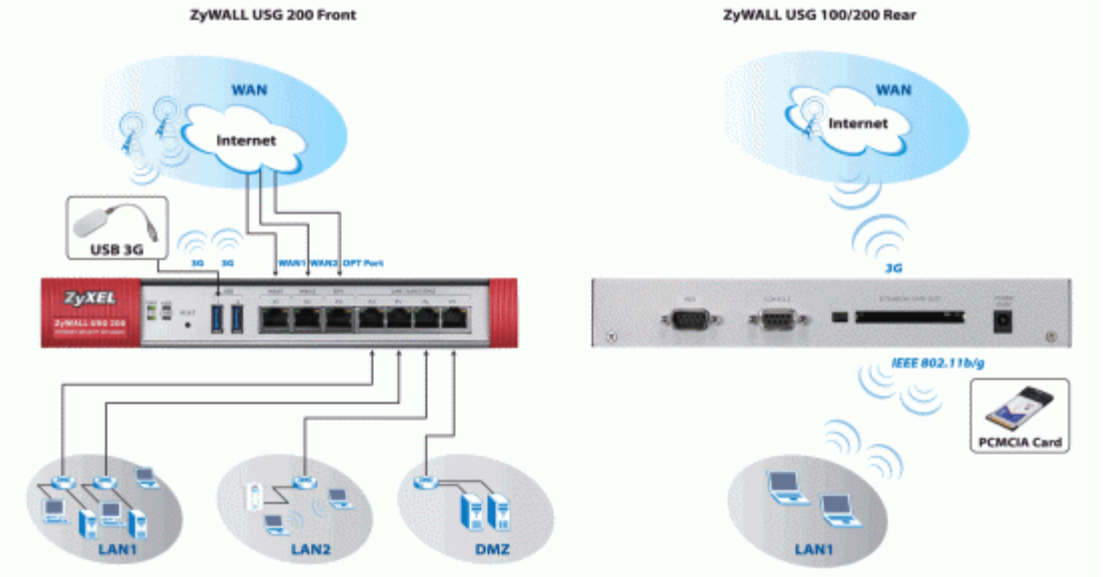
With the ZyWall USG100 Unified Threat Management appliance, Zyxel dares to go beyond the firewall concept and tread where Symantec, Sonicwall, Fortinet and WatchGuard reign supreme.

The word "firewall" conjures up all sorts of images, and therein lies the problem. That word has become a catchall for an abundance of security products, both software- and hardware-based, which can share very little in common. While the industry continues to struggle with the question of what exactly a firewall is, networking vendor Zyxel Communications has decided to move beyond the term firewall and classify its latest device, the Zywall USG100, as a Unified Threat Management appliance.

Simply put, the USG100 is much more than a firewall; it is an appliance that protects networks from a variety of security threats, from malware to intrusions to spam. What's more, the USG100 offers VPN support—SSL (Secure Sockets Layer) and IP Security—as well as bandwidth management and a slew of other features.

At first glance, the USG100's feature set seems impressive, especially at an MSRP of just $649, but one has to realize that the UTM market is crowded at best, oversaturated at worst and dominated by industry giants such as Symantec, Sonicwall and Fortinet. All of those vendors have products that are pretty close in features to Zyxel's USG100, making Zyxel's leap into the market a challenging one.

Fortunately, Zyxel has a few elements on its side when it comes to entering a challenging market. First off, the company has a strong channel commitment and is devoted to partners. Secondly, the USG100 is offered at a price that is several hundred dollars lower than its competitors. Thirdly, Zyxel has gone to great lengths to incorporate features that attempt to best the competition in several areas, ranging from speed to capacity to ease of use.



Zyxel is positioning the USG100 as a comprehensive security appliance for offices with up to 25 users. That clearly places the unit in the small business realm, a market saddled by many challenges. Small businesses have some unique needs centered on affordability and ease of use. What's more, small businesses need access to the same level of security that is commonly available to enterprises, just without the complexity. Zyxel has recognized those needs and has built the USG100 from the ground up to service the small business market, taking a different approach than many other vendors that "dumb down" their enterprise offerings to serve the small business market.

The USG100 offers a feature set that includes:

- ICSA-certified firewall (rated at 100M bps)
- Anti-virus: (ICSA-certified Zyxel Anti-Virus and Kaspersky Lab)
- Intrusion detection and prevention
- VPN (ICSA-certified IPSec , SSL, L2TP, up to 50 tunnels); two licenses included.
- Instant messaging and peer-to-peer management
- Anti-spam
- User-aware configuration and policy engine
- Bandwidth management and traffic prioritization
- Multiple ISP link support for high availability and redundancy
- Content filtering
- Support for 3G wireless networks (High-Speed Downlink Packet Access and Evolution Data Optimized)

The physical device sports two USB ports, two 10/100/1000 Ethernet WAN ports, five 10/100/1000 Ethernet LAN ports, a serial port (for dial-up modems), an RS232 console port and a PCCard port for PCMCIA-based communications cards. The unit includes brackets for rack-mounting and a 12-volt external power brick.

Administrators will find the unit very easy to deploy. After plugging the unit in, administrators simply point a Web browser at a default address to download a security certificate and access the installation wizard.

