

## 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) <u>https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\_doGoviewsolutiondetails=&solutionid=sk103839&partition=General&product=All%22</u>
- 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

General Properties	Check Point Gate	way - Gene	eral Properties				
I opology ■ NAT	Machine						
HTTPS Inspection	Name:	NGTX-EPN	I-NGSE			Color:	Black
- Platform Portal	IPv4 Address:	172.23.23.1	168	Resolve from Nar	me		
- Logs	IPv6 Address:				_		
- Hit Count	Comment						
• Other	Comment.						
	Secure Internal Co	mmunication	ı ——				
	Communicatio	n Certific	ate State: Trust	established		T	est SIC Status
	Platform						
	Fiduoini						
	Hardware: Op Software Blades Network Secur	ty Blades:	Version:	R77.30 -	os: Gaia	SM1003	• Ge
	Hardware: Op Software Blades Network Security Vetwork Security	ty Blades: S	Version: GG103 gement (4) Application	R77.30   Manageme Control	os: Gaia ent Blades: (	SM1003 vorking & Clus	▼ Ge
	Hardware: Op Software Blades Network Security Vetwork Security Firewall	ity Blades: S	Version:  GG103  pement (4)  Application URL Filteri	R77.30  Manageme Control ng	ent Blades: ( Adv. Netv Quality of S	SM1003 vorking & Clus	
	Hardware: Op Software Blades Network Security Vetwork Security Firewall IPSec VPN	ty Blades: S (1) Manag	Version:  GG 103  Gement (4)  Application URL Filteri Data Loss	R77.30  Manageme Control ng Prevention	Adv. Netv Quality of S Multicasts	SM1003 vorking & Clus Service, Dynamic upport. Wire spe with SecureXI a	Case     Stering     Seturing and     sed packet     mod binh
	Hardware: Op Software Blades Network Security V Firewall IPSec VPN Policy S Mobile Acc	en server ty Blades: (1) Manag ierver ess	Version:  GG103  GG103  Application URL Filteri Data Loss Threat Em	Manageme     Manageme     Control ng Prevention ulation	Adv. Netv Quality of S Multicast s inspection availability ChateXM	SM1003 vorking & Clus Service, Dynamic uppot. Wire spe with SecureXL a or load sharing v	Case     Stering     character     char
	Hardware: Op Software Blades Network Securit V Firewall IPSec VPN Mobile Acc IPS	ty Blades: S (1) Manag	Version: GG103 gement (4) Application URL Filter Data Loss Threat Em Threat Em Advanced Networ	Manageme     Manageme     Control     ng     Prevention     udation     reaction	Adv. Netv Quality of 3 Multicast s inspection availability Cluster/L.	SM1003 vorking & Clus Service, Dynamic uppot, Wite spe- with SecureXL a or load sharing v	Cat     Stering     Shouting and     ind high     with
	Hardware: Op Software Blades Network Security V Firewall IPSec VPN O Policy S Anti-Bot Anti-Bot	en server ty Blades: S ( (1) Manag ierver ess	Version: GG103 gement (4) Application URL Filteri Data Loss Threat Em Threat Em Advanced Networ Clustering: Durario 6 Durario	R77.30  Manageme Control ng Prevention utation raction king & 20 utation	os: Gaia ent Blades: ( Adv. Netv Quality of S Multicast s inspection availability ClusterXL.	SM1003 vorking & Clus Service, Dynamic uppot. Wire spec with SecureXL a or load sharing v	Cat
	Hardware: Op Software Blades Network Securit V Firewall IPSec VPN Objects IPS Anhibot Anhibot Anhibot	erver	Version:  GG103  gement (4)  Application URL Filter  Data Loss  Threat Em  Threat Em  Custering:  Dynamic F  SacureM	Control     rection     detain	Adv. Netv Adv. Netv Quality of 3 Multicast s inspection availability ClusterAL	SM1003 vorking & Clus Service, Dynamic uppot, Wire spec with SecureXL a or load sharing v	Cae
	Hardware: Op Software Blades Network Securt Firewal IPSec VPN Policy S AnthRot AnthRot Email Securt Email Securt Email Securt Email Securt Email Securt	erver (1) Manag (1) Manag (erver ess (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	Version:  SG103  gement (4)  Application URL Filter Data Loss Threat Ext Avanced Networ Clustering:  Dynamic F SecureXL Doss	Manageme     Manageme	Adv. Netv Adv. Netv Quality of S Multicast s availability ClusterXL.	SM1003 vorking & Cluss Service, Dynamic upport. Wire spe with SecureVL a or load sharing v	clering cleri
	Hardware: Op Software Blades Network Securt Verwork Securt Picewal Policy S Anti-Bot Anti-Bot Emal Secu I dentily Aw Motiona	erver (1) Manag (1) Manag (erver ess ) (arnerss	Version:  GG103  GG103  GG103  Application URL Filteri Data Loss Threat Ext Advanced Networ Cluttering Dynamic F SecureML QoS	Manageme     Manageme     Manageme     Prevention     utation     Routing	Adv. Netv Quality of 3 Multicast s inspection availability Cluste/QL	SM1003 vorking & Clus Service, Dynamic uyopt. Wire type with SecureX1, a or load sharing v	Cee
	Hardware: Op Software Blades Network Securt IPSec VPN Mobile Acc IPS Anti-Span Secure Identity Aw Monitoring	ty Blades: (1) Manag (1) Manag	Version: SG103  amenet (4)  Application URL Filter Data Loss Threat Em Threat Em Chatenge Secured L Qas	Manageme     Manageme     Manageme     Manageme     Manageme     Manageme     Acoution     Acouting	Adv. Netv Quality of 3 Multicast s inspection availability Clustekd More Info	SM1003 vorking & Cluss Service, Dynamic upport. Wrie spe with Secure24, a with Secure24, a	Cee

