

WELCOME TO THE FUTURE OF CYBER SECURITY

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 <u>GenV attacks</u> 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 <u>Infinity</u> architecture allows customers to protect data center and cloud hosted applications as well as roaming users. Security polices 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 <u>Check Point Research</u>.

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	
Access Control Policy	
Gateway object configuration	
MTA configuration	5
Details of the Threat Prevention profile applied to the traffic	7
Understanding protections and their confidence level	
Mail protections defined in the profile	9
Anti-Virus settings of the Threat Prevention Profile	
Decide which file types to be blocked by Anti-Virus	
Working with Threat Indicators imported from 3 rd party static or dynamic sources	
Configure the Anti-Virus Blade to work in hold mode	
Preventing unknown attacks	13
Gateway settings for Threat Emulation	
Define the emulation environment(s) and advanced settings	15
Removing potential malicious content from files	
Configuring the threat prevention profile for Threat Extraction	
Monitoring the MTA functionality	
Monitoring the MTA using CPVIEW	
SmartView – MTA Live Monitoring	
SmartView – MTA Overview	
SmartView – MTA Troubleshooting	23
Exporting logs to 3 rd party SIEM solutions	23
Configuring the Anti-SPAM Blade	
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	1 9 8 8 2	 Log Packet Capture Forensics
Protect important resources	* Any	💭 web_server	— N/A	🗐 Key Resources	1 9 0 0 0	 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 <u>published at CheckMates</u> 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
Manageme	ent (1)						
Network Set	ervices (2)						
 Published S 	Services (3-5)						
3	14	MTA access	🖶 AdminPC	📼 R8030gw	💟 smtp	🕀 Accept	E Log
4	208	Access to web server	 User_Network net_172.27.254.0 	web_server	 http https ssh 	🕀 Accept	E Log
5	9	Remote Desktop	A User_Network	adserver	Remote_Desktop_Protocol	🕀 Accept	E Log
Access to In	nternet (6)						
Clean up (7	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.

Check Point Gateway - R803	0gw					8	×
General Properties	Machine —— Name: IPv4 Address: IPv6 Address:	R8030gw 172.27.254.30		Resolve from Name	Color: Black	•	
	Comment: Secure Internal Communication: Trust established Platform Hardware: Open server Version: R80.30 OS: Gaia Get						
	Network Security Access Contro Firewall IPSec VPN Policy Mobile Acc Application URL Filterii Identity Aw Content Av	r (6) Management	(0) SandB Thr Threat IPS Ant	ast: eat Emulation eat Extraction Prevention: -Bot -Virus	Advanced Networking & Clusteri Dynamic Routing SecureXL QoS Monitoring Other: Data Loss Prevention Anti-Spam & Email Security	ing:	ſ
	Co Uni	ontent Awarer ntent Awareness s fied access policy.	ness oftware I	olade provides data visibi	lity and enforcement in	ncel	

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.

- General Properties Network Management	Enable as a Mail Transfer Age	nt (MTA)			
⊡ NAT	Mail Forwarding				
HTTPS Inspection HTTP/HTTPS Proxy	📰 🔛 🖴 🗾 Type	e to Search	٩		
⊡ ICAP Server — Anti-Bot and Anti-Virus	Domain	Next Hop		Comment	ts
⊡ Threat Emulation	ngtpdemo.local	🖳 web_server			
Threat Extraction Platform Portal					
UserCheck Mail Transfer Agent					
… IPS ⊡ Logs	Add signature to scanned ema	ails:			
Fetch Policy Optimizations	Email secured by Check Point				~
Hit Count	SMTP/TLS				
⊡ Other	Please follow these steps in order t	to enable TLS inspe	ction:		
	Step 1				
	Import certificate for SMTP/TL	S			
	Sten 2				
	Enable SMTP/TLS				
	Implied Rule				
	Create an implied rule at the to	op of the Access Cor	trol Policy: (2)		
	Source		Destination	Services	Action
	* Any		This device	💟 smtp	🕀 Accept
	Advanced Settings				
	Configure Settings				
					OK Canad

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 <u>sk142932</u> 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.

