In this lesson, you will learn how to use FortiGate to protect your network against intrusions and how to monitor and control network applications that may use standard or non-standard protocols and ports—beyond simply blocking or allowing a protocol, port number, or IP address.

Objectives

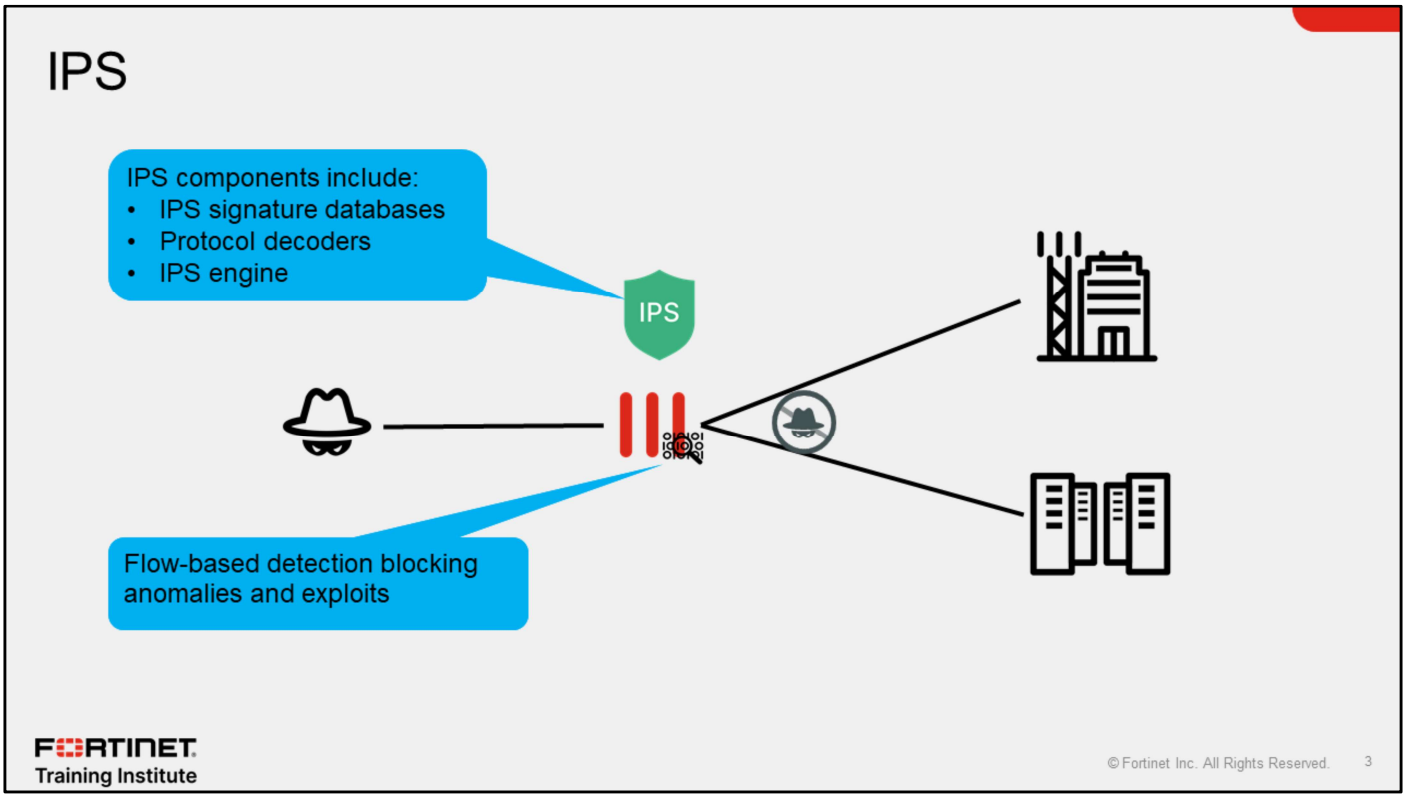
- Configure an intrusion prevention system (IPS) sensor
- Troubleshoot IPS high-CPU usage
- Configure application control in profile mode
- Monitor application control events
- Troubleshoot traffic matching with application control profile issues

FORTINET Training Institute

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in intrusion prevention systems (IPS), you will be able to implement an effective IPS solution to protect your network from intrusion.

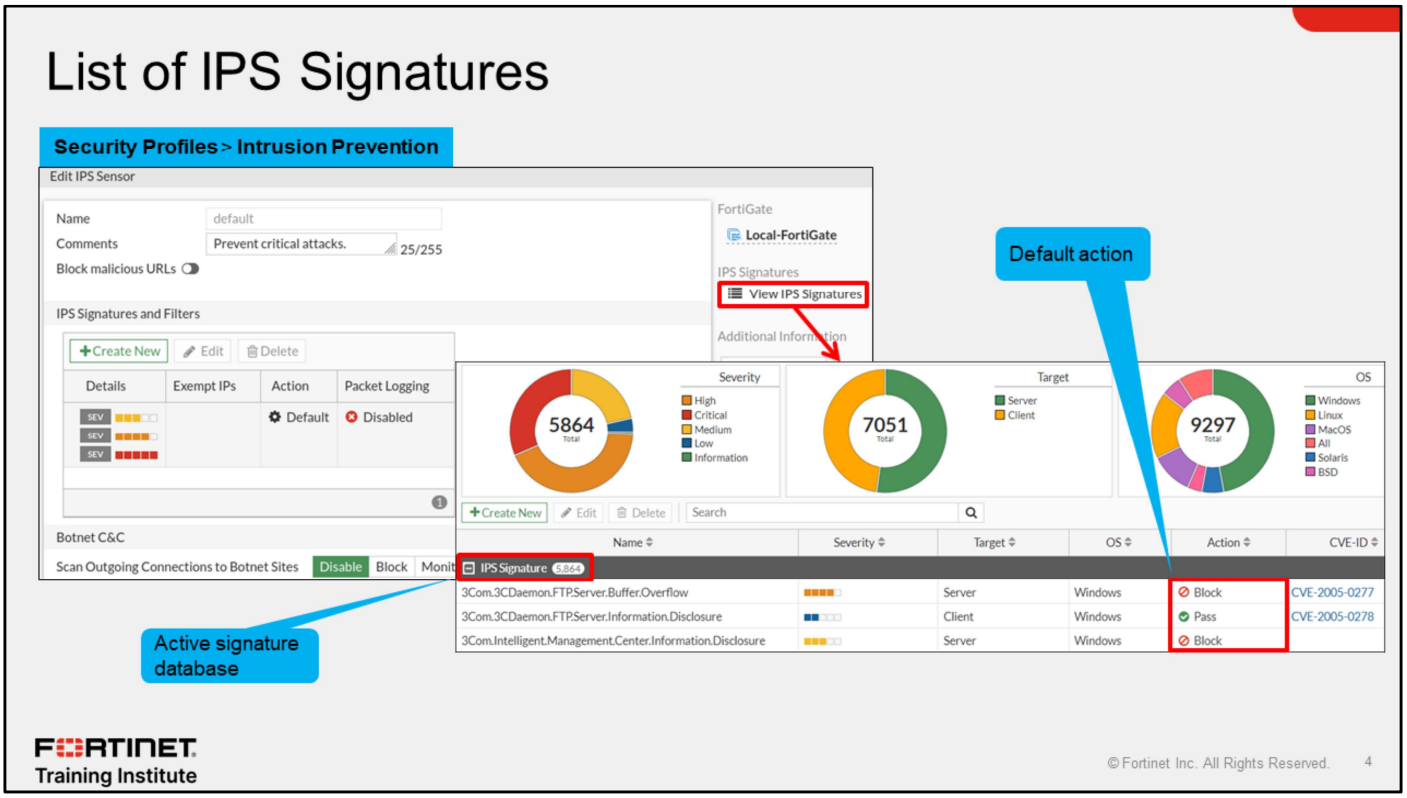
By demonstrating competence in configuring and monitoring the application control features that are available on FortiOS, you will be able to use and maintain application control in profile mode in an effective manner.



IPS on FortiGate uses signature databases to detect known attacks, like exploits. Rate-based IPS signatures also allows you to detect anomalies, which are unusual behaviors in the network, such as higher-than-usual CPU use or network traffic. Rate-based IPS signatures are part of behavioral analysis, like DoS policies and protocol constraints inspection, which detect and monitor (and, in some cases, block or mitigate) anomalies, because they reveal the symptoms of a new, never-previously-seen attack.

Unlike proxy-based scans, IPS works in flow-based inspection and is not limited to IANA standard ports. Protocol decoders parse each packet according to the protocol specifications. If the traffic doesn't conform to the specification—if, for example, it sends malformed or invalid commands to your servers—then the protocol decoder detects the error.

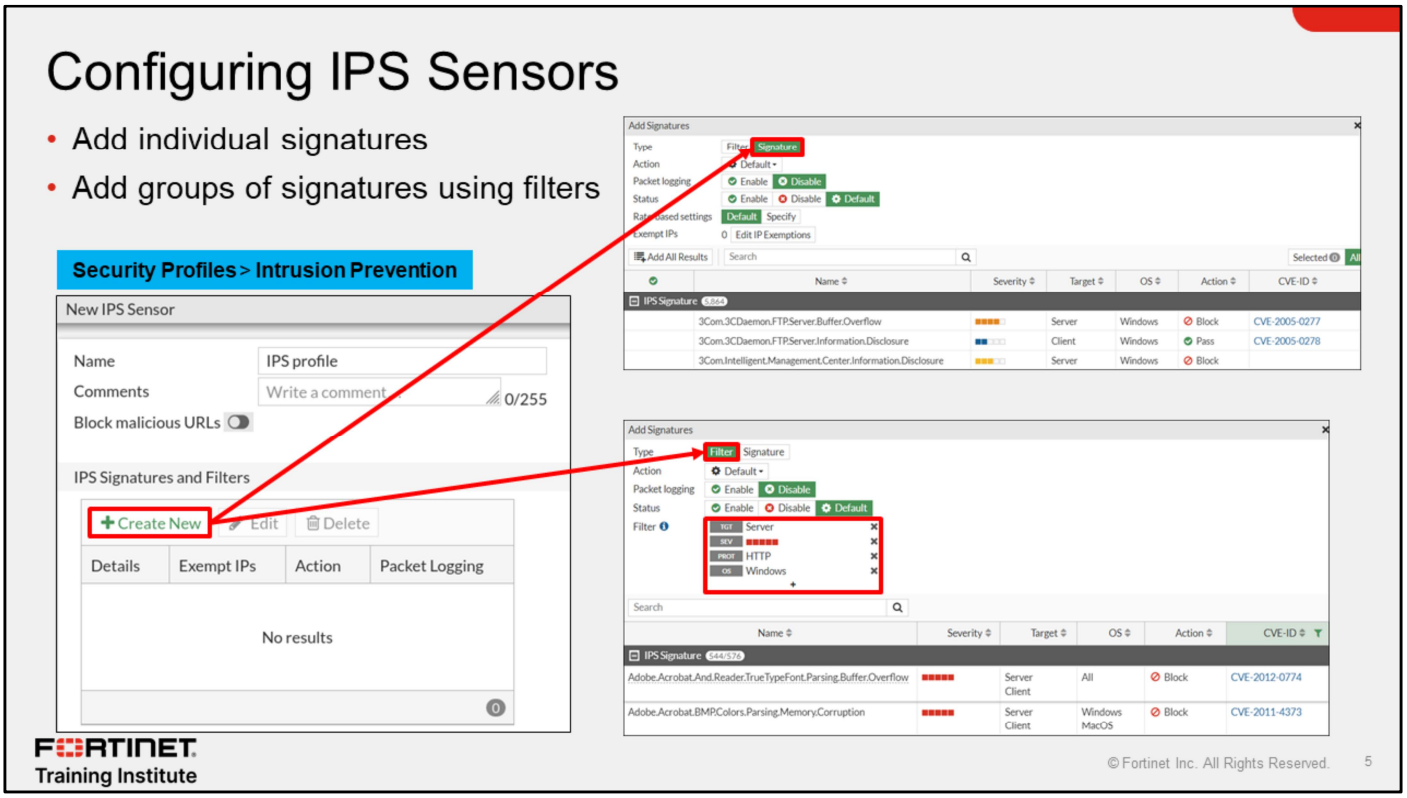
Another important IPS component is the engine. The IPS engine is responsible for IPS and protocol decoders, in addition to application control, flow-based antivirus protection, web filtering, and email filtering.



