CHAPTER 8

SECURITY ELEVATION

YOU DESERVE THE BEST SECURITY

Learning Objectives

- Demonstrate an understanding of Application Control & URL Filtering and Autonomous Threat Prevention capabilities and how to configure these solutions to meet an organization's security requirements.

Application Control & URL Filtering

- Granular control of social networks
- Applications and application features
- Identify, allow, block, or limit usage

Provides application security and identify control

Controls access to millions of websites by category, users, groups, and machines

Application Control & URL Filtering Use Cases

Use Case	Solution
Learn About Applications	Use Check Point comprehensive AppWiki to understand what applications are used for and to determine risk levels.
Create a Granular Policy	Make rules to allow or block applications or Internet sites by individual application, application or URL categories, or risk levels.
Track Employees Online Usage	Based on traffic results, change policies to be more effective.
Keep Policies Updated	Application and URL Filtering Database is updated regularly with applications and site categories to help keep policies current.
Custom Applications, Sites, Categories, and Groups	Applications, websites, categories, and groups that are not in the Application and URL Filtering Database can be created for use in the Policy.

Main Features of Application Control & URL Filtering

- Granular Application Control
- Largest application library with AppWiki
- Integrated into Security Gateways
- Central Management
- SmartEvent Analysis

Application Control

- ✓Provides the industry’s strongest application security and identity control.
- ✓Lets IT teams create granular polices based on users or groups.
  - ➢Identify, block, or limit usage of Web 2.0 applications and social networking widgets.

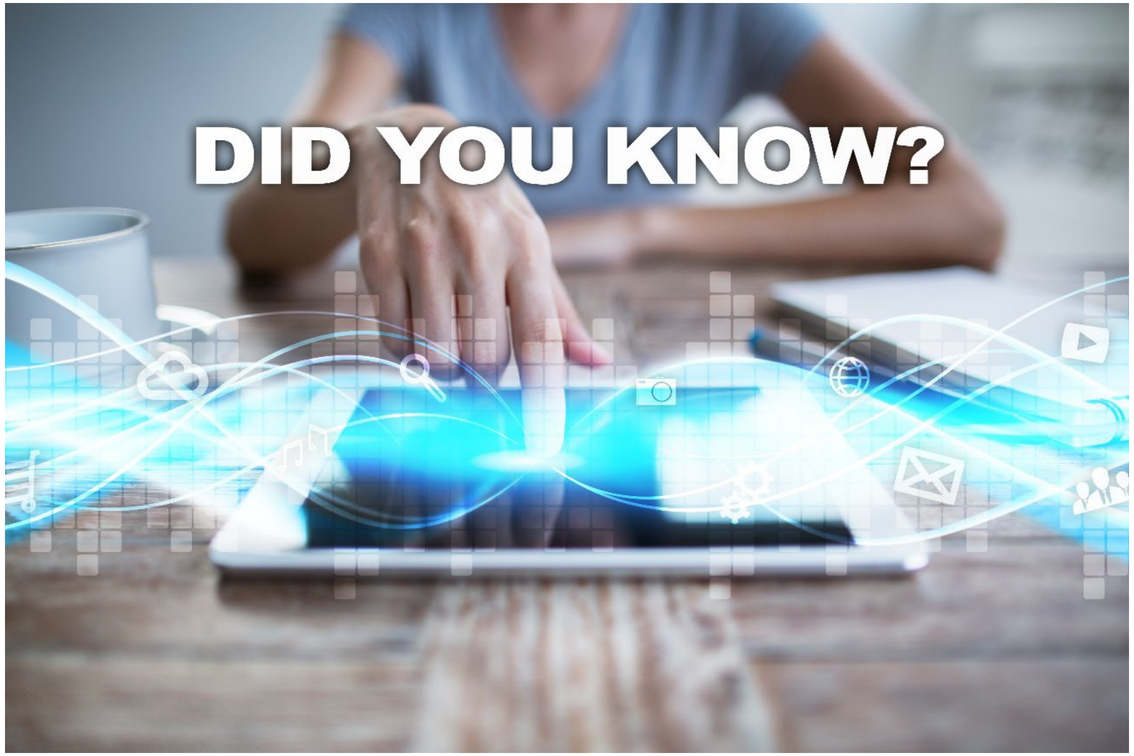
Application Control

The Check Point Secure Web Gateway solution protects an organization from online security threats and infections by enforcing company policy and filtering Internet-bound traffic.