MTA traffic to Gateway R8030gw	* Any	* Any	— N/A	MTA Security	1 8 8 8 6	E Log
						Packet Capture

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.

General Policy	Blades Activation			
Mail IPS Anti-Virus Threat Emulation Threat Extraction Indicators Malware DNS Trap	SandBlast Image: SandBlast	Active Protections Performance Impact: Severity: Activation Mode High Confidence: Medium Confidence: Low Confidence:	 High or lower Low or above Prevent Prevent Detect 	* * *
			OK	Cancel

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.

maintained by R&D and the confidence level attribute may change over time.

Vetflix Phishing	g Campaign Log	in and Billing Information	Performance Impact Medium	Severity Critical	Confidence Level High
Attack ID: Last Update: Supported Products:	CPAI-2017-1041 21-March-2018 Security Gateway:	Threat Description: A common method for Phishing, used in malspam campaigr into a designated website controlled by the attacker or in ord IPS Protection: This protection detects attempts to exploit this vulnerability.	ns, is the use of hyperlinks inside su er to make the user divulge confid	uch a seemingly valid entity, i ential information.	n order to direct the victim
Tags: Vendor: Product: Threat Year: Protection Type: Protocol:	Generic Generic 2017 Phishing SMTP	Attack Detection: Attack Name: Phishing Enforcement Protection Attack Information: Netflix Phishing Campaign Login and Bill Additional Tags: Product Prevalence: Common, Protection Tuning: Non-Conf	ling Information igurable, Threat Prevalence: Comr	non, Protected Asset: CLIENT	

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



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.

Profiles			ଦ୍ 🔞	×
Profile p	Security rotecting resources most important for my business c	loned from Stri	ict profile	
 ✓ General Policy ✓ Mail General Exceptions MIME Nesting Links Inside Mails Anti-Virus Threat Emulation Threat Extraction Indicators Malware DNS Trap 	General Emulate emails for malicious content (requi Scan emails for viruses (requires Anti-Virus) Extract potentially malicious attachments (region) Extract potentially malicious attachments (region) Enable MTA Live Monitoring Malicious Email Policy on MTA Gateway This policy requires MTA to be enabled on the Block the malicious email Deliver the malicious email and: Remove attachments and links Add an X-Header to the email Add a prefix to the email subject Add customized text to the email body Send a copy to the following list: + × Mo items found	res Threat Emu equires Threat I /S the Security Ga Configure Configure	lation) Extraction) teway	
		ОК	Cancel	

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.

Profiles				୯ ଡ ା ×
Profile pr	Security rotecting resources r	most importan	t for	my business cloned from S
 General Policy Mail General Exceptions MIME Nesting Links Inside Mails 	Links Inside N Scans maliciou Inspect first: Inspect first:	Mails us links (URLs) 4096 10	insid	le email messages (B) of email messages URLs in email messages

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.

Profiles	<u>୍</u> ରୁ ହ x
Profile pr	Security rotecting resources most important for my business cloned from Strict profile
 General Policy Mail General Exceptions MIME Nesting Links Inside Mails 	UserCheck Settings Prevent: * No message (without User * Ask: Company Policy Anti-Virus * Show: Once a day * Configure Protected Scope Inspect incoming files from the following interfaces: External And DMZ * Inspect incoming and outgoing files
Anti-Virus Threat Emulation Threat Extraction Indicators Malware DNS Trap	Protocol Web (HTTP/HTTPS) FTP Mail (SMTP) - according to profile Mail settings File Types
	 Process file types known to contain malware Process all file types Enable deep inspection scanning (impacts performance) Process specific file type families Configure Archives Enable Archive scanning (impacts performance) Configure
	OK Cancel

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 todays sophisticated Gen V attacks require solutions powered by artificial intelligence and machine leaning 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.

