

ZyXEL



All-in-one – vereinte Sicherheit auf hohem Level



Unified Security

- Flexibilität dank Hybrid-VPN
- Geschützte IP-Telefonie (VoIP)
- Gefahr Peer-to-Peer-Applikationen
- Netzwerk-Segmentierung
- Ausfallsicherheit durch High-Availability
- Netzwerk-Reporting

ROWA Computer AG
Grubenstrasse 2
5070 Frick
Tel. 062 865 20 21 - Fax 062 865 20 30
info@rowa.ch - www.rowa.ch



Sicherheit versus Flexibilität

Sicherheit in neuen Dimensionen

Die Sicherheitsanforderungen wachsen mit der Komplexität unserer Systeme und Strukturen. Neue Endgeräte und Arbeitswelten mit mobilen Mitarbeitern an Heim-Arbeitsplätzen oder im Aussendienst erfordern neue Sicherheitslösungen. Auch möchten Geschäftspartner und Lieferanten heute auf wichtige Unternehmensressourcen (z. B. Produkt- und Lagerinformationen) zugreifen können.

Sicherheitsrisiko fremder Netzwerke

Wenn User auf Unternehmensdaten zugreifen, befinden sie sich zum Teil in Internet-Cafés, Flughäfen oder Hotels. Die eingesetzten Endgeräte sind vielseitig: PDAs mit SSL, Windows-Mobile-Nutzer via L2TP, Smartphones, private PCs oder PCs aus fremden Netzwerken.

Neuer Trend: Hybrid-VPN

Bisher galten hauptsächlich IPSec-basierte VPN-Verbindungen als Lösung für den sicheren Remote-Zugriff. Heute bietet Hybrid-VPN, welches IPSec, L2TP und SSL umfasst, das ideale Werkzeug, um sämtlichen Anforderungen gerecht zu werden.

UTM für sichere Zugangskontrolle

UTM-Funktionen wie Anti-Virus und Intrusion-Prevention filtern Schädlinge bereits am Gateway. Darüber hinaus kann mit Hilfe einer Reporting-Software eine zuverlässige Kontrolle aller Netzwerk-Bewegungen gewährleistet werden. Alarmer bei kritischen Ereignissen ermöglichen ein schnelles Reagieren.

Neue Firewall-Generation

Mit der ZyWALL USG-Serie lanciert ZYXEL eine neue Generation von Security-Gateways. Die ZyWALL USG-Modelle basieren auf einem neuen Firewall-Betriebssystem und bieten mehr Performance, mehr Features und sind mit einer objektorientierten Konfiguration flexibler in der Verwaltung.

ROWA Computer AG
Grubenstrasse 2
5070 Frick
Tel. 062 865 20 21 - Fax 062 865 20 30
info@rowa.ch - www.rowa.ch

Flexibilität dank Hybrid-VPN

VPN: Die Qual der Wahl

Bei VPN besteht heute die Wahl zwischen IPSec, SSL und L2TP. Pauschal gesagt, ist sicher ein Mix aus allen drei möglichen Zugriffsarten die beste Lösung. SSL und IPSec bzw. L2TP-VPN bieten unterschiedliche Vorteile. Die Wahl der VPN-Technologie ist immer vom Einsatz abhängig.

IPSec-VPN – fest installiert

Als Beispiel sei hier ein User erwähnt, der nicht nur jederzeit den Netzwerkzugang benötigt (always-on), sondern ebenso sämtliche Applikationen wie beispielsweise VoIP nutzt. Für diesen Benutzer ist IPSec-VPN die logische Wahl: Da auf dem Endgerät die Installation eines Clients notwendig ist, ist hier eine höhere Sicherheit gewährleistet. Die ZyWALL Firewalls sind in der Lage, bis zu 1'000 solcher Verbindungen aufzubauen und selbstständig zu terminieren. Die dahinter liegenden Server können sich somit auf ihre Kernaufgaben konzentrieren, da die ZyWALL die komplette Rechenlast für das Entschlüsseln der VPN-Verbindungen übernimmt.

L2TP-VPN – gratis in Windows

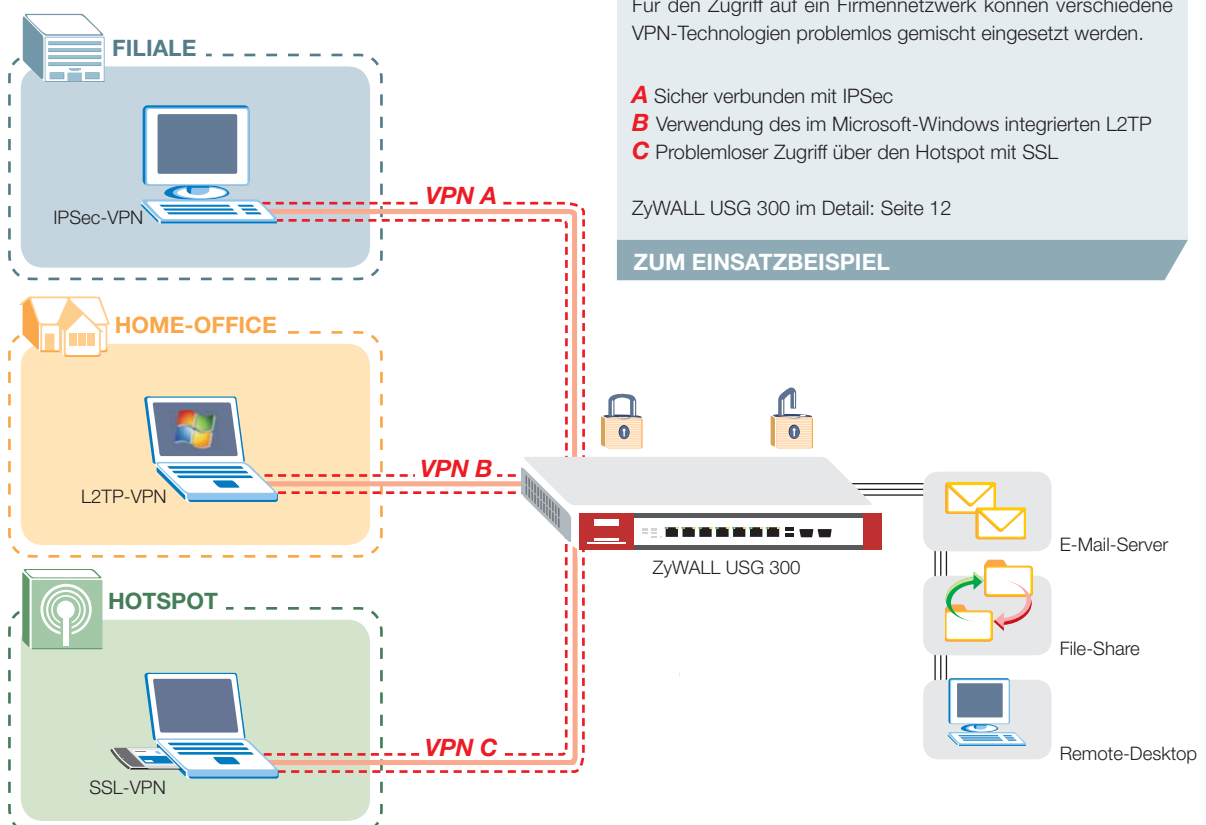
Windows-Benutzer verwenden am einfachsten den L2TP-Service, der bereits im Betriebssystem integriert ist. Der Kauf und die Installation einer zusätzlichen Software sind somit bei L2TP hinfällig.

SSL-VPN – mobil flexibel

Ist ein schneller Zugang ohne Konfiguration auf dem Notebook oder über Smartphones gewünscht, ist SSL-VPN die erste Wahl. Mobile Benutzer, die in öffentlichen Internet-Cafés oder auf dem Flughafen auf Firmenressourcen zugreifen wollen, stellen lediglich eine Verbindung per Browser her, und schon können sie flexibel und schnell die gewünschten Informationen abrufen. Auch für Geschäftspartner und Kunden muss ein Zugriff einfach und ohne Konfigurationsaufwand möglich sein. SSL-VPN bietet hierfür die ideale Lösung.

