Getting Started with ThreatSTOP

ThreatSTOP® delivers automated firewall policy updates powered by real-time threat intelligence. This guide will enable you to get started and immediately begin protecting every device on your network.

1. Create a Protection Policy
2. Add a Device
3. Configure the Device
4. View Reports of Blocked Threats
5. Setup Alerts

QSG Version 1.1. Last Updated Sep. 15, 2016

ThreatSTOP™

ThreatSTOP

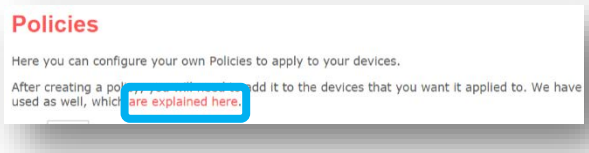
Create a Protection Policy Block List

ThreatSTOP offers fully customizable self-managed block policies to fit an array of security needs. Follow the steps below to create a custom protection policy that suits your device-specific needs.

1 Login and open the Policies & Lists tab

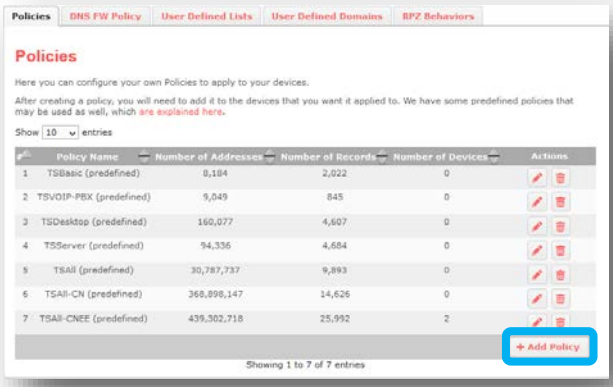
Enter your ThreatSTOP username and password to login to the customer portal, click on the **Policies & Lists** tab at the top left of the page.

ThreatSTOP encourages users to create custom policies that match their security needs. However, pre-defined policies are available, you can learn about them by clicking the **explained here** link.

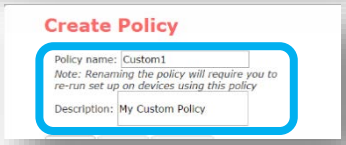


2 Add a custom policy and give it a name

Click **Add Policy** on the bottom right of the **Policies** tab.

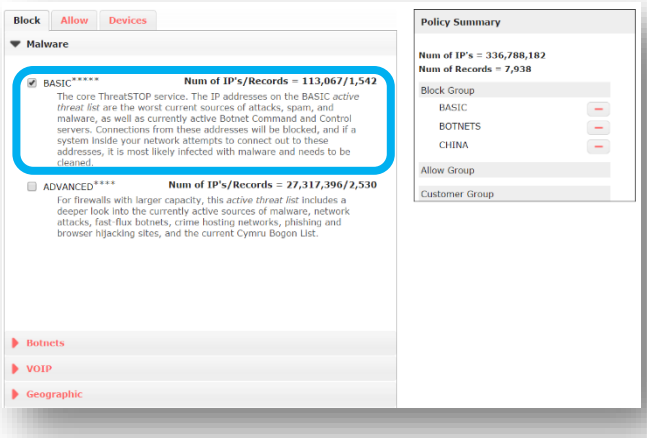


Enter a **Policy Name** and **Description**



3 Select threat categories to block

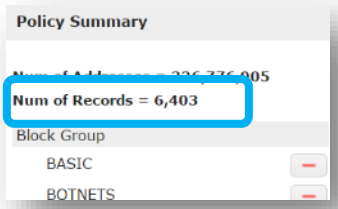
Browse through the available categories and select the threat lists you want to include in your custom policy. Use the checkbox to add or remove lists from the policy.



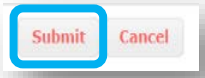
4 Review and submit the changes to your custom block policy

Once you've added the threat lists you want to protect against, you should review the total **Number of Records** it contains to ensure it does not exceed the max policy size limits of your network device.

Consult the documentation for your device and adjust your policy as needed.



Click **Submit** when you've finished making additions or changes to the policy.