Profiles	ଦ୍ 📀	×				
Profile p	Security rotecting resources most important for my business cloned from Strict profile					
 ✓ General Policy ✓ Mail General Exceptions 	Activation Enable indicator scanning Indicator Items Select specific indicator action:					
' MIME Nesting Links Inside Mails	Name Actions File Name DummyIndicators Prevent exampleIndicators.csv					
Anti-Virus ▶ Threat Emulation ▶ Threat Extraction	Reference: Indicator Bulletin; Feb 20, 2014 Description:					
Indicators Malware DNS Trap						

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 <u>sk132193</u> and this <u>white paper</u> posted on CheckMates.

Indicators					* ●	Search
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.

Advanced Settings	Threat Prevention Engin	le Settings Q 👔 🗙
	General	Fail Mode
Data Loss Prevention	Anti-Bot	In case of internal system error Allow all connections (Fail-open)
Configure in SmartDashboard 🗖	Threat Emulation	Block all connections (Fail-close)
	Threat Extraction	Check Point Online Web Service
Mobile Access	UserCheck	Block connections when the web service is unavailable
Configure in SmartDashboard 🕿		Resource classification mode Background - requests are allowed until categorization is complete Hold - requests are blocked until categorization is complete
Compliance		O Custom - configure different settings depending on the service Customize
Settings Inactive Objects		Connection Unification
		Session unification timeout (minutes): 600
Nanagement API		HTTP Inspection
Advanced Settings		Enable HTTP inspection on non standard ports for Threat Prevention blades
🗙 Anti-Snam & Mail		OK Cancel

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.

Profiles	Q 0 X
Profile protecti	I rity ng resources most important for my business cloned from Strict profile
 General Policy Mail Anti-Virus Threat Emulation 	UserCheck Settings Prevent: * No message (without User * Ask: Company Policy Threat E * Show: Once a day * Configure Protected Scope
Emulation Environment Advanced Threat Extraction Indicators Malware DNS Trap	 Inspect incoming files from the following interfaces: All • Inspect incoming and outgoing files Protocol Web (HTTP/HTTPS) FTP FTP Mail (SMTP) - according to profile Mail settings File Types Process all enabled file types Process specific file type families Configure Archives Block archives containing these prohibited file types Configure
	OK Cancel

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	I 8 8 8 2	 Log Packet Capture Forensics
Protect important resources	* Any	💭 web_server	— N/A	📕 Key Resources 🛛	8888	 Log Packet Capture Forensics

Gateway settings for Threat Emulation

The gateway object has been configured using the cloud services.

Check Point Gateway - R803	0gw	?	×
General Properties Network Management NAT HTTPS Inspection HTTP/HTTPS Proxy CAP Server	Activation Mode Activation Mode		
Anti-Bot and Anti-Virus Threat Enulation Advanced Threat Enulation Hatform Portal UserCheck Mail Transfer Agent IPS Cogs Fetch Policy Optimizations Hit Count Other	Analysis Location Select where the analysis will take place: Check Point ThreatCloud Check Point Thre		

The advanced settings have been left to default.

Check Point Gateway - R80	30gw		?
General Properties Network Management NAT HTTPS Inspection HTTP/HTTPS Proxy ICAP Server Arti-Bot and Arti-Vrus Threat Emulation Advanced Threat Extraction Platform Portal UserCheck Mail Transfer Agent	Resource Allocation Enulation will stop according to the value spec Logs > Local Storage >When disk space is be Unit memory allocation Configure When limit is exceeded traffic is blocked with Image Management Subse all the images that are assigned in the Use specific images:	sfied in: low <value> start deleting old files" (only relevant in local emulation) track: 📄 Log 🔹 👔</value>	
IPS B- Logs Fetch Policy Optimizations Hit Count B- Other	Image WinXP,Office 2003/7,Adobe 9 Win7,Office 2013/7,Adobe 9 Win7,Office 2010,Adobe 9.4 Win7,Office 2013,Adobe 11 Win7,Office 2013,Adobe 11 Win7, 64b,Office 2013,Adobe 11 Win8.1 64b,Office 2013,Adobe 11 Win8.0 64b,Office 2016,Adobe 10	WinXP,Office 2003/7,Adobe 9	
		•	
When limit is ex	ceeded traffic is blocked wi	th track: 🗎 Log	-

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.

