

Threat Emulation/Threat Extraction

Module 5: Threat Emulation/Threat Extraction

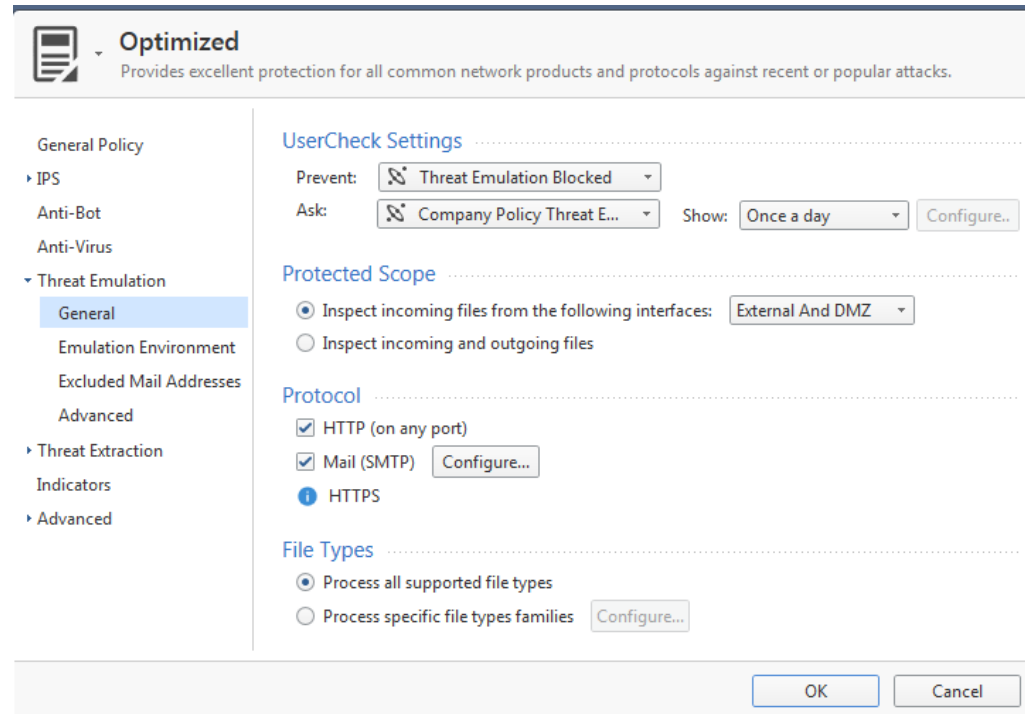
Instructor: Kim Winfield

Objectives

- Threat Emulation and the concept of Sand Boxing
- Threat Emulation as a service in the cloud and local
- Threat Extraction when Threat Emulation isn't enough

Threat Emulation

- To enable Threat Emulation General Settings




The screenshot shows the 'Optimized' settings window for Threat Emulation. The left sidebar lists various settings categories, with 'Threat Emulation' expanded and 'General' selected. The main panel displays the 'General' settings for Threat Emulation, including 'UserCheck Settings', 'Protected Scope', 'Protocol', and 'File Types'.



Optimized
Provides excellent protection for all common network products and protocols against recent or popular attacks.

General Policy

- General Policy
- IPS
- Anti-Bot
- Anti-Virus
- Threat Emulation
 - General**
 - Emulation Environment
 - Excluded Mail Addresses
 - Advanced
- Threat Extraction
- Indicators
- Advanced

UserCheck Settings

Prevent:  Threat Emulation Blocked

Ask:  Company Policy Threat E... Show: Once a day 

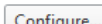
Protected Scope

☒ Inspect incoming files from the following interfaces: External And DMZ

☐ Inspect incoming and outgoing files

Protocol

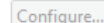
☒ HTTP (on any port)

☒ Mail (SMTP) 