- 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



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

N	ew Profile	Down	8 23
	General Properties	Advanced	
	Emulation Environment Excluded Mail Addresses	Emulation Connection Handling Mode	
L	Advanced	Background - connections are allowed until emulation handling is complete	
		Hold - connections are blocked until emulation handling is complete	
		Custom - configure handling mode depending on the service	

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.

Overview	* Policy	- HELLING	High Add Rule • High Add Esco	otion = spft Delete 🥜 Actions •	Q Initial Policy		0010
Threat Wild	No Name	Protected Scope	Protection/Site/File/Indicator	Action	Track	Justali On	Comments
Exception Groups           Gateways           Prefectors           Prefectors           States           Vertifies           Vertifies           Vertifies           Vertifies           Prefectors           Prefectors	1	itt Any		R_Detect * It Detect Emulation So Detect	🕼 Log 🌀 Packet Capture	(j) A8	
Treck Logs <sup>e</sup> Analyze & Report <sup>e</sup>							

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.



file's sha1	file's event_id	file type	insert time	status
  0.335f193bcfa8cc564827436a16b4bc4708b8412  0c7c0eabeb6d58e978d7dc9a931ef7cbb1a649ab  10db9cf76ff1687e41c316a3678572303b193ac  14cbeb67ac336cc5522b39c702486362e900  17cde5de5ca733f6f9f2d1b2b3408a4f37ca827a  1a04a66aa5b069241baafdd1c627e2c07495dc  1a6bca62e0ac2937e3eaa374c7d62fdc21ee55ff  27676d86f57c7231d6da092a152c2ea779b34773  21e3845d51d63a9d8a229c00e40cc19af7676224		  exe  scr  scr  jar  doc  xls  jar  doc	17 Minutes 17 Minutes 17 Minutes 17 Minutes 17 Minutes 17 Minutes 17 Minutes 17 Minutes 17 Minutes	Upploaded to Cloud, waiting for response. [Upploaded to Cloud, waiting for response.
3314bf9a08955082cc17c7c27447b4e3cf073ab5  1b4c91f565443014f66993f4ec828018d6b1398b  363167d9965ca8b034c8f8a80a049ba6dd95037a	{0000036-009E-004C-9E96-C24EE80E3020}  {000006A-00FF-004B-864F-23652BA1BEBE}  {0000001E-0027-0041-88F3-85DE098AF9A9}	doc  swf  xls	7 Minutes  7 Minutes  7 Minutes	Uploaded to Cloud, waiting for response. Uploaded to Cloud, waiting for response. 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.