After FortiGate downloads a FortiGuard IPS package, new signatures appear in the signature list. When configuring FortiGate, you can change the **Action** setting for each sensor that uses a signature.

The default action setting is often correct, except in the following cases:

- Your software vendor releases a security patch. Continuing to scan for exploits wastes FortiGate resources.
- Your network has a custom application with traffic that inadvertently triggers an IPS signature. You can change the action setting until you notify Fortinet so that the FortiGuard team can modify the signature to avoid false positives.



There are two ways to add predefined signatures to an IPS sensor. One way is to select the signatures individually. After selecting a signature in the list, the signature is added to the sensor with its default action.

The second way to add a signature to a sensor is using filters. FortiGate adds all the signatures that match the filters.

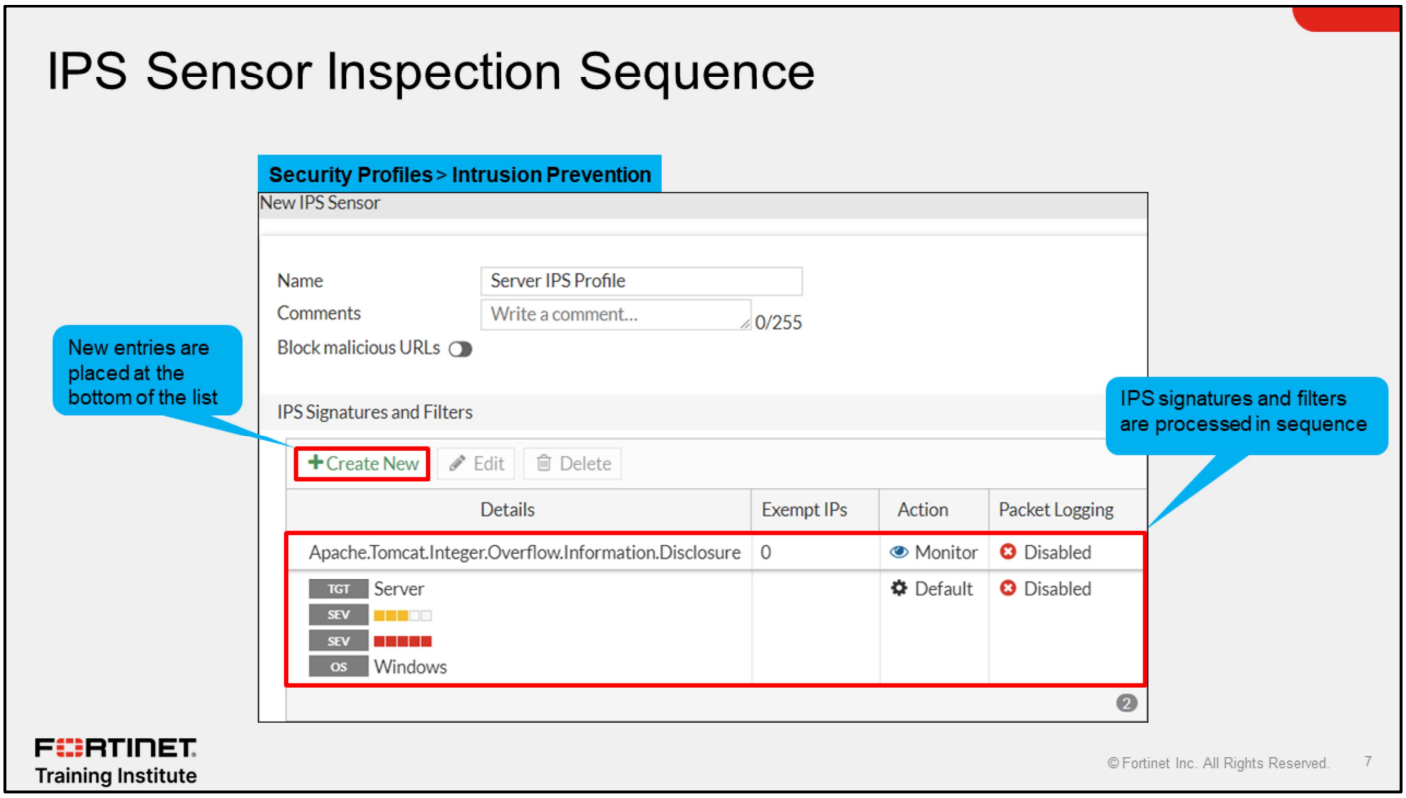
The purpose of the IPS feature is to protect the inside of the network from outside threats.

Configuring IPS Sensors—Rate-Based Signatures

- Add rate-based signatures to block traffic when the threshold is exceeded during a time period

FORTINET Training Institute

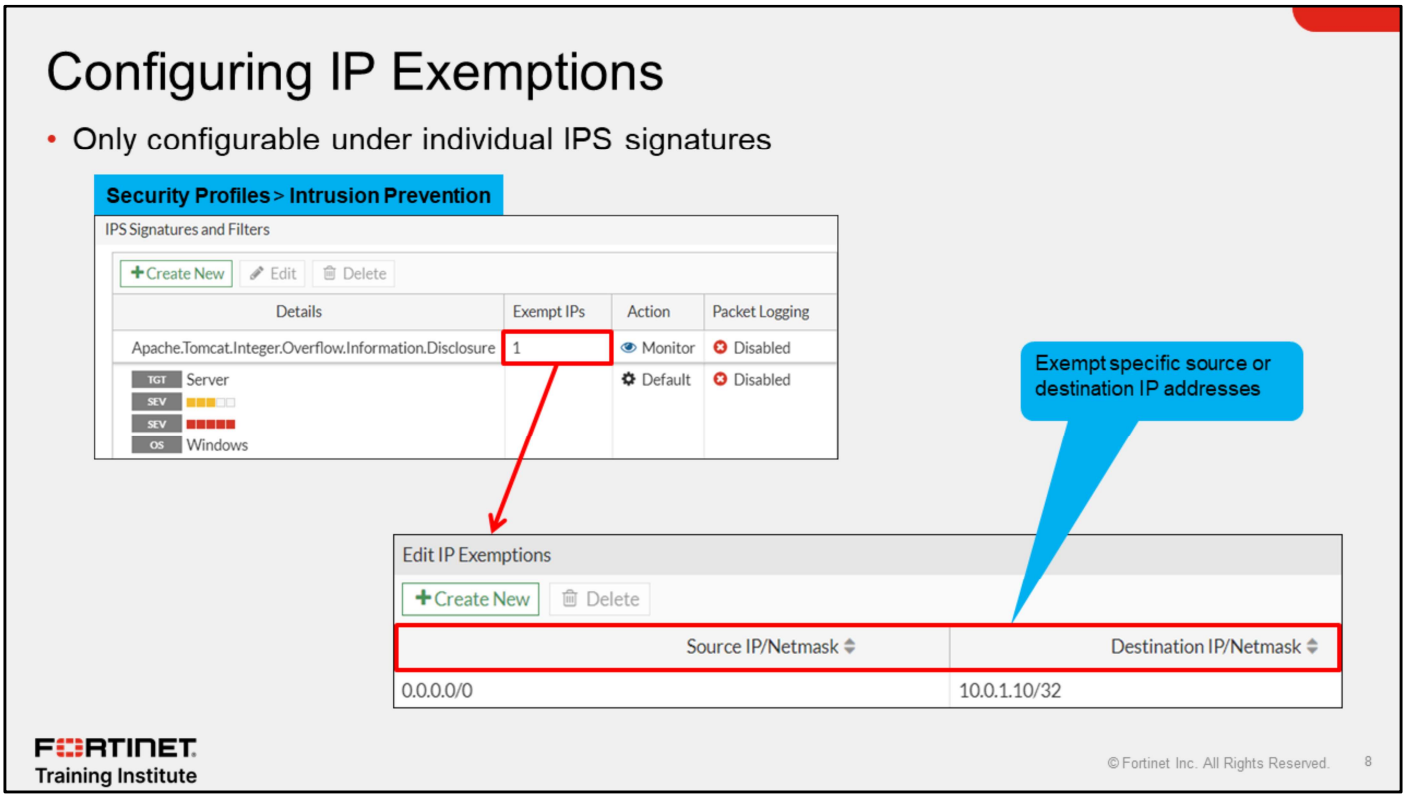
You can also add rate-based signatures to block specific traffic when the threshold is exceeded. On the CLI, If you set the command `rate-mode` to `periodical`, FortiGate triggers the action when the threshold is reached during the configured **Duration** time period. You should apply rate-based signatures only to protocols you use. This saves system resources and can discourage a repeat attack. FortiGate does not track statistics for that client while it is temporarily blocklisted.



When the IPS engine compares traffic with the signatures in each filter, order matters. The rules are similar to firewall policy matching; the engine evaluates the filters and signatures at the top of the list first, and applies the first match. The engine skips subsequent filters.

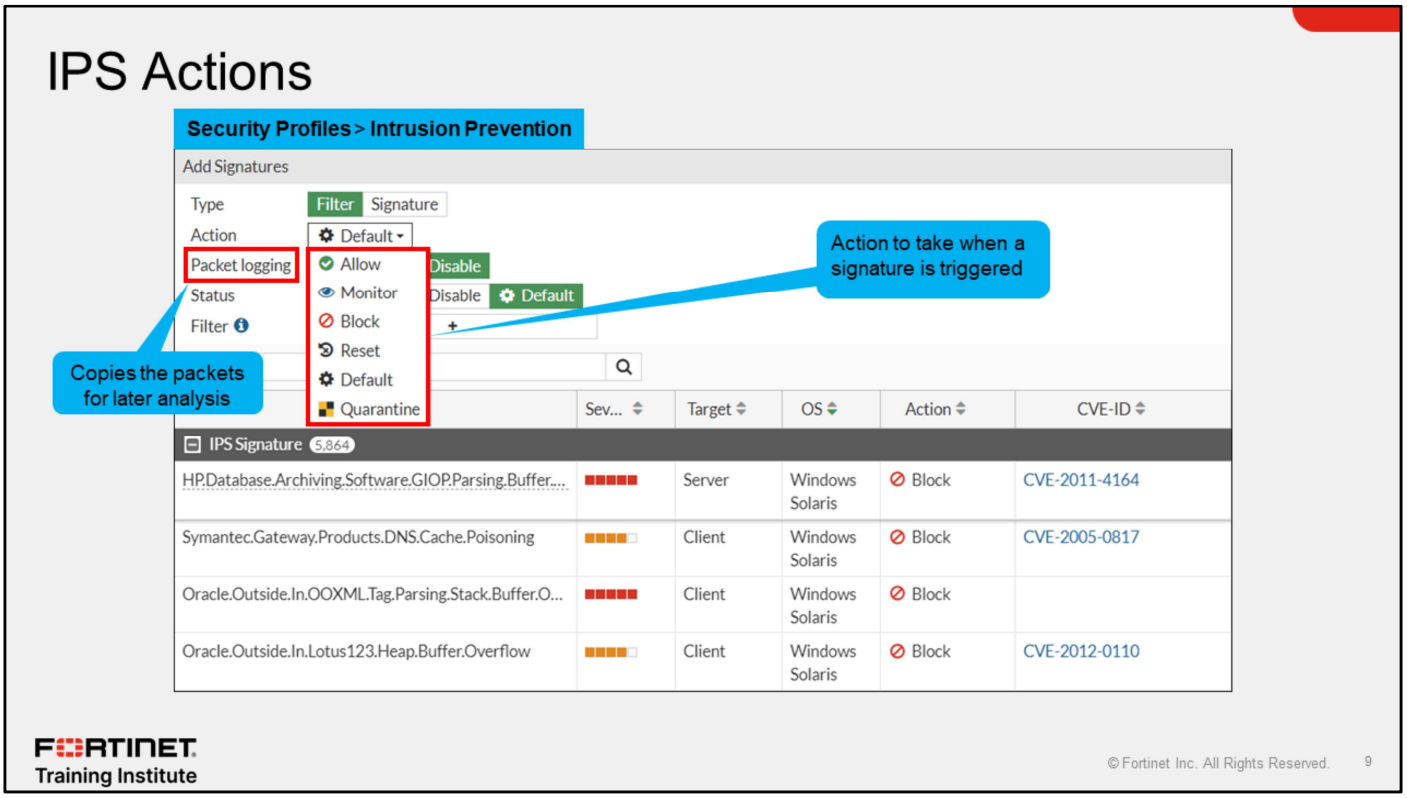
So, position the most likely matching filters, or signatures, at the top of the list. Avoid making too many filters, because this increases evaluations and CPU usage. Also, avoid making very large signature groups in each filter, which increase RAM use.