☒ HTTPS

File Types

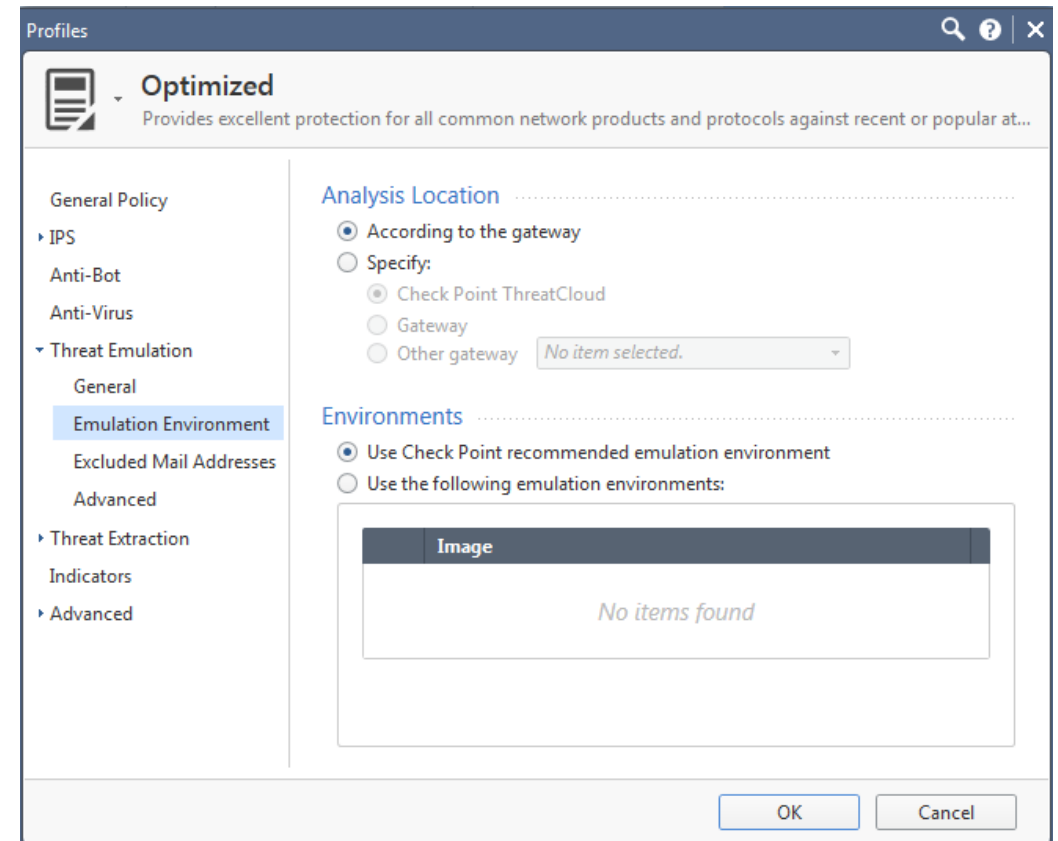
☒ Process all supported file types

☐ Process specific file types families 

OK Cancel

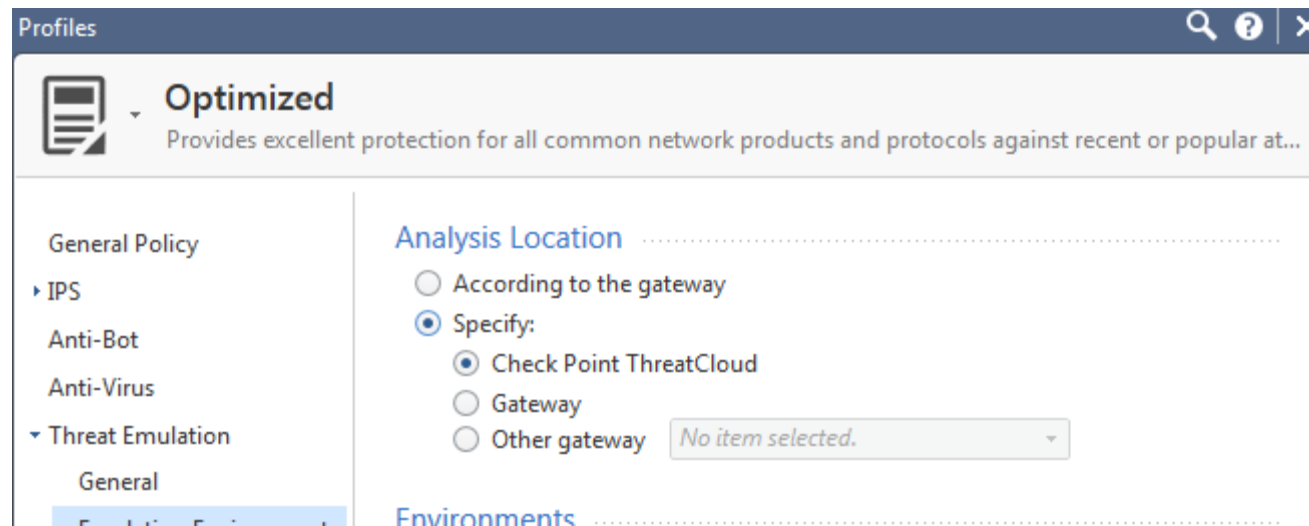
Threat Emulation Cloud and Local Implementation

