# brocade-update-firewall

NPM module to update banned IP addresses list in Brocade's RBL service protection class.

### Emerging Threats fwip rules

Downloads [Emerging Threats](https://www.proofpoint.com/us/threat-intelligence-overview) raw IPs for firewall block lists, and then updates the RBL protection class in Brocade. This service protection class is applied to virtual servers to reject traffic from know bad IP addresses.

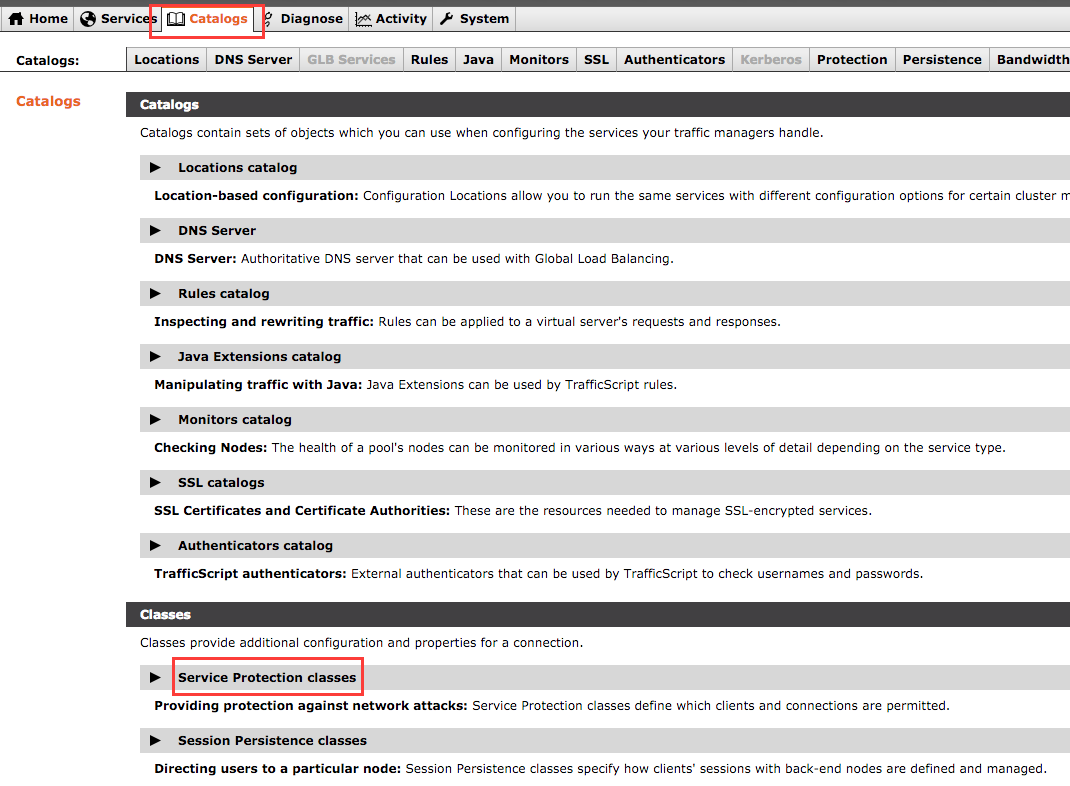
## Requirements

The following components are required to run this module –

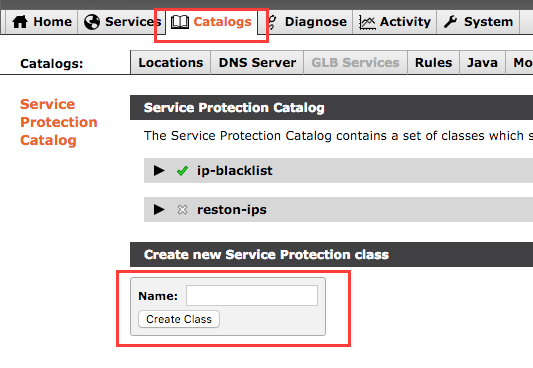
* git
* nodejs (5.9.1 or above)