In the event of a false-positive outbreak, you can add the triggered signature as an individual signature, and then set the action to **Monitor**. This allows you to monitor the signature events using IPS logs, while investigating the false-positive issue.



Sometimes, it is necessary to exempt specific source or destination IP addresses from specific signatures. This feature is useful during false-positive outbreaks. You can temporarily bypass affected endpoints until you investigate and correct the false-positive issue.

You can configure IP exemptions on individual signatures only. Each signature can have multiple exemptions.



When you create a new entry to add signatures or filters, you can select the action by clicking **Action.**

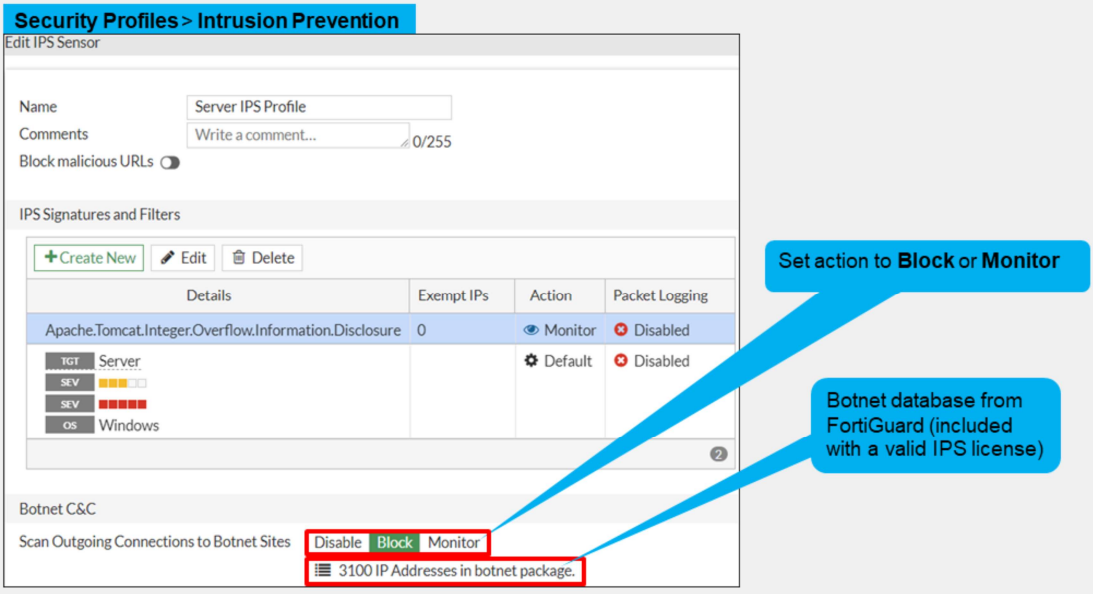
Select **Allow** to allow traffic to continue to its destination. Select **Monitor** to allow traffic to continue to its destination and log the activity. Select **Block** to silently drop traffic matching any of the signatures included in the entry. Select **Reset** to generate a TCP RST packet whenever the signature is triggered. Select **Default** to use the default action of the signatures.

Quarantine allows you to quarantine the attacker's IP address for a set duration. You can set the quarantine duration to any number of days, hours, or minutes.

If you enable **Packet logging**, FortiGate saves a copy of the packet that matches the signature.

You can set these actions on hold for new FortiGuard IPS signature by enabling the `override-signature-hold-by-id` CLI command. During the time defined by the CLI command `signature-hold-time`, the action is then set to **Monitor** to avoid false positives, with a log created including the message '`signature is on hold`'.

Enabling Botnet Protection

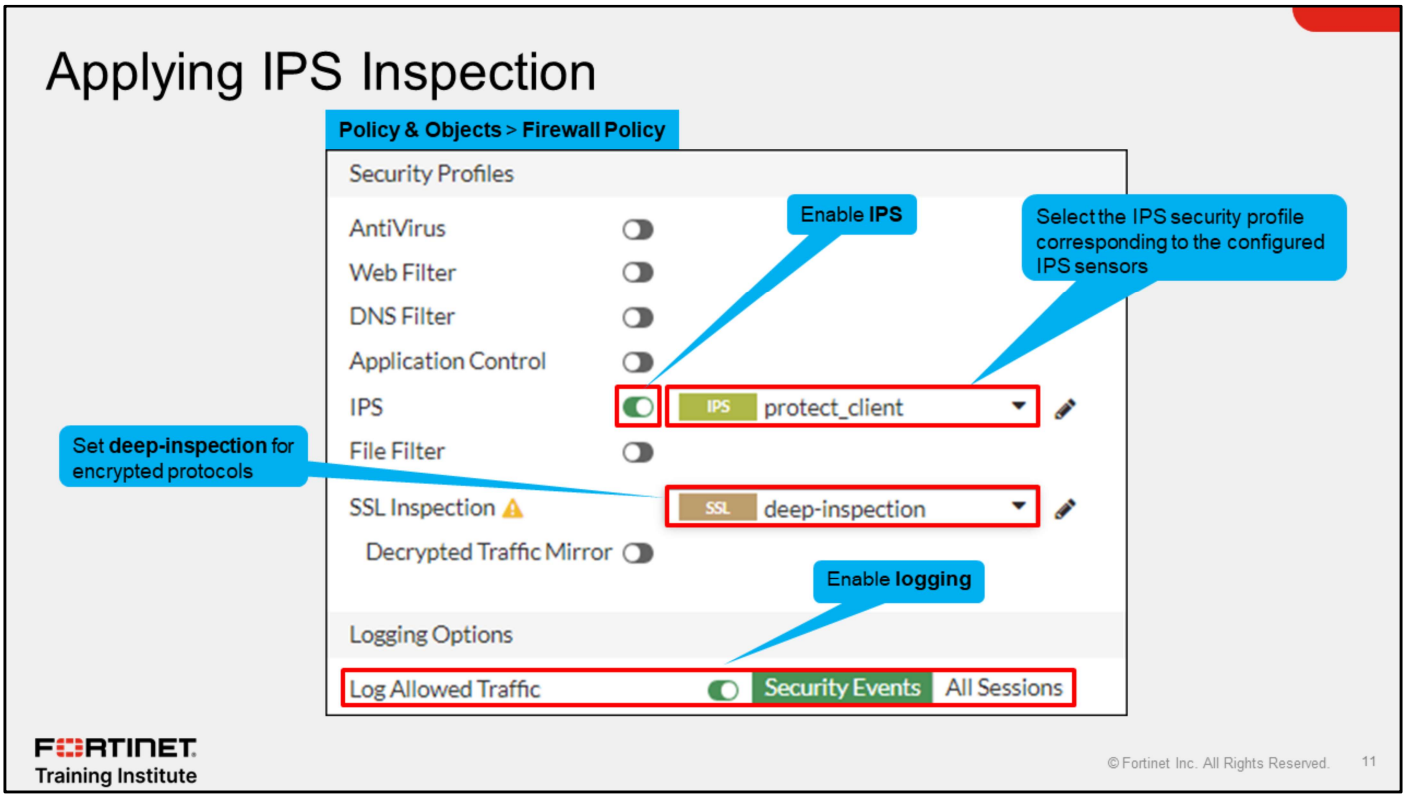


FORTINET Training Institute

For consolidated botnet protection, you can enable botnet scanning on the IPS profile that you apply the firewall policy on.

There are three possible actions for **Botnet and C&C**:

- **Disable**: Do not scan connections to botnet servers
- **Block**: Block connections to botnet servers
- **Monitor**: Log connections to botnet servers

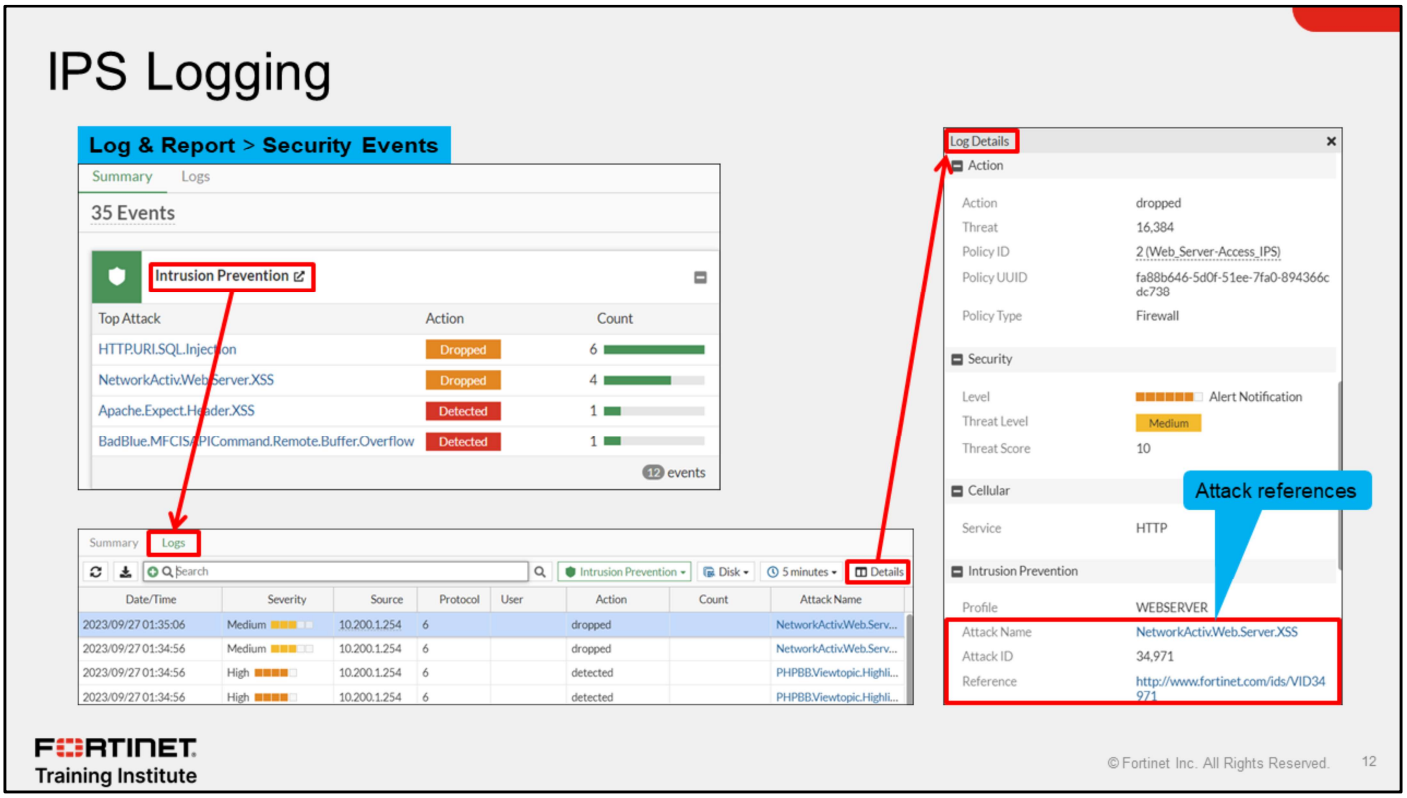


To apply an IPS sensor, you must enable **IPS** and then select the sensor in a firewall policy.

