RADWARE DEFENSEPRO INTEGRATION AND MITIGATION PROCESS GUIDE

The StealthWatch System uses Radware's DefensePro® to mitigate DDoS (distributed denial-of-service) attacks. The DDoS Alarm Dashboard and the DDoS Traffic Dashboard in the StealthWatch Management Console (SMC) provide you with data that assists you in detecting and investigating DDoS-related activity. The activity could include DDoS security events that have triggered an alarm, or spikes and changes in traffic patterns on your network that might indicate a DDoS threat or a DDoS attack as it is starting to occur. If you deem it necessary, you can activate the mitigation process from the DDoS Alarm Dashboard.

When the mitigation process has been initiated, the StealthWatch System notifies the DefensePro device of the DDoS policies and BGP route to use (if you are using the DefensePro device for BGP traffic diversion). Next, the DefensePro device makes a BGP announcement to the applicable router to start diverting all traffic from the target subnet mask to the DefensePro device. Finally, the DefensePro device applies the DDoS policies to block the attack traffic, and the legitimate traffic is re-routed back to your network.

If you entered a mitigation duration, mitigation will end automatically; otherwise, you end the mitigation process manually when you determine that the attack has terminated. Use APSolute Vision™ to monitor the DefensePro device and use its reporting capabilities to determine the status of the attack.

This document describes how to do the following:

- Integrate a Radware DefensePro device with the StealthWatch System.
- Mitigate a DDoS attack to your network using DefensePro.

Procedures

This document includes the following procedures (perform them in the order shown):

1. Deploy DefensePro on your network.
2. Enable global parameters for DefensePro
3. Configure DefensePro using SSH.
4. Add DefensePro to the StealthWatch System.
5. Enable mitigation for policies.
6. Define mitigation actions for alarms.
7. Edit Default DefensePro policies.
8. Start the mitigation process.

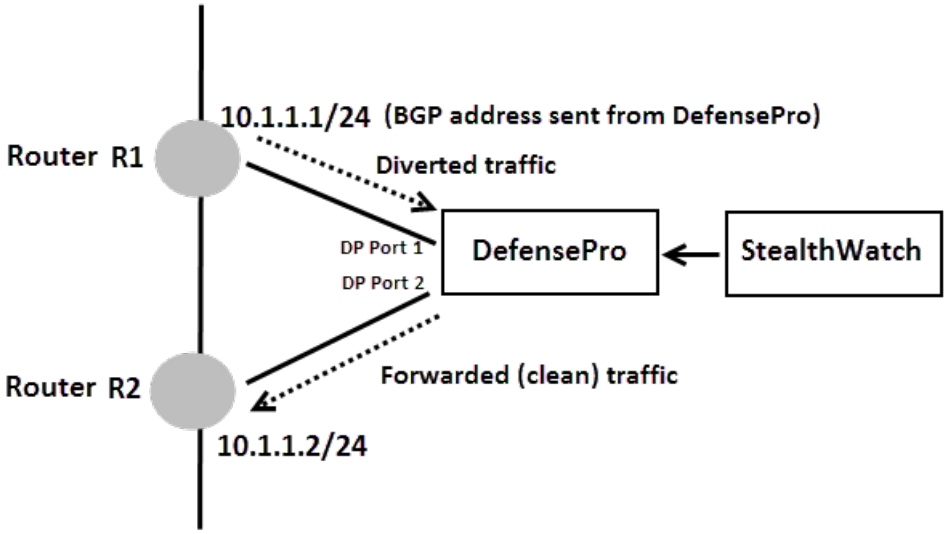
9. Monitor the mitigation process.
10. End the mitigation process.

Deploying DefensePro on Your Network

The following actions must be taken to deploy DefensePro on your network:

- Set up the DefensePro device with static routes.
- Configure the DefensePro device as a BGP (Border Gateway Protocol) neighbor (if you are using DefensePro for BGP traffic diversion).
- Configure each router so that it has the ability to use the BGP route to divert traffic from the target subnet mask. This can be done using metrics, weights, or AS pathing.

The diagram shown below, and the information that follows it within this section, presents one example of how you can deploy DefensePro on your network.



DefensePro physical connectivity

The DefensePro device connects through Port 1 to the perimeter router R1 and through Port 2 to the core router R2. A static forwarding rule is set on the DefensePro device between Ports 1 and 2. Security policies are further defined on top of the static forwarding rule.

Basic router configuration

Each of the routers use a separate physical interface with a dedicated network address configured for traffic diversion and injection. The diagram in this section illustrates using network 10.1.1.0/24, with R1 using the address 10.1.1.1 and R2 using the address 10.1.1.2.

Traffic diversion

When you start the mitigation process, the StealthWatch System notifies the DefensePro device of the DDoS policies and BGP route to use. Next, the DefensePro device makes a BGP announcement to the perimeter router R1 to divert all traffic from the target subnet mask to the DefensePro device. The DefensePro device then applies the DDoS policies to block the attack traffic.

Forwarding Clean Traffic

The DefensePro device forwards the clean traffic to the core router R2. The core router R2 uses its routing logic to forward the traffic to the destination.

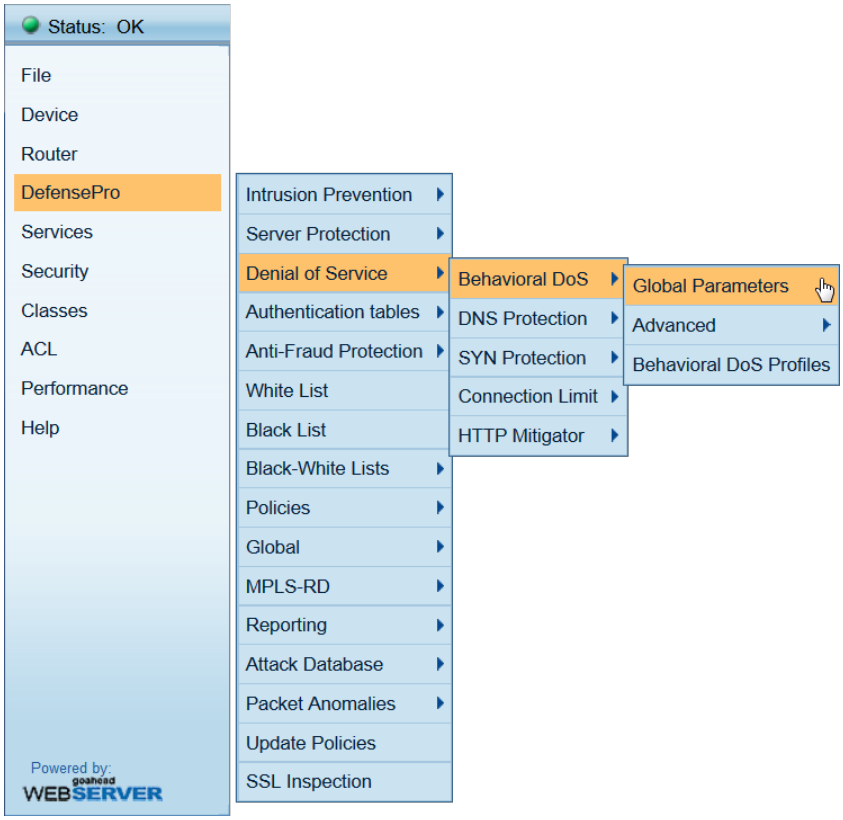
Enabling Global Parameters for DefensePro

