

A General

A01. What is UTM?

UTM (Unified Threat Management) is a new term for all-in-one firewall appliances that integrate multiple features such as Anti-Virus, IDP (Intrusion Detection Prevention), Anti-Spam and VPN. With UTM, businesses are better equipped to fight against ever evolving network attacks and streamline network management efforts.

A02. What's new in ZyWALL UTM ?

Your ZyWALL UTM model comes with the following features:

1. New and improved ZyNOS v4.00
2. An accompanying ZyWALL Turbo Card
3. Free 3-month Anti-Virus+IDP and Anti-Spam trial services
4. Free 1-month Content Filtering service

A03. What's new in ZyNOS v4.00?

In addition to the new, improved GUI design, ZyNOS v4.00 is integrated with the following features:

I. Enhanced Anti-Virus and IDP performance

Install the cutting-edge ZyWALL Turbo Card hardware accelerator on the ZyWALL UTM, and you get worry-free network security and better performance than before. It's a proof that ZyWALL UTM is worth every of your investment dollar.

II. Integrated Gateway Anti-Virus

Integrated with world-class Kaspersky Anti-Virus scanning engine, the ZyWALL UTM gives you the ultimate network with quick response, up-to-the-minute signature updates and effective virus elimination/notification process.

III. Feature-Complete UTM

With the new and improved ZyNOS v4.00, ZyWALL UTM comes with a wide range of security features (Firewall, VPN, Bandwidth Management, Load Balance, Content Filtering, Anti-Virus, IDP (Intrusion Detection and Prevention) and Anti-Spam) in one single device. ZyWALL UTM is your best choice for an application layer firewall.

IV. Round-the-Clock Protection

From the renowned ZYXEL Security Distribution Network, ZyWALL UTM performs regular automatic signature updates to deliver the highest protection possible against an ever-changing virus threats.

A04. What are the key features of the ZyWALL UTM's Anti-Spam?

I. High Spam Detection Rate

- 98% high spam catching rate and 0.05% low false positive rate.
- More than 1 million spam filter checks and real-time spam pattern updates.
- Ability to block spam with non-English content with language independent filters.

II. Phishing Protection with Antifraud E-mail Filters

III. Consistent Accuracy

- Instant fine-tune spam filters based on real-time statistical models with Advanced SpamCompiler™ System
- Intelligent spam filters with Genetic/Neural Fuzzy Logic Algorithm and Bayesian Analysis.

IV. Customizable spam threshold for detection effectiveness and accuracy.

V. Blacklisting and Whitelisting

You can create blacklists to block spam based on the IP address, sender name, or MIME header and customize whitelists bypass spam filters for e-mail from trusted partners.

A05. What are the key features of ZyWALL UTM's Content Filtering Feature?

Key features of ZyWALL Content Filtering security service:

- Filter out malicious web content, including: ActiveX, Java Applet, Cookie and Web proxy.
- URL / Keywords blocking: user can define custom black / white list by URL or keyword.
- Category-based dynamic database licensed from BlueCoat. It provides 52 categories and covers hundreds of millions of unique web pages. Besides that, the database is constantly updated so it's precise and reliable.

A06. Can I upgrade my existing ZyWALL device to take advantage of the new ZyNOS v4.00?

To take full advantage of the new and improved ZyNOS v4.00, all you have to do is upgrade the firmware on your ZyWALL. And, it's free.

Upgrade to ZyNOS v4.00 and enjoy our free three-month Anti-Virus+IDP/Anti-Spam trial services. To obtain a valid license, purchase an iCard to enjoy these security services.

A07. Why should I get ZyWALL UTM?

In addition to amazing network protection, ZyWALL UTM also outperforms similar products in its class. With ZyWALL UTM, you get out-standing features unmatched by others.

I. World's first SecuASIC™ hardware accelerator:

ZyWALL UTM is an ASIC-accelerated system for improved network performance. No other systems can screen real-time traffic for content-based threats at broadband data rates.

II. Comprehensive real-time protection against Internet threats:

Replace those inefficient security hardware with the all-in-one ZyWALL UTM. You can get ZyWALL UTM at a fraction of the cost and still enjoy outstanding comprehensive network protection with real-time traffic virus/ spam inspection. Simply put, ZyWALL UTM gives you the features you need at a fraction of the cost.

B UTM Related

B01. Why performance matters in UTM firewall appliances?

Most often when you activate multiple security features on a networking device, you get network protection at the price of performance degradation. This creates a bottleneck in your network resulting in slowed services. Only ZyWALL UTM's advanced SecuASIC™ technology can enable you both the security and performance you need while keeping you up-to-date Anti-Virus protection.

B02. Why should I need a network-based Anti-Virus solution when I have already installed Anti-Virus software on the computers?

