

Preventing known and unknown attacks based on email as attack vector

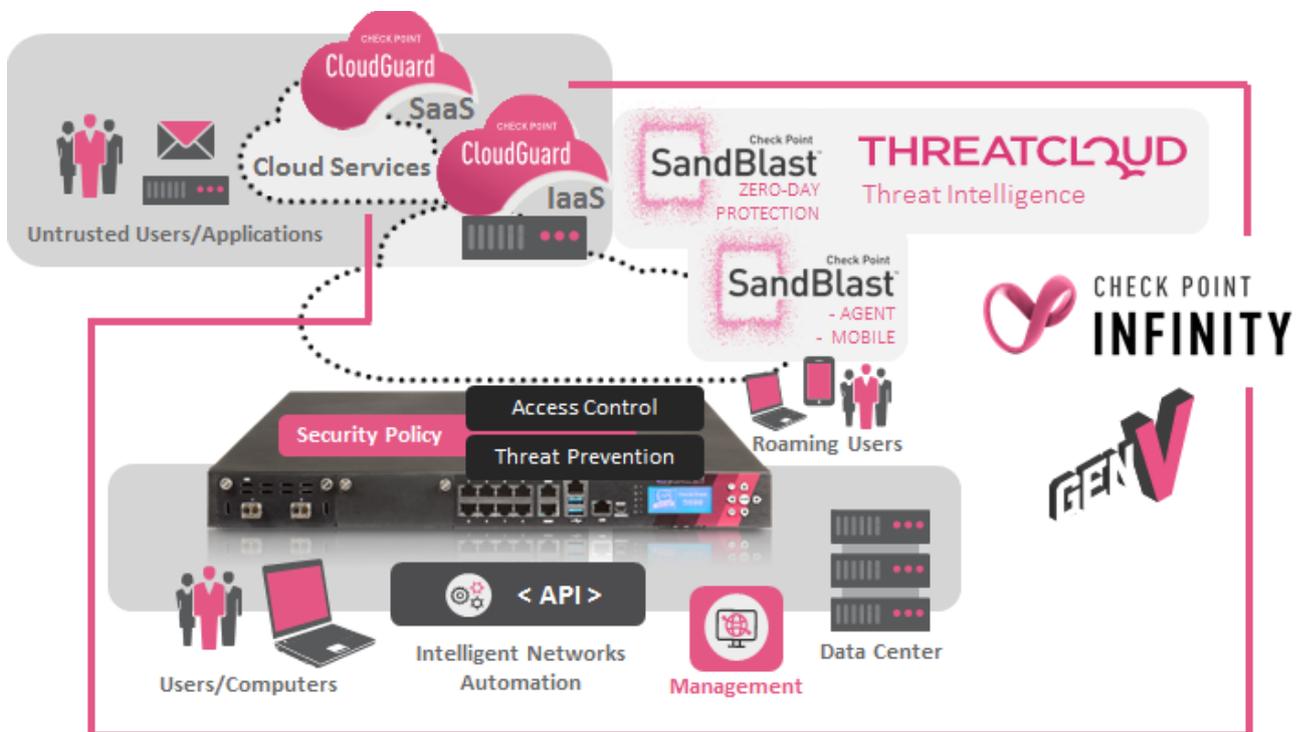


About this white paper

This document outlines some key elements for the defense against known and unknown [GenV attacks](#) available in the release R80.30. This version is focused on email as an attack vector. A separate document will cover web traffic as an attack vector.

The [Infinity](#) architecture allows customers to protect data center and cloud hosted applications as well as roaming users. Security policies can be harmonized and controlled by a central management infrastructure. Cloud services, Cloud hosted applications, data center applications, endpoints and mobile devices all benefit from the Threat Intelligence provided by [Check Point Research](#).

The Infinity architecture is open for integration to 3rd parties and automation processes supported by API's available on the management and gateway components.



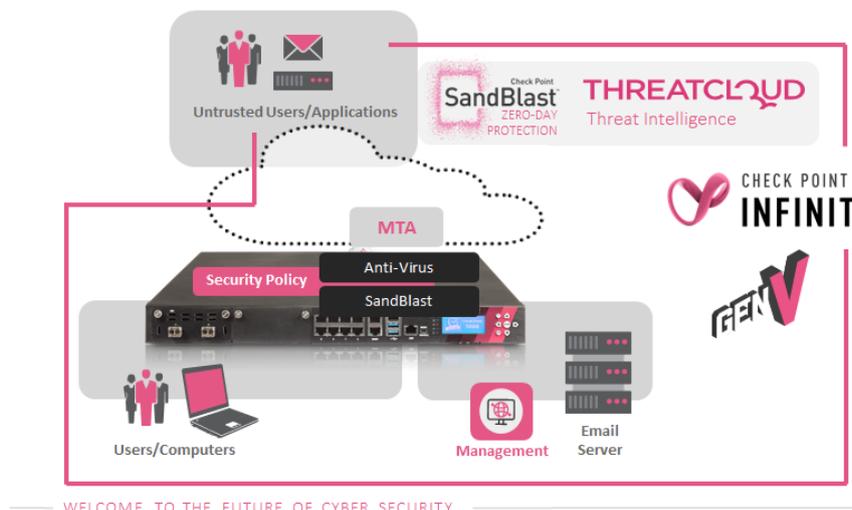
WELCOME TO THE FUTURE OF CYBER SECURITY

Table of content

Preventing known attacks.....	3
Access Control Policy	4
Gateway object configuration	4
MTA configuration	5
Details of the Threat Prevention profile applied to the traffic.....	7
Understanding protections and their confidence level	8
Mail protections defined in the profile.....	9
Anti-Virus settings of the Threat Prevention Profile	10
Decide which file types to be blocked by Anti-Virus	11
Working with Threat Indicators imported from 3 rd party static or dynamic sources.....	11
Configure the Anti-Virus Blade to work in hold mode.....	12
Preventing unknown attacks	13
Gateway settings for Threat Emulation.....	14
Define the emulation environment(s) and advanced settings	15
Removing potential malicious content from files.....	16
Configuring the threat prevention profile for Threat Extraction.....	17
Monitoring the MTA functionality	19
Monitoring the MTA using CPVIEW	20
SmartView – MTA Live Monitoring.....	21
SmartView – MTA Overview	22
SmartView – MTA Troubleshooting.....	23
Exporting logs to 3 rd party SIEM solutions.....	23
Configuring the Anti-SPAM Blade.....	24
Recommended SecureKnowledge articles for further studies	25

Preventing known attacks

The diagram below shows the lab environment this document is based on.



The threat prevention security policy in the lab is based on a source and destination schema which matches the traffic flow. The 'Key Resources' Threat Prevention profile is protecting the web and email server.

Name	Source	Destination	Protection/Site/File/Blade	Action	Track
MTA traffic to Gateway R8030gw	* Any	* Any	- N/A	MTA Security	Log Packet Capture Forensics
Protect important resources	* Any	web_server	- N/A	Key Resources	Log Packet Capture Forensics

Rule #1 was created automatically by the system when the MTA functionality was enabled on the gateway and originally had the 'Optimized' profile assigned. The profile 'MTA Security' has been built cloning the 'Key Resources' profile.

Design guideline: The IPS Blade protections are applied to traffic handled by the passive streaming engine. The passive streaming engine is not able to intercept encrypted such as SMTPs, but it provides protections such as Anti-Phishing to block known Phishing attacks. See the white paper [published at CheckMates](#) about the Context Aware packet processing architecture.

The MTA functionality enabled on the gateway allows the receipt of emails transported over SMTP/SMTPs (SMTP protected by TLS). With the MTA function enabled the Anti-Virus Software Blade allows blocking of known attacks. Customers may decide to activate the Anti-SPAM Software Blade using the configuration guidelines outlined in this document.

Design guideline: Enterprise customers often continue using an Anti-SPAM solution well-tuned over years to meet the requirements of the enterprise. Customers selecting SandBlast as a solution against Zero-Day Attacks intending to continue using their established Anti-SPAM solution must place the Check Point gateway as next hop MTA behind the Anti-SPAM gateway.

Subsequent to actions performed by the Anti-Virus Blade looking for known attacks, the SandBlast Blades perform extraction of potential malicious content and forward attachments to an emulation environment. In this example the emulation is performed by the SandBlast Cloud service but it could as well be executed by a dedicated appliance hosted in the data center.

Access Control Policy

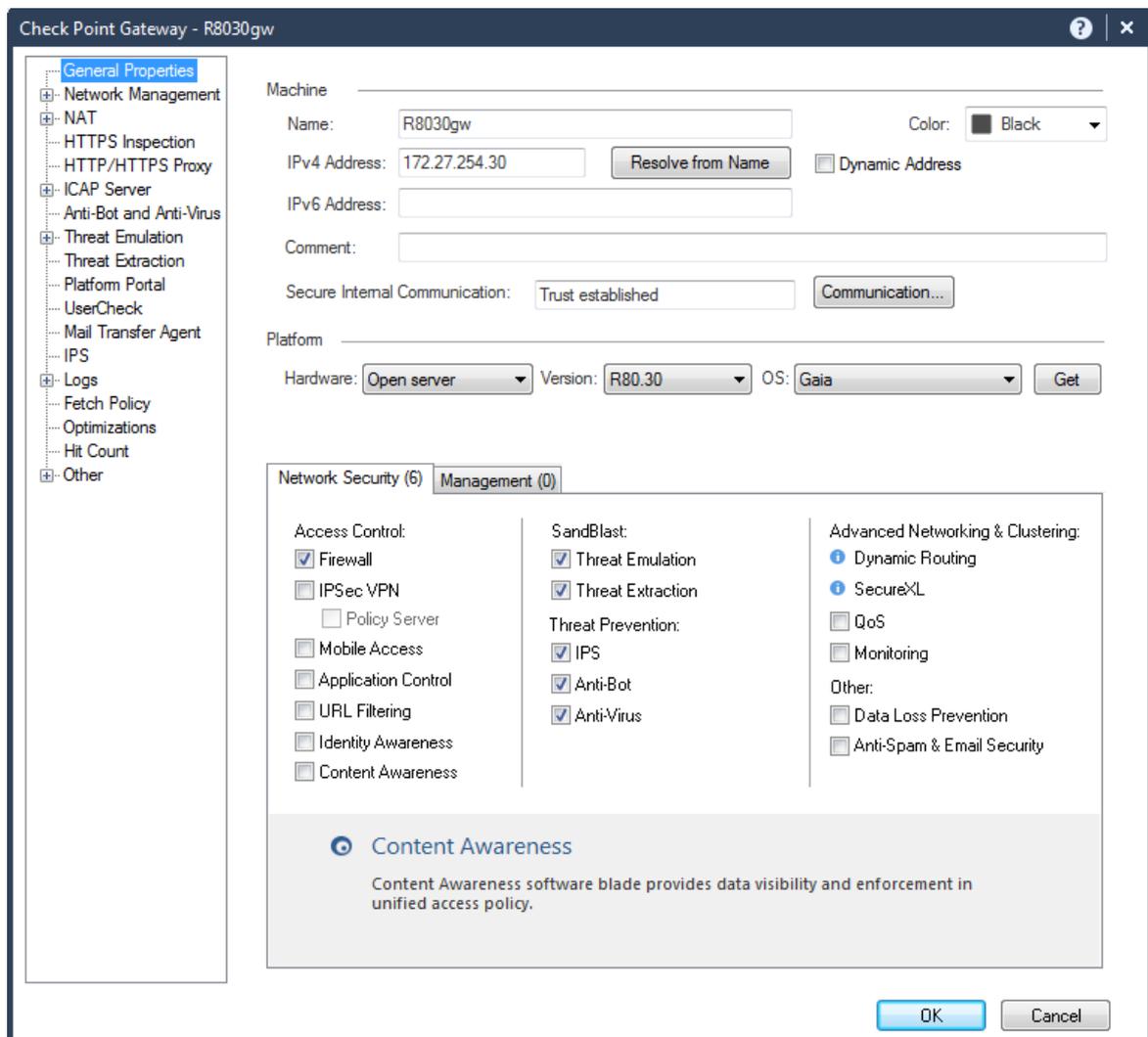
The incoming traffic is first checked against the Access Control Policy before Threat Prevention is performed. Below the extract of the lab policy allowing traffic directed to the MTA in rule #3.