Log in to the DefensePro Web user interface and enable the global parameters for the following four features:

- Behavioral DoS
- DNS Protection
- SYN Protection
- HTTP Mitigator

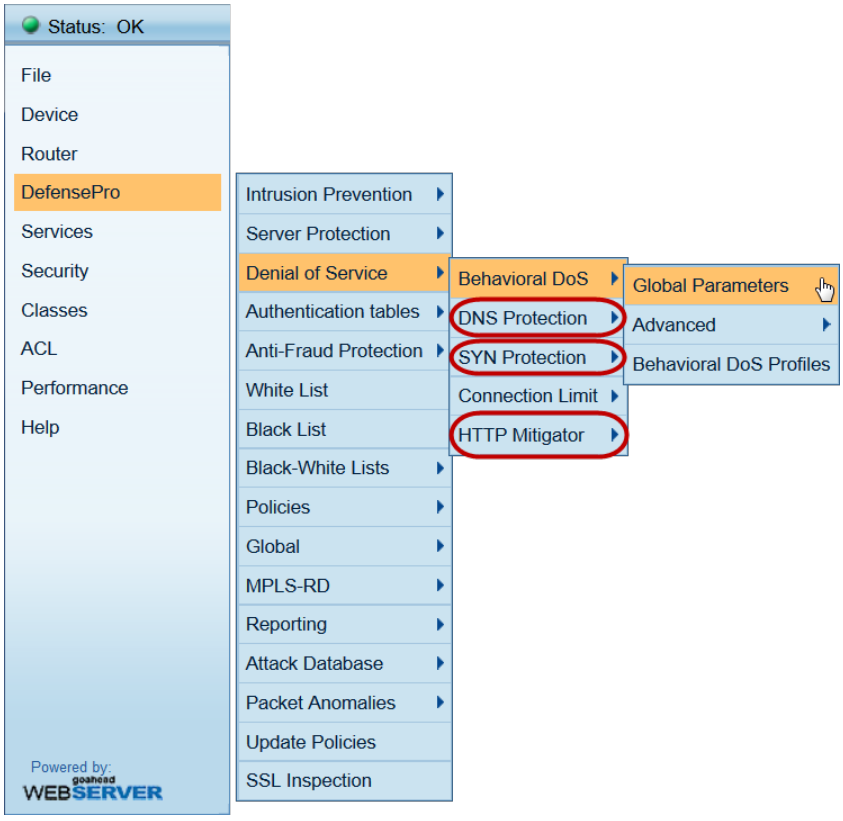
To set the global parameters for each of these four features, complete the following steps.

1. Log in to the DefensePro Web user interface.
2. From the left navigation pane, click DefensePro > Denial of Service > Behavioral DoS > Global Parameters.



3. The Behavioral DoS Global Parameters page is displayed:

4. Ensure that *enable* is displayed in the Bahavioral DoS Status drop-down list box.
5. Click **Set**.
6. Repeat steps 2-5, substituting each time one of the three options that are circled in the following image in place of the Behavioral DoS option in step 2.



Configuring DefensePro Using SSH

Configure the DefensePro device to enable it to communicate with the StealthWatch System.

To do this, complete the following steps.

1. SSH to the DP (both the default username and password are *radware*).
2. Type the following command:

```
Manage terminal more-prompt set off
```

3. When the command entered in step 2 has finished running, type the following command:

```
Dp dns-protection global status set enable
```

4. When the second command has finished running, reboot the DefensePro device.

Adding DefensePro to the StealthWatch System

Use the Radware DefensePro dialog to add the DefensePro device to the StealthWatch System.

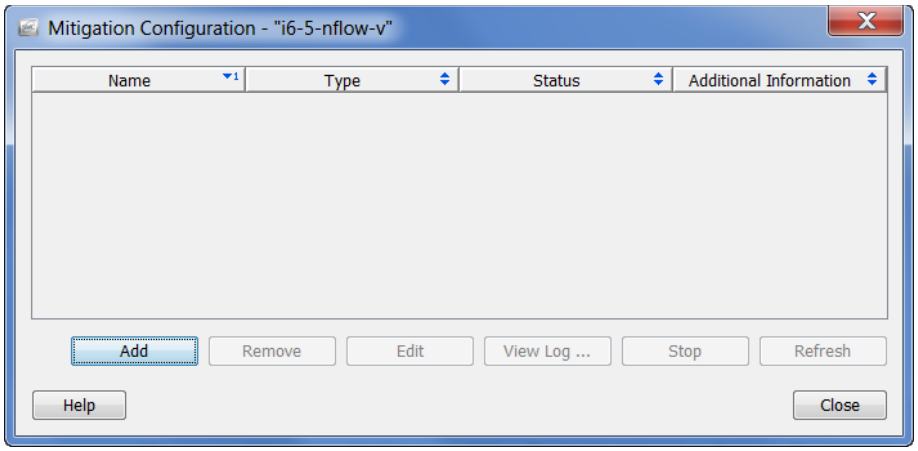
You can add up to five mitigation devices per FlowCollector. The FlowCollector pushes the policy being used for the current attack to ALL devices that are connected to that FlowCollector.

StealthWatch can automatically mitigate the following alarms, blocking the target IP address:

- High Target Index
- ICMP Received
- Max Flows Served
- New Flows Served
- SYNs Received
- UDP Received

To add and configure the DefensePro device, complete the following steps.

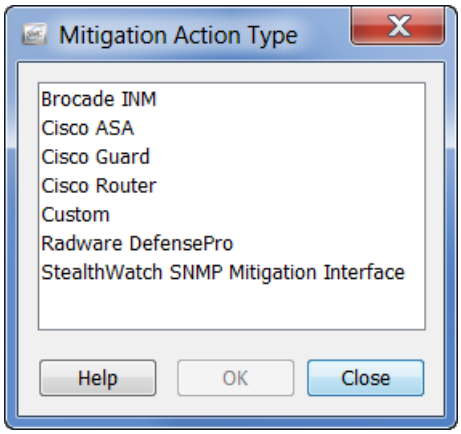
1. In the SMC, right-click a StealthWatch FlowCollector in the Enterprise tree and click **Configuration > Mitigation Configuration** from the pop-up menu. The Mitigation Configuration dialog opens.