Network-based Anti-Virus devices (like the ZyWALL) is typically deployed on the network edge is the first line of defense against virus attacks. Network-based Anti-Virus devices stop viruses from spreading into or out of the network and reduce processing load on the individual computers. In addition, network-based Anti-Virus devices are highly manageable and IT managers can enforce corporate security policy against commonly used protocols including SMTP, POP3, HTTP and FTP.

On the other hand, client-based Anti-Virus solution is designed to protect the endpoint within the corporate network. It requires software installation on each computer making updates a management burden. and higher managerial overhead because of its nature. On top of this, client-based Anti-Virus is slow in stopping virus threads through real-time traffic (such as from the Internet).

For best protection, security-aware companies tend to deploy both solutions because these two solutions are pretty much complementary in nature.

B03. Why bundle Anti-Virus and IDP features together?

The IDP feature can stop live network attacks while the Anti-Virus feature will scan, detect and destroy files that are infected with virus/worms. Armed with BOTH features, you are guaranteed to have the ultimate tool to guard your network from most types of attacks coming from any network.

B04. Can I subscribe to the Anti-Virus service alone or IDP service alone?

No. Because the Anti-Virus and IDP services are bundled together, you can not subscribe to any one of them alone.

Once you subscribed to the AV+IDP security service of ZyNOS v4.00, you can enable the Anti-Virus feature alone, IDP feature alone or both the Anti-Virus & IDP features.

B05. What are the hardware requirements to run Anti-Virus+IDP services?

- I. For owners of ZyWALL 5 UTM, ZyWALL 35 UTM or ZyWALL 70 UTM, no additional hardware is required. A ZyWALL Turbo Card is already bundled with the device to activate the Anti-Virus+IDP security service.
- II. For existing ZyWALL 5, ZyWALL 35 or ZyWALL 70 owners, you need to upgrade the firmware to ZyNOS v4.00 and purchase a ZyWALL Turbo Card. Before you activate the Anti-Virus+IDP security service, you must insert the ZyWALL Turbo Card into the ZyWALL.

For detailed information on how to acquire a ZyWALL Turbo Card, please contact your local reseller.

B06. Should I shutdown the ZyWALL device when I am going to install the ZyWALL Turbo Card?

Yes. First off, you have to power off the ZyWALL device; then you are clear to insert the ZyWALL Turbo Card into the device. Never insert or unplug the ZyWALL Turbo Card while the device is powered on.

B07. Now I know that the ZyWALL Turbo Card is a must to use the Anti-Virus+IDP service, what can I benefit from the ZyWALL Turbo Card?

With the ZyWALL Turbo Card installed, you can benefit from ZyXEL's unique SecuASIC™ technology that improves Anti-Virus+IDP performance and provides unmatched protection against network security threats.

B08.Can I insert ZyWALL Turbo Card and a wireless LAN card into the ZyWALL?

No. Your ZyWALL comes with one expansion slot. You can only insert one card (a ZyWALL Turbo Card or a wireless LAN card) into the ZyWALL.

B09. What's the difference between a gateway Anti-Spam and a client-based Anti-Spam filter?

A gateway Anti-Spam (such as your ZyWALL) is deployed on the network edge to inspect e-mail as they arrive to the mail server(s) and internal hosts. A client-based Anti-Spam filter (such as the one that comes with major email programs) is a piece of software installed on a computer to filter spam. The major differences between the two are:

I. Flexibility and Sensitivity

On the ZyWALL, you can adjust the spam threshold (an index number to determine if an e-mail is spam or not). By adjusting the spam threshold, you can fine tune the sensitivity of the Anti-Spam filter. This feature is not available on a client-based Anti-Spam.

II. Phishing

ZyWALL's Anti-Spam can effectively identify phishing e-mail. This is another feature that client-based Anti-Spam cannot provide.

III. Real-time Anti-Spam Update

ZyWALL's Anti-Spam updates real-time giving you effective spam detection. However, client-based Anti-Spam only gets updated at specific time intervals (for example, Outlook's Anti-Spam filter is updated monthly with Windows Update).

ZyWALL's Anti-Spam feature is complementary with client-based Anti-Spam filter.

B10.What if my e-mail service provider or my company mail server already provides Anti-Spam filter service, is there any other reason why I should still use ZyWALL Anti-Spam?

Yes, it is recommended that you set up and use ZyWALL's Anti-Spam in addition to any Anti-Spam filter service that you may already have. This is because:

I. You get additional layer of protection

Since the accuracy rate of Anti-Spam filters differ, the ZyWALL double-tags spam e-mails that are already tagged from the other Anti-Spam filter service to give you the reassurance that important customer e-mail are not accidentally tagged as spam and deleted. Furthermore, the ZyWALL may catch spam that are undetected by the other Anti-Spam filter service, thus giving you additional layer of spam protection.

II. You get protection from phishing

Phishing, being a new scam method, may not be detected by the other Anti-Spam filter service. This is compensated by ZyWALL's intelligent Anti-Spam phishing detection.

