

## POC Guide

Version 9.1

## Contents

1.	Change Log.....	5
2.	How to use this document .....	7
3.	Licensing and Appliances .....	8
3.1	Public Cloud and Appliance quota and licensing .....	8
3.2	Supported Private Cloud emulation devices .....	9
3.3	NGTX licensing .....	10
4.	PoC Implementation Examples .....	11
4.1	General considerations .....	11
4.2	Mirror (SPAN) mode .....	13
4.3	SMTP/TLS Prevent (MTA) and HTTP (SPAN).....	14
4.4	Production CP Gateway HTTP/S (Inline) and SMTP/TLS (MTA) .....	16
4.5	SandBlast – Ports needed between GUI/GW/SB .....	17
5.	Sizing PoC and Production environment.....	18
6.	Installing a Sandblast appliance .....	19
6.1	Stand-alone vs. multiple private cloud.....	19
6.2	TE-X Appliance ISO.....	19
6.3	R77.30 Management AddOn .....	20
6.4	Enable Hyper-Threading.....	20
6.5	Recommended Jumbo Hotfix – R77.30/R80.10(EA) .....	20
6.6	Updating TE images and engine .....	21
6.6.1	General info and configuration .....	21
6.6.2	Online Update .....	22
6.6.3	Offline Update .....	23
6.7	CPU-Level Threat Detection.....	24
7.	Configuration.....	25
7.1	General Considerations .....	25
7.2	Anti-Virus and Anti-Bot configuration .....	26
7.3	IPS.....	29
7.4	Threat Emulation.....	30
7.4.1	TE Images.....	30
7.4.2	Minimum recommended images .....	31
7.4.3	Hybrid mode.....	31
7.4.4	Multiple Private Cloud appliances .....	31
7.4.5	TE filetypes .....	32
7.4.6	Different “Links inside mails/documents” features .....	33
7.5	MTA.....	34
7.5.1	Show currently installed Postfix version .....	34
7.5.2	General MTA settings .....	34
7.5.3	BCC mode.....	35
7.5.4	How-to block file extensions in Postfix .....	37
7.5.5	Recommended MTA Best-Practises .....	38
7.5.5.1	Raising the MTA header length limit .....	38
7.5.5.2	Setting a Postfix hostname .....	39
7.5.5.3	Upstream MTA delivery issues (tcp_timestamp) .....	40
7.5.5.4	Implementing cleanup script.....	41
7.5.5.5	Next hop redundancy / failover .....	41
7.5.5.6	Outgoing TLS.....	41
7.5.5.7	Special considerations when using MTA on a gateway cluster .....	42
7.5.5.8	Feed MTA logs into SmartView Tracker / SmartLog.....	44
7.5.5.9	/var/log/maillog size for PoC.....	46

7.5.5.10	Debugging and Performance Troubleshooting Kit .....	47
7.6	SmartEvent .....	48
7.6.1	How to configure e-mail alerts for High and Critical TE events .....	48
7.6.2	Bugfix for TE events with more than 3 malicious images .....	52
8.	ICAP .....	53
8.1	ICAP Server .....	54
8.2	Configuration .....	54
8.2.1	Configuration files .....	54
8.2.2	Configure emulation images .....	55
8.2.2.1	All or recommended images .....	55
8.2.2.2	Configure specific emulation images .....	55
8.2.2.3	Adding Windows 10 image for ICAP emulation .....	56
8.2.3	Attaching an ICAP Client .....	56
8.3	Logging .....	57
8.3.1	General logging .....	57
8.3.2	Enable logging of benign files .....	57
8.3.3	Debug logging .....	57
8.4	ICAP daemon troubleshooting .....	58
8.4.1	Start manually and get errors on startup .....	58
8.4.2	Verify ICAP daemon is running .....	58
8.5	Sample configurations .....	59
8.5.1	SQUID proxy .....	59
8.5.1.1	SQUID compilation flags and version .....	59
8.5.1.2	SQUID sample configuration .....	59
8.5.2	McAfee Web Gateway 7.6 .....	61
8.5.2.1	Configuring the Check Point ICAP Server .....	61
8.5.2.2	Configuration McAfee ICAP client .....	62
8.6	ICAP Miscellaneous .....	71
8.6.1	Add "Protection Type: ICAP emulation" to SmartLog/Event searches .....	71
8.6.2	Access.log – available log variables .....	72
8.6.3	ICAP Server response codes .....	73
9.	Threat Extraction .....	74
9.1	Out-of-the box .....	74
9.2	Parallel/Serial mode .....	74
9.3	Add option to "send original email" .....	74
9.4	Demo via Web Browser Plugin .....	75
9.5	Demo with MTA environment .....	75
10.	TE/TX API .....	76
10.1	TE API documentation .....	76
10.2	Enabling API ports .....	76
10.3	Enabling API logging .....	77
11.	Testing & Troubleshooting .....	78
11.1	I have a problem - where is the log ? .....	78
11.2	Test emulation .....	79
11.3	Image/Engine Update .....	79
10.3.1	Check image and detection rule versions .....	79
10.3.2	Check TE engine version .....	80
10.3.3	Check ThreatCloud Update server connectivity .....	80
10.3.4	Remove all images and start again .....	81
10.3.5	Force update from CLI .....	82
10.4	Useful TECLI commands .....	83
10.5	Useful MTA/Postfix commands .....	84
10.6	How-to send an email with attachment from CLI .....	85
10.7	SNMP Monitoring .....	86

10.7.1	TE SNMP OIDs .....	86
10.7.2	Extend SNMP Monitoring .....	89
10.7.2.1	Enable SNMP.....	89
10.7.2.2	Extend available SNMP OIDs.....	89
10.7.2.3	Postfix mailqueue monitoring script.....	90
10.7.2.4	Email queue monitoring script .....	90
10.7.2.5	Running VM instances monitoring script.....	90
10.7.2.6	Test extended SNMP values .....	91
10.8	How-to handle False-positives/False-negatives during a PoC .....	92
10.8.1	False-negatives.....	92
10.8.2	False-positives .....	92
10.9	How-to issue a license via User Center .....	93
10.9.1	Cloud emulation .....	93
10.9.2	Local emulation.....	95
10.10	Miscellaneous .....	96
10.10.1	Getting data behind empty TE forensic reports.....	96
10.10.2	Set TED.ELG logsize and logrotate .....	99
10.10.3	Blocking filetypes inside archives .....	101
11.	Important SKs and hotfixes.....	102

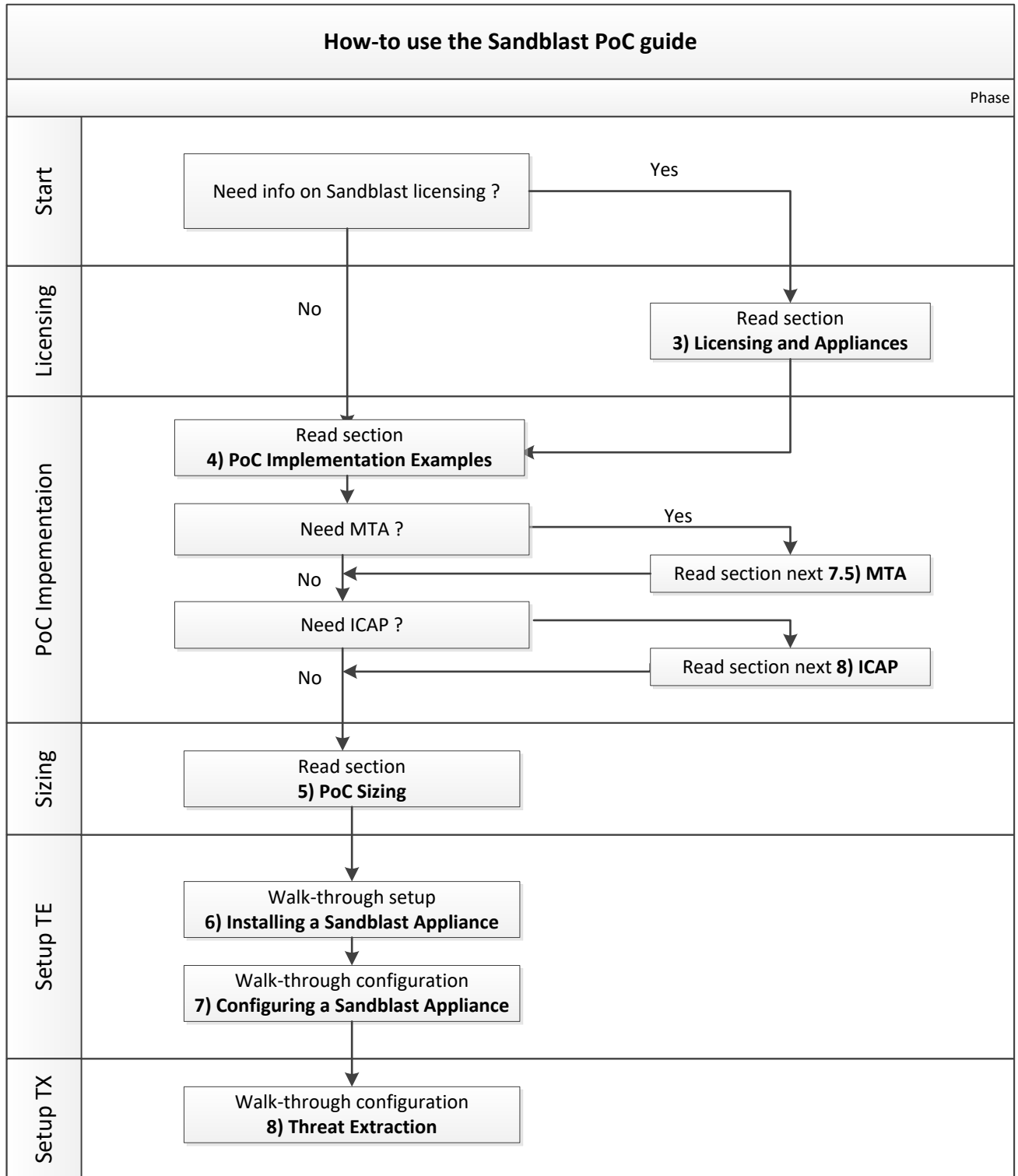
# 1. Change Log

Editor	Date	Version	Comments
Igor Freidin	June 1 <sup>st</sup> 2015	V1	Initial document
Thomas Werner	Sept 23 <sup>rd</sup> 2015	V2/3	Restructure
Thomas Werner	Sept 28 <sup>th</sup> 2015	V4	Added content
Thomas Werner	Oct 2 <sup>nd</sup> 2015	V5	Added content
Thomas Werner	Oct 21 <sup>th</sup> 2015	V6	Added Hyper-Threading AV setting for MTA inspection
Tom Kendrick		V6.1	Fixed typos
Thomas Werner	Nov 2 <sup>nd</sup> 2015	V6.2	Added important notes to 6.5 <i>CPU-Level Threat Detection</i> ; added redundant MTA next hop info
Thomas Werner	Nov 3 <sup>rd</sup> 2015	V6.3	Added Stand-alone info and tecli for "save all sample" option; restrict concurrent VMs running
Thomas Werner	Nov 06 <sup>th</sup> 2015	V6.4	Restructured MTA section Added MTA logging to SmartView Tracker / SmartLog
Thomas Werner	Nov 11 <sup>th</sup> 2015	V6.5	Added information on stand-alone Sandblast PoC (section 6.1)
Thomas Werner	Jan 08 <sup>th</sup> 2016	V6.6	Added MTA infos for cluster deployment (section 7.4.2) Updated TX infos (section 8) Added FP/FN handling (section 9.5)
Thomas Werner	Jan 11 <sup>th</sup> 2016	V6.7	Errata
Thomas Werner	Jan 29 <sup>th</sup> 2016	V6.8	Added flow diagram
Thomas Werner	Feb 03 <sup>rd</sup> 2016	V6.9	Added SmartEvent bug info and email alerting
Thomas Werner	Feb 04 <sup>th</sup> 2016	V7.0	Added 9.1) <i>I have a problem – where is the log ?</i> and 10) <i>Important hotfixes and SKs</i>
Tom Kendrick	Feb 22 <sup>nd</sup> 2016	V7.1	Update to redundant MTA next hop info
Thomas Werner	May 04 <sup>th</sup> 2016	V7.2	Updated redundant MTA next hop mechanism Added outgoing TLS configuration
Thomas Werner	June 20 <sup>th</sup> 2016	V7.3	Added AV URL reputation setting (p. 29); added "Blocking filetypes inside archives" (9.7.3); added workaround for emails getting queued in Postfix (7.4.2)
Thomas Werner	July 4 <sup>th</sup> 2016	V7.4	Corrected typo in 7.4.3
Thomas Werner	July 25 <sup>th</sup> 2016	V7.5	Added section 7.4.2 <i>Recommended MTA fixes</i>
Thomas Werner	July 26 <sup>th</sup> 2016	V7.6	Fixed page numbering and typos
Thomas Werner	Sept 26 <sup>th</sup> 2016	V8.0	Added SNMP monitoring and ICAP section;
Thomas Werner	Oct 05 <sup>th</sup> 2016	V8.1	Removed obsolete "Threat Cloud information sharing" section
Thomas Werner	Nov 24 <sup>th</sup> 2016	V8.2	Corrected misleading information in MTA section
Thomas Werner	Dec 13 <sup>th</sup> 2016	V8.3	Added <ul style="list-style-type: none"> <li>- NGTX licensing (3.3)</li> <li>- Ports needed (4.5)</li> <li>- IPS (7.3)</li> <li>- Minimum recommended images (7.4.2)</li> <li>- Different link functionalities (7.4.5)</li> <li>- TX serial mode info (9.3)</li> </ul>
Thomas Werner	Dec 28 <sup>th</sup> 2016	V8.4	Errata

Editor	Date	Version	Comments
Thomas Werner	Feb 03 <sup>rd</sup> 2017	V8.5	<ul style="list-style-type: none"> <li>- selecting specific emulation images for ICAP (8.6.2)</li> <li>- added important notes on 7.5.2 BCC mode</li> <li>- added 7.5.3 How-to block file-extensions in Postfix</li> <li>- added 6.5 Recommended JHF</li> </ul>
Thomas Werner	June 05 <sup>th</sup> 2017	V8.6	<ul style="list-style-type: none"> <li>- changed ICAP manual starting directive</li> <li>- changed ICAP service name</li> <li>- added Win10 image support for ICAP (8.2.1.1)</li> <li>- added ICAP daemon troubleshooting infos</li> <li>- added Threat Extraction "send original email" infos (9.3)</li> <li>- added how to send email w attachment from cmdline info (10.6)</li> </ul>
Thomas Werner	Oct 12 <sup>th</sup> 2017	V8.7	<ul style="list-style-type: none"> <li>- Revised whole document and ICAP section</li> <li>- Added 7.5.5.1) Raise email header limit</li> <li>- Added 10) TE API</li> </ul>
Thomas Werner	Oct 16 <sup>th</sup> 2017	V8.8	- Added additional MTA Best-Practises
Thomas Werner	Oct 23 <sup>th</sup> 2017	V8.9	- Setting a Postfix hostname
Thomas Werner	Nov 24 <sup>th</sup> 2017	V9.0	- Minor fixes
Thomas Werner	Jan 10 <sup>th</sup> 2018	V9.1	<ul style="list-style-type: none"> <li>- Minor fixes</li> <li>- New JHF recommendations</li> </ul>

## 2. How to use this document

The purpose of this document is to provide a Step-by-Step/Best-Practice PoC guide for a Sandblast PoC installation.



## 3. Licensing and Appliances

### 3.1 Public Cloud and Appliance quota and licensing

For a POC including Public Cloud (ThreatCloud) emulation you'll need a cloud quota license.

#### 1. Cloud Quota

Defines the maximal number of emulations allowed per month. A cloud quota, can be automatically created via User Center Quick Evaluation option.

You can use:

- CPSB-NGTX-EVAL to be generated for:



This is the recommended eval license for TE cloud (public) emulation

- Existing (already licensed) production gateways where you want to enable TE/TX blade with emulation in Public Cloud
  - In Hybrid mode (e.g EXE files configured for Public Cloud emulation and other files for local emulation) on a existing gateway where TE blade is enabled and forwarding traffic is configured for another dedicated local emulation GW and ThreatCloud
- CPSG-CPSM-EVAL
    - All-In-One license that includes a Public Cloud (TE/TX) license for 75.000 files/month

If you need bigger Public Cloud license per month you must approach Solution Center to get an appropriate license. We found out that also assigning multiple CPSB-NGTX-EVALs is adding the included quotas cumulative (but that's not the official way ☺).

To check the current cloud license status use:

```
# cpstat threat-emulation -f contract
```



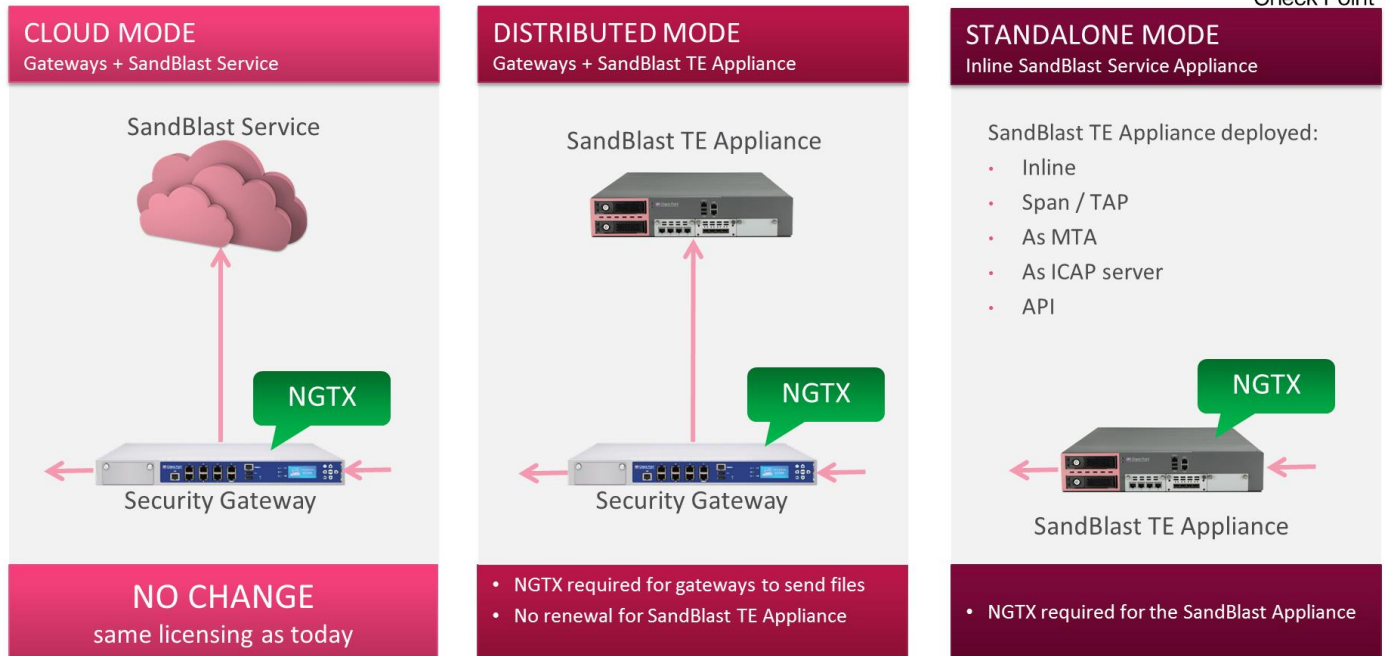


### 3.3 NGTX licensing

## DEPLOYMENT MODES & LICENSING



Check Point



## 4. PoC Implementation Examples

### 4.1 General considerations

As a rule of thumb – the device should see file downloads (HTTP/S), **and the incoming e-mail traffic (SMTP/TLS)**

**⚠️ SMTP/S is where we currently see most of the threats so inspecting/seeing this is very important. As some of the incoming mail might be in SMTP/TLS – enabling MTA is mandatory.**

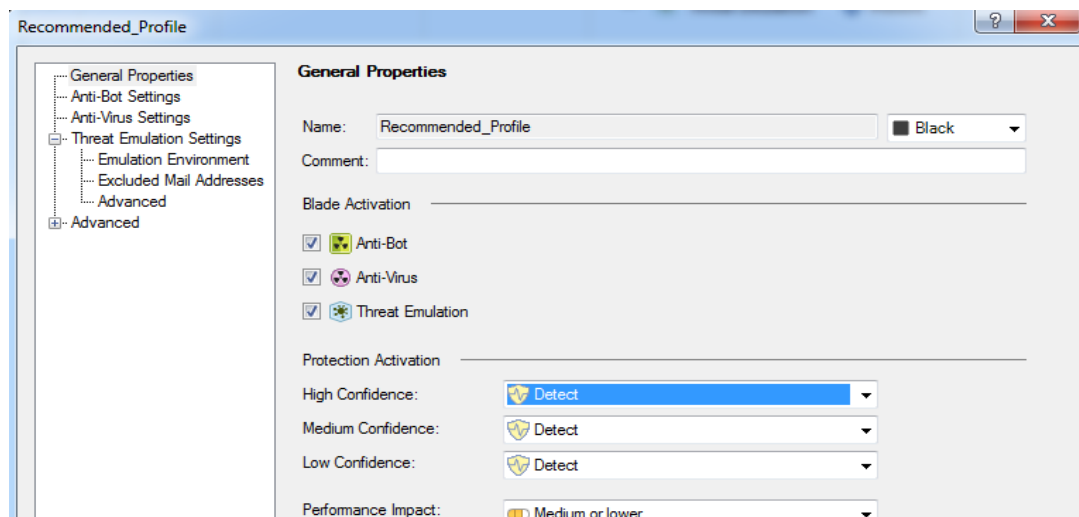
*You need MTA if*

- A. You want to inspect SMTPS/TLS traffic
- B. You want to use Prevent mode for SMTP/TLS
- C. You want to do Threat Extraction on SMTP traffic

#### Using a Mirror (SPAN) port

- Span ports tend to lose packets, according to the switch capabilities and the actual network throughput. This can cause Threat Emulation (and the rest of the blades) not to inspect some traffic. Take this into consideration – if some files are not shown in logs in span port, make sure (e.g. using tcpdump) that all of the packets indeed arrived correctly.
- The span port must be configured to support the combined overall throughput of the uplink and downlink seen. **For example – 100Mbps span port cannot span a 60Mbps sync connection – as it needs to pass 120Mbps to the device.** Such mistakes are pretty common, and can easily cause the PoC to be ruined. Make sure the span port can handle the traffic load. Prefer TAP deployment if possible.

In Mirror mode deployments always configure all blades to be in 'detect mode' and 'background' (not to hold connections). Otherwise, the content after the held/dropped packet will not be inspected.



When working in monitor mode the gateway cannot, naturally, drop/hold the traffic. Nevertheless, a configuration that causes it to 'hold' / 'drop' the traffic will cause the device to stop inspecting the rest of the connection – as the client / server will continue communicating when the gateway 'thinks' that the connection is in hold / was terminated.

If traffic from the Management of the gateway is seen on the monitor port of the same gateway follow the below steps to avoid anti-spoofing issues and unstable traffic:

Edit -> `$FWDIR/boot/modules/fwkernel.conf`

Add the appropriate line to the file:

For IPv4 traffic –

`fwx_bridge_reroute_ipv4=<management_ip>`

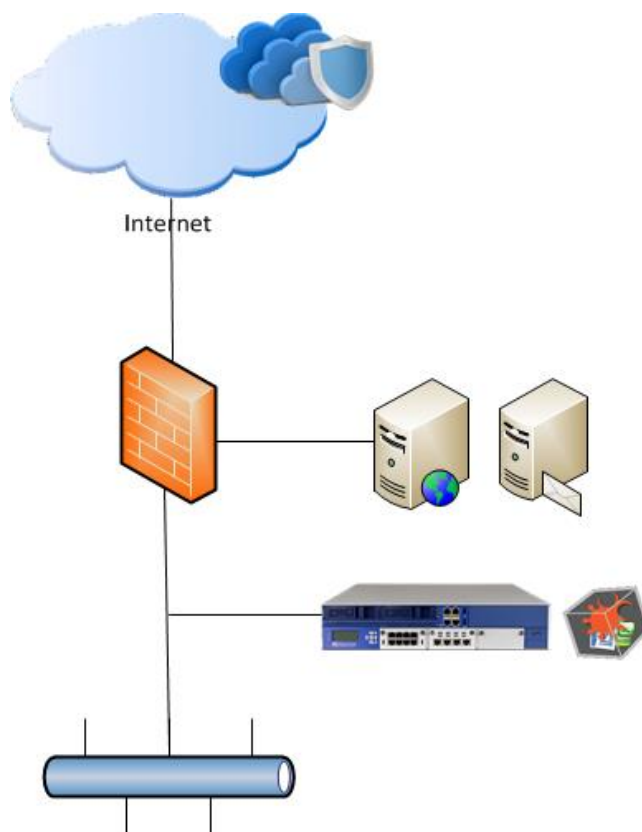
For IPv6 traffic –

`fwx_bridge_reroute_ipv6=<management_ip>`

<management\_ip> is the IP address of the management interface.

Afterwards reboot the Security Gateway.

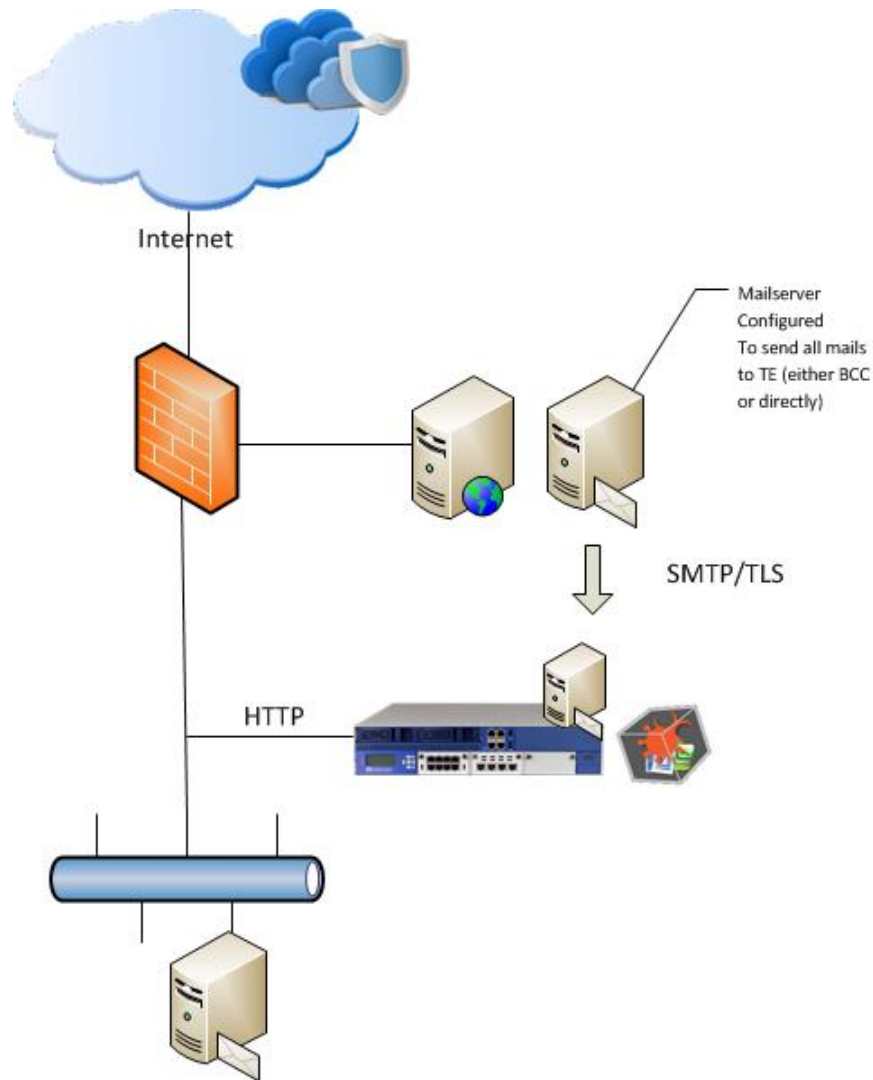
## 4.2 Mirror (SPAN) mode



Sandblast considerations in this scenario:

- Pros
  - no changes in production environment needed
- Cons
  - no HTTPS inspection
  - no SMTPS/TLS inspection
  - no Prevent mode

### 4.3 SMTP/TLS Prevent (MTA) and HTTP (SPAN)



Sandblast considerations in this scenario

- Pros
  - Inspection of SMTPS/TLS via MTA possible
  - If needed Prevent-mode is possible for SMTP/SMTPS
  - TX can be evaluated if Sandblast MTA is in the mail stream as full MTA
- Cons
  - no HTTPS inspection
  - changes to production MTA needed to forward or BCC mails to Sandblast appliance MTA

#### *Tipps*

- To eliminate seeing SMTP traffic twice you need a proper FW ruleset on the TE appliance
- when using BCC configure Nullhost on appliance MTA (see section “Configuration”).