Zyxel really did its homework when it comes to easy setup. The setup wizard starts by offering a choice of either a single ISP or dual ISP configuration. The dual ISP portion of the wizard

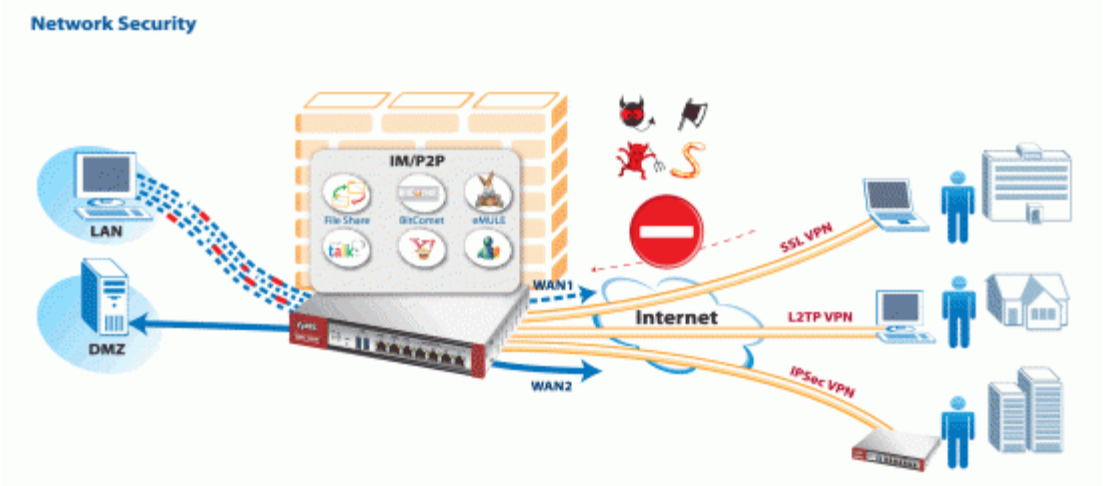
autopopulates the options for connecting to two separate ISPs and helps administrators define whether those connections should be used for failover or high availability or be bonded together.

Choosing the single ISP option skips over the high-availability options and dives right into the basic setup of the unit. Here, administrators will need to know some details about the ISP and the local network. The wizard does an excellent job of stepping administrators through the WAN setup portion of the install; installers can choose from PPOE, cable modem, DSL or most any other type of broadband Ethernet setup. Once the basics are set up, administrators will have to register the device and select what service subscriptions are to be used. Anti-spam protection is free, while other security services have a yearly fee associated with them. A combined package for $340 offers a year's worth of anti-virus, content filtering and IDS/IPS (intrusion detection services/intrusion protection services). The various security services are also available a la carte.

The setup wizard can also optionally launch the VPN Advanced Wizard, which walks users through the process of defining VPN connectivity and which encryption method should be used. While the process is complex in the terms and definitions used, any administrator should be able to breeze through advanced VPN settings using the wizard.

Other setup chores are wizard-driven, but administrators may want to turn to the product's quick-start guide to make setup easier. Zyxel includes a CD with the USG100 that contains comprehensive documentation in PDF form. The very detailed documentation offers diagrams and tips on how to deploy the device.

Administrators will definitely want to refer to the documentation to define rules, roles and zones. The device offers a high level of configurability, allowing it to address the most arcane of implementations. Luckily, an abundance of examples are included in the documentation to make the setup chores as easy as possible. The documentation also sports several tutorials that will help administrators get quickly up to speed on the intricacies of the product and also can educate administrators on many of the standards and terms used by today's security devices.



Once the device is fully configured, administrators can turn to the browser-based status screen to keep an eye on things. The status screen supports drilling down into individual management objects and can launch reports and process notifications via e-mail or other methods. Solution providers can remotely monitor and manage the device, perhaps rolling the product into an SLA (service-level agreement) or managed services offering. Either way, the USG100 offers plenty of administrative capabilities to make it easy to manage and monitor.

Extensive logging delivers management reports that can be used for technical as well as administrative and management information. Administrators can generate reports showing traffic, blocked sites, VPN usage and so on, allowing them to quickly demonstrate ROI of the device and associated services.

For end users, the implementation of the device is seamless. All the typical desktop user will notice is a lack of virus infections, a reduction in spam and an increase in WAN reliability. What's more, the content filtering engine can be set up to offer "nonjudgmental" warnings about accessing unapproved sites and can have a positive spin based upon protecting the user from dangerous content.

Administrators will appreciate how straightforward the setup of rules, policies and filtering is. That ease of use also applies to traffic management, where definitions can be quickly done to maximize VOIP (or other) traffic to prevent lost packets or slow performance for mission-critical applications. That "traffic shaping" can be based upon user, destination or type of traffic encountered, a truly flexible way of handling something as critical as network traffic. Using Zyxel's Application Patrol configuration allows traffic shaping to be driven by specific applications, allowing administrators to further fine-tune performance for line-of-business applications.

The product's implementation of dual virus scanners helps administrators take a layered approach to protecting users and the network from malware. Zyxel's own anti-virus engine helps to keep things safe at the edge of the network, while the bundled Kaspersky Lab anti-virus engine serves as a catchall for anything that may get past the edge and attempt to infect endpoints inside the network.

All things considered, Zyxel offers an excellent alternative to the mainstream products on the market for protecting the small business network or branch office from the ills of the Internet. The USG100 proves to be affordable, reliable and easy to use and would be a welcome addition to any small network seeking enterprise-level protection. The company's commitment to the channel ensures that plenty of qualified dealers and installers are available and that the product should be easy to purchase and deploy for end users.