PROTECTSTAR

AWARD

2005

www.protectstar.com

ZyXEL
ZyWALL P1

PROTECTSTAR®
for your security

Einleitung

Die **ZyWALL P1** wird vom Hersteller **ZyXEL** als „**portable und persönliche Internet-Sicherheitslösung**“ angeboten und bietet Benutzern eine Vielzahl an Möglichkeiten. Vom simplen Schutz des Außendienstnotebooks mittels der integrierten Firewall bis hin zu komplexen **VPN-Konfigurationen**.

Mit ihrem **geringen Gewicht** und **kompakten Abmessungen** bietet die ZyWALL P1 vor allem mobilen Anwendern die Möglichkeit einer VPN-Verbindung zur Errichtung eines eigenen privaten und sicheren Hotspots. Die Plug-and-Play fähige Lösung von ZyXEL ist leicht zu Installieren und ermöglicht Anwendern so, sich entspannt auf das (mobile) Arbeiten zu konzentrieren.

Sicherheit

Im Testlabor von ProtectStar konnte die **ZyWALL P1** von ZyXEL in den Hardwarerevisionen **V3.64(XJ.4)** und **V3.64(XJ.5)** getestet werden. Turnusmäßig musste die Sicherheitslösung schwierige und umfassende Testreihen durchlaufen.

Die leistungsstarken Sicherheitsmechanismen des Gerätes arbeiten mit der ICSA zertifizierten ZyXEL ZyNOS Plattform zusammen, die eine ausgezeichnete **Stateful Packet Inspection** Firewall und Schutz vor **DDoS/DoS** Angriffen bietet.

Auf den Testreihen stand neben **DoS-Angriffen** und **Attacken** auf den **Web-Server** der ZyWALL P1, zusätzlich noch unterschiedliche Portscans (SYN, tcp) sowie Angriffe auf die verschiedenen **IP-basierten Tunnel** der ZyWALL P1. Im Rahmen dieser Testreihen konnten **keine** sicherheitsrelevanten Mängel festgestellt werden.

Die Testergebnisse, welche unter anderem mit dem „Penetrator“ des dänischen Herstellers SecurityPoint erzielt werden konnten waren zum Zeitpunkt des Tests mit **gut bis sehr gut** zu bewerten. Keiner der **6403** unterschiedlichen Exploits und Angriffe hatte Erfolg.

Den **dreistündigen** Dauer-Penetrationstest hat das portable Gerät ebenfalls **erfolgreich** absolviert. Als **sehr problematisch** erwies sich jedoch die ZyWALL P1 im Umgang mit ARP-Angriffen. Die ZyWALL P1 bietet **unzureichenden Schutz** gegen „falsch“ formatierte „arp-requests“. Es ist somit bereits in den Werkseinstellungen möglich, **den Transfer von Daten komplett zu unterbinden**. Dies betrifft sowohl das LAN als auch das WAN Interface. Gerade auf dem WAN-Interface sind die Einstellungen restriktiver gesetzt.

Nach Rücksprache mit ZyXEL Deutschland und ZyXEL Taiwan erwies sich die Sicherheitslücke als echt. ZyXEL reagierte innerhalb weniger Stunden mit einem Patch **V3.64(XJ.6).** Die Sicherheitslücke wurde damit bereinigt. Wir empfehlen allen Anwendern **umgehend** ihre Appliances mit dieser aktuellen Firmware zu **aktualisieren**.

Leider gibt es für die ZyWALL P1 keine automatische Update-Funktion. Dies bedeutet, dass Firmware- oder Sicherheitsupdates auf den Webseiten von ZyXEL heruntergeladen und **manuell** installiert werden müssen. Einen Schatten auf die positiven Ergebnisse des Audits werfen jedoch die **Werkseinstellungen** der ZyWALL P1. So ist ab Werk der Remote-Zugang sowohl auf den **LAN** als auch auf dem **WAN-Interface** des Gerätes erlaubt, die es einem Außenstehenden erlauben könnten, essentielle Informationen über das System zu sammeln.

Das Management der ZyWALL P1 ist via **http**, **https**, **Telnet**, **ssh** sowie **snmp** möglich. Es wird empfohlen diese Dienste auf dem WAN-Interface des Gerätes direkt nach der Inbetriebnahme abzuschalten, sofern **Remote-Management** nicht ausdrücklich erwünscht ist. Weiterhin sollte das **Default-Passwort** umgehend geändert werden.

