AppPatrol UTM Setup

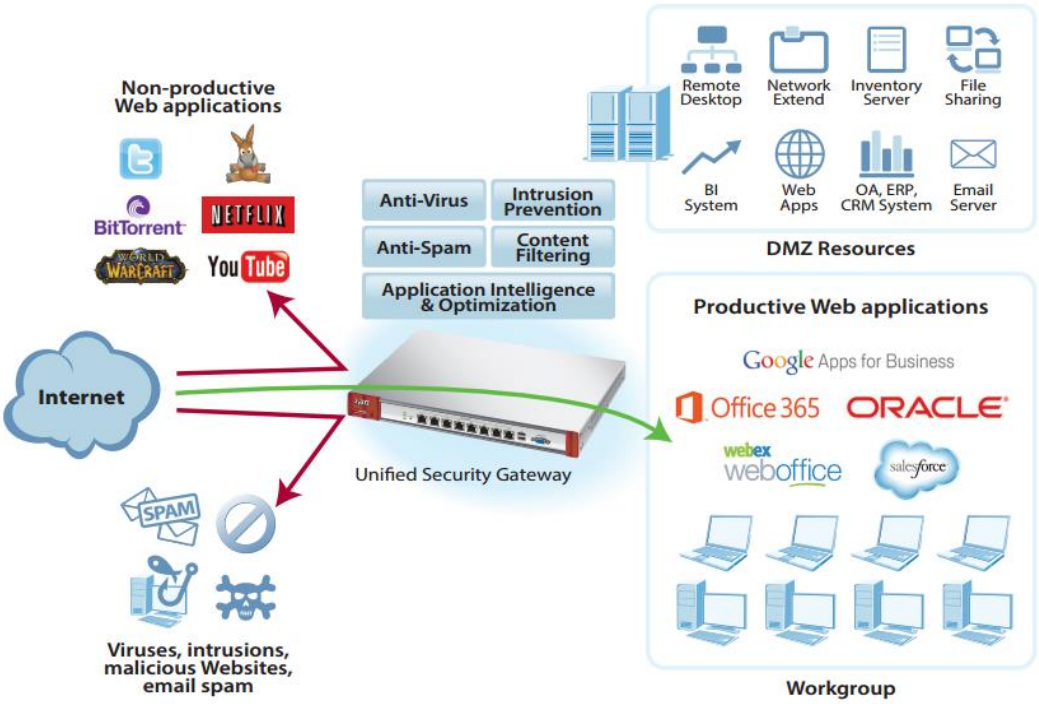
This document will provide a step-by-step list of instructions to create an App Patrol policy

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

App Patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols, instant messenger, Peer-to-Peer, Voice over IP, and streaming applications. The App Patrol UTM feature gives the network administrator the necessary tool to control what type of traffic is allowed on the network, allowing better control over network resources.


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.

Linked Services

Name	Remaining Amount	Total Amount	Trial	Status
Content Filter_Standard	396 days	396 days	Standard	Activate
Kaspersky Anti-Virus_Standard	396 days	396 days	Standard	Activate
IDP_Standard	396 days	396 days	Standard	Activated
Anti-Spam_standard	396 days	396 days	Standard	Activate
PKG_Update	1 piece	1 piece	Standard	Activated

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.

License Status

#	Service	Status	Registration Type	Expiration Date	Count
1	IDP/AppPatrol Signature Service	Licensed	Standard	2015-12-4	N/A
2	Anti-Virus Signature Service	Not Licensed			N/A
3	Anti-Spam Service	Not Licensed			N/A
4	Content Filter Service	Not Licensed			N/A
5	SSL VPN Service	Default			2
6	Managed AP Service	Default	Standard		2