III. You get flexible Anti-Spam filter sensitivity

Most Anti-Spam filter service providers do not allow you to change the spam threshold (an index number to determine if an e-mail is spam or not), making the Anti-Spam filter either too sensitive or useless for your network. With ZyWALL Anti-Spam, you can adjust the spam threshold to the detection sensitivity that best fit your network environment.

IV. You get additional Anti-Spam fine-tuning control

You can set up blacklists (always block/tag) or white lists (always allow) to customize ZyWALL Anti-Spam for your business needs. This, again, may not be a feature available for free from the other Anti-Spam filter service.

All these reasons compel you to use ZyWALL Anti-Spam for added protection. So, why not?!

B11. What if the company mail server already does Anti-Spam, is there any reason why I should still use ZyWALL Anti-Spam?

Yes, the reasons are:

I. Complementary filtering

The tagged-spam filtered by spam software will be tagged again by ZyWALL's Anti-Spam. But those undetected spam emails can be detected by ZyWALL's Anti-Spam feature.

II. Phishing

Not every spam software can detect phishing emails. The Anti-Spam service of ZyWALL can detect phishing emails.

B12. Can you give me a comparison of the current Anti-Spam solutions?

The following lists the four Anti-Spam solutions current on the market.

- Anti-Spam filter service provided by e-mail service providers (such as Yahoo, Hotmail)
- Gateway Anti-Spam filter (such as the ZyWALL)
- Anti-Spam filter feature on mail servers (this may be on your corporate mail servers)
- Client-based Anti-Spam filter (often a filtering program installed on individual computers)

The table below shows the differences between these Anti-Spam solutions.

	Email Service Provider Anti-Spam Filter	Gateway Anti-Spam Filter	Mail Server Anti-Spam Filter	Client-based Anti-Spam filter
Adjustable Sensitivity	No	Yes	Yes	Yes
Phishing Protection	No	Yes	No	No
Blacklist/Whitelist	No	Yes	Yes	Yes
TCO (Total Cost of Ownership)	Low to Medium (Depending on your email service level)	Low (Single cost for multiple mail servers)	High (Need to install and maintain software)	Very High (Need to install and maintain software for every users)

B13. Do I need to insert a ZyWALL Turbo Card to upgrade to and use ZyNOS v4.00?

No. You can upgrade the firmware on your ZyWALL to ZyNOS v4.00 without inserting a ZyWALL Turbo Card first. You can still enjoy the many features in ZyNOS v4.00 without a ZyWALL Turbo Card.

B14. Do I need to insert a ZyWALL Turbo Card to use the Anti-spam or Content Filtering service?

No. You can activate and use the Anti-Spam and Content Filtering services on the ZyWALL without inserting a ZyWALL Turbo card first.

B15. When must I insert a ZyWALL Turbo Card into my ZyWALL?

You only need to insert a ZyWALL Turbo Card into the ZyWALL when you want to activate and use the Anti-Virus+IDP feature.

C Upgrade Related

C01. Which ZyWALL models can be upgraded to ZyNOS v4.00?

You can upgrade the firmware on ZyWALL 5, ZyWALL 35 and ZyWALL 70 to ZyNOS v4.00. For ZyWALL 70, the ability to upgrade to ZyNOS v4.00 firmware depends on the device RAM size. See next for more information.

The ZyWALL UTM series are pre-loaded with ZyNOS v4.00.

C02. What are the special requirements for ZyWALL 70 ZyNOS v4.00 firmware upgrade?

There are two versions of ZyWALL 70: one with 32 MB and the other with 64 MB of RAM. You can only upgrade the firmware to ZyNOS v4.00 on a ZyWALL 70 with 64 MB of RAM.

To check the RAM size on the ZyWALL 70, enter the **sys atsh** command in the CLI.

Note:

- Do NOT directly upgrade the firmware to ZyNOS v4.00 for ZyWALL 70 using a previous firmware version (v3.62, v3.63 or v3.64). Follow the instruction described next for your ZyWALL 70 version.
- For ZyWALL 70 with 64 MB of RAM, you MUST upgrade the firmware to ZyNOS v3.65 first, then upgrade to ZyNOS v4.00.
- For ZyWALL 70 with 32 MB or RAM, you MUST upgrade to ZyNOS v3.65. You can NOT upgrade the firmware to ZyNOS v4.00 at this point.

The following table shows what firmware version is available for each ZyWALL models.

Firmware-Model Mappings				
Firmware Upgrade Available	ZyWALL 70 (32MB)	ZyWALL 70 (64MB)	ZyWALL 35	ZyWALL 5
v3.62/3.63/3.64	Yes	Yes	Yes	Yes (v3.62/3.64)
v3.65	Yes	Yes	No	No
v4.00	No	Yes	Yes	Yes

C03. What is ZyNOS v3.65 for ZyWALL 70?

