UTM 5000 WannaCry Technote

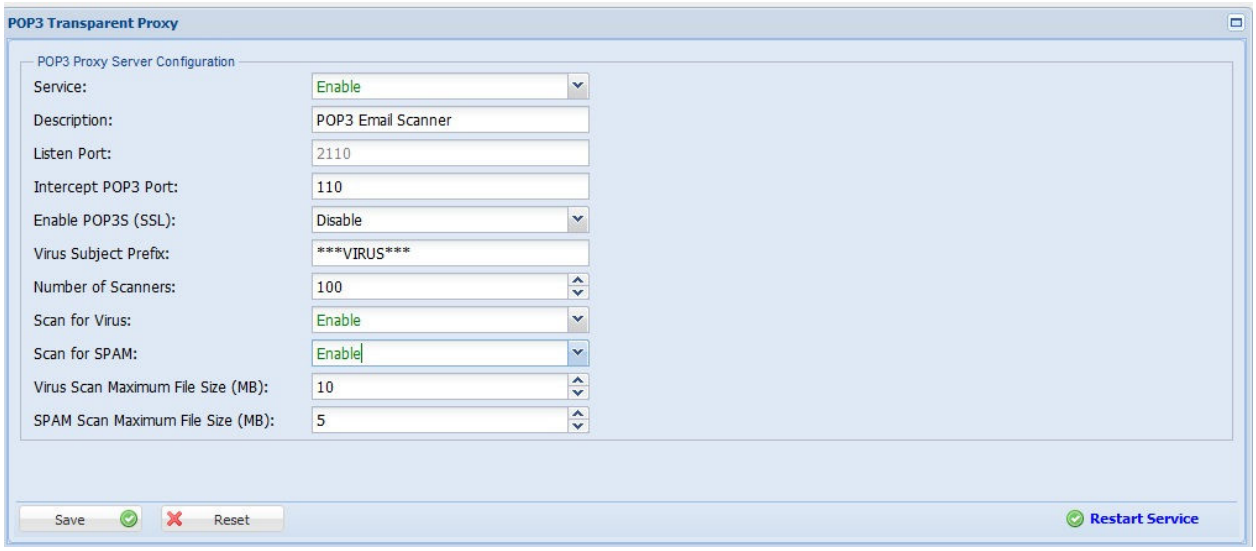
The news is full of reports of the massive ransomware infection caused by WannaCry. Although these security threats are pervasive, and ransomware has been around for a decade, what is new is this kind of diverse and integrated threat. WannaCry is so effective because it is all the worst threats at once. It is Ransomware backed by a Phishing scheme and an Exploit Kit web site and a Virus and a Worm and a Botnet. Only a Unified Threat Manager like the UTM-5000 can counter this kind of threat.

Arne Schönbohm, President of Germany's Federal Office for Information Security (BSI) states that "the current attacks show how vulnerable our digital society is. It's a wake up call for companies to finally take IT-security [seriously]".

The Wannacry ransomware payload is deployed if the target is susceptible any of the myriad exploits, so an ordinary firewall is totally inadequate. The UTM-5000 handles all of these threats simultaneously! The instructions for each WannaCry element, e.g. Botnets, can also be considered separately if you are only interested in stopping a particular exploit on the UTM-5000. Many exploits besides WannaCry use one or more of these known techniques.

