Firepower Data Path Troubleshooting Phase 3: Security Intelligence

Contents

Introduction

This article is part of a series of articles which explain how to systematically troubleshoot the data path on Firepower systems to determine whether components of Firepower may be affecting traffic. Please refer to the Overview article for information about the architecture of Firepower platforms and links to the other Data Path Troubleshooting articles.

This article covers the third stage of the Firepower data path troubleshooting, the Security Intelligence feature.

Prerequisites

- This article pertains to all of the currently supported Firepower platforms
- Security Intelligence for URLs and DNS was introduced in version 6.0.0

Troubleshooting the Firepower Security Intelligence Phase

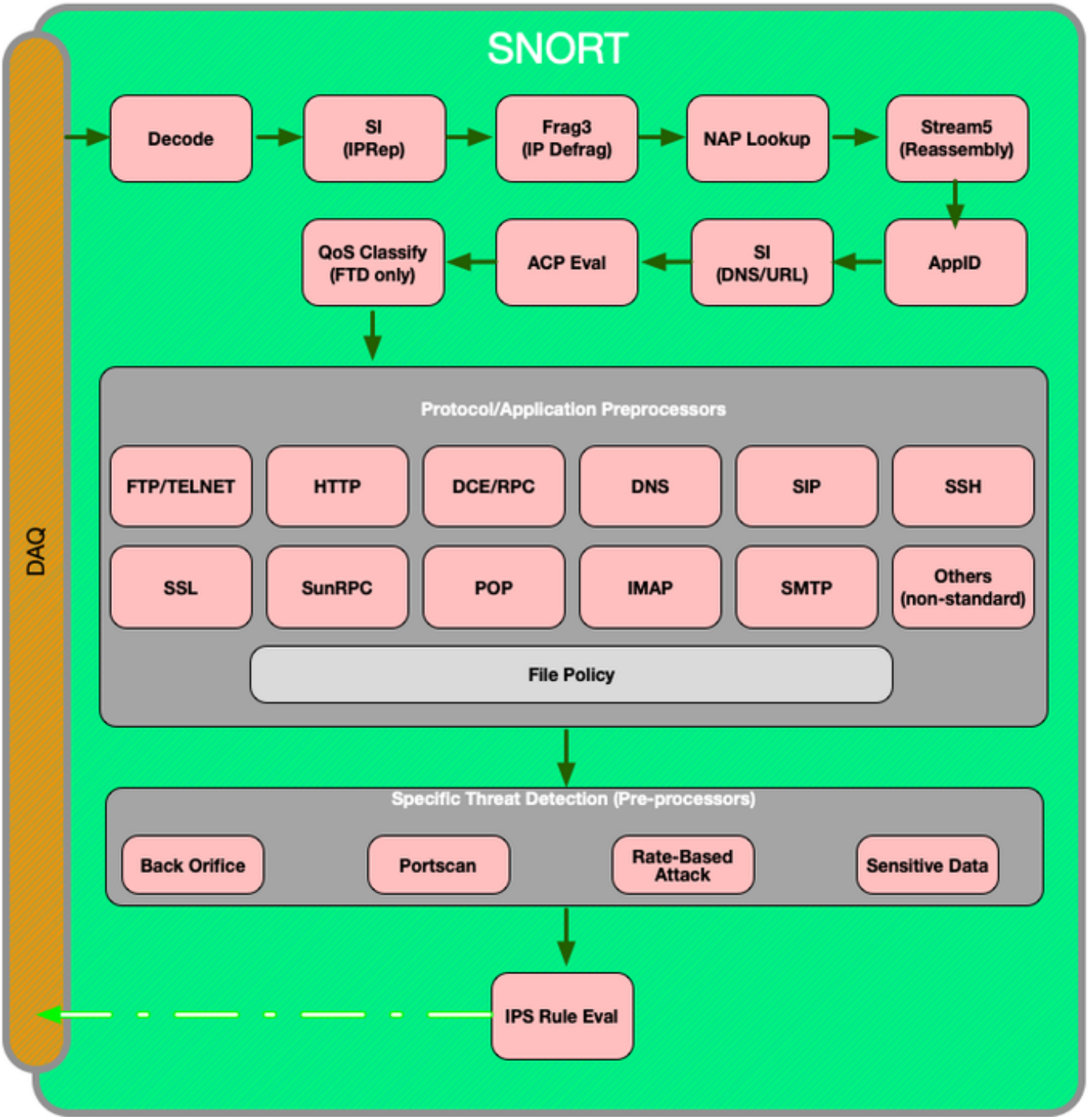
Security Intelligence is a feature that performs inspection against both blacklists and whitelists for:

- IP addresses (also known as "Networks" in certain portions of the UI)
- Uniform Resource Locators (URLs)
- Domain Name System (DNS) Queries

The lists within Security Intelligence can be populated by Cisco-provided feeds and/or user configured lists and feeds.

Security Intelligence reputation based on IP addresses is the first component within Firepower to

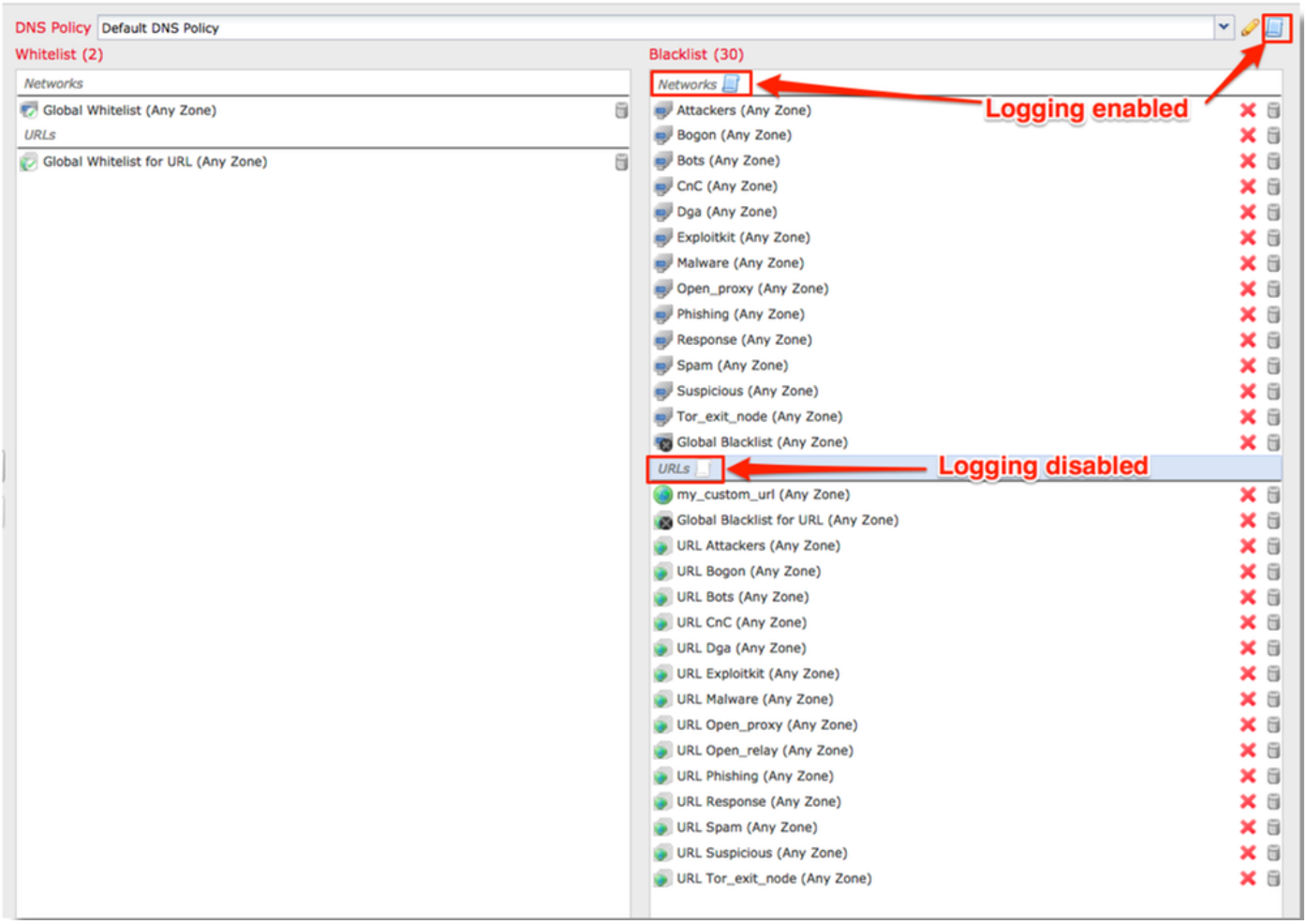
inspect the traffic. URL and DNS Security Intelligence is performed as soon as the relevant application protocol is discovered. Below is a diagram outlining the Firepower software inspection workflow.