- It is available as an on-premise or cloud-delivered network security service.

For additional information, refer to:

https://www.checkpoint.com/cyber-hub/network-security/what-issecure-web-gateway



Benefits of Application Control

- Identify and control applications in an IT environment.
- Automatically identify trusted software that has the authorization to run.
- Prevent all other unauthorized applications from executing.
- Eliminate unknown and unwanted applications.
- Reduce the risks and costs associated with malware.
- Improve overall network stability.
- Identify applications running within endpoint environment.
- Protect against exploits of unpatched OS and third-party application vulnerabilities.

Better Understanding of Data Environments with Application Control

Application Control:

- Provides knowledge about key areas of applications, web traffic, threats, and data patterns.
- Provides users a better understanding of applications or threats, behavioral characteristics, and usage.

Organizations gain knowledge about:

✓Traffic source and destination

✓Security rules and zones

URL Filtering

- URL (Uniform Resource Locator) filtering restricts the online content that individuals can access.
- Users are prevented from going to specific web sites and prohibited from using corporate resources in any way that could harmfully affect the organization.

- Controls access to millions of web sites by category, users, groups, and machines.
- Protects users from malicious sites.
- Enables safe use of the Internet.
- Educates users on Web Usage Policy in real time with UserCheck.

How URL Filtering Works

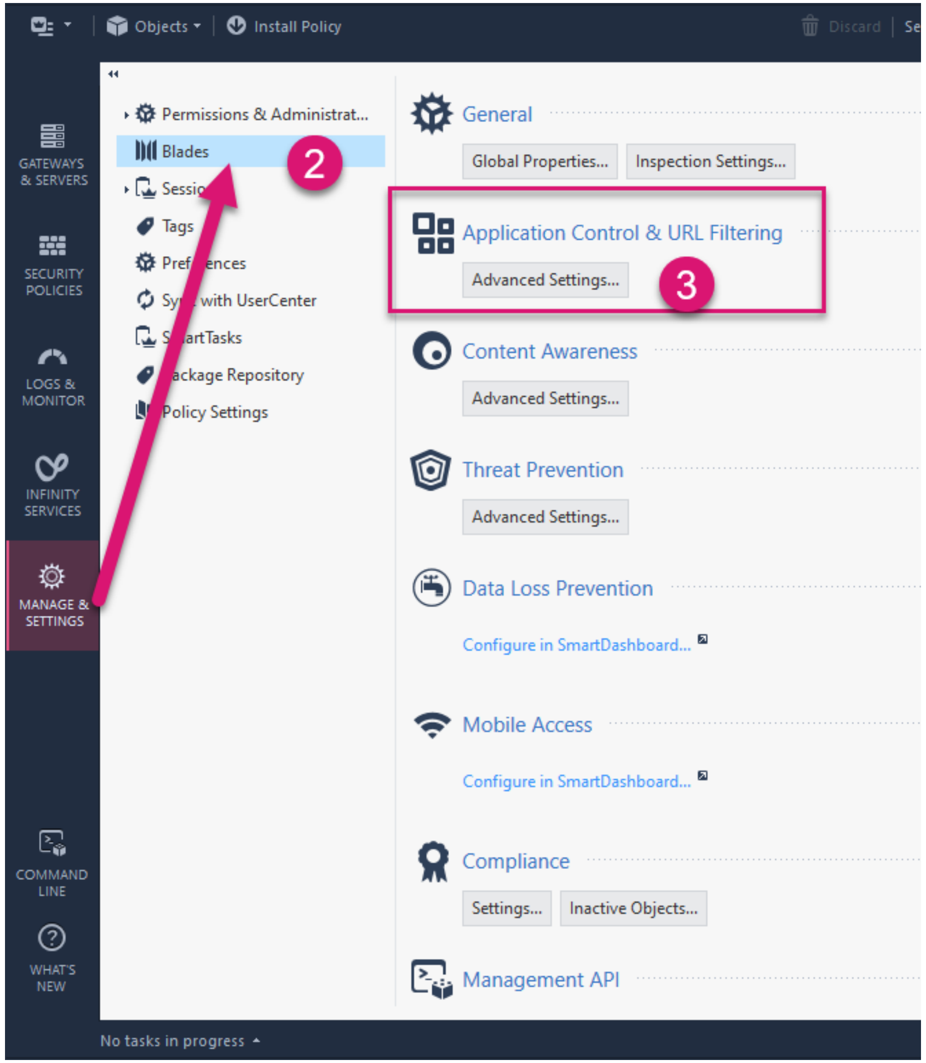
- Compares web traffic against URL filters.
- URL filter categories or groups include:
  - Blocked sites
  - Allowed sites
  - Defined IT Policies
  - Blocked or Allowed URL Filtering

