ZYXEL

Intrusion Detection and Prevention (IDP) & Application Patrol

Security Service

Today's networks are under attack from an ever-expanding array of threats - viruses, malware, and other exploits. Hackers are increasingly adept at avoiding detection, and unlike with automated threats like viruses, the goal of these intrusions is often the theft of specific personal or financial information. For this reason, users need more reliable safeguards to protect private data.

Zyxel Intrusion Detection and Prevention (IDP) provides a high-performance deep packet inspection engine to examine all incoming and outgoing traffic - including SSL traffic - for protocol deviations, content that signals an attack, or policy violations. Zyxel IDP can operate in detection and prevention modes to defend operating systems and shield enterprise application vulnerabilities. Zyxel IDP protects web applications from application-layer attacks including SQL injection and cross-site scripting. Detailed events provide valuable information, including who attacked, when the attack occurred, and what the attacker attempted to exploit. Administrators can be automatically notified via alerts when an incident occurs.

Managing employees who waste too much time on non-work related applications can be a major challenge for businesses. Administrators face losing not only productivity, but network bandwidth to unrestricted Internet use. Zyxel Application Patrol - leverage Deep Packet Inspection module - controls employee network use and covers 19 categories of application, allowing businesses customize management protocols based on specific applications and behaviors.

IDP Benefits

Threat prevention with SSL inspection

Secure Sockets Layer (SSL) encryption has seen extensive worldwide proliferation, with many popular Web and cloud-based services like Dropbox and Gmail offering users the ability to have their entire sessions encrypted. Unfortunately, attackers are also turning to encryption to evade detection, increasing the prevalence of malicious activity. Enterprises now face the challenge of how to inspect incoming and outgoing traffic for threats under SSL encryption.

Virtual patching: Shields vulnerabilities before they can be exploited and eliminates the operational pains of emergency patching, frequent patch cycles, and costly system downtime

Cost-effective solution: Provides network-wide protection for all users configured behind firewall with a single IPS subscription

Granular and precise: Identifies and controls thousands of applications and its behavior

Flexibly bandwidth: Various control mode including Prioritize, BWM (bandwidth management), Block

SSL inspection is the key to protecting your network from these threats. Zyxel IDP service supports SSL inspection, helping to scan the content at a URL accessed over SSL to apply policies and detect malware and viruses at the URL level. This action blocks threats that are hidden in SSL encrypted connections and facilitates deeper policy enforcement.

Continuous defense for superior protection

Zyxel IDP service provides weekly signature refreshment to all the subscribed appliances. Signatures are updated without interruption as new threats emerge, so you never have to leave your network exposed. Capability with imported customized signature is also provided for networks with specific defense needs.

Full coverage of network threats

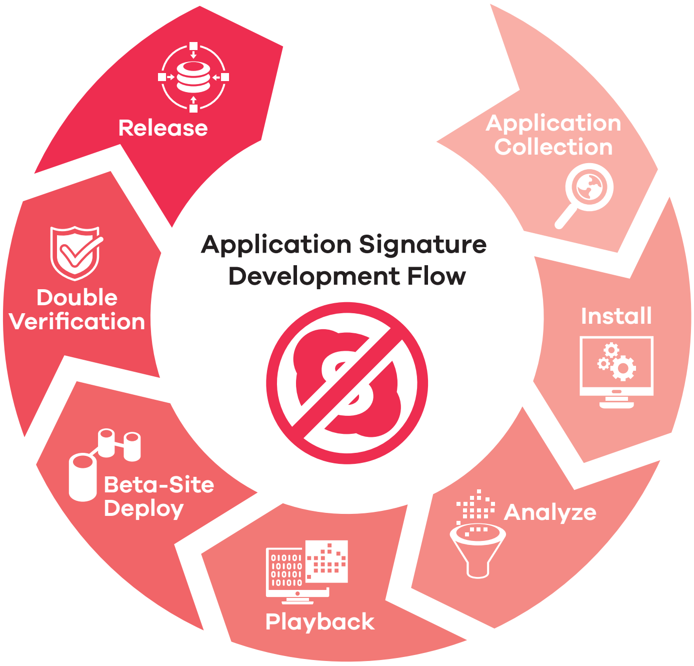
Zyxel IDP service supports layer 7 context-aware threat analysis, as well as behavior analysis, for detection of encrypted threats and applications to protect against both client-side and server-side vulnerabilities. The IDP signature can identify a wide variety of malware threats and attacks such as Trojans, backdoor applications, and DoS attacks, as well as other security hazards. We provide full protection, whether facing anomaly-based or vulnerability-based threats.

