Tuning Preprocessing in Passive Deployments

Typically, the system uses the static settings in your network analysis policy to preprocess and analyze traffic. With the adaptive profiles feature, however, the system can adapt to network traffic by associating traffic with host information and processing the traffic accordingly.

When a host receives traffic, the operating system running on the host reassembles IP fragments. The order used for that reassembly depends on the operating system. Similarly, each operating system may implement TCP in different ways, and therefore reassemble TCP streams differently. If preprocessors reassemble data using a format other than that used for the operating system of the destination host, the system may miss content that could be malicious when reassembled on the receiving host.

Tip In a passive deployment, Cisco recommends that you configure adaptive profiles. In an inline deployment, Cisco recommends that you configure the inline normalization preprocessor with the **Normalize TCP Payload** option enabled.

## Understanding Adaptive Profiles

License: Protection

Adaptive profiles enable use of the most appropriate operating system profiles for IP defragmentation and TCP stream preprocessing.

Using Adaptive Profiles with Preprocessors

License: Protection

Adaptive profiles help to defragment IP packets and reassemble streams in the same way as the operating system on the target host. The intrusion rules engine then analyzes the data in the same format as that used by the destination host.

Adaptive profiles switch to the appropriate operating system profile based on the operating system in the host profile for the target host, as illustrated in the following diagram.
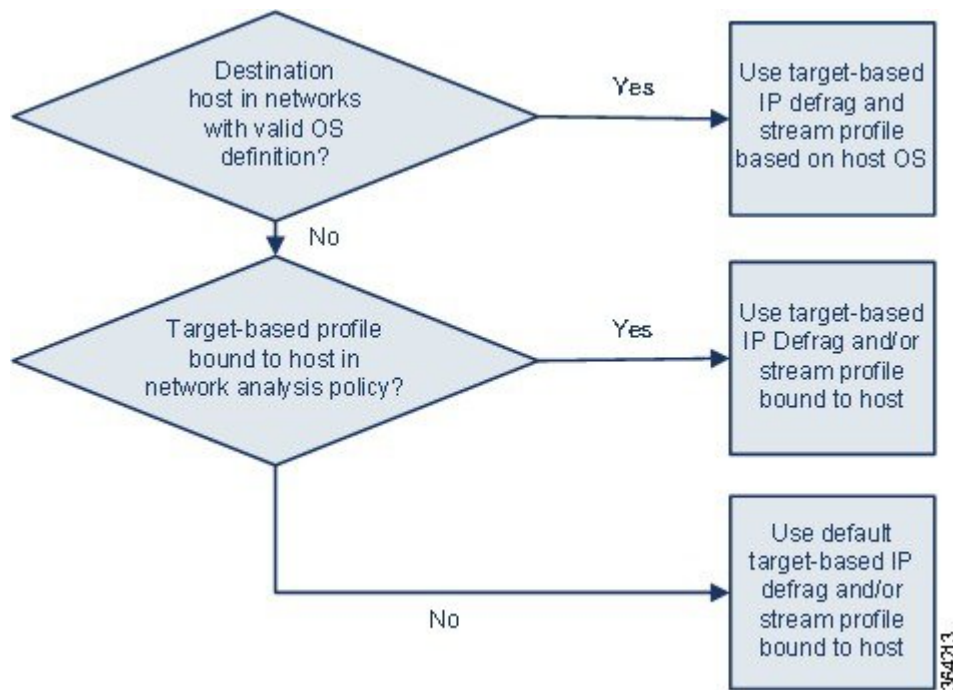
For example, you configure adaptive profiles for the 10.6.0.0/16 subnet and set the default IP Defragmentation target-based policy to Linux. The ASA FirePOWER module where you configure the settings includes the 10.6.0.0/16 subnet.

When a device detects traffic from Host A, which is not in the 10.6.0.0/16 subnet, it uses the Linux target-based policy to reassemble IP fragments. However, when it detects traffic from Host B, which is in the 10.6.0.0/16 subnet, it retrieves Host B's operating system data, where Host B is running Microsoft Windows XP Professional. The system uses the Windows target-based profile to do the IP defragmentation for the traffic destined for Host B.

Configuring Adaptive Profiles

License: Protection

To use host information to determine which target-based profiles are used for IP defragmentation and TCP stream preprocessing, you can configure adaptive profiles.

When you configure adaptive profiles, you need to bind the adaptive profile setting to a specific network or networks. To successfully use adaptive profiles, that network must be in the segment monitored by the device.

You can indicate the hosts in the network where adaptive profiles should be used to process traffic by specifying an IP address, a block of addresses, or a network variable with the desired value configured in the variable set linked to the default intrusion policy for your access control policy.

You can use any of these addressing methods alone or in any combination as a list of IP addresses, address blocks, or variables separated by commas, as shown in the following example:

```
192.168.1.101, 192.168.4.0/24, $HOME_NET
```

🔍

| **Tip** | You can apply adaptive profiles to all hosts in the network by using a variable with a value of any or by specifying 0.0.0.0/0 as the network value. |

To configure adaptive profiles:

Step 1	Select **Configuration** > **ASA FirePOWER Configuration** > **Policies** > **Access Control Policy**.
	The **Access Control Policy** page appears.
Step 2	Click the **edit** icon next to the access control policy you want to edit.
	The **access control policy editor** appears.
Step 3	Select the **Advanced** tab.
	The **access control policy advanced settings** page appears.
Step 4	Click the **edit** icon next to **Detection Enhancement Settings**.
	The **Detection Enhancement Setting**s pop-up window appears.
Step 5	Select **Adaptive Profiles - Enabled** to enable adaptive profiles.
Step 6	Optionally, in the **Adaptive Profiles - Attribute Update Interval** field, type the number of minutes that should elapse between synchronization of data.
		Note	Increasing the value for this option could improve performance in a large network.
Step 7	In the **Adaptive Profiles - Networks** field, type the specific IP address, address block, or variable, or a list that includes any of these addressing methods separated by commas, to identify any host in the network for which you want to use adaptive profiles.
	See Working with Variable Sets for information on configuring variables.
Step 8	Click **OK** to retain your settings.