Need for URL Filtering

- Control employee Internet access to inappropriate and illicit websites.
- Control bandwidth issues.
- Decrease legal liability.
- Improve organizational security.

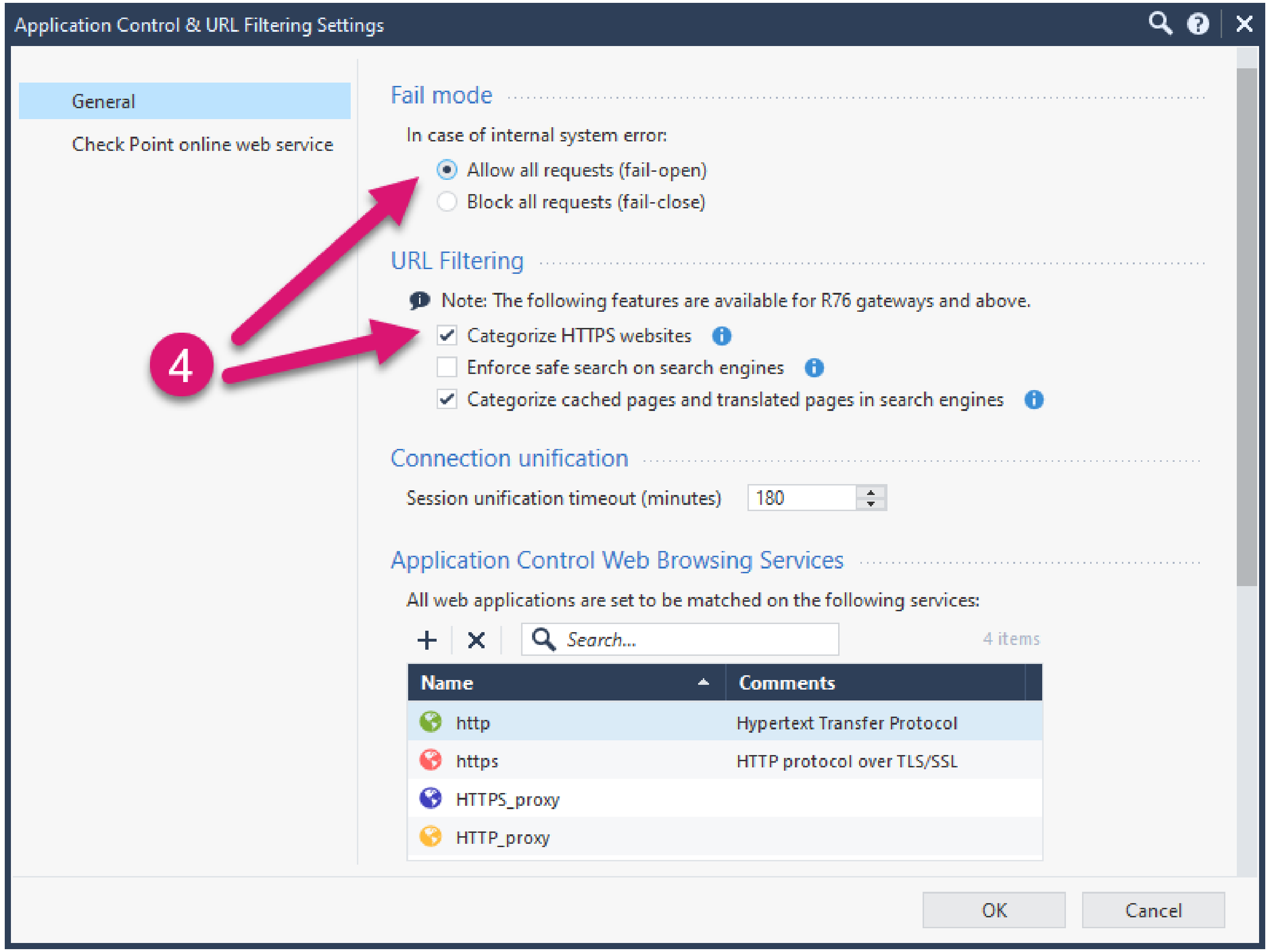
Configuring Application Control and URL Filtering

1. Connect to SmartConsole
2. From Manage & Settings, select **Blades**.
3. Under Application Control & URL Filtering, click **Advanced Settings**.



