



How to Prevent Ransomware and Other Advanced Malware

Including CryptoWall and CryptoLocker

The number of ransomware incidents has exploded in the last few years, infecting hundreds of thousands of systems worldwide. Ransomware is malware that's designed to hold your data hostage unless you pay up. Wait too long —or try to rescue it— and that data can be gone for good.

To protect your network and computers from ransomware and other malicious malware, be sure to first perform these fundamental tasks:

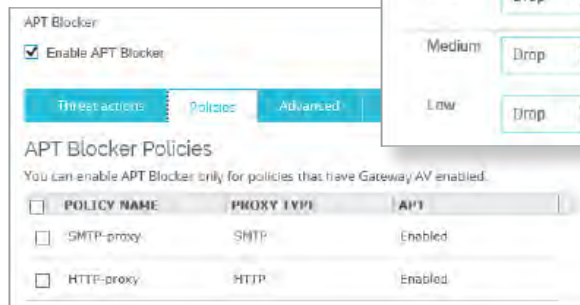
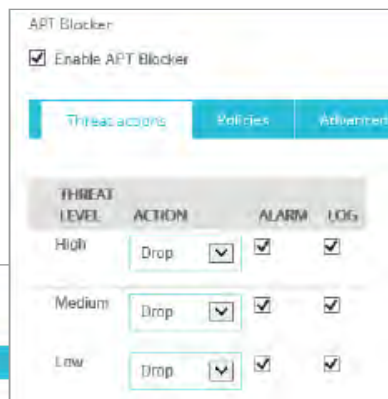
- Backup and recovery
- Segment BYOD (Bring Your Own Devices) from main network
- Run antivirus software on clients



Next, follow these steps on your Firebox for maximum ransomware protection:

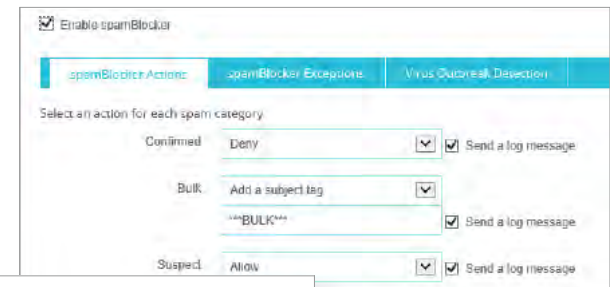
1. APT Blocker

- Enable APT Blocker on your HTTP, FTP, SMTP, and POP3 proxy policies.
- Enable the Alarm and Log options for email notifications.



2. spamBlocker

- Activate spamBlocker Wizard on your Firebox.
- Enable spamBlocker on your SMTP and POP3 proxies.



PROXY ACTION	FIREWALL POLICIES	TYPE	STATUS
SMTP-Incoming.1	SMTP-proxy	SMTP	Enabled
POP3-Client.Standard	POP3-proxy	POP3	Enabled



3. Signature Updates

- Make sure the signatures for Gateway AntiVirus, IPS, and Application Control are up to date.

4. Application Control

- Enable Application Control on all outgoing policies.
- Set action to Drop for the Crypto Admin application within Network Protocols.
- Block the following applications: BitComet, BitLord, BitTorrent Series, aMule, easyMule, eMule, eMule Plus.

CATEGORY	APPLICATION	BEHAVIOR	ACTION
<input type="checkbox"/> Network Protocols(3)	Cray Network Semaphore server	Connect	
<input type="checkbox"/> Network Protocols(3)	Cray SFS config server	Connect	
<input type="checkbox"/> Network Protocols(2)	Cray Unified Resource Manager	Connect	
<input checked="" type="checkbox"/> Network Protocols(2)	Crypto Admin	Connect	Drop
<input type="checkbox"/> Network Protocols(3)	Customer EXChange	Connect	
<input type="checkbox"/> Network Management	DCE-RPC	Access	
<input type="checkbox"/> Network Protocols(2)	DCTP	Connect	
<input type="checkbox"/> Network Protocols(3)	DDM-SSL	Connect	

5. WebBlocker

- Enable WebBlocker on your HTTP and HTTPS proxy policies.
- Make sure Extended Protection and Security are selected.

6. Gateway AntiVirus

- Enable Gateway AntiVirus on your HTTP, FTP, SMTP, POP3, TCP-UDP proxy policies.
- In the global Gateway AntiVirus settings, select the Enable Decompression option.
- In the HTTP Response > Content Types proxy action settings for Gateway AntiVirus, set the action to AV Scan.
- In the HTTP Response > Body Content Types proxy action settings for Gateway AntiVirus, set the action to Deny or AV Scan for .exe file .

