BIG-IP AFM Blacklisting Magic

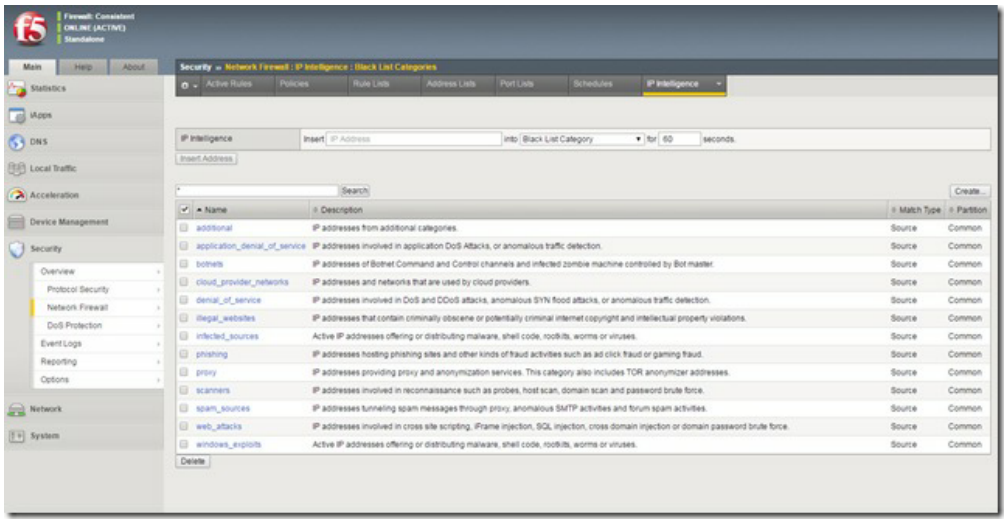
John Wagnon, 2016-31-03

Have you ever wondered which IP addresses floating around out there on the Internet are the good ones? The benign ones? The malicious ones? You get the idea. Peter Silva recently published an article that discusses the IP Intelligence feature of the BIG-IP where each IP address is examined and an intelligent decision is made about how good or bad the address is. As the BIG-IP compiles all the data from the IP Intelligence feeds, it can automatically add IP addresses to one or more Blacklist categories for a specified period of time.

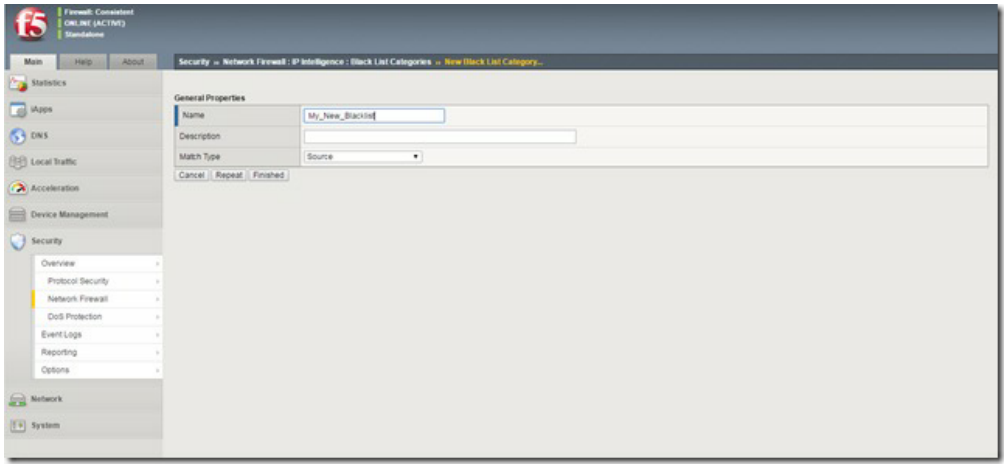
> **Blacklist** *(noun)* : a list of items (usernames, IP addresses, etc) that are denied access to a system

It's nice to know that you don't have to manually add all the Blacklist IP addresses any more. However, you certainly still have the flexibility to add items to a Blacklist category if you'd like.

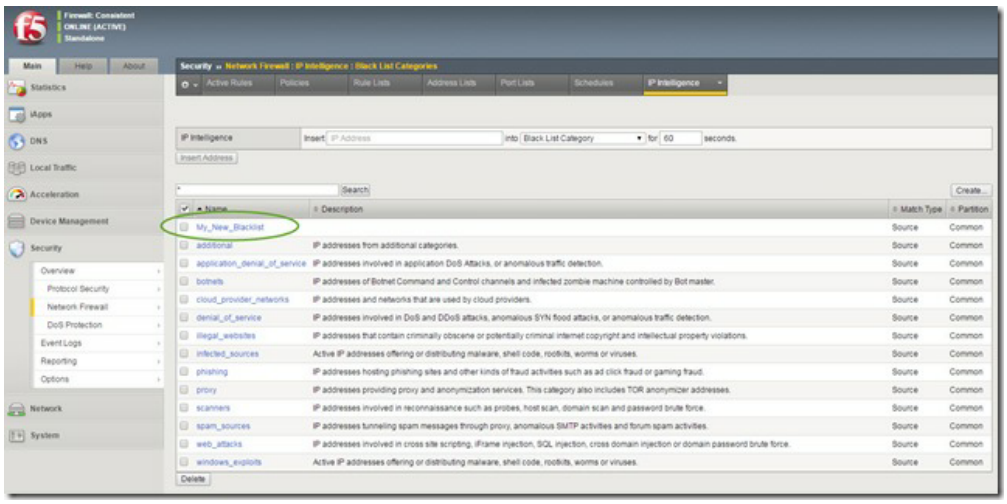
To view the Blacklist category names on the BIG-IP AFM, navigate to **Security >> Network Firewall >> IP Intelligence >> Black List Categories** and you will see the default categories listed there. The BIG-IP AFM comes preloaded with several Black List categories (i.e. botnets, phishing, spam_sources, etc). Check out the screenshot below for a view of the Black List category page.