ZyNOS v3.65 is designed specifically for ZyWALL 70. It verifies the RAM size requirement on your ZyWALL 70 before upgrade to ZyNOS v4.00 is allowed.

You **MUST** upgrade your ZyWALL 70's firmware to v3.65. This is a mandatory step before upgrading to ZyNOS v4.00.

ZyNOS v3.65 does **NOT** support the Anti-Virus+IDP and Anti-Spam features.

ZyXEL will continue to maintain both ZyNOS v3.65 and v4.00 for ZyWALL 70.

C04. What happens if I upgrade a ZyWALL 70 with only 32MB of RAM to ZyNOS v4.00?

The firmware upgrade process will fail and a warning message displays. A ZyWALL 70 with 32 MB or RAM cannot be upgraded to use ZyNOS v4.00.

C05. What happened if I upgrade a ZyWALL 70 directly to ZyNOS v4.00 without upgrading to v3.65 first?

The firmware upgrade process will fail and a warning message displays. You must upgrade to ZyNOS v3.65 first.

C06. What can I do if I have a ZyWALL 70 with 32 MB of RAM and still want to use the ZyNOS v4.00 Anti-Virus+IDP features?

For those who have a ZyWALL 70 with 32 MB of RAM and still want to use ZyNOS v4.00's Anti-Virus+IDP features, we introduce a special trade-in program.

From this special offer, you get a new ZyWALL 70 UTM (including a ZyWALL Turbo Card) and a 2-year Anti-Virus+IDP Gold iCard at a fraction of the cost! So hurry up and trade in that ZyWALL 70.

This trade-in program is only available for owners of ZyWALL 70 with 32 MB of RAM. Please contact your local reseller for more information.

C07. What if I trade in my 32 MB RAM ZyWALL 70, can I still use my existing registered Content Filtering service?

Yes. Your Content Filtering service registration information is still valid and available.

You can continue using the Content Filtering feature on your new ZyWALL 70 UTM until the end of your current Content Filtering license period.

C08. How do I upgrade my ZyWALL 5/35 to use ZyNOS v4.00?

For ZyWALL 5 or ZyWALL 35 with a previous firmware version, you can upgrade the firmware directly to ZyNOS v4.00. No special steps or checking are required. Your current ZyWALL configuration will still be available when you upgrade to ZyNOS v4.00.

It is recommended that you always back up the current working ZyWALL system configuration before a firmware upgrade.

C09. What is the default Anti-Virus/IDP/Anti-Spam/Content Filtering setting after a successful ZyNOS v4.00 firmware upgrade?

When you start the ZyWALL for the first time, the Anti-Virus+IDP, Anti-Spam and Content Filtering features are disabled by default.

To start using these features, you must enable them first on the ZyWALL.

To activate and use the Anti-Virus+IDP features, you must first insert a ZyWALL Turbo Card.

C10. Will my configuration settings still be there when I upgrade my ZyWALL firmware to ZyNOS v4.00?

Yes. All your configuration settings (such as system, firewall and VPN rules) are preserved after the firmware upgrade.

It is recommended that you always back up the current working ZyWALL system configuration before a firmware upgrade.

C11. Can I downgrade the firmware on my ZyWALL 70 to an earlier version?

Yes. You can downgrade the firmware of ZyWALL 70 from v4.00 to any of the following versions: v3.65/v3.64/v3.63/v3.62.

However, your configuration settings may not be fully preserved after a firmware downgrade since some features may not be available in an earlier firmware version.

We don't guarantee all the system configurations can be fully converted and reserved after a downgrade because

It is recommended that you always back up the current working ZyWALL system configuration before a firmware upgrade/downgrade.

C12. Can I downgrade a ZyWALL 5 or ZyWALL 35 running ZyNOS v4.00 back to ZyNOS v3.64 (or below)?

Yes, downgrade is supported.

Again, we don't guarantee all the system configurations can be fully converted and reserved since some feature settings may not be available on older firmware versions.

D Service License Related

D01. What are the ZyNOS v4.00 features that require an additional service license purchase?

With the ZyNOS v4.00, you need to buy an additional service license to use and activate the following security features:

- › Anti-Virus + IDP
- › Anti-Spam
- › Content Filtering

Note:

ZyNOS v4.00 comes with a free 3-month trial for these features.

D02. What service license can I get for my ZyWALL?

For ZyWALL UTM series, we offer the following service licenses.

	ZyWALL 5 UTM	ZyWALL 35 UTM	ZyWALL 70 UTM
Anti-Virus+IDP (Renewal)	iCard, 1-year Anti-Virus+IDP Silver iCard, 2-year Anti-Virus+IDP Silver	iCard, 1-year Anti-Virus+IDP Gold iCard, 2-year Anti-Virus+IDP Gold	
Anti-Spam	iCard, 1-year Anti-Spam Silver iCard, 2-year Anti-Spam Silver	iCard, 1-year Anti-Spam Gold iCard, 2-year Anti-Spam Gold	
Content Filtering	iCard, 1-year Content Filter Silver	iCard, 1-year Content Filter Gold	

For current ZyWALL series, we offer the following service licenses.