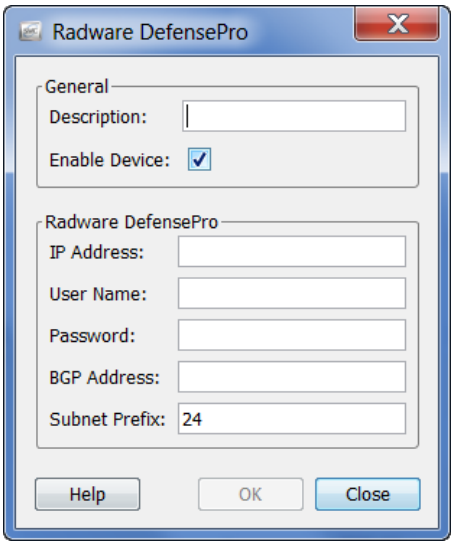
The following information is displayed.

Field	Description
Name	The descriptive name of the mitigation device.
Type	The mitigation device type.
Status	The status of the corresponding mitigation device, as follows: • Connected • Not Connected • Unknown
Additional Information	Additional information about the status of the mitigation device, as follows: • Failed – An attempt to communicate with the mitigation device was unsuccessful. Make sure the Enable device checkbox is selected in the corresponding Mitigation Configuration dialog. • Functioning Properly - The StealthWatch FlowCollector and the mitigation device are communicating successfully. • Session down – device closed.

2. Click **Add**. The Mitigation Action Type dialog opens with a list of mitigation devices that StealthWatch supports.



3. Select **Radware DefensePro** and click **OK**. The Radware DefensePro dialog opens.



4. Specify the device settings as indicated in the following table.

Field	Description
Description	A unique descriptive name. If you will be adding more than one DefensePro device, edit the name of the device. Each DefensePro device must have a unique name assigned to it. **Note:** You cannot use a semicolon in this field.
Enable Device	Select the **Enable Device** check box to enable the StealthWatch System to communicate with the DefensePro device. If you do not select this check box, the StealthWatch mitigation feature will not work.
IP Address	The IP address of the mitigation device.
User Name	A valid user name for the mitigation device. Leave this field blank if the device does not require a user name. **Note:** SSH requires a user name and password for authentication.
Password	The password that is defined on the mitigation device.
BGP Address	(This field is optional.) The BGP IP Peer address of the router that the DefensePro device will announce route changes to so traffic diversion can occur. If you do not select this check box, the DefensePro device will not divert traffic.
Subnet Prefix	This value determines the size of the network block on which diversion will be performed. You can enter a number from 8-32. **Example:** If the target IP to mitigate is 172.16.20.220, and the subnet mask prefix specified is 24 bits, then the network block diverted on would be 172.16.20.0/24. All hosts in this network range would be diverted. You would enter **24** as the value in the Subnet Prefix field.

5. Click **Close**. The device information dialog closes and this device is now included on the Mitigation Configuration dialog. The Status and Additional Information columns provide you with information about the status of the connection.

Important: You can add up to five mitigation devices per FlowCollector. The FlowCollector pushes the policy being used for the current attack to ALL devices that are connected to that FlowCollector.

6. Repeat steps 2 - 4 until you have added all of the mitigation devices you need to add for this StealthWatch FlowCollector.

You can also use the Mitigation Configuration dialog to perform the following actions:

- Remove a device from the StealthWatch System.
- Edit a device.
- View the logged messages for a device. The following information is available:

Field	Description
Date	The date and time of the logged message.
Direction	The direction of the message, as follows: • send – From the StealthWatch FlowCollector to the mitigation device. • recv – From the mitigation device to the StealthWatch FlowCollector. • <blank> – Any message posted to the log for which direction cannot be determined.
Message	The content of the logged message. Passwords are intentionally obscured and are displayed as a series of asterisks.

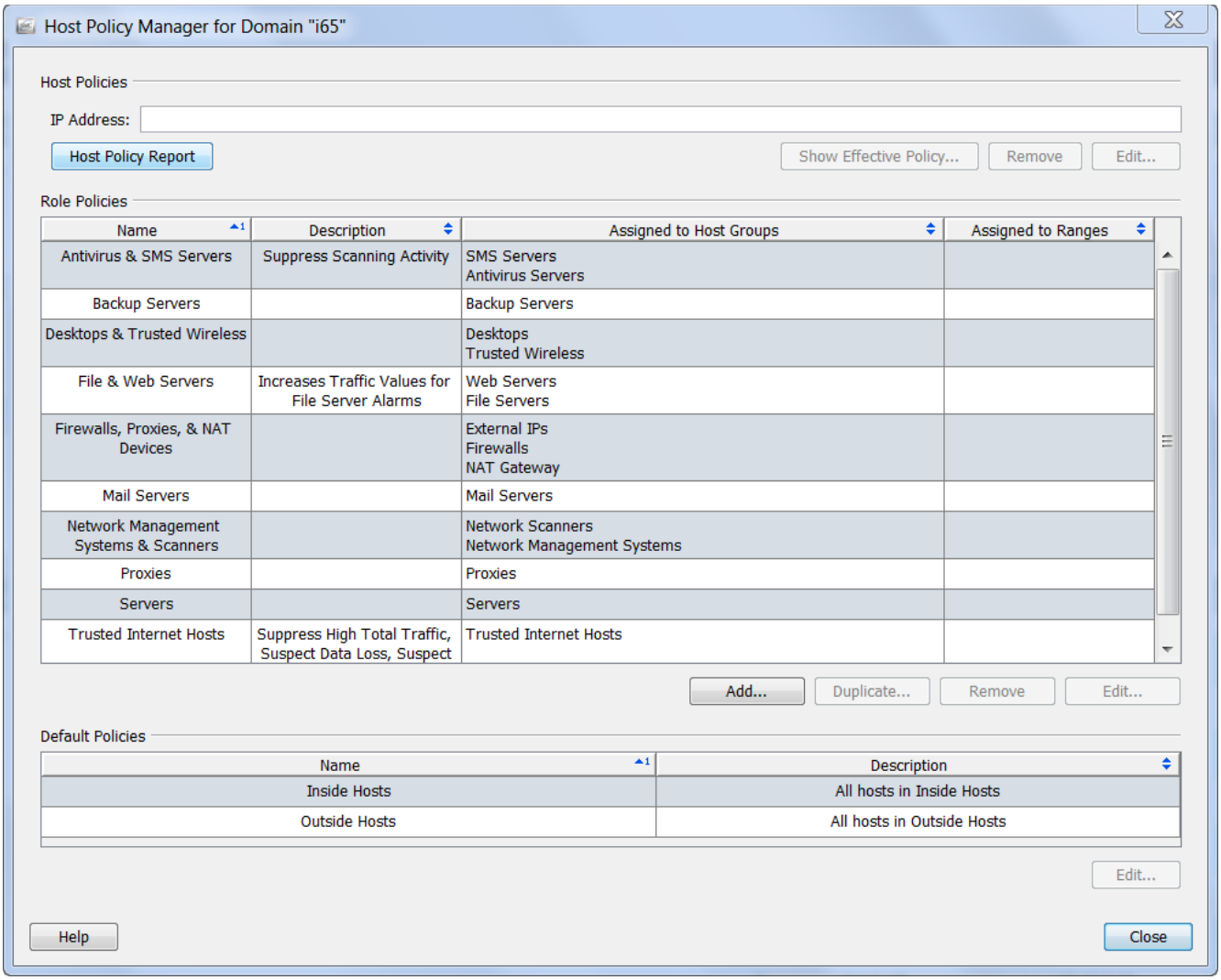
- Stop an attempt to establish a connection to a device. This button is available only when the Additional Information column shows *Pending*.