No.	Hits	Name	Source	Destination	Services & Applications	Action	Track
▶ Management (1)							
▶ Network Services (2)							
▼ Published Services (3-5)							
3	14	MTA access	AdminPC	R8030gw	smtp	Accept	Log
4	208	Access to web server	User_Network net_172.27.254.0	web_server	http https ssh	Accept	Log
5	9	Remote Desktop	User_Network	adserver	Remote_Desktop_Protocol	Accept	Log
▶ Access to Internet (6)							
▶ Clean up (7-8)							

Gateway object configuration

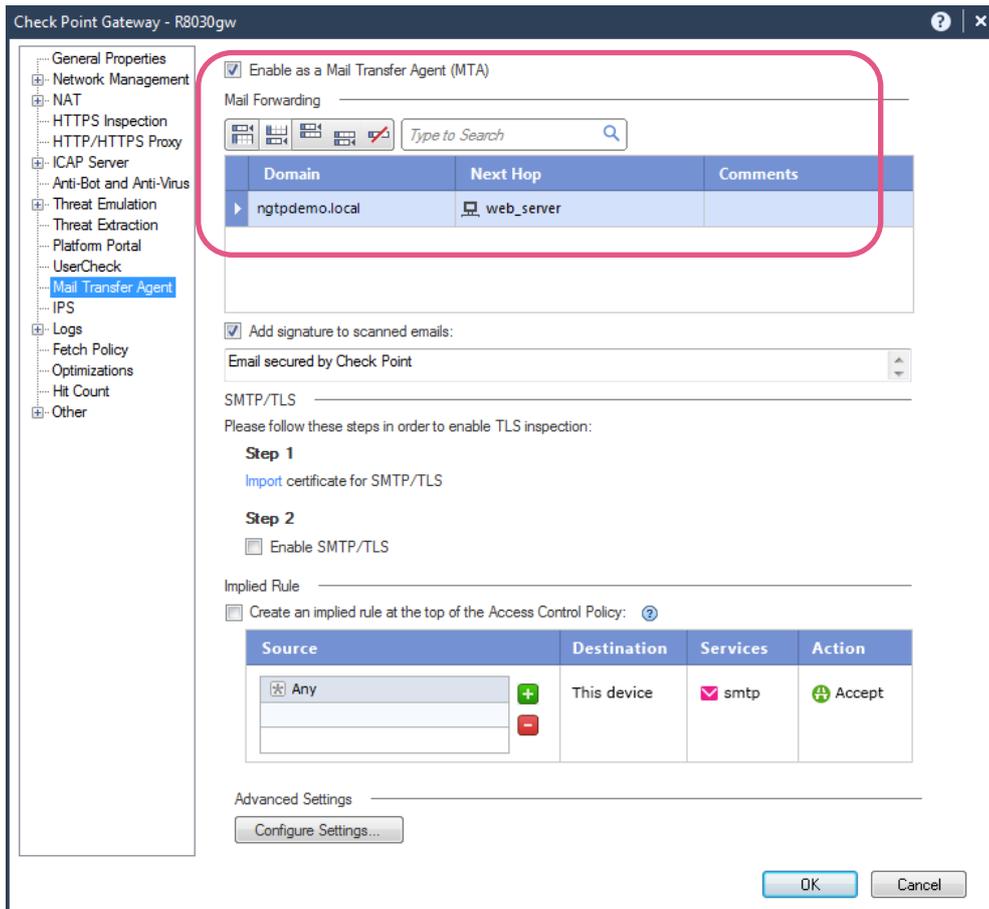
The security gateway is configured to apply Zero-Day Protection using the SandBlast functions and following the protection against known attacks performed by IPS and Anti-Virus Blade. The Anti-Bot functionality is outside the scope of this paper but it plays a key role identifying known attacks intending to spread to other network segments.

Design guideline: When enabling the MTA functionality a threat prevention policy rule will automatically be created applying the 'Optimized' profile on the traffic directed towards the MTA.



MTA configuration

In this lab the MTA is enabled for SMTP traffic only and to forward the traffic to the internal web and email server 'web_server'. It was decided to create a dedicated access control rule (see above) in favor of using an automatically created implied rule.



Design Guideline: In case of a need to change the default SMTP port the MTA is working on, administrators can follow the instructions provided in [sk142932](#) to change the relevant ports.

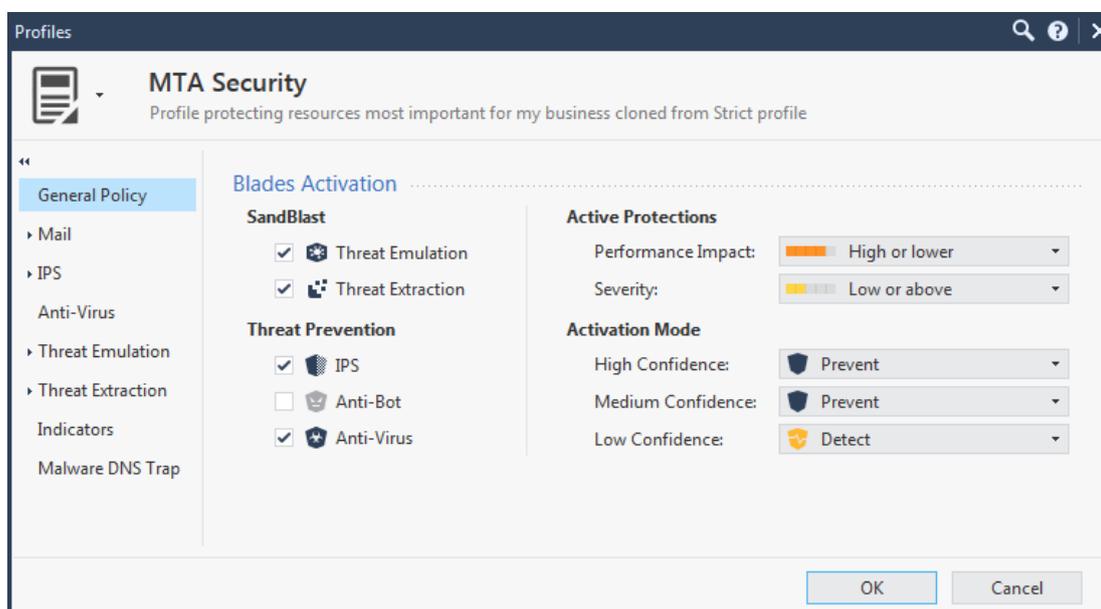
Details of the Threat Prevention profile applied to the traffic

The profile 'Key Resources' configured in this example describes the actions applied on the traffic matching the Threat Prevention rule.



The profile overviews screen defines the settings for activation of protections. In this case, all protections with a performance impact 'high or lower' and the severity level 'low or above' will be activated. Remember that each protection has meta-data describing these two attributes.

Once protections have been selected for activation, protections with their meta-data attribute 'confidence level' set to 'high' or 'medium' will be active in prevent mode. Protections where the 'confidence level' attribute is defined to 'low' will be active in detect mode.



A note about the confidence level attribute: This attribute is assigned by the R&D team in relation to the amount of information obtained about an attack prevented with the protections. The more information can be obtained, the higher the confidence level attribute is defined. Protections are maintained by R&D and the confidence level attribute may change over time.

In this IPS protection example preventing attacks against a Netflix Phishing campaign the confidence level is 'high' as time has passed since the initial outbreak of the campaign.

Netflix Phishing Campaign Login and Billing Information

Performance Impact
Medium

Severity
Critical

Confidence Level
High

<p>Attack ID: CPAI-2017-1041</p> <p>Last Update: 21-March-2018</p> <p>Supported Products: Security Gateway: R80, R77, R76, R75</p> <p>Tags:</p> <p>Vendor: Generic</p> <p>Product: Generic</p> <p>Threat Year: 2017</p> <p>Protection Type: Phishing</p> <p>Protocol: SMTP</p>	<p>Threat Description: A common method for Phishing, used in malspam campaigns, is the use of hyperlinks inside such a seemingly valid entity, in order to direct the victim into a designated website controlled by the attacker or in order to make the user divulge confidential information.</p> <p>IPS Protection: This protection detects attempts to exploit this vulnerability.</p> <p>Attack Detection: Attack Name: Phishing Enforcement Protection Attack Information: Netflix Phishing Campaign Login and Billing Information</p> <p>Additional Tags: Product Prevalence: Common, Protection Tuning: Non-Configurable, Threat Prevalence: Common, Protected Asset: CLIENT.</p>
---	--

Understanding protections and their confidence level

Use the 'Threat Tools > Protections' menu in SmartConsole to understand the protections provided by the Check Point update and real time online service. IPS protections will be downloaded by the gateway (default since R80.20) while Anti-Bot, Anti-Virus and Threat-Emulation protections are provided as real time service using secured and authenticated queries raised by the gateway against the ThreatCloud database.

See for example the 'URLs with Malware' protection listed below. This protection (updated on the 24th of May 2019) presents more than 9 million URLs. The details window below demonstrates that out of these about 34% have a low confidence level attribute assigned. About 16% are known with a medium level of confidence. The majority of the URLs of 49% are known with a high level of confidence to distribute malware.

