ZyWALL Series UTM Setup (IDP)

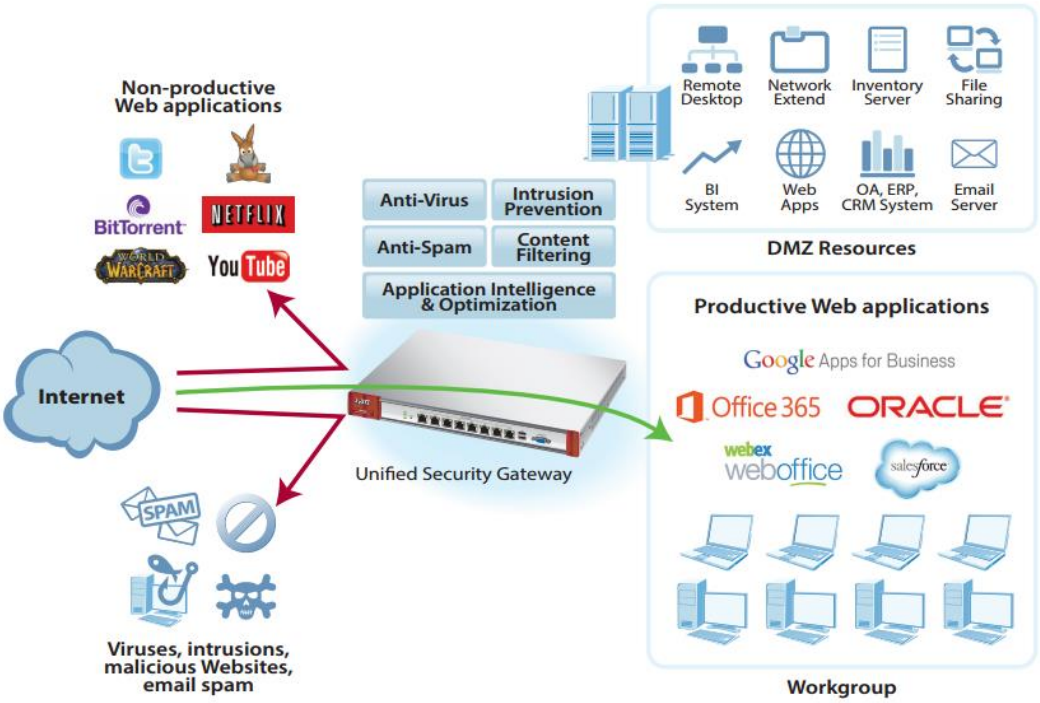
This guide is designed to help with the setup of the ZyWALL's IDP (Intrusion Detection and Prevention) feature.

Supported Devices

USG40 – Firmware version 4.10(AALA.0) and above
USG40W – Firmware version 4.10(AALB.0) and above
USG60 – Firmware version 4.10(AAKY.0) and above
USG60W – Firmware version 4.10(AAKZ.0) and above
USG110 – Firmware version 4.10(AAPH.0) and above
USG210 – Firmware version 4.10(AAPI.0) and above
USG310 – Firmware version 4.10(AAPJ.0) and above
USG1100 – Firmware version 4.10(AAPK.0) and above
USG1900 – Firmware version 4.10(AAPL.0) and above

Overview

The USG's IDP system can detect malicious or suspicious packets and respond instantaneously. IDP on the ZyWALL protects against network based intrusions.