	ZyWALL 5 UTM	ZyWALL 35 UTM	ZyWALL 70 UTM
Turbo Suite* (Anti-Virus+IDP Standard)	ZyWALL Turbo Suite, 1-year Anti-Virus+IDP Silver ZyWALL Turbo Suite, 2-year Anti-Virus+IDP Silver	ZyWALL Turbo Suite, 1-year Anti-Virus+IDP Gold ZyWALL Turbo Suite, 2-year Anti-Virus+IDP Gold	
Anti-Virus+IDP (Renewal)	iCard, 1-year Anti-Virus+IDP Silver iCard, 2-year Anti-Virus+IDP Silver	iCard, 1-year Anti-Virus+IDP Gold iCard, 2-year Anti-Virus+IDP Gold	
Anti-Spam	iCard, 1-year Anti-Spam Silver iCard, 2-year Anti-Spam Silver	iCard, 1-year Anti-Spam Gold iCard, 2-year Anti-Spam Gold	
Content Filtering	iCard, 1-year Content Filter Silver	iCard, 1-year Content Filter Gold	
Note	A ZyWALL Turbo Card is included in all Turbo Suite.		

D03. What is iCard?

The iCard contains the license number required for Anti-Virus/IDP/Anti-Spam/Content Filtering service registration and activation in your ZyWALL.

There are two iCard versions: **Gold** and **Silver**. The two versions differ in the license period and feature type. Selection of an iCard depends on your ZyWALL model.

D04. What kind of iCard should I buy?

It depends on the ZyWALL model you have, the security service you desire and the license period you need.

See the following table for the choices available for your ZyWALL model.

	Anti-Virus+IDP		Anti-Spam		Content Filtering	
	1 Year	2 Year	1 Year	2 Year	1 Year	2 Year
ZyWALL 2	N/A	N/A	N/A	N/A	1-year, Silver	N/A
ZyWALL 5	1-year, Silver	2-year, Silver	1-year, Silver	2-year, Silver	1-year, Silver	N/A
ZyWALL 35	1-year, Gold	2-year, Gold	1-year, Gold	2-year, Gold	1-year, Gold	N/A
ZyWALL 70	1-year, Gold	2-year, Gold	1-year, Gold	2-year, Gold	1-year, Gold	N/A

D05. What if I bought the wrong iCard for my ZyWALL?

Service registration and/or activation will fail. So make sure you get the right iCard for your ZyWALL model.

D06. Does ZyXEL offer free Anti-Virus+IDP trial service?

Yes. With ZyNOS v4.00, you get free 3-month Anti-Virus+IDP trial service. If you buy an iCard Anti-Virus+IDP license within this free trial period, you get an additional 3-period for free! To continue the service, purchase new iCard and register the service.

* Make sure you insert a ZyWALL Turbo Card before you activate and use the Anti-Virus+IDP services.

D07. Does ZyXEL offer free Anti-Spam trial service?

Yes. With ZyNOS v4.00, you get free 3-month Anti-Spam trial service. If you buy an iCard Anti-Spam license within this free trial period, you get an additional 3-period for free!

To continue the service, purchase new iCard and register the service.

* To use the Anti-Spam service, you do NOT need a ZyWALL Turbo Card.

D08. Do I need to insert a ZyWALL Turbo Card to use the Anti-Spam feature?

No. You do NOT need to insert a ZyWALL Turbo Card to activate and use the Anti-Spam service. The ZyWALL Turbo Card is specially designed to enhance the Anti-Virus and IDP inspection process on the ZyWALL. This reduce the processing load on the ZyWALL and provide better performance.

D09. Can I try the Content Filtering service for free? How long is the free trial period?

Yes. The free 30-day content filtering trial service is available for ZyWALL 2, ZyWALL 5, ZyWALL 35, ZyWALL 70, ZyWALL 5 UTM, ZyWALL 35 UTM and ZyWALL 70 UTM with ZyNOS v4.00.

E Anti-Virus Availability

E01. When will the ZyWALL UTM models be available?

The ZyWALL UTM models are scheduled to be available in September, 2005. Also available in September are ZyNOS v4.00, ZyWALL Turbo Card, iCard for Anti-Virus + IDP security service and iCard for the Anti-Spam service.

Contact your local reseller or visit <http://www.zyxel.com> for more information.

F Service Activation

F01. Why do I have to register?

You have to register your purchased ZyWALL devices because of the following reasons:

1. If you wanted to use the free trial service of ZyWALL's AV+IDP, AS or CF services, you have to activate it from within the web configurator of ZyWALL devices.
2. If you purchased iCard for a security service, you must activate the security service via the web configurator. The security services in ZyNOS v4.00 includes: AV+IDP, Anti-Spam and Content Filtering services.