PROXY ACTION	FIREWALL POLICIES	TYPE	STATUS
HTTP-Client-Standard.1	HTTP-proxy	HTTP	Enabled
SMTP-Incoming.1	SMTP-proxy	SMTP	Enabled
FTP-Client-Standard.1	FTP-proxy	FTP	Enabled

CONTENT TYPE	NAME	MATCH TYPE	VALUE	ACTION	LOG
AV Scan	exe*	Pattern Match	exe*		

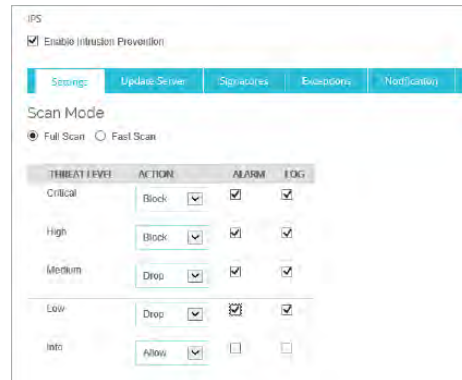


How to Prevent Ransomware and Other Advanced Malware



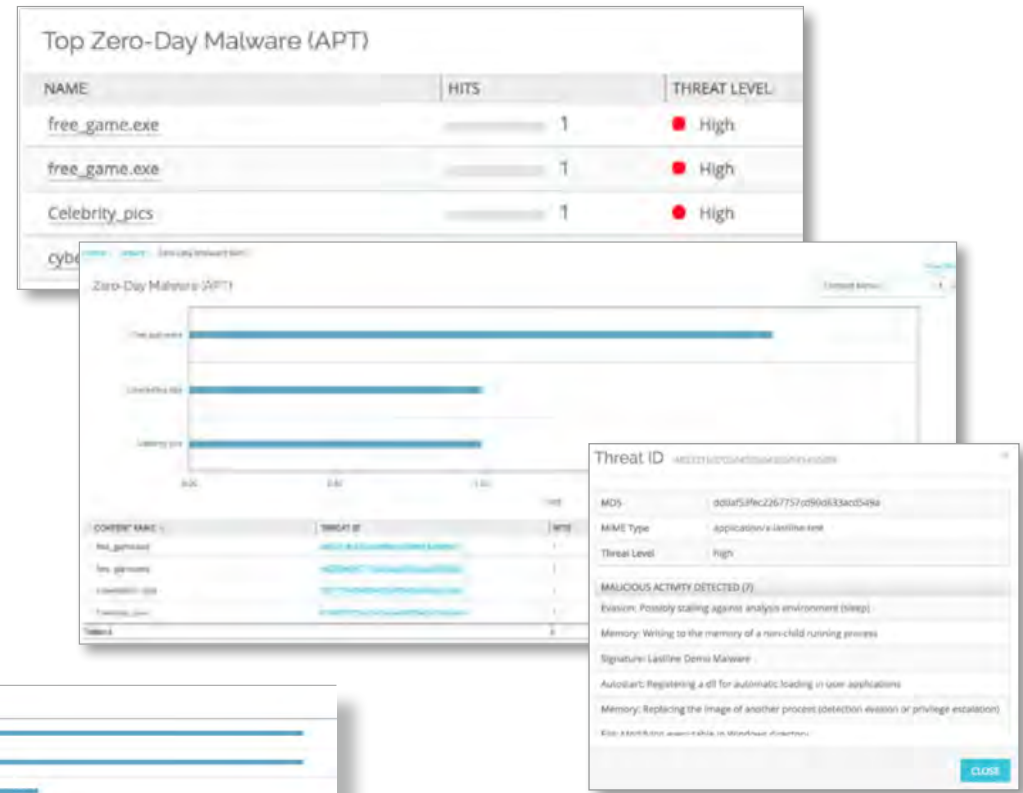
7. Intrusion Prevention (IPS)

- Enable IPS on all outbound policies.
- Set action to Block for Critical and High threat level traffic.
- Choose Alarm and Log for each threat level.
- Select Full Scan or Fast Scan depending on data sensitivity level.



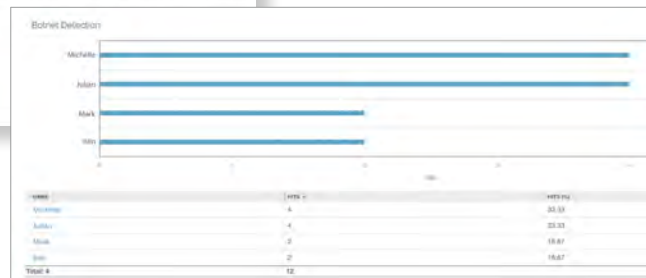
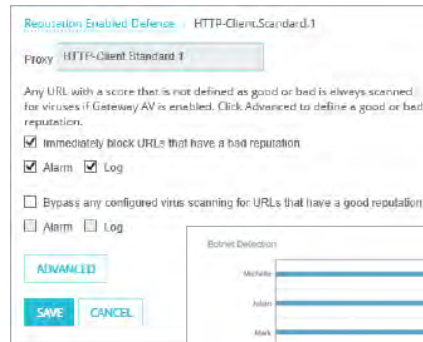
8. Dimension

- Use dashboard, logs, and reports to monitor for APTs and zero day malware.



9. Reputation Enabled Defense

- Enable Reputation Enabled Defense.
- Turn on the Alarm and Log options for notifications.
- Enable **Botnet Detection** - known botnet sites will be added to the Blocked Sites List



Protect your business and customers from ransomware and other malicious malware today.

For more information, visit www.watchguard.com/aptblocker.