Check Point Gateway - R80	30gw
General Properties Nat HTTPS Inspection HTTP/HTTPS Proxy CICAP Server Anti-Bot and Anti-Virus HTTP:/HTTPS Emulation Advanced Threat Endraction	Disk Space Management Measure free disk space in: MBytes Percentage When disk space is below 10 Percent, issue alert: Popup Alert When disk space is below 15 Percent, start deleting old files. Run the following script before deleting old files:
Platform Portal	
···· UserCheck ···· Mail Transfer Agent ···· IPS	Reserve 500 🔄 MBytes → for packet capturing.
⊡ Logs Local Storage	Use Monitor Information window to view current state of log partition.

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.

Profiles	Q. Ø X
MTA Securi	ty
Profile protecting	resources most important for my business cloned from Strict profile
44	Analysis Location
General Policy	According to the gateway
▶ Mail	Specify:
Anti-Virus	Check Point ThreatCloud
Threat Emulation	🔿 Local Gateway
General	Remote Emulation Appliances
Emulation Environment	Environments
Advanced	Use Check Point recommended emulation environment
Threat Extraction	 Use the following emulation environments:
Indicators	
	Image
Malware DNS Trap	Win7,Office 2010,Adobe 9.4
	✓ Win7 64b,Office 2010,Adobe 11
	Win8.1 64b, Office 2013, Adobe 11
	✓ Win10 64b,Office 2016,Adobe DC
	Win7,Office 2013,Adobe 11
configuration applied to Disabling static analysis it should not be selecte server and may be not	b the Anti-Virus Blade. Remember R80.30 has an improved streaming engine. will negatively impact the load on the emulation environment and therefore d. Logging every file scanned impacts the disk space required on the log necessary in a later stage of the operations life cycle.
server and may be not	
rofiles	Q, @ ×
Profile protect	curity cting resources most important for my business cloned from Strict profile
4	Emulation Connection Handling Mode
General Policy	
▶ Mail	Background - connections are allowed until emulation handling is complete
Anti-Virus	Hold - connections are plocked until emulation handling is complete
- Theoret French t	Custom - configure handling mode depending on the service Customize
 Inreat Emulation 	Static Applyria
General	Static Analysis
Emulation Environment	Disable static analysis for filtering files
Advanced	Logging

Log every file scanned

Threat Extraction

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 <u>sk145773</u>).

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.

Extract	ed Parts Configu	ration				Q 🕐	×
					Q Search		
	Name		Risk	Description			
	Custom Pro	perties	1 Very-Low	Custom document	properties		
~	Database Q	ueries	2 Low	Queries to remote	databases		
~	Embedded I	mages	4 High	Cleans images emb	edded in documents		
-	Embedded (Objects	4 High	Files and objects e	mbedded in documents		
~	Fast Save Da	ata	1 Very-Low	Stored data for fas	t document saving		
-	Linked Obje	ects	4 High	Links to files that a	re reviewed by another app	lication	
~	Macros and	Code	5 Critical	Microsoft Office ma	acros and PDF JavaScript co	de	
-	PDF 3D Artw	vork Annotati	3 Medium	3D Artwork Annota	ations		
~	PDF GoToR	Actions	3 Medium	Open other PDF fil	es		
-	PDF JavaScri	ipt Actions	S Critical	Execute JavaScript	code		
~	PDF Launch	Actions	4 High	Launch external ap	plications		
-	PDF Movie A	Actions	3 Medium	Play movie files			
~	PDF Sound	Actions	3 Medium	Play sound objects			
-	PDF Submit	Form Actions	4 High	Submit data to rem	note locations		
~	PDF URI Act	ions	3 Medium	Open Uniform Res	ource Identifier (URI) resour	rces	
-	Sensitive Hy	perlinks	3 Medium	Links to network/local file paths			
	Statistic Pro	perties	1 Very-Low	Statistic document properties			
	Summary Pr	operties	1 Very-Low	Summary documen	t properties		
					ОК	Cancel	

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 $\frac{sk145773}{s}$.

