

Applying Services to Manage Threats

You can configure services to control problem traffic, such as limiting bandwidth or blocking traffic, in response to detection of malicious traffic. The Threat Mitigation Application passes the defining attribute values of the attack type to the service as parameters for possible use in the policies. The Threat Mitigation Application supports service activation on the JUNOS forwarding interface, the JUNOS provider edge interface, or the JUNOS subscriber interface. You can configure only one of these interfaces as the service activation interface for the Threat Mitigation Application, but you can use an aggregate service to apply the policies on a combination of those interfaces.

The following example describes how to configure policies to decrease the amount of bandwidth available to the attacker and to block the attack or the attacker as implemented in the sample data. You can use any of these services or create your own services to define actions for the Threat Mitigation Application.

To configure services and policies to handle threats:

1. Create a policy that defines an action to be taken.

The sample data for each type of interface contains these policy groups:

- **blockAttack**—Blocks all traffic between the source and destination addresses for the specified protocol and ports. If the protocol or ports are not specified, then the default value is any protocol and any port.
- **blockAttacker**—Blocks all traffic coming from or going to the source address.
- **default**—Forwards traffic.
- **slowAttacker**—Limits the bandwidth available for all traffic coming from or going to the source address according to the specified rate.

For a policy folder that contains these policy groups for the JUNOS forwarding interface, see *ou = forwardingInterface, ou = thma, o = Policies, o = umc* in the sample data.

For a policy folder that contains these policy groups for the JUNOS provider edge interface, see *ou = peInterface, ou = thma, o = Policies, o = umc* in the sample data.

For a policy folder that contains these policy groups for the JUNOS subscriber interface, see *ou = subrInterface, ou = thma, o = Policies, o = umc* in the sample data.

2. Create a new scope or use an existing scope for the services that define actions to be taken in response to attacks on different interfaces.

For a sample scope that applies to the JUNOS forwarding interface, see *l = THMA-ForwardingInterface, o = Scopes, o = umc*.

For a sample scope that applies to the JUNOS provider edge interface, see *l = THMA-PeInterface, o = Scopes, o = umc*.

For a sample scope that applies to the JUNOS subscriber interface, see *l = THMA-SubrInterface, o = Scopes, o = umc*.

3. For the scope used in Step 2:
 - a. Create a service that defines actions to be taken in response to threats. You can create different types of services. For example, you can create aggregate services to apply the policies on these interfaces.

The sample data contains normal services that specify the policy group configured in Step 1.

For a sample service to block attacks on the forwarding interface, see *serviceName = BlockAttack, l = THMA-ForwardingInterface, o = Scopes, o = umc*.

- b. Assign the scope to a subscriber folder to make the service available to these subscribers.

For a sample on the JUNOS forwarding interface, see *ou = routers, retailerName = SP-THMA, o = Users, o = umc*.

For a sample on the JUNOS provider edge interface, see *ou = subscribers_pelf, retailerName = SP-THMA, o = Users, o = umc*.

For a sample on the JUNOS subscriber interface, see *ou = subscribers_subrIf, retailerName = SP-THMA, o = Users, o = umc*.

4. Create service subscriptions for subscribers. In the sample data, we create a subscription at the folder level to allow all subscribers in the folder to inherit the subscription. Configure the subscriptions to manually activate the service through the SRC-TMP.

For a sample implementation, see *serviceName = BlockAttack, retailerName = SP-THMA, o = Users, o = umc* in the sample data.

For information about configuring subscriptions, see [Configuring Subscriptions \(SRC CLI\)](#).

- Related Topics**
- [Configuring Threat Mitigation](#)
 - [Installing and Initially Configuring the Threat Mitigation Application](#)
 - [Configuring the Threat Mitigation Application](#)
 - [Examples: Classifying Subscribers and Interfaces for the Threat Mitigation Application](#)