Der Zugang zum System ist grundlegend in **zwei Stufen** getrennt. Die Abfrage des Passwortes erfolgt jedoch erst beim Betreten des sog. „**Advanced-Levels“**. Dieses Verhalten dient der besseren Administration durch den Systemverantwortlichen, während es auf der anderen

Benutzerfreundlichkeit

Die Installation und Konfiguration der ZyWALL P1 ist sehr **anwenderfreundlich** und der Installationsassistent hilft Benutzern das portable Gerät in einfachen Schritten zu konfigurieren.

Seite den Anwender davor **schützt**, das System durch **ungewollte Einstellungen** für den Einsatz im Firmennetzwerk unbrauchbar zu machen. Hier zeigen sich die **außerordentlichen Qualitäten** der ZyWALL P1. Neben den elementaren Systemeinstellungen wie beispielsweise der Konfiguration der IP-Adressen auf den beiden Schnittstellen, lassen sich hier **umfangreiche** und **individuelle** Einstellungen an der Firewall vornehmen, sowie das Verhalten des **IP-Sec** basierten **Virtual Private Networks** beeinflussen.

Die ZyWALL P1 unterstützt hier Administratoren durch die **Vielseitigkeit** der möglichen Einstellungen bezüglich des **Systemlogs**. Hier hat der Administrator nicht nur die Möglichkeit, bei einzelnen Verstößen gegen Firewallregeln eine Nachricht versenden zu lassen, sondern auch die Option, 23 einzelnen Oberhemen (VPN; IPSec, UPnP, PPPoE PacketFilter, usw.) loggen zu lassen. Die einzelnen Regeln lassen sich den **Bedürfnissen des Anwenders** bis ins Detail anpassen.

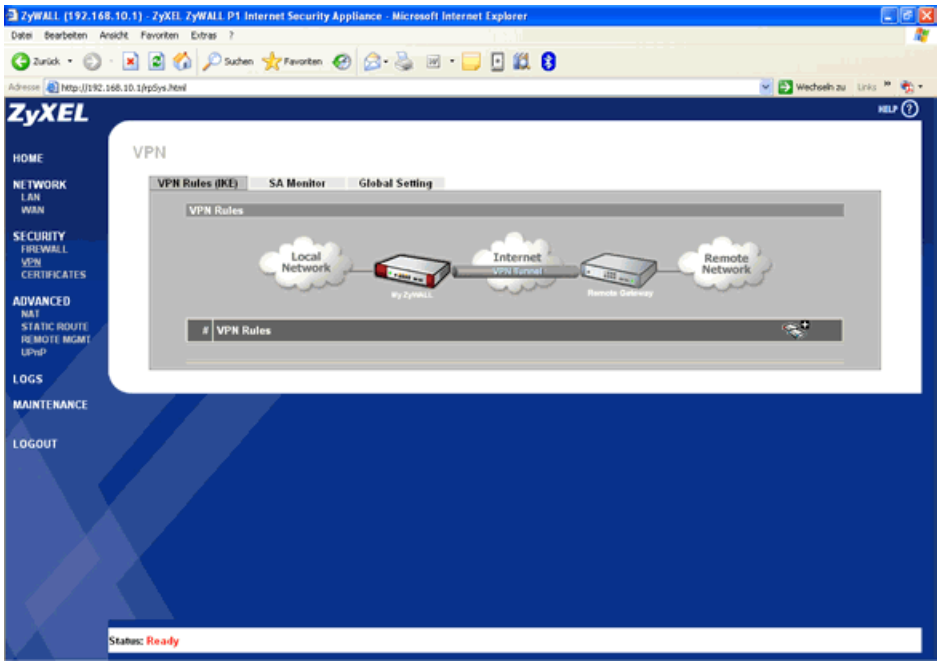
Zusätzlich zur Firewall schützt die optionale **Network-Address-Translation (NAT),** die hinter der ZyWALL P1 befindlichen Rechner und Systeme (bspw. angeschlossen durch einen Hub) absichert. Muss ein System dauerhaft erreichbar bleiben, bzw. wählt es sich von unterschiedlichen Standorten aus ein, kann der Dienst **DynDNS.org** problemlos genutzt werden. Die Appliance teilt dem DNS-System in diesem Fall die jeweils aktuelle IP-Adressen der WAN-Seite des Gerätes mit.

Die ZyWALL P1 kann sich im Bereich Sicherheit **vor** den aktuellen **Personal Firewalls platzieren**. Ausschlaggebend ist hier die externe Bauweise, welche das zu schützende System auch physikalisch von angrenzenden Netzwerken trennt. Somit ist der Schutz des eigenen Systems nicht von der sicheren Konfiguration des zugrunde liegenden Betriebssystems abhängig.

