NOMADIX®

Alloc8 – How to Guide:

Anonymous Proxy Detection

Enable Anonymous Proxy Detection

The Anonymous Proxy service is disabled by default. In order to enable this feature, navigate to **Configuration > Objects > Applications > Anonymous Proxy** using the Web UI.

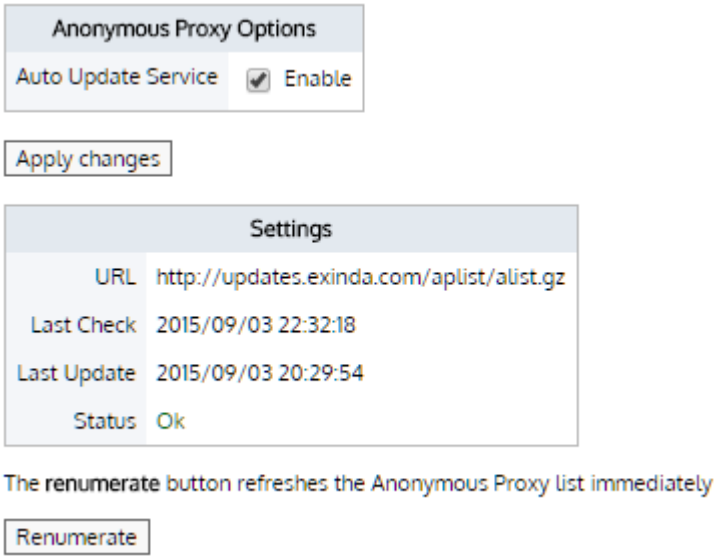

Figure 1: The form to configure and enable the Anonymous Proxy service.

This page allows you to enable the automatic update of the Anonymous Proxy service and also check when the definitions were last updated. The 'Renumerate' button allows you to force the Anonymous Proxy service to fetch the latest definitions immediately.

Given that Anonymous Proxies are constantly changing, the Anonymous Proxy service will automatically retrieve the latest Anonymous Proxy definitions from the Exinda servers on a daily basis. If the Anonymous proxy service is stopped or disabled the last retrieved definitions will be used for detection of Anonymous proxy.

> **Note** In order to receive daily Anonymous Proxy definition updates, the Alloc8 appliance must be able to contact the www.exinda.com web servers and the appliance must also have valid software subscription.

The Anonymous proxy ASAM is another component of the Anonymous Proxy detection. This works in combination with the Anonymous Proxy service and it is enabled by default.

To disable this Application Specific Analysis Modules (ASAM), navigate to **Configuration > System > Setup > Monitoring** using the Web UI. If the service is stopped and Anonymous proxy detection is no longer required, disabling the ASAM will clear the existing definitions.

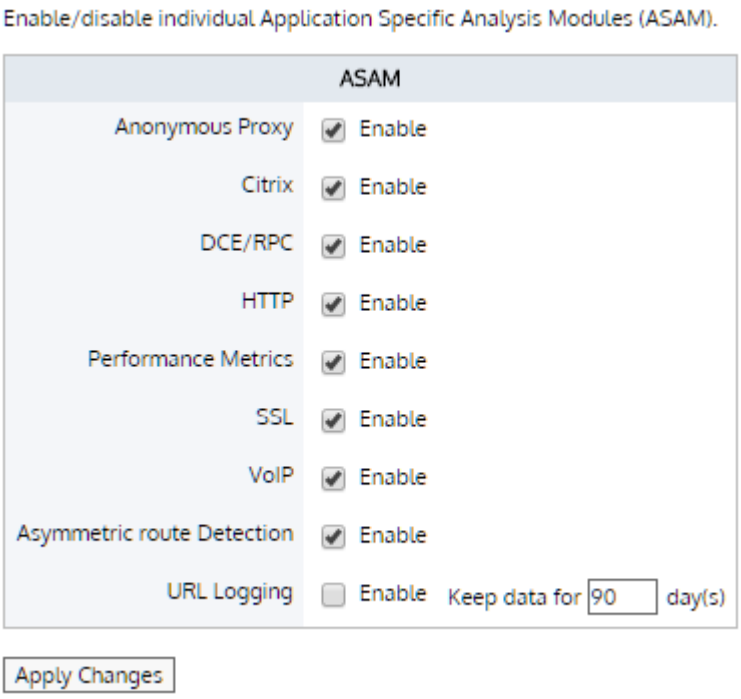

Figure 2: The form to enable/disable the Anonymous Proxy ASAM.