Protection	Blade	Engine	Known Today	Last Update
IPS	IPS	Signatures	10,033	5/23/2019
Reputation IPs	Anti-Bot	Reputation	62,095,265	5/24/2019
Reputation URLs	Anti-Bot	Reputation	243,363,031	5/24/2019
Reputation Domains	Anti-Bot	Reputation	243,857,965	5/24/2019
Mail Activity	Anti-Bot	Suspicious Mail Outbreaks	2,986,726	5/24/2019
Unusual Activity	Anti-Bot	Behavioral Patterns	23	5/24/2019
Malicious Activity	Anti-Bot	Signatures	7,279	5/24/2019
Viruses	Anti-Virus	Signatures	25,834,615	5/24/2019
URLs with Malware	Anti-Virus	Reputation	9,721,822	5/24/2019
File Types	Anti-Virus	File Type	89	5/24/2019
Exploit Detection	Threat Emulation	Exploit Detection	N/A	5/24/2019
Malicious Activity	Anti-Virus	Signatures	N/A	5/24/2019
Unusual Activity	Anti-Virus	Behavioral Patterns	16	5/24/2019
Links Inside Mail	Anti-Virus	Reputation	244,964,547	5/24/2019
Links Inside Mail	Anti-Bot	Reputation	236,009,847	5/24/2019

Summary | Activations

URLs with Malware | 9,721,822

General

Blade: Anti-Virus
 Engine: Reputation

Confidence Level

Low 34.11%
 Medium 16.68%
 High 49.21%

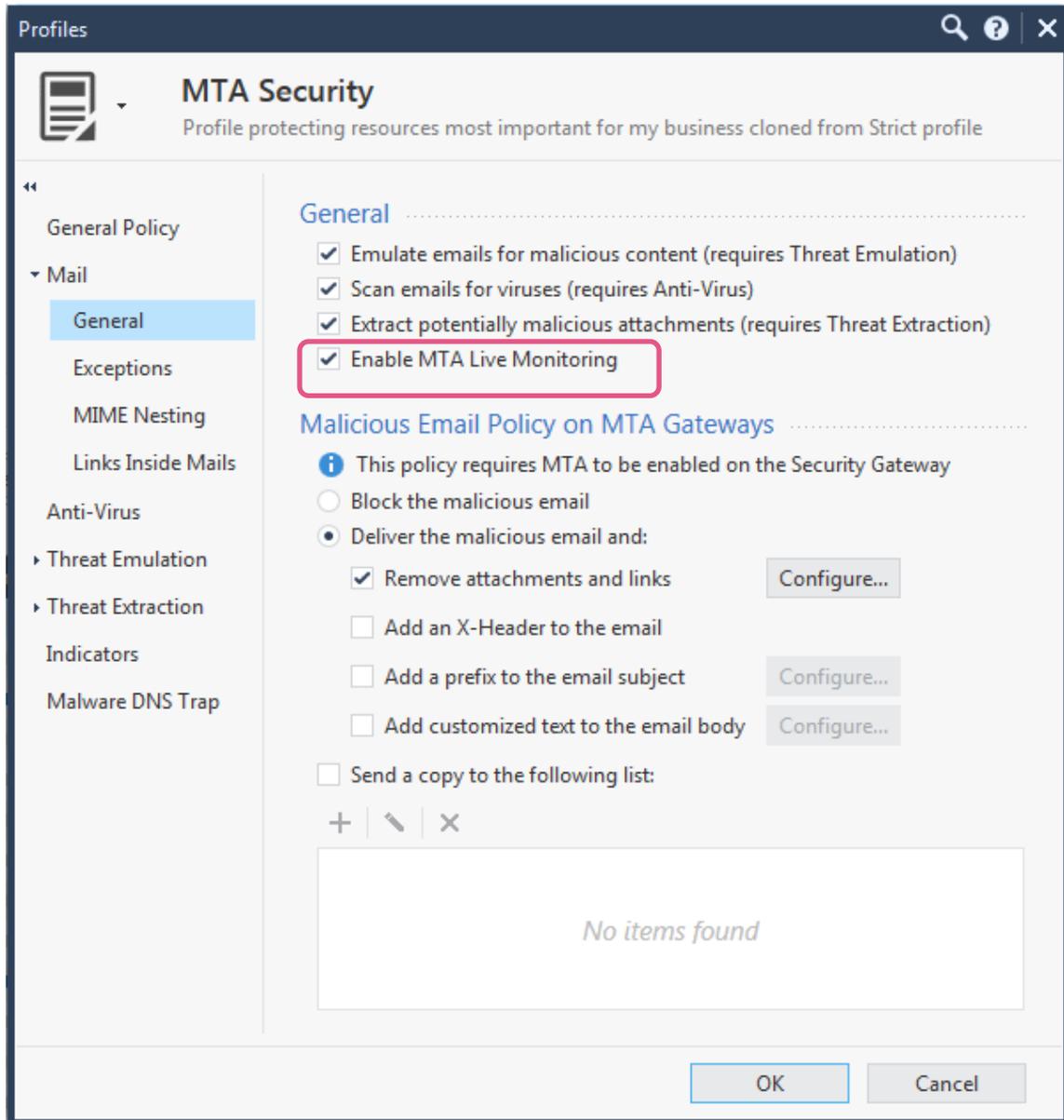
Performance Impact

Low 100.00%
 Medium 0.00%
 High 0.00%

Mail protections defined in the profile

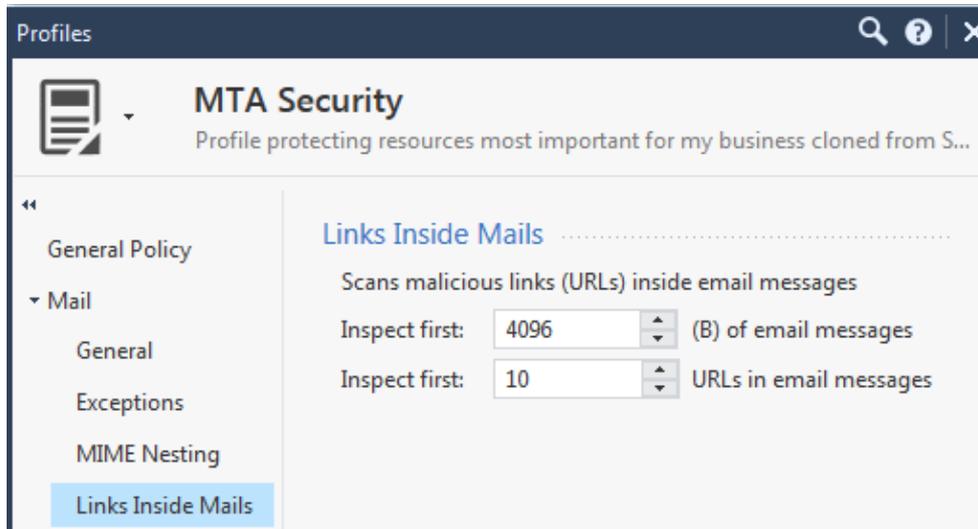
In R80.20 a new view for the mail protection configuration has been introduced and in R80.30 some improvements have been added.

MTA Live Monitoring provides information available in CPVIEW and SmartEvent about emails delivered and the related delay introduced by Zero-Day protection.



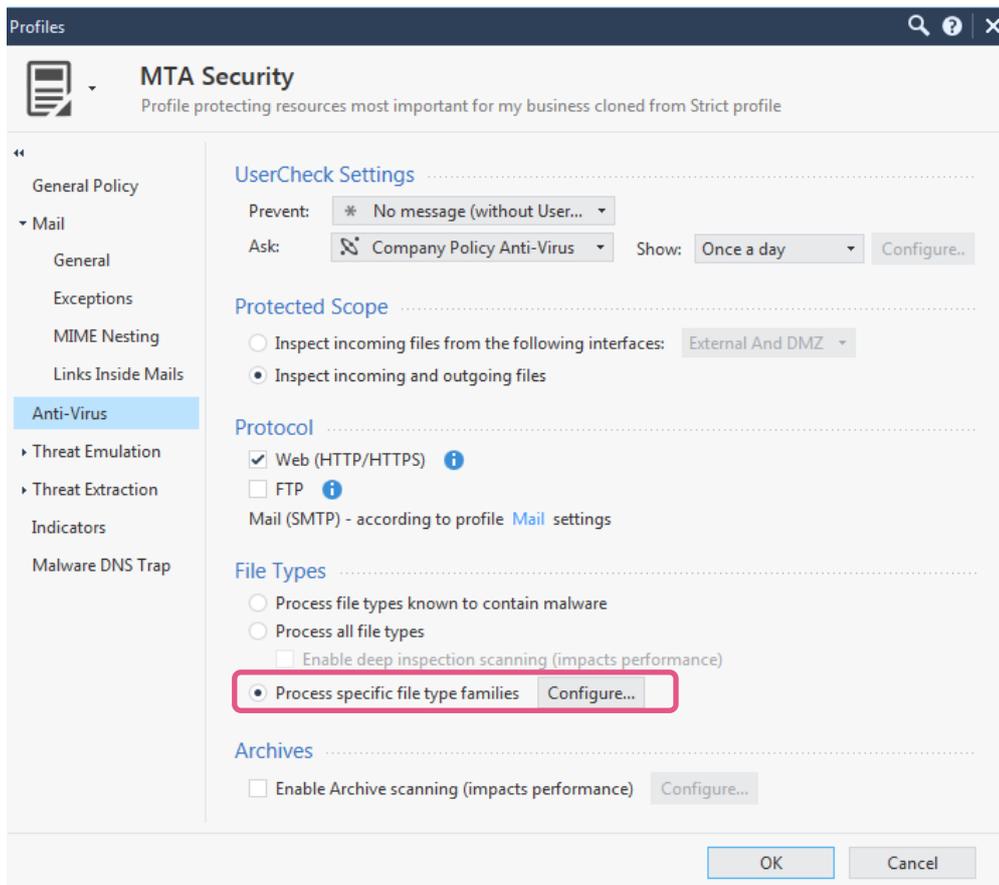
In this example the settings defined in 'exceptions' and 'MIME nesting' have been left to default.

The function 'links inside email' applies to the Anti-Virus engine checking links inside the message body.