# Modify the FW policy for MTA

## Null MTA for PoC

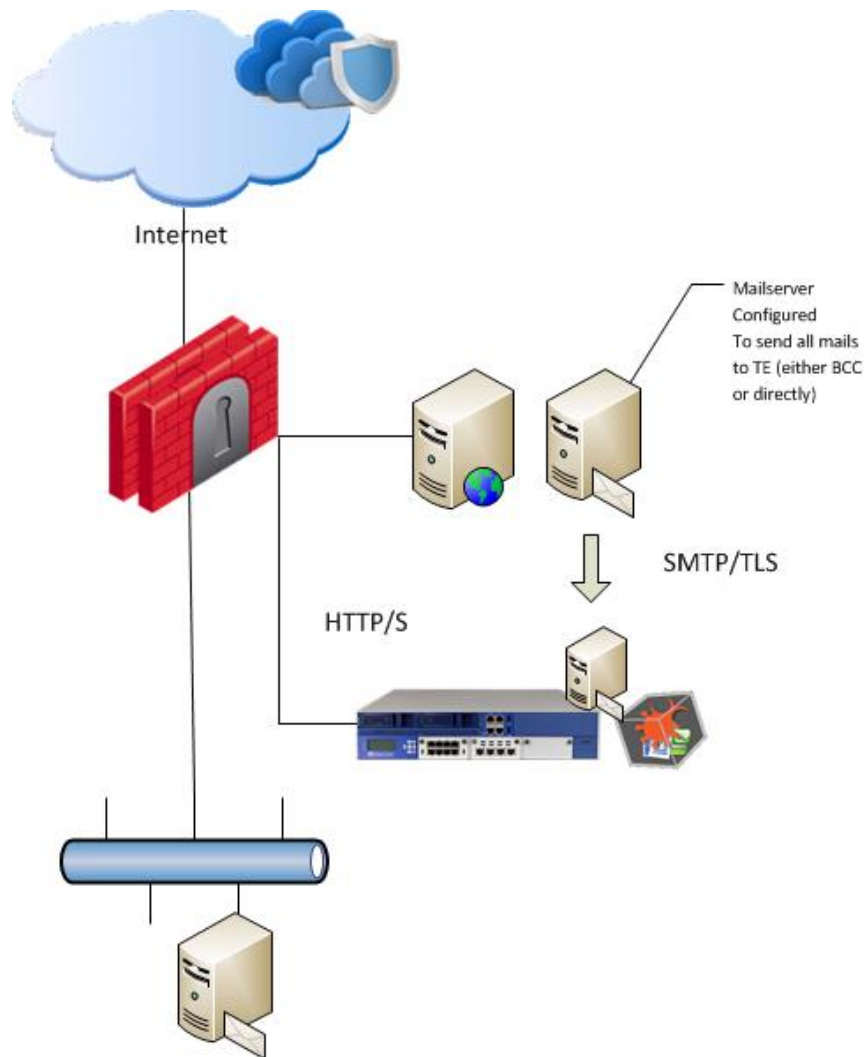
- To avoid the stream engine catching SMTP before the MTA you need to adjust the FW policy
  - Only relevant when on a SPAN port!

Policy

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time	Comment
1	0		Any	poc-gw	Any Traffic	smtp	accept	None	Policy Targets	Any	
2	0		Corporate-mail	Any	Any Traffic	smtp	drop	None	Policy Targets	Any	
3	0		Any	Any	Any Traffic	Any	accept	None	Policy Targets	Any	

- Rule 1 will allow the IPs of the GW to act as MTA
- Rule 2 will only inspect traffic from the internal email server to make sure that DLP/AntiSpam will work if needed
- These rules would make sure that the inbound emails to the internal email server will not be inspected twice

## 4.4 Production CP Gateway HTTP/S (Inline) and SMTP/TLS (MTA)



Sandblast considerations in this scenario

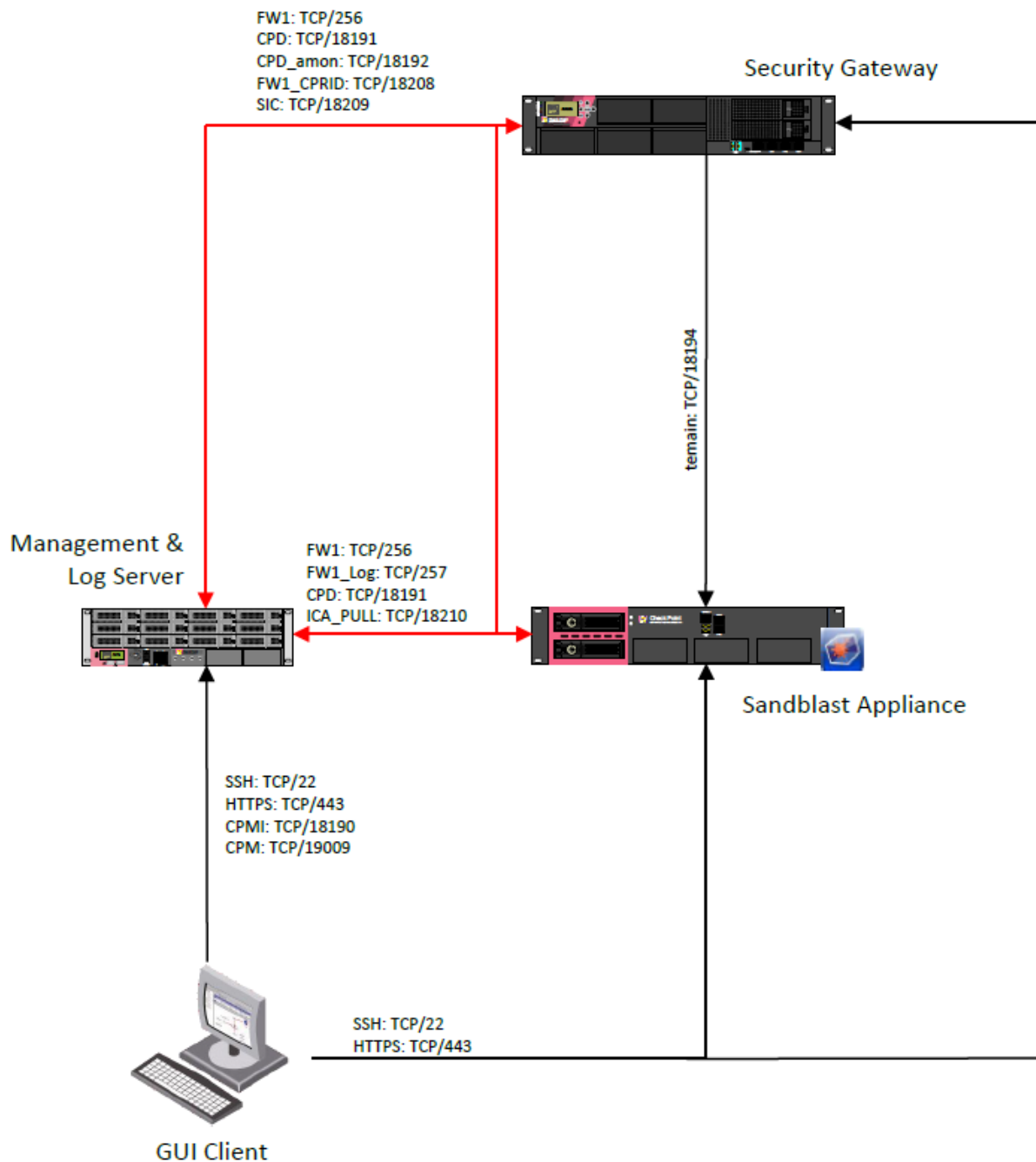
- Pros
  - Inspection of SMTPS/TLS via MTA possible
  - Inspection of HTTPS possible if activated on the CP gateway
  - If needed full Prevent-mode is possible
  - TX can be evaluated if Sandblast MTA is in the mail stream as full MTA
- Cons
  - changes to production CP gateway configuration
  - performance impact on CP gateway

### Tipps

- be sure to do sizing estimation for TE blade on productive CP gateway (see Section "Sizing")
- when using BCC configure Nullhost
- **when activating the TE blade on the gateway to configure the hand-off, a Threat Emulation engine will also be installed on this CP gateway. So engine updates are also relevant if available/needed**




## 4.5 SandBlast – Ports needed between GUI/GW/SB







## 5. Sizing PoC and Production environment


The following options are available to do a proper sizing for a Sandblast PoC (order is with decreasing sizing accuracy):

- 1) Do a Security Checkup or a TE Poc
  - a. “tecli show statistics” will give you all needed sizing information
  - b. additionally you can take a CPSIZEME and use the Appliance Sizing Tool ([https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk88160](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk88160))
- 2) Activate *TE Sizing mode* on an existing Check Point Gateway:  
[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk93598](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk93598)
  - a.  Performance Impact is almost the same as when running TE live. So do a proper sizing for the production gateway in advance -> use CPSIZEME and Appliance Sizing Tool ([https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk88160](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk88160)) to get an estimation how activating TE Sizing Mode will affect the gateway
- 3) Use our “average” calculation
  - a. per user calculate 2 files to be emulated for SMTP/TLS
  - b. per user calculate 5 files to be emulated for HTTP/S
  - c. The result is a file/day value which you can compare with our Sandblast appliance datasheet values (files/month)
  - d. Example:
    - i. Company with 5,000 users
    - ii. Uses both HTTP and SMTP
    - iii.  $(5,000 \text{ Users} * 2 \text{ files SMTP}) + (5,000 \text{ Users} * 5 \text{ files HTTP})$   
= 35,000 files per business day (10 hours workday)  
= 35,000 files/day \* 21 business days -> 735,000 files/month -> TE1000X

### TECHNICAL SPECIFICATIONS

	TE100X	TE250X	TE1000X	TE2000X / TE2000X HPP
				
<b>Performance</b>				
Recommended files/month	100K	250K	1M	1.5M / 2M
Recommended users	Up to 1,000	Up to 3,000	Up to 10,000	Up to 20,000
Throughput	150 Mbps	700 Mbps	2 Gbps	4 Gbps
Number of virtual machines	4	8	28	40 / 56

- 4) Use the maximal bandwidth of the customer and compare it to the above appliance datasheet

 All Sizing numbers in the datasheets are calculated with the “Recommended Check Point images” in use. This means with only two selected emulation images running. In a PoC it makes sense to activate all images to get the highest catch rate. Enabling additional images has a severe performance impact. Doubling number of emulation images cuts throughput performance of appliance by more than half.

## 6. Installing a Sandblast appliance

### 6.1 Stand-alone vs. multiple private cloud

#### One Stand-alone Sandblast appliance

If from a load perspective one Sandblast appliance is sufficient you can use the following deployment options:

- 1) *Without attaching to the customer's CP environment*  
You do the Sandblast PoC with only one self-sustaining Sandblast appliance. Therefore install the appliance as an all-in-one deployment with *gateway AND management* on one box. Afterwards you activate the relevant inspection blades AV/AB/TE and also the management blades like SmartLog, SmartEvent and the SmartEvent Correlation Unit. This setup will run only on a Mirror Port / MTA deployment as you cannot integrate this setup into a customer's existing Check Point infrastructure. The deployment methods are covered in section 4.2) *Mirror (SPAN) mode* and 4.3) *SMTP/TLS Prevent (MTA) and HTTP (SPAN)*.
- 2) *With attaching to the customer's CP environment*  
If you want to attach one Sandblast appliance to an existing customer Check Point Gateway/Cluster - like mentioned in section 4.4) *Production CP gateway HTTP/S (Inline) and SMTP/TLS (MTA)* - you will have to install the sandblast appliance without the management component during the initial GaiA setup.

#### Multiple Private Cloud appliances

If one Sandblast appliance is not able to take all the traffic load and you need multiple once there are two options:

- 1) *Without attaching to the customer's CP environment*  
In this scenario you will need one or more Check Point gateways acting as "harvesters" attached to a Mirror Port. These gateways will be configured to use multiple Sandblast appliances for emulation like described in 7.4.4) *Multiple Private Cloud appliances*.
- 2) *With attaching to the customer's CP environment*  
If a Check Point Gateway/Cluster is already in production at the customer you can also attach multiple Sandblast appliances directly to these gateways. See section 7.3.3) *Multiple Private Cloud appliances*.

### 6.2 TE-X Appliance ISO




Be sure to use the correct ISO for a TE-X-appliance (do not use an old TE appliance ISO)


Download link R77.30 ISO image for SandBlast appliances (TE-X Appliances):

[https://supportcenter.checkpoint.com/supportcenter/portal/role/supportcenterUser/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit\\_doGetdcdetails=&fileid=53306](https://supportcenter.checkpoint.com/supportcenter/portal/role/supportcenterUser/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=53306)

## 6.3 R77.30 Management AddOn

The Management Add-on package is needed for using Threat Extraction and also for some TE/AV functionalities (like “Scan links inside emails” option).

 There is no need to run a dedicated Management or SmartEvent Server within a Sandblast PoC. You can run Management, SmartLog, SmartEvent, AV, AB, TE on one Sandblast Appliance. The performance impact for Management, SmartLog, SmartEvent is almost negligible because of the much smaller event count in opposite to a full Security Checkup.

 If you integrate a TE appliance with an existing CP gateway of a customer the Add-on must be installed on the management server of the customer. Take this into consideration when planning/designing a PoC.

Download link R77.30 Management Add-on package:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk105412](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk105412)

## 6.4 Enable Hyper-Threading

Enabling Hyper-Threading will improve emulation performance on the appliances – in short activate it via

1. Run `cpconfig` command.
2. Choose 'Configure Hyper-Threading' option.
3. Select 'yes' to enable SMT.
4. The wizard enables SMT and updates the number of CoreXL FW instances automatically. If the wizard cannot update CoreXL automatically, then configure the CoreXL manually as described above (this is relevant in cases where CoreXL configuration was modified manually before enabling SMT).
5. Press `Enter` to continue.

More information can be found here:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk93000](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk93000)

## 6.5 Recommended Jumbo Hotfix – R77.30/R80.10(EA)

We strongly recommend installing at least JHF 292 – currently available as GA Jumbo Hotfix.

This will include important MTA enhancements, Threat Extraction enhancements and the ICAP hotfix:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk114613](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk114613)

If you decided to install the SandBlast Appliance with R80.10 (currently EA for SB Appliances) make sure to install at least Take 70.

## 6.6 Updating TE images and engine

### 6.6.1 General info and configuration

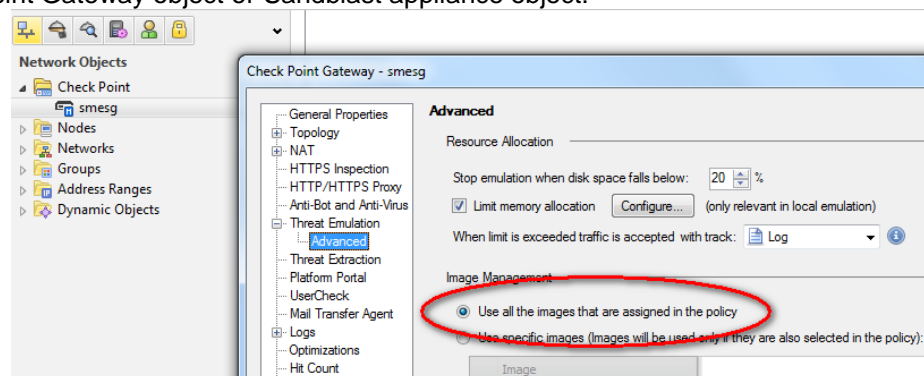
**!** Online update will download images and the current TE engine version. The total data volume is approx. 50GB. Take this into consideration when planning your PoC setup. At a customer with low bandwidth this could take some time.

**!** Only selected images in your Threat Prevention policy or corresponding CP object settings will be activated/installed. This is true for both Online or Offline update procedure.

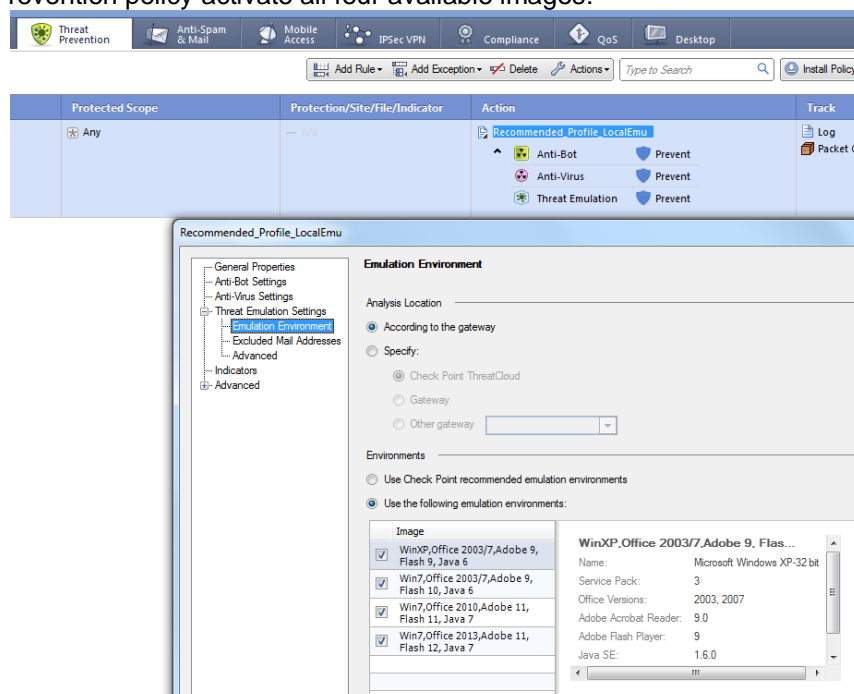
**!** If you only select “Use Check Point recommended emulation environments” you will only get two images (WinXP and Win7 with Office 2003/7). This will limit your catch rate.

#### **To get all images use the following configuration**

On the Check Point Gateway object or Sandblast appliance object:

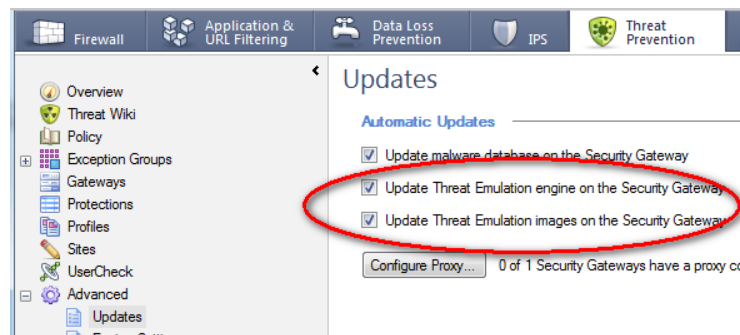


Within your Threat Prevention policy activate all four available images:

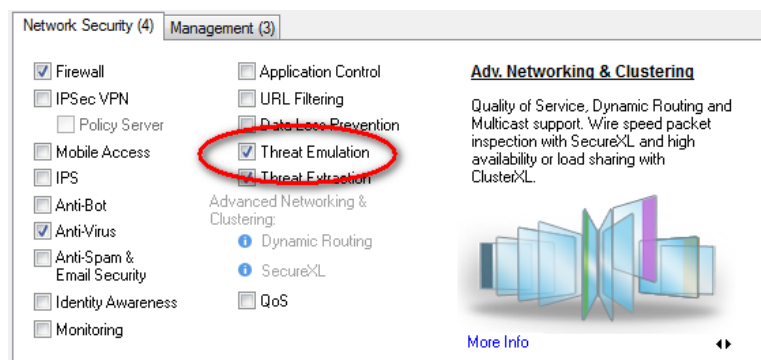


## 6.6.2 Online Update

After configuring the images you want to use (see section 6.5.1) activate the online update options:



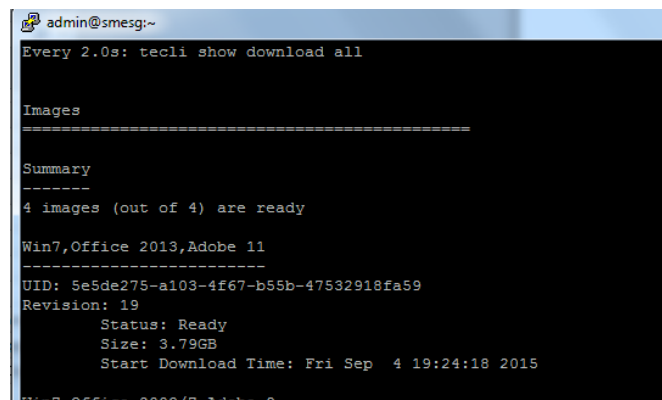
At last switch on the TE blade and install the policy:



You should then see the gateway downloading the images either via SmartDashboard:



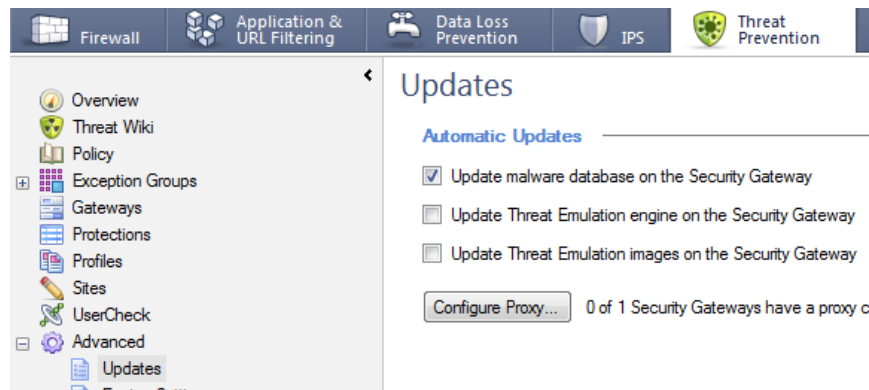
Or in more detail via the CLI command `# watch tecli show download all`



Also check if the latest engine version is applied via `# tecli advanced engine version`.

## 6.6.3 Offline Update

Deactivate the online update option if needed:



Download the latest Offline Update package from:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk92509](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk92509)

The Offline Update procedure is also described in the above SK.  
You could see the proper initialization of the images via the CLI command

```
# tecli show download all
```

```
admin@smesg:~
Every 2.0s: tecli show download all

Images
=====

Summary
-----
4 images (out of 4) are ready

Win7,Office 2013,Adobe 11
=====
UID: 5e5de275-a103-4f67-b55b-47532918fa59
Revision: 19
  Status: Ready
  Size: 3.79GB
  Start Download Time: Fri Sep  4 19:24:18 2015
Win7,Office 2003/7,Adobe 9
```

Also check if the latest engine version is applied via

```
# tecli advanced engine version
```

```
[Expert@smesg:0]# tecli a e v
Threat emulation engine version is: 43.990000082
[Expert@smesg:0]#
```

## 6.7 CPU-Level Threat Detection

You can check the CPU Level detection status via:


```
# tecli a a s | grep CPU-Level
```


```
[Expert@smesg:01# tecli a a s | grep CPU-Level  
CPU-Level Detection: UNSUPPORTED  
[Expert@smesg:01#
```



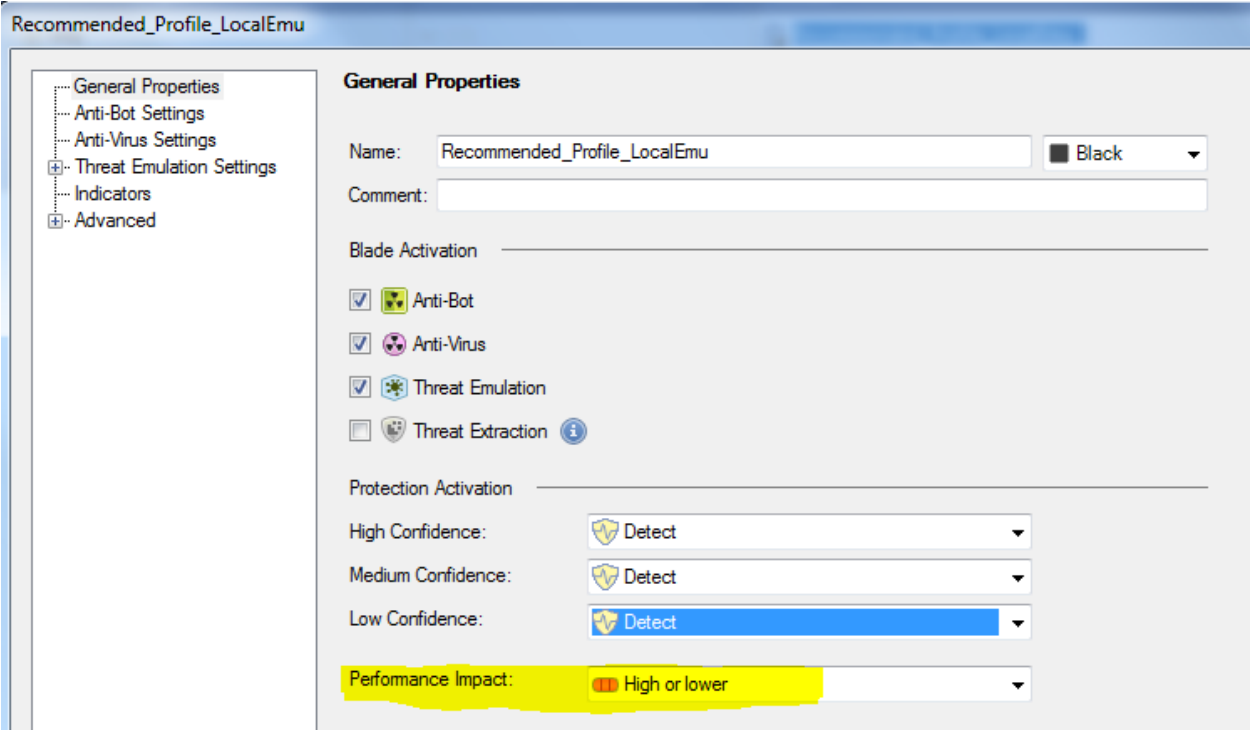
## 7. Configuration

### 7.1 General Considerations

 **Always strive** to enable all Threat Prevention blades Anti-Virus, Anti-Bot in addition to Threat Emulation. This will provide you the best catch rate in a PoC. Other vendors like FireEye devices have a built in Anti-Virus and Anti-Bot functionalities (they tend not to talk about the built in Anti-Virus, but it exists and viewable in CLI and other tools) – so a fair comparison must include these capabilities as well.

