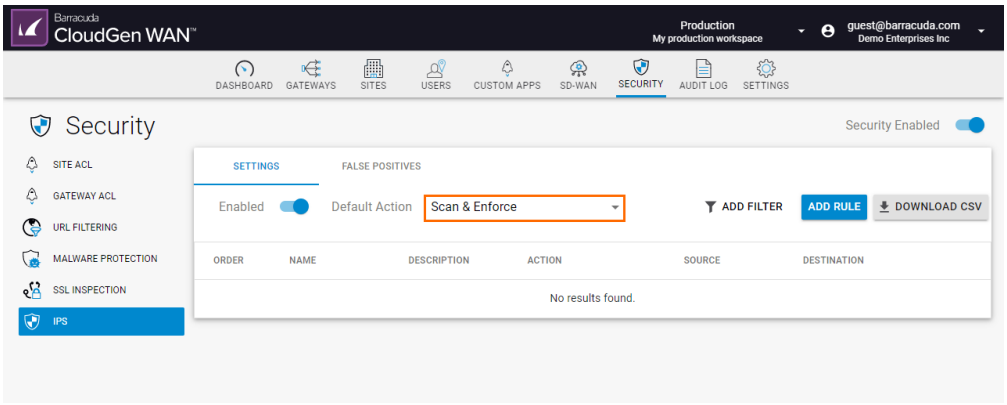
IPS

https://campus.barracuda.com/doc/93882905/

The Intrusion Prevention System (IPS) actively monitors local and forwarding traffic for malicious activities and can also block suspicious traffic. The IPS engine analyzes network traffic and continuously compares the bitstream with its internal signatures database for malicious code patterns.



IPS Features

TCP Stream Reassembly

The CloudGen WAN engine provides support for TCP Stream Reassembly (SRA). In general, TCP streams are broken down into TCP segments that are encapsulated in IP packets. By manipulating how a TCP stream is segmented, it is possible to evade detection, for example, by overwriting a portion of a previous segment within a stream with new data in a subsequent segment. This method allows hackers to hide or obfuscate the network attack. The CloudGen WAN engine receives the segments in a TCP conversation, buffers them, and reassembles the segments into a correct stream, for example, by checking for segment overlaps, interleaved duplicate segments, invalid TCP checksums, and so forth. Afterwards, the CloudGen WAN engine passes the reassembled stream to the IPS engine for inspection.

URL Obfuscation

The IPS engine provides various countermeasures to avert possible network attacks based on the following URL encoding techniques:

- Escape encoding (% encoding)
- Microsoft %u encoding
- Path character transformations and expansions (/./ , //, \ )
- Premature URL ending

- Long URL
- Fake parameter
- TAB separation
- FTP Evasion

The IPS engine can avert FTP exploits where the attacker tries to evade the IPS by inserting additional spaces and Telnet control sequences in FTP commands.

TCP Split Handshake

The IPS engine provides an evasion countermeasure technique that can block the usage of TCP split-handshake attacks. Although the TCP split handshake is a legitimate way to start a TCP connection (RFC793), it can also be used by hackers to execute various network attacks by gaining access to the internal network by way of establishing a trusted IP connection, thus evading firewall and IPS policies.

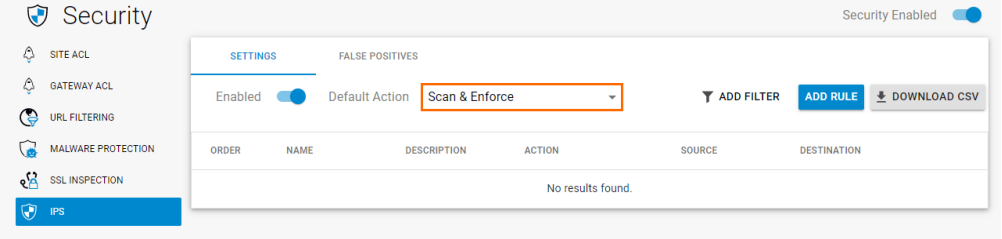
Before You Begin

- If you want to select users or groups in the policies, you must first connect your Azure Active Directory. For more information, see How to Connect Your Azure Active Directory with Barracuda Cloud Control.

Settings

Select the Default Action

1. Open https://cloudgenwan.barracudanetworks.com/ and log in with your existing Barracuda Cloud Control account.
2. Go to **SECURITY > IPS > SETTINGS**.
3. Select the default action.
   - **Do Not Scan** – IPS does not scan traffic matching the criteria.
   - **Scan & Log** – IPS only scans and logs the events.
   - **Scan & Enforce** – IPS is enforced.