ZyWALL USG mit Hybrid-VPN

Die richtige Wahl der Remote-Verbindung hängt von den Bedürfnissen des Nutzers ab – Hybrid-VPN, wie sie von den ZyWALL USG angeboten wird, ist daher die ideale Möglichkeit, sicher und flexibel alle Anforderungen abzudecken.





Doppelte Zugriffssicherheit

Unsicherheitsfaktor Mensch

Passwörter werden mit Post-its an den Bildschirm geklebt oder leichtfertig Kollegen mitgeteilt. In stets weiterentwickelten Sicherheitssystemen bleibt der Mensch ein ständiger Gefahrenfaktor. Mit einer zusätzlichen Token-Authentifizierung lässt sich der Schutz wirksam erhöhen. Es reicht nicht mehr, nur Username und Passwort einzutippen. Zusätzlich muss eine vom Token generierte 6-stellige Nummer (One-time-password/OTP) eingegeben werden.

2-Faktoren-Authentifizierung

Da die Token-Nummer bei jedem Anmeldevorgang neu generiert wird, muss ein potenzieller Eindringling nebst Username und Passwort im Besitz des Tokens sein, um sich einloggen zu können. Ähnlich wie beim E-Banking mit Streichlisten sind also zwei Faktoren zur Identifikation notwendig. Zuerst wird das Passwort eingegeben, danach die jeweils neu generierte Nummer des Tokens. Die Sicherheit wird deutlich verbessert und das Gefahrenrisiko durch Unachtsamkeit der Mitarbeiter reduziert.

Token für SSL-VPN

Bei SSL-VPN besteht theoretisch das grösste Risiko darin, dass ein Zugriff missbraucht wird. SSL-VPN kommt ohne Client-Software aus. So erfolgt der Zugriff auf die Daten oft aus einem Internet-Café oder von einem anderen öffentlichen PC. Da ist es schnell möglich, dass eine Passwortheingabe vom Browser gespeichert und danach von Dritten abgerufen wird. Ebenfalls lässt sich die Passwortheingabe von einem im Hintergrund installierten Keylogger einfach protokollieren.



Auch dieses Problem lässt sich mit einer 2-stufigen Authentifizierung lösen: Die ZyXEL Token sind für den Einsatz mit SSL-VPN der ZyWALL USG oder SSL 10 ausgelegt.

«OTP-Server-Software»

Die Authentifizierungs-Software lässt sich auf einem bestehenden Windows 2000/2003-Server installieren. Einzige Anforderung an den Server: es läuft kein weiterer RADIUS-Dienst darauf.

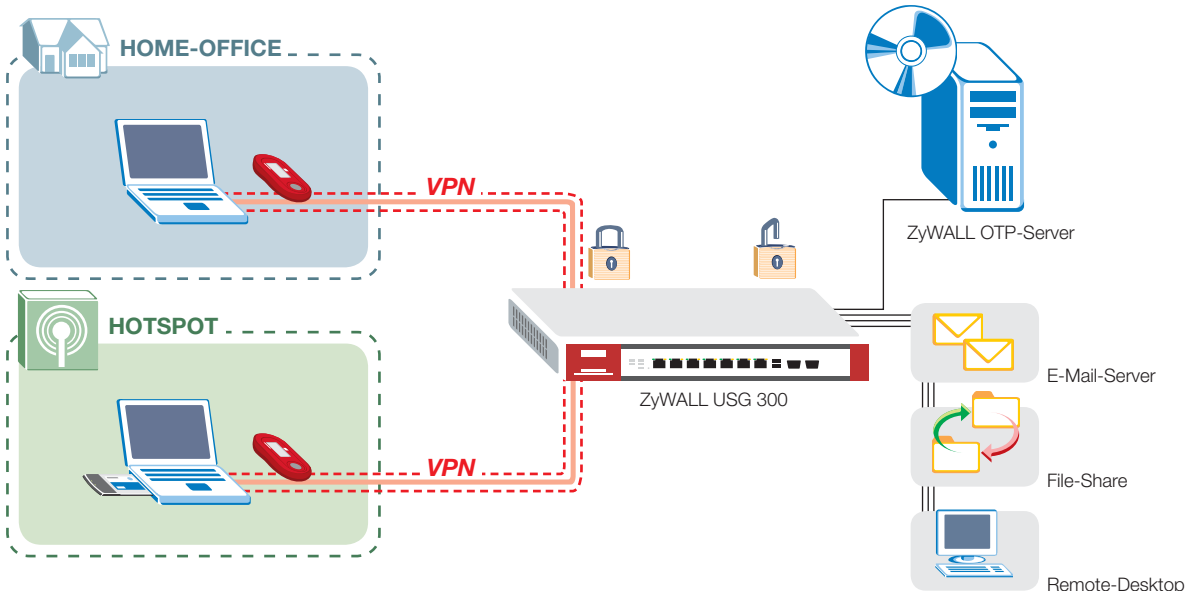
Netzwerk mit SSL nachrüsten

Bei bestehenden Firewalls mit UTM-Services kann die SSL-Terminierung mit dem Einsatz einer ZyWALL SSL 10 nachgerüstet werden.

Sicherer Remote-Zugriff über SSL-VPN mit Token und UTM-Schutz: Ein Angreifer bräuchte zusätzlich zu Benutzernamen und Passwort den entsprechenden Token, um ins Netzwerk einzudringen. Ereignisgesteuert (per Tastendruck) wird ein sechsstelliger PIN sichtbar. Jeder Token ist einem bestimmten User zugewiesen.

ZyWALL USG 300 im Detail: Seite 12

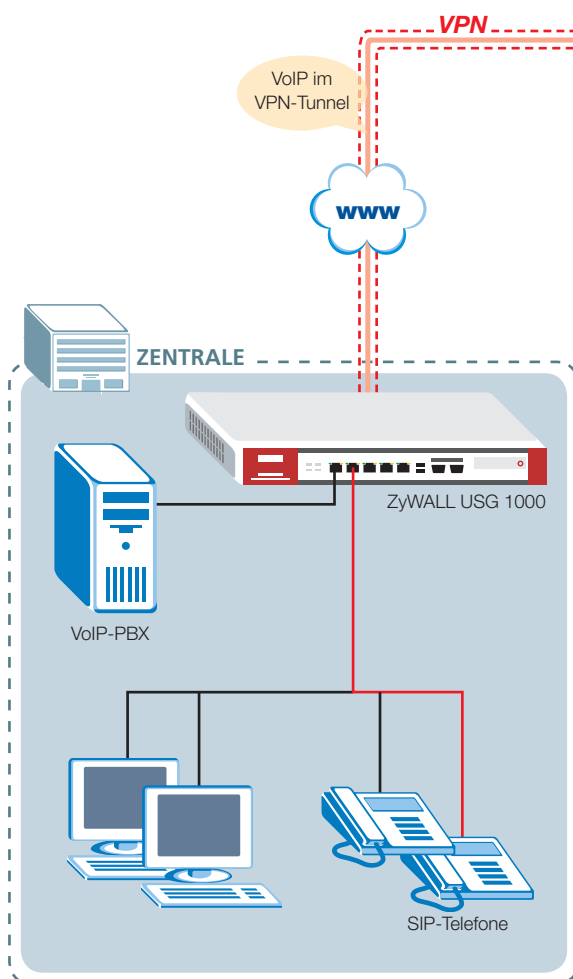
ZUM EINSATZBEISPIEL



Geschützte IP-Telefonie (VoIP)

Komplexe Vernetzungen

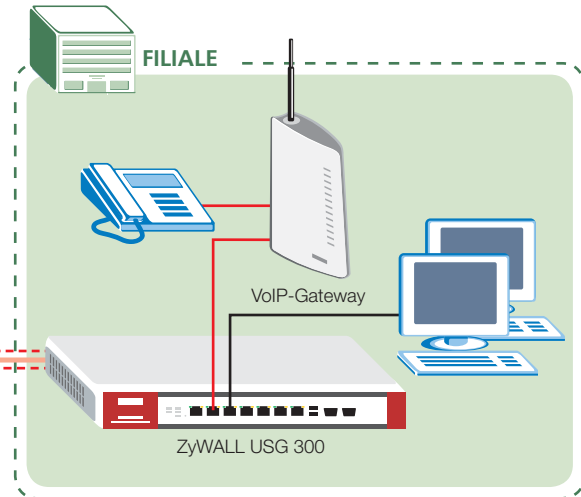
Mit der Globalisierung nimmt die Vernetzung stetig zu. Auch kleine und mittelständische Unternehmen müssen Schritt halten: Es gilt, Filialen sicher zu erschliessen und den Verkaufsstellen jederzeit eine sichere Verbindung zum zentralen Firmen-Netzwerk zu garantieren.