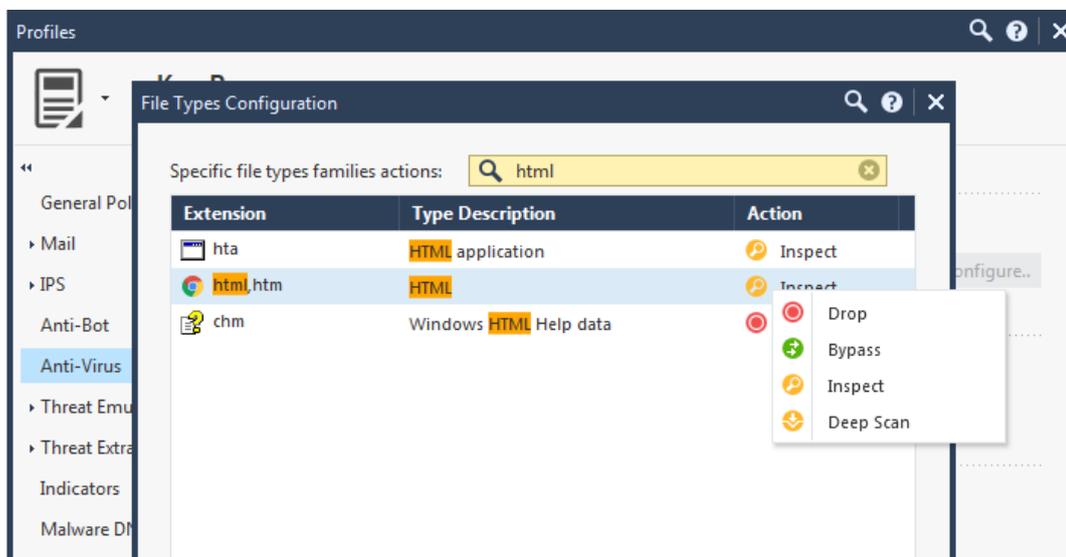
Anti-Virus settings of the Threat Prevention Profile

Known attacks are prevented using the Anti-Virus functionality available on the gateway. In this example only specific file types have been configured for analysis to keep the lab simple and to reduce load.



Decide which file types to be blocked by Anti-Virus

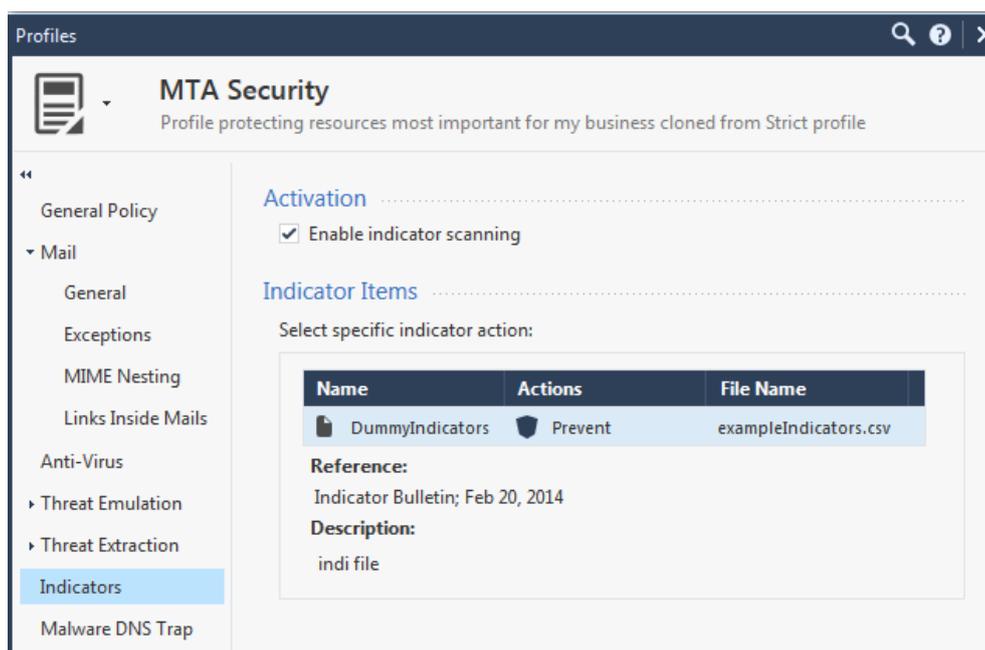
The option 'process only specific file type families' allows granular management of file types the Anti-Virus Blade shall inspect. Administrators may want to drop certain file types at this stage to limit the load on emulation services (applies to both dedicated emulation appliances and cloud hosted emulation service).



Design guideline: The 'Deep Scan' function may provide additional security to prevent known attacks but experience shows that today's sophisticated Gen V attacks require solutions powered by artificial intelligence and machine learning such as Check Point SandBlast for prevention. This is why in this lab 'Deep Scan' was not used at all.

Working with Threat Indicators imported from 3rd party static or dynamic sources

The 'Indicators' menu allows selecting imported Threat Indicators from 3rd party source. Starting with R80.30 these indicators are now applied by the Anti-Virus Blade even on traffic handled by the MTA function. In earlier versions indicators have only been applied to traffic handled in streaming mode.



Threat indicators can be imported and maintained using the relevant menu in SmartConsole using formatted csv files. The format of these files is documented in the Threat Prevention Administration Guide.

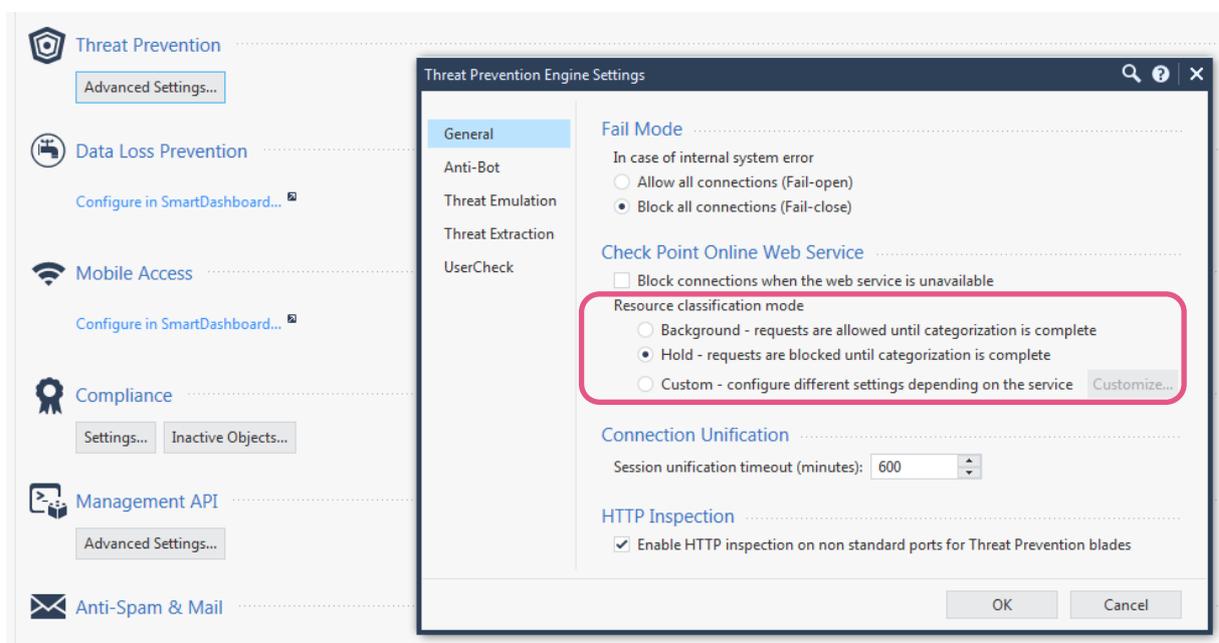
Since R80.20 custom IoC feeds can even be dynamically updated using the function documented in [sk132193](#) and this [white paper](#) posted on CheckMates.



Name	Actions	File Name	Description	Comments
DummyIndicators	Prevent	exampleIndicators.csv	indi file	used in the lab

Configure the Anti-Virus Blade to work in hold mode

Even if SMTP traffic will be handled by the MTA, the Anti-Virus Blade should be configured to work in 'Hold' mode. In the advanced settings related to Threat Prevention you can define working in background or hold mode.



Understand the 'Connection Unification' timeout setting will impact the log suppression for Threat Prevention related logs.

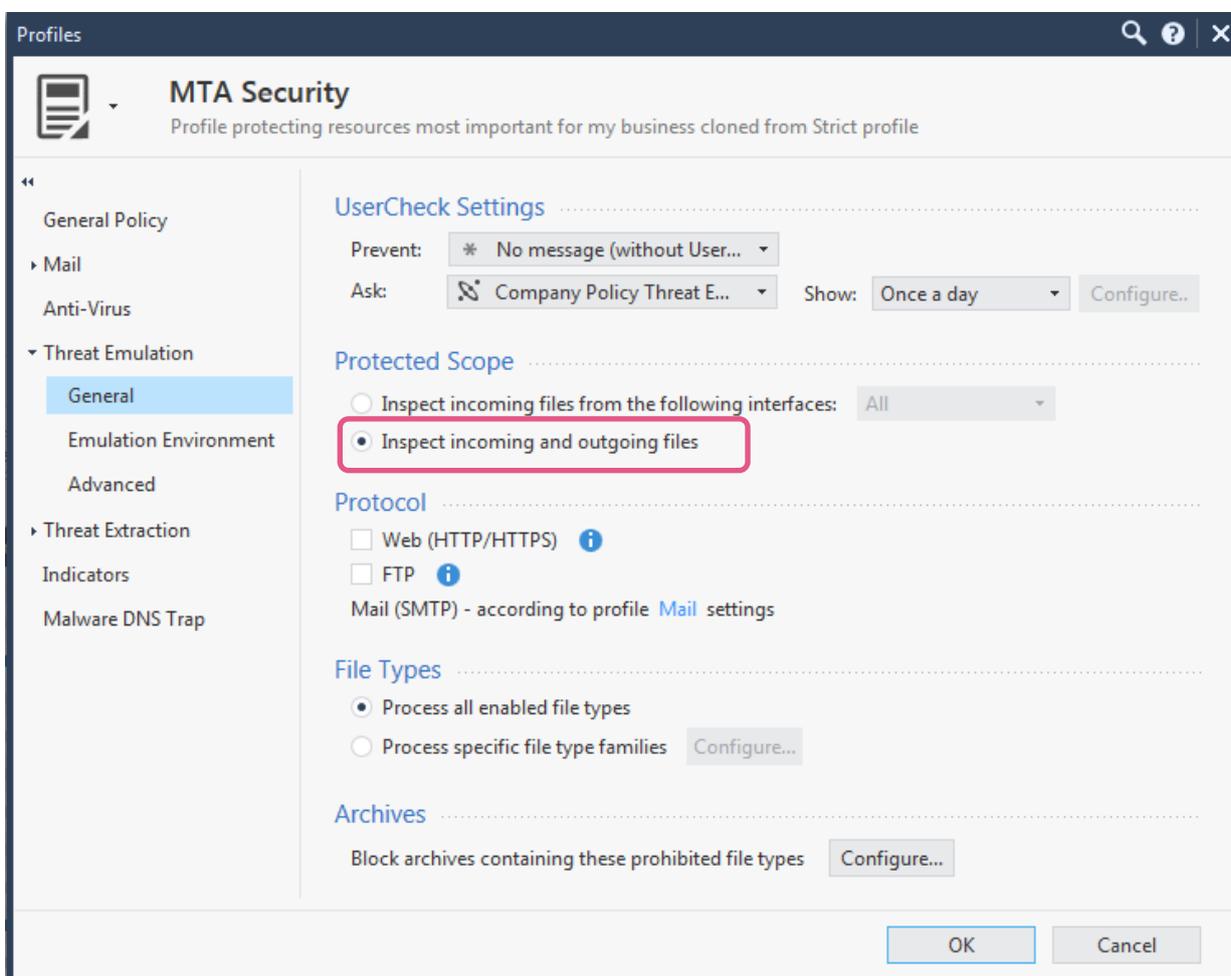
Design guideline: In R80.30 the streaming engine responsible for applying sequencing and packet stream related security has been improved. In R80.30 and later, 'Hold' mode should be configured, and the 'Fail Mode' set to reflect the business need and risk analysis.