Certain vulnerabilities apply only to encrypted connections and FortiGate can't identify the threat reliably if it can't parse the payload. For this reason, you must use an SSL inspection profile, usually **deep-inspection**, if you want to get the maximum benefit from your IPS features.

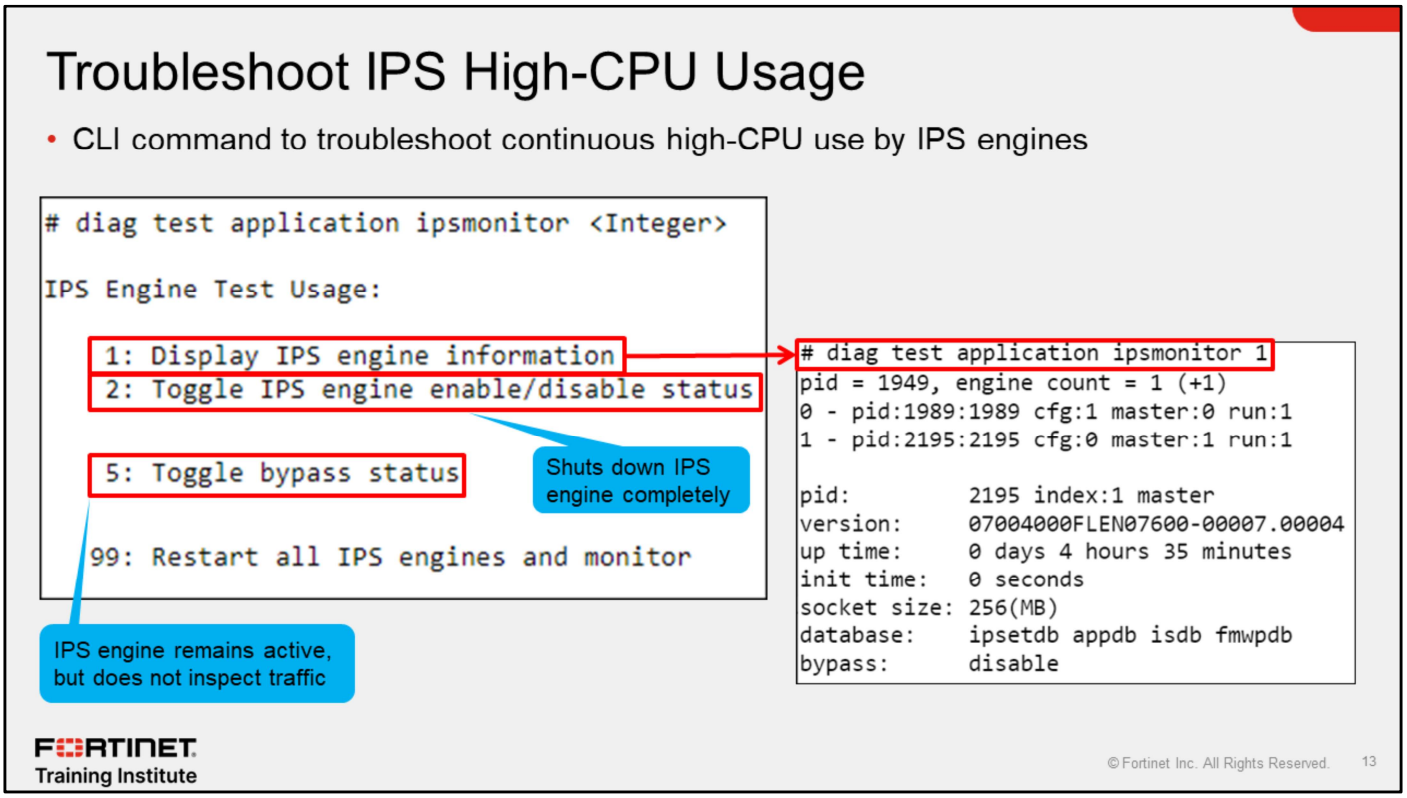
By default, FortiGate logs all security events. This means you can see any traffic that is being blocked or monitored by IPS.

If you think some traffic should be blocked but is passing through the policy, you should change the **Log Allowed Traffic** method to **All Sessions**. This logs all traffic processed by that firewall policy, and not just the traffic that is blocked or monitored by the security profiles. This can help you in identifying false negative events.



If you enabled security events logging in the firewall policies that apply IPS, the logs are available on the **Security Events** pane on the **Log & Report** page. You can view the logs by clicking on **Intrusion Prevention**.

You should review IPS logs frequently. The logs are an important source of information about the kinds of attacks that are being targeted at your network. This helps you develop action plans and focus on specific events, for example, patching a critical vulnerability.



While using IPS, short spikes in CPU usage by IPS processes can be caused by firewall policy or profile changes. These spikes are usually normal. Spikes might happen when FortiGate has hundreds of policies and profiles, or many virtual domains. Continuous high-CPU use by the IPS engines is not normal, and you should investigate it. You can use the command shown on this slide, along with displayed options, to troubleshoot these issues.

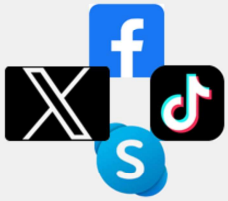
If there are high-CPU use problems caused by the IPS, you can use the `diagnose test application ipsmonitor` command with option `5` to isolate where the problem might be. Option `5` enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

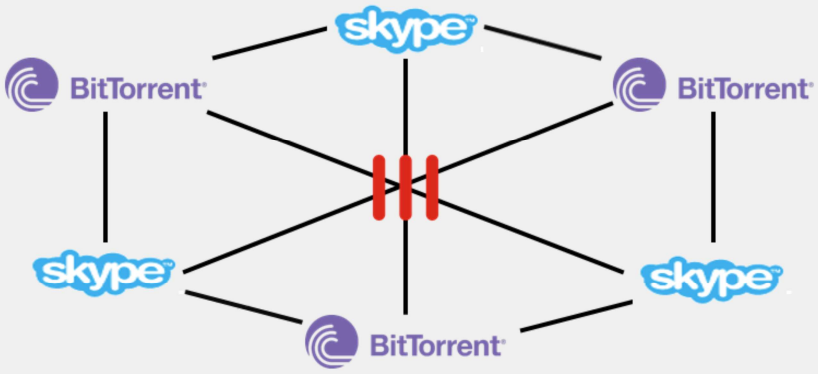
If the CPU use remains high after enabling IPS bypass mode, it usually indicates a problem in the IPS engine, which you must report to Fortinet support. You can disable the IPS engine completely using option `2`. If you want to restore IPS inspection of traffic after you finish troubleshooting, use option `2` again. At any time, you can check the status of the IPS engines using option `1`.

Another recommendation to keep in mind is that if you need to restart the IPS, use option `99`, as the slide shows. This guarantees that all the IPS-related processes restart correctly.

Application Control

- Uses the IPS engine in flow-based scan
- Detects and acts on network application traffic
- Appropriate for detecting peer-to-peer (P2P) applications





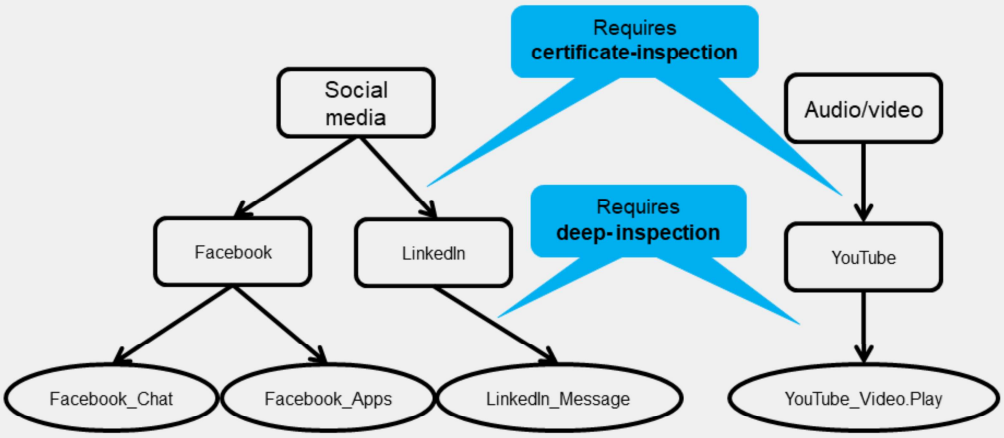
FORTINET Training Institute

As previously mentioned, the IPS engine is also responsible for application control. You can configure application control in proxy-based and flow-based firewall policies. However, because application control uses the IPS engine, which uses flow-based inspection, the inspection is always flow-based.

Application control identifies applications, such as Google Talk, by matching known patterns to the application transmission patterns. Therefore, an application can be accurately identified, only if its transmission pattern is unique. However, not every application behaves in a unique way. Many applications reuse pre-existing, standard protocols and communication methods. For example, many video games, such as *World of Warcraft,* use the BitTorrent protocol to distribute game patches. Still, with the help of the IPS engine, application control analyzes network traffic and detects application traffic, even if the application is using standard or non-standard protocols and ports. It doesn't operate using built-in protocol states. As a consequence, application control is better suited for detecting P2P protocols, because they use port randomization, pinholes, and changing encryption pattern techniques.