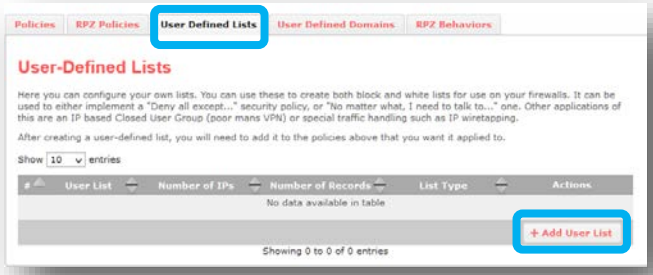
ThreatSTOP

Create a Protection Policy Allow List

You can tailor protection for your network by creating your own self-managed allow lists and block lists. Follow the steps below to create a custom allow list and add it to the policy you just created.

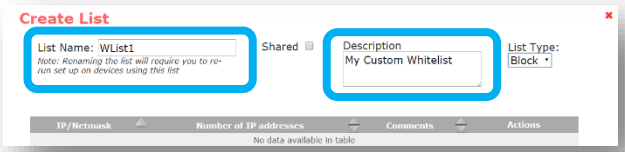
1 Open the Add User List page

Open the **Policies and Lists** page, and select the **User Defined Lists** tab. At the bottom right, click on **Add User List**.

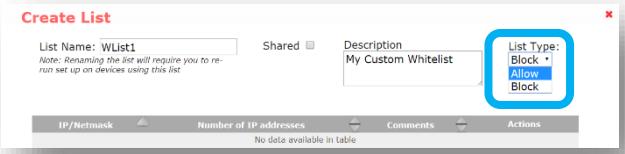


2 Name your custom allow list

Enter a name for your list in the **List Name** field, and add a **Description**.

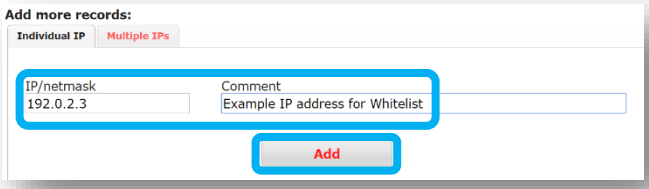


Since this will be an allow list, select **Allow** from the **List Type** drop-down menu. (*For custom block-lists you would select Block instead*).

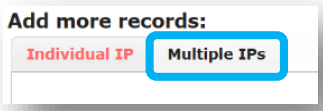


3 Add IP addresses to your policy

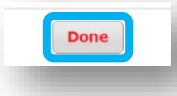
In the **IP/netmask** field add an IP address you want included in this allow list. Add a **Comment** for the IP address, and click **Add** to save changes.



Add multiple **IP/Netmasks** using the **Multiple IPs** tab to save time.

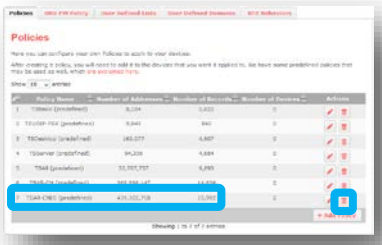


When you have finished adding IPs click **Done** to commit all additions to the list.

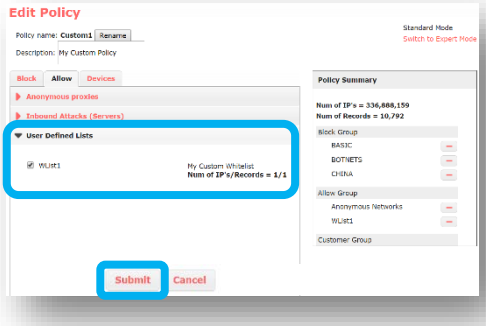


4 Add the allow list to your policy

Click the **Edit** icon next to your custom policy in the **Policies** tab of the **Policies & Lists** page.



In the **Allow** tab of **Edit Policy**, open the **User Defined Lists** category. Check the box next to the allow list you created. Click **Submit** to save changes.

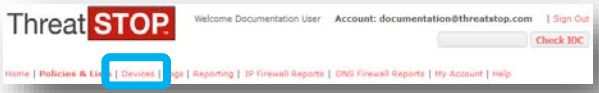


Add a Network Device

Once you have created a protection policy, you will then select the device or network appliance that will run the ThreatSTOP Firewall Service. Follow the steps below to add a supported device.