Die Konfiguration der ZyWALL P1 erfolgt über eine übersichtliche und verständliche Weboberfläche. Hier ist nicht nur das optisch ansprechende Design des Web-Interfaces erwähnenswert, sondern vor allem das **sechssprachige** (Englisch, Deutsch, Französisch, Spanisch, Japanisch, Spanisch, Italienisch) Konfigurationsmenü.

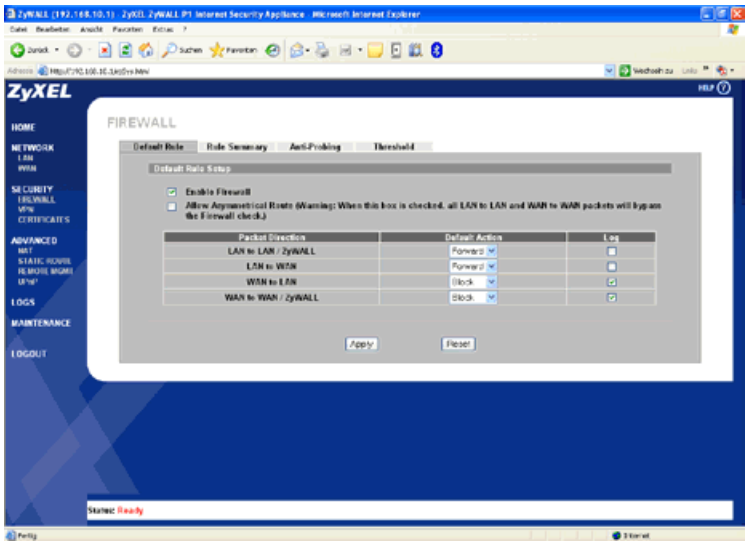
Kein anderer Hersteller auf dem IT-Markt bietet ein mehrsprachiges Konfigurationsmenü in einem derartig großen Umfang an. Die ZyWALL P1 bietet Anwendern neben dem Web-Interface, welches via **http** und **https** erreichbar ist den Zugang mittels **Telnet** und **Secure-Shell** an. Das Web-Interface ist **schnell**, neigte jedoch bei einigen Testreihen auch zu **Fehlermeldungen** des Web-Servers, der einzelne Seiten der Konfiguration nicht abrufen konnte und dies dem Anwender mit einer Fehlermeldung anzeigte.

Der Einsatz der **ZyWALL P1** kann, aufgrund der **portablen** externen Ausführung, mit jedem **beliebigen Client** betrieben werden, zur Not auch auf Systemen, die nicht über einen Web-Browser verfügen wie



beispielsweise ein temporär aufgestellter Server. Unerfahrenen Anwendern stellt das System der ZyWALL P1 sog. „Wizards“ zur Verfügung, die bei der Konfiguration des Internet-Zugangs sowie des optionalen VPNs behilflich sind. Die in jedem Dialog verfügbare **Online-Hilfe** macht es zudem möglich, sich im System mühelos zu Recht zu finden. Das auf CD-Rom mitgelieferte, **über 350 Seiten starke Handbuch** beschreibt neben den einzelnen Funktionen der ZyWALL P1, auch Grundlagen und Geschehen hinter den möglichen Einstellungen.

Benutzer die mittels **Telnet** oder **Secure-Shell** das System der ZyWALL P1 administrieren möchten, sieht sich einem Interface gegenüber, das an Geräte von **Bay-Networks** erinnert. Navigiert wird hier mittels Kommandos, die jedoch einige Einarbeitung und Erfahrung erfordern.



Die unterschiedlichen Zugänge sind in ihrem Funktionsumfang vergleichbar, so dass dem Web-Interface bezüglich seiner **hervorragenden Zugänglichkeit** wohl häufiger der Vorzug gegeben wird.

Die vom Hersteller beigelegte **Ledertasche** biete einen erweiterten Schutz gegen Kratzer und kleinere Schläge, wie sie etwa durch unsanftes Absetzen einer Notebooktasche entstehen könnten. Gerade jedoch bei einem für den mobilen Einsatz konzipierten Gerät wäre - unabhängig der Gewichtszunahme - ein noch stabileres Gehäuse praktisch.