 AV and AB blade activation makes sense only if you see this traffic as a stream, e.g. if a TE appliance is on a Mirror Port. If the TE appliance only works as an emulation device getting traffic from a CP gateway AV and AB will be of limited use.

In addition also activate all detection signatures with Performance Impact “High or lower”:



The screenshot shows the configuration window for 'Recommended\_Profile\_LocalEmu'. The left sidebar contains a tree view with the following items: General Properties (selected), Anti-Bot Settings, Anti-Virus Settings, Threat Emulation Settings, Indicators, and Advanced. The main panel displays the 'General Properties' configuration. It includes fields for 'Name' (Recommended\_Profile\_LocalEmu) and 'Comment'. Below these are sections for 'Blade Activation' and 'Protection Activation'. In the 'Blade Activation' section, checkboxes are present for Anti-Bot, Anti-Virus, Threat Emulation, and Threat Extraction. In the 'Protection Activation' section, there are three rows for 'High Confidence', 'Medium Confidence', and 'Low Confidence', each with a dropdown menu set to 'Detect'. At the bottom, the 'Performance Impact' is set to 'High or lower'.

Section	Item	Value / Status
Blade Activation	Anti-Bot	Checked
	Anti-Virus	Checked
	Threat Emulation	Checked
	Threat Extraction	Unchecked
Protection Activation	High Confidence	Detect
	Medium Confidence	Detect
	Low Confidence	Detect
Performance Impact		High or lower

## 7.2 Anti-Virus and Anti-Bot configuration

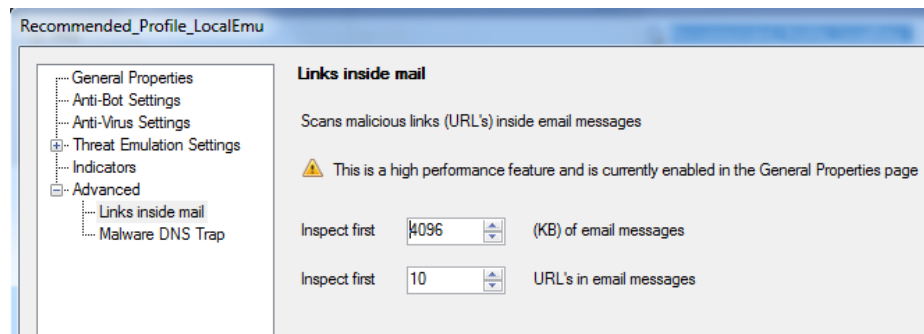
Anti-Virus and Anti-Bot blades require constant internet access in order to work

**!** For PoCs it is best-practise to keep AV in DETECT mode because otherwise AV “kills” the SMTP connection from the sending MTA which could cause impact even in a BCC setup

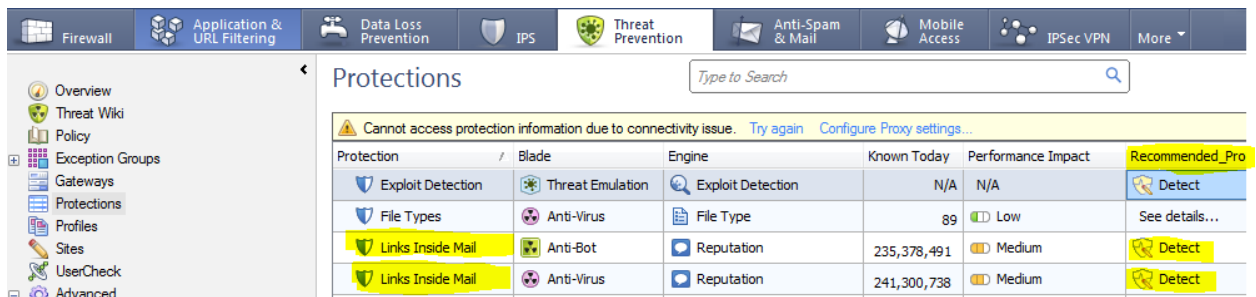
**!** IPS inspection on incoming mails will only work if SMTP is clear-text and not TLS encrypted because IPS works on the network stream to the MTA.

### Enable inspection of Links inside emails

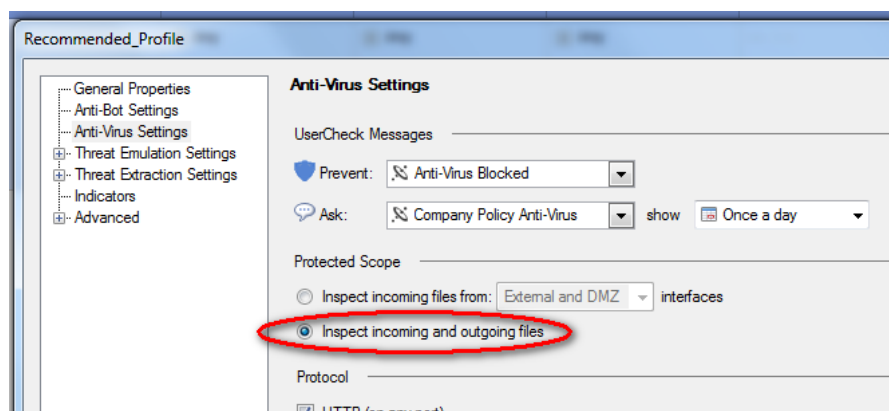
Also be sure to enable Anti-Virus and Anti-Bot inspection of links inside emails [sk105412](#)



Make sure that this feature is activated inside your TP profile:



### Enable inspection of “Incoming and outgoing” files



This will enable AV stream scanning on incoming MTA traffic.

If you have an incorrect topology or a one-leg interface implementation (e.g. MTA with one interface) you also need to reconfigure an additional configuration file to enable AV URL reputation on clear-text email network stream to the MTA:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk109573](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk109573)

Follow these steps:

1. Backup the file `$FWDIR/conf/malware_config` on the Security Gateway.
2. Edit the file `$FWDIR/conf/malware_config` in Vi editor.
3. Under `[email_links_classification]` section, set the value of the parameter "`scan_all_traffic`" to true:

**[email\_links\_classification]**


...

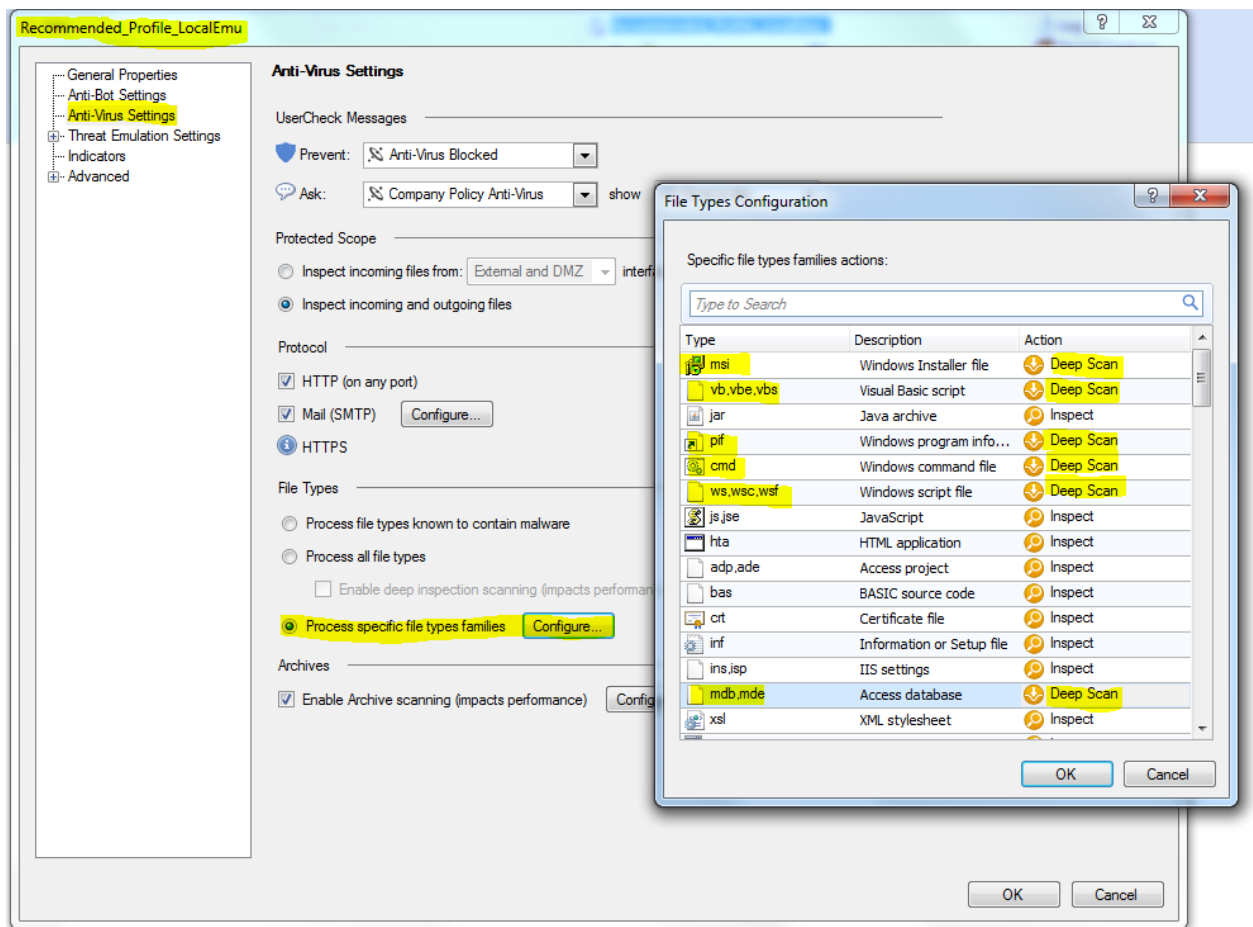
**`scan_all_traffic=true`**

...

4. Save changes in the file and exit from Vi editor.
5. Install the Threat Prevention policy.

## Enable 'AV Deep Scanning'

-  Do not enable "Deep Scan" on all files because then DLP has to reassemble every file passing (on top of streaming inspection; this will cause massive CPU usage)
- Deep Scan only for
  - Msi, pif, cmd, swf, wsc, wsf, chm, hlp, lnk, swf, bat, pdf, com, class
  - exe (all different types)
  - dll, reg
  - vb, vbs, vbe
  - All Microsoft Office file types



## 7.3 IPS

Since the latest licensing change in November 2016 we now have a NGTX license of the gateway and/or SandBlast appliance which enables us to use also IPS functionalities.


Since February/March 2016 (ever since Locky become wide spread), we have been developing IPS detection over Mail and HTTP and released several IPS protections to block all ransomware infection steps using scripts:


### 1. Mail Attachments (soon also to look at HTTP(s) traffic as well)

- **Suspicious Executable Mail Attachment** - Detects executable mail attachments file type: cpl/vbe/vbs/pif/com/scr/bat/cmd/ace/exe/hta/jar
- **Suspicious Mail Attachment Containing JavaScript Code** - Detects downloaders file type: js/jse/wsf and inside archive files: zip, gzip, rar, recursive zipped files
- **Microsoft Office Mail Attachment Containing Malicious Downloader** – Detects Locky campaigns with specific patterns and indicators which are not common to other ransomwares
- **Suspicious Image Attachment In Phishing Mail** – Detects Locky campaigns with specific patterns and indicators which are not common to other ransomwares
- **Suspicious Microsoft Publisher Mail Attachment** – Detects Publisher attachments with Macro downloaders
- **Suspicious Metadata Mail Phishing Containing Attachment** – Detects known campaigns with DOCM attachments

### 2. Over both Mail and HTTP

- **Microsoft Office Files Containing Malicious Downloader**
- **Microsoft Office Files Containing Malicious VBScript Downloader**

 For PoCs it is best-practise to keep IPS in DETECT mode because otherwise IPS “kills” the SMTP connection from the sending MTA which could cause impact even in a BCC setup

 IPS inspection on incoming mails will only work if SMTP is clear-text and not TLS encrypted because IPS works on the network stream to the MTA.

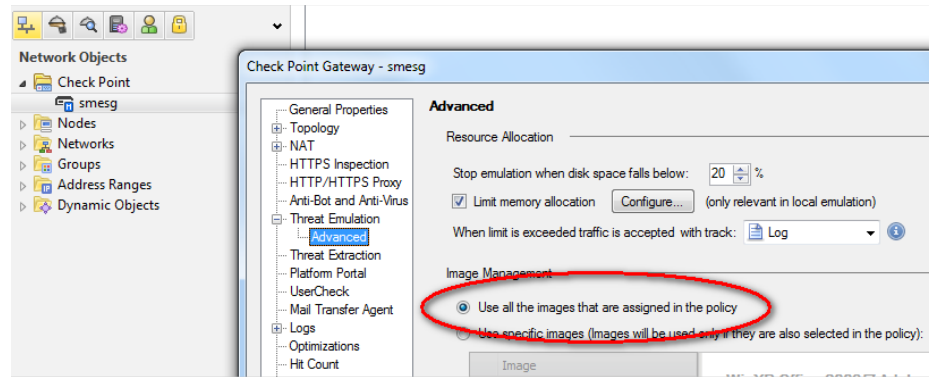
## 7.4 Threat Emulation

### 7.4.1 TE Images

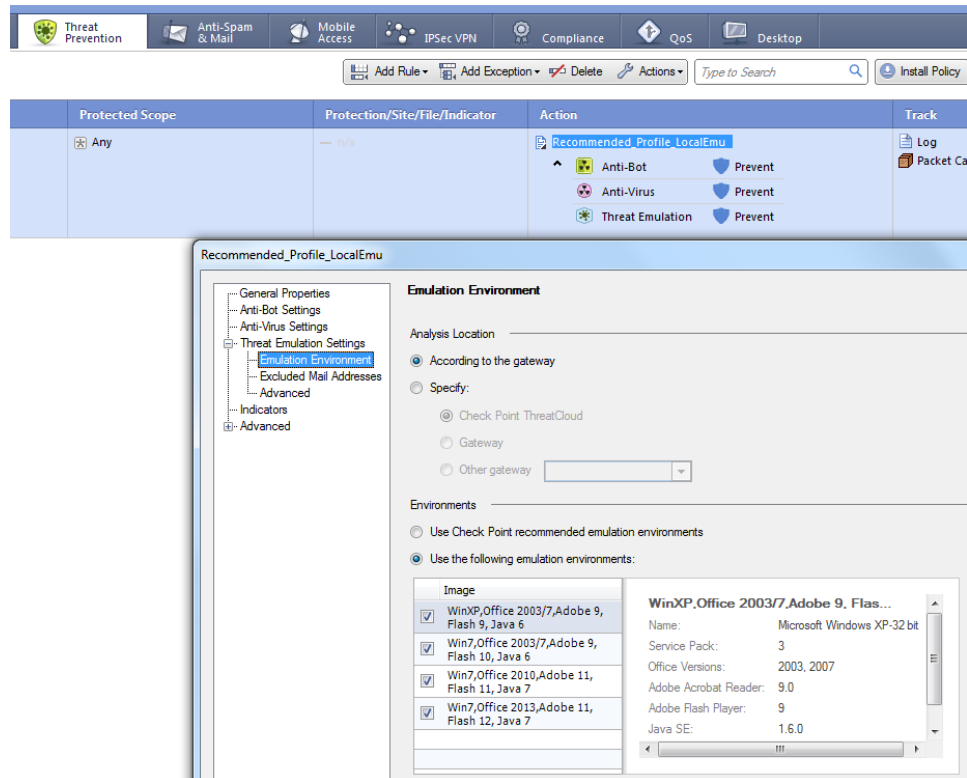
Enabling all images for Threat Emulation leads to a higher detection rate.

**To get all images use the following configuration**

On the Check Point Gateway object or Sandblast appliance object:



Within your Threat Prevention policy activate all four available images:



## 7.4.2 Minimum recommended images

We recommend that you start at least with the following image combinations:

WinXP, Office 2003/7 + Win7 64-bit, Office 2010 + Win7, Office 2013

or

WinXP, Office 2003/7 + Win7, Office 2010 + Win8.1, Office 2013

You should have at least every Office version and in addition one 64-bit image.

But remember that adding additional images has a severe performance impact as EVERY file must be opened on an additional VM instance.

## 7.4.3 Hybrid mode

Enabling all images for Threat Emulation on a Sandblast appliance for higher detection rate may have high performance impact. You can consider emulating specific (non-personal) files like EXE in Threat Cloud. Therefore the gateway or Sandblast appliance needs an additional TE Cloud license/subscription.

## 7.4.4 Multiple Private Cloud appliances

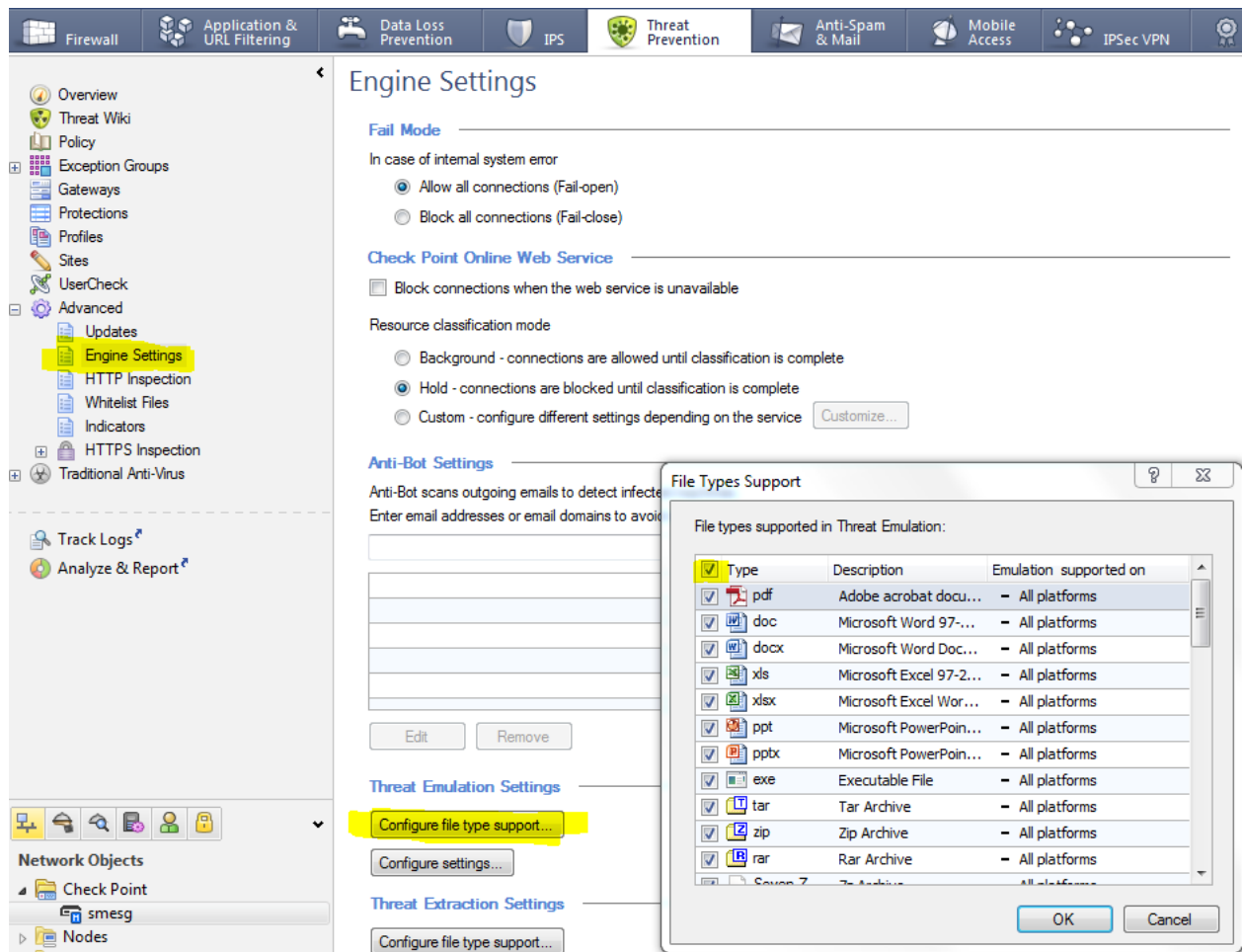
Regarding performance for local emulation PoCs you can also consider enabling emulation “load sharing” for further TE scaling, follow [sk102309](#). With this configuration an existing GW will be the “traffic collector” forwarding files for emulation to multiple Private Cloud Appliances.




The steps mentioned in the SK must be issued on the traffic collector(s).

## 7.4.5 TE filetypes

Be sure to switch on all TE supported filetypes:



 The filetype list is pulled from Threat Cloud through the Management Server. So be sure the Management Server has Internet connectivity. This is also true for the selectable images in the TP profile and CP object settings.



## 7.4.6 Different “Links inside mails/documents” features

Currently we have the following functionalities:

### 1. Links inside emails

- a. See Section 7.2
- b. This is an AV blade functionality
- c. It only works on links inside the email body
- d. It checks link reputation against our Threat Intelligence

### 2. Check links inside email attached documents

- a. This is a TE blade functionality
- b. Available since TE engine 47.990000102 or later
- c. Can be controlled via “tecli advanced analyzer ...”
- d. Check links inside documents
- e. It checks link reputation against our Threat Intelligence

### 3. Emulate links from email body

- a. This is available with JHF 226 or higher
- b. This is a TE blade functionality
- c. It will try to download a file from a link DIRECTLY pointing to that file and after successful download emulate it

## 7.5 MTA

### 7.5.1 Show currently installed Postfix version

```
# /opt/postfix/usr/sbin/postconf -d | grep mail_version
```

Latest version since JHF225 should show:  
mail\_version = 3.1.0

### 7.5.2 General MTA settings

MTA can work alongside 'normal' file reassembly (stream mode). It is highly recommended when prevent capabilities are needed for SMTP traffic as the device functioning as MTA completes the transaction with the sending server, inspects the file and only then opens the connection to a destination mail server. This removes the risk of timeouts when the connection is hold and the file is inspected in streaming mode.

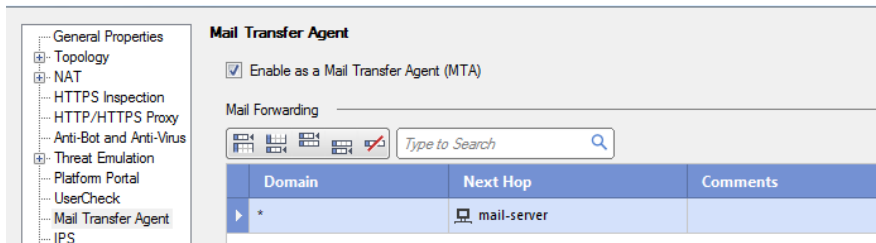
Even when running a 'detect only' PoC MTA has two major advantages:

- It can handle encrypted mail traffic passing via SMTP/TLS
- It doesn't suffer from possible packet loss issues in SPAN/Tap mode deployments.

In both cases, configuring the device as MTA is likely to increase the detection rate.

 In case of private cloud deployments, both the sending gateway and the private cloud appliance can act as an MTA. **Best-practice is to use the MTA on the Private Cloud appliance**, but both options are viable and supported.

Enabled MTA with Next Hop to the next customer mail-server (used with Prevent mode):



## 7.5.3 BCC mode



For **BCC mode** - Enabled MTA with Next Hop configured as Nullhost with IP 0.0.0.0:

**Mail Transfer Agent**

☒ Enable as a Mail Transfer Agent (MTA)

Mail Forwarding

Type to Search

Domain	Next Hop	Comments
*	hostt-0.0.0.0	

In order to configure MTA for 'BCC Monitor mode' deployment, the network administrator should configure his existing mail relay to send **a copy (BCC)** of the email to the Check Point device configured as MTA, and this device should be configured to forward all traffic to '0.0.0.0' (aka Null MTA, which means – delete it after emulation).



### Block SMTP stream inspection

If the same SMTP traffic is available via MTA and a configured SPAN port it will be inspected twice and cause additional load and double detections. This is only true for unencrypted SMTP traffic.

## Modify the FW policy for MTA

### Null MTA for PoC

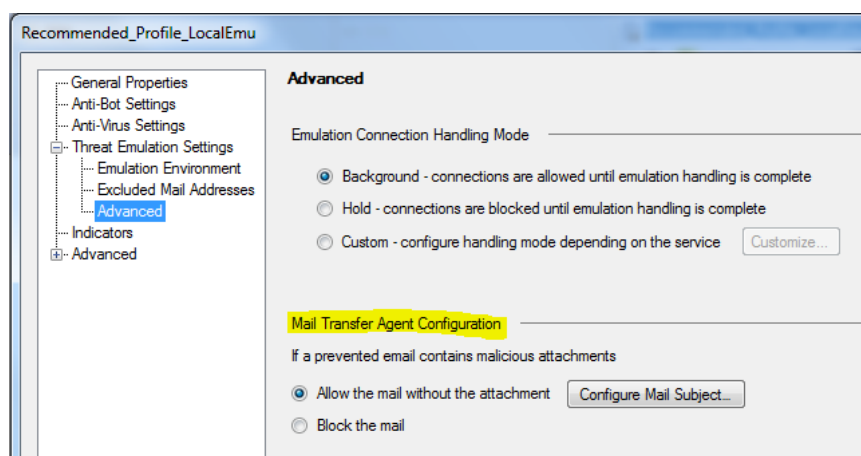
- To avoid the stream engine catching SMTP before the MTA you need to adjust the FW policy
  - Only relevant when on a SPAN port!