Configuring Application Control and URL Filtering (Continued)

4. From General, under Fail mode, enable **Allow all requests (fail-open)** and under URL Filtering, enable **Categorize HTTPs websites**.



Application Control & URL Filtering Settings

Fail mode

In case of internal system error:

● Allow all requests (fail-open)
○ Block all requests (fail-close)

URL Filtering

Note: The following features are available for R76 gateways and above.

☑ Categorize HTTPS websites
□ Enforce safe search on search engines
☑ Categorize cached pages and translated pages in search engines

Connection unification

Session unification timeout (minutes) 180

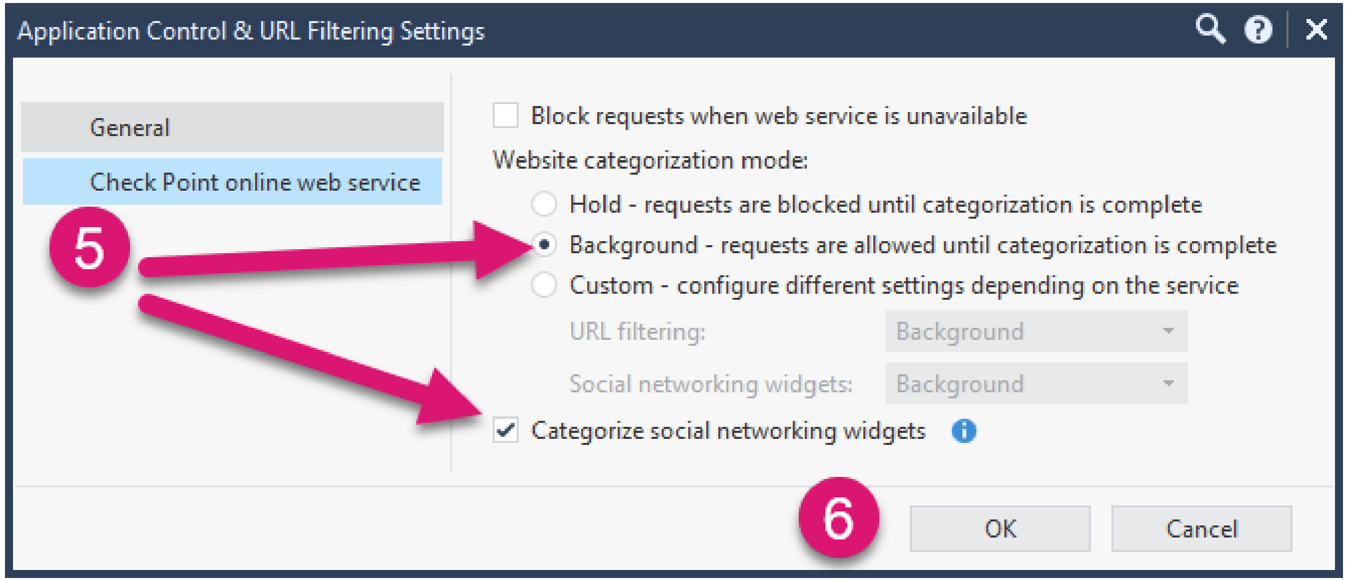
Application Control Web Browsing Services

All web applications are set to be matched on the following services:

Name	Comments
http	Hypertext Transfer Protocol
https	HTTP protocol over TLS/SSL
HTTPS_proxy	
HTTP_proxy	

Configuring Application Control and URL Filtering (Continued)

5. From Check Point online web service, select **Background** and select **Categorize social networking widgets**.
6. Click Ok.
7. Install the policy.