- To Select Emulation Location
 - Either Local or Cloud or another Gateway
- Choose Environments
 - Windows Operating Systems



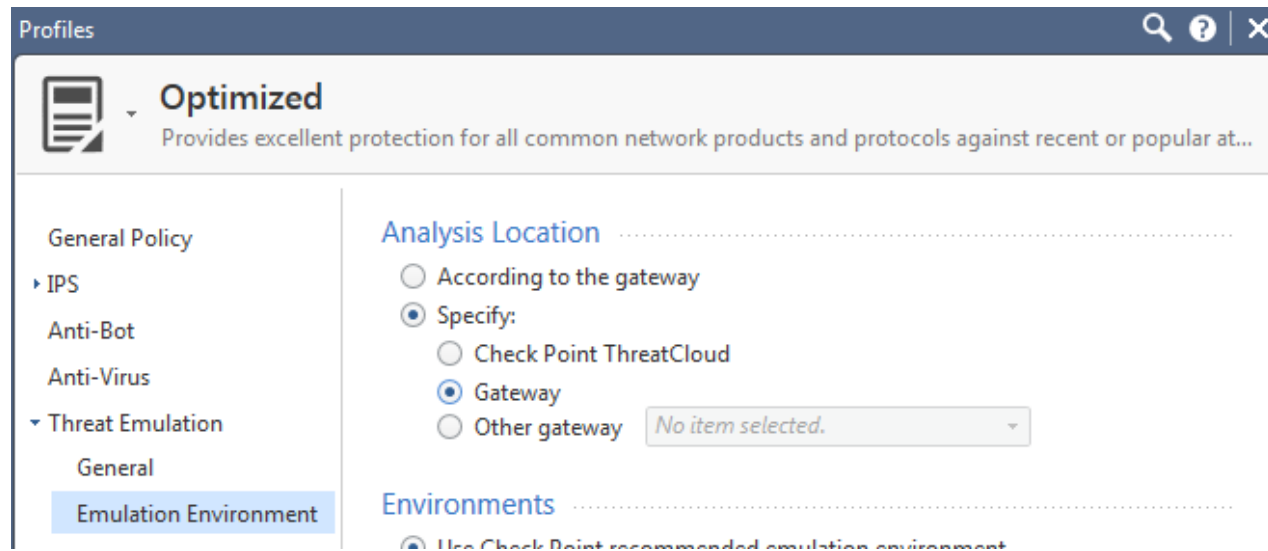
Threat Emulation

- Cloud Emulation
 - Service Contract for Threat Emulation is required
 - Internet Access from the Gateway where Cloud Emulation is enabled
 - Select Check Point Threat Cloud in SmarConsole