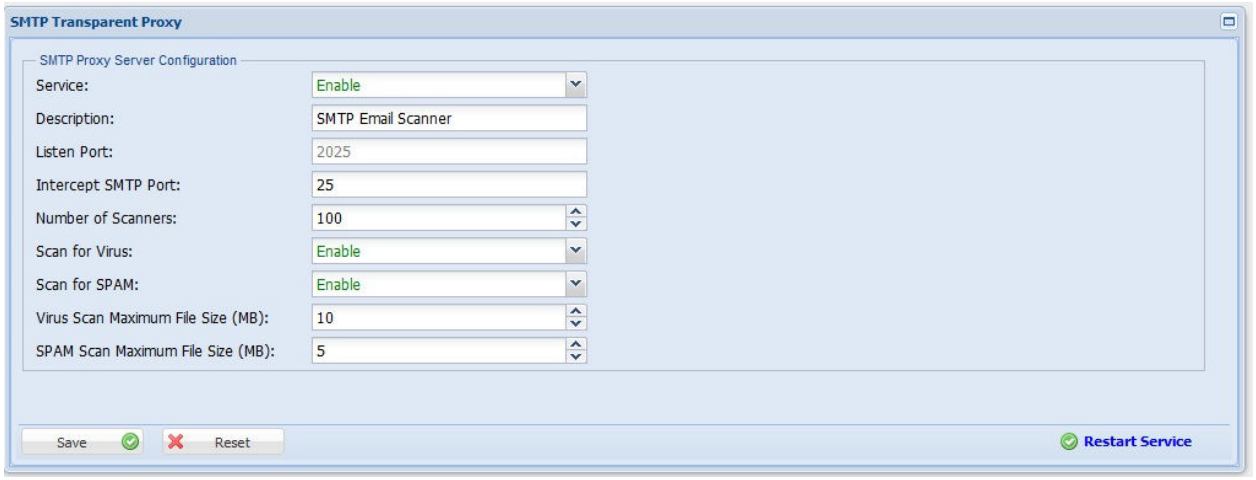
Phishing Virus

A Phising Email is a clever, or dumb, attempt to get a user to open an infected file from a SPAM (or targeted) email. The integrated email Virus Scanner on the UTM-5000 is always up to date and prevents both incoming and outgoing viruses in phishing emails. The Virus scanner for incoming and outgoing emails are configured separately. Incoming email, i.e. POP3, is configured under **Configuration - Email Security - POP3 Email Proxy.**

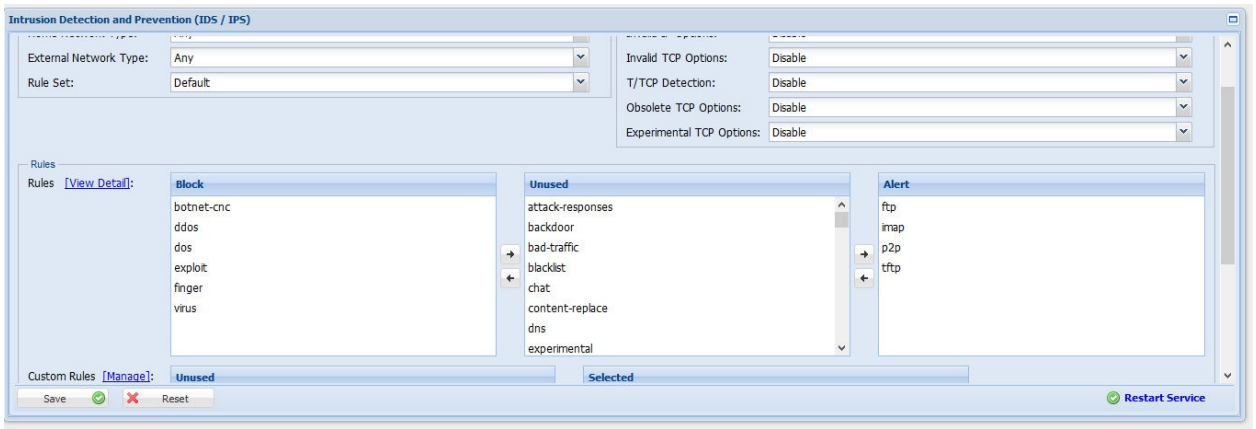


Enabling this service will flag virus containing emails before the user receives them. You can additionally configure the IDS/IPS system to alert or drop based on the flags.

Outgoing email, i.e. SMTP, is configured under Configuration - Email Security - SMTP Email Proxy.



Once incoming and outgoing emails are scanned you can configure the IPS/IDS system to drop virus flagged emails under **Configuration - Web Security - IDS/IPS.** Move the rules for "virus" from **unused** to the **block** or **alert** list by clicking the arrows.

