

Configuring Application Rulebase Rules (NSM Procedure)

The Application Policy Enforcement (APE) rulebase enables you to limit bandwidth for specified users and/or applications. You can configure APE rules to detect network traffic based on application signatures. The APE rules are sent as part of the IDP rulebase, and the attacks are mapped from the corresponding application.

To configure an APE rulebase rule:

1. In the NSM navigation tree, select **Policy Manager > Security Policies**.
2. Select and double-click the security policy to which you want to add the APE rulebase rule.
3. Click **New** in the upper right corner of the policy viewer and select **Add Application Rulebase**.
4. Click the **New** button within the rules viewer to add a rule
5. Modify the property of the rule by right-clicking the table cell for the property and making your modifications.
6. Configure or modify the rule using the settings described in Table 1.
7. Click **OK** to save your changes.

Table 1: APE Rulebase Rule Properties

| Option | Function | Your Action |
|---------------------|---|---|
| No. | Specifies if you want to add, delete, copy, or reorder rules. | Right-click the table cell for the rule number and make your required modifications. |
| Match > Source | Specifies the address object that is the source of the traffic. | Select any to monitor network traffic originating from any IP address. NOTE: For guidelines on specifying match parameters, see the <i>IDP Concepts and Examples Guide</i> . |
| Match > User Role | Specifies the user roles to match the session for the rule to be applied. If a value for User Role matches, the Source parameter is not consulted. Matching based on user role depends on integration with a compatible Juniper Networks IC Series Unified Access Control appliance. | Right-click the table cell to select user roles. |
| Match > Destination | Specifies the address object that is the destination of the traffic, typically a server or other device on your network. | Select the destination object. NOTE: You can also negate one or more address objects to specify all destinations except the excluded object. |

Table 1: APE Rulebase Rule Properties (continued)

| Option | Function | Your Action |
|---------------------|---|---|
| Match > Service | <p>Requires one of the specified services to match the session for the rule to be applied. Services are Application Layer protocols that define how data is structured as it travels across the network. The IDP engine can inspect services that use TCP, UDP, RPC, and ICMP transport layer protocols. If the application running on the destination server uses standard ports, you can select from predefined services. If the application running on the destination server uses nonstandard ports, you must create a custom service object.</p> | <p>Right-click the table cell and select any one of the required options.</p> <p>If you specify named values for both service and application, only the application value is used.</p> <p>It is recommended to specify Default for the service parameter and configure the application parameter instead.</p> <p>Specify Any to not use service as a key to your match.</p> <p>NOTE: To apply an APE action to all traffic matching source and destination parameters, set both the service parameter and the application parameter to Any.</p> |
| Match > Application | <p>Requires one of the specified applications to match the session for the rule to be applied. The predefined list of applications is populated by the application identification feature. The application identification feature identifies the application regardless of port. Port-independent application identification simplifies rule configuration and ensures that you do not miss applications running on nonstandard ports. Hence it is recommended to use the application parameter instead of the service parameter whenever possible.</p> | <p>Right-click the table cell and make your required modifications.</p> <p>If you specify named values for both service and application, only the application value is used.</p> <p>Specify Any to not use application as a key to your match.</p> <p>NOTE: To apply an APE action to all traffic matching source and destination parameters, set both the service parameter and the application parameter to Any.</p> |

Table 1: APE Rulebase Rule Properties (continued)

| Option | Function | Your Action |
|--------------|--|--|
| Action | Specifies which actions to perform against attacks that match rules in your security policy. | <p>Right-click the table cell and select any one of the following options:</p> <ul style="list-style-type: none"> ■ None — IDP takes no action against the connection. ■ Drop Packet — IDP drops a matching packet before it can reach its destination but does not close the connection. ■ Drop Connection — IDP drops the connection without sending an RST packet to the sender, preventing the traffic from reaching its destination. ■ Close Client — IDP closes the connection to the client and not to the server. ■ Close Server — IDP closes the connection to the server and not to the client. ■ Close Client and Server — IDP closes the connection and sends a RST packet to both the client and the server. ■ Diffserv Marking — Assigns the service differentiation value indicated to the packet, then passes it on normally. ■ Rate Limiting — IDP enforces a rate limit for all current sessions that match the rule (separate limits for client-to-server and server-to-client traffic). If the limit has not been reached, IDP forwards the packets. If the limit has been reached, IDP behaves as if no bandwidth is available. |
| Notification | Specifies logging options. Packet capture is not applicable for APE rulebase rules. | Right-click the table cell and select Configure to display a dialog box where you can configure logging options. |
| VLAN Tag | Specifies rules to traffic on certain VLANs. Normally, for a rule to take effect, it must match the packet source, destination, service, and attack objects. If the VLAN cell is populated with a value other than any, then the rule will also consider the packet's VLAN tag when determining a match. | Right-click the table cell to assign a VLAN object to a rule or to set the VLAN tag value to none. |
| Install On | Specifies target IDP devices for the rule. By default, IDP security policy rules can be applied to any IDP device. | Right-click the table cell and select Select Target to display a dialog box to specify the IDP devices to which the rule can be installed. |
| Comments | Adds notations about the rule. This setting is optional and does not affect the functionality of the security policy rule. | Right-click the table cell and select Edit Comments to display a dialog box where you can make notations about the rule. |

You can verify the APE rulebase functionality in your lab and view APE related statistics in the Command-Line Interface (CLI). It is recommended that you retain defaults for APE rulebase. By default:

- IDP does not limit the rate of sessions that do not match APE rules. Rate limiting is done by service based till application is identified in the session i.e. default services running on the port.
- When the application identification feature fails to identify the application, IDP does not try to match the rule but instead applies the default rate limit (if any). You can modify this so that in cases where application identification fails, IDP attempts to match the session to the standard protocol and port for the application.

For more information, see the *IDP Concepts & Examples guide*.

- Related Topics**
- Intrusion Detection and Prevention Devices and Security Policies Overview
 - Modifying IDP Rulebase Rules (NSM Procedure)