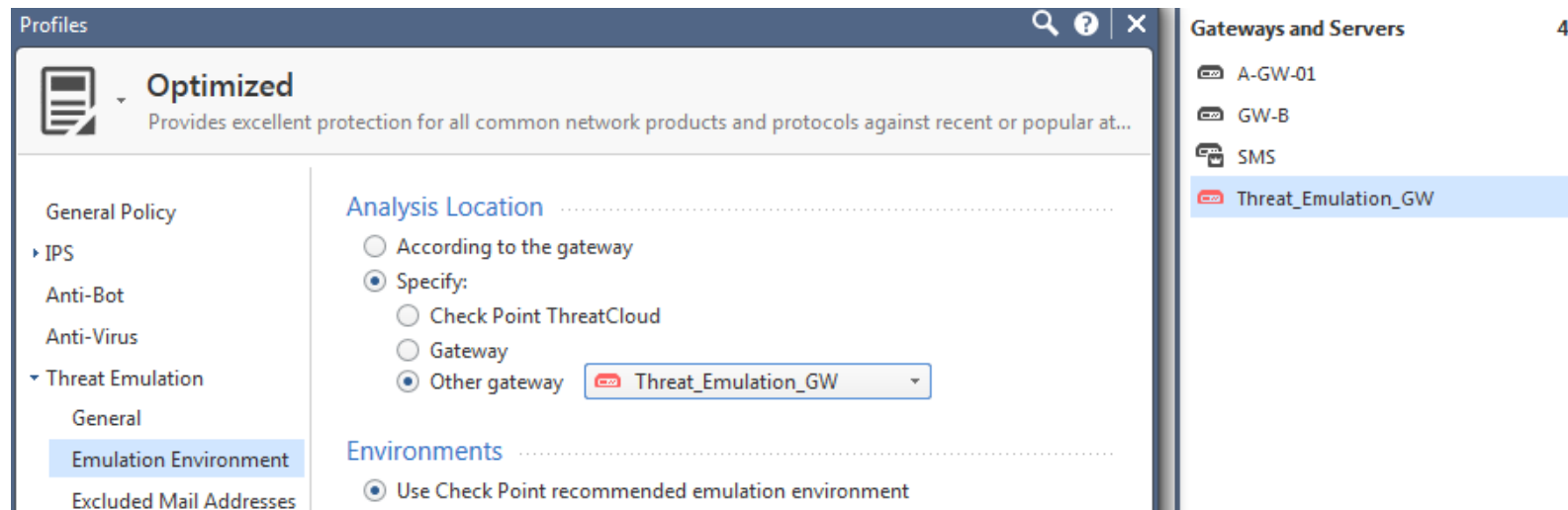
Threat Emulation

- Local Emulation
- Select This Gateway
 - Download of the Virtual Environments Selected will take several hours depending on speed of the internet connection