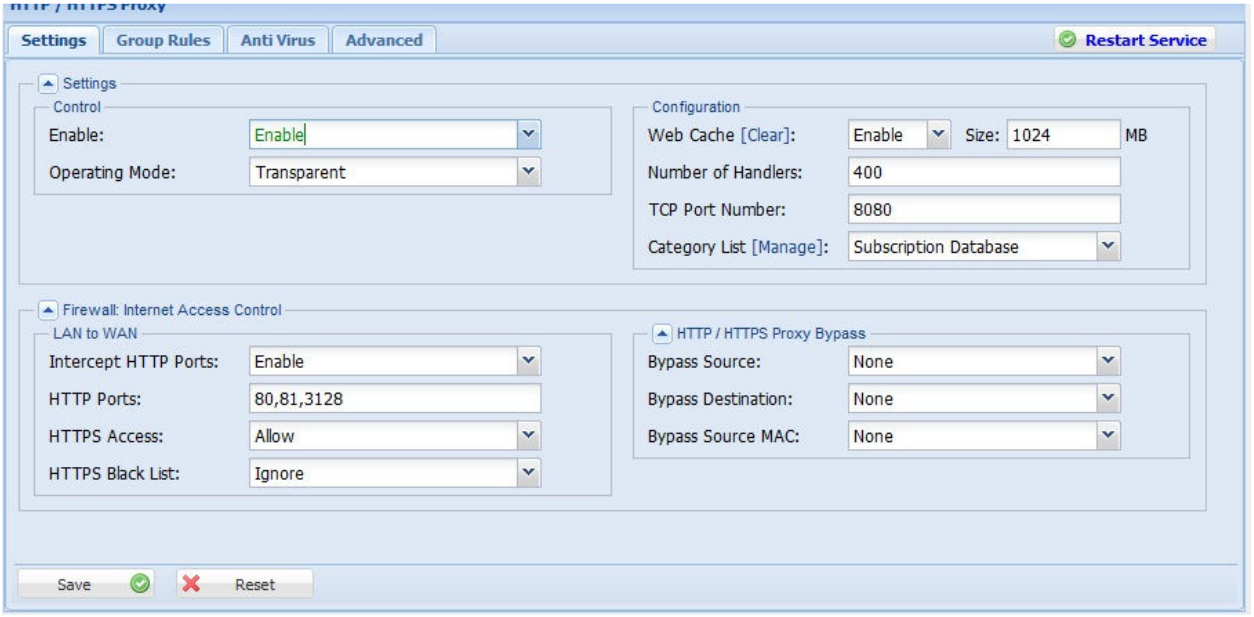


If you add virus emails to the block list they will be silently blocked by the UTM. Once you are finished with the settings select **Save** and **Restart Service**.

Exploit Kit Web Server

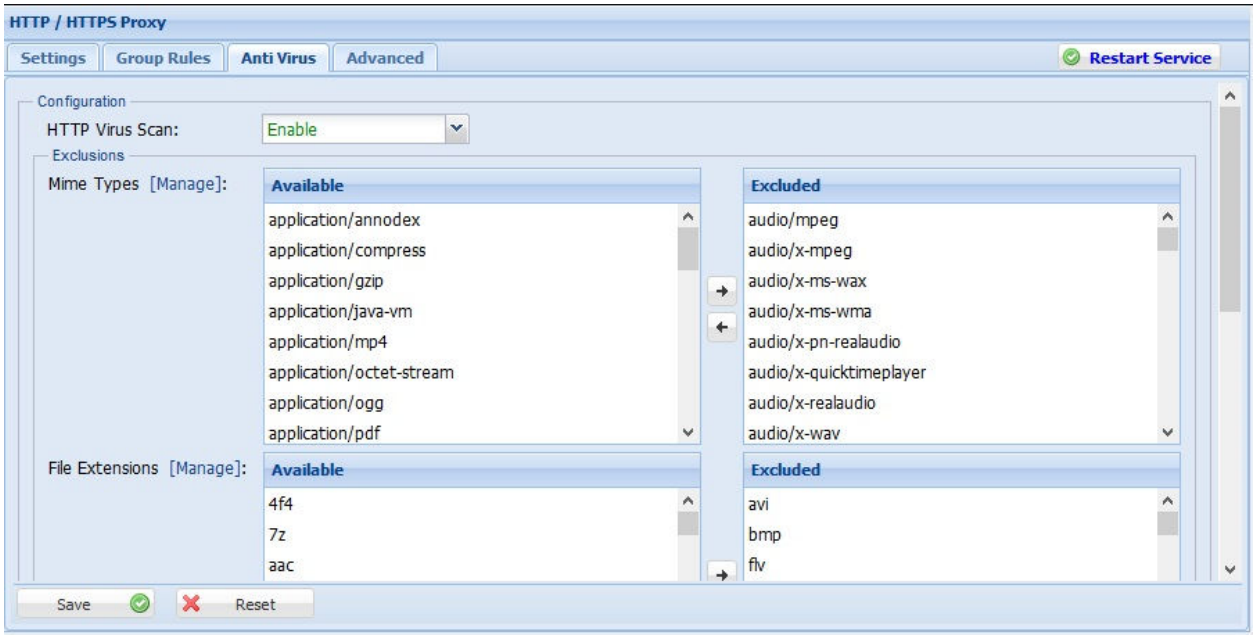
Phising emails may not contain actual virus files so as to avoid virus scanners. Instead they can contain links to exploited web servers with corrupted code that contains the virus. This virus may