Enabling Mitigation for Policies

You can enable the StealthWatch System mitigation feature for specific policies, which can be assigned to one or more host groups. For example, you may want to enable the mitigation feature for the Inside Hosts default policy. You can also enable the feature for only a few host groups, or even for specific host IP addresses.

To use the SMC to enable the mitigation feature for specific host groups or IP addresses, complete the following steps.

1. From the Main menu, click **Configuration > Host Policy Manager**. The Host Policy Manager dialog opens.



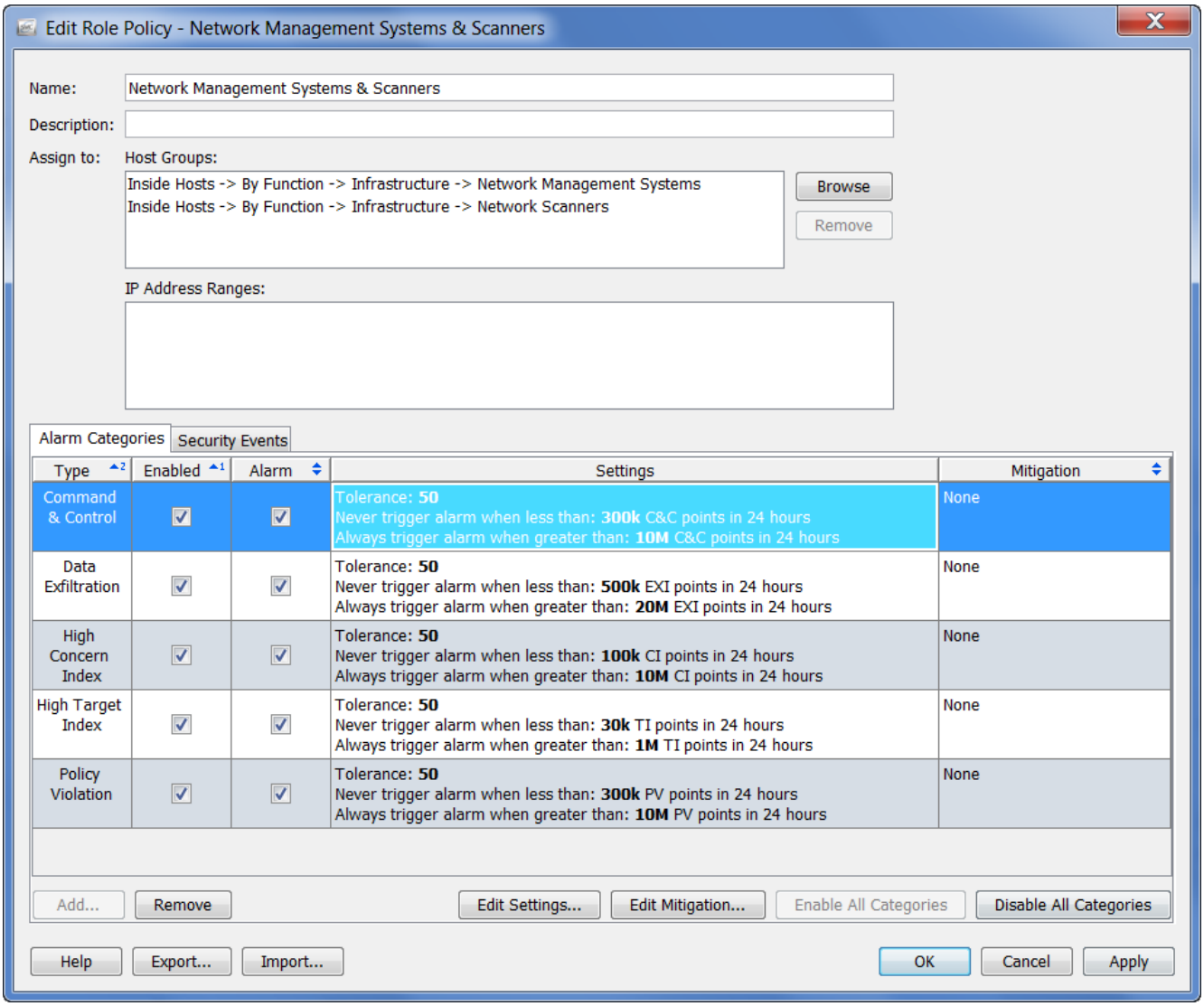
2. Do one of the following:

   To enable the mitigation feature for a

   - Default policy – Within the Default Policies section, highlight the row that contains the applicable host name and click **Edit**. The Edit Default Policy dialog opens.
   - Role policy – Within the Role Policies section, highlight the row that contains the applicable policy name and click **Edit** (if the policy exists) or **Add** (if adding a new role policy). In the “Assign to: Host Groups:” section, click **Browse** to select the host group(s) to which the policy applies, and then click **OK** to return to the Edit Role Policy dialog.
   - Host policy - Within the Host Policies section, enter the applicable IP address and click **Edit**. The Edit Host Policy dialog opens.

3. On the Alarm Categories tab, in the Enabled column, select the check box for each alarm category you want to mitigate. (If the desired alarm category isn’t listed, click **Add** to add it.) This also will cause the alarm category to be visible on the SMC Web App and the SMC client reports.

Note: If you want a particular alarm category to alarm based on security events that have contributed to that category, select the check box in the Alarm column.



4. On the Security Events tab, in the Enabled column, select the check box for each security event you want to mitigate. (If the desired security event isn't listed, click **Add** to add it.) This will also cause the security event to contribute index points to an alarm category.