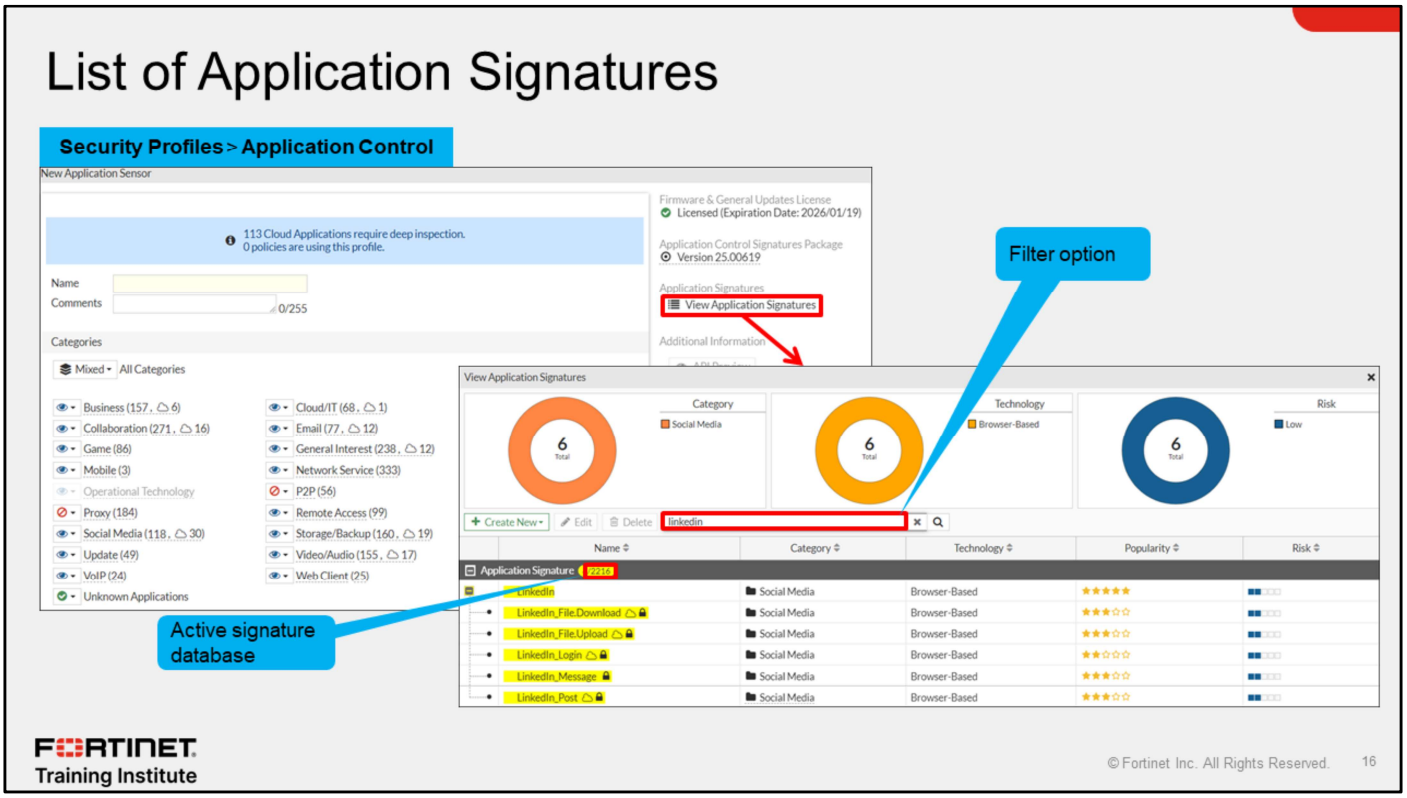
Application Control—Hierarchical Structure

- Application control signatures are organized in a hierarchical structure
  - The parent signature takes precedence over the child signature



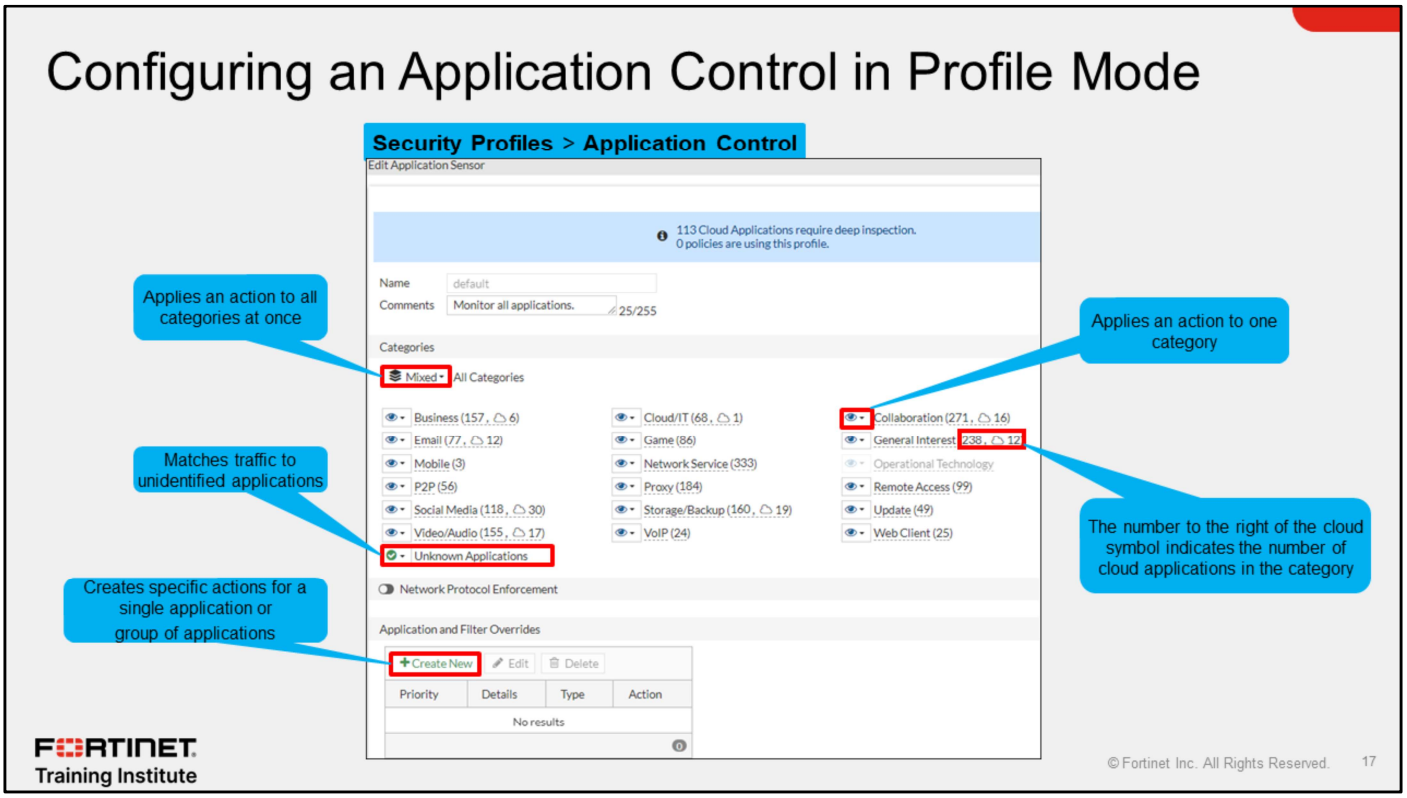
FORTINET Training Institute

Many web applications offer functionality that can be embedded in third-party websites or applications. For example, you can embed a Facebook **Like** button at the end of an article, or reference a YouTube video on an educational website. FortiOS gives administrators all the tools they need to inspect subapplication traffic. The FortiGuard application control signature database is organized in a hierarchical structure. This gives you the ability to inspect the traffic with more granularity. You can block Facebook applications while allowing users to collaborate using Facebook chat.



After FortiGate downloads a FortiGuard Application Control Signature package, new signatures appear in the signature list.

In the example shown on this slide, the signatures are filtered with `linkedin`, showing its category and the corresponding hierarchical structure.

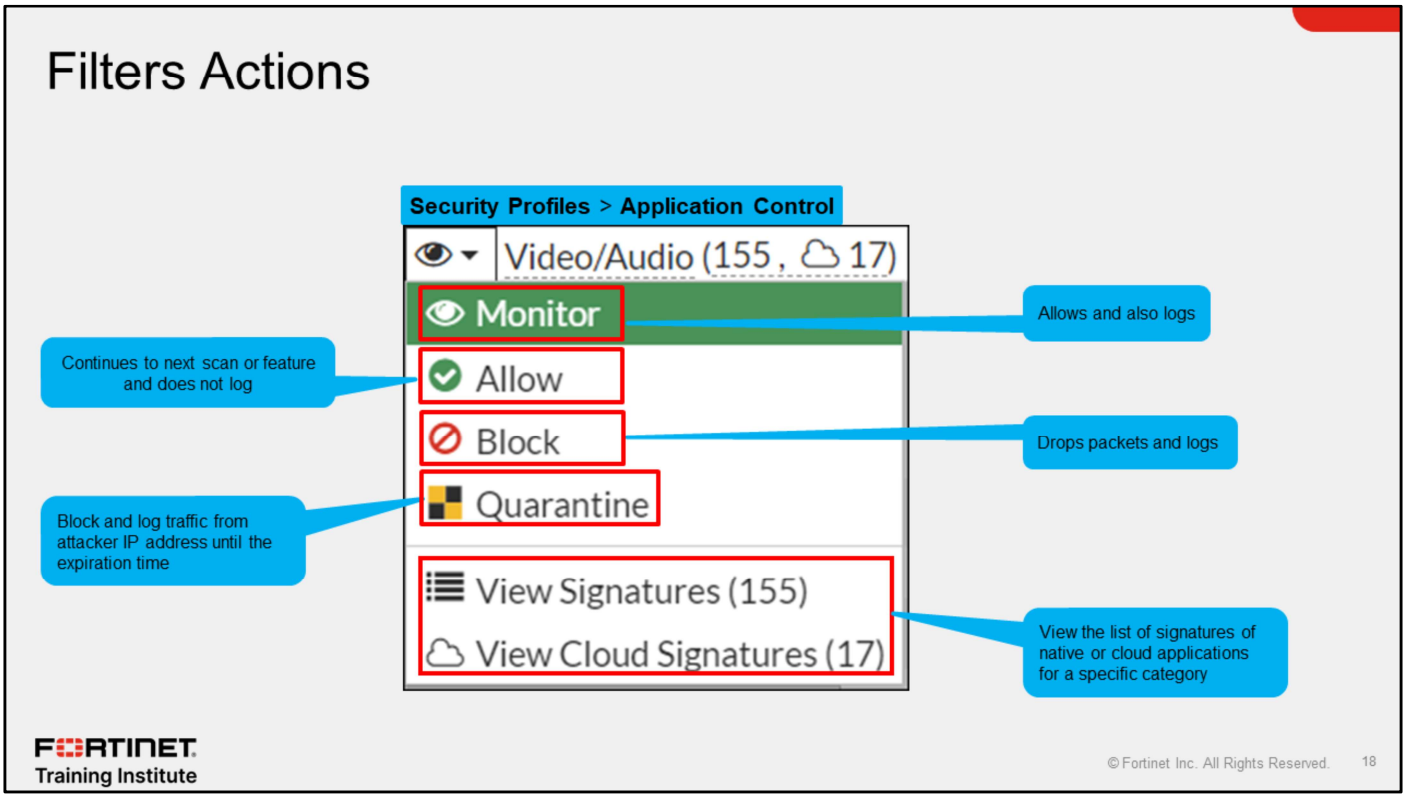


In profile-based mode, you configure application control profiles on the **Application Control** page.

The application control profile consists of three different types of filters:

- Categories: Groups applications based on similarity. For example, all applications that are capable of providing remote access are grouped in the **Remote Access** category. The **Unknown Applications** category refers to traffic that can't be matched to any application control signature. You can configure an action per category or to all of them.
- Application overrides: Provides the flexibility to control specific signatures and applications.
- Filter overrides: Useful when a predefined category does not meet your requirements and you want to modify the action for all applications based on criteria that are not available in categories. Besides category, the additional criteria are behavior, protocol, vendor, popularity, risk, or the technology used by the applications.

At the top of the **Application Control** profile page, you will see a summary of how many cloud applications require deep inspection. Cloud applications that use SSL encryption cannot be scanned without a deep inspection profile. FortiGate must decrypt the traffic in order to perform inspection and control application traffic.