Application Control & URL Filtering Settings

General

Check Point online web service

□ Block requests when web service is unavailable

Website categorization mode:

○ Hold - requests are blocked until categorization is complete

● Background - requests are allowed until categorization is complete

○ Custom - configure different settings depending on the service

URL filtering: Background

Social networking widgets: Background

☑ Categorize social networking widgets

Autonomous Threat Prevention

- Provides out-of-the-box Threat Prevention, which reduces administrative overhead.

Single Click Configuration

Streamlined Configuration and Deployment

Automatic Configuration Updates

Optional Customization

The Threat Prevention configuration is always up-to-date without the need for manual labor.

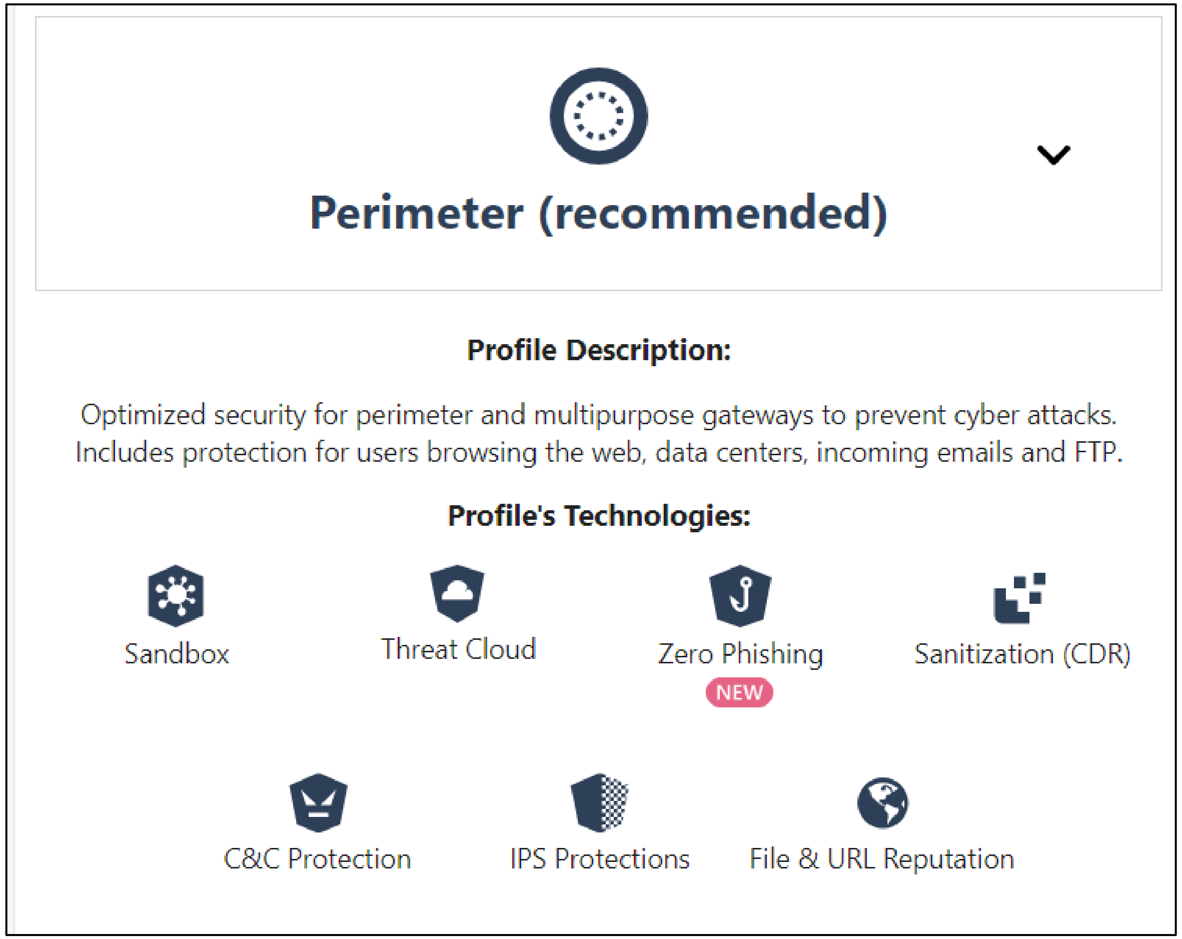
Autonomous Threat Prevention Profiles

- Recommended for Perimeter Profile (Default):
  - Provides optimized security for the perimeter Gateway and protection for users browsing the web, data centers, incoming emails, and FTP.
  - Recommended for multiple protections on the same Gateway.
  - Most like the Custom Threat Prevention Optimized profile.
- Data Center East/West Profile:
  - Optimized security to prevent cyberattacks on data centers. Includes extensive protection over servers and east–west traffic.