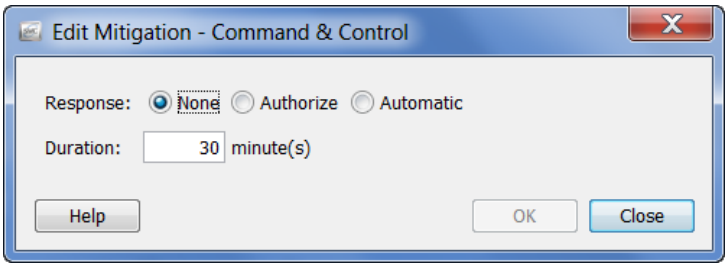
Note: If you want an individual security event to alarm, select the check box in the Alarm column.

Defining Mitigation Actions for Alarms

You can now define the mitigation actions for the desired individual alarms. To do this, complete the following steps.

1. Continuing from step 4 in the previous section, from the Edit Policy dialog that is now open, select the row that contains the alarm for which you want to enable mitigation, and then click **Edit Mitigation**. The Edit Mitigation dialog opens (the contents may vary depending on the alarm).

> **Note:** Lancope provides recommended default settings for each mitigation action. You can change these settings to suit your network needs whenever desired.



2. Click the desired mitigation response based on the following descriptions.

Field	Description
Response	Choose from the following: • None - No mitigation can occur; disables all mitigation actions for the alarm. • Authorize (manual mode) - When the alarm occurs, the StealthWatch System asks you for authorization before starting the mitigation process, and a red “Not Blocking” icon appears in the Mitigation column in the Alarm Table. Use this setting if you prefer to manually block connections. • Automatic - When the alarm occurs, the StealthWatch System immediately starts the mitigation process.
Duration	The length of time (in minutes) that you want the blocking action to be in effect. When this time period expires, the mitigation process ends. **Note:** A duration of 0 (zero) indicates infinity, meaning the mitigation action will be in effect until the mitigation process is manually ended.

3. When you have specified the mitigation settings for the alarm, click **OK**. Your settings are displayed on the Edit Role Policy dialog.
4. Repeat steps 1 through 3 to configure the mitigation settings for any additional alarms.
5. When finished, click **OK,** and then close the remaining dialogs.

Editing Default DefensePro Policies

> **Note:** This procedure is optional.

When the DefensePro device is integrated with the StealthWatch System, the StealthWatch System creates default profiles and adds them to the DefensePro device.

When the mitigation process begins, StealthWatch creates a new policy on the DefensePro device for the current attack with details of the target IP address and mitigation duration value. The policy then uses the default profiles to use to perform mitigation (i.e., policies are built from profiles). Profiles are basically guidelines that Radware uses to determine how to best scrub the attack traffic.

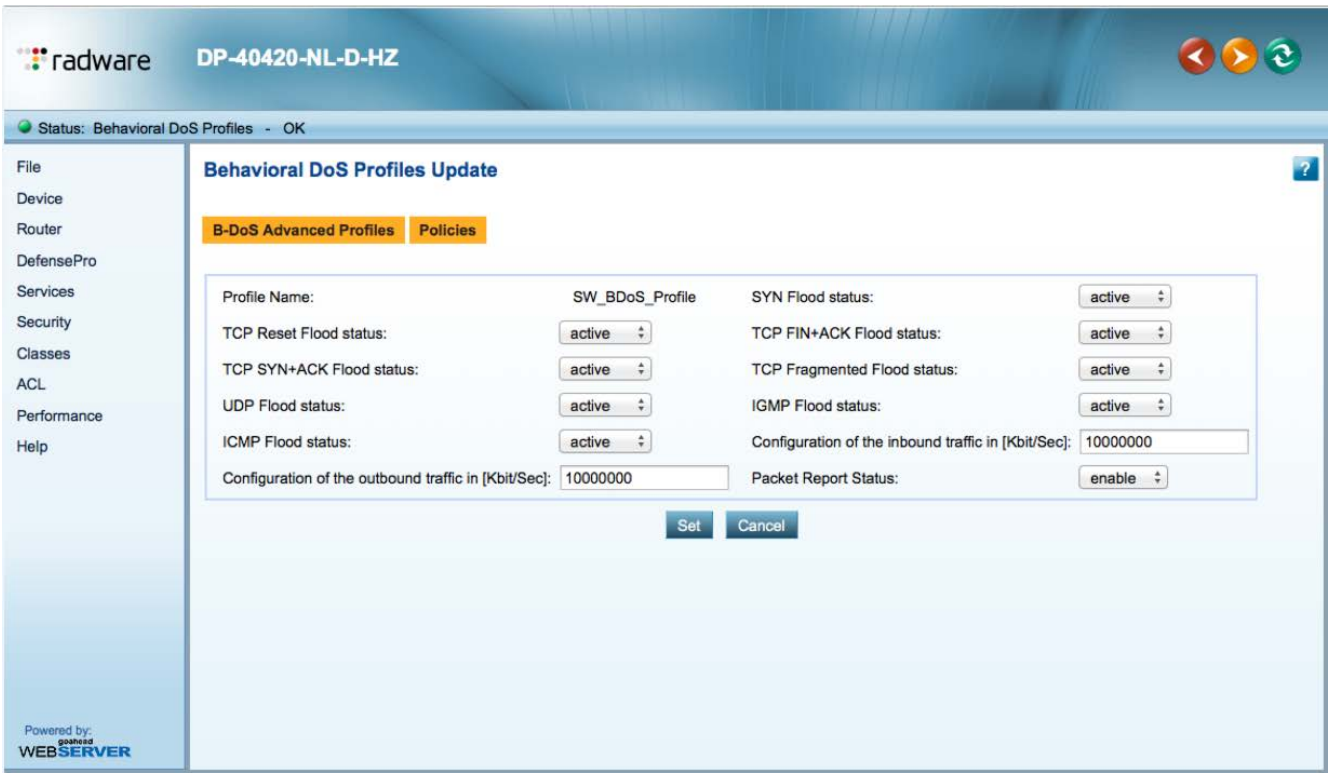
If desired, you can adjust these profiles to make them more specific to your network.