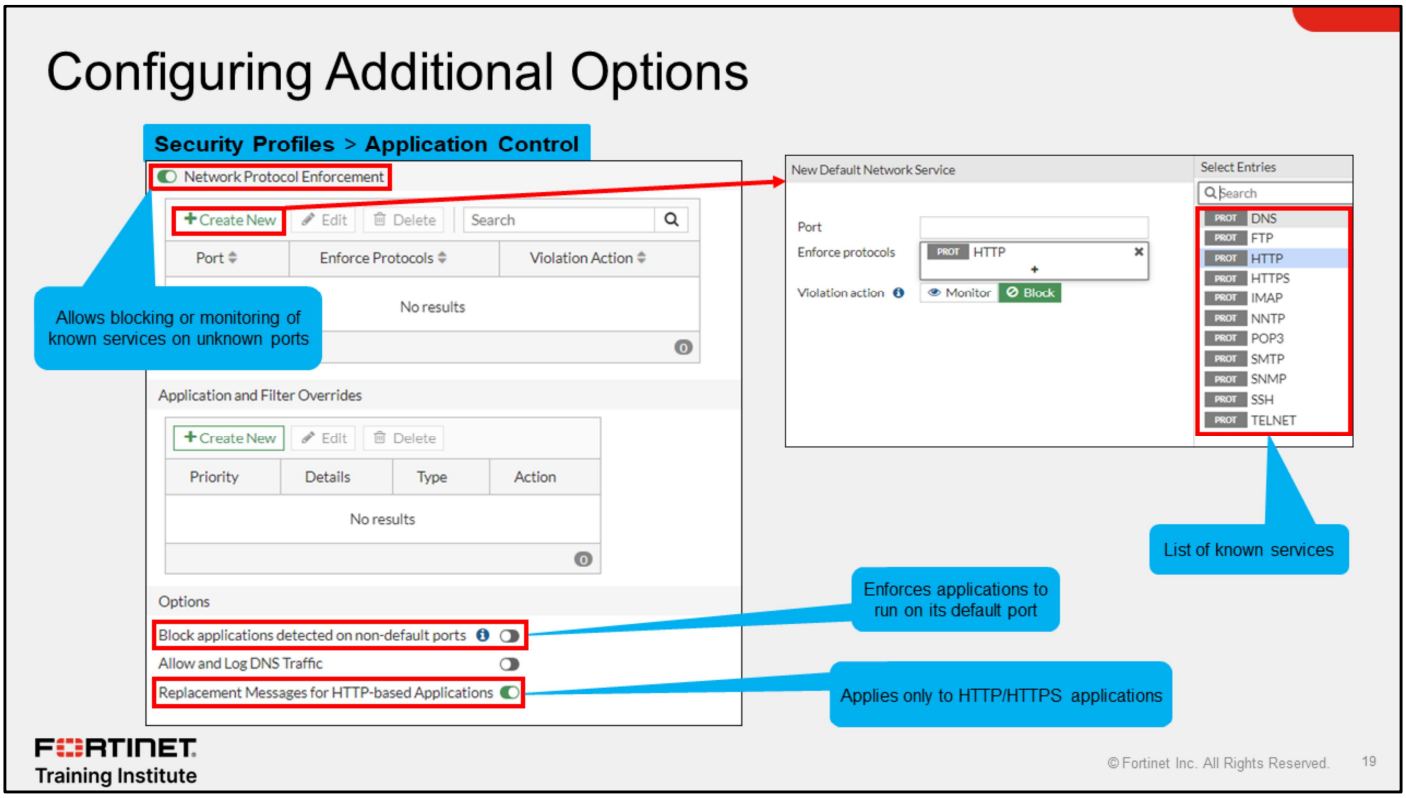
For each filter in the application control profile, you must indicate an action—what FortiGate does when traffic matches. Actions include the following:

- **Allow**: Passes the traffic and does not generate a log
- **Monitor**: Passes the traffic, but also generates a log message
- **Block**: Drops the detected traffic and generates a log message
- **Quarantine**: Blocks the traffic from an attacker IP address until the expiration time is reached, and generates a log message

The **View Signature** action allows you to view signatures from a particular category only and is *not* a configurable action. The **View Cloud Signatures** action allows you to view application signatures for cloud applications from a particular category.

Which is the correct action to choose?

If you're not sure which action to choose, **Monitor** can be useful initially, while you study your network. Later, after you have studied your network traffic, you can fine-tune your filter selection by choosing the most appropriate action. The action you choose also depends on the application. If an application requires feedback to prevent instability or other unwanted behavior, then you might choose **Quarantine** instead of **Block**. Otherwise, the most efficient use of FortiGate resources is to block.



The **Application Sensor** provides also additional options.

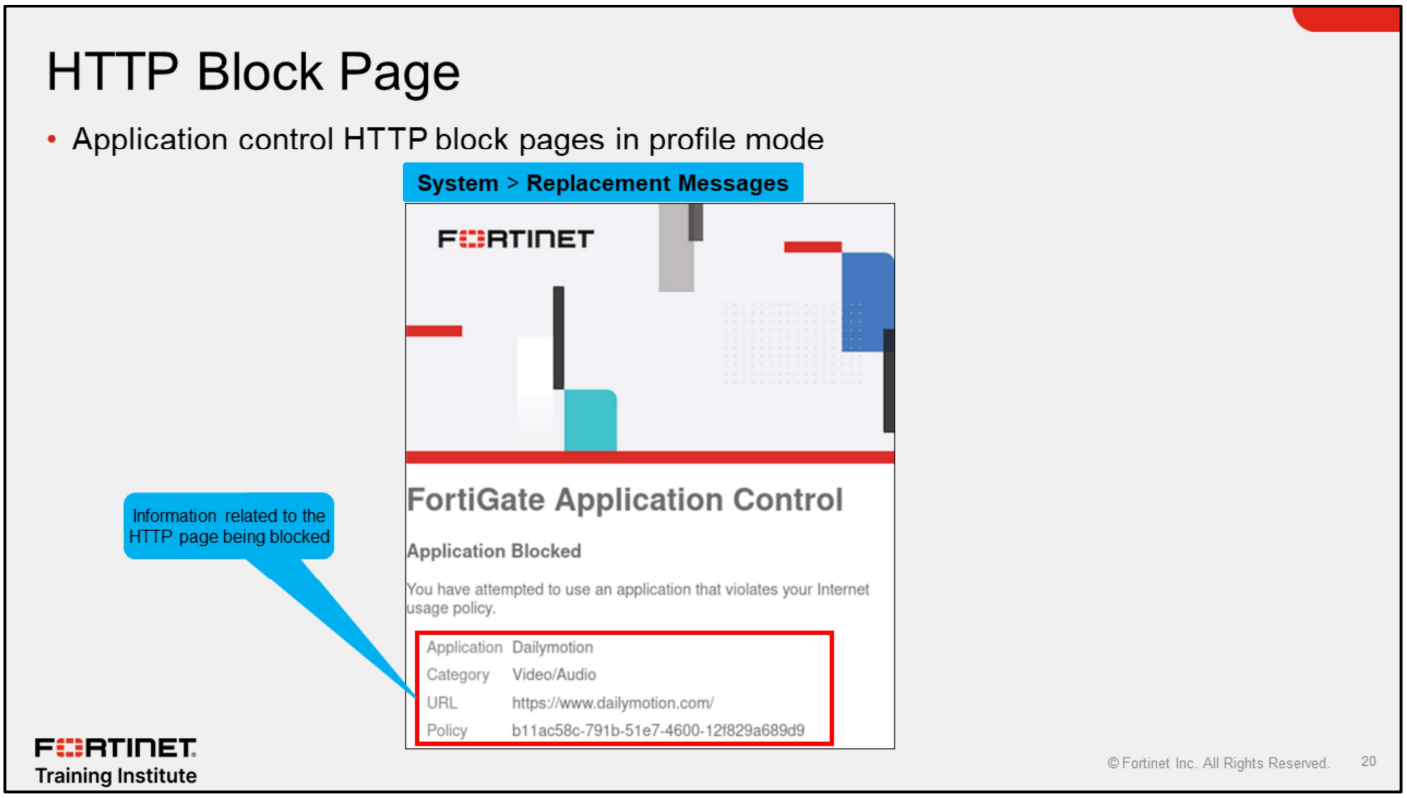
Network Protocol enforcement allows you to configure network services (for example, FTP, HTTP, and HTTPS) on known ports (for example, 21, 80, and 443), while blocking those services on other ports.

The feature takes action in the following scenarios:

- When one protocol dissector confirms the service of network traffic, **Network Protocol Enforcement** can check whether the confirmed service is allowlisted under the server port. If it is not, then the traffic is considered a violation and IPS can take the action (for example, block) specified in the configuration.
- There is no confirmed service for network traffic. It would be considered a service violation if IPS dissectors rule out all the services enforced under its server port, for example, if port 21 is configured for FTP and the protocol dissector could not decide on the exact service but is sure it is not FTP. If the port of the non-FTP traffic is 21, it will be a violation.

With the **Block applications detected on non-default ports** option, FortiGate compares the ports used by the application with the ones defined in FortiGuard application signatures. The traffic is blocked if it does not match.

The **Replacement Messages for HTTP-based Applications** setting allows you to replace blocked content from HTTP/HTTPS applications with an explanation for the user's benefit. For non-HTTP/HTTPS applications, FortiGate only drops the packets or resets the TCP connection.



For HTTP-based applications, application control can provide feedback to the user about why their application was blocked. This is called a block page, and it is similar to the one you can configure for URLs that you block using FortiGuard web filtering.

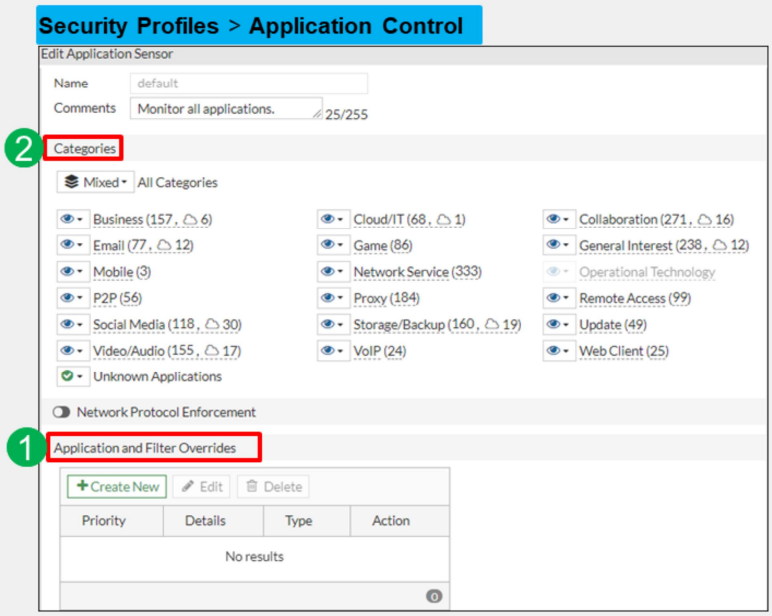
It is also worth mentioning that, if deep inspection is enabled in the firewall policy, all HTTPS-based applications provide this block page.

The block page contains the following information:
- Signature that detected the application (in this case, Dailymotion)
- Signature's category (in this case, Video/Audio)
- URL that was specifically blocked (in this case, the index page of `www.dailymotion.com`), since a web page can be assembled from multiple URLs
- User name (if authentication is enabled)
- Group name (if authentication is enabled)
- UUID of the policy governing the traffic

The last item in this list can help you to identify which policy on FortiGate blocked the page, even if you have a large number of policies with many FortiGate devices securing different segments.