Determine That Logging is Enabled for Security Intelligence Events

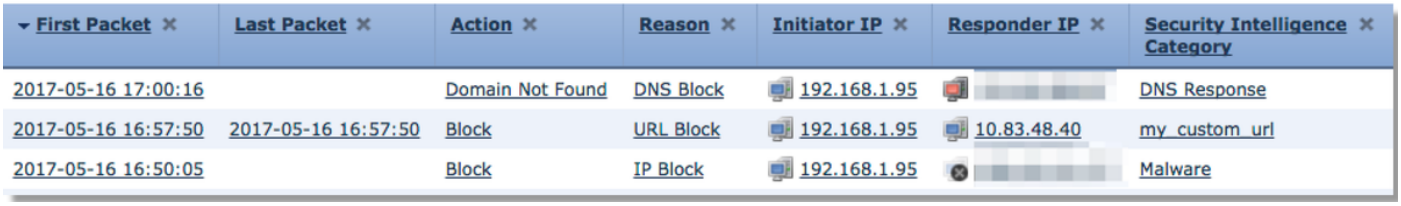
Blocks at the Security Intelligence level are very easy to determine as long as logging is enabled.

This can be determined on the Firepower Management Center (FMC) User Interface (UI) by navigating to **Policies > Access Control > Access Control Policy**. After clicking the edit icon next to the policy in question, navigate to the **Security Intelligence** tab.