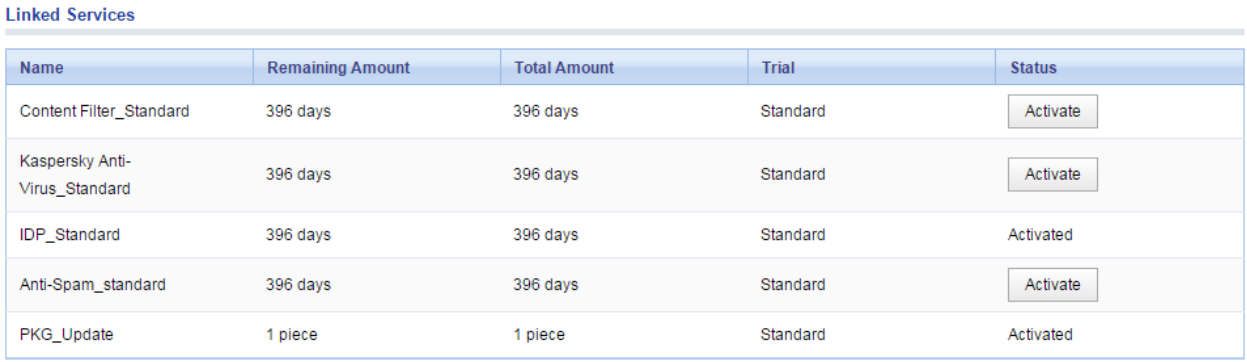

Non-productive Web applications
BitTorrent
NETFLIX
WORLD WARCRAFT
YouTube
Internet
SPAM
Viruses, intrusions, malicious Websites, email spam
Anti-Virus
Intrusion Prevention
Anti-Spam
Content Filtering
Application Intelligence & Optimization
Unified Security Gateway
Remote Desktop
Network Extend
Inventory Server
File Sharing
BI System
Web Apps
OA, ERP, CRM System
Email Server
DMZ Resources
Productive Web applications
Google Apps for Business
Office 365
ORACLE
webex weboffice
salesforce
Workgroup

Register USG to MyZyXEL.com 2.0

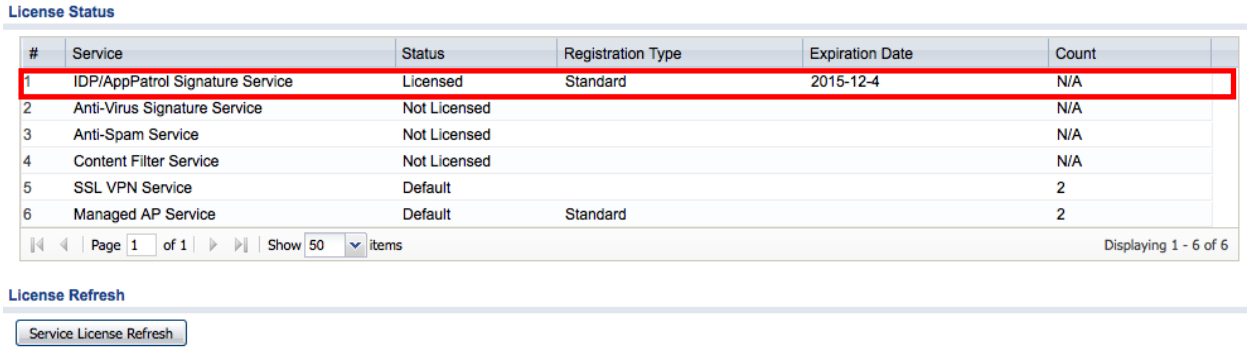
Registration of the device is required to be able to activate UTM services. Please look at the "Registering ZyWALL ZLD Routers" document for instructions on completing the registration process for your router.

Activate Licenses

To activate the UTM licenses for the USG please login to your MyZyXEL.com account at https://portal.myzyxel.com. Once logged in you will see the dashboard windows which shows all devices registered under the account. Select the router you wish to activate the license on from the list. Click the **Activate** button for the services you wish to enable.



On the router go to menu **Configuration → Licensing → Registration** and click on the *Service* tab. Click the button **Service License Refresh** to have the router check with the MyZyXEL.com server for any changes to licensing, etc.