ZUM EINSATZBEISPIEL

Viele Unternehmen setzen VoIP für die Kommunikation ein. Mit VPN-Tunnels findet die Übermittlung von Daten (inkl. VoIP) mit/zwischen Filialen in einem geschützten Umfeld statt.

ZyWALL USG 300 / USG 1000 im Detail: Seite 12



Daten und VoIP geschützt im IPSec-VPN-Tunnel

Viele Firmen nutzen VoIP, um die Gesprächskosten mit Filialen oder Partnerfirmen zu senken. Um die Gesprächsdaten vor Angreifern zu schützen, wird VoIP auf der öffentlichen Strecke in einem VPN-Tunnel verpackt. IPSec als VPN-Technologie bewährt sich für das Verbinden von ganzen Netzwerken.

Schnell trotz Verschlüsselung

Auch der Datenaustausch über die VPN-Firewalls ist durch Verschlüsselung wirksam geschützt und bietet einen hervorragenden Datendurchsatz bei höchster Verfügbarkeit. Eine einfache, intuitive Verwaltung der Geräte ermöglicht Mitarbeitern in Niederlassungen und im Aussendienst einen schnellen Zugriff auf Informationen im zentralen Netzwerk.

VoIP – Trend und Gefahr

Voice-over-IP ist in aller Munde. Laut dem Marktforschungsunternehmen Gartner werden bis 2008 über 90 % aller neuen Telefonzentralen auf der VoIP-Technologie basieren. Die zunehmende Verbreitung von VoIP ist für Hacker und Cracker eine grosse Verlockung. Mit so genannten «Man-in-the-Middle»-Attacken werden VoIP-Pakete mit Hilfe von im Internet verfügbaren Tools auf fremde Rechner umgeleitet und dort als normale Audio-datei gespeichert. Weitere Gefahren sind beispielsweise Denial-of-Service-Attacken (DoS). Eine VPN-Verbindung macht ein solches Abhören unmöglich. Die ZyWALL USG-Serie unterstützt VoIP über VPN und sichert so die VoIP-Infrastruktur.

Gefahr Peer-to-Peer-Applikationen

Wo lauern Gefahren?

Diverse Statistiken zeigen, dass viele Angriffe durch den sorglosen Umgang der User mit Programmen resp. das Surfverhalten ausgelöst werden. Während E-Mail- und FTP-Verkehr in der Regel auf sicherheitsrelevante Aspekte überprüft werden, ist das bei Peer-to-Peer (P2P) oder Instant-Messaging (IM) meist nicht der Fall. Wie behält der IT-Administrator die zentrale Kontrolle über die elektronische Kommunikation im Firmennetzwerk?

20 % verwenden Peer-to-Peer

Eine zentrale Überwachung der elektronischen Kommunikation gehört ins Pflichtenheft eines IT-Administrators. Viele Netzwerkadministratoren sind nicht sicher, ob in ihrem Netzwerk IM (Skype, GoogleTalk, MSN) und P2P wie BitTorrent oder FastTrack verwendet werden. Und die wenigsten von ihnen verfügen über ein Tool, um dies zu kontrollieren, geschweige denn, um die Gefahren abzuwenden.

Alles oder nichts... oder IDP!

«MSN-Chat wird bei uns hauptsächlich für den Informationsaustausch mit Geschäftspartnern verwendet», antworteten viele KMUs in einer telefonischen Befragung. Werden MSN oder Skype im Netzwerk toleriert, ist ein generelles Ausmerzen der P2P-Gefahren nicht möglich. Sinnvoll ist in diesem Fall ein System, das benutzerorientiert eine Anwendung zulässt oder blockiert. Zudem wird oft gewünscht, eine maximale Bandbreite und ein Zeitfenster festlegen zu können.

Application-Patrol

Durch die entsprechenden IDP-Signaturen lässt sich für gewisse Benutzer problemlos das Chatten erlauben und z. B. der File-Transfer mit MSN sperren. Das umfassende Tool «Application-Patrol» innerhalb des IDP-Dienstes ermöglicht die benutzerspezifische Konfiguration, das heisst, wer was und wann mit welcher Bandbreite ausführen darf.

Signaturen aktualisieren!

Potenzielle Schwachpunkte, Angriffe und Anwendungen verändern sich stetig. Eine nachhaltige Kontrolle ist deshalb nur mit einem aktiven IDP-Service und aktualisierten Signaturen möglich.

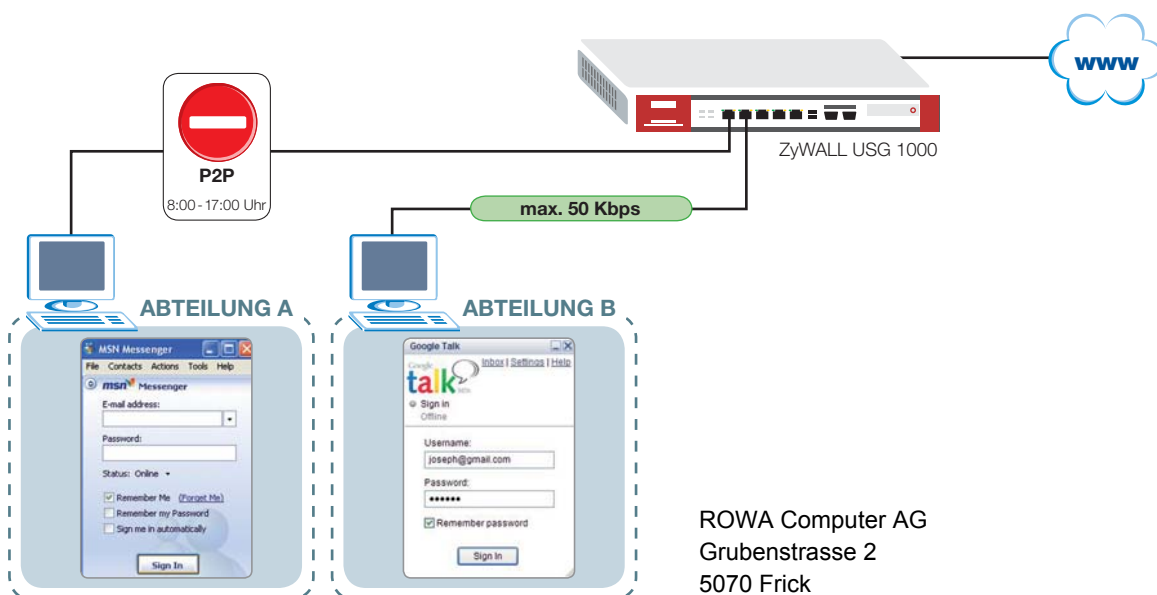
IDP ergänzt Anti-Virus

IDP erkennt resp. verhindert die Aktivität und Auswirkung von Viren und Trojanern. Besser wäre aber, die Schädlinge bereits durch eine wirkungsvolle Anti-Virus-Lösung am Gateway zu vernichten. Sicherheitsexperten empfehlen deshalb einen kombinierten Einsatz von Anti-Virus und IDP in der Firewall.