Policy

No.	HRs	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time	Comment
1	0		Any	pcc-gw	Any Traffic	smtp	accept	None	Policy Targets	Any	
2	0		Corporate-mail	Any	Any Traffic	smtp	drop	None	Policy Targets	Any	
3	0		Any	Any	Any Traffic	Any	accept	None	Policy Targets	Any	

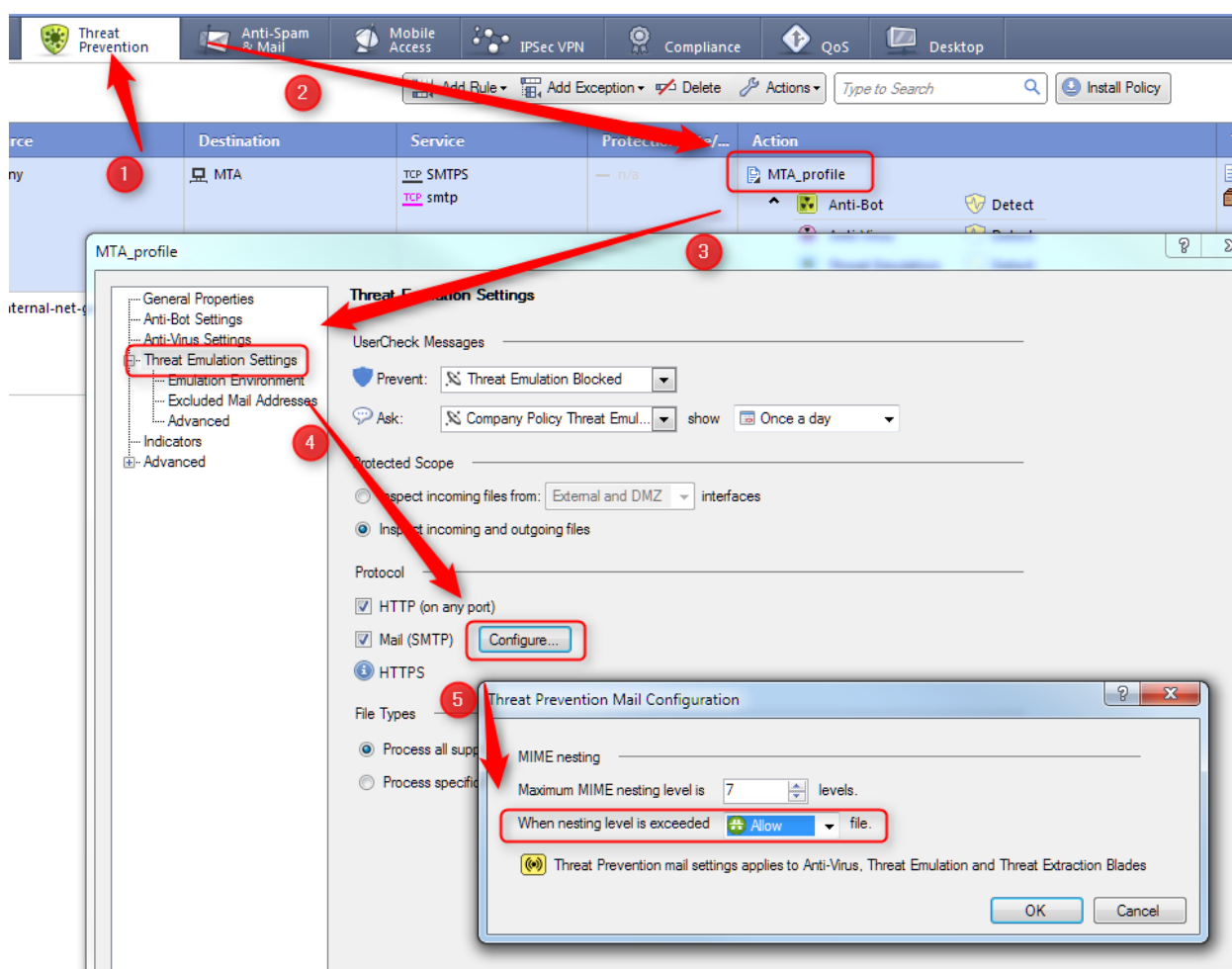
- Rule 1 will allow the IPs of the GW to act as MTA
- Rule 2 will only inspect traffic from the internal email server to make sure that DLP/AntiSpam will work if needed
- These rules would make sure that the inbound emails to the internal email server will not be inspected twice

These MTA settings are only available when you install the R77.30 Management AddOn package:



### ⚠ Deactivate maximum MIME nesting level blocking

Be sure to change the MIME nesting level protection from “Block” to “Allow”. Otherwise E-Mails can get blocked even in BCC leading to NDRs:



## 7.5.4 How-to block file extensions in Postfix

Follow [SK101870](#) to add your own Postfix configurations.

If not already down create your Postfix options file which will be merged with main.cf on Threat Prevention policy install via SmartDashboard:

```
# touch $FWDIR/conf/mta_postfix_options.cf
```

### How-to block certain file extensions

- Add the following line to mta\_postfix\_options.cf:

```
mime_header_checks = regexp:/opt/postfix/etc/postfix/blocked_attachments
```

- Add a similar line to /opt/postfix/etc/postfix/blocked\_attachments:

```
/name=[^>]*\.(js|mht|html)/ REJECT
```

- Install Threat Prevention Policy via SmartDashboard
- Check if Postfix option is merged to main.cf:

```
# cat /opt/postfix/etc/postfix/main.cf | grep block
```

Should display:

```
mime_header_checks = regexp:/opt/postfix/etc/postfix/blocked_attachments
```

The above example will **reject** all emails which contain attachment extensions with JS, MHT, HTML. Blocking is logged via /var/log/maillog:

```
Mar 3 08:36:30 2017 smesg postfix/cleanup[27967]: 25A879C006E: reject: header Content-Type: application/x-javascript;? name="hell.js" fr
; from=<jlennon@lab.local> to=<linda@acme.com> proto=ESMTP helo=<[10.2.1.10]>: 5.7.1 message content rejected
Mar 3 08:36:32 2017 smesg postfix/smtpd[27964]: disconnect from unknown[10.2.1.10]
Mar 3 08:36:47 2017 smesg postfix/smtpd[27964]: connect from unknown[10.2.1.10]
Mar 3 08:36:47 2017 smesg postfix/smtpd[27964]: 87F4C9C006E: client=unknown[10.2.1.10]
Mar 3 08:36:47 2017 smesg postfix/cleanup[27967]: 87F4C9C006E: message-id=<58B92B1E.5080901@lab.local>
Mar 3 08:36:47 2017 smesg postfix/cleanup[27967]: 87F4C9C006E: reject: header Content-Type: application/x-javascript;? name="hell.JS" fr
; from=<jlennon@lab.local> to=<linda@acme.com> proto=ESMTP helo=<[10.2.1.10]>: (5.7.1 message content rejected)
Mar 3 08:36:48 2017 smesg postfix/smtpd[27964]: disconnect from unknown[10.2.1.10]
```

### Disclaimer

This solution is not “officially” provided by Check Point. Postfix configuration changes are supported by “best-effort” via TAC

## 7.5.5 Recommended MTA Best-Practises

Install at least JHF version 226 on the appliance running the MTA.

### 7.5.5.1 Raising the MTA header length limit

We highly recommend raising the default header length limit to 65535. Further information can be found in Scenario 3 of the following SK:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk106739](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk106739)

If you do not raise the limit it might lead to emails getting not inspected.  
To raise the limit follow these instructions:

1. Connect to the command line.
2. Log in to the Expert mode.
3. Backup the current *\$FWDIR/conf/mail\_security\_config* file:

```
[Expert@HostName:0]# cp -v $FWDIR/conf/mail_security_config{,_ORIGINAL}
```

4. Edit the current *\$FWDIR/conf/mail\_security\_config* file:

```
[Expert@HostName:0]# vi $FWDIR/conf/mail_security_config
```

5. Add the value of the ***max\_header\_len*** parameter under **[general]** tab:

```
max_header_len=65536
```

6. Save the changes and exit from Vi editor.
7. Restart Check Point services on Security Gateway ('cpstop;cpstart')

## 7.5.5.2 Setting a Postfix hostname

In some environments the next-hop MTA will only accept emails from the Check Point MTA when our MTA has a proper FQDN set. This is **NOT** achieved by setting host- and domainname in the GAIa WebUI.

To set a Postfix FQDN hostname follow:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk101870](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101870)

Summary:

### **Security Gateway's hostname**

The default Security Gateway's hostname, as it appears in mail headers and SMTP protocol connections, is the name of the Security Gateway's object in the SmartDashboard.

To change the Security Gateway's hostname in mail headers and SMTP protocol connections, add the following line to the '\$FWDIR/conf/mta\_postfix\_options.cf' file:

**myhostname=DESIRED\_NAME**

### 7.5.5.3 Upstream MTA delivery issues (tcp\_timestamp)

To resolve problems for the upstream MTA delivering emails to our MTA deactivate the TCPTIMESTAMP setting:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk62700](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk62700)

TCP timestamps can be disabled in the following way:

- Connect to command line on the involved machine (over SSH, or console).
- Log in to Expert mode (on Gaia / SecurePlatform OS).
- Configure the relevant parameter for OS kernel:

**On Gaia / SecurePlatform:**

```
[Expert@HostName]# sysctl net.ipv4.tcp_timestamps=0
```

To verify:

Either run

```
[Expert@HostName]# sysctl net.ipv4.tcp_timestamps
```

Or run

```
[Expert@HostName]# cat /proc/sys/net/ipv4/tcp_timestamps
```

**Important Note:**

Do **NOT** run the 'sysctl -w net.ipv4.tcp\_timestamps=VALUE' command (with "-w" flag). This will change the desired value in the /etc/sysctl.conf file and will reload this configuration file, which contains the value that disables IPv4 Forwarding. As a result, this will cause complete traffic outage, and will require a complete restart of Check Point services (cpstop; cpstart).

**Note:**

This 'sysctl' command disables the TCP timestamps only *on-the-fly* (until the next reboot).

To disable the TCP timestamps *permanently* (to survive reboot), follow these steps:

Edit the configuration file in Vi editor:

```
[Expert@HostName]# vi /etc/sysctl.conf
```

Modify  
from

```
## Turn on TCP timestamps  
net.ipv4.tcp_timestamps = 1
```

to

```
## Turn on TCP timestamps  
net.ipv4.tcp_timestamps = 0
```

Save the changes and exit from Vi editor.

[...]

**Note:**

This change will only be applied to local connections (connections where the source or destination is the gateway).



### 7.5.5.4 Implementing cleanup script

Implement the following cleanup scripts:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk117634](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk117634)

### 7.5.5.5 Next hop redundancy / failover

If you need next-hop redundancy please follow this SK:

[https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.SearchResultMainAction&eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk110369](https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.SearchResultMainAction&eventSubmit_doGoviewsolutiondetails=&solutionid=sk110369)

### 7.5.5.6 Outgoing TLS

If you need outgoing email encryption add the following line to `$FWDIR/conf/mta_postfix_options.cf` and reinstall the TP policy on the gateway:

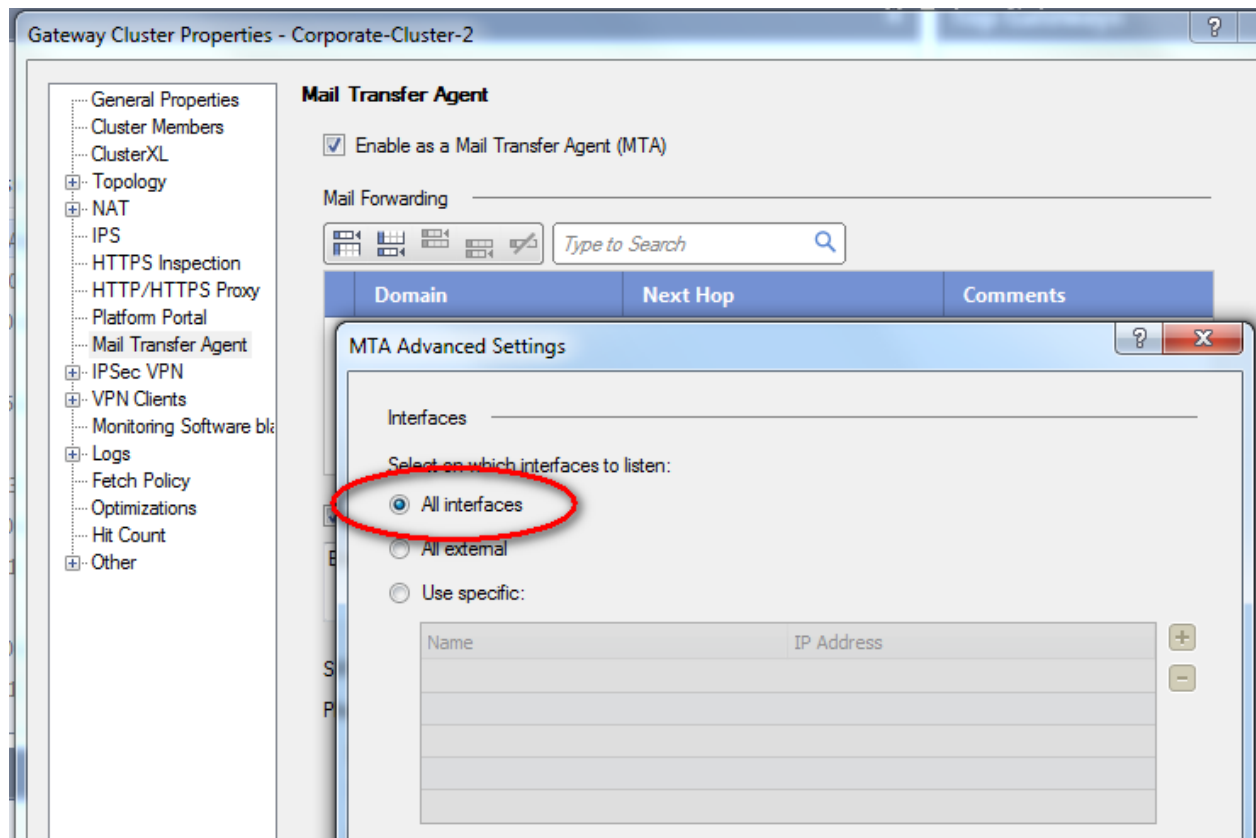
```
smtp_use_tls=yes
```



Don't use other Postfix TLS parameters like `smtp_tls_security_level=may` because they may cause serious issues e.g. bypassing TE

### 7.5.5.7 Special considerations when using MTA on a gateway cluster

When activating the MTA on a gateway cluster (to use TE hand-off to a local Sandblast appliance or TE Cloud) you currently must activate the MTA to listen on ALL interfaces (see [https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk107093](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk107093)):



#### **⚠ WARNING**

By default an implied rule is created allowing traffic to ALL interfaces on port 25 (SMTP). This will also leave the external interface on a cluster with a listening MTA. If the Check Point MTA is not the first MTA in the customers mail flow receiving emails from external we strongly recommend the following procedure to switch from this implied rule to FW rulebase MTA access.

```

admin@smesg:~
#define ENABLE_ICA_SSL
#define ENABLE_ISP_REDUNDANCY_PINGS
#define ENABLE_SWTP_SMS
#define ENABLE_SWTP_GW
#define ENABLE_STORMCENTER_BLOCKLISTS
#define ENABLE_VPN_CA_SERVERS_ENROLMENT
#define ENABLE_AV_HTTP
#ifdef CONTENT_SECURITY_ACTIVE
#define ENABLE_AV_SIGNATURE_UPDATE
#endif
/* #define ENABLE SMTP TO GW */
#define ENABLE_VRRP_PROTOCOL
#define ENABLE_INTEGRITY_SERVER_TRAFFIC
#define ENABLE_EPS_ENFORCE
#define DLPGWS_TRAFFIC
#define ENABLE_DYNAMIC_ROUTING_SYNC
#define ENABLE_GX_SAM

#define LAST_IMPLIED_RULE_NUM_USED 0x7a

#define IMPLIED_RECORD_CONN(rn) (PRE_COM_TAG_MATCH or RECORD_CONN(rn))

#ifdef IPV6_FLAVOR
"/opt/CPsuite-R77/fw1/lib/implied_rules.def" 2507L, 94813C written

```

To disable implied rule for access to **all GW IPs on port 25**:

- Edit \$FWDIR/lib/implied\_rules.def on the Management Server
- comment out the #define ENABLE\_SMTP\_TO\_GW line (as shown in the screenshot above)
- then install FW policy.

Afterwards you have to explicitly allow MTA access to the interfaces you need, e.g. with the following ruleset:

## Policy

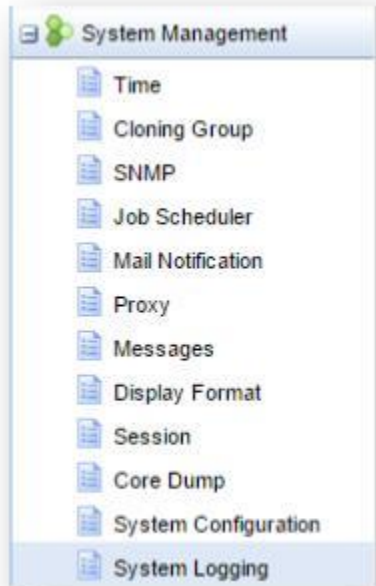
No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
1	0	Allow access to internal MTA	Net-10.2.1.0	MTA_int	Any Traffic	TCP smtp	accept	Log
2	0	Deny all other MTA traffic	Any	smesg	Any Traffic	TCP smtp	drop	Log

⚠ Also make sure that the following hotfix is installed in this environment:  
[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk109198](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk109198)

## 7.5.5.8 Feed MTA logs into SmartView Tracker / SmartLog

### Enabling Syslog forwarding to the Management Server

Email logs can be sent through to SmartLog using a feature in GAIa, but a change is needed on GAIa. Using GAIa, enable forwarding of Syslog to the management server under System Management -> System Logging.



Click to enable Syslog messages to be forwarded to the management server, then click apply. All Syslog messages will be sent to the management server and customer should confirm the additional logging space added.



You can then search based on email in SmartLog:  
Email message examples – shown here. Double click to open.

Query Top Results	Time	S...	L...	Origin	A...	Host
• Top Sources	11/Jun/2015 14:27:42	☺		gw		
• Top Destinations	11/Jun/2015 14:27:41	☺		gw		
• Top Services	11/Jun/2015 14:13:43	☺		gw		
• Top Actions	11/Jun/2015 14:13:42	☺		gw		
• Top Blades	11/Jun/2015 14:01:36	☺		gw		
• Top Origins	11/Jun/2015 14:01:36	☺		gw		
• Top Firewall Rules	11/Jun/2015 14:01:35	☺		gw		
• Top Users	11/Jun/2015 14:01:35	☺		gw		
• Top Applications	11/Jun/2015 13:56:42	☺		gw		
	11/Jun/2015 13:56:42	☺		gw		
	11/Jun/2015 13:51:47	☺		gw		
	11/Jun/2015 13:46:47	☺		gw		
	11/Jun/2015 13:41:47	☺		gw		
	11/Jun/2015 13:41:11	☺		gw		
	11/Jun/2015 13:41:11	☺		gw		
	11/Jun/2015 13:36:42	☺		gw		
	11/Jun/2015 13:33:05	☺		gw		
	11/Jun/2015 13:33:05	☺		gw		
	11/Jun/2015 13:33:05	☺		gw		

Message ID – shown here. Shows the message

More	
Default Device Mess...	<22>postfix/qmgr[27613] 9FB431778038: from=<tkendrick@checkpoint.com>, size=3789, nrcpt=1 (queue active)
Facility	mail system
Syslog Severity	Informational

### 7.5.5.9 /var/log/maillog size for PoC

Postfix message transfers are logged to /var/log/maillog.  
These logs are rotated after 65kb size and four rotated logs are stored by default.

In environment with high email volumes this sometimes only stores logs for several minutes.  
To extend the logs follow:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk93505&](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk93505&)

In short

- 1) Switch off email debugs if enabled:

```
[Expert@HostName:0]# fw debug in.emaild.mta off TDERROR_ALL_ALL=0
```

- 2) edit /etc/cpsshell/log\_rotation.conf:

```
admin@Gateway:/var/log
# File          max size      backlog
/var/log/messages      65536 4
/var/log/maillog        65536 4
/var/log/send_alert     65536 10
/var/log/blade_config   65536 15
/var/log/pingable_hosts 65536 10
/var/log/log_servers    65536 3
/var/log/routing_messages 64536 4
/var/log/wtmp           65536 4
/var/log/lastlog        262400 4
/var/log/secure         64536 4
/var/log/auditlog       65536 4
/var/log/asgaudit.log   102400 4
/var/log/smd_smo.log    524288000 1
/var/log/smd.log        1048576 4
/etc/cpsshell/log_rotation.conf
```

And change e.g. to 1MB files with 10 rotated files

```
admin@Gateway:/var/log
File          max size      backlog
/var/log/messages      65536 4
/var/log/maillog        10485760 10
/var/log/send_alert     65536 10
/var/log/blade_config   65536 15
/var/log/pingable_hosts 65536 10
/var/log/log_servers    65536 3
/var/log/routing_messages 64536 4
/var/log/wtmp           65536 4
/var/log/lastlog        262400 4
/var/log/secure         64536 4
/var/log/auditlog       65536 4
/var/log/asgaudit.log   102400 4
/var/log/smd_smo.log    524288000 1
/var/log/smd.log        1048576 4
"/etc/cpsshell/log_rotation.conf" 47L, 1926C
```

## 7.5.5.10 Debugging and Performance Troubleshooting Kit

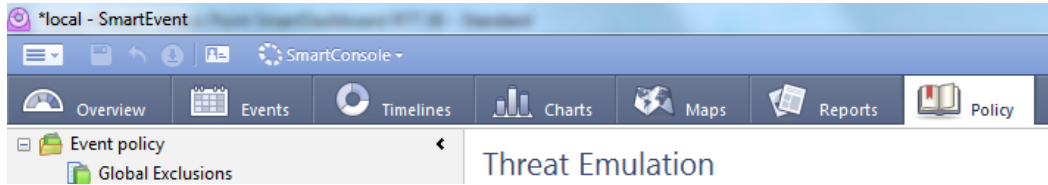
Further troubleshooting and performance tuning kit can be found here:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk120260](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120260)

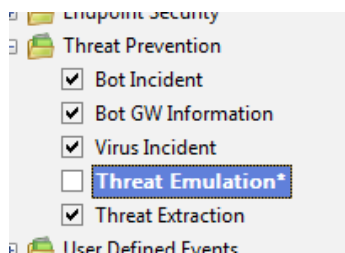
## 7.6 SmartEvent

### 7.6.1 How to configure e-mail alerts for High and Critical TE events

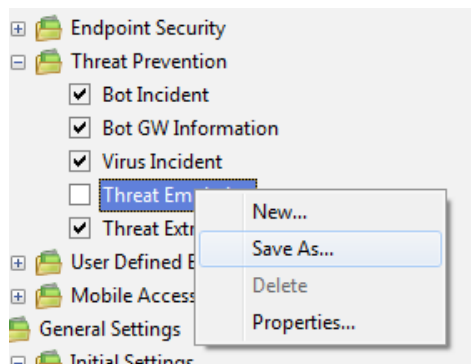
- 1) Goto the SE policy:



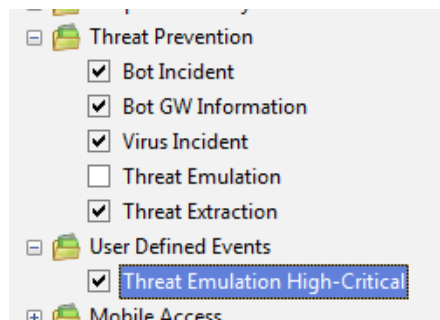
- 2) In the Event policy expand the *Threat Prevention* section and disable the default Threat Emulation rule



- 3) Afterwards save the rule with the name "Threat Emulation High-Critical"

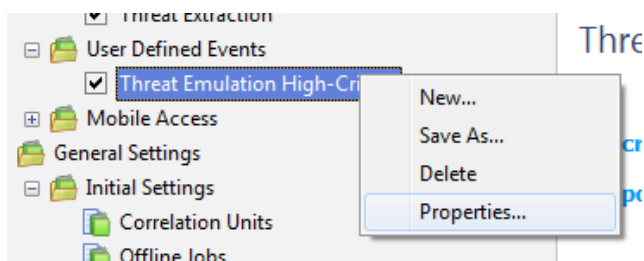


A new folder *User Defined Events* appears:

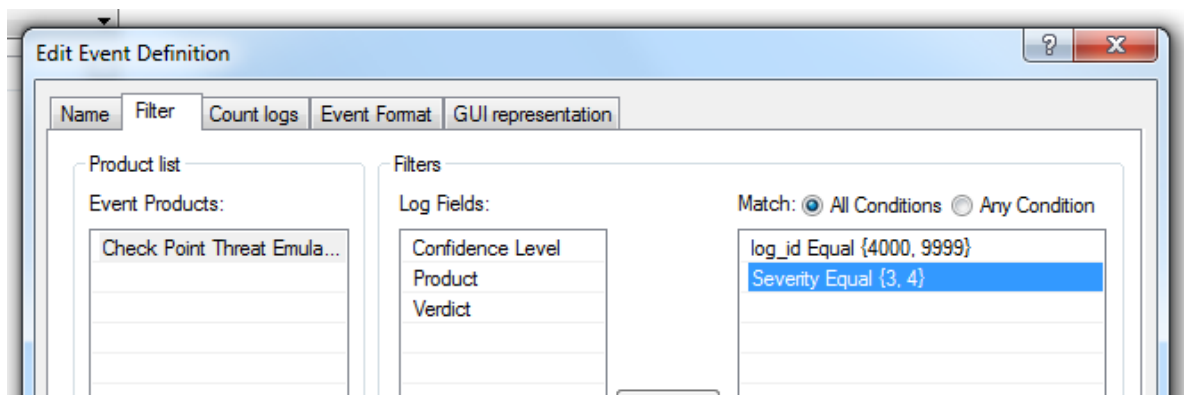




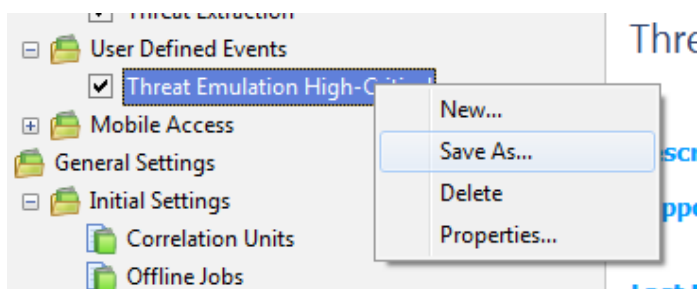
- 4) Right-click on the new rule and select *Properties*



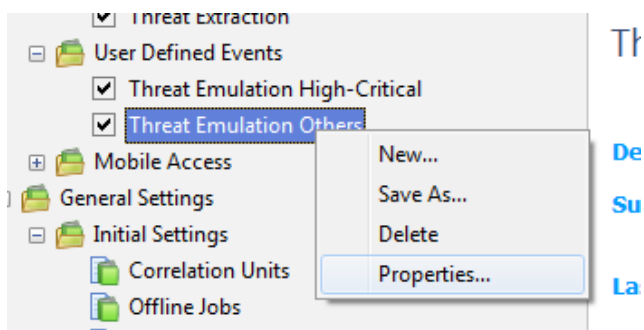
- 5) Select Tab *Filter* and with *Show more fields* add the *Severity* field equal to values **3** (High) and **4** (Critical)



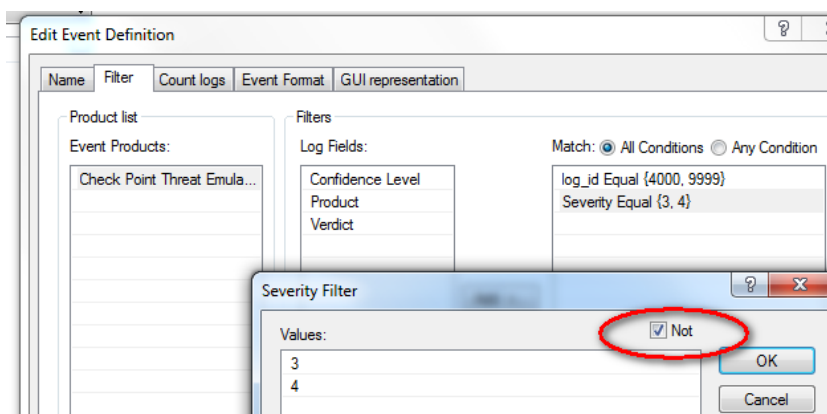
- 6) Now copy this newly created rule to "Threat Emulation Others"



- 7) Again edit the properties of this new rule



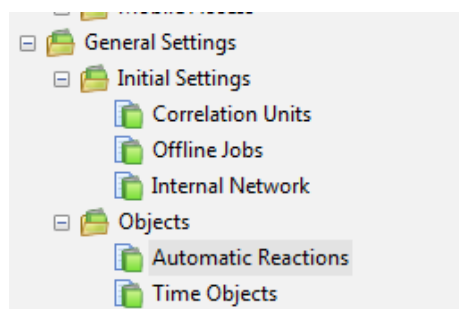
8) On the filter just negate the severities by selecting *Not*



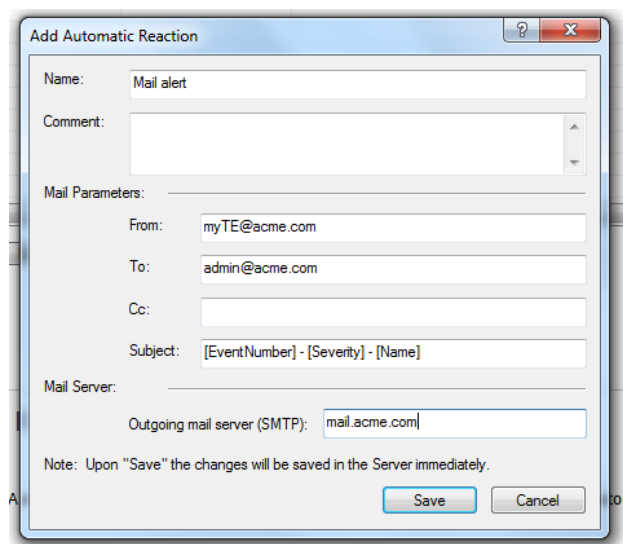
Now we have split the old rule “Threat Emulation” into “Threat Emulation High-Critical” and “Threat Emulation Others”. This is necessary because when you activate mail alerts for the default rule you would also get an email for all benign files probably flooding the admins mailbox. Also be aware that because of these rules events are created within SmartEvent. So simply applying the severity filter to the default rule would lead to missing informational, low, medium TE events in SmartEvent because there is no rule for these severities anymore.