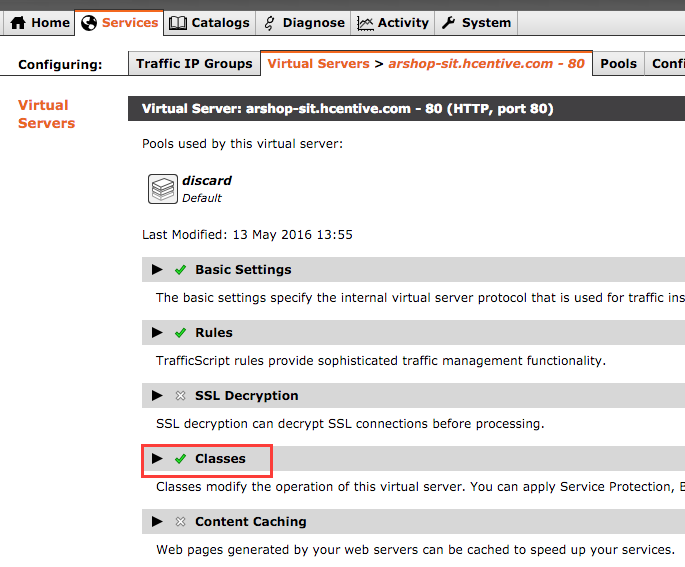
## Installation and configuration

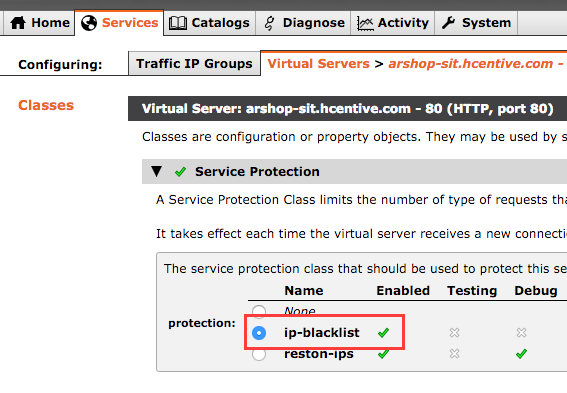
Create a Service Protection Class from the Brocade console by navigating to Catalogs and then clicking Service Protection Classes



Catalogs -> Service Protection classes

Enter a name for your service protection class and click Create Class 

Attach this class to a virtual server 

Select your service protection class and click Update 

Check out the repository from git -

$ git clone https://git.demo.hcentive.com/brocade-update-firewall

Go to the brocade-update-firewall directory and update configuration attributes to connect to the Brocade API -

$ cd brocade-update-firewall

Make the following changes to configure Brocade API endpoint –

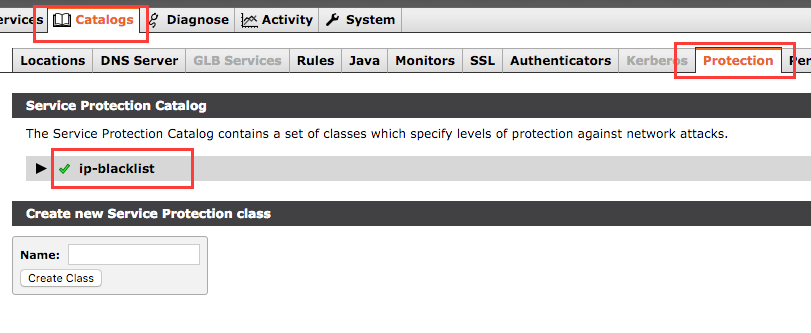
* Rename conf/brocade.json.template to conf/brocade.json.
* Replace API\_HOST with the private IP address of the Brocade load balancer.
* Replace YOUR\_API\_USERNAME with the username that has permissions to make API calls, e.g. restapi.
* Replace YOUR\_API\_PASSWORD with the password for the API user.