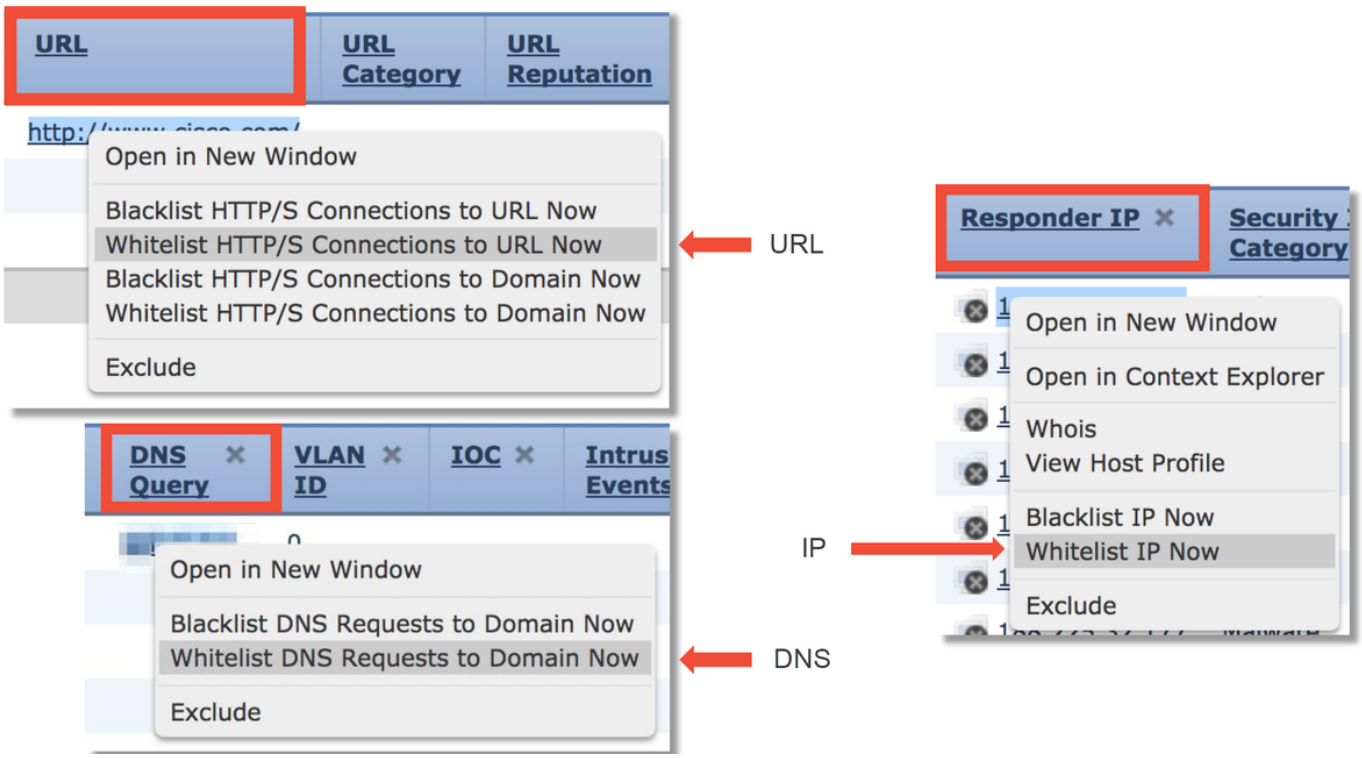
Review the Security Intelligence Events

Once logging is enabled, you can view the Security Intelligence Events under **Analysis > Connections > Security Intelligence Events**. It should be clear as to why the traffic is being blocked.



First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

As a quick mitigation step, you can right click on the IP, URL or DNS Query being blocked by the Security Intelligence feature and choose a whitelist option.



If you suspect that something got incorrectly put onto the blacklist, or you want to request to change the reputation you can open a ticket directly with Cisco Talos at the following link:

https://www.talosintelligence.com/reputation_center/support

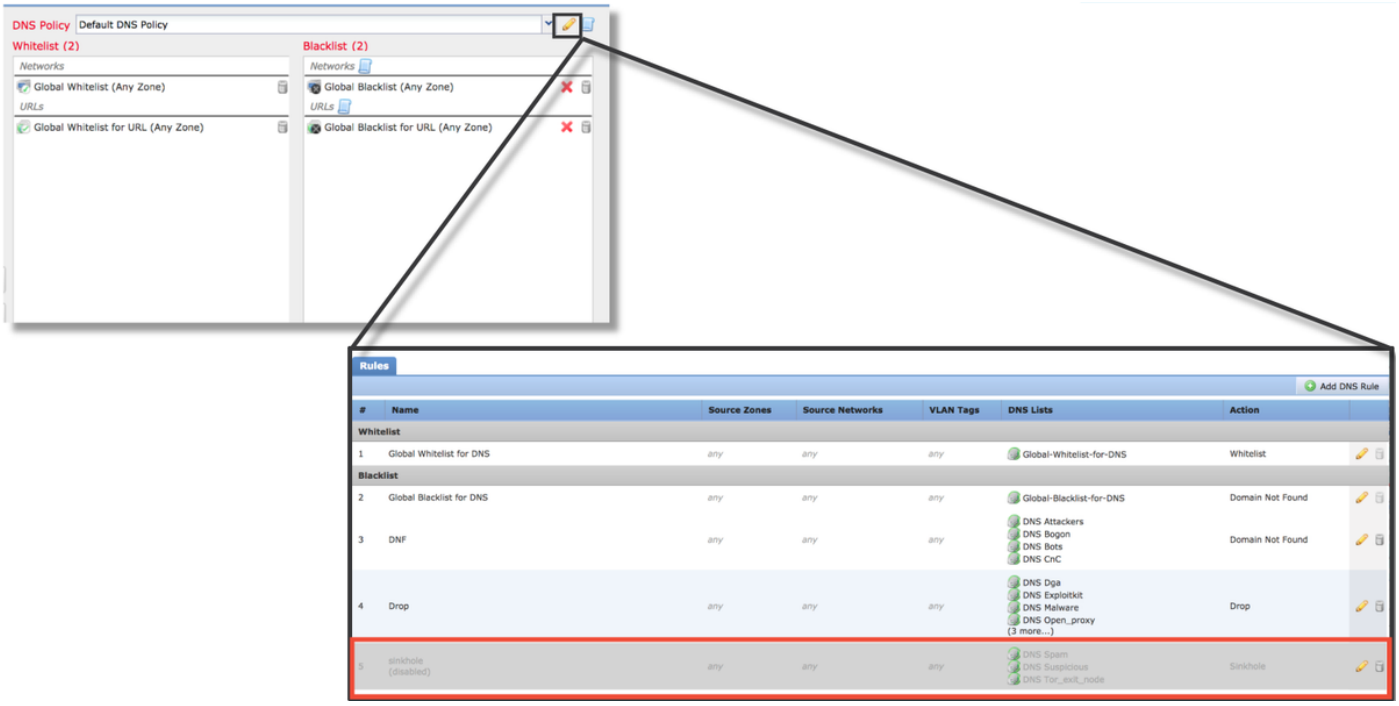
You can also provide the data to the Cisco Technical Assistance Center (TAC) to investigate if an item should be removed from the blacklist.