After we split the rules **we now configure the mail alert for the “Threat Emulation High-Critical” rule:**

1) Goto *Automatic Reactions*

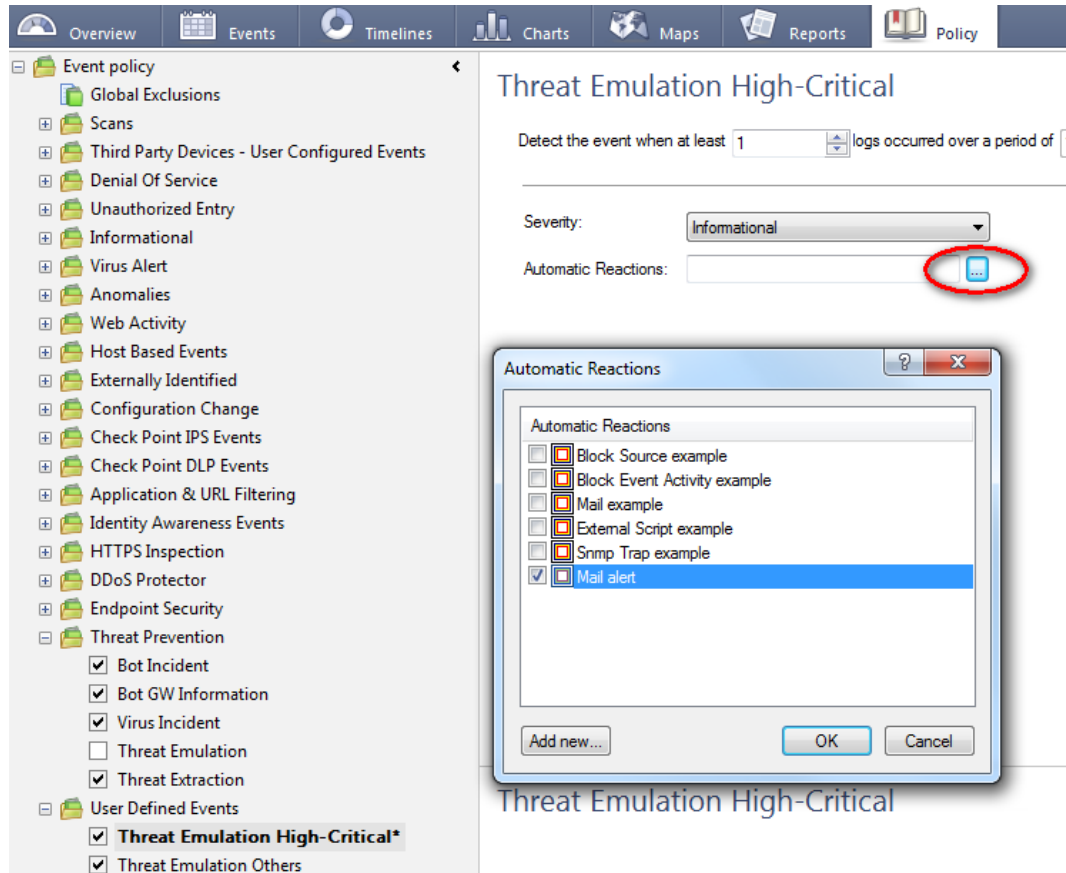


2) Create a new automatic response for mail

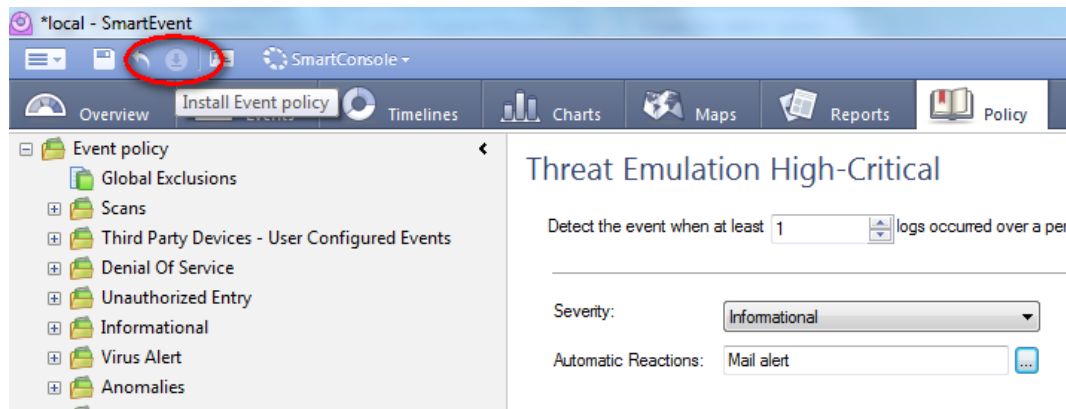


► Be sure that the SmartEvent server has mail relay permission on the “Outgoing mail server”

3) Now add the newly created automatic response to the rule



4) Do not forget to install the SmartEvent policy once you are done with the changes



⚠ When using this be aware of the following limitation:  
[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk106392](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk106392)

## 7.6.2 Bugfix for TE events with more than 3 malicious images

Within SmartEvent R77.30 there is currently a bug so that Threat Emulation logs appear in SmartLog / SmartView Tracker, but the events are missing in SmartEvent R77.x. This only happens if more than 3 images have the verdict malicious for a certain file. More infos can be found here:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk108492](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108492)

To remediate the issue follow this procedure on the SmartEvent server (so in case you have a all-in-one Sandblast Appliance and use SmartEvent there issue the commands on this appliance):

1. Connect to command line on machine that runs the involved SmartEvent server R77.x.
2. Log in to Expert mode.
3. Stop the SmartEvent services:

```
[Expert@HostName:0]# evstop
```

4. Connect to the events database:

```
$CPDIR/database/postgresql/bin/psql -U cp_postgres -p 18272 events_db
```

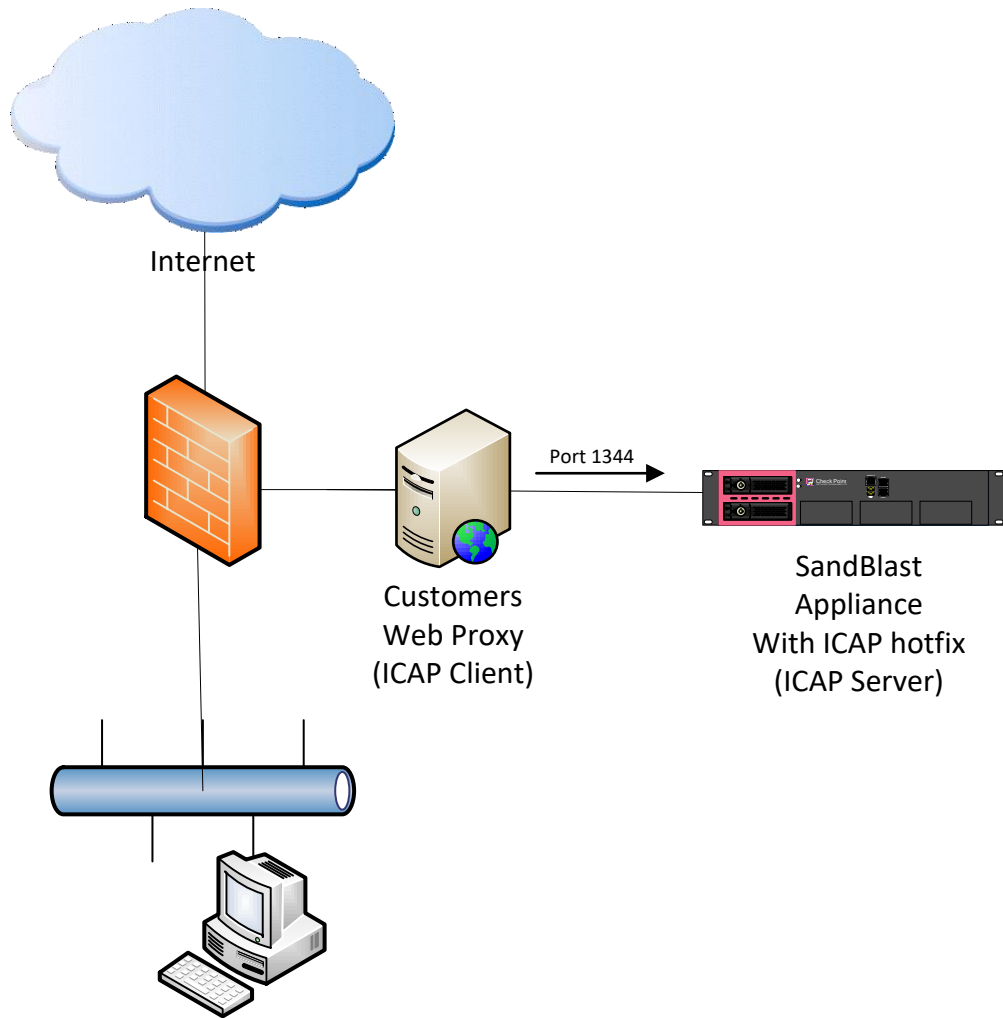
5. In the prompt, enter the following two commands:

```
alter table multipacketcapture alter column packet_capture_unique_id type varchar(2048);  
\q
```

6. Start the SmartEvent services:

```
[Expert@HostName:0]# evstart
```

## 8. ICAP



## 8.1 ICAP Server

The official ICAP Server SK mentions requirements, release notes and general information regarding the new ICAP server functionality.

Check Point support for Internet Content Adaptation Protocol (ICAP) server

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk111306](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111306)

ICAP Server is included since JHF 272.

```
Start:          # icap_server start
Stop:           # icap_server stop
Reconfiguration: # icap_server reconf
```

### Note:

- (1) **ICAP does not choose emulation images based on any of your TP profiles**
- (2) Choosing to emulate on all images will result in an attempt to emulate the files on all known images, even if some of them aren't available.
- (3) "Recommended Images" means two images (Win7/Office2013, WinXP/Office2003-7)

## 8.2 Configuration

### 8.2.1 Configuration files

Filename	Location	Purpose
<b>c-icap.conf</b>	\$FWDIR/c-icap/etc/	ICAP Server process configuration file e.g. for changing ICAP server port
<b>c-icap.magic</b>	\$FWDIR/c-icap/etc/	Filetypes supported by ICAP
<b>virus_scan.conf</b>	\$FWDIR/c-icap/etc/	e.g. for adding filetypes from c-icap.magic, maximum file size
<b>libsb_mod.conf</b>	\$FWDIR/c-icap/etc/	e.g. for adding filetypes from c-icap.magic
<b>Tpapi.py</b>	\$FWDIR/c-icap/scripts/	Script used to send ICAP received files to TE API
<b>Block message</b>	\$FWDIR/c-icap/share/c_icap/templates/virus_scan/en  -rwxr-x--- 1 admin bin 392 Mar 30 09:02 <b>VIRUS_FOUND</b>	Block messages displayed when malware is found. If you change them don't forget to run ICAP daemon reconf command  VIRUS_FOUND is used as template for a block message; this message can be localized

## 8.2.2 Configure emulation images

### 8.2.2.1 All or recommended images

Choose emulation on all images or only on recommended images:

1. Open for editing: `$FWDIR/c-icap/etc/libsb_mod.conf`
2. Change the field `sb_mod.AllImages` to `off` (for recommended) or `on` (for all)

### 8.2.2.2 Configure specific emulation images

Not officially supported but there is a way of selecting only specific images to emulate on:

- Edit `$FWDIR/c-icap/etc/libsb_mod.conf`
- Change the field `sb_mod.AllImages` to `on`
- Edit `$FWDIR/c-icap/scripts/TPAPI.py`
- Add "#" in front of images you do not want to emulate on:

```
image_to_name = {
    # 'e50e99f3-5963-4573-af9e-e3f4750b55e2': 'WinXP,Office 2003/7,Adobe 9',
    # '7e6fe36e-889e-4c25-8704-56378f0830df': 'Win7,Office 2003/7,Adobe 9',
    # '8d188031-1010-4466-828b-0cd13d4303ff': 'Win7,Office 2010,Adobe 9.4',
    # '5e5de275-a103-4f67-b55b-47532918fa59': 'Win7,Office 2013,Adobe 11',
    # '3ff3ddae-e7fd-4969-818c-d5f1a2be336d': 'Win7 64b,Office 2013,Adobe 11',
    # '6c453c9b-20f7-471a-956c-3198a868dc92': 'Win8.1 64b,Office 2013,Adobe 11',
}

te_images = [
    # {'id': 'e50e99f3-5963-4573-af9e-e3f4750b55e2', 'revision': 1},
    # {'id': '7e6fe36e-889e-4c25-8704-56378f0830df', 'revision': 1},
    # {'id': '8d188031-1010-4466-828b-0cd13d4303ff', 'revision': 1},
    # {'id': '5e5de275-a103-4f67-b55b-47532918fa59', 'revision': 1},
    # {'id': '3ff3ddae-e7fd-4969-818c-d5f1a2be336d', 'revision': 1},
    # {'id': '6c453c9b-20f7-471a-956c-3198a868dc92', 'revision': 1},
]
```

### 8.2.2.3 Adding Windows 10 image for ICAP emulation

Even though you activate the Win10 image in the GUI it will not be used by the ICAP emulation because the images for image are solely selected based on a configuration file. To add the Win10 image follow this procedure:

- Edit `$FWDIR/c-icap/etc/libsb_mod.conf`
- Change the field `sb_mod.AllImages` to **on**

Edit `$FWDIR/c-icap/scripts/TPAPI.py` and add the following yellow lines:

```
image_to_name = {
    'e50e99f3-5963-4573-af9e-e3f4750b55e2': 'WinXP,Office 2003/7,Adobe 9',
    '7e6fe36e-889e-4c25-8704-56378f0830df': 'Win7,Office 2003/7,Adobe 9',
    '8d188031-1010-4466-828b-0cd13d4303ff': 'Win7,Office 2010,Adobe 9.4',
    '5e5de275-a103-4f67-b55b-47532918fa59': 'Win7,Office 2013,Adobe 11',
    '3ff3ddae-e7fd-4969-818c-d5f1a2be336d': 'Win7 64b,Office 2013,Adobe 11',
    '6c453c9b-20f7-471a-956c-3198a868dc92': 'Win8.1 64b,Office 2013,Adobe 11',
    '10B4A9C6-E414-425C-AE8B-FE4DD7B25244': 'Win10 64b,Office 2016, Adobe DC'
}

te_images = [
    {'id': 'e50e99f3-5963-4573-af9e-e3f4750b55e2', 'revision': 1},
    {'id': '7e6fe36e-889e-4c25-8704-56378f0830df', 'revision': 1},
    {'id': '8d188031-1010-4466-828b-0cd13d4303ff', 'revision': 1},
    {'id': '5e5de275-a103-4f67-b55b-47532918fa59', 'revision': 1},
    {'id': '3ff3ddae-e7fd-4969-818c-d5f1a2be336d', 'revision': 1},
    {'id': '6c453c9b-20f7-471a-956c-3198a868dc92', 'revision': 1},
    {'id': '10B4A9C6-E414-425C-AE8B-FE4DD7B25244', 'revision': 1}
]
```

### 8.2.3 Attaching an ICAP Client

Configure the ICAP client to communicate with the ICAP server's "sandblast" service.

For example: `icap://<ip address>:1344/sandblast`



## 8.3 Logging

### 8.3.1 General logging

Logging is limited to the following log files – so no ICAP daemon logs in the GUI/SmartLog:

```
$FWDIR/log/c-icap/server.log  
$FWDIR/log/c-icap/access.log
```

#### *Highly Recommended*

To extend the by default limited access log follow these steps:

- 2) `vi /opt/CPsuite-R77/fw1/c-icap/etc/c-icap.conf`
- 3) Search for “AccessLog /opt/CPsuite-R77/fw1/log/c-icap/access.log”
- 4) Add this line before the above finding:
  - `LogFormat accessFormat "%tl, %la %a %im %iu %is %huo '%<ho' '%{X-Infection-Found}<ih'"`
- 5) Change the AccessLog line to:
  - `AccessLog /opt/CPsuite-R77/fw1/log/c-icap/access.log accessFormat`

So the section in c-icap.conf should now look like this:

```
LogFormat accessFormat "%tl, %la %a %im %iu %is %huo '%<ho' '%{X-Infection-Found}<ih'"  
AccessLog /opt/CPsuite-R77/fw1/log/c-icap/access.log accessFormat
```

### 8.3.2 Enable logging of benign files

Enable/Disable logs on benign files:

1. Open for editing: `$FWDIR/c-icap/etc/libsb_mod.conf`
2. Change the field `sb_mod.LogBenign` to `on`

### 8.3.3 Debug logging

To enable debug logging:

1. Open for editing: `$FWDIR/c-icap/etc/c-icap.conf`
2. Change `DebugLevel` value to: 7
3. Restart the c-icap service.

Note ! Enabling debug logs can affect performance.

## 8.4 ICAP daemon troubleshooting

### 8.4.1 Start manually and get errors on startup

To get ICAP server daemon error messages on the terminal when starting launch daemon with:

```
# $FWDIR/c-icap/bin/c-icap -N -D -d 10 -f $FWDIR/c-icap/etc/c-icap.conf
```

### 8.4.2 Verify ICAP daemon is running

```
[Expert@sandblast]# netstat -na | grep 1344
```

Result should show:


```
tcp          0          0 0.0.0.0:1344          0.0.0.0:*          LISTEN
```

```
[Expert@sandblast]# ps ax | grep c-icap
```

Result should show:

```
16443 ?          Ss      0:00 c-icap -N -f /opt/CPsuite-R77/fw1/c-icap/etc/c-icap.conf
16448 ?          Sl      0:00 c-icap -N -f /opt/CPsuite-R77/fw1/c-icap/etc/c-icap.conf
16453 ?          Sl      0:00 c-icap -N -f /opt/CPsuite-R77/fw1/c-icap/etc/c-icap.conf
16460 ?          Sl      0:00 c-icap -N -f /opt/CPsuite-R77/fw1/c-icap/etc/c-icap.conf
19319 pts/2    S+      0:00 grep c-icap
```

## 8.5 Sample configurations

 All of the following sample configurations are provided as a guideline. It is the customer's responsibility to configure their ICAP clients properly. We do not take responsibilities for any side effects caused by the below settings as we are no 3<sup>rd</sup> party Web proxy specialists :-)

### 8.5.1 SQUID proxy

#### 8.5.1.1 SQUID compilation flags and version

Squid Cache: Version 3.3.8

Ubuntu - configure options:

```
'--build=x86_64-linux-gnu' '--prefix=/usr' '--includedir=${prefix}/include' '--mandir=${prefix}/share/man' '--infodir=${prefix}/share/info' '--sysconfdir=/etc' '--localstatedir=/var' '--libexecdir=${prefix}/lib/squid3' '--srcdir=. ' '--disable-maintainer-mode' '--disable-dependency-tracking' '--disable-silent-rules' '--datadir=/usr/share/squid3' '--sysconfdir=/etc/squid3' '--mandir=/usr/share/man' '--enable-inline' '--enable-async-io=8' '--enable-storeio=ufs,aufs,diskd,rock' '--enable-removal-policies=lru,heap' '--enable-delay-pools' '--enable-cache-digests' '--enable-underscores' '--enable-icap-client' '--enable-follow-x-forwarded-for' '--enable-auth-basic=DB,fake,getpwnam,LDAP,MSNT,MSNT-multi-domain,NCSA,NIS,PAM,POP3,RADIUS,SASL,SMB' '--enable-auth-digest=file,LDAP' '--enable-auth-negotiate=kerberos,wrapper' '--enable-auth-ntlm=fake,smb_lm' '--enable-external-acl-helpers=file_userip,kerberos_ldap_group,LDAP_group,session,SQL_session,unix_group,wbinfo_group' '--enable-url-rewrite-helpers=fake' '--enable-eui' '--enable-esi' '--enable-icmp' '--enable-zph-qos' '--enable-ecap' '--enable-ssl' '--enable-ssl-crtld' '--disable-translation' '--with-swapdir=/var/spool/squid3' '--with-logdir=/var/log/squid3' '--with-pidfile=/var/run/squid3.pid' '--with-filedescriptors=65536' '--with-large-files' '--with-default-user=proxy' '--enable-linux-netfilter' 'build_alias=x86_64-linux-gnu' 'CFLAGS=-g -O2 -fPIE -fstack-protector --param=ssp-buffer-size=4 -Wformat -Werror=format-security -Wall' 'LDFLAGS=-Wl,-Bsymbolic-functions -fPIE -pie -Wl,-z,relro -Wl,-z,now' 'CPPFLAGS=-D_FORTIFY_SOURCE=2' 'CXXFLAGS=-g -O2 -fPIE -fstack-protector --param=ssp-buffer-size=4 -Wformat -Werror=format-security'
```

#### 8.5.1.2 SQUID sample configuration

```
acl localnet src 192.168.6.0/24
acl localnet src 10.0.0.0/8
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443        # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#
#Next Proxy configuration
#
#follow_x_forwarded_for allow all
#cache_peer 194.29.36.43 parent 8080 0 no-query no-digest
#never_direct deny localnet
#never_direct allow all
#forwarded_for on

#
#access list
#
http_access allow Safe_ports
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localhost
http_access allow localnet
http_access deny all
#

#sslproxy_cert_error allow all
#always_direct allow all
```

```

#ssl_bump allow all

http_port 8080

#http_port 8080 ssl-bump cert=/etc/squid3/certs/teProxy.pem key=/etc/squid3/certs/teProxy.pem ssl-bump
generate-host-certificates=on dynamic_cert_mem_cache_size=4MB

# SSL Bump Config
#ssl_bump stare all
#ssl_bump bump all

hierarchy_stoplist cgi-bin ?
debug_options ALL,1
coredump_dir /var/spool/squid3
refresh_pattern ^ftp:      1440      20%      10080
refresh_pattern ^gopher:   1440      0%       1440
refresh_pattern -i (/cgi-bin/|\?) 0      0%       0
refresh_pattern (Release|Packages|.gz)*$ 0      20%      2880
refresh_pattern .          0      20%      4320
visible_hostname Azoulay's proxy

#ICAP

icap_enable off
icap_preview_enable on
icap_preview_size 1024
icap_send_client_ip on

#icap_service service_req reqmod_precache icap://82.80.83.10:1344/virus_scan
#adaptation_access service_req allow all

#icap_service service_resp_pre respmod_precache icap://82.80.83.10:1344/virus_scan
#icap_service service_resp_post respmod_postcache icap://82.80.83.10:1344/virus_scan
#adaptation_access service_resp_pre allow all
#adaptation_access service_resp_post allow all
#Until HERE

#DO NOT COPY
#new_c-icap_integration
#icap_service service_req reqmod_precache icap://192.168.24.250:1344/virus_scan
#adaptation_access service_req allow all
#icap_service service_resp_pre respmod_precache icap://192.168.6.25:1344/virus_scan
#icap_service service_resp_post respmod_postcache icap://192.168.6.25:1344/virus_scan
#adaptation_access service_resp_pre allow all
#adaptation_access service_resp_post allow all

```

## 8.5.2 McAfee Web Gateway 7.6

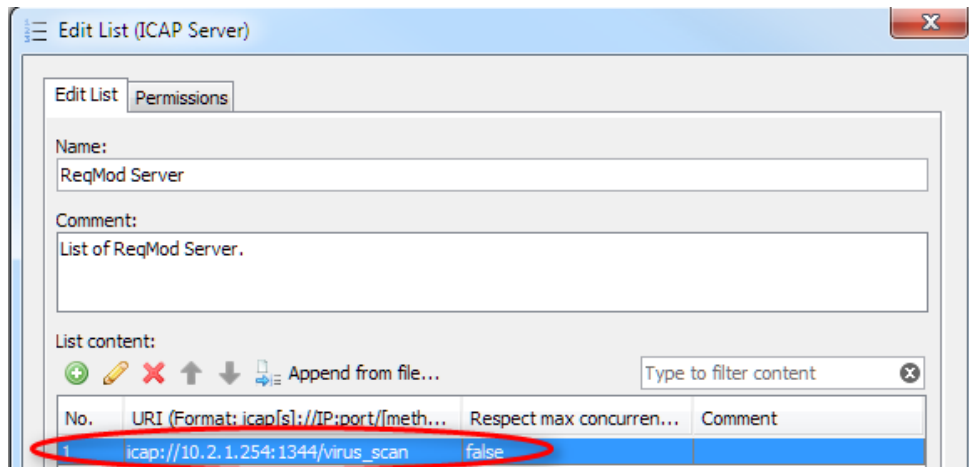
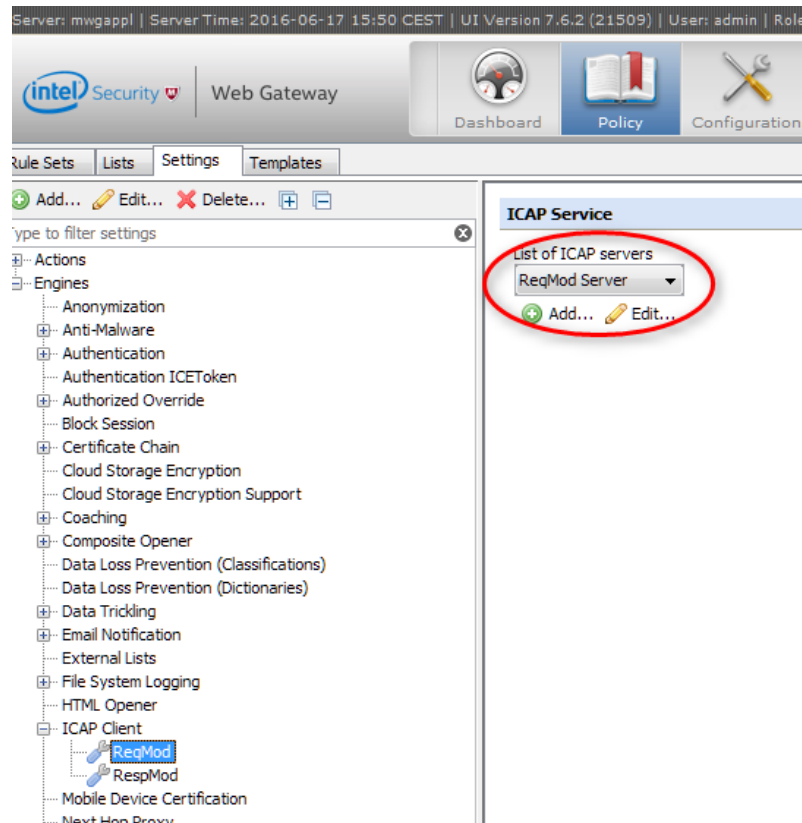
Below settings will be enforced by the McAfee Web Gateway in PREVENT mode meaning it will wait for the TE's answer until emulation is completed. If you need a "background" scanning configuration for McAfee Web Gateway and the customer does not know how to implement this please contact us via our mailing list.