DoS	Buffer Overflow
Access Control	Scan
Trojan/ Backdoor	Malware
Web Attack	Others

Application Patrol Benefits

Continuous strengthening and precise categorization

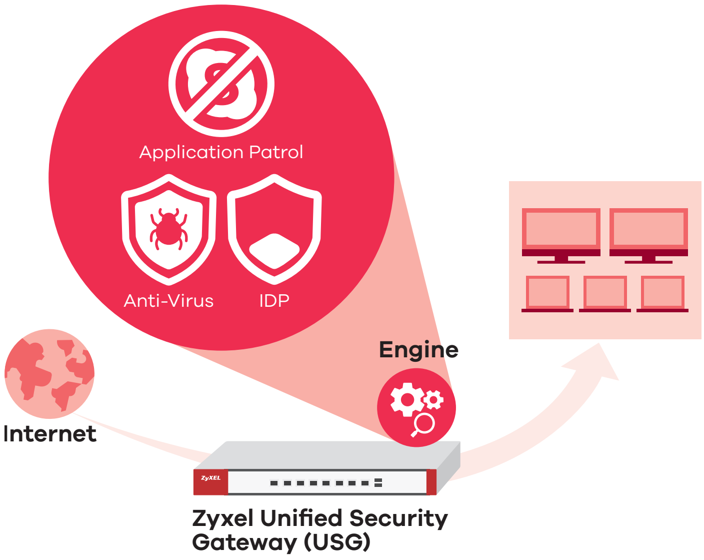
Zyxel Application Patrol is designed to provide the layer 7 application management, categorize covers the well-known network applications such as social, gaming, productivity, and other web applications and behaviors. Zyxel database supports over thousands of applications and its behaviors, along with the growing and ever-changing applications, our operate work with the repeating collect, analyze and Inspect verify flow cycle.



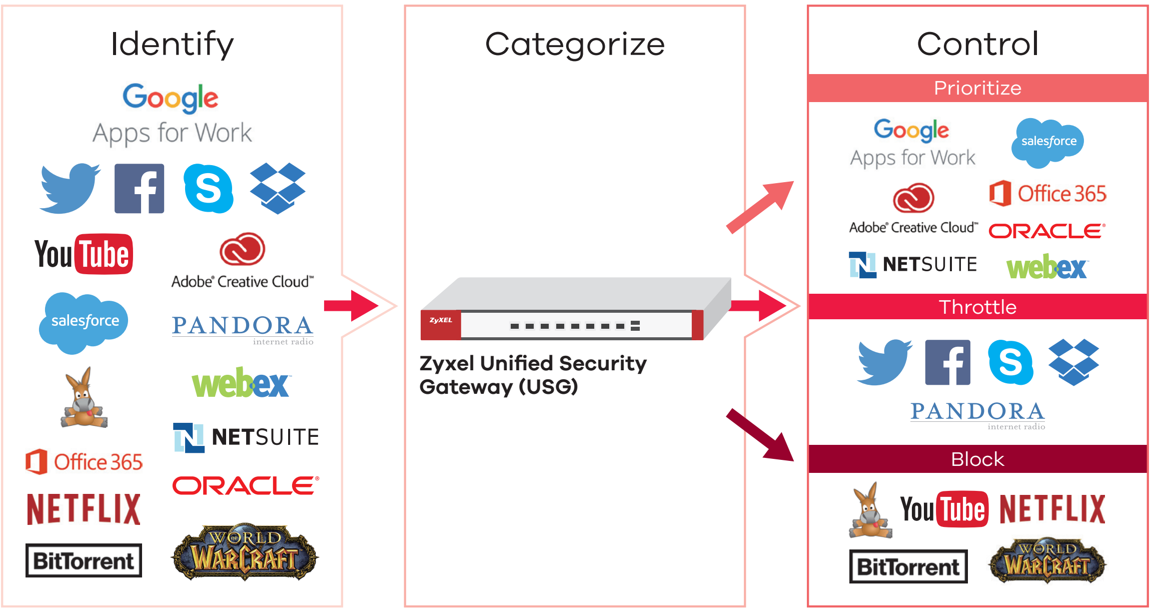
Smart single-pass scanning engine

Traditional scan engine has common defects including high latency and low performance, the reason was a difficult integration using multi-vendors. Zyxel provides the single-pass scanning engine, which compares packet with Anti-Virus, IDP and Application Patrol at the same time to significantly reduces latency and offers an unprecedented combination of speed and coverage.