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 <u>sk101553</u>.

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.

Profiles	9, 10 ×
MTA Secu Profile protectir	rity ng resources most important for my business cloned from Strict profile
 General Policy Mail Anti-Virus Threat Emulation General Emulation Environment Advanced Threat Extraction General Advanced Indicators Malware DNS Trap 	UserCheck Settings Image: Allow the user to access the original files that are not malicious according to Threat Emulation Image: Allow access only to original files that are not malicious according to Threat Emulation User Check Message: Image: Check Message: Check Message: Image: Check Message:
	OK Cancel

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

Threat Ext	raction Supported Fi	le Types	• •
File ty	pes supported in Th	reat Extraction: Q Search	1
	Туре	Description	
~	🛃 bmp	Bitmap Image	
~	dib 🔝	DIB (Device-Independent B	3itmap)
	eps	EPS graphics	
	psd 📄	Photoshop Document	
	📄 tga	TGA graphics	
	рсх	Legacy PC Paintbrush grap	hics
	📄 mpo	Multi Picture Object	
	dcm	DCM image	
~	👜 dotx	Word template	
~	🖳 dotm	Word macro-enabled temp	plate
~	🔊 xitx	Excel template	
~	🔊 xlsm	Excel macro-enabled work	book
~	💐 xltm	Excel macro-enabled templ	late
~	🔊 xisb	Excel binary worksheet	
~	🔊 xlam	Excel add-in	
		O	K Cancel

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 $\frac{sk120260}{sk109699}$ and the advanced technical reference guide $\frac{sk109699}{sk109699}$.

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.

Check Point Smart View	General Oven	view Access Control	Threat Prevention	Application Usage	Content	Awareness Cont
★ Favorites ③ Recent		Open	📌 Export to PDF 🛛 = Actions -	v mta		
Logs	Favorites	Name	Category	Last Viewed	Created by	Creation Date
Reports	*	MTA Live Monitoring	General	1 day ago	Check Point	
	*	MTA Overview	General	1 day ago	Check Point	
Tasks	*	🛄 MTA Troubleshooting	General	1 day ago	Check Point	
ScheduledArchive						

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.

C Write: Word document without Macro attached	
<u>File Edit View Insert Format Options Tools H</u> elp	
Send Spell - U Attach - G Security - 🗔 Sa	ave *
From: peter <peter@ngtpdemo.local> peter@ngtpdem •</peter@ngtpdemo.local>	Attachments:
To: A peter@ngtpdemo.local	WordDoc_no_macros.docx
Subject: Word document without Macro attached	
Body Text 👻 Variable Width 👻	
no macro	

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 <u>sk101878</u>.

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

子 admin@pdp_broker_1:~	
CONTEN Software-blades Threat-Emulation	
Overview SysInfo Network CPU I/O Software-bla	ades Hardware-Health Advanced
Overview VPN IDA DLP Threat-Prevention Threat	-Emulation Content-Awareness QoS URI
МТА	
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 irresponsive	0
Attachment removal error	0
Links removal error	0

CPVIEW.Software-bla	des.Threat-Em	ulation.MTA.	Queues	
Overview SysInfo Ne	twork CPU I/O	Software-bl	lades Hardwai	re-Health
Overview VPN IDA DL	P Threat-Preve	ention Threa	at-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.