Scanning Order

- The IPS engine identifies the application
- The application control profile scans for matches in this order:
  1. Application and filter overrides
  2. Categories

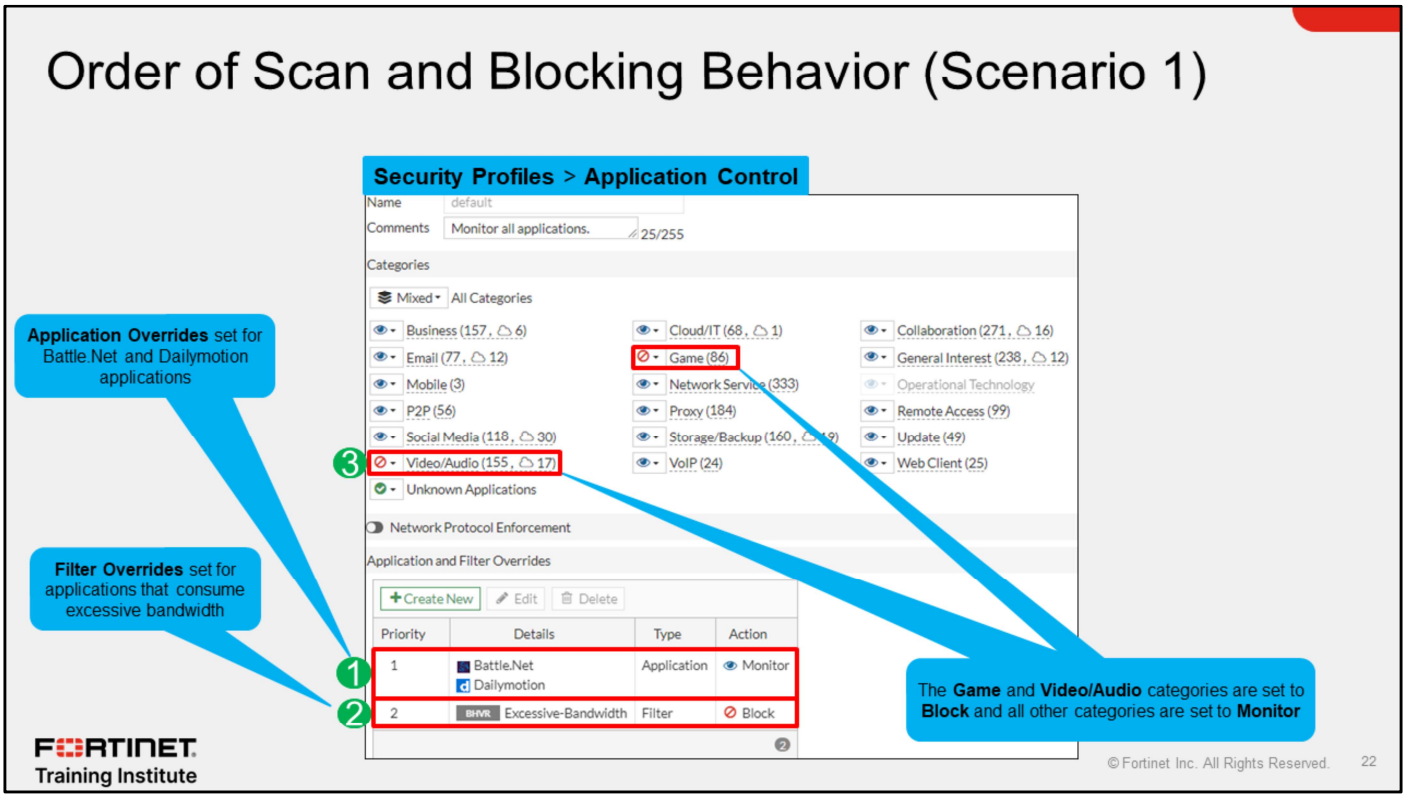


FORTINET Training Institute

With these multiple filters, which one has the priority?

After the IPS engine examines the traffic stream for a signature match, FortiGate scans packets for matches, in this order, for the application control profile:

1. Application and filter overrides: If you have configured any application overrides or filter overrides, the application control profile considers those first. It looks for a matching override starting at the top of the list, like firewall policies.
2. Categories: Finally, the application control profile applies the action that you've configured for applications in your selected categories.



In the example profile shown on this slide, the application control profile blocks the **Game** and **Video/Audio** categories. All other categories are set to **Monitor**, except **Unknown Applications**, which is set to **Allow**.

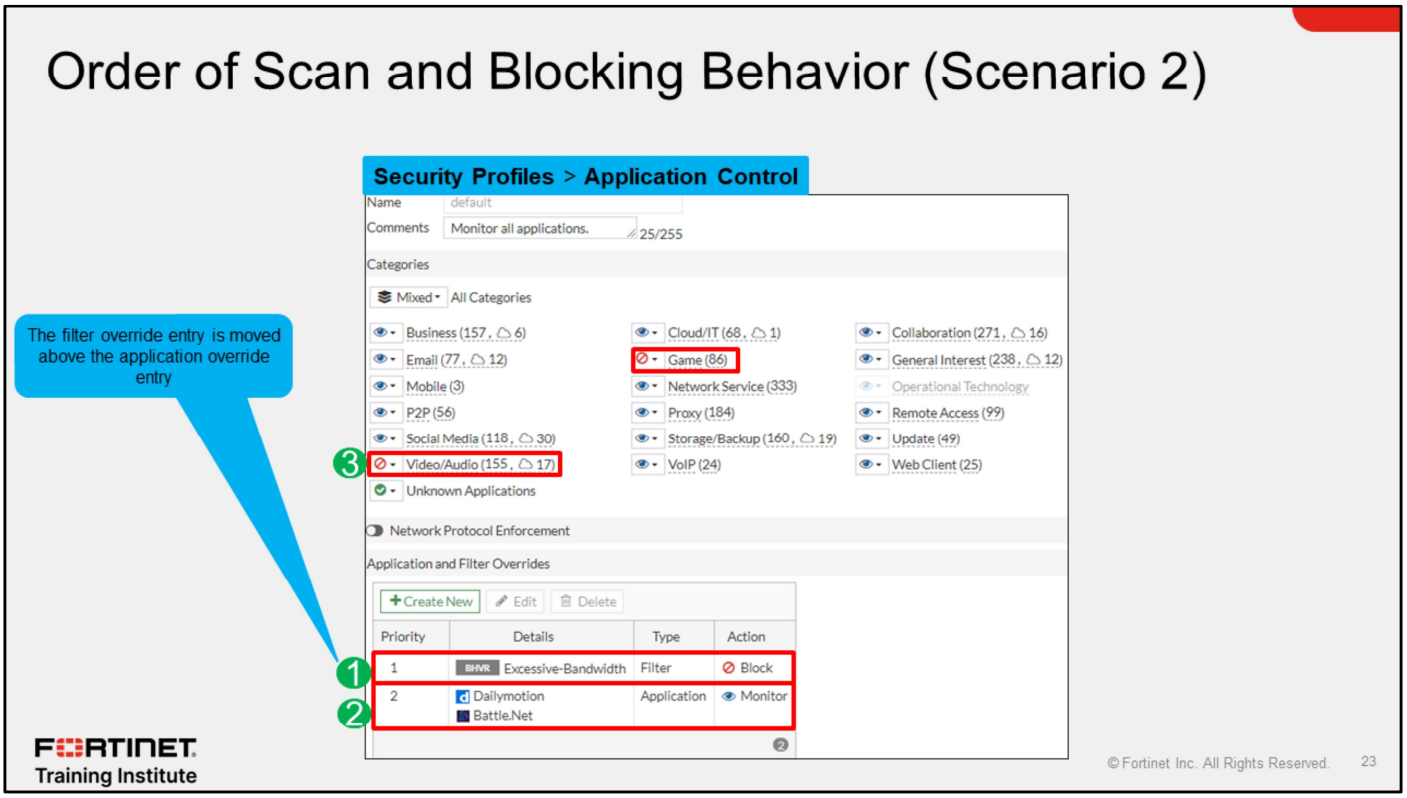
In the **Application and Filter Overrides** section, you can see that some exceptions are specified. Instead of being set to **Block**, **Battle.Net** (**Game**), and **Dailymotion** (**Video/Audio**) are set to **Monitor**. Because application overrides are applied first in the scan, these two applications are allowed, and generate logs.

Next, the scan checks for **Application and Filter Overrides**. Because a filter override is configured to block applications that use excessive bandwidth, it blocks all applications using excessive bandwidth, regardless of categories that allow these applications.

This slide shows an example of how several security profile features could work together, overlap, or work as substitutes, on the same traffic.

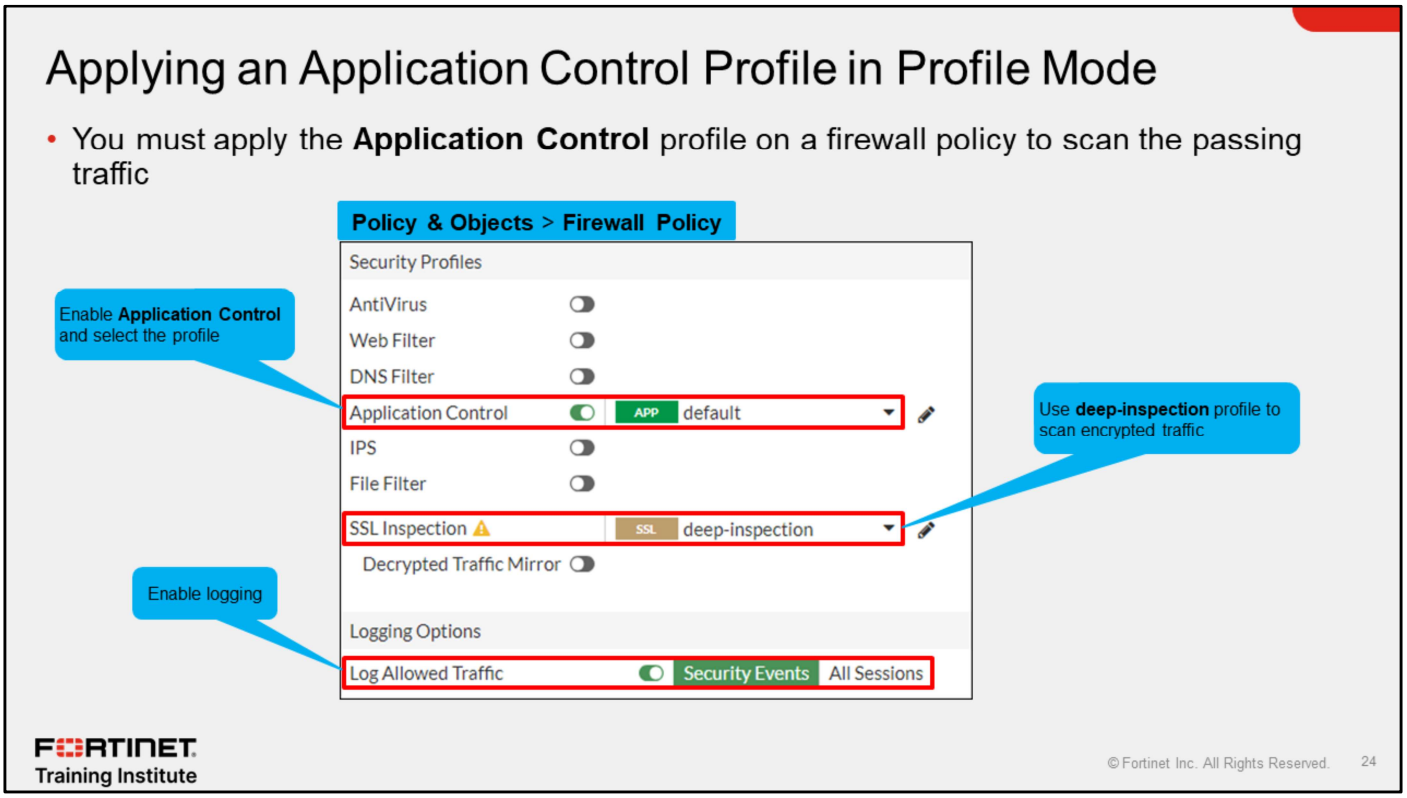
After the application control profile scan is done, FortiGate begins other scans, such as web filtering. The web filtering scan could block Battle.Net and Dailymotion, but it would use its own block message. Also, web filtering doesn't check the list of application control overrides. So, even if an application control override allows an application, web filtering could still block it.

Similarly, static URL filtering has its own exempt action, which bypasses all subsequent security checks. However, application control occurs before web filtering, so that the web filtering exemption *cannot* bypass application control.



In the example profile shown on this slide, the filter override has been moved above the application override. In this scenario, the filter override (**Excessive-Bandwidth**) is blocked and, since **Dailymotion** falls under the excessive bandwidth category, Dailymotion is blocked even though it is set to **Monitor** under the **Application and Filter Overrides** section.