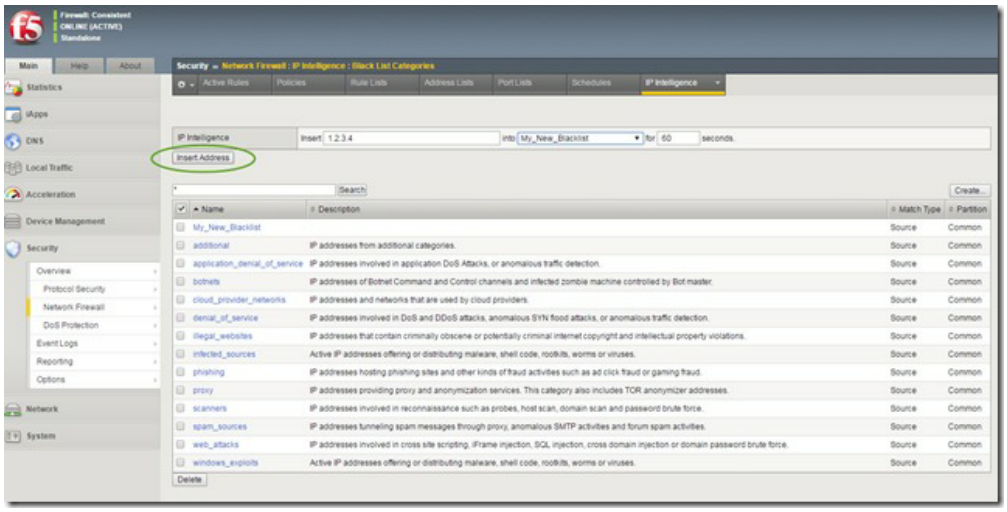
In addition to the categories already loaded on the BIG-IP, you can create your own categories as well. To do this, simply click the "Create" button on the upper/right portion of the Black List Category page, and you can create a name, description, and Match Type (Source, Destination, or Both) for your category. These categories are important when creating IP Intelligence policies because, when you create an IP Intelligence policy, you can specify what action to take on an IP address from a particular feed list when it matches an IP address in one of your Black List categories. See the screenshot below for details on creating a new Black List Category.



Now that you have a new Black List category, it will show up in the full listing of Black List categories. Notice in the screenshot below that my newly created Black List Category is listed.

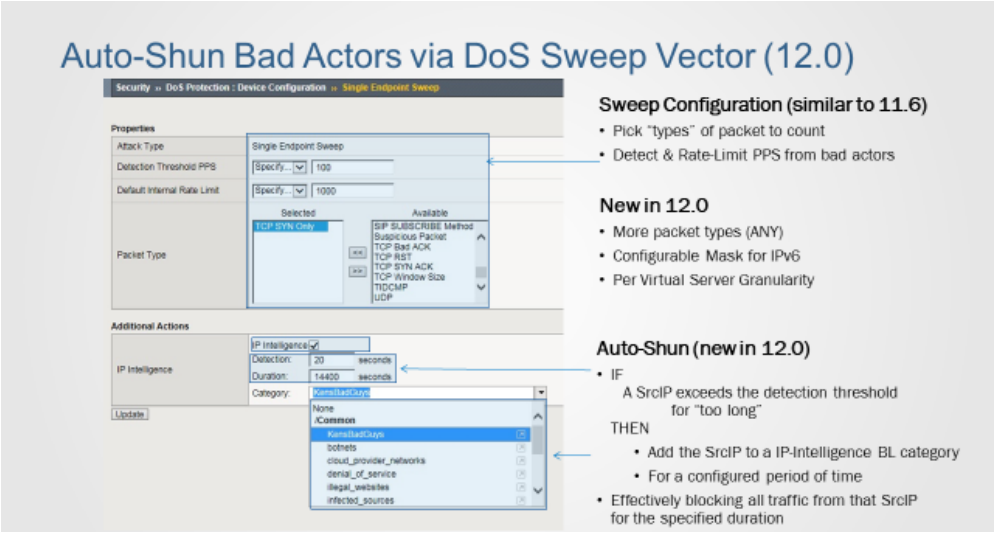


While the BIG-IP AFM will take care of automatically adding bad IP addresses to the various Black List Categories, you can still manually add IP addresses and assign them to a Black List Category as well. To do this, you navigate to the Black List Category page and type in the IP address in top portion of the page and select a Black List Category from the dropdown menu. Finally, you specify (in seconds) the amount of time the IP address should stay in that particular Black List category. See the screenshot below for details:



Auto-Shun in Version 12.0

In BIG-IP version 12.0, the "auto-shun" feature was introduced. It allows you to configure a DoS protection profile to watch for a Source IP address and, if it exceeds the detection threshold for a given period of time, it is automatically added to a Blacklist category for a configurable period of time. See the chart below for more details:



Many organizations struggle with maintaining a good and timely list of bad IP addresses, but now you have the power of the BIG-IP AFM that can do it all for you automatically!

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com