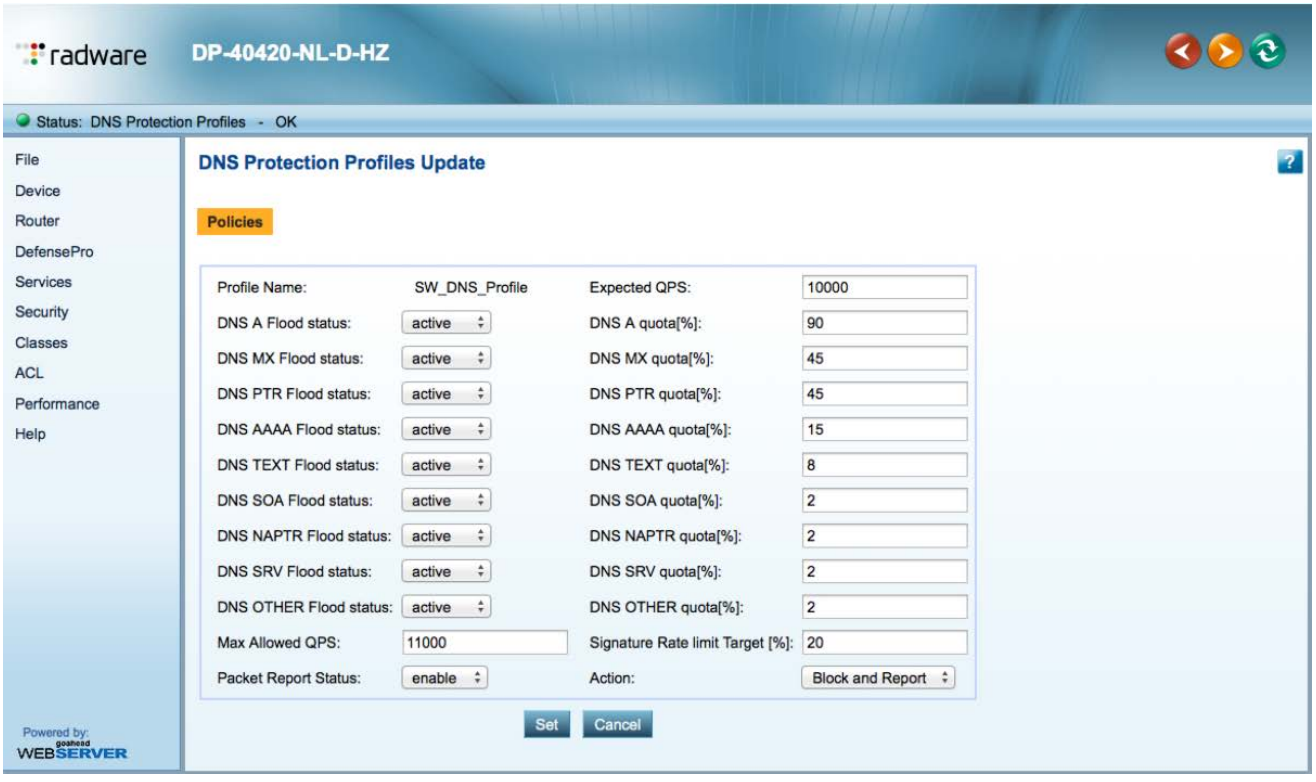
> **Important:** Although you can edit these profiles, ensure that you ***do not*** delete or rename them. If you do, you will not be able to mitigate an attack.

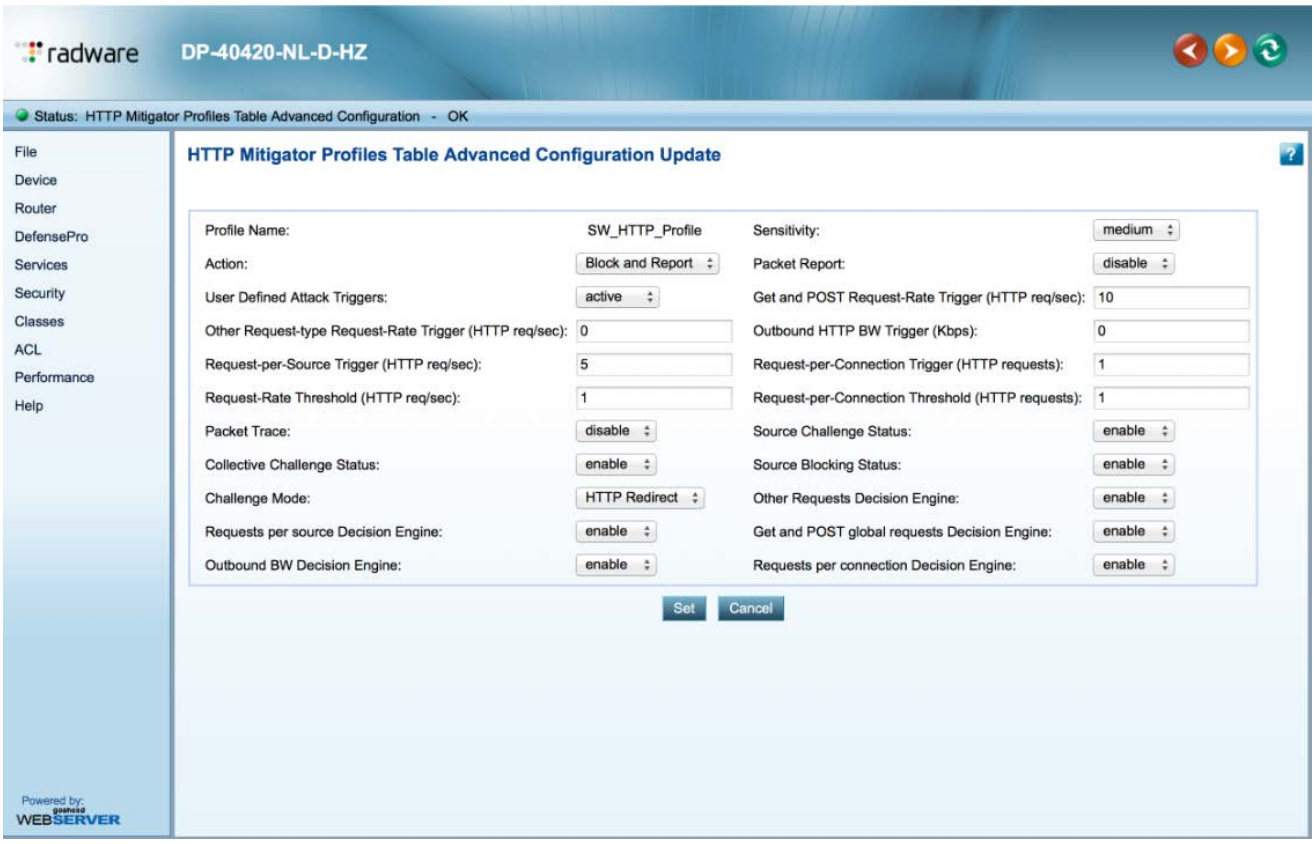
Listed below are the default profiles (along with each profile's navigation path) that are pre-configured in the DefensePro Web user interface.