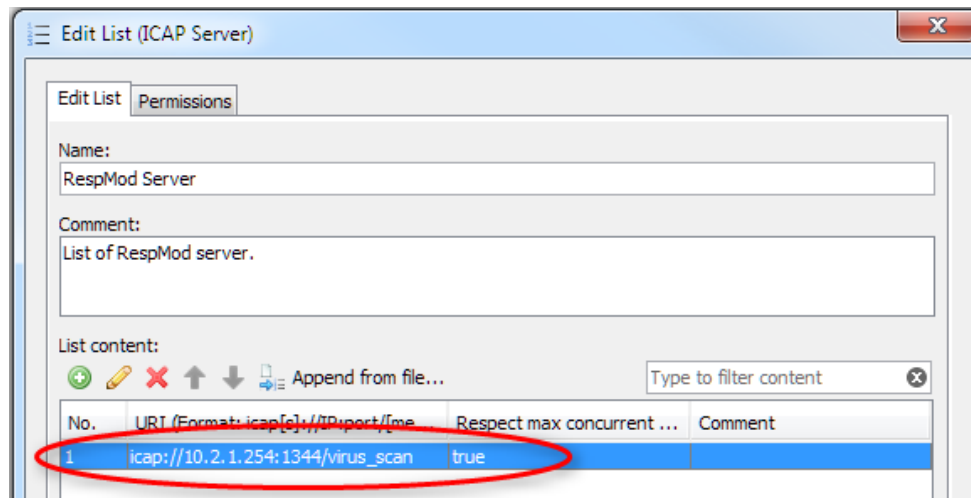
### 8.5.2.1 Configuring the Check Point ICAP Server

Use our default settings as described in the ICAP release notes.

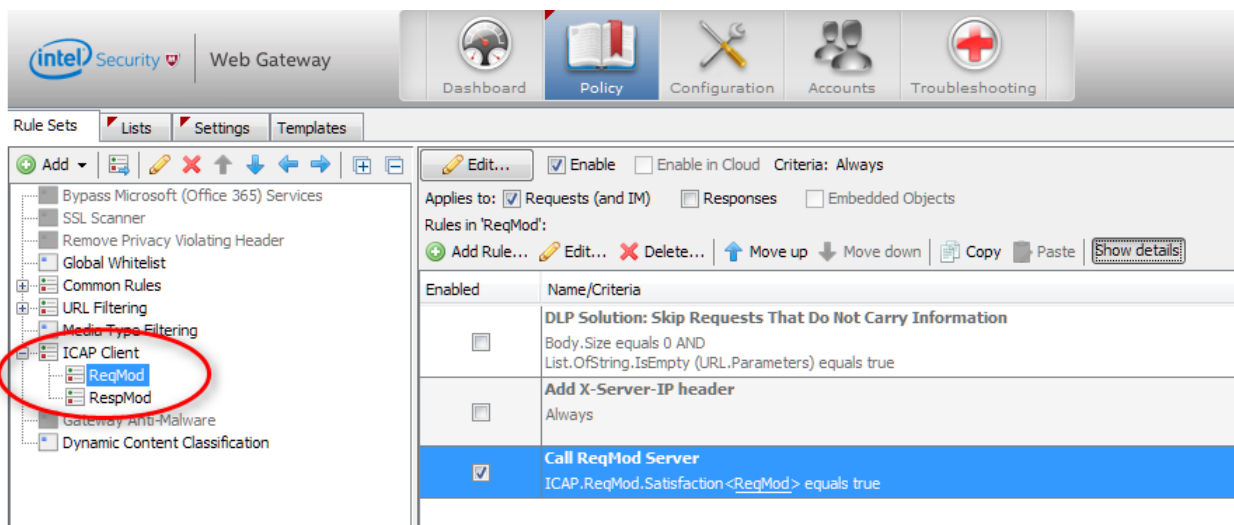
### 8.5.2.2 Configuration McAfee ICAP client

Under *Policy -> Settings -> ICAP Client* change **both** the **ReqMod** and **RespMod** defaults (we configure both but you only need RespMod for file downloads and ReqMod for file uploads):

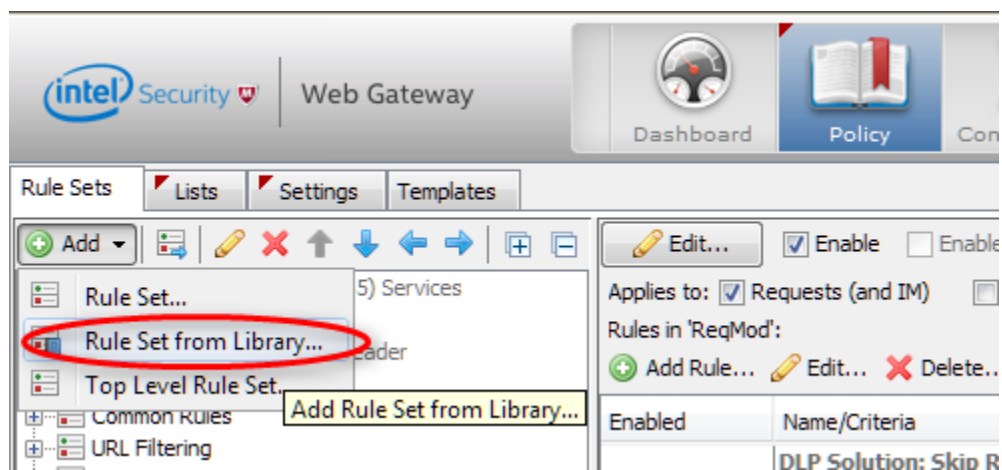


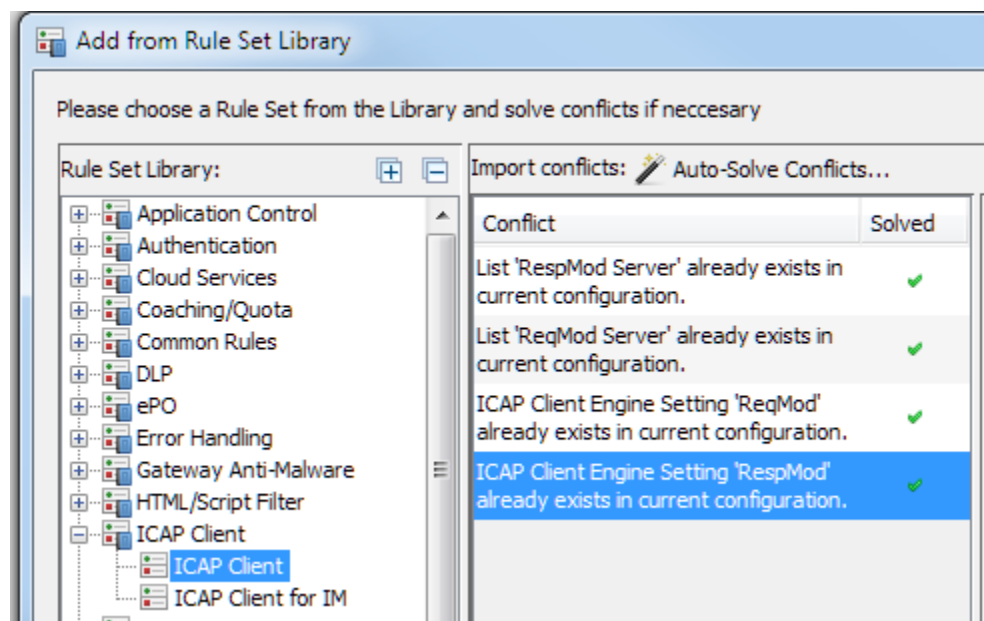


Under *Policy* -> *Rule Sets* check if ICAP Client section is present:



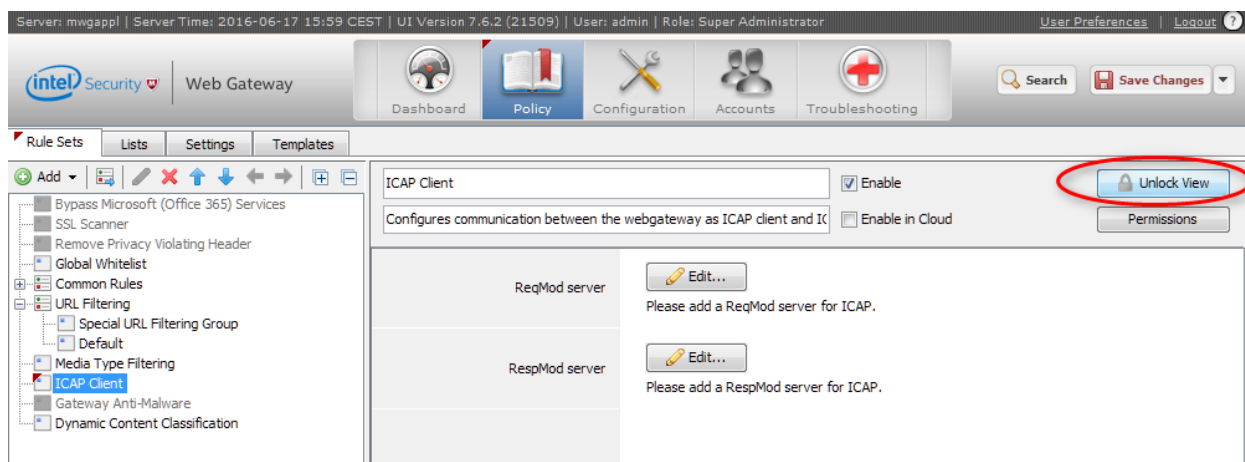
If not you can add it via *Add -> Rule Set from Library*:



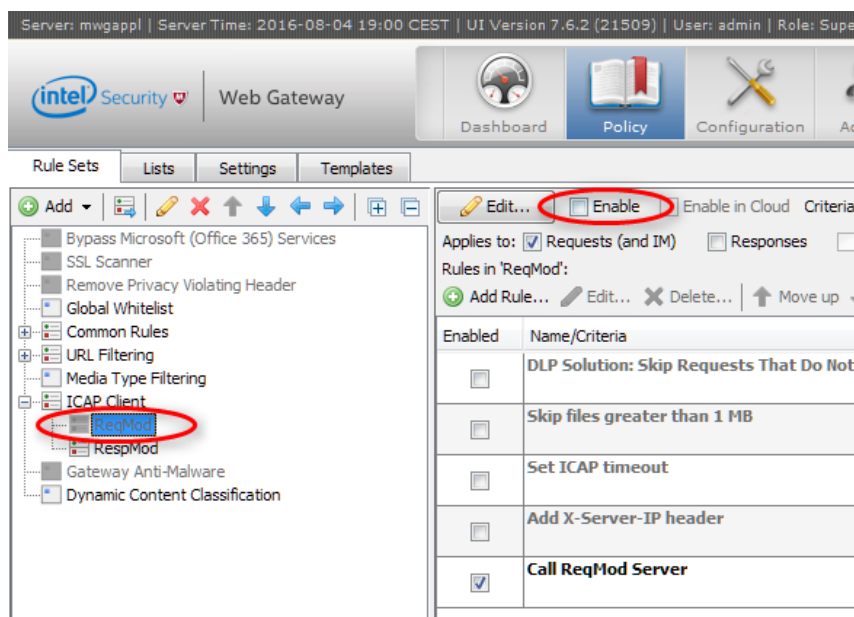




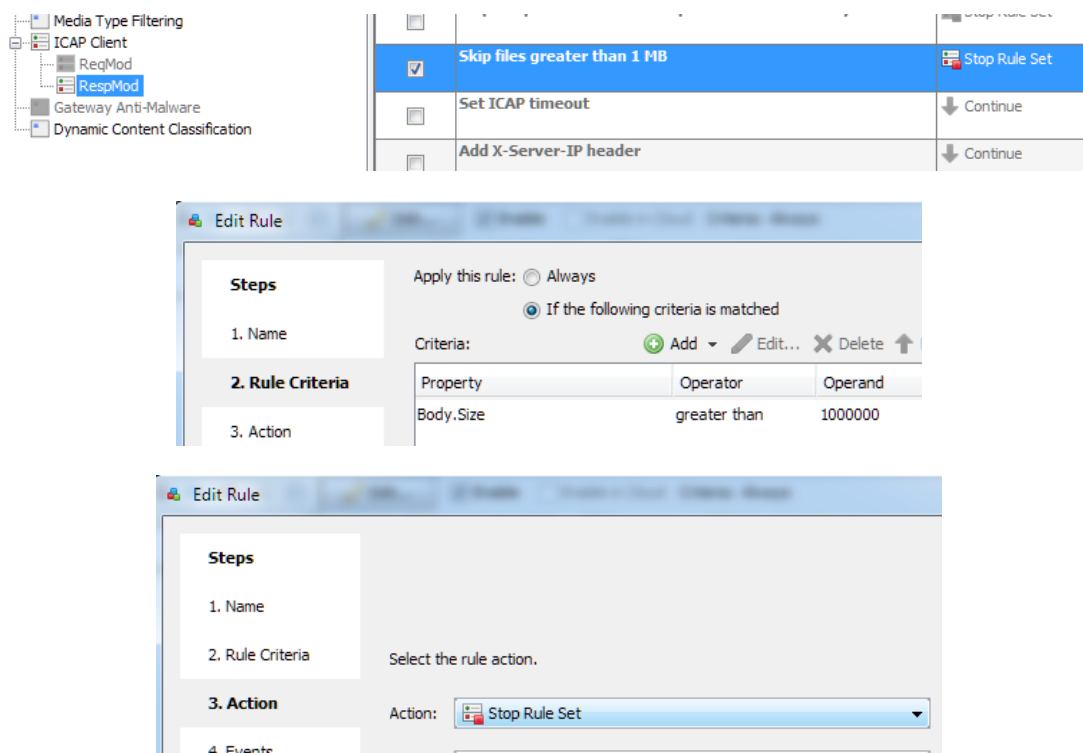
To edit the imported rule set “Unlock View”:



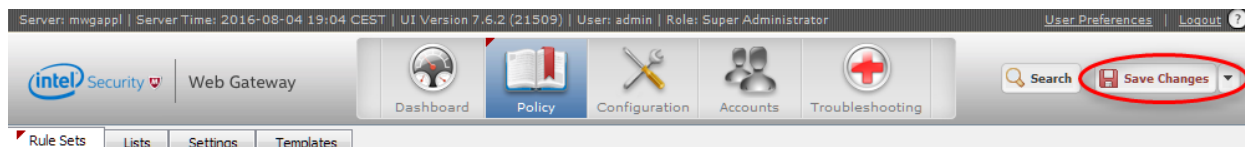
You can disable “ReqMod” if it is not needed to pass downloaded files (only for file uploads):



If you want to bypass file downloads e.g. bigger than 1 MB you have to add the following “Skip files greater than 1MB” rule to the **RespMod** ruleset:

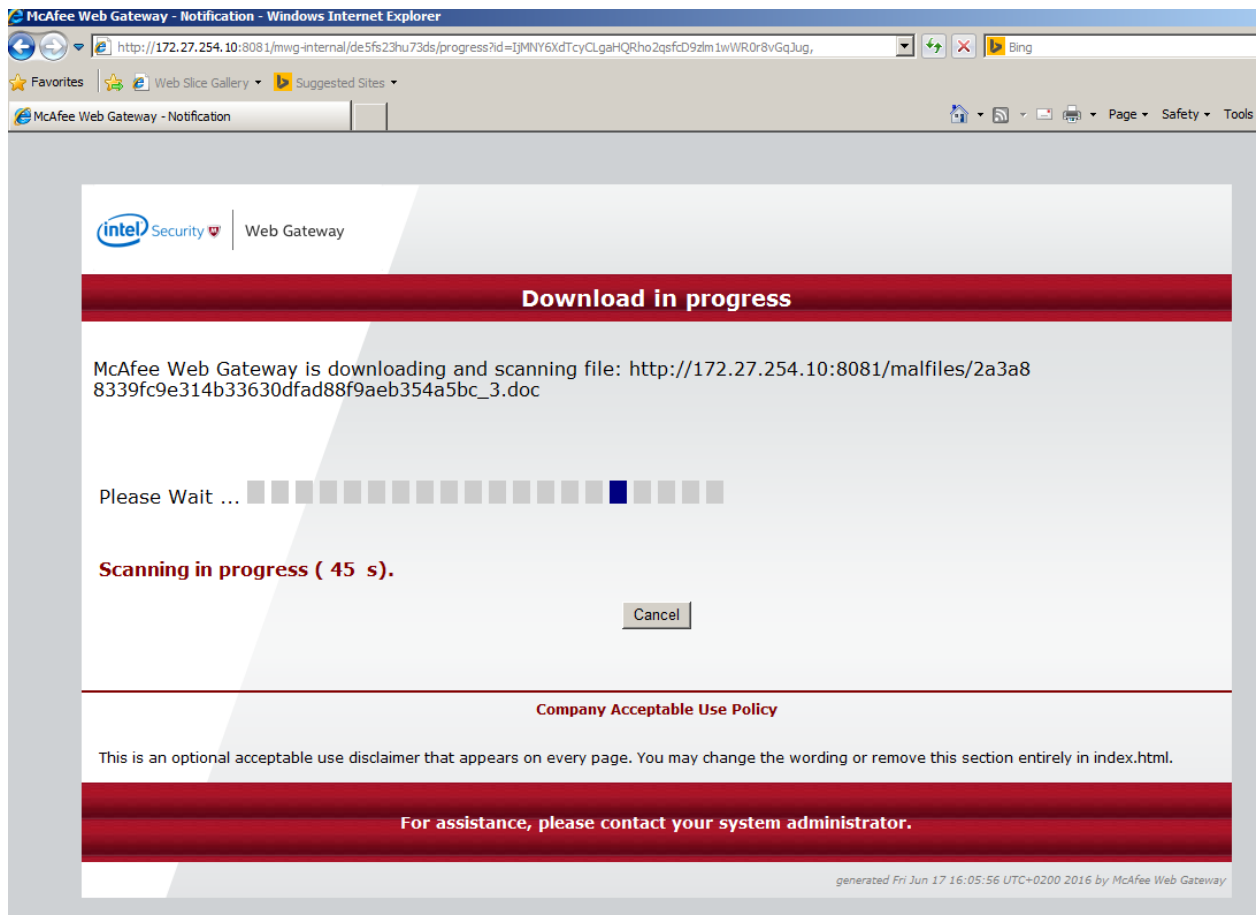


Don't forget to save your changes at the end:



This is what you get when trying to download a malicious file detected by TE:

6) Client McAfee Web Gateway Progress page:



## 7) Access.log and "tecli s e e"

```
admin@smesg:/opt/CPsuite-R77/fw1/log/c-icap
drwxrwx--- 10 admin bin 4096 Jun 17 07:50 ..
-rw-r--r-- 1 admin root 87756 Jun 17 15:04 access.log
-rw-r--r-- 1 admin root 3344 Jun 17 14:21 server.log
[Expert@smesg:0]# tail -f access.log
17/Jun/2016:15:03:14 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:03:25 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:03:36 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:03:47 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:03:58 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:04:09 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:04:20 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:04:31 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:04:42 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:04:53 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'

17/Jun/2016:15:05:04 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:05:11 +0100, 10.2.1.254 10.2.1.11 REQMOD virus_scan 200 http://172.27.25
4.10:8081/malfiles/2a3a88339fc9e314b33630dfad88f9aeb354a5bc_3.doc '-' '-'
17/Jun/2016:15:05:15 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:05:26 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:05:37 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:05:48 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:05:59 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'

admin@smesg:/opt/CPsuite-R77/fw1/c-icap/share/c_icap/templates/virus_scan/en
Every 2.0s: tecli s e e Fri Jun 17 15:06:06 2016

Pending emulating requests: 0
Running virtual machines: 2
Number of emulated files: 1

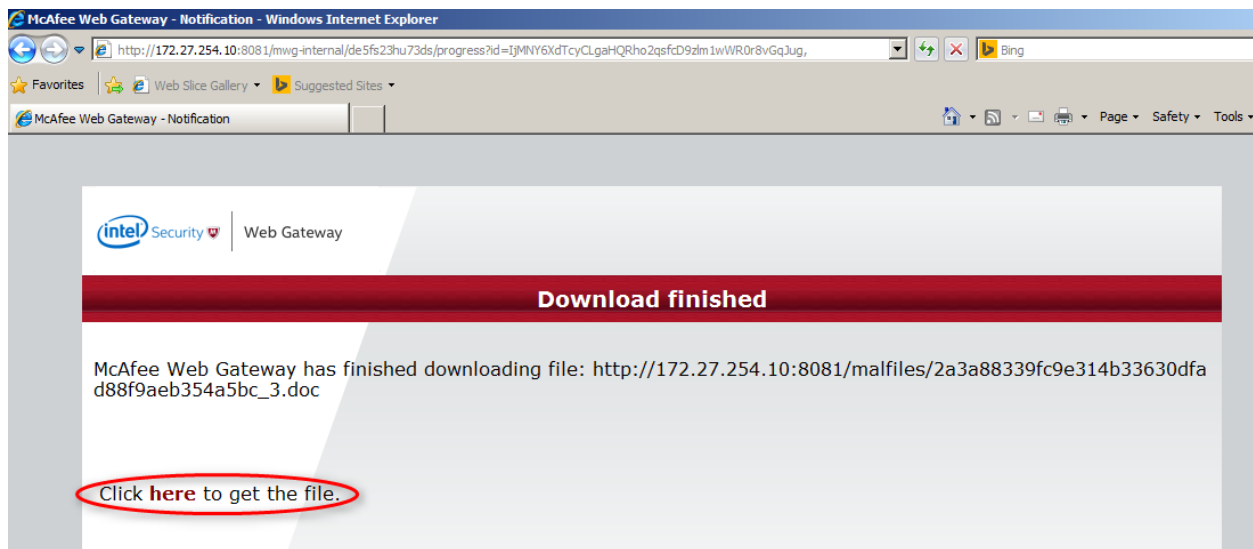
File ID (SHA1) File Name Emulation Required St
atus
-----
02a635887e30125b51915af9e6ecdb9a872d16a4 2a3a88339fc...3.doc Win7,Office 2013... Ma
licious
WinXP,Office 200... Ma
licious
```

## 8) After emulation is finished we sent back the malicious verdict:

Access.log

```
17/Jun/2016:15:08:01 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:08:12 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:08:23 +0100, 10.2.1.254 10.2.1.11 OPTIONS virus_scan 200 - '-' '-'
17/Jun/2016:15:08:25 +0100, 10.2.1.254 10.2.1.11 RESPMOD virus_scan 200 http://172.27.2
54.10:8081/malfiles/2a3a88339fc9e314b33630dfad88f9aeb354a5bc_3.doc 'HTTP/1.0 403 Forbid
den' 'Type=0; Resolution=2; Threat=Unknown;'
```

9) At the client you still get the download link:

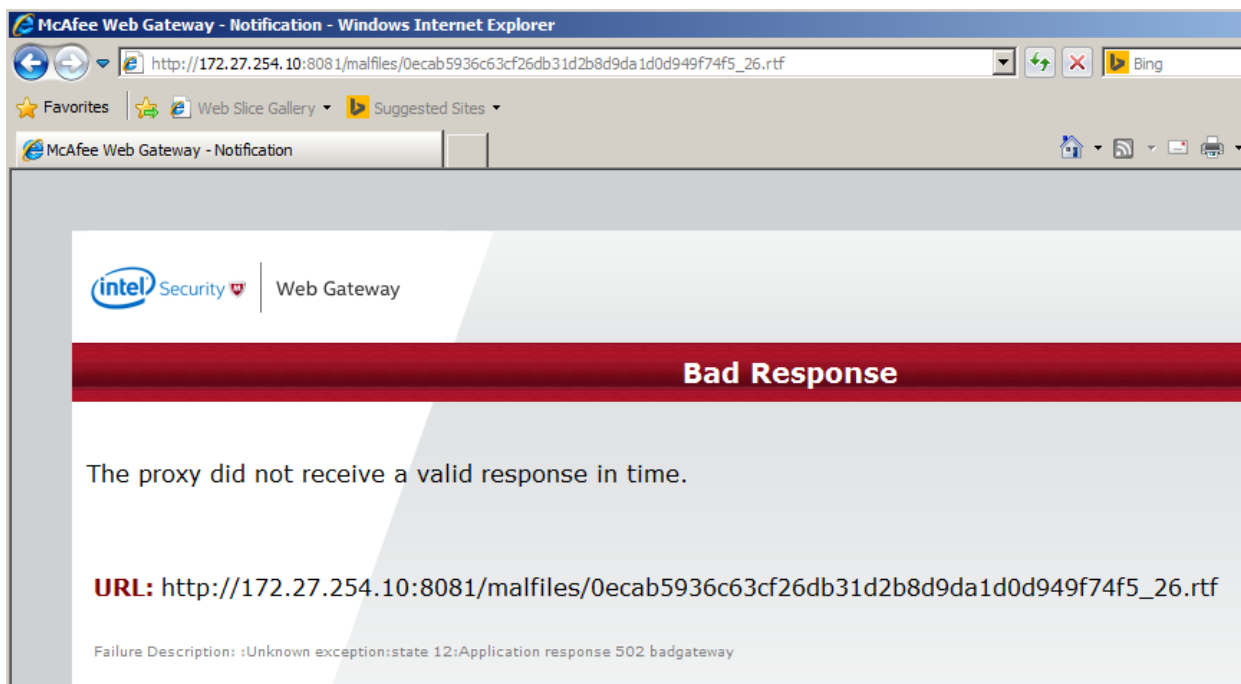


10) But when clicking on “here”:

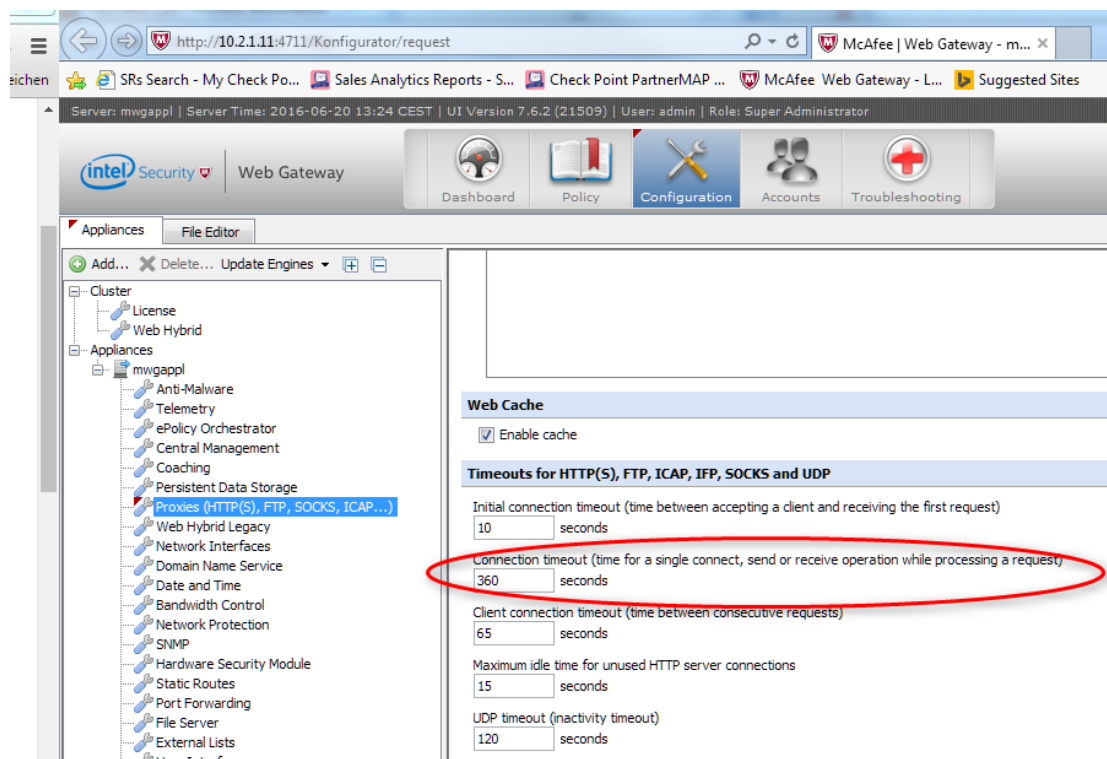


Note: The above screenshot is already a customized VIRUS\_FOUND template (see section 3.2.1)

If you experience proxy timeouts like this:



Raise the timeout value from default 120sec. to > 300 sec.