During the registration, the web configurator will communicate with myZyXEL.com in the background and transmits required information onto myZyXEL.com so that the registration or activation could be accomplished.

F02. What else can I do with the myZyXEL.com account?

- ▶ Access to firmware and security service updates.
- ▶ Receive update notification on ZyWALL related services, firmware, and products.
- ▶ Manage (activate, change or delete) your ZyWALL security services online.

In summary, myZyXEL.com delivers a convenient, centralized way to register all your ZyWALL security appliances and security services. It eliminates the hassle of registering individual ZyWALL appliances and upgrades to streamline the management of all your ZyWALL security services.

Instead of registering each ZyWALL product individually, using myZyXEL.com allows you to have a single user profile where you can manage all your product registration and service activation.

F03. With the launch of ZyNOS v4.00, is there any changes in myZyXEL.com?

Yes. Because of the ZyNOS v4.00 launch, we proudly introduce the new registration flow on myZyXEL.com. However, you can still register devices running older firmware versions.

F04. Which ZyWALL models and services can be registered via myZyXEL.com?

The following table shows what myZyXEL.com registration type is available for your ZyWALL.

Models for Registration on myZyXEL.com				
	Device Registration	Anti-Virus+IDP Service Activation	Anti-Spam Service Activation	Content Filtering Service Activation
New Registration Flow	ZyWALL 5 (v4.00) ZyWALL 35 (v4.00) ZyWALL 70 (v4.00)	ZyWALL 5 (v4.00) ZyWALL 35 (v4.00) ZyWALL 70 (v4.00)	ZyWALL 5 (v4.00) ZyWALL 35 (v4.00) ZyWALL 70 (v4.00)	ZyWALL 5 (v4.00) ZyWALL 35 (v4.00) ZyWALL 70 (v4.00)
Previous Registration Flow	ZyWALL2 (v3.62) ZyWALL 5 (v3.64/v3.62) ZyWALL 35 (v3.64 or below) ZyWALL 70 (v3.65 or below)	N/A	N/A	ZyWALL2 (v3.62) ZyWALL 5 (v3.64/v3.62) ZyWALL 35 (v3.64 or below) ZyWALL 70 (v3.65 or below)
Note	Devices running ZyNOS v4.00 must use the New Registration Flow.			

F05. What's the difference between the two registration flows on myZyXEL.com?

- ▶ In the new registration flow, you can register and activate services using the ZyWALL's WebGUI. In the previous registration flow, the registration is done in the myZyXEL.com registration website in a separate browser window
- ▶ The new registration flow is user-friendly for the new and the experienced. In the new registration flow, it's no longer necessary to open another web browser window to register your device. Instead, the registration flow is embedded in the device's WebGUI. Furthermore, you are not required to manually enter the MAC address of a device because the MAC address will be automatically sent to myZyXEL.com during the registration process.

F06. If I were new to myZyXEL.com, what are the required fields when I register my ZyWALL device on myZyXEL.com?

The required fields include: user name, password, a valid email address and country.

F07. What's the benefit of entering valid email address when I'm registering my devices on myZyXEL.com?

If you entered the valid email address during registration, you are going to:

1. Receive advance notifications (in email) prior to the expiration date of your free trial or license subscription. This may help avoid interruptions of your current security service subscriptions.
2. Receive latest advisories (in email) from our ZSRT. The advisory contains latest signature release information and helpful security news.

F08. When using the new registration flow, do I have to create a new account if I already have a myZyXEL.com account?

No. Your existing myZyXEL.com account is still valid. You can still use the existing myZyXEL.com account to register a device and activate a service.

F09. After the registration is complete using the new registration process, what kind of information is stored on myZyXEL.com server?

Your user profile is stored on myZyXEL.com after the registration is done. User profile information includes the user name, password, email address, country and your registered products and services.

F10. What is mySecurityZone?

- mySecurityZone is a free service portal that is accessible to everyone.
- Anyone can browse the latest security news and updates from ZSRT (ZyXEL Security Response Team), access free resources and subscribe to our free newsletter.
- For those who have a registered ZyWALL and a myZyXEL.com account, you can log in to mySecurityZone (with the same myZyXEL.com account information) to view detailed description on Anti-Virus+IDP policies and perform virus searches. In addition, you automatically receive our advisory newsletters with the latest security updates and other valuable information.

What can I do with mySecurityZone if I have a registered ZyWALL and a myZyXEL.com account?

In mySecurityZone you can:

- ▶ Access to all security resources and get free advisory newsletters.
- ▶ Display or share ZyWALL security information (such as Anti-Virus/IDP policy)
- ▶ Search for all ZyWALL product information

F11. What is the Update Server?

The Update Server is designed for Anti-Virus+IDP security service subscribers to ensure that the signature file on their devices is up-to-date. This allows effective virus detection and threat prevention.