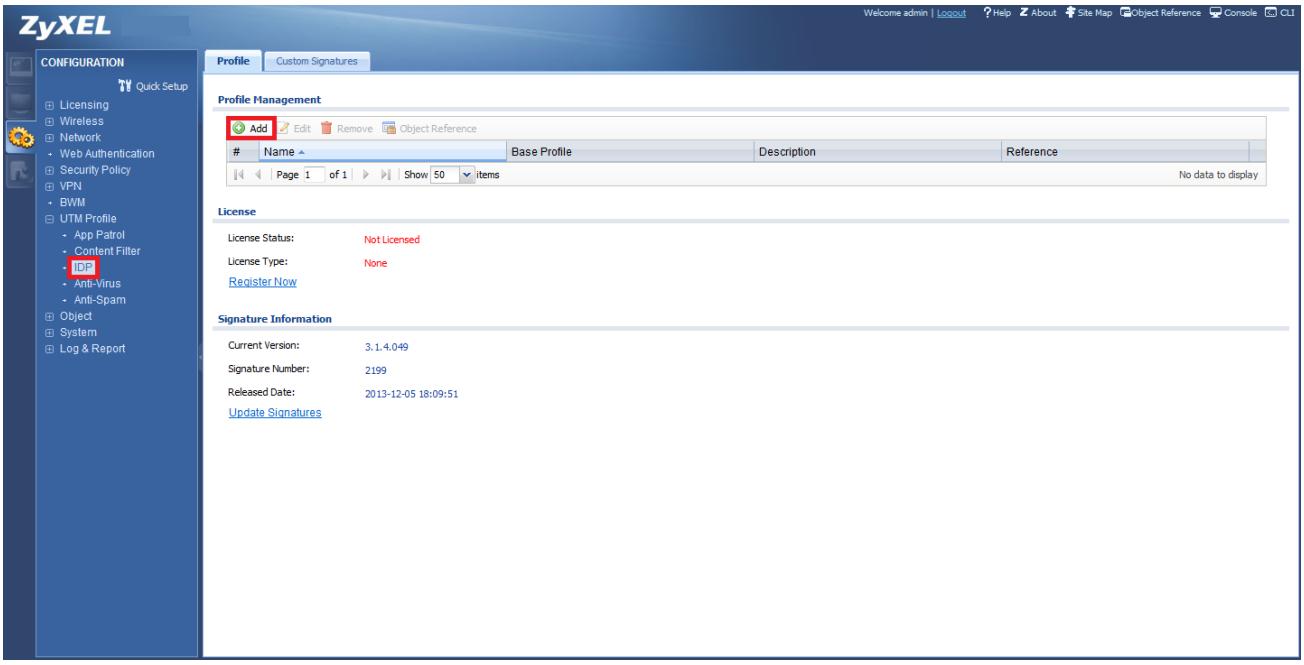


Download/Update Service Signatures

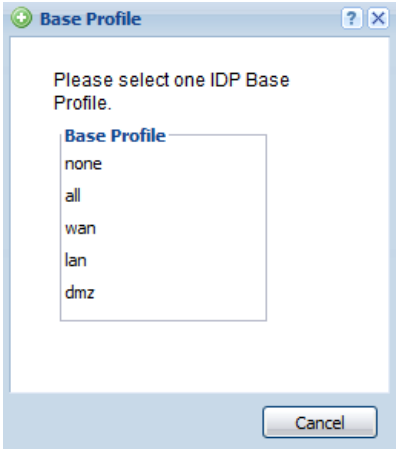
Now that the device has been registered and licenses activated, go to menu **Configuration → Licensing → Signature Update** and click the *IDP/AppPatrol* tab to update the signatures. Click the **Update Now** button to download latest signature version.
Signatures must be downloaded before creating an IDP (Intrusion, Detection and Prevention) profile, especially if you have just registered and activated the license. If you do not download the signatures you will not be able to create the profile as there will be no service filters to add to the profile.

Creating IDP Profile

From the web configuration screen go to **Configuration → UTM Profile → IDP**, click the **Add** button to insert a profile.



You will be prompted to select a ***Base Profile***.



- **NONE**: *All signatures are disabled. No logs are generated nor are actions taken.*
- **ALL**: *All signatures are enabled. Signatures with a high or severe severity level (greater than three) generate log alerts and cause packets that trigger them to be dropped. Signatures with a very*

low, low or medium severity level (less than or equal to three) generate logs (not log alerts) and no action is taken on packets that trigger them.