Preventing unknown attacks

In this example the SandBlast cloud services are used to emulate files to disclose malicious activity and clean potential malicious content. In the threat prevention profile you define the actions for Threat Emulation and Threat Extraction to be applied to the traffic.

The improved streaming engine present in R80.30 allows the functions to be executed when the traffic is streamed through the gateway. When using the MTA functionality email traffic will be handled by this instance.

A note about UserCheck: It has not been used in this lab. Understand that UserCheck is based on HTTP Redirect and it can't be applied when HTTPS traffic is passing the gateway unless you enable HTTPS inspection. The improvements available in R80.30 for HTTPS inspection are out of scope of this document.

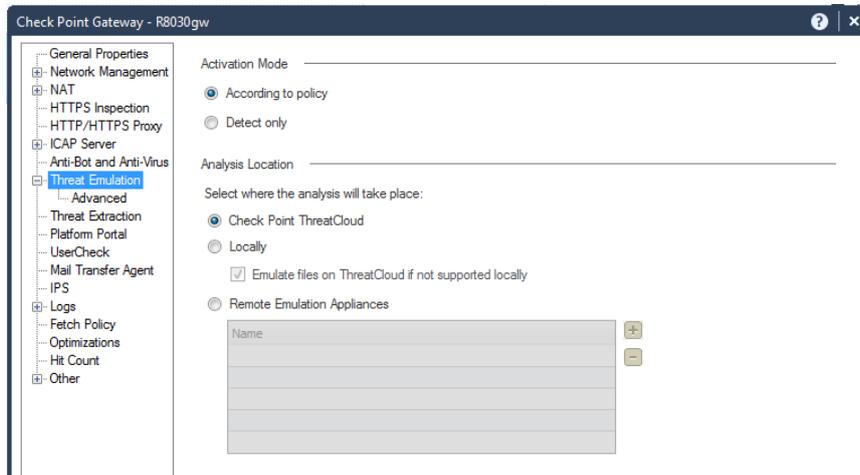


Design guideline: Using 'inspect incoming and outgoing files' meets the requirement defined in the threat prevention policy using the source and destination schema.

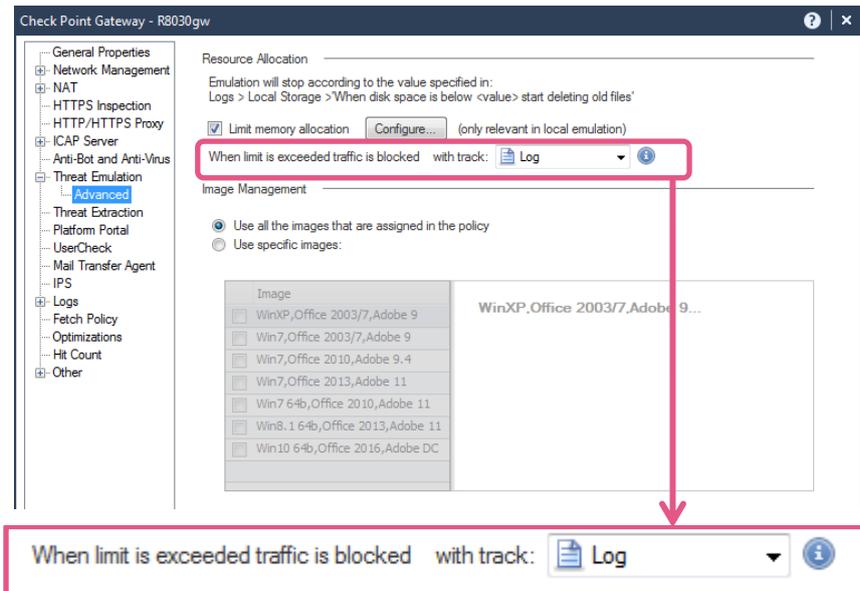
Name	Source	Destination	Protection/Site/File/Blade	Action	Track
MTA traffic to Gateway R8030gw	* Any	* Any	- N/A	MTA Security	Log Packet Capture Forensics
Protect important resources	* Any	web_server	- N/A	Key Resources	Log Packet Capture Forensics

Gateway settings for Threat Emulation

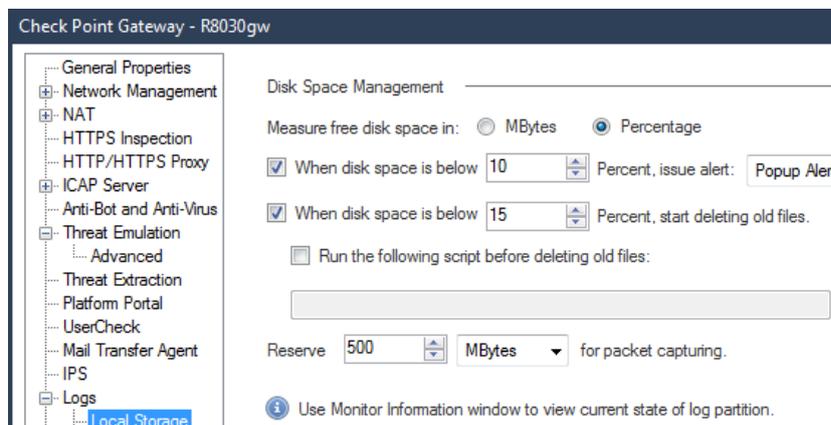
The gateway object has been configured using the cloud services.



The advanced settings have been left to default.

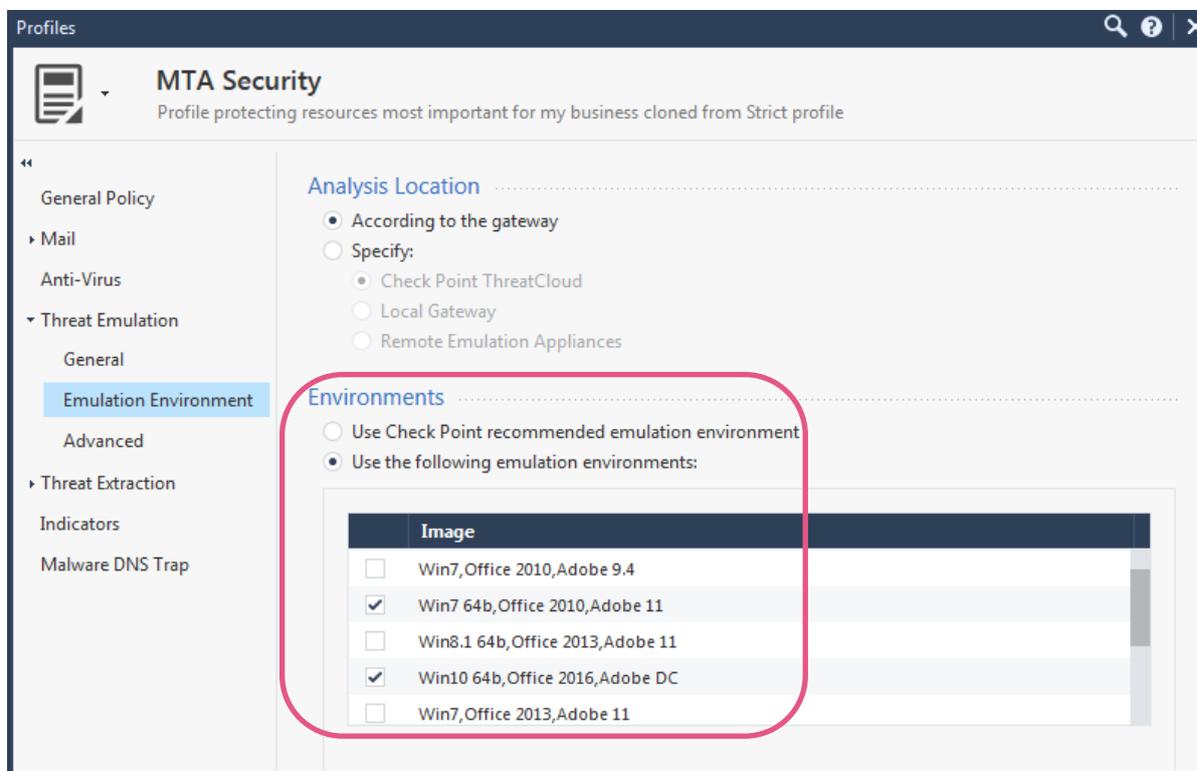


Design guideline: Review the log storage settings of your gateway to ensure that emulation actions are not interrupted if the gateway is running out of disk space.