1 Open the Devices tab

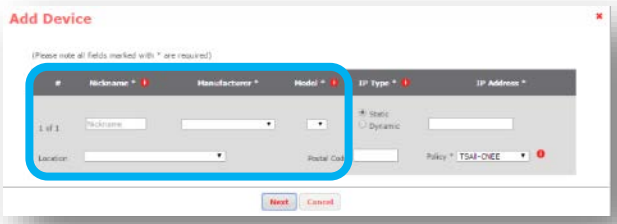
Click on the **Devices** tab toward the top of the page.



Click on the **Add Device** button at the bottom right of the window.

2 Complete the Add Device fields

Complete the fields by entering or selecting your device information in the fields provided.

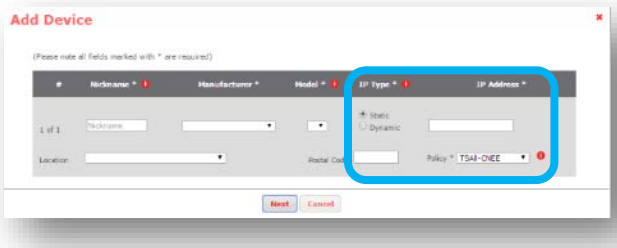


Enter a **name** for your device and select the **manufacturer** and **model** from the drop-down menus. Next, select your **location** and enter your **postal code**.

3 Add the public IP address and select your policy

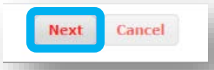
Add the **public IP address** of your device and select the **IP type**[1].

If you created a custom policy in the previous steps, select it from the **Policy** drop-down list.



Alternatively, you can use one of the pre-defined policies. Descriptions for the pre-defined policies can be found by clicking here.

When you've completed all fields click **Next** to save the changes.



[1] If your public IP is dynamic, you'll need to sign up for a dynamic DNS service such as No-IP.com. Once setup, enter your dynamic hostname in this field. If you're unsure of your public IP address, visit this link to discover it.

Configure the Network Device

After selecting and adding your device, you will configure your device to run the ThreatSTOP service. Follow the steps below to configure your device.

1 View your newly added device

Click on the **Devices** tab again, you should be able to view your newly added device details in the **Devices Under ThreatSTOP Protection** window. You are now ready to configure the device.

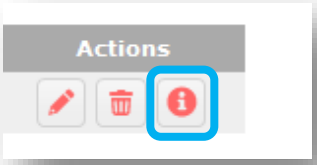
2 Allow time for your device to register

The registration of new devices with ThreatSTOP can take **up to 15 minutes** following the completion of the installation. While this new device registration is taking place, review these useful resources:

- ThreatSTOP FAQs
- Resources & Case Studies
- ThreatSTOP Documentation Center

3 Open the installation documents

Installation information is provided for your specific device based on the manufacturer and model.



To the right of your device details, click on the information icon found in the **Actions** section.

Follow the instructions step-by-step to complete the installation and configuration of your device.

4 Uploading logs to enable reporting

On the next page we'll cover the powerful reporting that empowers you to better understand the inbound and outbound attacks blocked by the ThreatSTOP service.

We strongly recommend you leave log uploading in the default enabled state – **if you disable log uploading, reporting will not function.**

ThreatSTOP

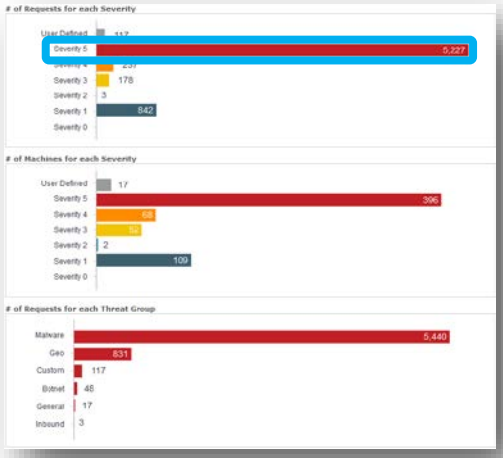
View Blocked Threats (DNS Firewall Reports)

ThreatSTOP is now automatically protecting your network using the custom policy you created. You can view reports showing results of the security enforcement taking place. Allow a minimum of 24-48 hours* before checking your report (depending on the protection policy to be enforced on the network traffic). Follow the steps below to view the threats being blocked on your network.