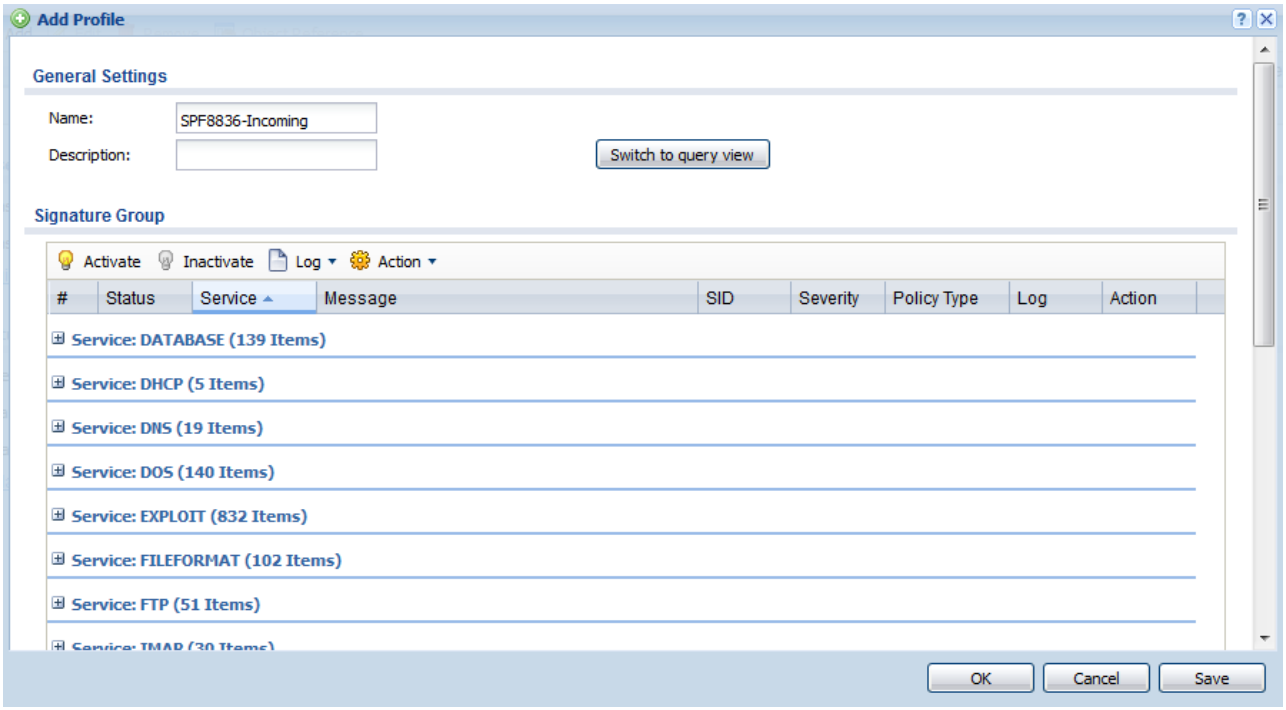
- **WAN**: *Signatures for all services are enabled. Signatures with a medium, high or severe severity level (greater than two) generate logs (not log alerts) and no action is taken on packets that trigger them. Signatures with a very low or low severity level (less than or equal to two) are disabled.*

- **LAN**: *This profile is most suitable for common LAN network services. Signatures for common services such as DNS, FTP, HTTP, ICMP, IM, IMAP, MISC, NETBIOS, P2P, POP3, RPC, RSERVICE, SMTP, SNMP, SQL, TELNET, TFTP, and MySQL are enabled. Signatures with a high or severe severity level (greater than three) generate logs (not log alerts) and cause packets that trigger them to be dropped. Signatures with a low or medium severity level (two or three) generate logs (not log alerts) and no action is taken on packets that trigger them. Signatures with a very low severity level (one) are disabled.*

- **DMZ**: *This profile is most suitable for networks containing your servers. Signatures for common services such as DNS, FTP, HTTP, ICMP, IMAP, MISC, NETBIOS, POP3, RPC, RSERVICE, SMTP, SNMP, SQL, TELNET, Oracle, and MySQL are enabled. Signatures with a high or severe severity level (greater than three) generate log alerts and cause packets that trigger them to be dropped. Signatures with a low or medium severity level (two or three) generate logs (not log alerts) and no action is taken on packets that trigger them. Signatures with a very low severity level (one) are disabled.*