Benutzerspezifische Konfiguration von Application-Patrol:
Abteilung A darf MSN-Chat zwischen 8 und 17 Uhr nicht verwenden, MSN-File-Transfer ist jedoch erlaubt; Abteilung B kann GoogleTalk verwenden, erhält aber eine limitierte Bandbreite von 50 Kbps.

ZyWALL USG 1000 im Detail: Seite 12

ZUM EINSATZBEISPIEL



ROWA Computer AG
Grubenstrasse 2
5070 Frick
Tel. 062 865 20 21 - Fax 062 865 20 30
info@rowa.ch - www.rowa.ch

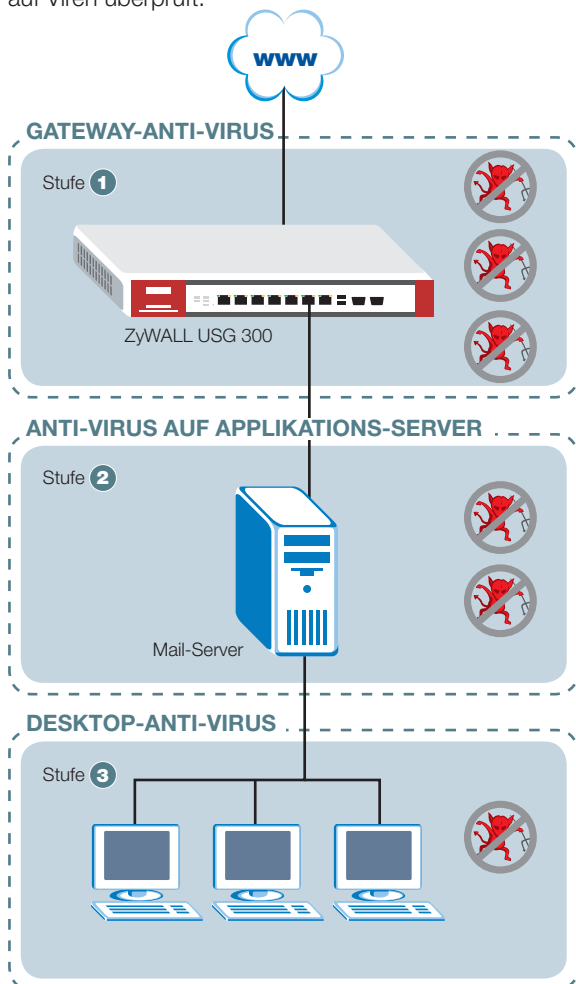
Dreistufige Viren-Bekämpfung

Mehrstufiger Anti-Viren-Schutz

Teleworker oder mobile Benutzer verwenden oft private und dadurch schlecht kontrollierbare Hardware für den Zugriff auf Firmen-Ressourcen. Um die Nutzer im Netzwerk möglichst effizient vor Virenbefall zu schützen, ist eine mehrstufige Sicherheit notwendig. Daten werden an verschiedenen Stellen überprüft.

1 Gateway-Anti-Virus

Die Anti-Viren-Funktion der ZyWALL USG überprüft den Datenverkehr an der Pforte zum Internet. Inspiziert werden folgende Protokollarten: FTP, HTTP, SMTP, POP3, IMAP4. Auch der Datenfluss in einem VPN-Tunnel wird auf Viren überprüft.



ZUM EINSATZBEISPIEL

3-stufiger AV-Schutz: Je früher die Gefahren abgewehrt werden, desto effektiver. Am besten ist es immer, einen Schädling vor Eintritt ins Netzwerk abzufangen.

ZyWALL USG 300 im Detail: Seite 12

2 Anti-Virus auf Applikations-Server

Die auf Server-Ebene installierte Anti-Viren-Software überprüft alle File-Zugriffe sowie den ein- und ausgehenden E-Mail-Verkehr.

3 Desktop-Anti-Virus

Ein aktueller Anti-Viren-Schutz auf dem Arbeitsplatzrechner darf nicht fehlen! Über einen USB-Stick oder eine CD gelangt ein Virus sonst schnell ins Netzwerk.

Wie funktioniert Viren-Inspektion?

Firewall-Hersteller führen die Viren-Inspektion auf unterschiedliche Weise durch. Die grossen Vorteile der ZyXEL Gateway-Anti-Virenlösung sind:

- Keine Limitierung von Filegrößen

Die Datenpakete werden einer «Streaming-based-Inspection» unterzogen, also einer Untersuchung in Echtzeit. Dadurch gibt es keine Einschränkungen der Dateigrößen resp. Delays bei grossen Files.

- Untersuchung FTP, HTTP, SMTP, POP3, IMAP4

Die Lösung beschränkt sich nicht nur auf die Bekämpfung per E-Mail eingeschleuster Viren. Durch die Untersuchung weiterer Zugriffsarten wie HTTP oder FTP kann ein umfassenderer Schutz gewährt werden.

- Kein Problem mit komprimierten Files

Damit auch komprimierte Dateien auf Viren untersucht werden, findet der Signaturenvergleich ebenfalls in folgenden File-Typen statt: zip, gzip, pkzip und rar.

Virus entdeckt, was nun?

Entspricht ein untersuchtes Datenpaket dem Muster einer Anti-Viren-Signatur, wird die infizierte Stelle überschrieben und das File somit unschädlich gemacht. Der Administrator wird per E-Mail benachrichtigt. Ebenso kann der Benutzer via Windows-Nachrichtendienst informiert werden. Im Web-GUI der Firewall ist aufgelistet, welche Viren, Würmer oder Trojaner das System vernichtet hat. Zur besseren Übersicht sind auf der Statusseite das Total und die fünf Top-Viren aufgeführt.

Lassen sich mp3-Files blockieren?

Ja, denn in White-/Blacklisten lassen sich bestimmte Dateinamen oder -typen definieren, die am Gateway gesperrt oder zugelassen werden sollen. Selbstverständlich ist diese Überprüfung zwischen allen Sicherheitszonen möglich.

Freies oder sicheres Surfen?

Surfen kann gefährlich sein!

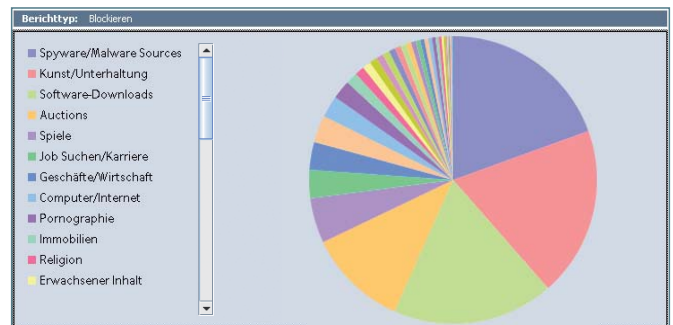
Statistiken zeigen, dass 25 % der Befragten während der Arbeitszeit Peer-to-Peer-(P2P)-Portale besuchen. Durch die unkontrollierte Nutzung von P2P-Software besteht die Gefahr, sich Viren, Würmer und schadhafte Programme ins Netzwerk zu holen. Unternehmensrichtlinien zur Internetnutzung erhöhen zwar das Bewusstsein über mögliche Gefahren, können diese aber nicht verhindern. Content-Filter, die einen Basischutz bieten, werden in weniger als 50 % aller Unternehmen eingesetzt.

Logging vor Blocking

Anstatt den Internetzugang von Anfang an einzuschränken, lassen sich die Zugriffe auch über einen bestimmten Zeitraum aufzeichnen. Ein übersichtlicher Report bildet danach die Entscheidungsgrundlage, welche nicht geschäftsrelevanten Kategorien und Seiten gesperrt werden sollen. Kategorien, die von Firmen immer wieder gesperrt werden, sind z. B. Spyware-verseuchte oder pornografische Seiten.

Arbeitgeber trägt Verantwortung!