Zyxel Application Patrol provides up to 19 categories and thousands of applications and its behavior, utilizes the DPI engine, enabling administrators to identify and categorize applications. In addition to filtering and classifying data, the application can establish blocks or traffic quota control policies, giving priority to productive applications and throttling acceptable network traffic, while simultaneously blocking unapproved applications, thus boosting productivity and preventing bandwidth abuse.



Application Diagram



Category List

- Business
- Bypass proxies and tunnels
- Database
- File transfer
- Games
- Instant messaging
- Mail and collaboration
- Mobile
- Network management
- Network protocols
- P2P
- Private protocol
- Remote access terminals
- Security update
- Social network
- Streaming media
- Voice over IP
- Web
- Web IM

Features

Intrusion Detection and Prevention

- Signature-based and behavior-based scanning
- Support exploit-based and vulnerability-based protection
- Support Web attacks like XSS and SQL injection
- Streamed-based engine
- Support SSL inspection
- Inspection on various protocols
  - HTTP/HTTPs, FTP/FTPs, SMTP/SMTPs, POP3/POP3s and IMAP/IMAPs
- Support compression files
  - ZIP, GZIP, BZIP2, RAR
- Customizable signature & protection profile
- Customizable new signature checking period: Hourly/ Daily/Weekly
- Automatic new signature update mechanism support

Application Patrol

- Streamed-based engine
- Identifies and control thousands of applications and its behaviors
- Support 19 application categories
- Granular control over the most important applications
- Application bandwidth management
- Real-time application statistics and reports

Compatible Security Appliances

Category	Product	
Next-Gen USG Performance Series	USG40/40W/60/60W	
Next-Gen USG Advanced Series	USG110/210/310	
Next-Gen USG Extreme Series	USG1100/1900	
VPN Firewall	ZyWALL 110/310/1100	

Compatible Security Appliances License Overview

License	Anti-Virus		Anti-Spam		Content Filtering 2.0		IDP with Application Patrol		Hotspot Management		Device HA Pro
	1 year	2 years	1 year	2 years	1 year	2 years	1 year	2 years	1 year	One-time	One-time
Next-Gen USG Series											
USG40/40W	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-	-	-
USG60/60W	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-	-	-
USG110	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
USG210	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
USG310	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
USG1100	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
USG1900	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPN Firewall Series											
USG20-VPN	-	-	Yes	Yes	Yes	Yes	-	-	-	-	-
USG20W-VPN	-	-	Yes	Yes	Yes	Yes	-	-	-	-	-
ZyWALL 110	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ZyWALL 310	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ZyWALL 1100	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Compatible Security Appliances Performance Overview

License	Firewall (Mbps)	Firewall + IPS (Mbps)	Firewall + AV (Mbps)	Firewall + UTM (AV+IDP)(Mbps)	Maximum Concurrent Connections	New Session Rate
Next-Gen USG Series						
USG40/40W	400	55	50	50	20,000	1,000
USG60/60W	1,000	120	90	90	40,000	1,000
USG110	1,600	250	300	250	60,000	2,800
USG210	1,900	300	350	300	80,000	2,800
USG310	5,000	500	450	450	200,000	8,000
USG1100	6,000	550	500	500	500,000	8,000
USG1900	7,000	650	550	550	500,000	8,000
VPN Firewall Series						
USG20-VPN	350	-	-	-	20,000	2,000
USG20W-VPN	350	-	-	-	20,000	2,000
ZyWALL 110	1,600	250	300	250	60,000	2,800
ZyWALL 310	5,000	500	450	450	200,000	8,000
ZyWALL 1100	7,000	650	550	550	500,000	8,000

ZYXEL

Your Networking Ally

For more product information, visit us on the web at www.zyxel.com

Copyright © 2017 Zyxel Communications Corp. All rights reserved. Zyxel, Zyxel logo are registered trademarks of Zyxel Communications Corp. All other brands, product names, or trademarks mentioned are the property of their respective owners. All specifications are subject to change without notice.