1 Open the DNS Firewall Reporting section

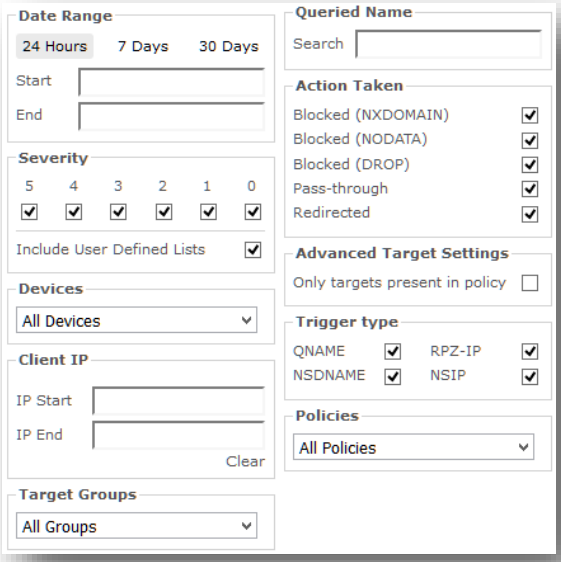
Click on **DNS Firewall Reports** to open and view summary reports for your device.

Outbound connection attempts blocked by ThreatSTOP are displayed with default filter values.



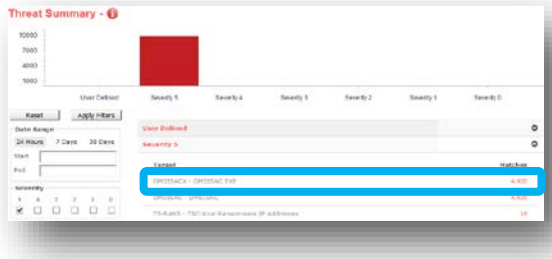
2 Select Report Parameters

Choose the **Date Range**, **Severity** level, protected **Devices**, **Client IP** range, **Target Groups**, **Queried Name**, **Action Taken**, **Trigger type**, or **Policies** by which to filter results and click **Apply**.



3 Initial summary data can be refined

By clicking on graph data you can drill down into threat intelligence to gain insight into specific threat types.



*__Note__: In some cases manual setup of reporting is required.

4 Drill down to view more detail

You can drill down to view more details in each of the summary screens. Click **on the name of a threat** to display a list of all connection attempts and data made by that threat.

From here you can also click on URI information to learn more about why ThreatSTOP is classifying this communication attempt as a threat.

ThreatSTOP

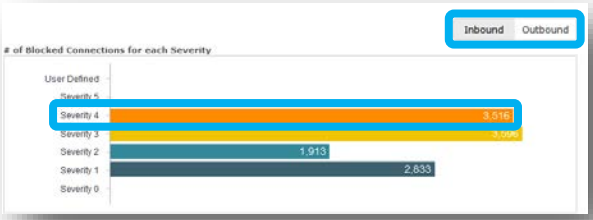
View Blocked Threats (IP Firewall Reports)

ThreatSTOP is now automatically protecting your network using the custom policy you created. You can view reports showing results of the security enforcement taking place. Allow a minimum of 24-48 hours* before checking your report (depending on the protection policy to be enforced on the network traffic). Follow the steps below to view the threats being blocked on your network.

1 Open the IP Firewall Reporting section

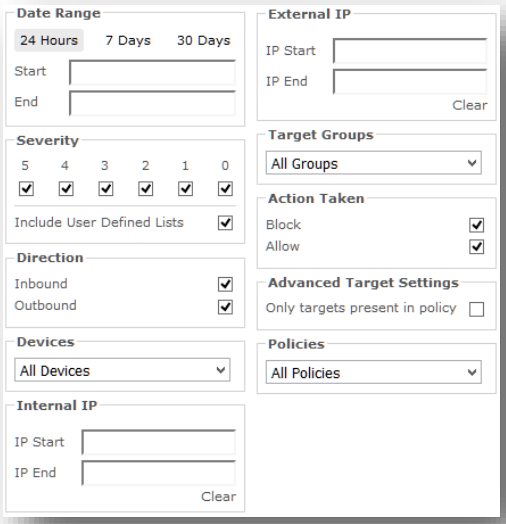
Click on **IP Firewall Reports** to open and view reports for your device.