Page 1 of 1 | Show 50 items | Displaying 1 - 6 of 6

License Refresh

Service License Refresh

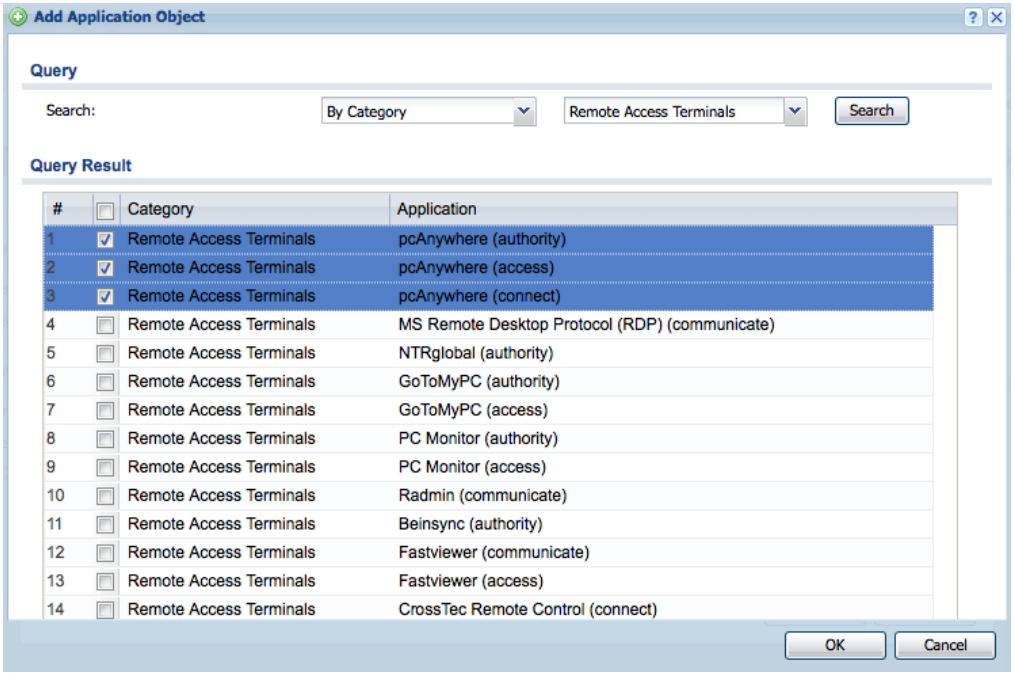
Download/Update Service Signatures

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 the App Patrol 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.