Autonomous Threat Prevention Profiles (Continued)

- Internal Network Profile:
  - Provides maximum security to prevent cyberattacks over internal traffic between internal users and internal servers.
- Strict Security for Perimeter Profile:
  - Provides maximum security to prevent cyberattacks over internal traffic between internal users and internal servers.
- Recommended for Guest Network Profile:
  - Detect mode profile to monitor cyberattacks attempts through a guest network (Wi-Fi) non-intrusively.

Technologies Used by Autonomous Threat Prevention Profiles



Perimeter (recommended)

Profile Description:

Optimized security for perimeter and multipurpose gateways to prevent cyber attacks. Includes protection for users browsing the web, data centers, incoming emails and FTP.

Profile's Technologies:

Each Autonomous Threat Prevention profile consists of a wide range of industry-leading protections, as shown in the figure.

Technologies Used by Each Profile

Autonomous Profile	Description
Sandbox	Prevents unknown, zero-day and advanced polymorphic attacks by executing suspicious files in evasion-resistant sandbox and applying advanced AI techniques. It is used in all Autonomous Threat Prevention profiles.
ThreatCloud	ThreatCloud is cloud-based real-time global threat intelligence using Check Point worldwide network of threat sensors. It is used in all Autonomous Threat Prevention profiles.

Technologies Used by Each Profile (Continued)

Autonomous Profile	Description
Zero Phishing (R81.20 and higher)	Prevents unknown zero-day and known phishing attacks on websites in real-time, by utilizing industry-leading, Machine-Learning algorithms and patented inspection technologies. URL-based Zero Phishing is used in the Recommended for Perimeter and Strict Security for Perimeter profiles. In-browser Zero Phishing is not used in any profile.

Technologies Used by Each Profile (Continued)

Autonomous Profile	Description
Sanitization (CDR)	Provides proactive prevention of unknown attacks from day zero, by sanitizing incoming files before delivering them to users. It is used in the following Autonomous Threat Prevention profiles: • Recommended for Perimeter profile • Strict Security for Perimeter profile
C&C Protection	Detects infected and compromised devices on the network. It blocks attacks and prevents damage by blocking malware C&C communications. It is used in all Autonomous Threat Prevention profiles.

Technologies Used by Each Profile (Continued)

Autonomous Profile	Description
IPS Protections	Implements advanced protections from network-based attacks and protects all IT systems, including servers, endpoints, industrial systems, and IoT. It is used in all Autonomous Threat Prevention profiles.
File & URL Reputation	Examines files and URLs through the ThreatCloud repository for reputation. It is used in all Autonomous Threat Prevention profiles.

Customized Profiles

Autonomous Threat Prevention profiles can also be customized for an organization’s specific needs using exceptions and advanced settings to mold policies in accordance with the requirements of a company's network environment.

Monitoring Threat Prevention

- Log Sessions - Consolidated logs based on sessions.
- Packet Captures - Greater insight into traffic that generated the log
- Advanced Forensic Details - Additional fields that hold information that can be used for advanced forensic analysis of the traffic that triggered a protection.

Log Sessions

To manage log volume, Threat Prevention logs are consolidated based on sessions.

- This is the default.
- Session starts when a user first accesses an application or site.

During a session:

- Gateway records one log for each application or site accessed by the user.
- All user activity included in the log.

View the **Suppressed Logs field** to determine the number of connections made during the session.

Packet Captures

- With the packet capture feature activated,
  - ➢The Security Gateway sends a packet capture file with the log to the Log Server.
  - ➢Packet captures can be opened from the log or saved for later review.

Advanced Forensic Details

Support the following protocols:

- DNS
- FTP
- HTTP
- HTTPS
- SMTP

Review Questions

1. List at least two use cases for Application Control.

2. How does URL filtering work?

3. What is the recommended profile supported by Autonomous Threat Prevention?

Lab 8A

Integrating Security with a Unified Policy

Lab 8B

Elevating Security with Autonomous Threat Prevention