Die Regeln bezüglich privater Internetnutzung in Firmen sind unterschiedlich. Viele Unternehmen kümmern sich nur unzureichend um das Surfverhalten ihrer Mitarbeiter. Arbeitgeber mit Lehrlingen tragen dabei eine besonders grosse Verantwortung. Objektiv betrachtet, gibt es einige Webseiten, die nicht im Interesse einer Firma sind – sei es aus geschäftsrelevanten oder Sicherheitsgründen.



Grafische Auswertung aller blockierten Seiten in einem Schweizer KMU.

Produktivität steigern

Ein richtig eingesetzter Content-Filter hat direkten Einfluss auf die Produktivität der Mitarbeiter und wird sich innert kürzester Zeit auszahlen. Mit den neuen ZyWALL USG-Modellen lassen sich Kategorien dauerhaft oder während der Arbeitszeiten blockieren. So kann nach Arbeitsschluss wieder privat gesurft werden.

Klare Firmen-Richtlinien

Bei der Internetnutzung durch Private und Firmen gilt es immer, auch rechtliche Aspekte zu beachten. Unsachgemässe Internetnutzung kann für die Unternehmensleitung juristische Konsequenzen mit sich bringen. Im Dokument «Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz» des eidgenössischen Datenschutzbeauftragten sind nähere Informationen über die rechtlichen Pflichten des Arbeitgebers ersichtlich.

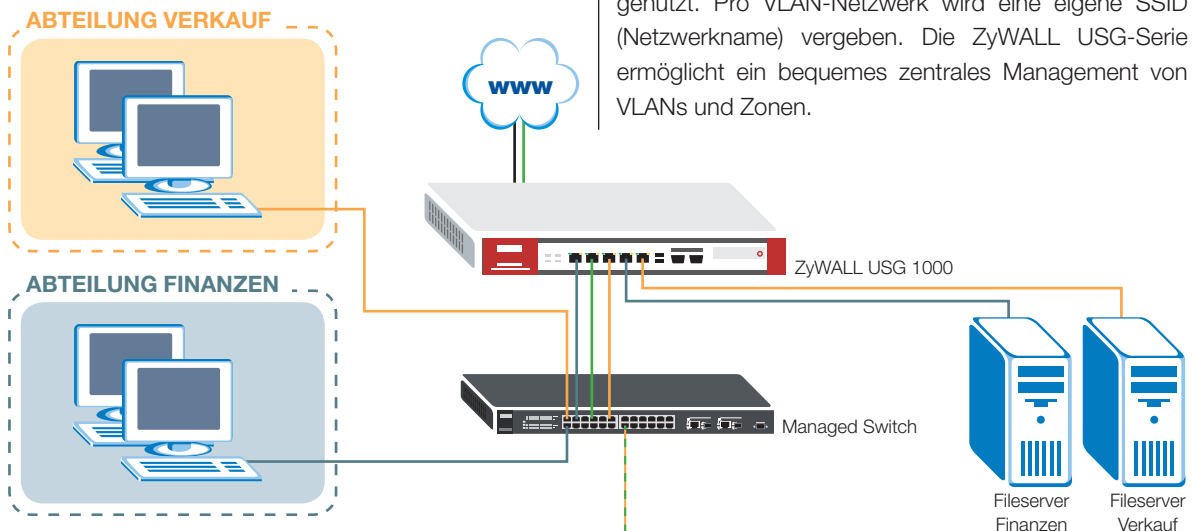
<input checked="" type="checkbox"/> Adult/Mature Content	<input checked="" type="checkbox"/> Pornography	<input checked="" type="checkbox"/> Sex Education
<input checked="" type="checkbox"/> Intimate Apparel/Swimsuit	<input checked="" type="checkbox"/> Nudity	<input checked="" type="checkbox"/> Alcohol/Tobacco
<input checked="" type="checkbox"/> Illegal/Questionable	<input checked="" type="checkbox"/> Gambling	<input checked="" type="checkbox"/> Violence/Hate/Racism
<input checked="" type="checkbox"/> Weapons	<input type="checkbox"/> Abortion	<input checked="" type="checkbox"/> Hacking
<input checked="" type="checkbox"/> Phishing	<input type="checkbox"/> Arts/Entertainment	<input type="checkbox"/> Business/Economy
<input checked="" type="checkbox"/> Alternative Spirituality/Occult	<input checked="" type="checkbox"/> Illegal Drugs	<input type="checkbox"/> Education
<input type="checkbox"/> Cultural/Charitable Organizations	<input type="checkbox"/> Financial Services	<input checked="" type="checkbox"/> Brokerage/Trading
<input checked="" type="checkbox"/> Online Games	<input type="checkbox"/> Government/Legal	<input checked="" type="checkbox"/> Military
<input type="checkbox"/> Political/Activist Groups	<input type="checkbox"/> Health	<input type="checkbox"/> Computers/Internet
<input type="checkbox"/> Search Engines/Portals	<input checked="" type="checkbox"/> Spyware/Malware Sources	<input checked="" type="checkbox"/> Spyware Effects/Privacy Concerns
<input type="checkbox"/> Job Search/Careers	<input type="checkbox"/> News/Media	<input type="checkbox"/> Personals/Dating
<input type="checkbox"/> Reference	<input type="checkbox"/> Open Image/Media Search	<input type="checkbox"/> Chat/Instant Messaging
<input type="checkbox"/> Email	<input type="checkbox"/> Blogs/NewsGroups	<input type="checkbox"/> Religion
<input type="checkbox"/> Social Networking	<input type="checkbox"/> Online Storage	<input type="checkbox"/> Remote Access Tools
<input type="checkbox"/> Shopping	<input checked="" type="checkbox"/> Auctions	<input type="checkbox"/> Real Estate
<input type="checkbox"/> Society/Lifestyle	<input type="checkbox"/> Sexuality/Alternative Lifestyles	<input type="checkbox"/> Restaurants/Dining/Food
<input type="checkbox"/> Sports/Recreation/Hobbies	<input type="checkbox"/> Travel	<input type="checkbox"/> Vehicles
<input type="checkbox"/> Humor/Jokes	<input type="checkbox"/> Software Downloads	<input checked="" type="checkbox"/> Pay to Surf
<input checked="" type="checkbox"/> Peer-to-Peer	<input type="checkbox"/> Streaming Media/MP3s	<input checked="" type="checkbox"/> Proxy Avoidance
<input type="checkbox"/> For Kids	<input type="checkbox"/> Web Advertisements	<input type="checkbox"/> Web Hosting

Mit dem ZyXEL Content-Filter lässt sich Internetverkehr einfach kontrollieren. Dabei stehen 60 Kategorien zur Auswahl.

Netzwerkzonen einrichten

Gefahren durch zentrale LAN-Zone

In KMUs sind die unterschiedlichen Abteilungen über ein Netzwerk verbunden. Oft befinden sich alle Benutzer in derselben LAN-Zone. Dadurch lassen sich keine benutzerspezifischen Richtlinien definieren, und alle User kommunizieren direkt miteinander. Die Abschottung einzelner Abteilungen resp. vertraulicher Daten ist nicht möglich. Im schlimmsten Fall erfolgt ein unbefugter Zugriff von Mitarbeitern auf den PC der Finanzabteilung oder auf andere Ressourcen. Ist zudem ein Rechner infiziert, so ist in kürzester Zeit das ganze Netzwerk davon betroffen.