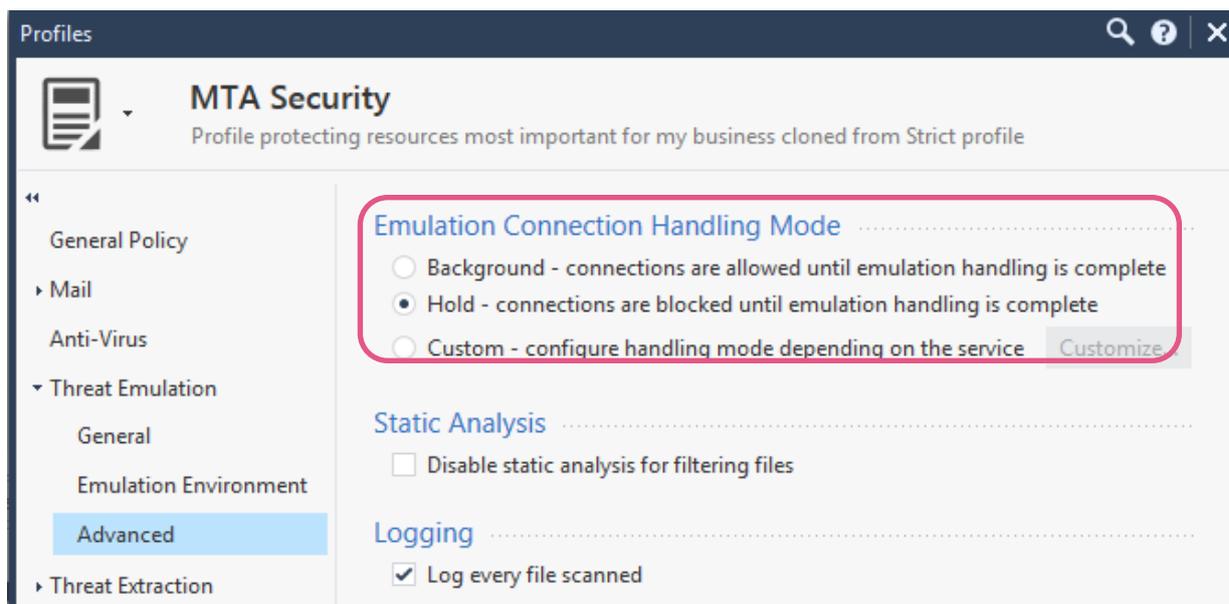


Define the emulation environment(s) and advanced settings

Configure the environment(s) where files are opened for emulation in the relevant menu of the threat prevention profile.



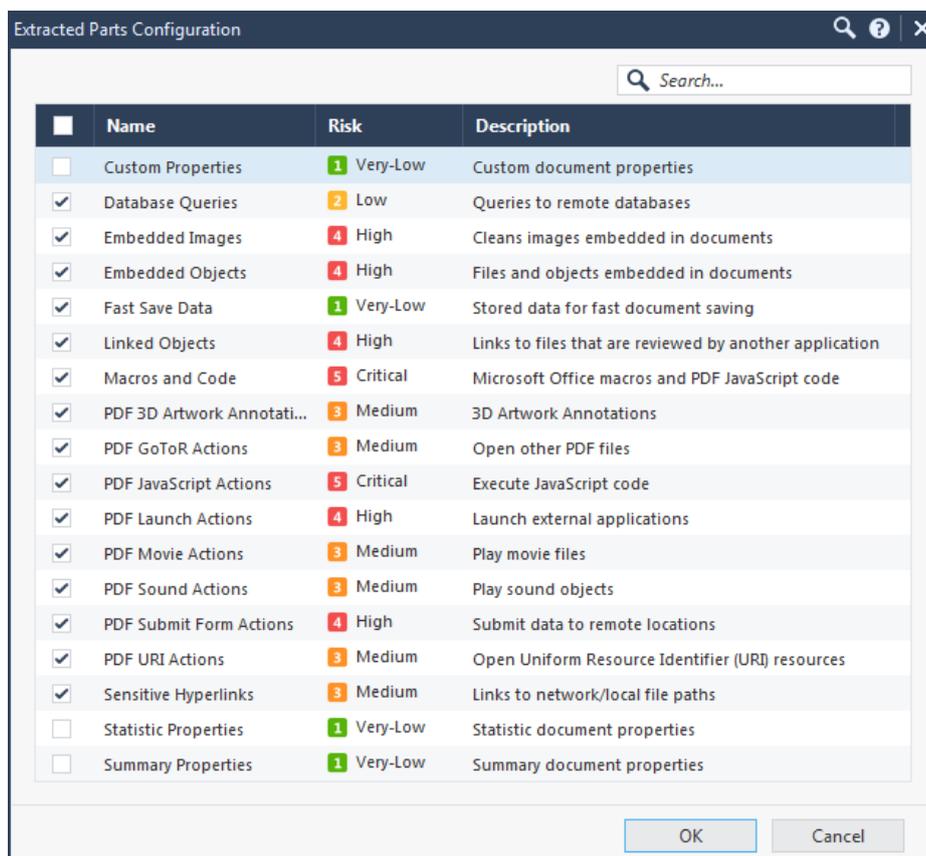
Design guideline: Configure the 'Hold' mode for Threat Emulation to be consistent with the configuration applied to the Anti-Virus Blade. Remember R80.30 has an improved streaming engine. Disabling static analysis will negatively impact the load on the emulation environment and therefore it should not be selected. Logging every file scanned impacts the disk space required on the log server and may be not necessary in a later stage of the operations life cycle.



Removing potential malicious content from files

SandBlast provides the function to extract potential malicious content from files using in office business called Threat Extraction. Starting with R80.30 this function is supported for web traffic in addition to email traffic (see [sk145773](#)).

The list of potential malicious content subject for inspection and a potential extraction can be configured in the 'extraction method' settings menu of the threat prevention profile. The list is shown below.



Design guideline: Threat Extraction functions are performed on the gateway itself – not in the cloud services or on a dedicated emulation appliance. You therefore want to evaluate the performance impact this function has when applied to web traffic as documented in [sk145773](#).

Note: Make yourself familiar with the monitoring functionalities introduced in R80.30 for the MTA functionality provided by the SmartEvent and CPVIEW.

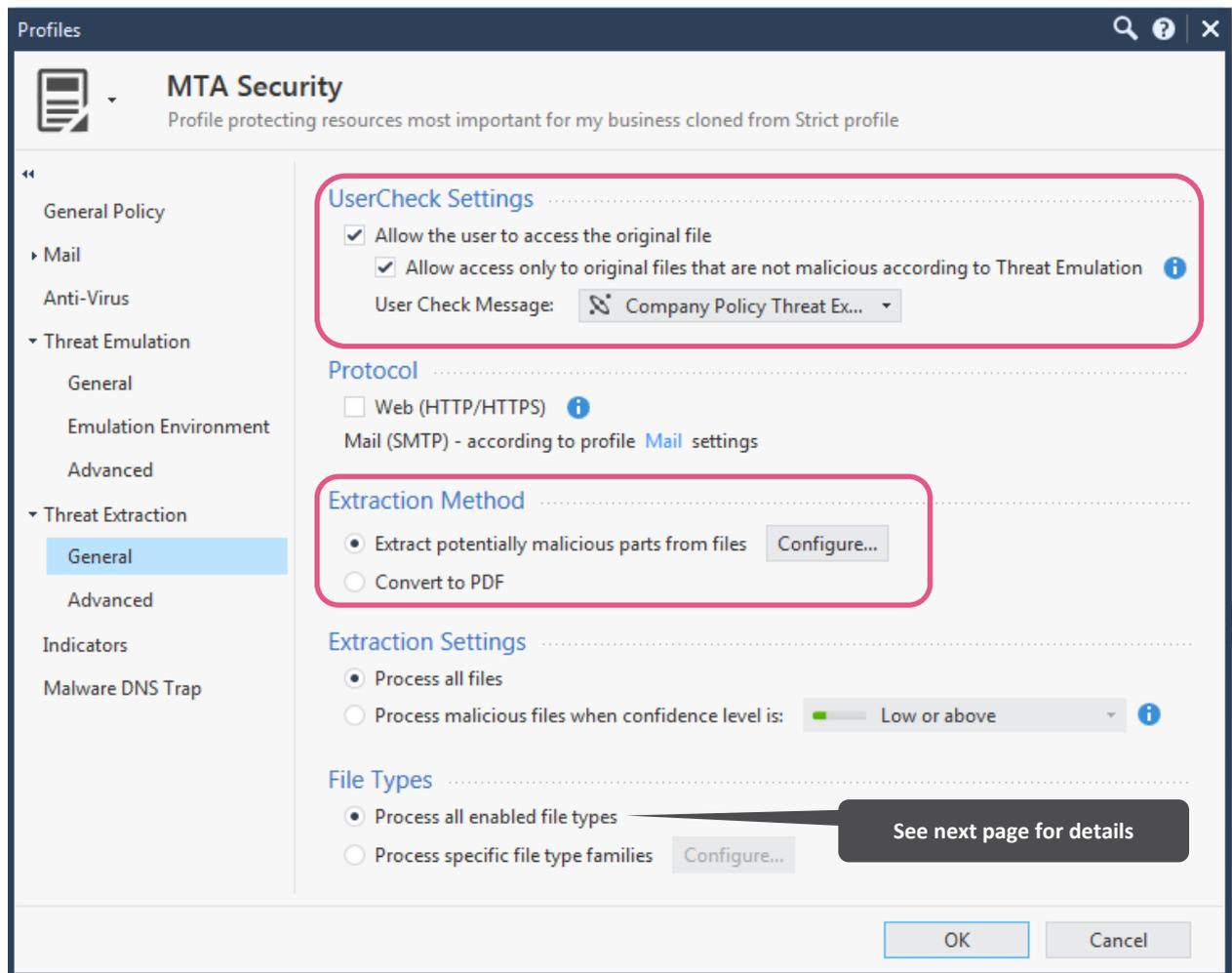
A list of file types supported by Threat Extraction and their related formats is documented in [sk101553](#).

Configuring the threat prevention profile for Threat Extraction

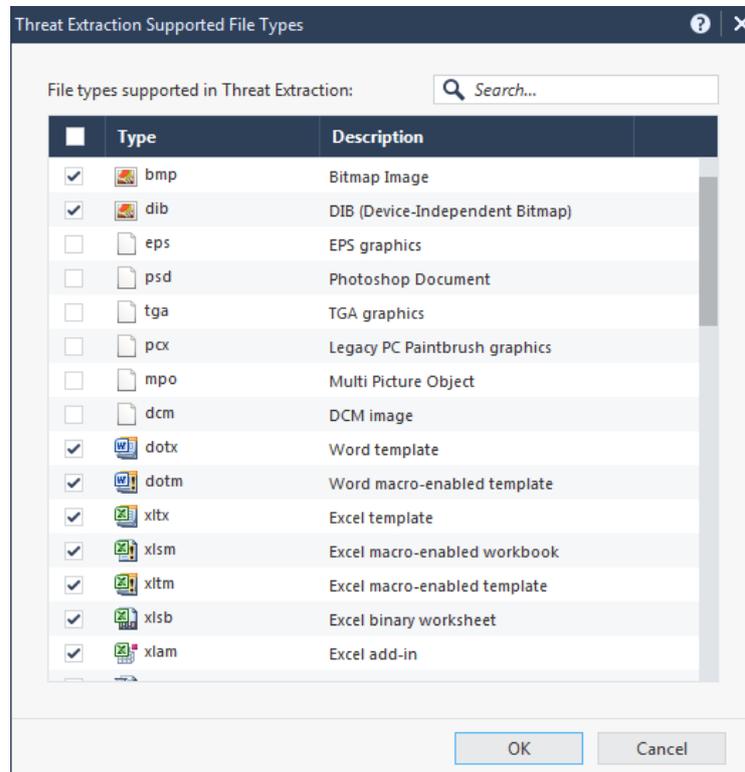
The configuration for the extraction functionality is defined in the profile settings. You can allow users downloading the original file but this setting should be evaluated carefully.