Control Anonymous Proxy Traffic

Once the Alloc8 appliance identifies traffic as an Anonymous Proxy, it is classified as the "Anonymous Proxy" application. This means that any Anonymous Proxy traffic will show up in the real-time monitoring screen and other monitoring reports as "Anonymous Proxy".

Inbound Applications

Application Name	Transfer Rate (kbps)	Packet Rate (pps)	Flows	Distribution (%)
Total	**177.348**	**52**	**129**	
HTTP	119.675	22	33	
IKE	26.096	7	17	
HTTPS	15.154	4	10	
IMAP-SSL	5.043	2	1	
Skype	3.448	4	36	
SSH	2.672	5	2	
Anonymous Proxy	2.184	2	7	
SMTP	1.806	4	2	
ICMP	0.530	1	4	
BitTorrent	0.506	1	3	
DNS	0.130	0	1	
ExindaCom	0.104	0	12	

Outbound Applications

Application Name	Transfer Rate (kbps)	Packet Rate (pps)	Flows	Distribution (%)
Total	**78.713**	**57**	**131**	
HTTP	41.652	26	33	
IKE	9.341	8	17	
HTTPS	5.634	5	10	
ssdp	5.268	1	2	
SSH	5.072	4	2	
SMTP	3.791	2	2	
Anonymous Proxy	2.745	2	7	
Skype	2.594	4	36	
IMAP-SSL	1.166	2	1	
ExindaCom	0.620	1	12	
ICMP	0.376	0	4	
BitTorrent	0.328	1	3	
DNS	0.105	0	1	

Figure 3: The Anonymous Proxy application is shown on the real-time monitoring screen.

It is also possible to create Optimizer Polices using the Anonymous Proxy application, like you would any other application. The Optimizer Policy configuration form below shows how to create an Optimizer Policy that will block Anonymous Proxies.

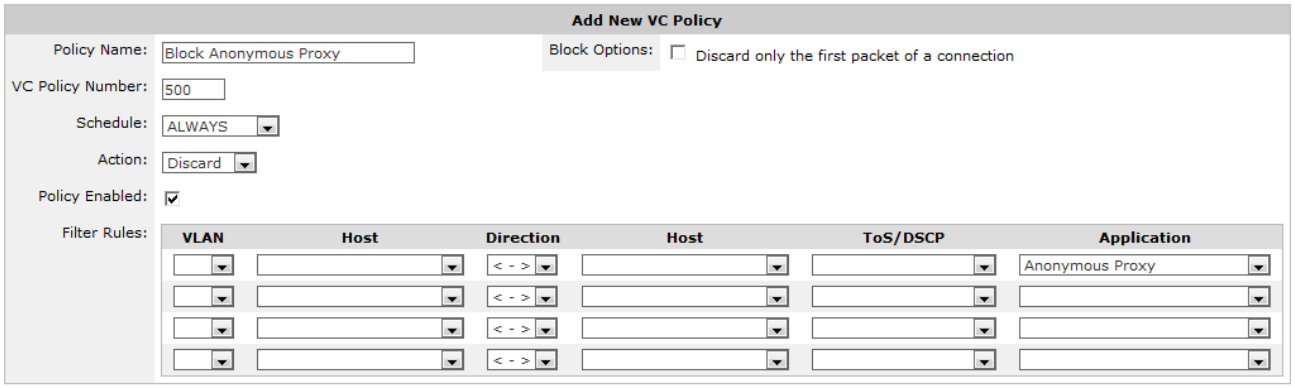

Figure 4: Blocking Anonymous Proxies using the Optimizer.

Note By default, the Anonymous Proxy application is part of the Recreational application group. This means that any policy that references the Recreational application group will also be referencing the Anonymous Proxy application. If you want to block Anonymous Proxies, the discard policy must be above any policy that references the Recreational application group.