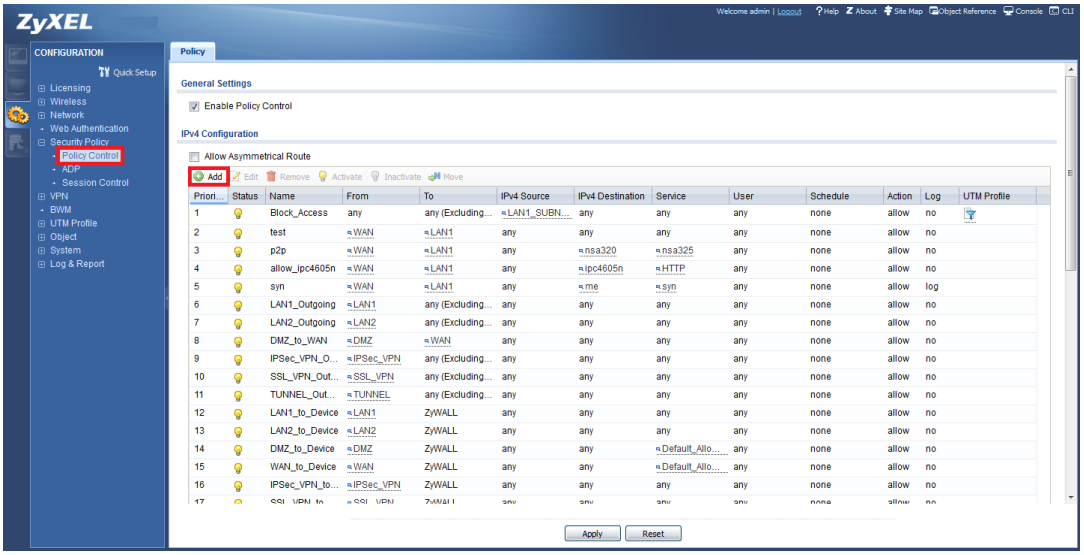
Once you have selected the Base Profile you will see a list with all the

IDP signatures used for the profile. Give the profile a name and click **OK** to apply the settings.

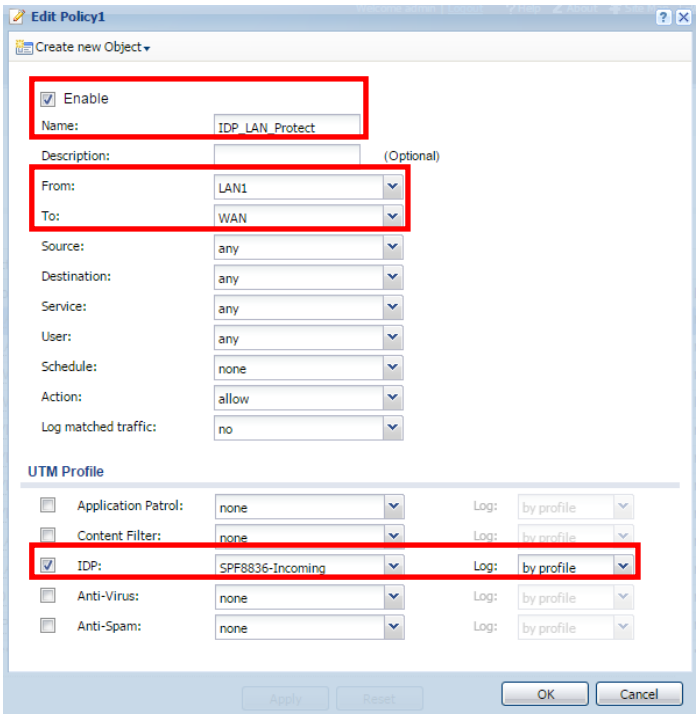


Creating UTM Security Policy

From the web configuration screen go to **Configuration → Security Policy → Policy Control**, click the **Add** button to insert a rule to check against intrusions using the IDP profile created on the previous step.



- Give the Policy Control rule a name
- Select the packet direction ***From:* LAN1** (Internal Network)
- Select the packet direction ***To:* WAN** (Internet)
- Scroll down to the **UTM Profile** option and check the box next to IDP, select the profile you created and whether or not you wish the ZyWALL to log an entry any time this Policy Control rule is tripped.


Edit Policy1
Create new Object
Enable
Name:
IDP_LAN_Protect
Description:
(Optional)
From:
LAN1
To:
WAN
Source:
any
Destination:
any
Service:
any
User:
any
Schedule:
none
Action:
allow
Log matched traffic:
no
UTM Profile
Application Patrol:
none
Log:
by profile
Content Filter:
none
Log:
by profile
IDP:
SPF8836-Incoming
Log:
by profile
Anti-Virus:
none
Log:
by profile
Anti-Spam:
none
Log:
by profile
Apply
Reset
OK
Cancel