attack the browser or any other web enabled application. These pages will fail to connect through the UTM-5000 Transparent Web Proxy. Dangerous web page code is blocked by Anti-Virus and known dangerous web sites can be blocked through content filtering. The dangerous site lists are kept up to date by the subscription service. The HTTP/S Proxy Service is enabled under **Configuration - Web Security - HTTP/S Proxy - Settings**.



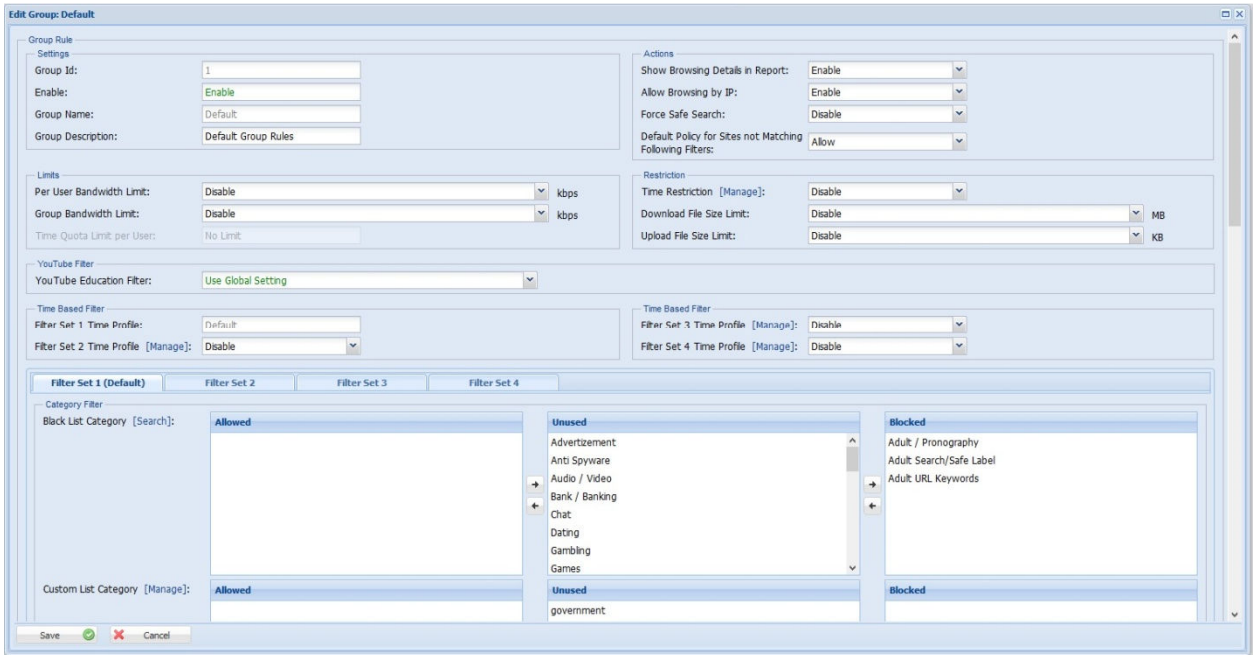
Once the service is enabled there are two components that work against dangerous web sites. There is Anti-Virus that blocks malicious code and Content Filtering the blocks a list of known dangerous web sites.