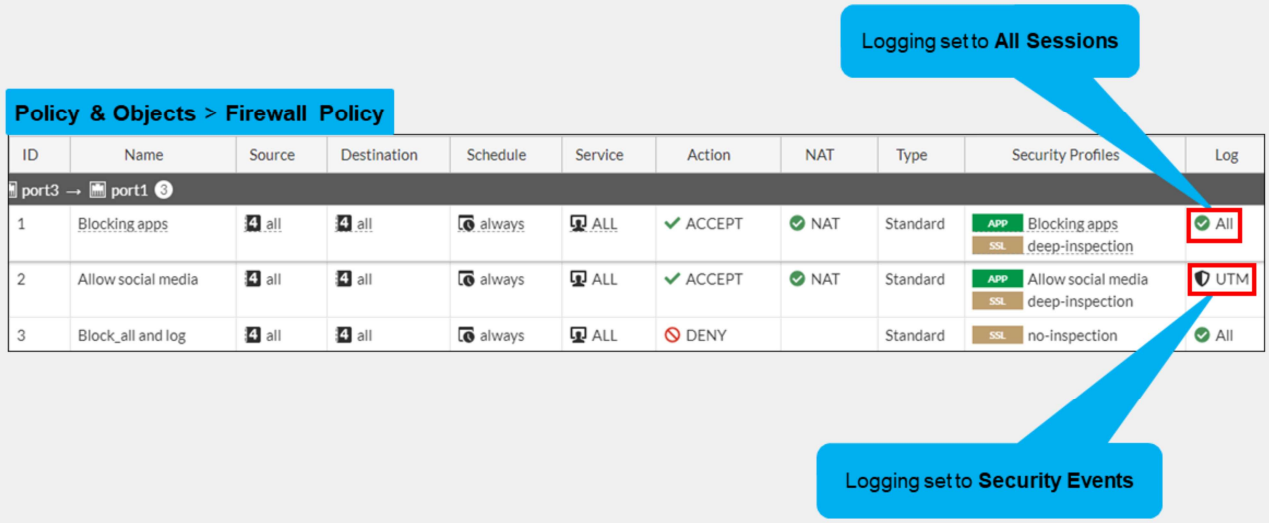
The priority in which application and filter overrides are placed takes precedence.



After you configure an application control profile, you must apply it to a firewall policy. This instructs FortiGate to start scanning application traffic that is subject to the firewall policy.

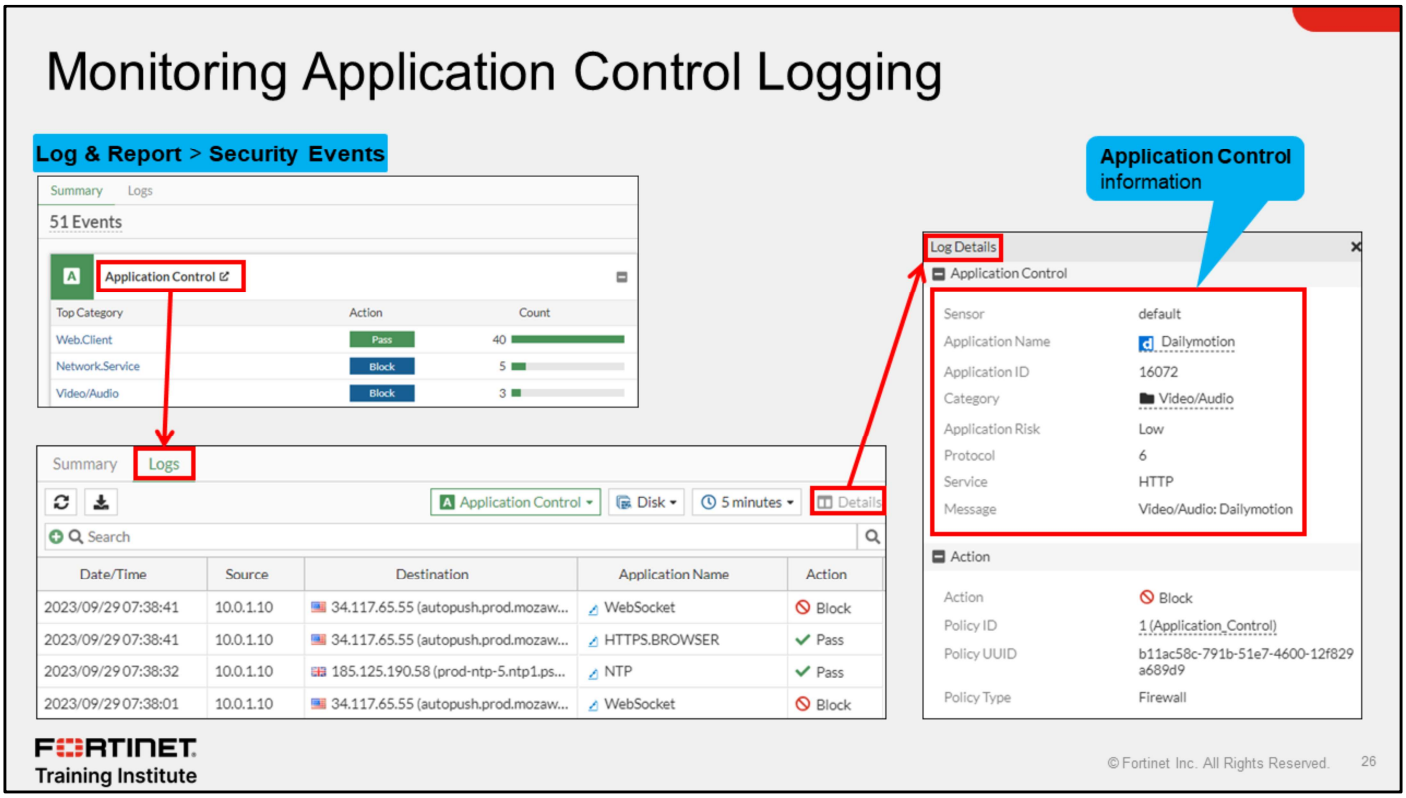
Logging Application Control Events

- Example of NGFW profile-based mode firewall policies



FORTINET Training Institute

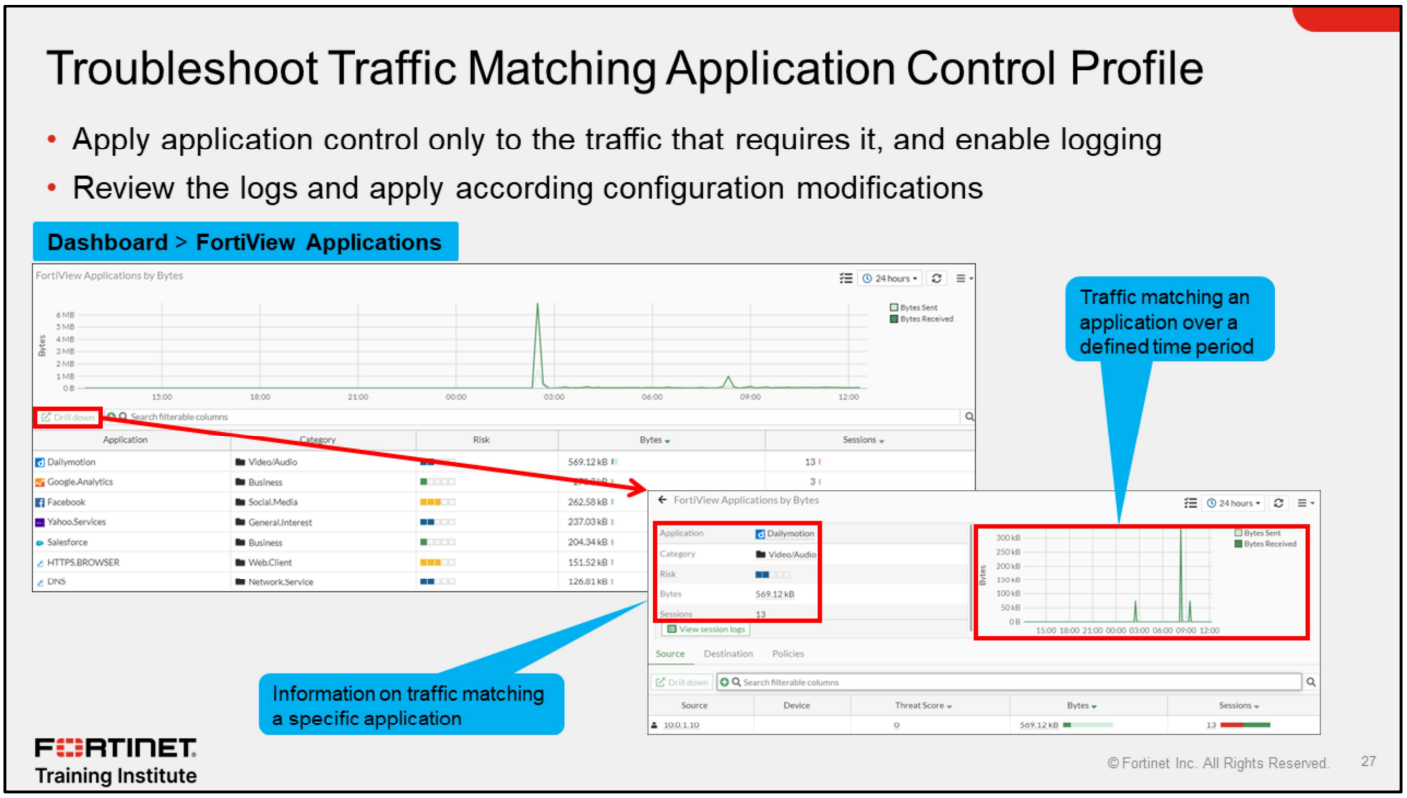
When you enable the logging of security events or all sessions on a firewall policy, application control events are also logged. It allows you to monitor the application control use.



FortiGate logs all application control events on the **Log & Report** > **Security Events** page. You can view the logs by clicking on **Application Control**.

In the example shown on this slide, the default application control profile blocks access to **Dailymotion**. You can view this information in the **Log Details** section, as well as information about the log source, destination, application, and action.

You can also view the details on the **Forward Traffic** logs pane, where firewall policies record activity. You can also find a summary of the traffic to which FortiGate applied application control. Again, this is because application control is applied by a firewall policy. To find out which policy applied application control, you can review either the **Policy ID** or the **Policy UUID** fields of the log message.



Because not all traffic requires an application control scan, you must monitor the security event logs. If a traffic match is incorrect, you must then modify your configuration by first finding the firewall policy involved. This firewall policy reference is available in the **Security Events** logs and also in the **Forward Traffic** logs.

You can also check the traffic matching with application control profiles on the **Dashboard** > **FortiView Applications** page. You can then select a specific application and drill down to view the sessions and bytes information for the traffic matching that application.

Knowledge Check

1. Which IPS action allows traffic and logs the activity?
   - A. Allow
   - ✓ B. Monitor

2. Which statement about application control is true?
   - ✓ A. Application control uses the IPS engine to scan traffic for application patterns.
   - B. Application control is unable to scan P2P architecture traffic.

3. Which statement about the HTTP block page for application control is true?
   - ✓ A. It can be used only for web applications.
   - B. It works for all types of applications.

Review

- ✓ Configure an intrusion prevention system (IPS) sensor
- ✓ Troubleshoot IPS high-CPU usage
- ✓ Configure application control in profile mode
- ✓ Monitor application control events
- ✓ Troubleshoot traffic matching with application control profile issues

FORTINET Training Institute

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you gained the skills and knowledge you need to configure, maintain, and troubleshoot the FortiGate IPS solution. You also learned how to use methods beyond simply blocking protocols, port numbers, or IP addresses, to monitor and control both standard and non-standard network applications.