Profile Name	Navigation Path
SW_BDoS_Profile	(DefensePro > Denial of Service > Behavioral DoS > Behavioral DoS Profiles)
SW_DNS_Profile	(DefensePro > Denial of Service > DNS Protection > DNS Protection Profiles)
SW_HTTP_Profile	(DefensePro > Denial of Service > HTTP Mitigator > Profiles)
SW_SYN_Profile	(DefensePro > Denial of Service > SYN Protection > Profiles > Profiles Parameters)

Refer to the following screens to see how the settings for each of the four profiles are configured.


radware
DP-40420-NL-D-HZ
Status: Behavioral DoS Profiles - OK
File
Device
Router
DefensePro
Services
Security
Classes
ACL
Performance
Help
Powered by:
WEBSERVER
Behavioral DoS Profiles Update
B-DoS Advanced Profiles
Policies
Profile Name: SW_BDoS_Profile
SYN Flood status: active
TCP Reset Flood status: active
TCP FIN+ACK Flood status: active
TCP SYN+ACK Flood status: active
TCP Fragmented Flood status: active
UDP Flood status: active
IGMP Flood status: active
ICMP Flood status: active
Configuration of the inbound traffic in [Kbit/Sec]: 10000000
Configuration of the outbound traffic in [Kbit/Sec]: 10000000
Packet Report Status: enable
Set
Cancel


radware
DP-40420-NL-D-HZ
Status: DNS Protection Profiles - OK
File
Device
Router
DefensePro
Services
Security
Classes
ACL
Performance
Help
Powered by:
WEBSERVER
DNS Protection Profiles Update
Policies
Profile Name: SW_DNS_Profile
Expected QPS: 10000
DNS A Flood status: active
DNS A quota[%]: 90
DNS MX Flood status: active
DNS MX quota[%]: 45
DNS PTR Flood status: active
DNS PTR quota[%]: 45
DNS AAAA Flood status: active
DNS AAAA quota[%]: 15
DNS TEXT Flood status: active
DNS TEXT quota[%]: 8
DNS SOA Flood status: active
DNS SOA quota[%]: 2
DNS NAPTR Flood status: active
DNS NAPTR quota[%]: 2
DNS SRV Flood status: active
DNS SRV quota[%]: 2
DNS OTHER Flood status: active
DNS OTHER quota[%]: 2
Max Allowed QPS: 11000
Signature Rate limit Target [%]: 20
Packet Report Status: enable
Action: Block and Report
Set
Cancel


radware
DP-40420-NL-D-HZ
Status: HTTP Mitigator Profiles Table Advanced Configuration - OK
File
Device
Router
DefensePro
Services
Security
Classes
ACL
Performance
Help
Powered by: WEBSERVER
HTTP Mitigator Profiles Table Advanced Configuration Update
Profile Name: SW_HTTP_Profile
Sensitivity: medium
Action: Block and Report
Packet Report: disable
User Defined Attack Triggers: active
Get and POST Request-Rate Trigger (HTTP req/sec): 10
Other Request-type Request-Rate Trigger (HTTP req/sec): 0
Outbound HTTP BW Trigger (Kbps): 0
Request-per-Source Trigger (HTTP req/sec): 5
Request-per-Connection Trigger (HTTP requests): 1
Request-Rate Threshold (HTTP req/sec): 1
Request-per-Connection Threshold (HTTP requests): 1
Packet Trace: disable
Source Challenge Status: enable
Collective Challenge Status: enable
Source Blocking Status: enable
Challenge Mode: HTTP Redirect
Other Requests Decision Engine: enable
Requests per source Decision Engine: enable
Get and POST global requests Decision Engine: enable
Outbound BW Decision Engine: enable
Requests per connection Decision Engine: enable
Set
Cancel


radware
DP-40420-NL-D-HZ
Status: SYN Protection Profiles Parameters - OK
File
Device
Router
DefensePro
Services
Security
Classes
ACL
Performance
Help
Powered by: WEBSERVER
SYN Protection Profiles Parameters Update
Syn Protection Profiles
Profile Name: SW_SYN_Profile
Authentication Method: safe-reset
HTTP Authentication: enable
HTTP Authentication method: Redirect
Set
Cancel

Starting the Mitigation Process

Once you have determined that an alarm is severe enough to require mitigation, start the mitigation process. If you have set the mitigation action for the alarm to *Authorize* in the Edit Mitigation dialog, you will do this manually. If you set the mitigation action to *Automatic*, the StealthWatch System immediately starts the mitigation process.

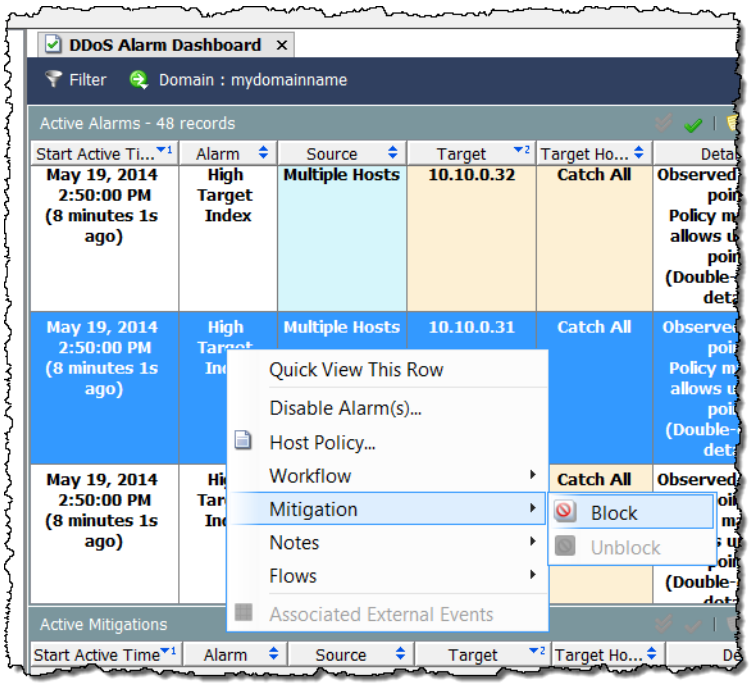
> **Note:** Certain alarm conditions can be set to cause the StealthWatch System to automatically start the mitigation process.

When the mitigation process has been initiated, the StealthWatch System notifies the DefensePro device of the DDoS policies to apply and the BGP route to use. Next, the DefensePro device makes a BGP announcement to the applicable router to start diverting all traffic from the target subnet mask to the DefensePro device. Finally, the DefensePro device applies the DDoS policies to block the attack traffic, and the legitimate traffic is re-routed back to your network.

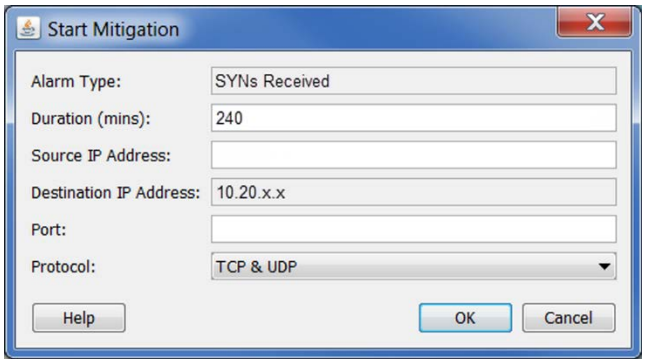
> **Important:** The DefensePro device must be running for the DDoS mitigation feature to work.