Segmente schaffen Überblick

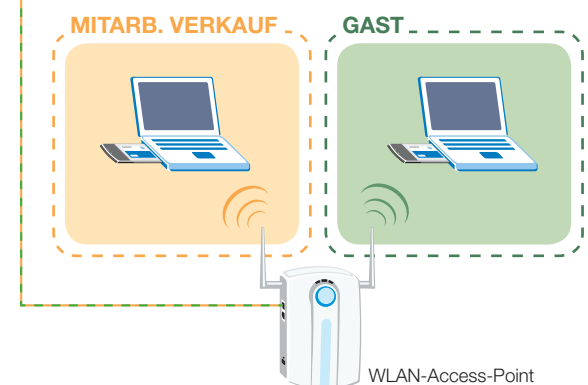
Eine moderne Infrastruktur sollte Abteilungen durch verschiedene Zonen (VLANs – virtuelle LANs) trennen. Dies erhöht die Sicherheit innerhalb der Firma und ermöglicht die schnellere Eingrenzung bei Fehlern. Mit der neuen USG-Serie von ZyXEL lassen sich zentral auf der Firewall mehrere Benutzergruppen mittels VLANs einfach definieren.

Eigenständige Sicherheitszonen

Auf allen USG-Firewalls sind mehrere Sicherheitszonen individuell konfigurierbar. So kann zum Beispiel pro Abteilung und File-/Mailserver eine eigene Firewall-Zone (Sicherheitszone) definiert werden. Dank eines objektorientierten Konfigurationskonzepts lassen sich die vorgängig aufgesetzten VLANs (Abteilungen) den einzelnen Zonen zuweisen. Zum Schluss muss noch die Sicherheits-Policy für die Zonen definiert werden. Damit sind spezifische Sicherheitsrichtlinien pro Abteilung und sogar pro Benutzer möglich.

Segmentierung von WLAN-Benutzern

Firmen stellen das WLAN in der Regel nicht nur ihren Mitarbeitern zur Verfügung. Auch die Gäste erhalten in Sitzungszimmern den drahtlosen Zugriff auf das Internet. Die beiden Benutzergruppen erfordern jedoch unterschiedliche Sicherheitseinstellungen in Bezug auf den Ressourcen-Zugriff. Während Mitarbeiter beim Zugriff auf interne Server eine verschlüsselte WLAN-Verbindung benötigen, muss sichergestellt werden, dass Gäste von der internen IT-Welt abgetrennt sind. Mittels VLAN lassen sich über einen Access-Point gleich beide Benutzergruppen bedienen. Dazu wird beim Access-Point (z. B. NWA-3x00-Serie) die Multi-SSID-Funktion genutzt. Pro VLAN-Netzwerk wird eine eigene SSID (Netzwerkname) vergeben. Die ZyWALL USG-Serie ermöglicht ein bequemes zentrales Management von VLANs und Zonen.



ZUM EINSATZBEISPIEL

Unterschiedliche Benutzergruppen mit eigenen Sicherheitsprofilen werden zentral verwaltet. Der Switch unterstützt Tag- und Port-based VLANs. Gäste erhalten nur den Zugriff aufs Internet.

ZyWALL USG 1000 im Detail: Seite 12

Ausfallsicherheit garantiert

Verfügbarkeit Zentrale

Es besteht ein Trend zur Zentralisierung von Systemen. Dabei wird für Unternehmen die Systemverfügbarkeit am Hauptsitz überlebenswichtig. Denn ganze Aussenstellen oder alle Heim-Arbeitsplätze sind handlungsunfähig, wenn die IP-Sec-VPN-Verbindung zum Firmennetzwerk unterbrochen wird. Viele Firmen setzen zentrale ERP-/CRM-Systeme ein, die höchste Verfügbarkeit beanspruchen.

Backup über zweiten WAN-Port

Ein zweiter WAN-Port mit entsprechender zusätzlicher VPN-Regel erhöht die Verfügbarkeit erheblich. Um die Ausfallsicherheit bei einem Internet-Provider abzusichern, bindet man den zweiten WAN-Port am besten bei einem anderen Provider an. Ausserdem minimieren zwei unterschiedliche Zugangstechnologien (xDSL, Kabel, Standleitung) das Ausfallrisiko zusätzlich. Ist eine Verbindung unterbrochen, werden die VPN-Tunnels automatisch über den zweiten WAN-Port aufgebaut. Bei Bedarf lässt sich die Last des ausgehenden Datenverkehrs auf die verschiedenen WAN-Verbindungen verteilen und somit die Bandbreite vergrössern.

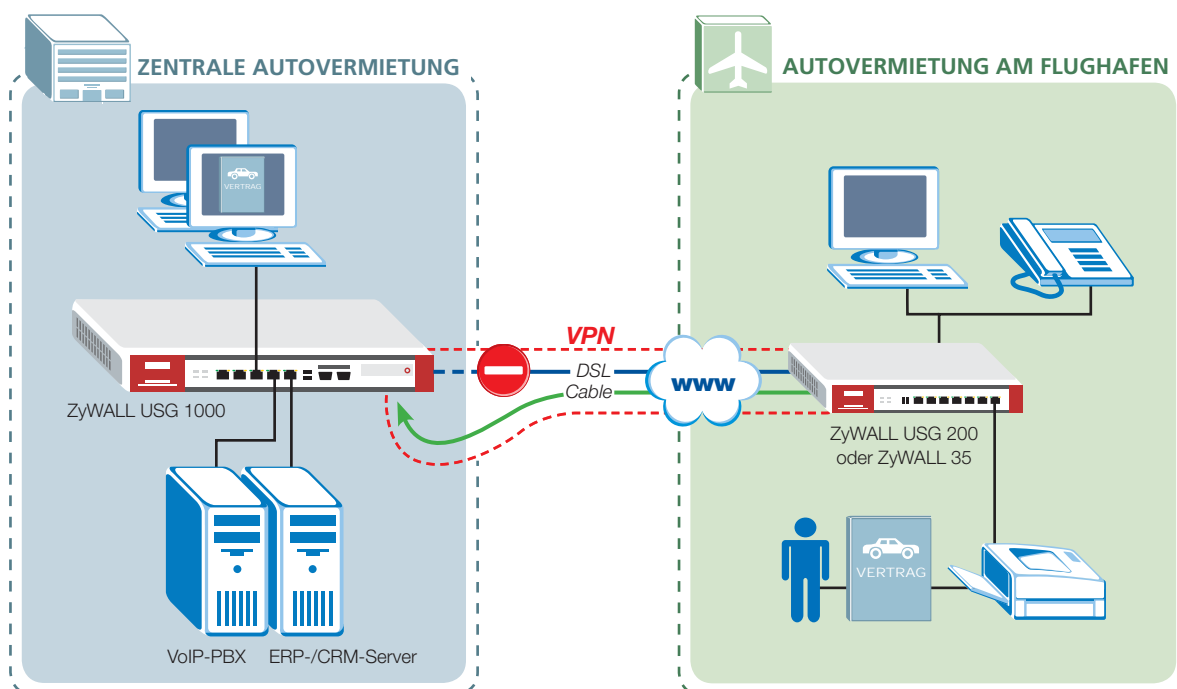
Ausfallsicherheit Hardware

Die Hardware-Funktion High-Availability (HA) stellt die Internetverbindung auch beim Ausfall einer Firewall sicher. Als Backup wird eine zweite Firewall im Hot-Standby-Modus parallel zur ersten Firewall aufgesetzt. Die Konfiguration zwischen den beiden Firewalls wird automatisch in regelmässigen Abständen abgeglichen. Fällt die erste Firewall aus, übernimmt sofort die zweite die Gateway-Funktion.

Ein Internetausfall kann ganze Unternehmensprozesse lahm legen und verheerende Konsequenzen nach sich ziehen. Dieses Beispiel zeigt, dass dank redundant ausgelegtem VPN-Zugriff die Mietverträge am Flughafen ausgedruckt werden können, auch bei einem Ausfall der DSL-Verbindung im Hauptsitz.