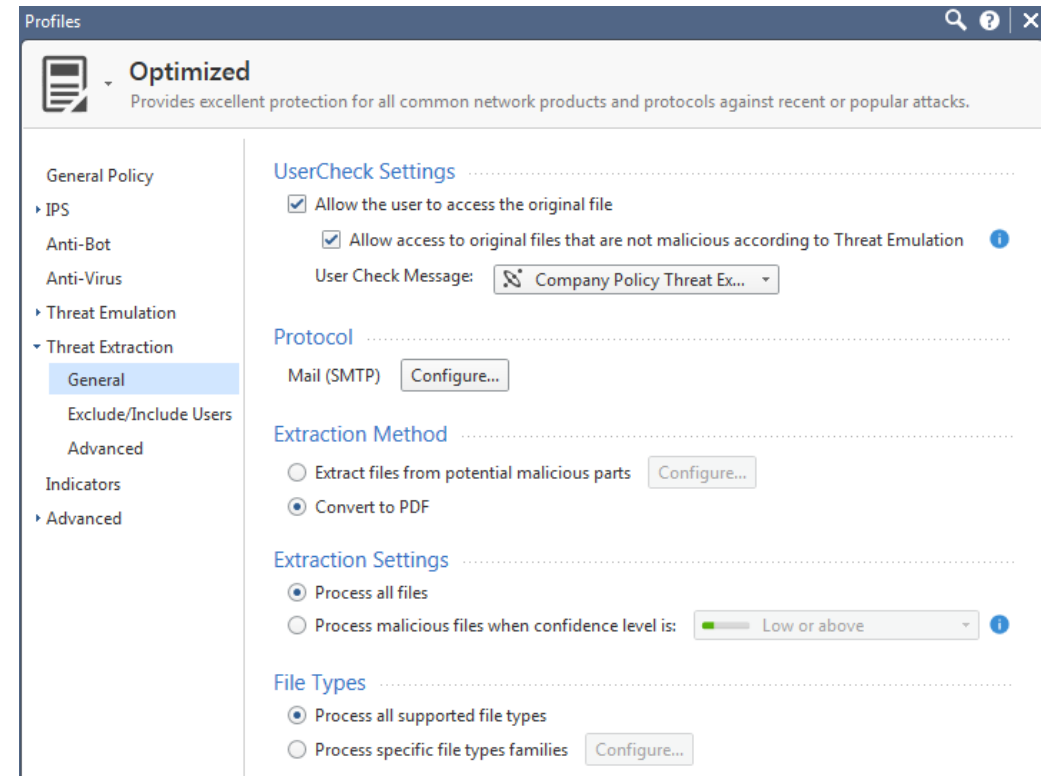
Threat Emulation

- Local Emulation
- Select This Gateway
 - Download of the Virtual Environments Selected will take several hours depending on speed of the internet connection



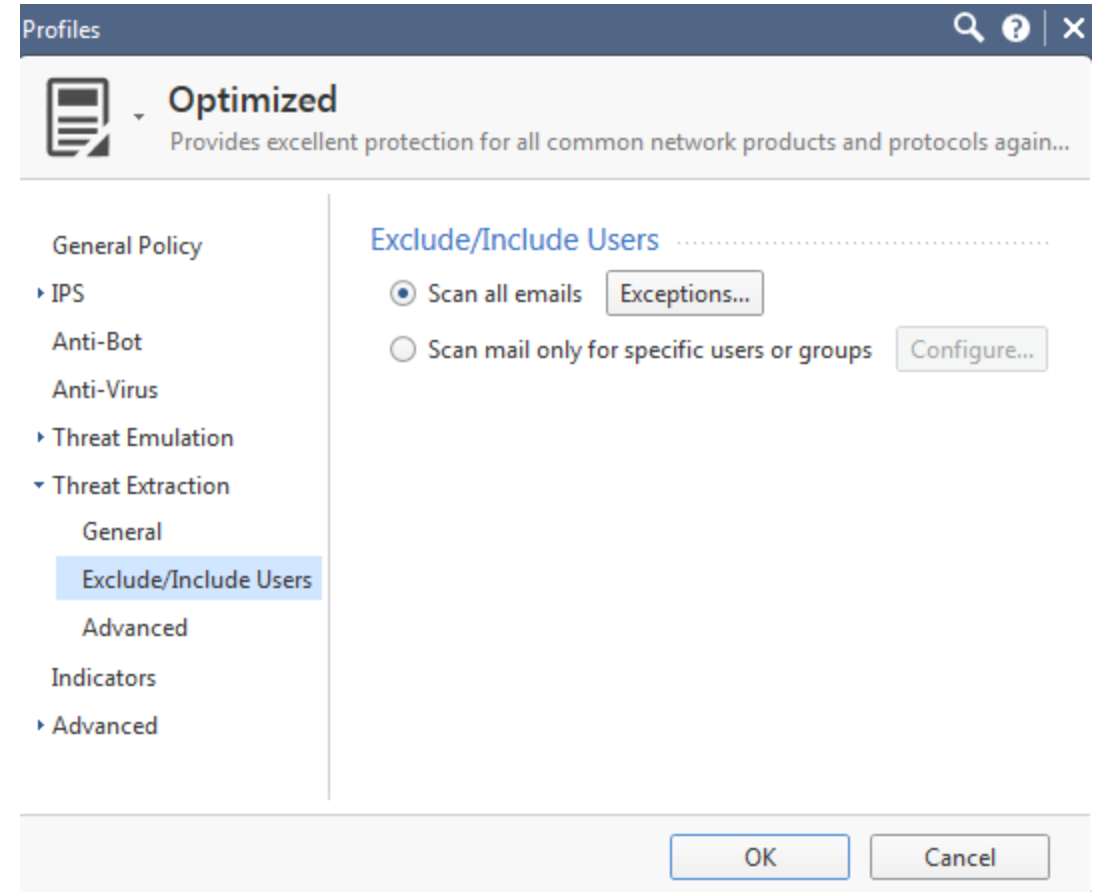
Threat Extraction

- Threat Emulation Identifies potential threats and removes them.
- Threat Extraction Identifies potential threats and cleans the document by removing the potential threat and returning a readable document to the user.