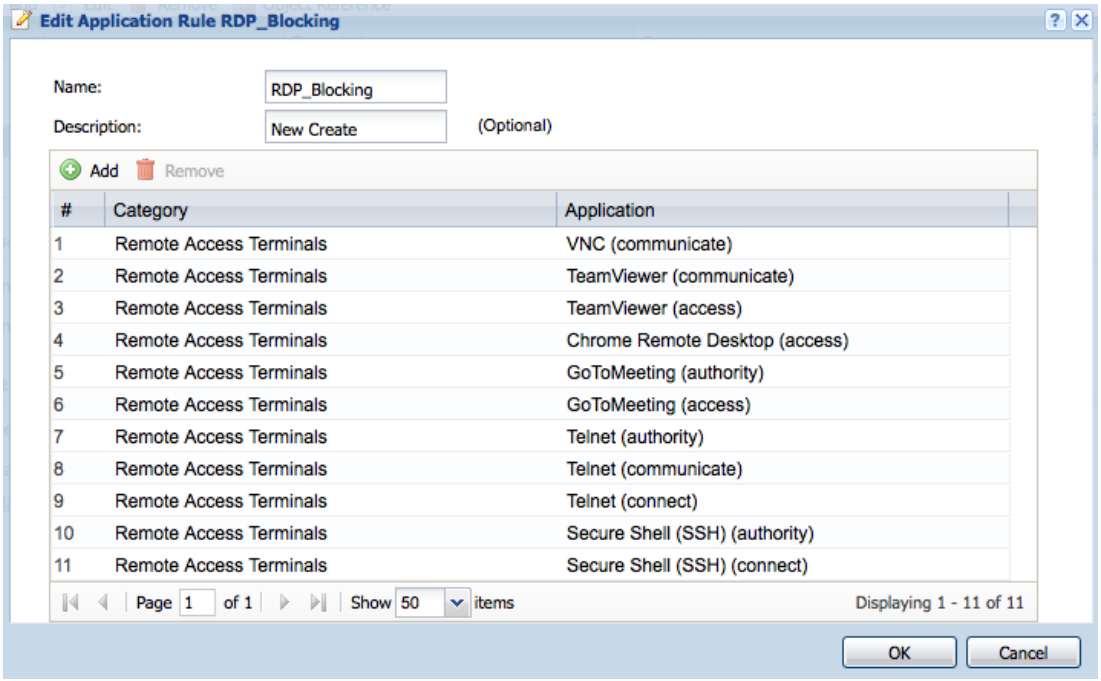
Application Object Setup

First step in configuring the AppPatrol service successfully on the USG router is to setup the application objects. To accomplish this go to menu **Configuration → Object → Application**. In the "Application" menu click the **Add** button to insert a new policy. On the rule editor window provide a name for the Application Object and click the **Add** button to select the services that will be members of this object. You can query the different supported services based on name or category. For this example we will be using the category query.

- Click the dropdown for the different category options and select the desired category to select the services you wish to add to the application object. For this example we will be selecting the "Remote Access Terminals" category.
- Scroll through the different services and check the box for those services you want to add to the member list.
- Click **OK** to add all the selected services to the member list.



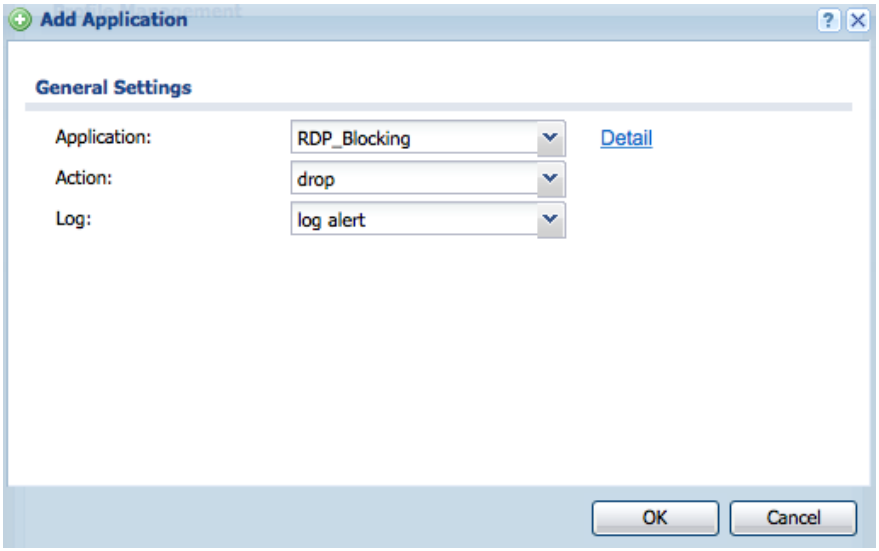
- You will now see a list of all the services you have added to the member list. Click **OK** to finish adding the Application Object.



AppPatrol Profile

Now that the application group(s) has/have been created we need to add them to an AppPatrol Profile. Go to menu **Configuration → UTM Profile → App Patrol** to insert the profile. Click the **Add** button to insert the profile.