ZyWALL USG 1000 / USG 200 im Detail: Seite 12 und 13

ZUM EINSATZBEISPIEL





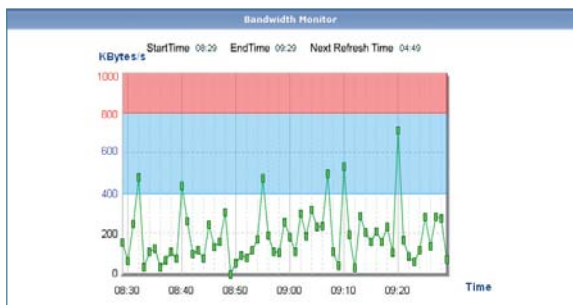
Security ist Chefsache

Netzwerk im Griff

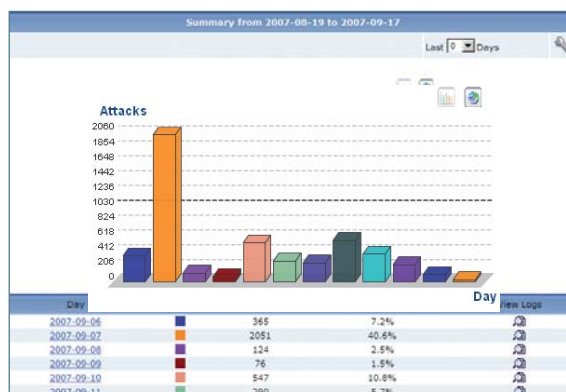
Die Sicherheit ist zu wichtig, als dass sie delegiert werden kann. Eine regelmässige Auswertung der Ereignisse im Netzwerk ist unabdingbar. Ein solcher Report sollte übersichtlich sein und die für eine Firma wichtigsten Kennzahlen enthalten. Dazu gehören Netzwerkzustand, Bandbreitenbedarf nach Anwendung oder IP-Adresse, Angriffe, erkannte Viren, Kategorien der aufgerufenen Websites etc.

Effizientes Reporting-System

ZyXEL Vantage Report (VRPT) ist ein Web-basiertes, zentralisiertes Reporting-System für das schnelle Sammeln und Analysieren von Informationen innerhalb eines verteilten Netzwerks. Zudem ermöglicht VRPT dem Systemadministratoren, eine oder mehrere ZyWALL-Firewalls zu überwachen. Die voreingestellten Syslog-Analysemechanismen liefern einen schnellen Überblick über den Netzwerkzustand. Der Standort des Reporting-Servers kann im Firmennetzwerk oder extern beim System-Integrator sein.



Auf einen Blick zeigt die Übersichtsseite die aktuelle Netzwerkbelastung.



Wie häufig wurde das Netzwerk in den letzten Tagen attackiert? Per Mausclick bietet VRPT nähere Angaben zum Angriffs-Typ und woher er gestartet wurde.

Sicherheitseinstellungen up-to-date

Umstellungen im Netzwerk, z. B. mit neuen Servern, erfordern meistens eine Anpassung der Sicherheitseinstellungen. Dazu benötigt man die gesammelten Informationen des Reports über Netzwerkzugriffe, VPN-Verkehr zwischen Standorten, Bandbreitennutzung und Angriffe etc. Die gewünschten Reports werden automatisch im HTML- oder PDF-Format via E-Mail zugestellt. Die Häufigkeit und der Empfängerkreis sind frei definierbar.

Analyse des Datenverkehrs

Der Report deckt unsachgemässe Internetnutzungen auf. Ebenfalls erkennt er zeitraubende oder bandbreitenintensive Aktivitäten. Dies bietet dem Systemadministratoren sowie der Geschäftsleitung den schnellen Überblick über die wichtigsten Vorgänge im Netzwerk.

INFO



Vorteile Vantage Reporting:

- umfassende grafische Auswertungen per E-Mail
- Web-basierte Benutzerschnittstelle
- Multi-ZyWALL-Unterstützung für Filialen oder mehrere Kunden
- einfache Handhabung

Produkte im Detail

ZyXEL ZyWALL USG 300 Unified-Security-Gateway bis 75 User

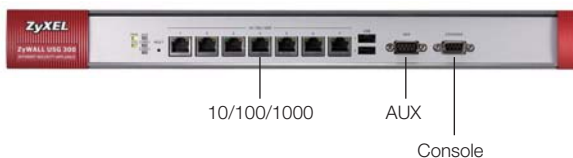


Einsatzgebiet

Die ZyWALL USG 300 bietet umfassenden Schutz für kleine und mittlere Unternehmen bis 75 Benutzer. Dank der objektorientierten Konfiguration kann der IT-Administrator die Sicherheit im Netzwerk bis auf Benutzer-Ebene festlegen. Die integrierten VPN-Technologien (IPSec, SSL, L2TP) ermöglichen eine flexible Einbindung von Remote-Usern an verschiedenen Standorten.

Spezielle Funktionen

Mit bis zu 100 Mbps VPN-Durchsatz ist sie als Zentrale für die Anbindung eines Filialnetzes ausgelegt. Die Unterstützung von mehreren WAN-Ports als Verbindungs-Backup und das WAN-Load-Balancing erlauben eine zuverlässige Internetanbindung. Die Hardware-High-Availability ermöglicht die Installation einer zweiten ZyWALL USG 300 zur Sicherstellung der Redundanz.



Features ZyXEL ZyWALL USG 300

- Hybrid-VPN (IPSec, SSL, L2TP)
- umfassende Gefahren-Abwehr (AV/IDP/CF)
- IM-/P2P-Management
- flexible Security-Zonen
- benutzerspezifisches Regelwerk
- Bandbreiten-Management
- High-Availability
- Artikel: 3303
- Referenzpreis: CHF 2'420.–

ZyXEL ZyWALL USG 1000 Unified-Security-Gateway bis 200 User

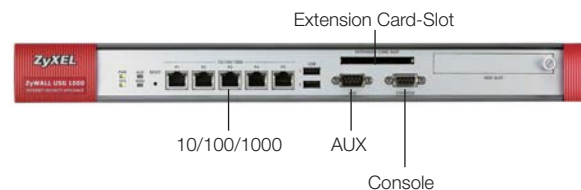


Einsatzgebiet

Die ZyWALL USG 1000 bietet eine umfassende Palette von Sicherheitservices auf einer robusten, leistungsfähigen Plattform. Sie ist für mittlere Unternehmen bis zu 200 Mitarbeiter ausgelegt. Dank des hohen Durchsatzes für Firewall, VPN und UTM ist die Datenprüfung auch zwischen den verschiedenen internen Sicherheitszonen möglich.

Spezielle Funktionen

Die Einbindung von Remote-Usern an unterschiedlichen Standorten ermöglicht ein integriertes IPSec-, L2TP- und SSL-VPN. Mit dem hochleistungsfähigen VPN-Konzentrator können auch grosse VPN-Netzwerke problemlos verknüpft werden. Die VPN-Funktion «Hub and Spoke» reduziert den Administrationsaufwand in komplexen Multi-Site-Konstellationen. Die ZyWALL USG 1000 verwaltet bis zu 200'000 gleichzeitige NAT-Sessions und hält damit grösstem Ansturm stand.



Features ZyXEL ZyWALL USG 1000

- hochleistungsfähiger VPN-Konzentrator
- Hybrid-VPN (IPSec, SSL, L2TP)
- umfassende Gefahren-Abwehr (AV/IDP/CF)
- IM-/P2P-Management
- benutzerspezifisches Regelwerk
- Bandbreiten-Management
- High-Availability
- Artikel: 3304
- Referenzpreis: CHF 5'340.–

ZyXEL ZyWALL USG 100
Unified-Security-Gateway bis 25 User



Die ZyWALL USG 100 findet ihren Einsatz in kleinen Unternehmen oder Aussenstellen mit bis zu 25 Benutzern. Als VPN-Technologien werden IPSec, L2TP und SSL unterstützt, was verschiedene Verbindungsoptionen ermöglicht. UTM-Dienste wie IDP/AV/CF schützen das Netzwerk umfassend. Mit zwei WAN-Ports kann dieses Modell redundant ans Internet angeschlossen werden.