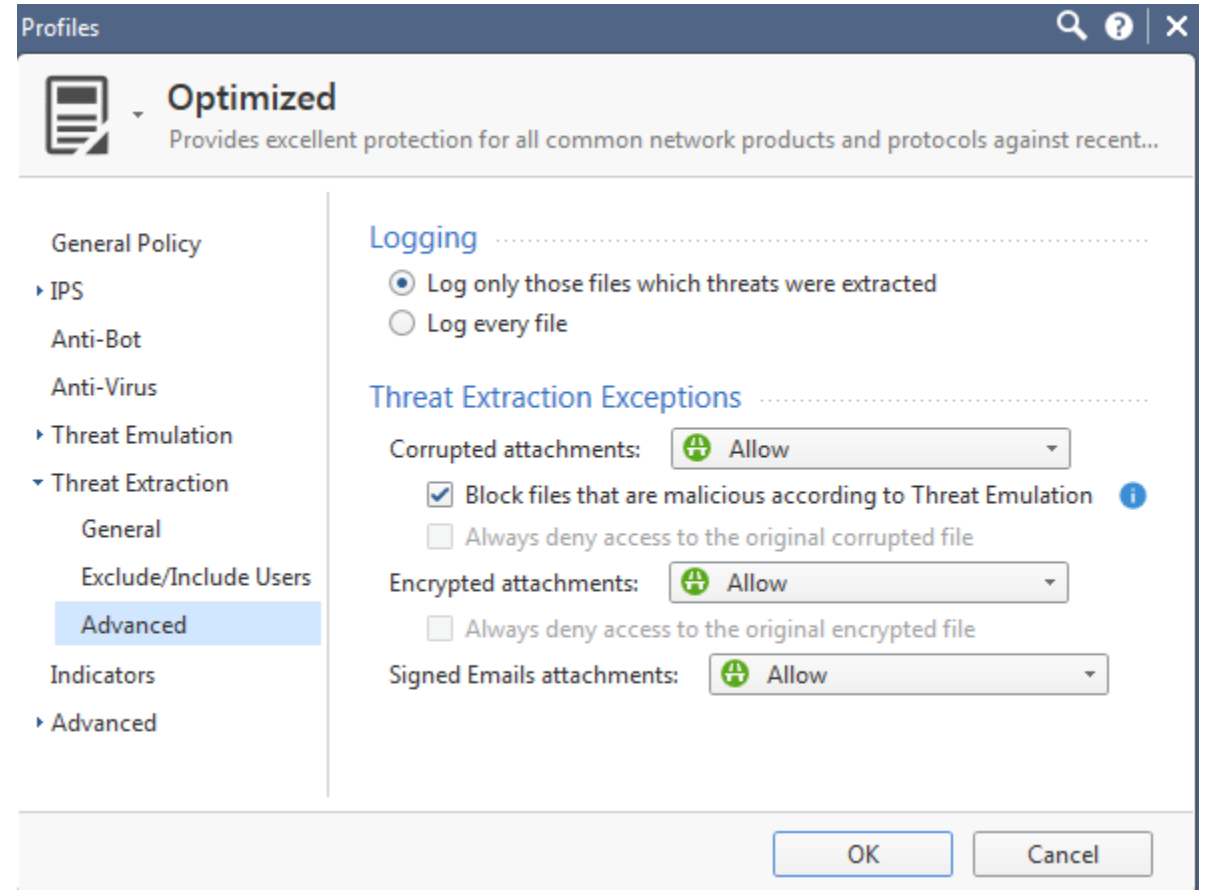
Threat Extraction

- User Inclusions and Exclusions
- All E-mail is scanned with Exceptions or
- Mail can be scanned for only specific users and groups



Threat Extraction

- Advanced Settings for Logging
 - Log only files which threats were extracted
 - Log every file
- Threat Extraction Exceptions
 - Handling of Corrupted attachments
 - Encrypted attachments
 - Signed e-mail attachments



Summary

- Used Threat Emulation to Sand Box Potential Attacks
- Configured a Cloud Implementation of Threat Emulation and learned the requirements for Local Emulation
- Used Threat Extraction to clean infected documents

Bibliography

R80.10 Threat Prevention Admin Guide California: USA