Your ZyWALL regularly checks for any signature file updates and downloads signature files from the Update Server.

The Update Server is hosted by ZyXEL to provide security protection with 24x7 monitoring service. With dedicated IDC (International Data Center) for a global distributed architecture, we ensure top-notch Update Server quality of service and zero-downtime for all security service subscribers

F12. Since keeping signatures updated is crucial, what has ZyXEL done to ensure that the Update Server will always be available to customers?

At ZyXEL, important steps are taken to ensure the availability of the Update Server. These include the following:

(1) Dedicated server rooms

We have deployed server farms in IDCs (International Data Centers) located in Taiwan and Germany. The two IDCs are configured for redundancy and server load balancing to ensure the maximum availability of our Update Server.

(2) NOC-grade 24x7 monitoring

ZyXEL has created standard procedure and a dedicated team to monitor the status and operation of the Update Server. This is to detect failures of any kind and fix them in the shortest time possible so that system downtime could be minimized. In addition, this helps ZyXEL to ensure SLA (Service Level Agreement) to our valued customers.

F13. Who maintains mySecurityZone and the Update Server?

"mySecurityZone" and the "Update Server" are maintained by the dedicated ZyXEL Security Response Team (ZSRT). Created with a group of security experts, ZSRT first detects any new virus outbreaks, collect data samples and analyse the samples to create an Anti-Virus+IDP pattern, This pattern is then published as an advisory to mySecurityZone and sent to newsletter subscribers.

F14. Do I have to pay for myZyXEL.com and mySecurityZone services?

No. You can access the free resources on myZyXEL.com and mySecurityZone sites without additional fees.

On myZyXEL.com, you need to purchase an iCard to register and activate security services on your device.

For those with a registered ZyWALL and a myZyXEL.com account, you get the latest security advisory and access to all Anti-Virus+IDP signature information on mySecurityZone.

F15. What is ZSDN?

ZSDN (ZyXEL Security Distribution Network) is a set of service portals designed to provide easy-to-use and always-on service to ZyXEL customers and resellers. ZSDN is composed of myZyXEL.com, mySecurityZone, the Update Server and ZSRT.

F16. How do I access the security portals?

You can access ZyXEL security portals at the following web sites:

myZyXEL.com

<http://www.myzyxel.com/myzyxel/>

mySecurityZone

<https://mysecurity.zyxel.com/mysecurity/>

For the Update Server, there is currently no publicly-accessible web sites. it is only accessible for registered ZyWALL devices with Anti-Virus+IDP services activated.

G Hands-on

G01. Are the signature database in Kasperky's Anti-Virus software and ZyWALL Anti-Virus different?

Yes. The two virus signature databases are different.

The signatures in ZyWALL's virus database are carefully selected and updated. The reasons for doing this are:

- Increased performance and efficiency
- Reduced database size with no virus patterns that are very old.
- Lowered false-positive rate

For ZyNOS v4.00, the signatures are chosen and delivered to ZyXEL by Kaspersky so that our Anti-Virus subscribers can always keep their virus signatures updated.

G02. For the signature database in ZyNOS v4.00, what are the criteria for selecting those signatures out of the complete Kaspersky signature database?

The signatures for ZyNOS v4.00 chosen by Kaspersky are based on the following criteria:

I. Active (In the Wild):

The complete Kaspersky's signature database contains over 130K of virus patterns. However, not all of them are relevant in today's virus threats. Thus viruses are classified as in the "zoo" and "in the wild". Viruses in the "zoo" are almost non-existent and listed in the database for precautionary reasons. The most important ones are classified "in the wild" (<http://www.wildlist.org>), viruses in this group are "active", and should be taken care of more carefully. According to Kaspersky, the number of viruses in the "zoo" is over 120K. Thus these are the ones that we need to address.

II. Infectious through networks:

Not all viruses are spread via networks. Some only infect the host that executed the virus code (host-based) but will not spread to other hosts on the network. Since our product is aimed to deliver gateway Anti-Virus protection, we focus on those viruses which can be spread via networks instead of those host-based viruses.

III. Top 20 of Kaspersly Anti-Virus Database:

Kaspersky always updates the top 20 in their signature database. This is also included in ZyXEL's signature updates.

Based on the above criteria, Kaskersky helps screen the list of important virus signatures (between 1K to 1.5K) for the ZyWALL devices and sets the update priority to the selected signatures. After the list is chosen and updated, Kaspersky sends the update to ZyXEL. Thus, for a gateway Anti-Virus solution, what matters is not how old the virus signature is but whether the virus is active or not and the

G03. Is the ZyWALL's Anti-Virus feature implemented as a proxy to process large files?

No, we don't implement a proxy to store large files for Anti-Virus inspection.

G04. Will ZyWALL be able to inspect an e-mail with a large attachment (for example, more than 5MB in size) that contains a virus?