Design Guideline: Allowing users to download the original file may open up your network for potential malicious elements. Administrators should involve all relevant groups in the business organization prior to leave the default setting shown below.

The extraction methods setting configures the gateway either converting documents to PDF or extracting potential malicious elements based on the settings shown on the previous page.

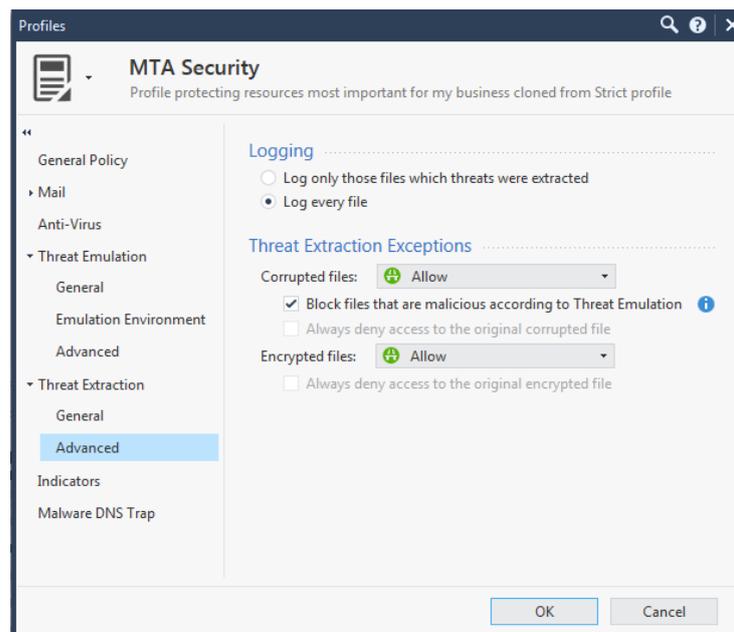


Configure the file types subject to the extraction functionality in the relevant menu.



You may wish to review the default advanced settings to ensure they reflect your business needs. In this lab it was configured to have a log message for every file handled.

Design guideline: Review the configuration for the exceptions as you may want to block corrupted and/or encrypted files instead of leaving the default setting allowing these files.

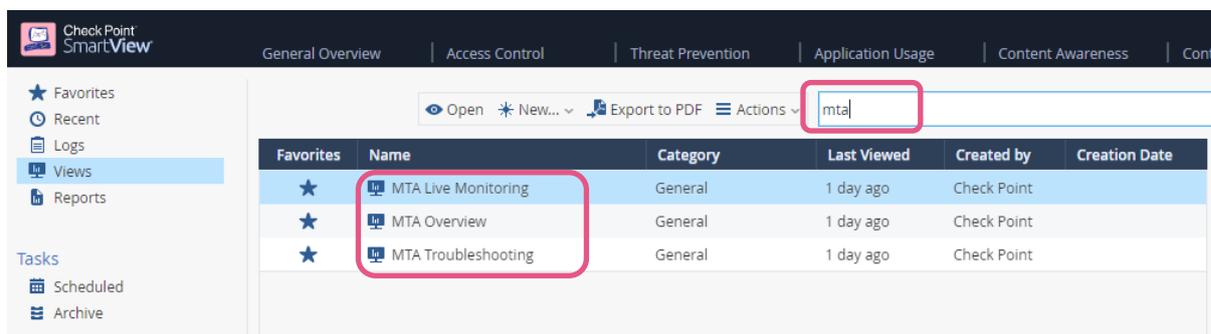


Monitoring the MTA functionality

The R80.30 release improves monitoring functionalities partially introduced in earlier versions. The MTA can be monitored using CPVIEW and SmartEvent.

Design guideline: In case in-depth monitoring and troubleshooting is required the administrator is encouraged to review the documentation in [sk120260](#) and the advanced technical reference guide [sk109699](#).

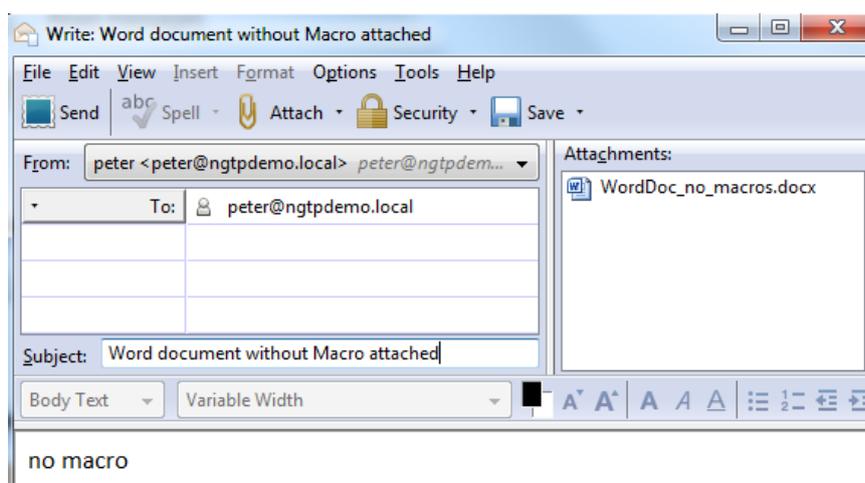
Customers purchasing a SmartEvent license have predefined templates available to view the MTA activities. You can access these templates using the SmartConsole > Logs & Monitor menu or SmartView interface using a web browser. The following screenshots are based on a web browser accessing SmartView.



For the following screenshots some demo email traffic was generated. A Thunderbird portable email client has been configured to use the MTA on the gateway as email server.

Note: When working in a lab environment make sure to have DNS resolution working for the instances taking SMTP protocol. Modifying the /etc/hosts file on the systems may be sufficient depending on the systems used in the environment.

Emails with attached documents with and without macros, documents including links and a Phishing email have been sent multiple times. Keep in mind the gateway maintains a cache of files forwarded for emulation, and that logging about malicious phishing emails is subject to log suppression.



Monitoring the MTA using CPVIEW

While emails are processed by the MTA instance CPVIEW will show the current live activities.

Design guideline: Keep in mind that you can configure CPVIEW to collect historical statistics following the guidelines provided in [sk101878](#).

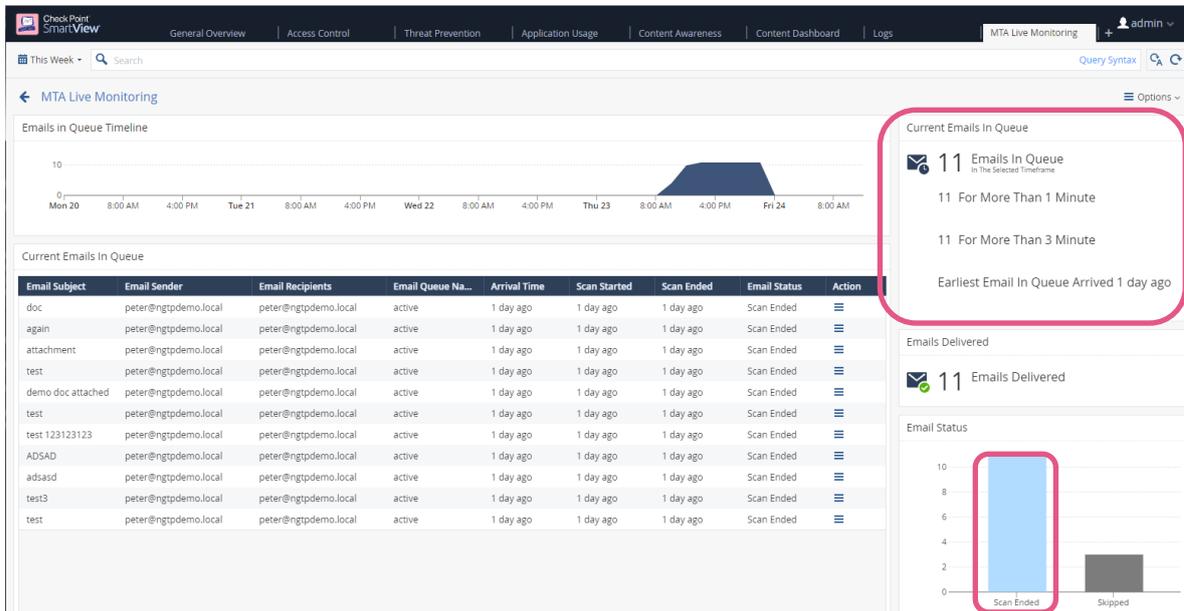
Use the Software-blades > Threat-Emulation menu to see the statistics.

```
admin@pdp_broker_1:~
-----
| CPVIEW.Software-blades.Threat-Emulation
|-----
| Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced
|-----
| Overview VPN IDA DLP Threat-Prevention Threat-Emulation Content-Awareness QoS URI
|-----
| MTA
|-----
| Queues Monitoring
|-----
| Mail Statistics:
|-----
| Mails Received                                0
| Mails With TE Supported Attachments          0
| Mails Processed                              0
| Mails Limits Exceeded                       0
| Mails Modified                               0
| Mails Deferred                               0
| Mails Blocked                                0
| Mails Skipped Due To Excluded Recipients    0
| Mails Skipped Due To Excluded Sender        0
| Mails With TE Failures                      0
| Mails With MTA Failures                    0
|-----
| Failures:
|-----
| Header size exceeds maximum                 0
| Malformed mime                             0
| Mime parsing error                          0
| Internal error                              0
| Emulation requests number exceeds maximum  0
| Emulation engine irresponsible              0
| Attachment removal error                   0
| Links removal error                        0
|-----
```

```
-----
| CPVIEW.Software-blades.Threat-Emulation.MTA.Queues
|-----
| Overview SysInfo Network CPU I/O Software-blades Hardware-Health A
|-----
| Overview VPN IDA DLP Threat-Prevention Threat-Emulation Content-A
|-----
| MTA
|-----
| Queues Monitoring
|-----
| Mail Statistics:
|-----
| Active Queue                                0
| Deferred Queue                              0
| Emaild Queue                               0
|-----
```

SmartView – MTA Live Monitoring

In the below screen you find the overview how long it took to manage the emails in the queue. Keep in mind the lab environment used for these tests has limited resources and a low Internet bandwidth.