Performance

Die ZyWALL P1 arbeitete in den Testreihen **schnell** und **zuverlässig**. Die vom Hersteller gemachten Angaben bezüglich der Performance zur ZyWALL P1 konnten im Testcenter von ProtectStar **bestätigt** werden. Die Stateful Packet Inspection Firewall kann Durchsatzraten von **80** MBit/s und VPN (DES, 3DES) **30 MBit/s** verarbeiten.

Das System bleibt auch unter Volllast administrierbar. Einen Timeout dynamisch aufgebauter Sessions (wie etwa bei einer http-Anfrage) bei ausgelasteten Schnittstellen konnten hier - im Gegensatz zu anderen Produkten auf dem Markt - nicht festgestellt werden.

Der Datendurchsatz ist für eine Lösung dieser Größen- / und Preisordnung **als gut zu bewerten.** Es sollte jedoch bedachte werden das die Appliance ausdrücklich für den Endanwender gedacht ist, und somit dem in einem Firmennetzwerk auftretenden Traffic an Schlüsselpositionen nur bedingt gewachsen wäre.

Support

Mit dem Erwerb der **ZyWALL P1** erhalten Anwender **zwei Jahre** Garantie und den kostenlosen ZyXEL Support inklusive. Deutschsprachige Anwender können unter www.zyxel.de oder www.zyxel.com (international) auf eine umfangreiche Wissensdatenbank (Knowledge-Base) und einem Download-Bereich zugreifen, wo die aktuellen Dateien und das Handbuch heruntergeladen werden können. Ebenfalls über diese Webseiten kann der Anwender eine Supportanfrage über ein vorgefertigtes Online-Formular stellen.

Für den Fall das die im Handbuch bereitgestellten Informationen dem Anwender nicht ausreichen sollten oder im Falle von technischen Problemen, steht ZyXEL den Anwendern in Deutschland via Telefon, Fax und E-Mail zur Verfügung.

Preis / Leistungsverhältnis

ZyXEL Deutschland bietet die **ZyWALL P1** zum Preis von Euro **199,00** inkl. Mehrwertsteuer an. Bei der Vielzahl an Einsatzmöglichkeiten ist dies ein gerechtfertigter Preis. Das hohe Schutzniveau sowie die sehr vielseitigen Konfigurationsmöglichkeiten machen die ZyWALL P1 zu einer **empfehlenswerten Lösung** wenn es um den Schutz von **einzelnen Telearbeitsplätzen** geht**.**

Sie ist damit auch eine ausgezeichnete Alternative zur Anschaffung von Personal Firewalls, da sie den Schutz bereits vor dem eigentlich zu schützenden System gewährleistet.

Fazit

Auf der technischen Seite kann die ZyWALL P1 **überzeugen**. Sie kombiniert **sehr guten Grundschutz** mit **guter Performance** und lässt das mobile Arbeiten zum Vergnügen werden.

Das **handliche und kompakte** Netzwerkgerät bietet mit der leistungsstarken Firewall und der „Network Outbreak Prevention“ sehr guten und individuellen Schutz vor Angriffen aus dem Internet und durch den geringen Verwaltungsaufwand werden komplexe Softwareinstallationen umgangen.

Die gute Unterstützung für IP-basierte VPNs, PPTP und PPPoE sorgen für stets gute Verbindungsmöglichkeiten mit der Außenwelt. Während den Testreihen zeigte sich auch, dass ZyXEL innerhalb weniger Stunden auf eine gefundene Sicherheitslücke (arp-requests / siehe Sicherheit) problemlos reagieren und ein Patch zur Verfügung stellen kann. Sowohl die Kommunikation als auch die Reaktion seitens ZyXEL waren diesbezüglich vorbildlich.

Einem **sehr guten Gesamturteil** stehen lediglich die etwas fragwürdige Verarbeitung des Gehäuses, sowie die Fehler des Webservers entgegen, die auf einigen Testsystemen beobachtet wurden.

Die per **Default** auf beiden Interfaces zu erreichende Systemkonfiguration ist ein Umstand, dem der Hersteller ZyXEL nachgehen sollte. Hier könnten durch restriktivere Grundeinstellungen (unaufmerksame) Anwender besser geschützt werden.

Die ZyWALL P1 von ZyXEL wird aufgrund der guten Testergebnisse mit dem „ProtectStar AWARD 2005“ ausgezeichnet

www.ProtectStar.com

PROTECTSTAR®
for your security

ProtectStar Inc.
1901 60th Place
Suite L 3604
Bradenton, FL 34203
USA

www.protectstar.com
testcenter@protectstar.com

Gestaltung: wo-pro werbung - www.wo-pro.de