Features ZyXEL ZyWALL USG 100

- Hybrid-VPN (IPSec, SSL, L2TP)
- Anti-Virus
- IDP/ADP
- Content-Filter
- Artikel: 3301
- verfügbar ab Q2/2008

ZyWALL USG 200
Unified-Security-Gateway bis 50 User



Die ZyWALL USG 200 schützt KMU-Netzwerke mit bis zu 50 Benutzern. Als VPN-Technologien werden IPSec, L2TP und SSL unterstützt, was verschiedene Verbindungsoptionen ermöglicht. Es lassen sich gleichzeitig bis maximal 10 SSL-VPN- und 100 IPSec-Verbindungen terminieren. UTM-Dienste wie IDP/AV/CF schützen das Netzwerk umfassend. Mit bis zu drei WAN-Ports kann dieses Modell redundant ans Internet angeschlossen werden.

Features ZyXEL ZyWALL USG 200

- Hybrid-VPN (IPSec, SSL, L2TP)
- Anti-Virus
- IDP/ADP
- Content-Filter
- Artikel: 3302
- verfügbar ab Q2/2008

NEU Objektorientierte Konfiguration

Die neue ZyWALL USG-Serie baut auf der objektorientierten Konfiguration auf. Alle Objekte werden nur einmal erfasst. Mit diesen Objekten wird danach das Regelwerk erstellt. Der grosse Vorteil dieser Lösung ist, dass die Objekte nur einmal an zentraler Stelle definiert werden müssen. Ändert sich ein Objekt, wird diese Änderung automatisch für alle erstellten Regeln übernommen.

Objekte:

- Benutzer/-Gruppen (lokal, RADIUS, LDAP, AD)
- IP-Adressen
- Services
- Zeitplan
- AAA-Server
- Auth. Methode
- Zertifikate
- ISP-Account
- SSL-Applikation

Neue ZyWALL USG-Serie

Funktionsübersicht



Features ZyXEL	ZyWALL USG 100	ZyWALL USG 200	ZyWALL USG 300	ZyWALL USG 1000
SPI-Firewall-Durchsatz (Mbps)	150	150	200	350
VPN-AES-Durchsatz (Mbps)	75	75	100	150
UTM-Durchsatz (Mbps)	24	24	48	100
max. IPSec-VPN	25	100	200	1'000
Concurrent Sessions	20'000	40'000	60'000	200'000
Concurrent SSL-VPN-Tunnel/s kostenlos	2	2	2	5
Concurrent SSL-VPN-Tunnel/s maximal	2	10	10	50
Ethernet-Ports (Zone konfigurierbar)	7 x 10/100/1000	7 x 10/100/1000	7 x 10/100/1000	5 x 10/100/1000
davon WAN-Ports	2	2 (plus 1 opt.)	frei konfigurierbar	frei konfigurierbar
VLAN-Support (802.1q)	✓	✓	✓	✓
objekt-/benutzer-orientierte Konfiguration	✓	✓	✓	✓
LDAP/RADIUS/MS AD	✓	✓	✓	✓
Hardware High-Availability	-	-	✓	✓
blockieren von Dateinamen/-typen wie MP3	✓	✓	✓	✓
Erweiterungslot 3G/WLAN	Q2/2008	Q2/2008	Q2/2008	Q2/2008
AV (HTTP, FTP, SMTP, POP3, IMAP4)	optional	optional	optional	optional
IDP/ADP	optional	optional	optional	optional
CF	optional	optional	optional	optional
Garantie (Jahre)	5	5	5	5
Artikel	3301	3302	3303	3304
Referenzpreis	verfügbar ab Q2/2008	verfügbar ab Q2/2008	CHF 2'420.–	CHF 5'340.–

Glossar

USG Unified-Security-Gateway («All-in-One»-Security-Lösung am Gateway).

Hybrid-VPN Verschiedene VPN-Technologien vereint (IPSec, L2TP, SSL), auf einem Gateway verfügbar.

HA (High-Availability) Hohe Verfügbarkeit durch Hardware-Redundanz.

P2P (Peer-to-Peer) Direkte Punkt-zu-Punkt-Verbindung zwischen zwei gleichgestellten Rechnern. P2P ist das Gegenteil von einem serverbasierten Netzwerk.

AV (Anti-Virus) Zonenbasierte Überprüfung des Datenverkehrs.

IDP (Intrusion-Prevention) Analysiert Dateninhalt bis ins Detail, erkennt netzwerkbasierende Angriffe.

ADP (Anomaly-Detection-Prevention) Anomalien bezüglich RFC-Standards. Abnormaler Datenverkehr (z. B. Port-Scan) wird erkannt und abgeblockt, schützt vor netzwerkbasierenden Angriffen.

CF (Content-Filter / Webfilter) Filter um z. B. illegale oder anstössige Webinhalte zu sperren.

VLAN (Virtual-Local-Area-Network, 802.1Q) Virtuell getrenntes Netzwerk zur Reduktion von Broadcast-Traffic und Steigerung der Zugriffssicherheit.

Application-Patrol Inspiziert und beendet bei Bedarf den Applikations-Typ durch Untersuchung des Payloads auf OSI-Layer 7 ohne Beachtung der Port-Nummer.

Application-Patrol auf der ZyWALL USG-Serie unterstützt:

1. generelle Protokolle wie HTTP, FTP, SMTP
2. Instant Messaging wie MSN, Yahoo Messenger, AOL-ICQ
3. P2P wie BT, eDonkey, Fasttrack, Gnutella
4. Streaming Protokolle – RTSP (Real-Time-Streaming-Protocol)



Bestehende ZyWALL-Modelle

Funktionsübersicht



Features ZyXEL	ZyWALL P1	ZyWALL 2 WG	ZyWALL 2 Plus
SPI-Firewall	✓	✓	✓
parallele IPSec-VPN-Session/s	1	5	5
LAN-Ports	1	4	4
WLAN	-	✓ 802.11a/b/g	-
3G-Option	-	✓	-
IDP	optional	-	-
AV	optional	-	-
CF	-	optional	optional
Artikel	2807	2808	2801
Referenzpreis	CHF 290.–	CHF 460.–	CHF 340.–

Ergänzende Lösungen



ZyXEL ZyWALL SSL 10	ZyXEL ZyWALL IPSec-VPN-Client	ZyXEL Authentication / User-Token
SSL-VPN-Appliance	VPN-Client-Software	2-Faktor-Authentifizierung mit Token
10 gleichzeitige SSL-Sessions	Windows 2000, XP, Vista	Server-Software
Erweiterbar auf 25 SSL-Sessions	Interoperabilität mit IPSec VPN-Gateways	Windows-Server 2000(SP3); 2003
Integration in LDAP, Active Directory, RADIUS, ZyXEL Authentication / User-Token	Mögliche Auslagerung der Konfiguration auf USB-Memory-Stick	Token mit 6-stelligem Einmalpasswort
Endpoint-Security	IPSec-VPN-Verschlüsselung DES/3DES/AES	Als Paket von 2, 5 und 10 Token erhältlich
Personalisiertes Web-Portal	Software mit 1, 5 und 10 Lizenz/en erhältlich	
Referenzpreis: CHF 560.–	Referenzpreis: ab CHF 95.–	Referenzpreis: ab CHF 140.–

Technische Dienstleistungen von Studerus Telecom:

	Reparaturservice innert 48 Stunden
	Support-Hotline Mo bis Fr, 8.30 bis 12.00 Uhr / 13.30 bis 19.00 Uhr
	Security-Kurse für IT-Professionals. Infos und Anmeldung unter www.studerus.ch/kurse

Express-Services

	Vorabaustausch-Service, Austauschgerät innert 4 Stunden		Onsite-Service, Servicetechniker innert 4 Stunden vor Ort Weitere Informationen zu den Express-Services: www.studerus.ch/express
--	---	--	--

ZyXEL

Vertretung für die Schweiz:

STUDERUS TELECOM

Studerus Telecom AG

Ringstrasse 1
8603 Schwerzenbach
info@studerus.ch
www.studerus.ch

ROWA Computer AG

Grubenstrasse 2

5070 Frick

Tel. 062 865 20 21 - Fax 062 865 20 30

info@rowa.ch - www.rowa.ch