You can click on the 'scanned email' bar and see the detailed list below

← MTA Live Monitoring > Scan Ended

Time	Blade	Ac	Ty	Int	Origin	Source	Destination	Email Sender	Email Recipient	Email Subject
May 23, 2019 12:52:36 ...	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	doc
May 23, 2019 11:36:02 ...	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	again
May 23, 2019 11:31:54 ...	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	attachment
May 23, 2019 11:30:50 ...	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	test
May 23, 2019 10:07:32 ...	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	demo doc attached
May 23, 2019 10:04:08 ...	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	test
May 23, 2019 10:03:20 ...	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	test 123123123
May 23, 2019 9:59:36 AM	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	ADSAD
May 23, 2019 9:59:04 AM	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	adsasd
May 23, 2019 9:53:28 AM	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	test3
May 23, 2019 9:50:09 AM	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	test

The emails documented with 'skipped' action have been related to an issue with the available disk space.

MTA Live Monitoring > Skipped

Time	Blade	Ac	Ty	Int	Origin	Source	Destination	Email Sender	Email Recipient	Email Subject	Email Status
May 23, 2019 12:48:45 ...	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	word	Skipped
May 23, 2019 12:43:17 ...	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	word	Skipped
May 23, 2019 12:31:59 ...	MTA				R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtptdemo.local	peter@ngtptdemo.local	link	Skipped

Card

Allow MTA May 23, 2019 12:31:59 PM

DETAILS

EMAIL HEADERS

Log Info

Origin: R8030gw

Time: May 23, 2019 12:31:59 PM

Blade: MTA

Product Family: Threat

Type: Log

Scan Information

Email Queue Name: N/A

Email Status: Skipped

Last Failure Reason: **Disk space limit was reached**

Arrival Time: 1 day ago

Email Information

Email Subject: link

Email Sender: peter@ngtptdemo.local

Email Recipient: peter@ngtptdemo.local

Email Message ID: <SCE6768C.2010708@ngtptdemo.local>

Traffic

Source: AdminPC (192.168.169.1)

Destination: R8030gw (172.27.254.30)

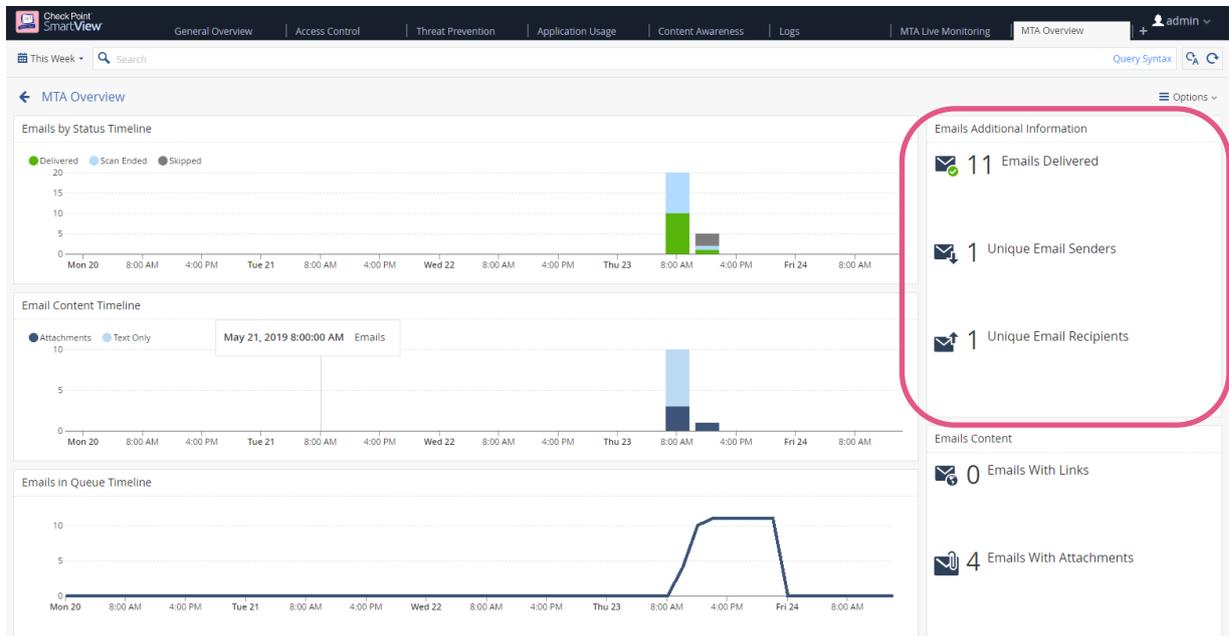
Source Port: 61022

Destination Port: 25

Last Failure Reason: Disk space limit was reached

SmartView – MTA Overview

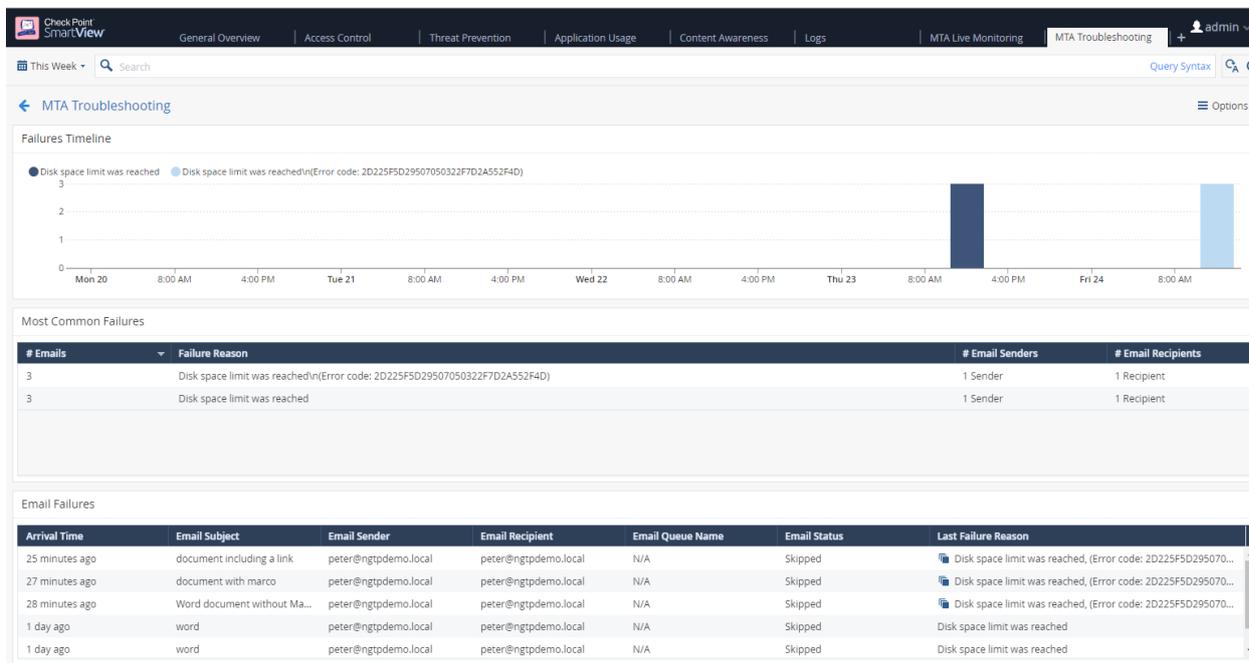
In this view you can see some statistics about the MTA.



Design guideline: Remember that all views provided in SmartView can be edited to better meet the business needs using the Options menu.

SmartView – MTA Troubleshooting

The troubleshooting view presents overview and details about email delivery failures.



Most common failures are listed as well as details about sender, recipient and the subject of the email.

# Emails	Failure Reason
3	Disk space limit was reached\n(Error code: 2D225F5D29507050322F7D2A552F4D)
3	Disk space limit was reached

Arrival Time	Email Subject	Email Sender	Email Recipient	Email Queue Name	Email Status	Last Failure Reason
27 minutes ago	document with marco	peter@ngtpdemo.local	peter@ngtpdemo.local	N/A	Skipped	Disk space limit was reach
28 minutes ago	Word document without Ma...	peter@ngtpdemo.local	peter@ngtpdemo.local	N/A	Skipped	Disk space limit was reach
1 day ago	word	peter@ngtpdemo.local	peter@ngtpdemo.local	N/A	Skipped	Disk space limit was reached
1 day ago	word	peter@ngtpdemo.local	peter@ngtpdemo.local	N/A	Skipped	Disk space limit was reached
1 day ago	link	peter@ngtpdemo.local	peter@ngtpdemo.local	N/A	Skipped	Disk space limit was reached

Exporting logs to 3rd party SIEM solutions

Customers can integrate into 3rd party SIEM solutions such as SPLUNK, Arcsight, QRadar or generic Syslog using the Check Point Log Exporter integrated in to R80.30 following the guidelines provided in [sk122323](#).

Configuring the Anti-SPAM Blade

In case the customer is looking for enabling the Anti-SPAM functionality on the gateway it is recommended following these guidelines.

Overview

The screenshot shows the 'Enforcing Gateways' configuration page for Anti-SPAM. A 'Database Updates' dialog box is open, showing proxy settings for updates. The dialog has tabs for 'Activation', 'Anti-Virus', 'Tracking Configuration', and 'Proxy'. The 'Proxy' tab is selected, showing fields for 'Host' and 'Port'. Below the fields, it states 'Proxy setting will be applied only after saving to the database.' and has 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Note: In case the gateway uses a proxy to access the Internet you need to configure the proxy settings in the 'database update' options in addition to other proxy settings.

Define the content based Anti-SPAM only to mark the emails for SPAM.

Content based Anti-Spam

The screenshot shows the 'Content based Anti-Spam' configuration section. The protection level is set to 'Low protection'. There are two checked options: 'Flag spam' and 'Flag suspected spam'. The section is titled 'Filter spam based on content fingerprint'.

[supported platforms](#)

This feature involves communication with an external server. For more information, refer to our [privacy policy](#).

Flag options

Flag subject

Add to Spam email subject line:

Add to Suspected Spam email subject line:

Flag Header

Security Gateway Engine settings

Scan only the first KB of each email.

UTM-1 Edge Engine settings

Spam confidence level:

Suspected spam confidence level:

Tracking options

Spam:

Suspected Spam:

Non spam:

Wide Impact

Define the IP reputation Anti-SPAM using the 'High protection'.

IP Reputation Anti-Spam

Filter spam from known spammers

Filter spam
 Filter suspected spam

High protection

This feature involves communication with an external server. For more information, refer to our [privacy policy](#).

UTM-1 Edge Engine settings

Spam confidence level:

Suspected spam confidence level:

Tracking options

Spam

Suspected Spam

Non spam

 Wide Impact

Recommended SecureKnowledge articles for further studies

Mail Transfer Agent – Advanced Technical Reference Guide [sk109699](#)

Configure MTA for load balancing/high availability [sk110369](#)

ThreatEmulation – Advanced Technical Reference Guide [sk114806](#)

ThreatExtraction – Advanced Technical Reference Guide [sk114807](#)