NATA LINE MAR	- New John and									
MTA Live Mor	nitoring								_	≡ 0
nails in Queue Tii	neline								Current Em	ails In Queue
10									X 11	Emails In Queue
									-0	In The Selected Timeframe
0 Mon 20 8:1	00 AM 4:00 PM Tue	21 8:00 AM 4:00 PM	Wed 22 8:00	AM 4:00 PM	Thu 23 8	8:00 AM 4:00 PM	Fri 24	8:00 AM	11 F	For More Than 1 Minute
									11 F	For More Than 3 Minute
urrent Emails In Q	lueue									
mail Subject	Email Sender	Email Recipients	Email Queue Na	Arrival Time	Scan Started	Scan Ended	Email Status	Action	Earli	iest Email In Queue Arrived 1 day
E mail Subject doc	Email Sender peter@ngtpdemo.local	Email Recipients peter@ngtpdemo.local	Email Queue Na	Arrival Time	Scan Started	Scan Ended 1 day ago	Email Status Scan Ended	Action	Earli	iest Email In Queue Arrived 1 day
imail Subject doc again	Email Sender peter@ngtpdemo.local peter@ngtpdemo.local	Email Recipients peter@ngtpdemo.local peter@ngtpdemo.local	Email Queue Na active active	Arrival Time 1 day ago 1 day ago	Scan Started 1 day ago 1 day ago	Scan Ended 1 day ago 1 day ago	Email Status Scan Ended Scan Ended	Action	Earli	iest Email In Queue Arrived 1 day
e mail Subject doc again attachment	Email Sender peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Recipients peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Queue Na active active active	Arrival Time 1 day ago 1 day ago 1 day ago	Scan Started 1 day ago 1 day ago 1 day ago	Scan Ended 1 day ago 1 day ago 1 day ago	Email Status Scan Ended Scan Ended Scan Ended	Action	Earli Emails Deli	iest Email In Queue Arrived 1 day vered
mail Subject loc Igain Ittachment est	Email Sender peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Recipients peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Queue Na active active active active	Arrival Time 1 day ago	Scan Started 1 day ago 1 day ago 1 day ago 1 day ago	Scan Ended 1 day ago 1 day ago 1 day ago 1 day ago	Email Status Scan Ended Scan Ended Scan Ended Scan Ended	Action	Earli Emails Deli	est Email In Queue Arrived 1 day vered Emails Delivered
mail Subject loc Igain Ittachment est Iemo doc attached	Email Sender peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Recipients peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Queue Na active active active active active	Arrival Time 1 day ago	Scan Started 1 day ago 1 day ago 1 day ago 1 day ago 1 day ago 1 day ago	Scan Ended 1 day ago 1 day ago 1 day ago 1 day ago 1 day ago 1 day ago	Email Status Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended	Action	Earli Emails Deli S 11	est Email In Queue Arrived 1 day vered Emails Delivered
imail Subject doc again attachment est Jemo doc attached est	Email Sender peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Recipients peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Queue Na active active active active active active active	Arrival Time 1 day ago	Scan Started 1 day ago 1 day ago 1 day ago 1 day ago 1 day ago 1 day ago 1 day ago	Scan Ended 1 day ago	Email Status Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended	Action	Earli Emails Deli 2011	est Email In Queue Arrived 1 day vered Emails Delivered
mail Subject doc again attachment est Jemo doc attached est est 123123123	Email Sender peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Recipients peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Queue Na active active active active active active active active	Arrival Time 1 day ago	Scan Started 1 day ago 1 day ago	Scan Ended 1 day ago	Email Status Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended	Action	Earli Emails Deli Email Statu	est Email In Queue Arrived 1 day vered Emails Delivered
imail Subject loc ggain ttachment est lemo doc attached est est 123123123 LDSAD	Email Sender peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Recipients peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Queue Na active active active active active active active active active	Arrival Time 1 day ago	Scan Started 1 day ago	Scan Ended 1 day ago	Email Status Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended	Action	Earli Emails Deli Caralistatu	est Email In Queue Arrived 1 day vered Emails Delivered
mail Subject loc gain ttachment est lemo doc attached est 123123123 uDSAD udsasd	Email Sender peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Recipients peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Queue Na active active active active active active active active active active	Arrival Time 1 day ago	Scan Started 1 day ago	Scan Ended 1 day ago	Email Status Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended	Action	Earli Emails Deli Constantion Email Statu	est Email In Queue Arrived 1 day vered Emails Delivered
mail Subject oc gain ttachment est est 123123123 DSAD dsasd est3	Email Sender peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Recipients peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local peter@ngtpdemo.local	Email Queue Na active active active active active active active active active active	Arrival Time 1 day ago 1 day ago	Scan Started 1 day ago 1 day ago	Scan Ended 1 day ago 1 day ago	Email Status Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended Scan Ended	Action Action	Earli Emails Deli Constant Email Statu 10 8	est Email In Queue Arrived 1 day vered Emails Delivered

