Check Point
SOFTWARE TECHNOLOGIES LTD.

ONE STEP AHEAD

SandBlast – NGTX Threat Emulation Activation

The Goal of this document is to focus on enabling Threat Emulation in organizations that purchased the NGTX package, but have not activated the service.
In this document we will recommend activating the service using Background mode in detect mode. This will provide higher level of visibility, little to no change to the environment and won't risk or effect critical business processes.

Traditional Signature based solutions such as: Anti-Virus and IPS focus only on known Malware and known vulnerabilities. With hundreds of new forms of malware hitting every hour, how do you protect against what you don't know?

Check point SandBlast Zero-day solution employs Threat Emulation (SandBox) capabilities to elevate network security to the next level with evasion resistant malware detection, and comprehensive protection from the most dangerous attacks.

Threat Emulation uses Checkpoint's proprietary and unique CPU-level inspection, stopping even the most dangerous attacks before malware has an opportunity to deploy and evade detection. SandBlast Threat Emulation uses OS-level inspection to examine a broad range of file types, including executables and data files.
With its unique inspection capabilities, SandBlast Threat Emulation delivers the best possible catch rate for threats, and is resistant to attackers' evasion techniques.

The NGTX package adds Check Point's SandBlast Zero-Day Protection capabilities to your existing check point gateway. Organizations will benefit from this innovative zero-day threat sandboxing capability, within the SandBlast solution.

How to Enable Check Point's Zero Day Protection (Threat Emulation)

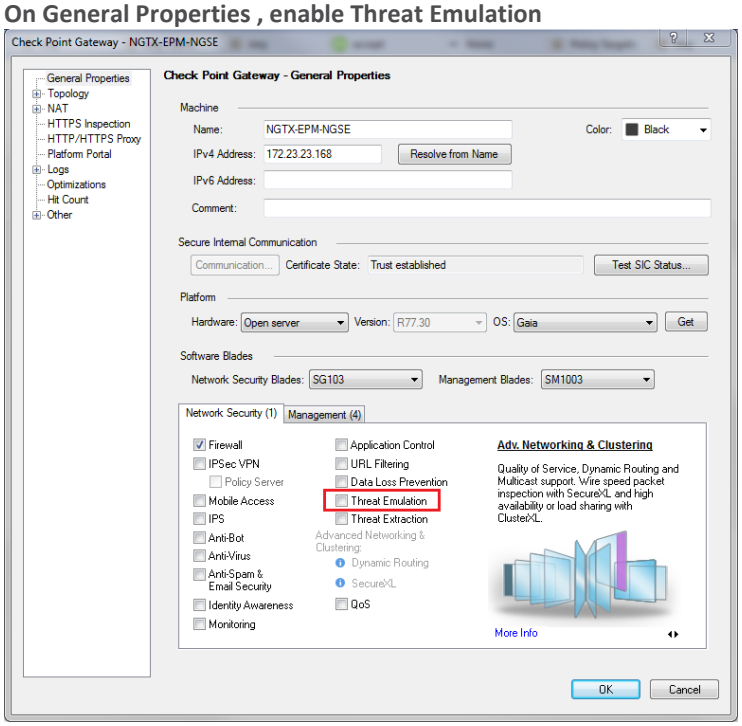
Before starting, please make sure the following apply:

a. Correct NGTX licenses and contracts are deployed on the GW
b. Support for SHA256 (either via relevant Jumbo HF or SHA256 HF)
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk103839&partition=General&product=All%22
c. Average CPU usage should be below 40% before enabling Threat emulation.

Note: Enabling threat emulation will increase the CPU load on the GW.
If the GW's average CPU is above 50% before enabling the threat emulation blade, please contact your local Check Point Security Engineer for further assistance.
*It is recommended that the average CPU utilization of any organizational GW will be under 50% in order to actively support organizational growth.
You can expect CPU increase of 5%-10% If Anti-Virus blade is already enabled, and if Anti-Virus isn't enabled than you can expect an average CPU increase of up to 20%

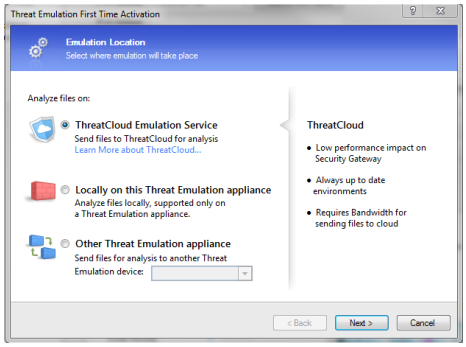
Activating Threat Emulation

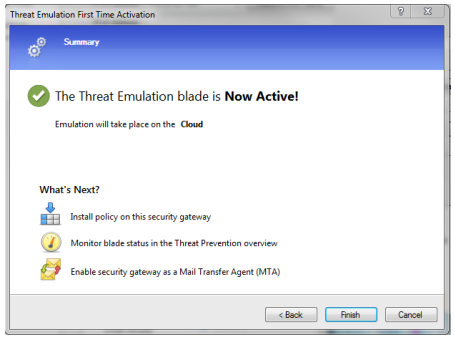
1. **Open Smart Dashboard and go to the GW Object you want to enable Threat Emulation on**
2. **On General Properties , enable Threat Emulation**



3. **The Threat Emulation First Time Wizard will be opened, and we will use the default option that is: Threat cloud emulation service.**

- TheartCloud Emulation Service option can be enabled on any CP GW, and files will be sent to Check Point's Cloud for emulation.