## 8.6 ICAP Miscellaneous

### 8.6.1 Add “Protection Type: ICAP emulation” to SmartLog/Event searches

In order to add a new “enum” to the protection type picker:

1. Edit the file:  
\$RTDIR/[conf/fields-enums.xml](#)
2. Search for “<name>protection\_type</name>”
3. Copy and add another “value” section inside it.
4. Change displayName and logValue accordingly.
5. Run evstop; evstart

Value should be “ICAP emulation” e.g.

```
<value>
    <logValue>ICAP emulation</logValue>
    <displayName>ICAP emulation</displayName>
    <icon>Blades/threat_emulation</icon>
    <icon_bw>Blades/threat_emulation</icon_bw>
    <story_script>story_threat_emulation</story_script>
    <picker>true</picker>
</value>
```

## 8.6.2 Access.log – available log variables

### Source

[http://c-icap.sourceforge.net/c-icap.conf-0.4.x.html#tag\\_LogFormat](http://c-icap.sourceforge.net/c-icap.conf-0.4.x.html#tag_LogFormat)

### LogFormat

#### Format:

LogFormat Name Format

#### Description:

Name is a name for this log format.

Format is a string with embedded % format codes. % format codes has the following form:

% [-] [width] [{argument}] formatcode  
if - is specified then the output is left aligned  
if width specified then the field is exactly width size  
some formatcodes support arguments given as {argument}

#### Format codes:

%a: Remote IP-Address  
%la: Local IP Address  
%lp: Local port  
%>a: Http Client IP Address. Only supported if the proxy client supports the "X-Client-IP" header  
%<A: Http Server IP Address. Only supported if the proxy client supports the "X-Server-IP" header  
%ts: Seconds since epoch  
%tl: Local time. Supports optional strftime format argument  
%tg: GMT time. Supports optional strftime format argument  
%>ho: Modified Http request header. Supports header name as argument. If no argument given the first line returned  
%huo: Modified Http request url  
%<ho: Modified Http reply header. Supports header name as argument. If no argument given the first line returned  
%iu: Icap request url  
%im: Icap method  
%is: Icap status code  
%>ih: Icap request header. Supports header name as argument. If no argument given the first line returned  
%<ih: Icap response header. Supports header name as argument. If no argument given the first line returned  
%lh: Http bytes received  
%Oh: Http bytes sent  
%lb: Http body bytes received  
%Ob: Http body bytes sent  
%l: Bytes received  
%O: Bytes sent  
%bph: The first 5 bytes of the body preview data. Non printable characters printed in hex form. Supports the number of bytes to output as argument.  
%un: Username  
%Sl: Service log string  
%Sa: Attribute value set by service. The attribute name must given as argument.

#### Default:

None set

#### Example:

LogFormat myFormat "%tl, %a %im %iu %is %l %O %lb %Ob %{10}bph"



## 8.6.3 ICAP Server response codes

{100, "Continue"},	/*Continue after ICAP Preview */
{200, "OK"},	
{204, "Unmodified"},	/*No modifications needed */
{206, "Partial Content"},	/*Partial content modification*/
{400, "Bad request"},	/*Bad request */
{403, "Forbidden"},	
{404, "Service not found"},	/*ICAP Service not found */
{405, "Not allowed"},	/*Method not allowed for service (e.g., RESPMOD requested For service that supports only REQMOD). */
{408, "Request timeout"},	/*Request timeout. ICAP server gave up waiting for a Request from an ICAP client */
{500, "Server error"},	/*Server error. Error on the ICAP server, such as "out of disk

## 9. Threat Extraction

### 9.1 Out-of-the box

Currently we only support TX with our MTA or the SandBlast Agent Browser Plugin.

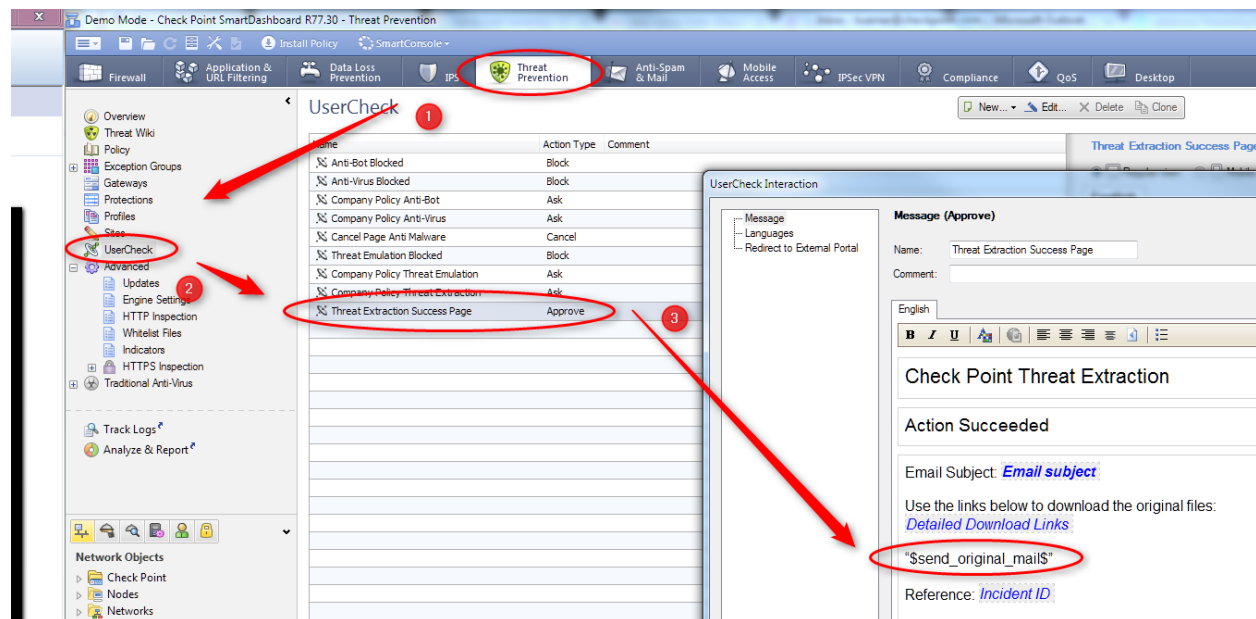
### 9.2 Parallel/Serial mode

If you want to use TX in “serial mode” after a file is processed by TE you need to set the following:

1. Edit `$FWDIR/conf/mail_security_config`
2. under "mta" section (look for "[mta]" within this file) add:  
`"te_adaptive_mode_disabled=1"`
3. install Threat Prevention policy

### 9.3 Add option to “send original email”

By default the user has only the option to download the original file via the UserCheck process. From JHF198 on you can add the option to send the original email again. To add this option the following UserCheck page has to be edited:



Simply add the string “\$send\_original\_mail\$”.

The sender of this email will be `admin@gatewayhostname.gatewaydomainname`.

## 9.4 Demo via Web Browser Plugin

Another way to demo Threat Extraction is to activate the TX Browser Plugin. The Plugin currently also supports uploading files to TE.

To use the TX browser plug-in with a local Sandblast appliance you need to follow this SK:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk108695](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108695)

You can also use the available SandBlast Partner Training Kit for demoing the web browser extension.

## 9.5 Demo with MTA environment

For demoing TEX with MTA we recommend using the available SandBlast Partner Training Kit.

## 10. TE/TX API

### 10.1 TE API documentation

API reference guide can be found here:

<https://community.checkpoint.com/community/threat-prevention/sandblast-api>

### 10.2 Enabling API ports

TE API port is enabled by default to listen on port 18194 when enabling the TE blade on an appliance.  
TX API port must be manually enabled one:

#### Enabling SCRUBD (responsible to provide Threat Extraction) to listen on port 18195

To enable SCRUBD API port search for “enable\_scrub\_web\_service” in GUIDBEDIT and set the value to “true”

The screenshot shows the 'Check Point Database Tool' interface. On the left, a tree view displays the database structure, including 'Administrators', 'Anti-Malware', 'Desktop', 'Device Management', 'Endpoint', and 'Global Properties'. The 'Anti-Malware' folder is expanded, showing various tables like 'anti\_malware\_exceptions', 'anti\_malware\_rulebase', and 'anti\_malware\_rulebase\_sec'. On the right, a table lists objects and their settings. Below this, a detailed view of the 'enable\_scrub\_web\_service' field is shown.

Object Name	Class Name	Last Modify Time
SBSettings_572842D5-AC68-6844-8...	scrub_blade_gateway_settings	Tue Aug 01 13:31:50 20...
SBSettings_Default	scrub_blade_gateway_settings	Tue Aug 01 13:24:52 20...
TE_General_Settings	te_general_settings	Thu Jul 27 07:24:43 201...
SB_General_Settings	sb_general_settings	Thu Jul 27 07:23:37 201...
TESettings_572842D5-AC68-6844-8...	threat_emulation_blade_gateway_settings	Thu Jul 27 07:23:37 201...
TESettings_Default	threat_emulation_blade_gateway_settings	Thu Jul 27 07:23:37 201...
ABSettings_Default	antimalware_blade_gateway_settings	Thu Jul 27 07:23:37 201...
General_Settings	antimalware_general_settings	Thu Jul 27 07:23:37 201...
TE_Updates	te_autoupdate	Thu Jul 27 07:23:37 201...
AntiMalwareUpdates	antimalware_autoupdate	Thu Jul 27 07:23:37 201...

Field Name	Type	Value	Valid Values	Default Value
color	string	black		black
comments	string			
compress_repository_files	boolean	true		true
connected_gw	string	{572842D5-AC68-6844-8837-5...		
cpfc_async_timeout_in_seconds	unumber	115	5~3600	115
delete_files_older_than	boolean	true		true
delete_files_older_than_days	unumber	30	1~59	14
enable_scrub_web_service	boolean	true		
inspection_stopped_track	reference	Log ('rulebase_tracks' table)		
obfuscate repository files	boolean	true		true

Also look for further entries with "enable\_scrub\_service"

When both API ports are enabled you should see them listening on 18194 and 18195:

```
[Expert@TE2000X:0]# netstat -nap | grep 18194
tcp        0      0 0.0.0.0:18194        0.0.0.0:*           LISTEN      17403/temain
[Expert@TE2000X:0]# netstat -nap | grep 18195
tcp        0      0 0.0.0.0:18195        0.0.0.0:*           LISTEN      13179/scrubd
[Expert@TE2000X:0]#
```

## 10.3 Enabling API logging

Logging for TX API is enabled by default – to also get logs for TE API run:

```
# tecli advanced remote emulator logs enable
```

TE API logs look like this:

The screenshot displays the Check Point SmartView Log interface. The main log table shows a series of events from 'Today' at 11:31:46 to 10:18:54, all originating from 'TE2000X' and destined to '172.16.2.190'. The event at 11:31:45 is highlighted, showing a '0.0.0.0 downloaded a malicious file' message. A red box highlights the message text in the log entry. Below the log table, a 'Log Details' window is open, providing a comprehensive view of the event. The 'Log Info' tab shows the event occurred at 'Today 11:31:45' on the 'TE2000X' blade, categorized as a 'Network' event with a 'Detect' action, 'Critical' severity, and 'High' confidence level. The 'Threat Emulation' section indicates a 'CPU-Level Detection Event: Unexpected Process Crash Malicious Filesystem Activity Malicious Registry Activity Malware signature matched ( Malicious Binary.crnqsm ) Suspicious activity observed ( Malicious by Office macro analyzer ) Unexpected Process Creation'. The 'Emulated File' section lists the file name as 'tex\_example\_calc.doc', file type as 'doc', file size as 39445 bytes, and provides MD5 and SHA1 hashes. The 'Traffic' section shows the protocol as '-1', source port as '-1', and service as 'IP/-1'. The 'More' section shows the file's SHA256 hash and origin as 'TE2000X'. The 'Protection Name' is 'Exploited doc document', and the 'Scope' is '0.0.0.0'. The 'Destination Port' is '-1'. The 'Malicious Activity De...' section lists the activity as 'Win7,Office 2013,Adobe 11: emulator, WinXP,Office 2003/7,Adobe 9: emulator.'.

## 11. Testing & Troubleshooting

### 11.1 I have a problem - where is the log ?

Problem	Logfile	Comment
Emulation fails	\$FWDIR/log/ted.elg	Ted.elg is the logfile of the threat emulation daemon
Mail is not delivered	/var/log/maillog	Maillog is the Postfix mail transport log; emaild.mta.log is the internal MTA log connected to TED
	\$FWDIR/log/emaild.mta.elg	
TE engine update fails	\$FWDIR/log/te_engine_log_file.elg	
	\$FWDIR/log/te_file_downloader.elg	
	\$FWDIR/log/ted.elg	
TE image update fails	\$FWDIR/log/te_file_downloader.elg	
	\$FWDIR/log/ted.elg	
TE image initialization fails	\$FWDIR/log/te_image_prep_util.elg	
Threat Extraction fails	\$FWDIR/log/scrubd.elg	Scrubd.elg is the general logfile of the Threat Extraction daemon; scrub_cp_file_convert.d.elg is the log for the file conversion process
	\$FWDIR/log/scrub_cp_file_convert.d.elg	
File aggregation from stream does not work	\$FWDIR/log/dlpu.elg	DLPU is the process responsible for aggregating files from the network stream

Note: All of these logs have also debug options to get more info inside the log

## 11.2 Test emulation

If you like to manually add a file to emulation you can do this via CLI:

```
# te_add_file -f=/tmp/test.pdf
```

This file will be shown in the logs as SMTP emulation

## 11.3 Image/Engine Update

### 10.3.1 Check image and detection rule versions

```
# tecli show download all
```

This will show you the revision number of the downloaded images:

```
[Expert@smesg:0]# tecli show download all

Images
=====

Summary
-----
4 images (out of 4) are ready

Win7,Office 2013,Adobe 11
-----
UID: 5e5de275-a103-4f67-b55b-47532918fa59
Revision: 19
      Status: Ready
      Size: 3.79GB
      Start Download Time: Fri Sep  4 19:24:18 2015

Win7,Office 2013,Adobe 9
```

And also the available detection rule revisions:

```
Detection Rules
=====

Win7,Office 2013,Adobe 11
-----
UID: 5e5de275-a103-4f67-b55b-47532918fa59
Revision: 42010
      Status: Ready
      Size: 56.7KB
      Start Download Time: Fri Sep  4 20:01:17 2015
Revision: 43006
      Status: Trying to download
      Size: 0.0B
      Start Download Time: Fri Sep 11 09:55:19 2015
```

Compare latest image versions to:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk92509](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk92509)

## 10.3.2 Check TE engine version

You can check the current TE engine version:

```
# tecli advanced engine version
```

```
[Expert@smesg:0]# tecli a e v
Threat emulation engine version is: 43.990000082
[Expert@smesg:0]#
```

Compare latest engine versions to:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk95235](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk95235)

## 10.3.3 Check ThreatCloud Update server connectivity

Check for general connection to Threat Cloud Update servers:

```
# ping te.checkpoint.com
```

```
[Expert@smesg:0]# ping te.checkpoint.com
PING te.g03.checkpoint.com (194.29.39.23) 56(84) bytes of data.
```

See if you get feedback from update servers:

```
# curl -vk https://te.checkpoint.com
```

```
[Expert@smesg:0]# curl -vk https://te.checkpoint.com
* About to connect() to te.checkpoint.com port 443 (#0)
*   Trying 194.29.39.23...
*   connected
* Connected to te.checkpoint.com (194.29.39.23) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using AES256-SHA
* Server certificate:
*   subject: C=US; ST=California; L=San Carlos; O=Check Point
ckpoint.com
*   start date: 201
*   expire date: 201
*   subjectAltName: te.checkpoint.com matched
*   issuer: C=U
*   SSL certificate verify result: unable to get local issu
> GET / HTTP/1.1
> User-Agent: curl/7.27.0
> Host: te.checkpoint.com
> Accept: */*
>
< HTTP/1.1 403 Forbidden
< Date: Wed, 23 Sep 2015 09:08:52 GMT
```



### 10.3.4 Remove all images and start again

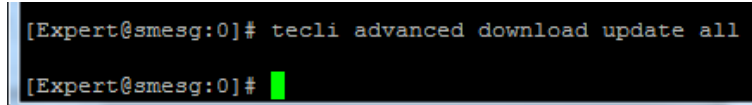
To delete all existing images and start again:

- delete old images  
# rm -rf /var/log/files\_repository/images
- Kill Threat Emulation daemon and rerun update  
# fw kill ted  
# tecli a d u a

## 10.3.5 Force update from CLI

You can force an update:

```
# tecli advanced download update all
```

A terminal window with a black background and white text. The prompt is [Expert@smesg:0]#. The command tecli advanced download update all has been entered. The prompt is now [Expert@smesg:0]# followed by a green cursor bar.

```
[Expert@smesg:0]# tecli advanced download update all  
[Expert@smesg:0]#
```

This command will not give you any feedback.

Feedback regarding the update process can be obtained via:

```
$FWDIR/log/ted.elg  
$FWDIR/log/te_file_downloader.elg  
$FWDIR/log/te_engine_log
```

If update still does not initialize kill TED:

```
# fw kill ted
```

## 10.4 Useful TECLI commands

A small collection of TECLI commands:

### License

Show license

```
# cpstat threat-emulation -f contract
```

### Updates

Force update of images and engine:

```
# tecli advanced downloads update all
```

### Check engine version

```
# tecli advanced engine version
```

### Check image versions

```
# tecli show download images
```

### Check image status

```
# tecli show download all
```

### Add local file for emulation testing

```
# te_add_file -f=putty.exe
```

### Clear cache

```
# tecli cache clean
```

### Show TE status

```
# tecli show statistics
```

### Show Emulation status by image/file type

```
# tecli s e v s
```

```
# tecli s e e
```

### Show Remote Emulation queue for TE cloud (on harvesting GW)

```
# tecli s r q
```

### Save all files passing through TE in /var/log/all\_files/ (watch disk space !)

```
# tecli advanced attributes set save_all_files 1
```

### Restrict number of running concurrent VMs

```
# tecli advanced attributes set max_vm no_of_vms
```

### Debugging (full debug)

```
# tecli debug set all all
```

logfiles in /var/log/opt/CPsuite-R77/fw1/log/

- o ted.elg

- o te\_file\_downloader.elg => download status new images/engine

## 10.5 Useful MTA/Postfix commands

Useful commands for troubleshooting our TE MTA:

### Postfix log

`/var/log/maillog`

### Show current queue

```
# /opt/postfix/usr/sbin/postqueue -c /opt/postfix/etc/postfix/ -p
```

### Show one mail from queue (5632E28B0044 is a sample Queue ID from show queue)

```
# /opt/postfix/usr/sbin/postcat -c /opt/postfix/etc/postfix/ -q 5632E28B0044 |  
more
```

### Attempt immediate delivery of queue content

```
# /opt/postfix/usr/sbin/postqueue -c /opt/postfix/etc/postfix/ -f
```

### Delete one message from queue (5632E28B0044 is a sample Queue ID from show queue)

```
# /opt/postfix/usr/sbin/postsuper -c /opt/postfix/etc/postfix/ -d 5632E28B0044
```

### Delete ALL messages from queue

```
# /opt/postfix/usr/sbin/postsuper -c /opt/postfix/etc/postfix/ -d ALL
```

### Show postfix configuration

```
# /opt/postfix/usr/sbin/postconf -c /opt/postfix/etc/postfix/
```

### Get postfix version

```
# /opt/postfix/usr/sbin/postconf -c /opt/postfix/etc/postfix/ | grep  
mail_version
```

### Pipe text (" ThisIsAnMaillogEntry") into maillog

```
# /opt/postfix/usr/sbin/postlog -c /opt/postfix/etc/postfix/  
ThisIsAnMaillogEntry
```

### Start/Stop postfix

```
# /opt/postfix/usr/sbin/postfix -c /opt/postfix/etc/postfix stop
```

-> this command does not seem to have any impact on the postfix process ID - don't know if it really restarts postfix

### Restart postfix

```
# /opt/postfix/usr/sbin/postfix -c /opt/postfix/etc/postfix reload
```

### Further information

"postqueue" command -> <http://www.postfix.org/postqueue.1.html>

Postfix Website -> <http://www.postfix.org/>

## 10.6 How-to send an email with attachment from CLI

How to send mail with attachment from Gaia OS?

E.g. to reinject a previously caught malicious file to TE MTA locally:

```
[Expert@gw]# cd /var/log/mal_files/

[Expert@gw]# ls
4bddeb07094936013a660ac7dc263261eea2e1dc.pdf
8ee725923c3a29c59ea16083e02cc3f1409dd49d.doc
ba7809dd229b8256ce36428e5ccf514de4ea8177.doc

[Expert@gw]# uuencode 4bddeb07094936013a660ac7dc263261eea2e1dc.pdf
4bddeb07094936013a660ac7dc263261eea2e1dc.pdf | $FWDIR/bin/sendmail -t localhost -s
"inspect file" -f "a@b.cz <mailto:a@b.cz>" "a@test.local <mailto:a@test.local>"
```

First mail address is sender, second one is recipient.