The inbound communications blocked by ThreatSTOP are displayed by default. Outbound can be seen by clicking **Outbound**. Details can be seen by clicking on a bar in the graph.



2 Select Report Parameters

Choose the **Date Range**, **Severity** level, **Device**, **IP address**, **Target Group**, **Actions**, **Policy** and whether you want to view details for **Inbound** or **Outbound Connections**. Click **Apply** this will update the graphs based on your criteria.



3 Initial summary data can be refined

By clicking on graph data you can drill down into threat intelligence to gain insight into specific threat types.

*__Note__: In some cases manual setup of reporting is required.

4 Drill down to view more detail

You can drill down to view more details in each of the summary screens. Click **on the name of a threat** to display a list of all connection attempts and data made by that threat.

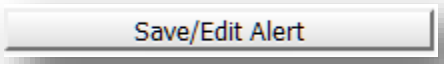
From here you can also click on URI information to learn more about why ThreatSTOP is classifying this communication attempt as a threat.

Alerts

One of issue that has been encountered in the Information Security space is Alarm Fatigue. A state in which alarms and warnings are tuned out by the person receiving them due to excessive false warnings. To help alleviate this, ThreatSTOP has created an Alert system that can have a cool off period. This allows the user to turn an alert off for a test period. If it returns it can be investigated further and remediated.

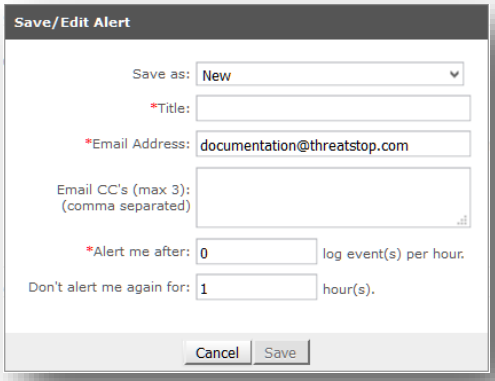
1 Open the report for which you want to set the alert

Click on **IP Firewall** or **DNS Firewall Reports** to open and view reports for your device. Set your filters to view the details for which you would like to be alerted. Then click **Save/Edit Alert**.



2 Select Report Parameters

If this is a new report set the **Save as** field to **New**, provide a **Title**, at least one **Email Address** to receive copies of the alert, and how many times an event should be triggered before sending you an alert.

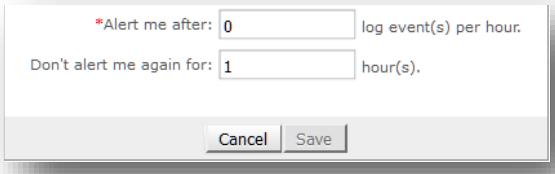


3 Alert data appears in email

By clicking on graph data you can drill down into threat intelligence to gain insight into specific threat types.

4 Set a Cool off period

If you find that an Alert is firing at a questionable rate set the **Don't alert me again for X hour(s)** to a new value and click **Save**.



Next Steps with ThreatSTOP

You've just added a powerful layer of protection, and the results you will experience can be immediate.

Your network is now blocking known malicious attacks and new emerging threats with ThreatSTOP's automated actionable threat intelligence. Continuous updates for your custom security policy will be delivered automatically and enforced by your network infrastructure.

To verify the ThreatSTOP service is blocking threats successfully, visit bad.threatstop.com from a host connected to the device with the ThreatSTOP service installed. This is a non-malicious site we've setup for testing purposes. If the service is working, you should not be able to view the page.

Your network security and satisfaction are very important to us. ThreatSTOP's Customer Success Team is standing by to ensure we deliver both.

Don't hesitate to contact us for assistance, or with any questions you have. We'd love to hear from you!

Customer Success Team

success@threatop.com

or

1 (855) 958-7867