To manually start the mitigation process, do the following.

1. From the Main menu, click **Status > Dashboards > DDoS Alarm Dashboard**.
2. In the Alarms Active section, right-click in any column in the row that contains the alarm you want to mitigate and click **Mitigation > Block**.



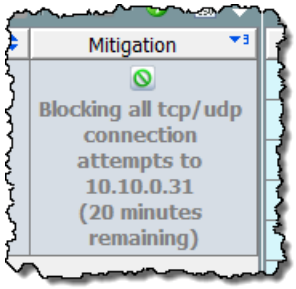
The Start Mitigation dialog opens.



3. Specify the mitigation settings as indicated in the following table. You can customize mitigation actions for each alarm based on a combination of target IP address, protocol, and/or port number. You can even specify how long the mitigation action is to run.

Field	Description
Alarm Type	The type of attack that was detected.
Duration (in minutes)	The length of time (in minutes) that you want the blocking action to be in effect. When this time period expires, the mitigation action stops. **Note:** A duration of 0 (zero) indicates infinity, meaning the mitigation action will be in effect until the mitigation process is manually ended.
Source IP Address	This field is ignored by the DefensePro device.
Destination IP Address	IP address of the host that the suspicious traffic targeted. The system enters this for you if the destination IP address is blocked during mitigation. If using a source-based alarm, this field is blank, and mitigation cannot occur. You can identify the probable target by completing the following steps: 1. In the Active Alarms section on the DDoS Alarm Dashboard, right-click the Source IP. 2. From the pop-up menu, click **Top > Peers > Total**. The Top Peers document is displayed. The peer appearing in the top row is the peer that is generating the highest percentage of traffic and is the probable target. Enter this peer's IP address in the Destination IP Address field on the Start Mitigation dialog.
Port	This field is ignored by the DefensePro device.
Protocol	This field is ignored by the DefensePro device.

4. Click **Ok**, when you have finished entering the mitigation settings. The mitigation process begins. In the Mitigation column in the Active Alarms section, the red "Not Blocking" icon is replaced with the green "Blocking" icon. Information about this alarm is now displayed in a row in the Active Mitigations section.



Monitoring the Mitigation Process

Use APSolute Vision™ to monitor the DefensePro device and use its reporting capabilities to determine the status of an attack. Use the Active Mitigations section on the DDoS Alarm Dashboard to see all alarms that are currently being mitigated. To see all mitigation actions, view the Mitigation Actions document.

To access the Mitigation Actions document, right-click a StealthWatch FlowCollector in the Enterprise tree and click **Status > Mitigation Actions** from the pop-up menu. The Mitigation Actions document opens and displays the following information.

Field	Description
Date/Time	When the blocking action was started.
Appliance	Name of the StealthWatch FlowCollector that reported the original alarm that prompted the blocking action.
Alarm ID	The unique ID number assigned to each alarm.
Alarm Type	Alarm type to which the blocking action responded.
Source Host	IP address of the host that originated the suspicious traffic. **Note:** "Multiple hosts" indicates multiple source IPs.
Source Host Groups	Host groups in which the host that originated the suspicious traffic resides.
Target Host	IP address of the host for which the suspicious traffic was intended. **Note:** "Multiple hosts" indicates multiple target IPs.
Target Host Groups	Host groups in which the host for which the suspicious traffic was intended resides.
Port	Interface through which the suspicious traffic traveled.
Protocol	Protocol used to transport the suspicious traffic.
Duration (minutes)	The length of time (in minutes) that you want the blocking action to be in effect. A 0 (zero) represents infinity, meaning that the connection will be blocked forever.
- continued -	

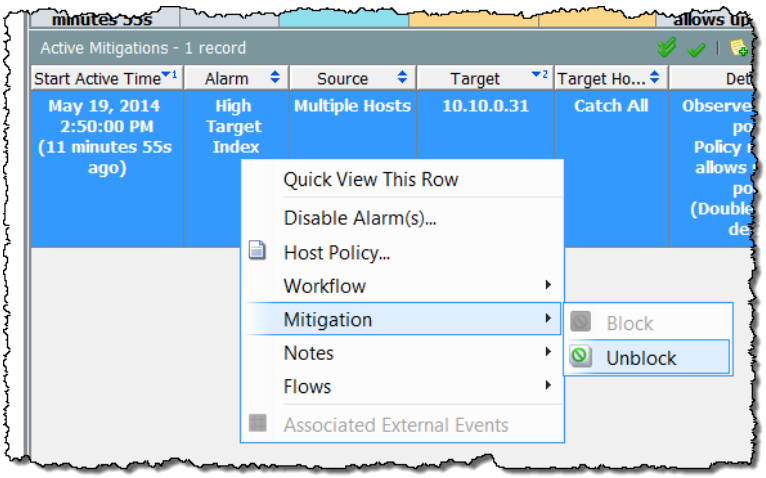
Status	The current status of the blocking action: • Not Started – The blocking action has not started. • Failed – The blocking action has failed. • Blocking – The connection is being blocked. • Unblocked – The blocking action was terminated. • Expired – The connection was blocked for the defined amount of time and is no longer blocked.
Devices	The mitigation devices that are performing the mitigation action.
Domain	Domain in which the StealthWatch FlowCollector resides.
Source Country	Country in which the host that originated the suspicious traffic is located.
Source Host Name	Name, if available, of the host that originated the suspicious traffic.
Source Host Group Path	The hierarchy of all the parent host groups for the host groups in which the source host belongs.
Target Country	Country in which the host is located that was the target of the suspicious traffic.
Target Host Name	Name, if available, of the host for which the suspicious traffic was intended.
Target Host Group Path	The hierarchy of all the parent host groups for the host groups in which the target host belongs.

Ending the Mitigation Process

If you entered a mitigation duration, mitigation will end automatically; otherwise, you end the mitigation process manually when you determine that the attack has terminated.

To manually end the mitigation process, complete the following steps.

1. From the Main menu, click **Status > Dashboards > DDoS Alarm Dashboard**.
2. In the Active Mitigations section, right-click in any column in the row that contains the alarm for which you want to end mitigation and click **Mitigation > Unblock**.



Contacting Support

If you need technical support, please do one of the following:

- Contact your local Lancope partner.
- Send an email requesting assistance to support@lancope.com.
- Call +1 800-838-6574.
- Submit a case using the Support form on the Customer Community Web site (community.lancope.com).

You will need to provide the following information:

- Your name
- Your company name
- Location

Document Feedback

If you have comments about this document, please contact Lancope at support@lancope.com. We appreciate your feedback.