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

÷	MTA Live Monitoring >	Scan End	ed						
₩	Time 👻	Blade	Ac Ty Int	Origin	Source	Destination	Email Sender	Email Recipient	Email Subject
	🔇 May 23, 2019 12:52:36	🖏 MTA	8	📼 R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	doc
	🔇 May 23, 2019 11:36:02	🏹 MTA		📼 R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	again
	🔇 May 23, 2019 11:31:54	🏹 MTA		📼 R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	attachment
	🔇 May 23, 2019 11:30:50	🏹 MTA		📼 R8030gw	Z AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	test
	🔇 May 23, 2019 10:07:32	🏹 MTA		📼 R8030gw	Z AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	demo doc attached
	🔇 May 23, 2019 10:04:08	🏹 MTA		📼 R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	test
	🔇 May 23, 2019 10:03:20	🏹 MTA		📼 R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	test 123123123
	🔇 May 23, 2019 9:59:36 AM	🏹 MTA		📼 R8030gw	Z AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	ADSAD
	🔇 May 23, 2019 9:59:04 AM	😽 MTA		📼 R8030gw	Z AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	adsasd
n	🔇 May 23, 2019 9:53:28 AM	MTA 🍣		📼 R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	test3
atistic	🔇 May 23, 2019 9:50:09 AM	🏹 MTA		📼 R8030gw	AdminPC (192.168.169.1)	R8030gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	test

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

ime 👻 Bli Ac	Ty In	Origin	Source	Destinatio	n	Email Sender	Email Recipient	Email Subject	Email Stat
)May 23, 2019 12:48:45 🛛 🖏 😗	B 1	🛤 R8030gw	Z AdminPC (192.168.169.1)	🗵 R8030g	gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	word	Skipped
🕽 May 23, 2019 12:43:17 🗣 🚯	🗎 ±	📾 R8030gw	Z AdminPC (192.168.169.1)	2 R8030g	w (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	word	Skipped
🔊 May 23, 2019 12:31:59 👒 🚳	E ±	R8030gw	AdminPC (192.168.169.1)	ZI R8030g	gw (172.27.254.30)	peter@ngtpdemo.local	peter@ngtpdemo.local	link	Skipped
		Card					□ × □		
		Allow SMTA	O May 23, 2019 12:31:59 PM						
		DETAILS	EMAIL HEADERS						
		Log Info		~	Email Information				
		Origin:	6 R8030gw		Email Subject:	link			
		Time:	May 23, 2019 12:31:59 PM		Email Sender:	peter@ngtpdemo.local			
		Biade:	MTA		Email Recipient	peter@ngtpdemo.local			
		Product Family:	Threat		Email Message ID:	<5CE6768C.2010708@ngtpdemo.	local>		
		Type:	Log		1000				
					Traffic				
		Scan Informatio	n	~	Source:	AdminPC (192.168.169.1)			
		Email Queue Name	: N/A		Destination:	R8030gw (172.27.254.30)			
		Email Status:	Skipped		Source Port:	61022			
		Last Failure Reason	Disk space limit was reached		Destination Port:	25			
		Arrival Time:	1 day ago				÷		
			T						
								1	
	1 =	st Epilure	Descon:	Diel	coace lin	nit was reach	had		
	LC	SUFAIIUI	Reason.	DISP	space in	nit was react	leu		

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.