Anti-Virus is enabled under **Configuration - Web Security - HTTP/S Proxy - Settings**.



You will not need to change the other setting unless you have a very advanced application.

Content Filtering in controlled by group, with a Default Group covering everyone not otherwise assigned. If you are using multiple groups then review the settings you want for each group. The default group setting can be edited under **Configuration - Web Security - HTTP/S Proxy - Group Rules**. Click on the edit icon in the table for the default group. You may need to scroll down or enlarge the windows to see all the settings.

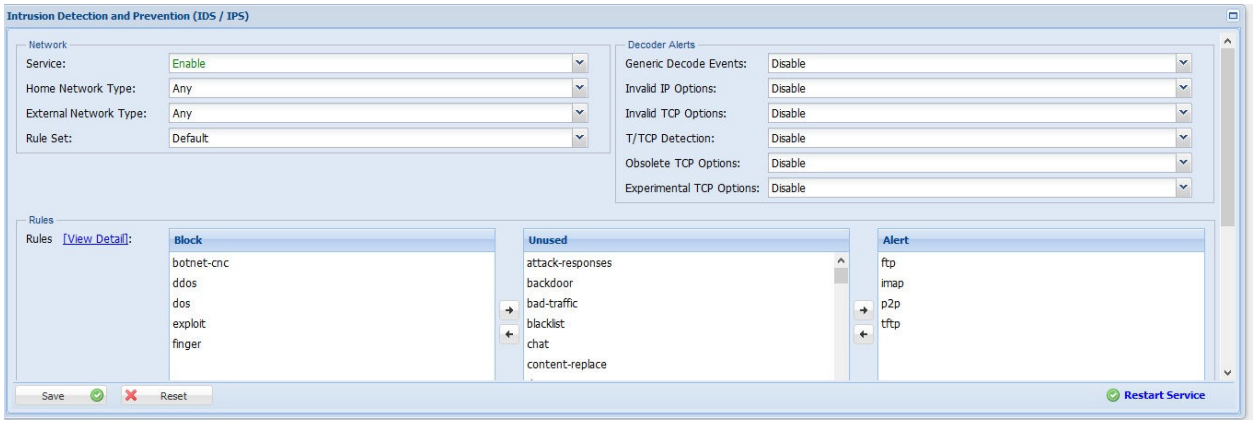


If you want to block content from known malware and phishing web sites, move those blacklist categories from "unused" to "active" using the arrow keys. Please note that pornography and adult web sites are blocked by default, so if you want your users to still enjoy that content move those categories to "unused". You can also leave the blocked list blank if you want to rely on the Anti-Virus and not block any content.

Once you are finished with the settings select **Save** and **Restart Service**.

DoublePulsar Botnet

Wannacry also installs the DoublePulsar backdoor, turning the device into an infected bot. Botnet computers create a slave network that can be exploited to send SPAM and mass DDOS attacks. The UTM-5000 Intrusion Detection Systems blocks botnet communication both incoming and outgoing. Botnets generate unwanted traffic congestion on your network and you may get warning letter from your ISP if your network has bots on it. The IDS/IPS system is enabled under **Configuration - Web Security - HTTP/S Proxy - IDS/IPS**.



Make sure IDS/IPS is enabled and move the "botnet" rule from **unused** to **block** by clicking on the arrow keys. Once you are finished with the settings select **Save** and **Restart Service**.

EternalBlue Worm

Infected devices attempt to propagate WannaCry automatically through a Windows vulnerability in the file sharing protocol. The UTM-5000 Intrusion Prevention System blocks known malware and corrupted SMB packets with an up to date threat list.

Conclusion

The WannaCry threat presents a workout for the many protections in your UTM system. Reviews the settings above and explore the additional rules, protections, and alerts you can implement on your UTM-5000.