4. **There will be a connectivity and compatibility checks and if all is correct you will see a summery that indicates that threat emulation blade is now active, press finish.**
5. **Threat emulation is now activated (Threat Emulation check box is checked), to download engine updates please install policy**

- Updates schedule can be configured from the Threat Prevention tab under advanced->Updates

How to Set Threat Emulation to Background and detect mode

The advantages of using Threat Emulation in Background and detect mode

By using Background mode in detect mode. You will receive a higher level of visibility, little to no change to the environment and won't risk or affect critical business procedures.

Background mode enable files to be sent for emulation and at the same time will be passed to the users.

Combined with detect mode that will allow files to enter your organization even if they are found as malicious.

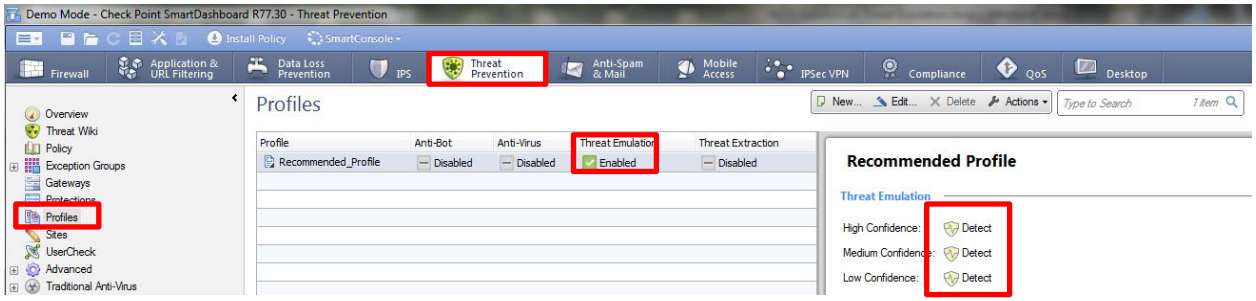
***This configuration will not block malware. It will only detect and inform the administrator.**

Using Check Point's Logs and Events will give you better understanding and higher level of visibility inside your network after enabling threat emulation.

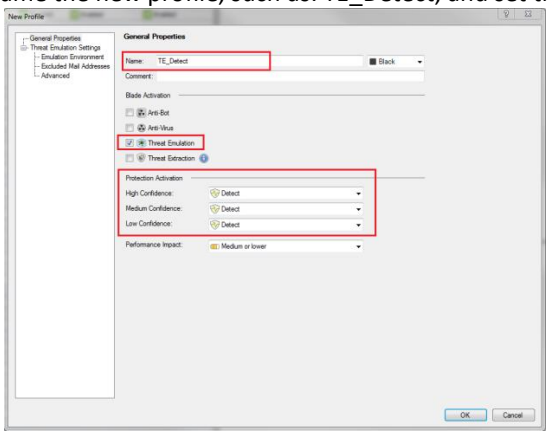
Check Point always encourages and promotes the use of prevent mode whenever possible.

1. **Configuring Detect mode and Background mode via profile and policy settings**

a. Navigate to Threat Prevention tab and then to profiles and create a new profile for threat emulation

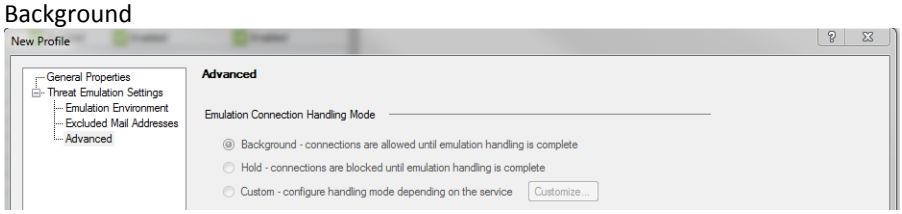


b. Name the new profile, such as: TE_Detect, and set the Protection Activations on all confidence levels to detect



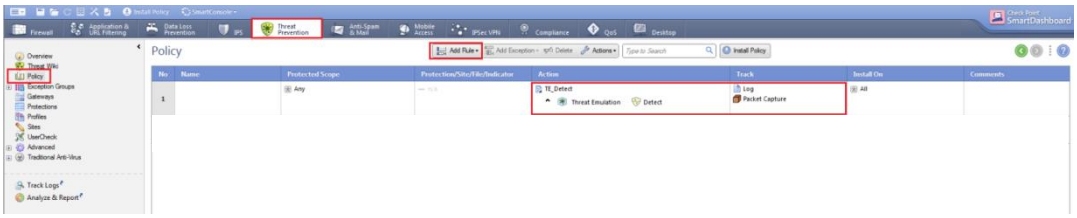
Please note that only The Threat Emulation blade is activated in this activation document.
More blades like Anti-Bot, Anti-Virus and Threat Extraction may be activated but certain consideration are needed.