## 10.7 SNMP Monitoring

### 10.7.1 TE SNMP OIDs

Currently these values can be queried by SNMP but are not part of the official Check Point MIB:

Description	OID	Blade
Threat Emulation Status Fields	1.3.6.1.4.1.2620.1.49	
Threat Emulation Status Code	1.3.6.1.4.1.2620.1.49.101	TE
Threat Emulation Status Short Description	1.3.6.1.4.1.2620.1.49.102	TE
Threat Emulation Status Long Description	1.3.6.1.4.1.2620.1.49.103	TE
Threat Emulation Engine Major Version	1.3.6.1.4.1.2620.1.49.29	TE
Threat Emulation Engine Minor Version	1.3.6.1.4.1.2620.1.49.30	TE
Threat Emulation Mode	<b>1.3.6.1.4.1.2620.1.49.19.0</b>	TE
Threat Emulation Queue Information	1.3.6.1.4.1.2620.1.49.1	TE
Threat Emulation Download Information	1.3.6.1.4.1.2620.1.49.2	TE
Threat Emulation Average Download Percentage	1.3.6.1.4.1.2620.1.49	TE
Threat Emulation Download Percentage	1.3.6.1.4.1.2620.1.49.3	TE
Threat Emulation Update Status	<b>1.3.6.1.4.1.2620.1.49</b>	TE
Threat Emulation Status	1.3.6.1.4.1.2620.1.49.16	TE
Threat Emulation Status Description	1.3.6.1.4.1.2620.1.49.17	TE
Threat Emulation Queue Info	1.3.6.1.4.1.2620.1.49.1	TE
	1.3.6.1.4.1.2620.1.49.1.1.1.0	TE
Threat Emulation Download Info	1.3.6.1.4.1.2620.1.49.2	TE
	<b>1.3.6.1.4.1.2620.1.49.2.1.2.x.0</b>	
Threat Emulation Download Percentage	<b>1.3.6.1.4.1.2620.1.49.3</b>	TE
Threat Emulation Scanned Files (Quantity)	<b>1.3.6.1.4.1.2620.1.49.4</b>	TE
Threat Emulation Scanned Files Total Count	1.3.6.1.4.1.2620.1.49.4.1	TE
Threat Emulation Scanned Files Count Last Day	1.3.6.1.4.1.2620.1.49.4.2	TE
Threat Emulation Scanned Files Count Last Week	1.3.6.1.4.1.2620.1.49.4.3	TE
Threat Emulation Scanned Files Count Last Month	1.3.6.1.4.1.2620.1.49.4.4	TE
Threat Emulation Malware Detected (Quantity)	<b>1.3.6.1.4.1.2620.1.49.5</b>	TE
Threat Emulation Malware Detected Total Count	1.3.6.1.4.1.2620.1.49.5.1	TE
Threat Emulation Malware Detected Count Last Day	1.3.6.1.4.1.2620.1.49.5.2	TE
Threat Emulation Malware Detected Count Last Week	1.3.6.1.4.1.2620.1.49.5.3	TE
Threat Emulation Malware Detected Count Last Month	1.3.6.1.4.1.2620.1.49.5.4	TE
Threat Emulation Scanned Files On Threat Cloud (Quantity)	<b>1.3.6.1.4.1.2620.1.49.6</b>	TE
Threat Emulation Scanned Files On Threat Cloud Total Count	1.3.6.1.4.1.2620.1.49.6.1	TE

Threat Emulation Scanned Files On Threat Cloud Last Day	1.3.6.1.4.1.2620.1.49.6.2	TE
Threat Emulation Scanned Files On Threat Cloud Last Week	1.3.6.1.4.1.2620.1.49.6.3	TE
Threat Emulation Scanned Files On Threat Cloud Last Month	1.3.6.1.4.1.2620.1.49.6.4	TE
Threat Emulation Malware Detected On ThreatCloud (Quantity)	<b>1.3.6.1.4.1.2620.1.49.7</b>	TE
Threat Emulation Malware Detected On ThreatCloud Total Count	1.3.6.1.4.1.2620.1.49.7.1	TE
Threat Emulation Malware Detected On ThreatCloud Last Day	1.3.6.1.4.1.2620.1.49.7.2	TE
Threat Emulation Malware Detected On ThreatCloud Last Week	1.3.6.1.4.1.2620.1.49.7.3	TE
Threat Emulation Malware Detected On ThreatCloud Last Month	1.3.6.1.4.1.2620.1.49.7.4	TE
Threat Emulation Average Process Time (Quantity)	<b>1.3.6.1.4.1.2620.1.49.8</b>	TE
Threat Emulation Average Process Time Total Count	1.3.6.1.4.1.2620.1.49.8.1	TE
Threat Emulation Average Process Time Last Day	1.3.6.1.4.1.2620.1.49.8.2	TE
Threat Emulation Average Process Time Last Week	1.3.6.1.4.1.2620.1.49.8.3	TE
Threat Emulation Average Process Time Last Month	1.3.6.1.4.1.2620.1.49.8.4	TE
Threat Emulation Emulated File Size (File size - bytes)	<b>1.3.6.1.4.1.2620.1.49.9</b>	TE
Threat Emulation Emulated File Size Total	1.3.6.1.4.1.2620.1.49.9.1	TE
Threat Emulation Emulated File Size Last Day	1.3.6.1.4.1.2620.1.49.9.2	TE
Threat Emulation Emulated File Size Last Week	1.3.6.1.4.1.2620.1.49.9.3	TE
Threat Emulation Emulated File Size Last Month	1.3.6.1.4.1.2620.1.49.9.4	TE
Threat Emulation Queue Size (Quantity)	<b>1.3.6.1.4.1.2620.1.49.10</b>	TE
Threat Emulation Queue Size Total Count	1.3.6.1.4.1.2620.1.49.10.1	TE
Threat Emulation Queue Size Last Day	1.3.6.1.4.1.2620.1.49.10.2	TE
Threat Emulation Queue Size Last Week	1.3.6.1.4.1.2620.1.49.10.3	TE
Threat Emulation Queue Size Last Month	1.3.6.1.4.1.2620.1.49.10.4	TE
Threat Emulation Peak Size (Quantity)	<b>1.3.6.1.4.1.2620.1.49.11</b>	TE
Threat Emulation Peak Size Total Count	1.3.6.1.4.1.2620.1.49.11.1	TE
Threat Emulation Peak Size Last Day	1.3.6.1.4.1.2620.1.49.11.2	TE
Threat Emulation Peak Size Last Week	1.3.6.1.4.1.2620.1.49.11.3	TE
Threat Emulation Peak Size Last Month	1.3.6.1.4.1.2620.1.49.11.4	TE
Threat Emulation General Status Fields		
Threat Emulation Email Scanned	1.3.6.1.4.1.2620.1.49.12	TE
Threat Emulation Downloaded Files Scanned	1.3.6.1.4.1.2620.1.49.13	TE
Threat Emulation Files In Queue	<b>1.3.6.1.4.1.2620.1.49.14</b>	<b>TE</b>
Threat Emulation Number Of Emulation Environments	1.3.6.1.4.1.2620.1.49.15	TE

		TE
<b>Threat Emulation Contract Status Fields</b>		
<b>Contract Name</b>	1.3.6.1.4.1.2620.1.49.19	TE
<b>Cloud Subscription Expire Date</b>	1.3.6.1.4.1.2620.1.49.20	TE
<b>TE Cloud Hourly Quota</b>	1.3.6.1.4.1.2620.1.49.21	TE
<b>TE Cloud Monthly Quota</b>	1.3.6.1.4.1.2620.1.49.22	TE
<b>TE Cloud Remaining Quota</b>	1.3.6.1.4.1.2620.1.49.23	TE
<b>TE Maximal VMs Number</b>	1.3.6.1.4.1.2620.1.49.24	TE
<b>TE Subscription Status</b>	1.3.6.1.4.1.2620.1.49.25	TE
<b>TE Cloud Quota Status</b>	1.3.6.1.4.1.2620.1.49.26	TE
<b>TE Subscription Description</b>	1.3.6.1.4.1.2620.1.49.27	TE
<b>TE Cloud Quota Description</b>	1.3.6.1.4.1.2620.1.49.28	TE
<b>TE Cloud Quota Identifier</b>	1.3.6.1.4.1.2620.1.49.31	TE
<b>TE Cloud Monthly Quota Period Start</b>	1.3.6.1.4.1.2620.1.49.32	TE
<b>TE Cloud Monthly Quota Period End</b>	1.3.6.1.4.1.2620.1.49.33	TE
<b>TE Cloud Monthly Quota Usage for This GW</b>	1.3.6.1.4.1.2620.1.49.34	TE
<b>TE Cloud Hourly Quota Usage for this GW</b>	1.3.6.1.4.1.2620.1.49.35	TE
<b>Threat Emulation Is First Download</b>	1.3.6.1.4.1.2620.1.49.36	TE
<b>TE Cloud Monthly Quota Usage for Quota ID</b>	1.3.6.1.4.1.2620.1.49.37	TE
<b>TE Cloud Hourly Quota Usage for Quota ID</b>	1.3.6.1.4.1.2620.1.49.38	TE
<b>TE Cloud Monthly Quota Exceeded</b>	1.3.6.1.4.1.2620.1.49.39	TE
<b>TE Cloud Hourly Quota Exceeded</b>	1.3.6.1.4.1.2620.1.49.40	TE
<b>TE Cloud Last Quota Update GMT Time</b>	1.3.6.1.4.1.2620.1.49.41	TE



## 10.7.2 Extend SNMP Monitoring

### 10.7.2.1 Enable SNMP

1. # cpconfig
  - a. enable "SNMP Extension"
2. Clish
  - set snmp community <community-name> read-only
  - save config

#### Check OIDs for TE

TE OIDs => .1.3.6.1.4.1.2620.1.49

#### Show all TE related OIDs

# snmpwalk -v 2c -c <community-name> localhost .1.3.6.1.4.1.2620.1.49

#### Enable SNMP Agent

1. Clish
  - set snmp agent on
  - save config

### 10.7.2.2 Extend available SNMP OIDs

#### Select free OID for Postfix queue value

Free OID => .1.3.6.1.4.1.2620.1.250.1

#### Extend available SNMP values

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk78360](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk78360)

Add the following lines to /etc/snmp/userDefinedSettings.conf file:

```
extend .1.3.6.1.4.1.2620.1.250.1 postfix_queue /bin/sh
/home/admin/mailqueue.sh
extend .1.3.6.1.4.1.2620.1.250.2 emaild_queue /bin/sh
/home/admin/emaild_tmpdir.sh
extend .1.3.6.1.4.1.2620.1.252 vm /bin/sh /home/admin/running_vm.sh
```

### 10.7.2.3 Postfix mailqueue monitoring script

**/home/admin/mailqueue.sh**

```
# Extract Postfix queue size value
#!/bin/bash

MAILQ=$(/opt/postfix/usr/sbin/postqueue -c /opt/postfix/etc/postfix/ -p |
egrep '^--.*Request|^Mail.*empty')

if [[ $MAILQ =~ "empty" ]] ; then
    RESPONSE=0
    echo $RESPONSE
elif [[ $MAILQ =~ "Request" ]] ; then
    RESPONSE=$(echo $MAILQ|awk '{print $5}')
    echo $RESPONSE
else
    RESPONSE=error
fi
```

### 10.7.2.4 Emaild queue monitoring script

**/home/admin/emaild\_tmpdir.sh**

```
# Extract emaild temp file queue amount
#!/bin/bash
. /opt/CPshared/5.0/tmp/.CPprofile.sh
ls -l $FWDIR/tmp/email_tmp/ |grep emailtemp |wc -l
```

### 10.7.2.5 Running VM instances monitoring script

**/home/admin/running\_vm.sh**

```
# Extract amount of running VM Instances
#!/bin/bash
. /opt/CPshared/5.0/tmp/.CPprofile.sh
tecli s e e | grep "Running virtual machines"|awk '{print $4}'
```

## 10.7.2.6 Test extended SNMP values

### Test new values

MAILQUEUE

```
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2620.1.250.4.1.2.2.109.113.1
```

EMAILD\_TEMPDIR

```
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2620.1.251.4.1.2.3.101.109.102.1
```

## 10.8 How-to handle False-positives/False-negatives during a PoC

### 10.8.1 False-negatives

#### Check Point internal only

Try to get a sample from the customer e.g. from a competitor within this PoC and send it to [toc@checkpoint.com](mailto:toc@checkpoint.com). Before compress the file with ZIP and set a password "infected". TOC will create a ticket and will investigate the sample.

#### Partners

Open a support ticket at TAC

### 10.8.2 False-positives

#### Check Point internal only

Get the possible false-positive sample from the customer and send it to [toc@checkpoint.com](mailto:toc@checkpoint.com). Before compress the file with ZIP and set a password "infected". TOC will create a ticket and will investigate the sample.

#### Partners

Open a support ticket at TAC

- ▶ If it is a false-positive do not forget to remove the file from the appliance/gateway local cache. Otherwise it will stay in the cache with verdict "malicious" still creating further false-positives even if toc removed the cause.

You can remove a specific hash / extension via the command line with tecli:

```
[Expert@smesg:0]# tecli cache remove
Command: root->cache->remove

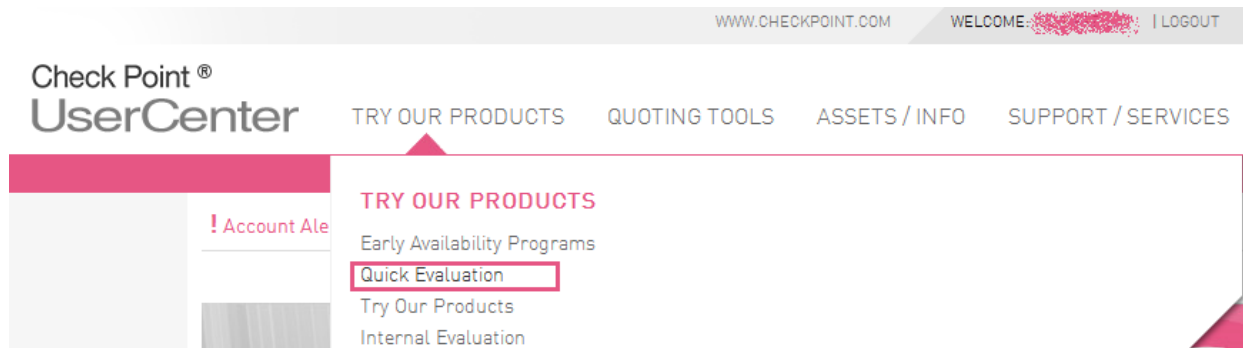
Available options:
  sha1           - remove records based on a specific hash
  filename       - remove records based on a specific file path
  extension      - remove records of a specific file extension from Local Cache
  benign         - remove specific benign records from Local Cache
  malicious      - remove specific malicious records from Local Cache
```

- ▶ Do not clear the whole cache as this will have a negative impact on performance !

## 10.9 How-to issue a license via User Center

### 10.9.1 Cloud emulation

Log-in your [User Center](#) account (create one for free if you don't have it)



#### Add Evaluation Product(s)

\* Select Evaluation Product:  [X] [v]

\* Select Account:  [v]

\* - Required Fields Ev

1 Selected Accounts

Products Blades Services Accessories Evaluations Support

**Summary** ▲

✕ Export ↓ Evaluate Blades ↓ Quick Evaluation

Issue Date	Total	Not Licensed Yet	Valid	Expired
<a href="#">Last 1-6 Months</a>	<a href="#">17</a>	<a href="#">5</a>	<a href="#">8</a>	<a href="#">4</a>
<a href="#">Last 7-12 Months</a>	<a href="#">67</a>	<a href="#">52</a>	<a href="#">0</a>	<a href="#">15</a>
<a href="#">Previous Periods</a>	<a href="#">13</a>	<a href="#">8</a>	<a href="#">2</a>	<a href="#">3</a>
<b>Total</b>	<b><a href="#">97</a></b>	<b><a href="#">65</a></b>	<b><a href="#">10</a></b>	<b><a href="#">22</a></b>

**Details** ▲

2 🔍 License ↔ Move ✎ Edit Info ✕ Export 📖 License Instructions 📄 Get Contracts

Filter:  2 Evaluations Last 1-6 Months ✕

<input type="checkbox"/>	Product Evaluation Name	SKU	Account ID	Key	IP	Issue Date
Issue Date: 13-May-2015						
1 <input checked="" type="checkbox"/>	<a href="#">Next Generation Threat Extraction Package Eval</a>	CPSB-NGTX-EVAL	6899238	0374CD		13-May-2015

Generate the EVAL license with IP of GW that will send files to Cloud emulation

## My Products

### License - Step 1 of 1

[View Licensing In](#)

Product Name	CPSB-NGTX-EVAL
Certificate Key	0374CD6-28283
Description	Next Generation Threat Extraction Package Eval

\* I would like this product to operate ☒ Using the Software Blade Architecture (R70 and above)  
☐ Using the NGX Architecture (R65 and below)

### License Information

Type of License (Central/Local):	Central	?
* Enter IP Address	1.1.1.1	?
* Hardware Brand Name	Check Point	
Other	-----Not relevant-----	
* Operating System	Gaia	
Tags		
Free Text		

License

“Get License File” to get the license and attach it to GW (thru CLI or SmartUpdate) or use “Show License Info” to copy/paste license instructions into SmartUpdate

### License

An email with the License(s) information and instruction on how to import the license(s) directly into your products was sent to igorf@checkpoint.com

✔ Licenses were generated successfully

<input checked="" type="checkbox"/>	Product/Feature	Description	Certificate Key	Version	Comments
<input checked="" type="checkbox"/>	CPSB-NGTX-EVAL	Next Generation Threat Extraction Package Eval	0374CD6-28283	Software Blades	

Get License File

Show License Info

Back To Products

## 10.9.2 Local emulation

For local TE emulation license can be automatically created via User Center Quick Evaluation option.

Follow the same procedure as above to generate CPSG-TE-VM56-EVAL (for TE2000), CPSG-TE-VM28-EVAL (for TE1000), CPSG-TE-VM8-EVAL (for TE250) license

Add Evaluation Product(s)	
* Select Evaluation Product	Select or search a product...
* Select Account:	Endpoint Package, 25 seats (Legacy) - CPEP-TS-EVAL
* Purpose for Evaluation:	<b>Threat Emulation</b> NGTX package including Threat Emulation cloud and Threat Extraction - CPSB-NGTX-EVAL TE2000 - Threat Emulation appliance with 56VMs - CPSG-TE-VM56-EVAL TE1000 - Threat Emulation appliance with 28VMs - CPSG-TE-VM28-EVAL TE250 - Threat Emulation appliance with 8VMs - CPSG-TE-VM8-EVAL
* - Required Fields	

CPSG-TE-EVAL is to be generated for local TE emulation GW when:

- either the TE appliance is traffic collector itself and does local emulation
- or TE appliance is traffic collector itself in hybrid mode (some files will be send to cloud and the rest will be emulated locally)
  - ⚠ additional NGTX license must be added to TE appliance
- or TE appliance and additional Check Point gateway exist in hybrid mode (TE appliance will do the local emulation and additional gateway will send part of configured files to cloud emulation)
  - ⚠ additional NGTX license must be added to Check Point gateway

## 10.10 Miscellaneous

### 10.10.1 Getting data behind empty TE forensic reports

- On SVT/SmartLog entry, click on view report:

**Threat Emulation: Detect**

localhost downloaded a malicious file.

Log Info	
Time	Sep 24, 2015 at 17:31:57
Number	550021
Type	Log
Origin	gw-304766

Threat Emulation	
Malware Activity	Malicious Filesystem Activity Malicious Regi... >>
Vulnerable Operating Systems	Summary Report Win7, Office 2003/7, Adobe 9, Flash 10, Java 6
Analyzed On	gw-304766
Severity	Critical
Confidence Level	High

Traffic	
Source	localhost (127.0.0.1)
Proxied Source IP	---
Destination	localhost (127.0.0.1)
Protocol	TCP tcp
Interface	---
Service	30580

Policy	
Action	Detect
Rule Name	<a href="#">Go to Policy</a>

Emulated File	
File Name	88307e5b70e8dfe6c5557779e4ac7065fae3a6b8.swf
File Type	swf
File Size	42.7 KB
File MD5	cbe7e8513776ad7117528e5b0541fe9c
File SHA-1	88307e5b70e8dfe6c5557779e4ac7065fae3a6b8

**127.0.0.1 downloaded a malicious file**

Log Info	
Time	Today 18:17:54
Blade	Threat Emulation
Product Family	Network
Action	Detect
Source	localhost (127.0.0.1)
Severity	Critical
Confidence Level	High

Threat Emulation	
Malware Action	Malicious Filesystem Activity Malicious Registry Activity
Forensics Report	<a href="#">View Report</a>
Vulnerable Operatin...	Win7, Office 2003/7, Adobe 9, Flash 10, J...
Analyzed On	gw-304766
Protection Type	SMTP Emulation

Emulated File	
File name	88307e5b70e8dfe6c5557779e4ac7065fae3a6b8.swf
File Type	swf
File Size (Bytes)	43697
File MD5	cbe7e8513776ad7117528e5b0541fe9c
File SHA1	88307e5b70e8dfe6c5557779e4ac7065fae3a6b8

Traffic	
Destination	localhost (127.0.0.1)
Protocol	TCP (6)
Source Port	-1
Service	TCP/30580

More	
Origin	gw-304766
Protection Name	Exploited swf document
Scope	255.255.255.255
Destination Port	30580
Service Name	TCP/30580
Malicious Activity De...	Win7, Office 2003/7, Adobe 9: emulator.



- On the browser opened, go to the address bar. Remove the filename (ThreatEmulationReport.html) to go to the containing directory and press enter.



- Then go to "data" directory, and click on "ThreatEmulation\_dataXML" file.

Name	Size	Date Modified
[parent directory]		
images/		8/14/13, 6:47:12 PM
AntiBot_dataXML.js	35.9 kB	8/14/13, 6:47:11 PM
AntiBot_layoutXML.js	14.9 kB	8/14/13, 6:47:11 PM
LinuxXML.js	22 B	8/14/13, 6:47:12 PM
LinuxXMLData.js	17 B	8/14/13, 6:47:12 PM
MultiUser_dataXML.js	6.1 kB	8/14/13, 6:47:11 PM
MultiUser_layoutXML.js	1.2 kB	8/14/13, 6:47:11 PM
SingleUser_dataXML.js	9.3 kB	8/14/13, 6:47:11 PM
SingleUser_layoutXML.js	1.2 kB	8/14/13, 6:47:11 PM
ThreatEmulation_Benign LayoutXML.js	6.2 kB	8/14/13, 6:47:12 PM
ThreatEmulation_dataXML	6.4 kB	9/24/15, 6:17:55 PM
ThreatEmulation_dataXML.js	6.6 kB	9/24/15, 6:17:55 PM
ThreatEmulation_LayoutXML.js	9.3 kB	8/14/13, 6:47:12 PM
ThreatEmulation_Summary_LayoutXML.js	2.3 kB	8/14/13, 6:47:12 PM
ThreatEmulation_XSLT.js	18.2 kB	8/14/13, 6:47:12 PM
ThreatEmulation_XSLT.xsl	18.0 kB	8/14/13, 6:47:12 PM

- That's the xml behind the report. The events are shown in the "Activities" section:





## 10.10.2 Set TED.ELG logsize and logrotate

By default TED.ELG will only grow to 10 MB and rotate ten times.  
This could be too few logs to troubleshoot or catch an event.

The settings can be changed via

```
tecli advanced attributes set max_size_per_log_file  
tecli advanced attributes set number_of_log_files
```

```
[Expert@smesg:0]# tecli adv att set  
Command: root->advanced->attributes->set  
  
Available options:  
static_cloud - Enable or disable static analysis on cloud server  
trusted_source - Enable or disable trusted source domains  
reclassifier - Enable or disable files reclassification  
file_type_logs - Enable or disable monitoring logs per file type  
archive_timeout - Set archive tool timeout in seconds  
archive_max_size - Set archive tool maximum inflate size in MB  
prohibited_file_types - configure file types that are prohibited in archives  
wait_queue_max_size - Set Cloud Error Handling maximum wait queue size  
wait_queue_timeout - Set timeout (in minutes) for retrying to send a file to the cloud after error  
save_all_files - Enable or disable saving all the files processed by ted  
verdicts_collector - Enable/Disable verdicts collector  
cloud_dns_name - Override cloud_dns_name attribute. Enter "-" to restore to default.  
emulation_upload_chunk_size - configure emulation upload chunk size  
emulation_enable_upload_split - configure emulation enable upload split  
whitening_mode - Enable or disable whitening mode  
max_size_per_log_file - Set max size per log file (effective after ted restart)  
number_of_log_files - Set number of log files (effective after ted restart)  
http_isolate_until_dns_isolated - Set http isolates until dns isolated  
false_positive_guard_file_types - Set false positive guard file types  
domains_threshold_enabled - Set domains threshold enabled  
domains_threshold_time_frame_in_minutes - (effective after ted restart)  
domains_threshold_max_consuming_files_in_frame - (effective after ted restart)  
api_log_path - Set path to api logs  
db_purge_interval - Set interval in minutes for purging the database  
db_purge_max_records - Set max records per database purge  
calc_sha256 - Enable or disable calculation of SHA256 for files  
disable_monitoring - Enable or disable VM documents monitoring - effective only with prior running "tecli advanced instrumentation off; tecli advanced download re  
monitored_events_limit - monitored events limit  
memory_dump - Enable or disable memory dump (effective after ted restart)  
pcap_enable - Enable or disable save pcap (will save only when report is created)  
pcap_number_of_packets - pcap number of packets  
huntress_mode - Enable or disable huntress mode
```

tecli advanced attributes show will print the current settings:

```
[Expert@smesg:0]# tecli adv att sh
Static Analysis on cloud server: ON
Re-classifier is: ON
Trusted source status is: ENABLED
Monitoring logs per file type: ON
Prohibited file types in archive files: Current file types list is empty.
Archive tool timeout in seconds: 30
Archive tool maximum inflate size in MB: 500
Cloud Error Handling maximum wait queue size: 5000
Cloud Error Handling wait queue timeout (minutes): 360
Saving all files: OFF
VerdictsCollector: OFF
Cloud dns name is : te.checkpoint.com
Emulation upload chunk size: 10485760
Emulation enable upload split : 1
Emulation mode is: OFF
Max size per log file (in bytes): 10485760
Number of log files : 10
Keep remote when dns rollover : 0
False positive guard file types : executables
Domains threshold enabled: 1
Domains threshold max consuming files in frame : 10
Domains threshold time frame in minutes : 60
Keep API Log Path :
DB purge interval: 10 minutes
DB max records per purge: 30000
Calculate SHA256: OFF
Disable Monitoring: OFF
Number of Events Limit 2000
Memory Dump: OFF
Pcap enable: OFF
Pcap number of packets: 1000
Huntress Mode: OFF
```

## 10.10.3 Blocking filetypes inside archives

To block certain filetypes inside archives (which is currently not possible with AV filetype blocking) use the following TECLI command:

### Enabling prohibited file types in archives

On the gateway, run the command:

```
tecli advanced attribute set prohibited_file_types <file_type1>,<file_type2>
```

For example to block every archive that contains an exe file run:

```
tecli advanced attribute set prohibited_file_types exe
```

### Disabling prohibited file types in archives

To reset the list of prohibited file types and disable the feature, run:

```
tecli advanced attribute set prohibited_file_types -
```

### Prohibited file types in archives status

To see the list of file types currently configured as prohibited run:

```
tecli advanced attribute show prohibited_file_types
```

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk101057](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101057)

## 11. Important SKs and hotfixes

This table is based on R77.30 without an jumbo hotfix applied. If you already installed a jumbo check if the needed fixes are included.

Scenario	Description	Relevant SK	Comment
<b>Sandblast Appliance TE100X, TE250X, TE1000X, TE2000X</b>	Sandblast Appliances and install images	<a href="#">SK106210</a>	Includes download link for X-Appliance install image
	CPU Level Hotfix	<a href="#">SK107333</a>	Only needed if CPU Level hotfix is not included in current ISO (ISOs before October 2015); can be checked with <i># tecli advanced attributes show   grep CPU</i>
	Multiple Private Cloud Support	<a href="#">SK102309</a>	
<b>TE General</b>	Supported file-types for emulation	<a href="#">SK106123</a>	
<b>TE on-premise</b>	TE Engine Update – What's new	<a href="#">SK95235</a>	Feature list of new TE engine releases
	TE Offline Update	<a href="#">SK92509</a>	How-to do offline image and engine updates; with download links in SK
	Create forensic report for benign	<a href="#">SK105737</a>	
	Blocking archive files according to contained file types	<a href="#">SK101057</a>	If you want to block file extensions in archive (currently not supported with AV) use this feature in TE
<b>TE cloud</b>	Cloud geo-restriction	<a href="#">SK97877</a>	
<b>MTA General</b>	Issues with non-ASCII characters in email subject	<a href="#">SK105164</a>	Hotfix available
	E-Mails are delayed for several hours in MTA	<a href="#">SK108878</a>	
<b>MTA on a CP cluster</b>	Unable to configure VIP for MTA	<a href="#">SK107093</a>	No fix currently available; restrict access to not used MTA interfaces by deactivating implied rule for port 25 and use firewall rules (see SandBlast PoC guide)
	Double inspection when running MTA on a cluster	<a href="#">SK109198</a>	Hotfix needs to be installed on the Management Server; contact Support to get fix
<b>SmartEvent</b>	TE events missing	<a href="#">SK108492</a>	Fix available in SK
	TE event action differs between SmartEvent and SmartLog	<a href="#">SK106392</a>	

SK only

SK and hotfix/download