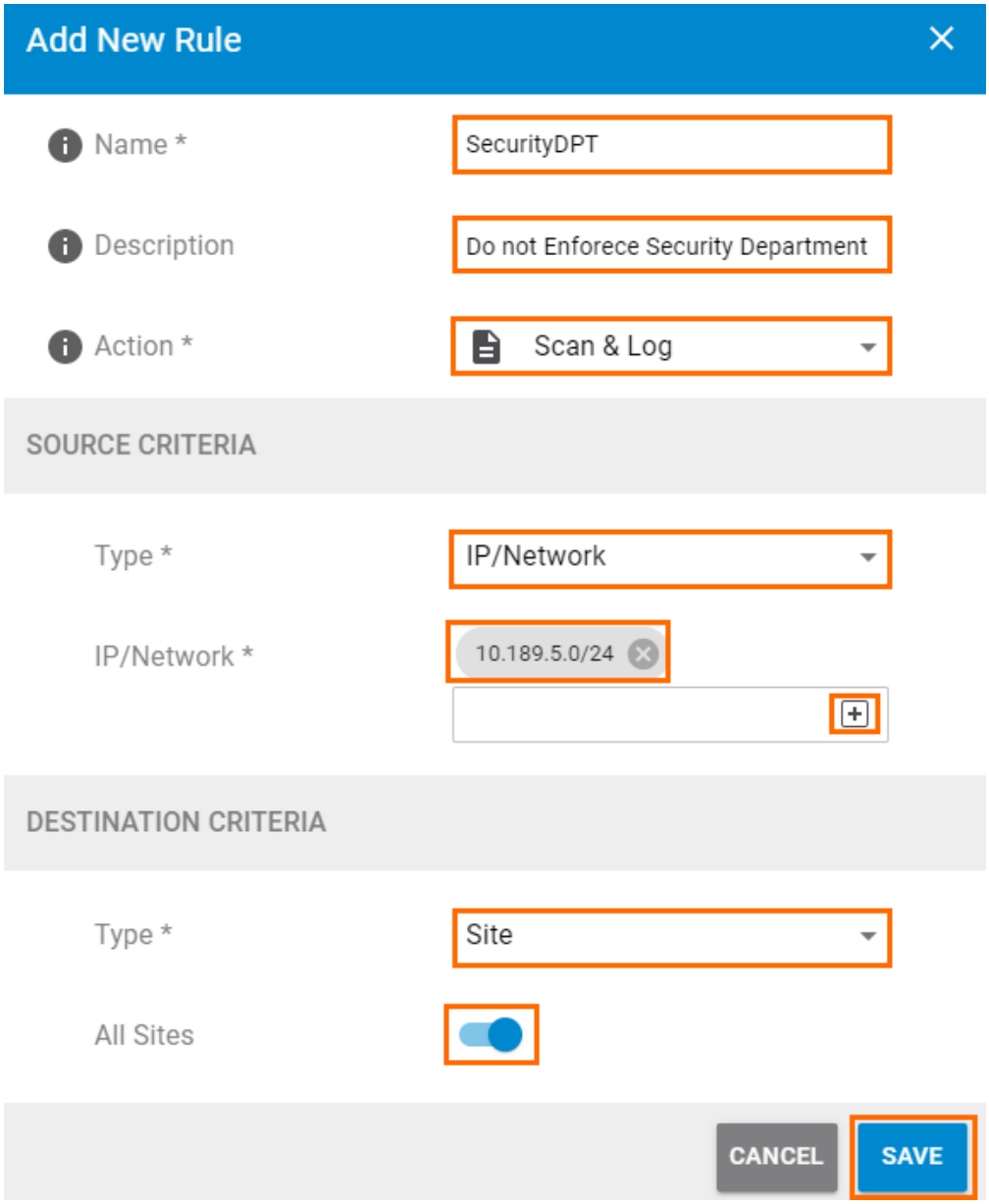
Add a Rule

1. Open https://cloudgenwan.barracudanetworks.com/ and log in with your existing Barracuda

Cloud Control account.
2. Go to **SECURITY > IPS > SETTINGS**.
3. Click **ADD RULE**:
4. The **Add New Rule** window opens. Specify values for the following:
   - **Name** – Enter a name.
   - **Description** – Enter description.
   - **Action** – Select an action:
     - **Do Not Scan** – IPS does not scan traffic matching the criteria.
     - **Scan & Log** – IPS only scans and logs the events.
     - **Scan & Enforce** – IPS is enforced.

   SOURCE CRITERIA
   - **Type** – Select a type. You can choose between IP/Network and Site.
   - **IP/Network** – Enter an IP or network address.

   DESTINATION CRITERIA
   - **Type** – Select a type. You can choose between IP/Network and Site.
   - **Application** – S elect an application. For more information, see How to Create Custom Applications.