- If you navigate to advanced tab you will notice that the Emulation Connection Handling mode is grayed out and set to Background



2. **Create a new threat prevention policy rule, above the current rules, with the newly created profile for Threat Emulation**

   This will insure that the Threat emulation policy will be set to Background and Detect mode and that it will have no effect on the current threat prevention rule base.



Please note that this setting will only enable Threat Emulation, please take under consideration if you have other Threat prevention blades active

3. **Install Threat Prevention policy to apply the changes**
4. **Open the Logs viewer, either Smart View Tracker or Smart Log, and filter Threat Emulation logs. Search the logs and verify that Threat Emulation Blade was updated successfully**
5. **Open an SSH connection to the GW, and run the following commands to verify that threat emulation is working and that GW's CPU usage is as expected.**

- '*top*' – this command will show you the average CPU usage of the GW (after running 'top' you can press 1 to view all CPUs and then SHIFT+W to save it)
- '*tecli show download all*' – to view that the updates and engine were downloaded successfully and are ready.
- '*tecli show cloud quota*' – to view the cloud quota and to verify the GW is connected to the cloud.
- '*tecli show cloud queue*' – to view the files that were sent to cloud emulation and their status.

```
[Expert@Delilah:0]# tecli show cloud quota

Quota identifier:                       9T32357
Quota subscription:                     OK (23 days left)
Assigned:                               3750 Hour / 75000 Month
Usage for gw:                           0 Hour / 0 Month
Usage for group:                        0 Hour / 0 Month
License state:                          ALLOW
Remain:                                 3750 Hour / 75000 Month
Exceeded:                               0 Hour / 0 Month
Next reset:                             8 Mins / 14 Days
Last update gw time:                    Wed Jan 18 11:06:36 2017
Last update server time:                Wed Jan 18 10:51:46 2017 GMT
Last update status:                     OK
Has contract:                           Yes
Gateway identifier:                     669a5446af0ec4cb831cf3ce69205cfc-bb34b84df943d785a
752ff5410abd99c
```

```
[Expert@Delilah:0]# tecli show cloud queue

|file's sha1                              |file's event_id                          |file type |insert time       |status
|-----------------------------------------|-----------------------------------------|----------|------------------|-----------------------------------------
|0a33f193bcfa8cc56d827436a16b4bc4708b8412|{00000020-0053-004D-A8FD-3EB4B48C4BB8}  |exe       |7 Minutes         |Uploaded to Cloud, waiting for response.
|0c7c0eabeb6d58e978d7dc9a931ef7cbb1a649ab|{00000057-0033-0046-838A-C4B50E27D9DC}  |scr       |7 Minutes         |Uploaded to Cloud, waiting for response.
|10db9cf76ff1687e41c316a3678572303b193aac|{00000077-00B6-0045-AED2-62FD3DB48956}  |exe       |7 Minutes         |Uploaded to Cloud, waiting for response.
|14cbeb607aec336cca5522b39c702486362e9040|{00000069-00B8-0049-9CD1-57D7A08DFD5C}  |scr       |7 Minutes         |Uploaded to Cloud, waiting for response.
|17cde5de5ca732f6f9f2d1b2b3408a4f37ca827a|{000000AA-008C-0044-A453-12695B063256}  |jar       |7 Minutes         |Uploaded to Cloud, waiting for response.
|1a04a68aa8b06992418aafdd1c62e72e07495d2c|{0000008F-006C-0041-81D4-5A3D18B0F434}  |doc       |7 Minutes         |Uploaded to Cloud, waiting for response.
|1a6bca62e0ac2937e3eaa374c7d62fdc21ee55ff|{00000057-00C8-0042-A4C6-4EF0457248C7}  |xls       |7 Minutes         |Uploaded to Cloud, waiting for response.
|27676d86f57c7231d6da092a152c2ea779b34773|{00000085-008B-0046-A343-B276F95A34C4}  |jar       |7 Minutes         |Uploaded to Cloud, waiting for response.
|21e3845d51d69a9d8a229c00e40cc19af76762a4|{0000009C-00A1-0048-8AFE-42253F3C0A61}  |doc       |7 Minutes         |Uploaded to Cloud, waiting for response.
|3314bf9a08955082cc17c7c27447b4e3cf073ab5|{00000036-009E-004C-9E96-C24EE80E3020}  |doc       |7 Minutes         |Uploaded to Cloud, waiting for response.
|1b4c91f56544301 4f66993f4ec828018d6b1398b|{0000006A-00FF-004B-864F-23652BA1BEBE}  |swf       |7 Minutes         |Uploaded to Cloud, waiting for response.
|363167d9965ca8b034c8f8a80a049ba6dd95037a|{0000001E-0027-0041-88F3-85DE098AF9A9}  |xls       |7 Minutes         |Uploaded to Cloud, waiting for response.
```

After a learning period we highly recommend that you move from detect mode to **prevent mode.**
Please note that in order to move to prevent it is recommended that you consult with your local Security Engineer.