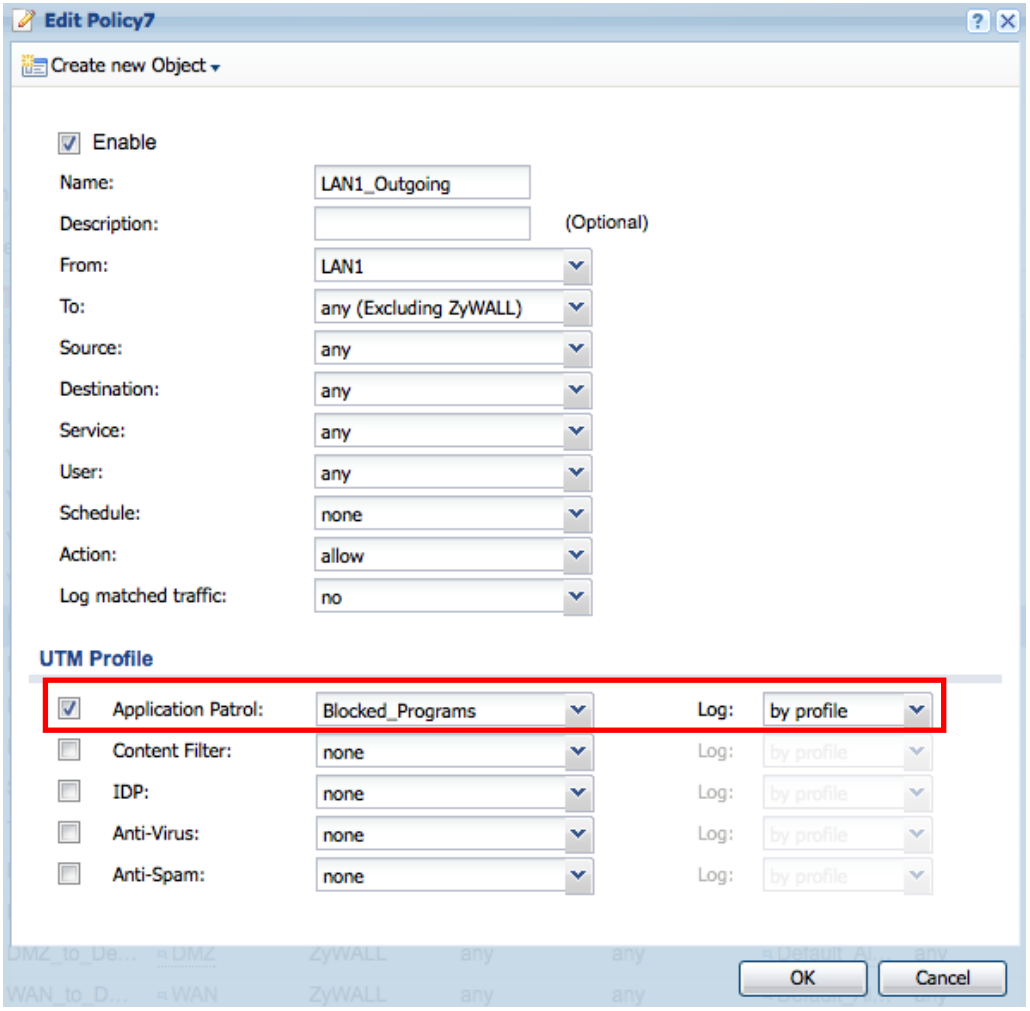
- Provide a name for the App Patrol profile.
- Under the "Profile Management" option click the **Add** button to insert application objects you wish to make part of the profile. Select what action to take when a service signature is triggered and whether you would like to log the traffic.



- Repeat the process to add any other application object to the App Patrol profile.

Policy Control Rule Setup

A policy needs to be created to apply the App Patrol services list against the network, users or certain IP address. The policy is very customizable so for this example we will be applying the service filter to the entire LAN1 zone. Go to **Configuration → Security Policy → Policy Control**. Find the LAN1_Outgoing policy and edit the rule. Scroll down to the "UTM Profile" feature and check the box to enable the Application Patrol, click on the dropdown and select the App Patrol profile to apply to this policy control rule.



Testing and Troubleshooting

To test if the App Patrol policy is working, open the application or website you have blocked. If the App Patrol block is based on a website the browser will just continue to try and load the page. If it is an application, it will fail to connect.
App Patrol not blocking the service:

- Reboot the router to close all open sessions. If there are open sessions to the service you are trying to block they will stay open until the TCP/UDP timeout occurs.
- Restart the application or clear the browsers cache.
- Check the Policy Control rule to make sure the computer you are using is part of the policy. Especially if you have selected a specific "Source Address" when you created the policy.
- Update IDP/AppPatrol signatures if running an older signature revision. To check what the current signature revision is go to http://mysecurity.zyxel.com/mysecurity/jsp/signature/signature.jsp
- Contact Tech Support for further assistance.