Check Point Smart View	General Overview Ac	cess Control Thre	at Prevention Ap	oplication Usage	Content Aware	ness Logs	1	MTA Live Monitoring	MTA Troubleshootir	ng + admin ~
🛱 This Week 👻 🔍 Sea										Query Syntax
← MTA Troublesho	ooting									
Failures Timeline										
Disk space limit was rea	ached Oisk space limit was reached\n(l	Error code: 2D225F5D29507050:	22F7D2A552F4D)							
3										
1										
0										
Mon 20	8:00 AM 4:00 PM	Tue 21 8:00 AM	4:00 PM	Wed 22	8:00 AM 4	:00 PM	Thu 23 8:00 4	M 4:00 PM	Fri 24	8:00 AM
Most Common Failure	:5									
# Emails								# Email Senders	# Ema	il Recipients
3	Disk space limit was reached\r	n(Error code: 2D225F5D29507	050322F7D2A552F4D)					1 Sender	1 Reci	pient
3	Disk space limit was reached							1 Sender	1 Reci	pient
Email Failures										
Arrival Time	Email Subject	Email Sender	Email Recipient	Ema	ail Queue Name	Email Sta	itus	Last Failure Reason		
25 minutes ago	document including a link	peter@ngtpdemo.local	peter@ngtpdemo.	local N/A	ι	Skipped		n Disk space limit wa	as reached, (Error code:	2D225F5D295070
27 minutes ago	document with marco	peter@ngtpdemo.local	peter@ngtpdemo.	local N/A	4	Skipped		n Disk space limit wa	as reached, (Error code:	2D225F5D295070
28 minutes ago	Word document without Ma	peter@ngtpdemo.local	peter@ngtpdemo.	local N/A	A.	Skipped		盾 Disk space limit wa	as reached, (Error code:	2D225F5D295070
1 day ago	word	peter@ngtpdemo.local	peter@ngtpdemo.	local N/A	ι	Skipped		Disk space limit was re	ached	
1 day ago	word	peter@ngtpdemo.local	peter@ngtpdemo.	local N/A	λ	Skipped		Disk space limit was re	ached	-

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

Most Common Failures								
# Emails	▼ F	ailure Reason						
3	D	Disk space limit was reached\n(Error code: 2D225F5D29507050322F7D2A552F4D)						
3	D	isk space limit w	as reached					
Email Failures								
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	n Disk space limit was reach		
28 minutes ago	Word document without Ma	peter@ngtpdemo.local	peter@ngtpdemo.local	N/A	Skipped	n 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 <u>sk122323</u>.

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.



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	
Filter spam based on content fingerprint • • <td>m</td>	m
This feature involves communication with an external ser	ver. For more information, refer to our privacy policy .
Rag options	
Flag subject	
Add to Spam email subject line:	[SPAM]
Add to Suspected Spam email subject line	[SUSPECTED SPAM]
Flag Header	
Security Gateway Engine settings	
Scan only the first 4096	KB of each email.
UTM-1 Edge Engine settings	
Spam confidence level: 90 🐳	
Suspected spam confidence level : 80	
Tracking options	
Spam Log	•
Suspected Spam	•
Non spam None	💌 🛞 Wide Impact

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

IP Reputation A	Anti-Spam					
Filter spam from know	 spammers Filter spam Filter suspected spam ication with an external server. For more information, refer to our privacy policy . 					
Spam confidence level:	90 A					
Suspected spam confiden	Suspected spam confidence level : 80					
Tracking options						
Spam	Log 👻					
Suspected Spam	Log					
Non spam	None 🔹 🚺 Wide Impact					

Recommended SecureKnowledge articles for further studies

Mail Transfer Agent – Advanced Technical Reference Guide <u>sk109699</u>

Configure MTA for load balancing/high availability skiintencommutation.org

ThreatEmulation – Advanced Technical Reference Guide <u>sk114806</u>

ThreatExtraction – Advanced Technical Reference Guide <u>sk114807</u>