> **Note:** Adding to the whitelist only adds an entry to the Security Intelligence whitelist in question, meaning that the object is allowed to pass the Security Intelligence check. However, all other Firepower components can still inspect the traffic.

How to Remove the Security Intelligence Configurations

In order to remove the Security Intelligence configurations, navigate to the **Security Intelligence** tab, as mentioned above. There are three sections; one for Networks, URL as well as a policy for DNS.

From there, the lists and feeds can be removed by clicking on the trashcan symbol.



Notice in the screenshot above, that all the IP and URL Security Intelligence lists have been removed except for the Global blacklist and whitelist.

Within the DNS Policy, which is where the DNS Security Intelligence configuration is stored, one of the rules is disabled.

> **Note**: In order to view the contents of the Global Blacklists and Whitelists, navigate to **Objects > Object Management > Security Intelligence**. Then, click on the section of interest (Network, URL, DNS). Editing a list will then show the contents, although the configuration must be performed within the Access Control Policy.

Verify the Configuration on the Backend

The Security Intelligence configuration can be verified on the CLI via the **> show access-control-config** command, which shows the contents of the active Access Control Policy running on the Firepower device.

```
> show access-control-config

==================[ My AC Policy ]==================
Description              :
Default Action            : Allow
Default Policy            : SOC
Logging Configuration
   DC                   : Enabled
   Beginning             : Disabled
   End                  : Enabled
Rule Hits                 : 0
Variable Set              : Default-Set

===[ Security Intelligence - Network Whitelist ]====
   Name                 : Global-Whitelist (List)
   IP Count             : 0
   Zone                 : any

===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Enabled
   DC                   : Enabled


--------------------[ Block ]---------------------
   Name                 : Attackers (Feed)
   Zone                 : any

   Name                 : Bogon (Feed)
   Zone                 : any
…[omitted for brevity]
```

Notice in the example above, that logging is configured for the Network Blacklist and at least two feeds have been included in the blacklist (Attackers and Bogon).

Whether an individual item is in a Security Intelligence list can be determined in expert mode. Please see the steps below:

There is a file for each Security Intelligence list with a unique UUID. The above example shows

how to identify the name of the list, using the **head -n1** command.

Data to Provide to TAC

Data	Instructions
Troubleshoot files from the FMC and Firepower device inspecting the traffic	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn
Screenshots of events (with timestamps included)	See this article for instructions
Text output from CLI sessions	See this article for instructions
If submitting a false positive case, provide the item (IP, URL, domain) to dispute.	Provide reasons and evidence of why the dispute should be performed.

Next Step

If it has been determined that the Security Intelligence component is not the cause of the issue, the next step would be to troubleshoot the Access Control Policy rules.

Click here to proceed with the next article.