Yes. The ZyWALL UTM Anti-Virus feature is able to scan e-mail attachments of any sizes. With a special algorithm implemented to deal with the file size problem, you can be rest assure that no matter how big the file size is, it is inspected by your ZyWALL UTM Anti-Virus

G05. What happens if the virus is in the e-mail attachment and that it is received by a user?

Even if the virus is hidden in a specific file within a file attachment in any part of the e-mail, your ZyWALL Anti-Virus can still detect and destroy the file portion that is infected. As a result, the user will get the file but can't open it. Thus, the user's computer will not be infected by the virus.

G06. Could I copy the IDP policy settings from one ZyWALL to another?

Yes. With ZyNOS v4.00, you can always back up your ZyWALL's IDP policy settings to your computer and import the backed up IDP settings to another ZyWALL using the WebGUI. Thus multiple ZyWALLs can have the same IDP policy settings.

G07. How do I keep Anti-Virus+IDP signatures updated?

We recommend that you configure your ZyWALL to automatically update the signature on an hourly basis so that the ZyWALL can check with our Update Server to see if there is new signature available. However, you can still change the update interval as you wish or perform a manual update anytime.

G08. How often does ZyXEL update Anti-Virus+IDP signatures?

ZyXEL updates Anti-Virus+IDP signature at least 5 times a week. These signatures are fully tested and the quality assured.

Once new virus is detected, ZyXEL will release the virus signature in the shortest time possible. Minimizing the impact of any new virus is always the first priority for our Anti-Virus+IDP service subscribers.

G09. Does Anti-Virus, IDP or Anti-Spam inspect VPN traffic?

No. Since a VPN connection is already encrypted and secured, VPN traffic will not be scanned Anti-Virus, IDP or Anti-Spam function in the current ZyNOS v4.00.

However, VPN traffic inspection will be supported in the forthcoming ZyNOS firmware release.

G10. Could I turn off the Anti-Virus+IDP, Anti-Spam or Content Filtering feature after a successful activation?

Yes. You always can turn off the Anti-Virus+IDP, Anti-Spam or Content Filtering feature after a successful activation.

G11. How to turn off the Anti-Virus+IDP, Anti-Spam or Content Filtering feature after a successful activation?

To turn off a security feature, you need to log on to the ZyWALL's WebGUI.

From the navigation panel, click SECURITY ' IDP (or ANTI-VIRUS or ANTI-SPAM or CONTENT FILTER) and clear the Enable check box.

G12. Is there any reason that forces user to turn off the Anti-Virus feature on a ZyWALL UTM?

Disabling the Anti-Virus function on a ZyWALL depends on your network requirements. With the Anti-Virus feature turned on, throughput will drop down to 3~4Mbps, which is more than enough for a gateway device in most networks.

From our experience, users of security devices from other vendors often turn off the Anti-Virus feature due to jitter or very low performance. These problems are almost non-existing with our ZyWALL which maintains superb network performance even with all security features turned on. Please refer to the lab test report

G13. With ZyWALL's Anti-Spam feature, what's the recommended actions against identified spam emails?

On the ZyWALL, you can either block or tag all identified spam.

If you choose to block them, you have no control over false-positives.

If you choose to tag them, you still have spam on your mail server and all network users have to configure the e-mail program to filter the spam e-mails into a dedicated folder.

Since your ZyWALL (with the world-class Mailshell Anti-Spam technology) produces very low false-positives, we recommend that you tag identified spam (the action chosen by most IT managers).

G14. What's the specification of the ZyNOS v4.00 Anti-Spam feature?

Specifications of Anti-Spam feature	
Supported protocols	POP3 and SMTP
Actions on spam	For POP3: Spam tagging For SMTP: Spam tagging or blocking
Default Setting	Enable Tag with the [SPAM]/[PHISHING] subject

G15. How reliable is the detection rate of the ZyWALL's Anti-Spam feature?

Reliability rate: 98%, 10% higher than Open Source SpamAssassin.

G16. How do I keep the Anti-Spam signatures updated?

Currently, with ZyNOS v4.00, there is no local spam signature database stored on the ZyWALL UTM devices. As a result, you don't have to update the Anti-Spam signature on your ZyWALL. The Anti-Spam score and queries between Anti-Spam-enabled ZyWALL devices and the external rating server take place dynamically and automatically in the background.

However, you may want to maintain your own black list/white list on the ZyWALL to maximize the effectiveness of the Anti-Spam security service.

G17. How do I keep the Content Filtering database updated?

Currently, with ZyNOS v4.00, there is no local Content Filtering signature database stored on the ZyWALL devices.

As a result, you don't have to update the content filtering database on the ZyWALL devices. The queries between Content Filtering-enabled ZyWALL devices and an external database server take place dynamically and automatically in the background.

However, you may want to maintain your own URL/keyword list on the ZyWALL to maximize the effectiveness of the Content Filtering service.