Run npm install to install dependencies and executable command to update the firewall. Run the update-fw command from the installation directory to update the blacklist -

$ npm install  
$ update-fw  
info: Updating ip-blacklist with 1644 addresses  
info: Updated ip-blacklist with 1644 addresses

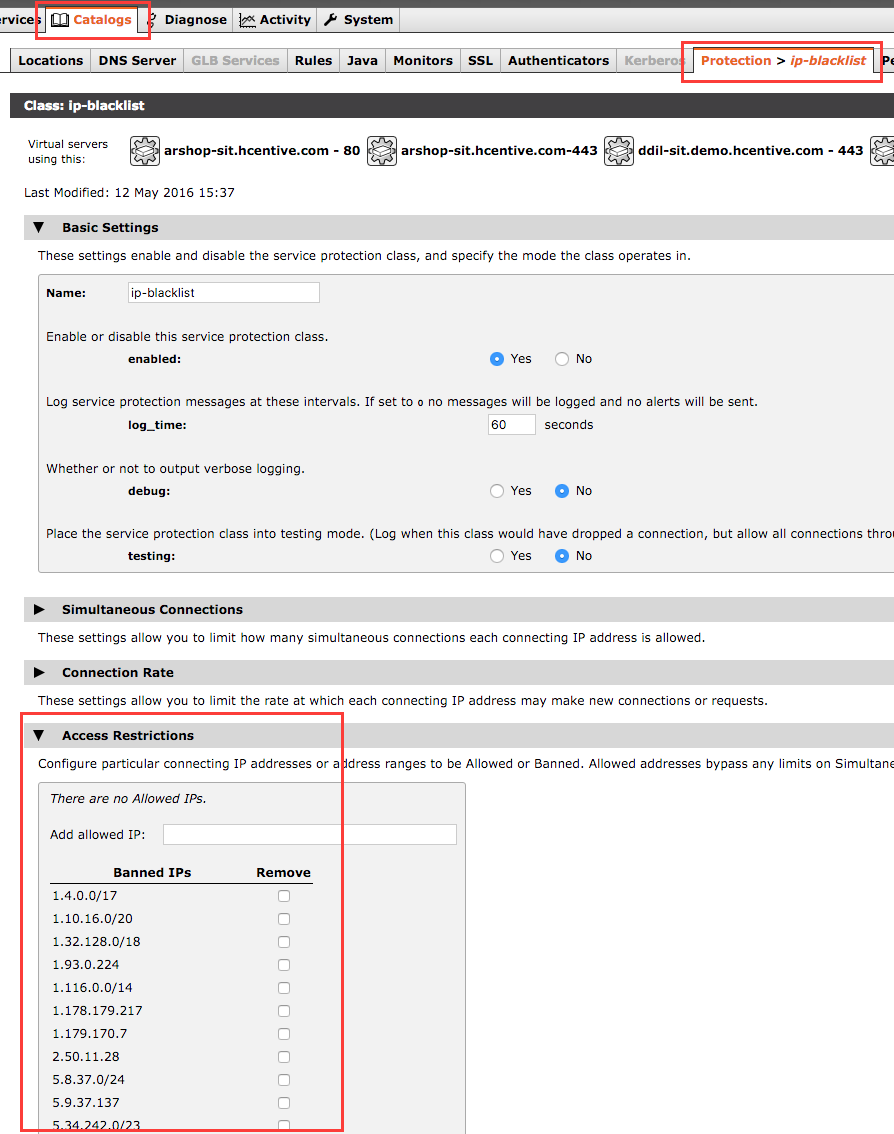
## Validation

Login to the Brocade console, navigate to Catalogs and click Service Protection Classes and select the ip-blacklist class from Service Protection Catalog



ip-blacklist

Drill down to the Access Restrictions section to view a list of banned CIDRs



Banned IPs

## Troubleshooting

### Remove an IP address from the banned IPs list

To remove an IP address from the banned IPs list click on the Remove checkbox next to the IP address and click Update under the Apply Changes section at the bottom of the page.

NOTE: The removed IP address will be added back to the protection class on the next run of this utility unless the IP address is removed from Emerging Threats' blacklist.

### Logs

Logs are written to info.log and error.log files the logs folder as default. The change location and names of the log files, update attribute values in default.json.