5. Click **SAVE**.

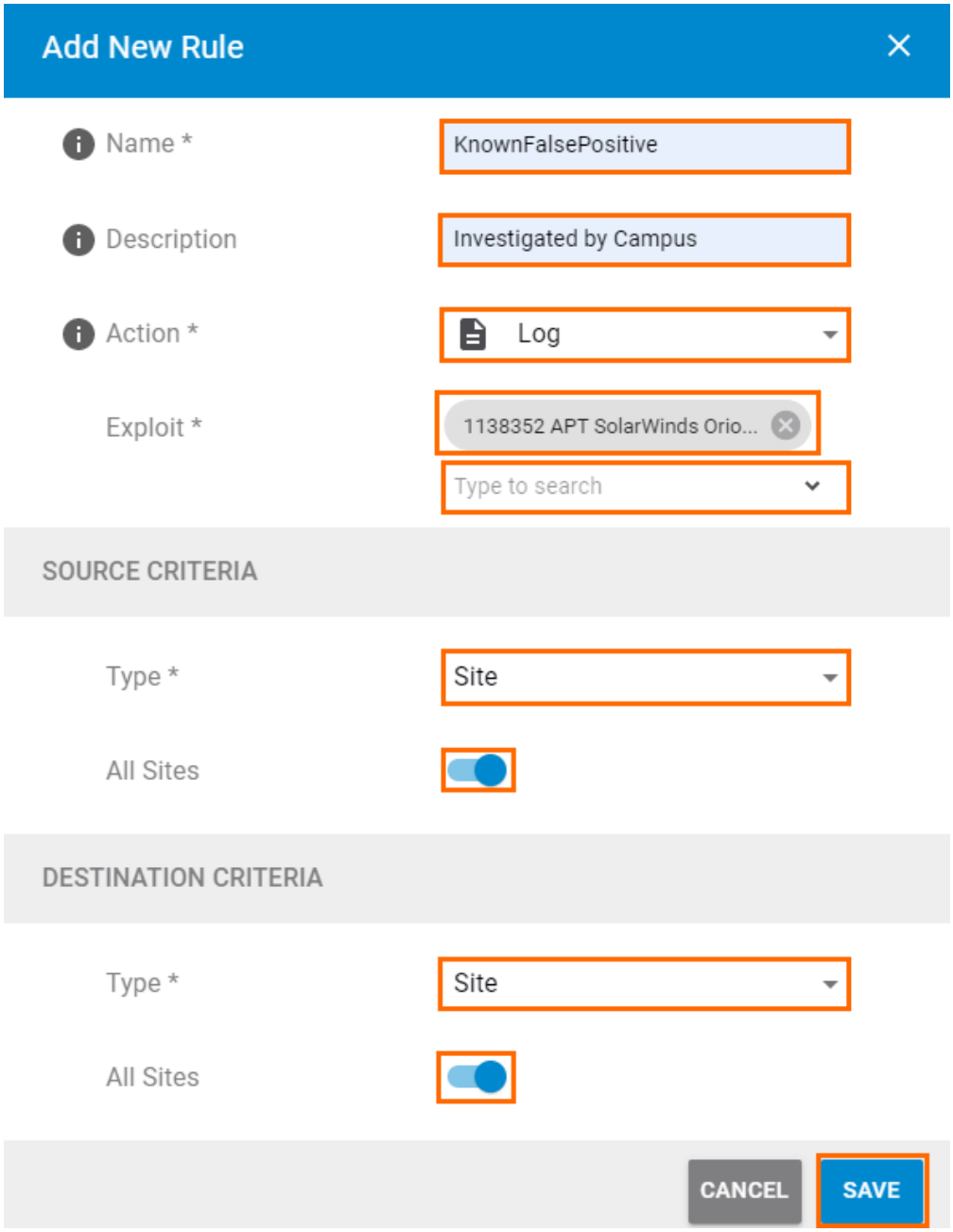
False Positives

In this section, you can configure the actions for false positives.

Add a Rule

1. Open https://cloudgenwan.barracudanetworks.com/ and log in with your existing Barracuda Cloud Control account.
2. Go to **SECURITY > IPS > FALSE POSITIVES**.
3. Click **ADD RULE**:

4. The **Add New Rule** window opens. Specify values for the following:
   - **Name** – Enter a name.
   - **Description** – Enter description.
   - **Action** – Select an action:
     - **Ignore** – IPS ignores this exploit.
     - **Log** – IPS only scans and logs the events.
     - **Enforce** – IPS is enforced.
   - **Exploit** – Select an exploit from the drop-down list, or type to search.
     SOURCE CRITERIA
   - **Type** – Select a type. You can choose between IP/Network and Site.
   - **IP/Network** – Enter an IP or network address.
     DESTINATION CRITERIA
   - **Type** – Select a type. You can choose between IP/Network and Site.
   - **Application** – S elect an application. For more information, see How to Create Custom Applications.


Add New Rule
Name *
KnownFalsePositive
Description
Investigated by Campus
Action *
Log
Exploit *
1138352 APT SolarWinds Orio...
Type to search
SOURCE CRITERIA
Type *
Site
All Sites
DESTINATION CRITERIA
Type *
Site
All Sites
CANCEL
SAVE

5. Click **SAVE**.

Figures