Firepower Data Path Troubleshooting: Overview

Contents

Introduction

The purpose of this guide is to help quickly identify whether a Firepower Threat Defense (FTD) device or Adaptive Security Appliance (ASA) with FirePOWER Services is causing a problem with network traffic. Also, it assists in narrowing down which Firepower component(s) should be investigated and what data should be gathered before engaging the Cisco Technical Assistance Center (TAC).

List of all the Firepower Data Path Troubleshooting Series Articles.

Firepower Data Path Troubleshooting Phase 1: Packet Ingress

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214574-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Troubleshooting Phase 2: DAQ Layer
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Troubleshooting Phase 3: Security Intelligence

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Troubleshooting Phase 4: Access Control Policy
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Troubleshooting Phase 5: SSL Policy
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Troubleshooting Phase 6: Active Authentication
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Troubleshooting Phase 7: Intrusion Policy
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Troubleshooting Phase 8: Network Analysis Policy

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214610-firepower-data-path-troubleshooting-phas.html

Prerequisites

- This article assumes one has a basic understanding of FTD and ASA platforms.
- Knowledge of open source snort is recommended, though not required.

For a complete listing of Firepower documentation, including Installation and Configuration Guides, please visit the documentation roadmap page.

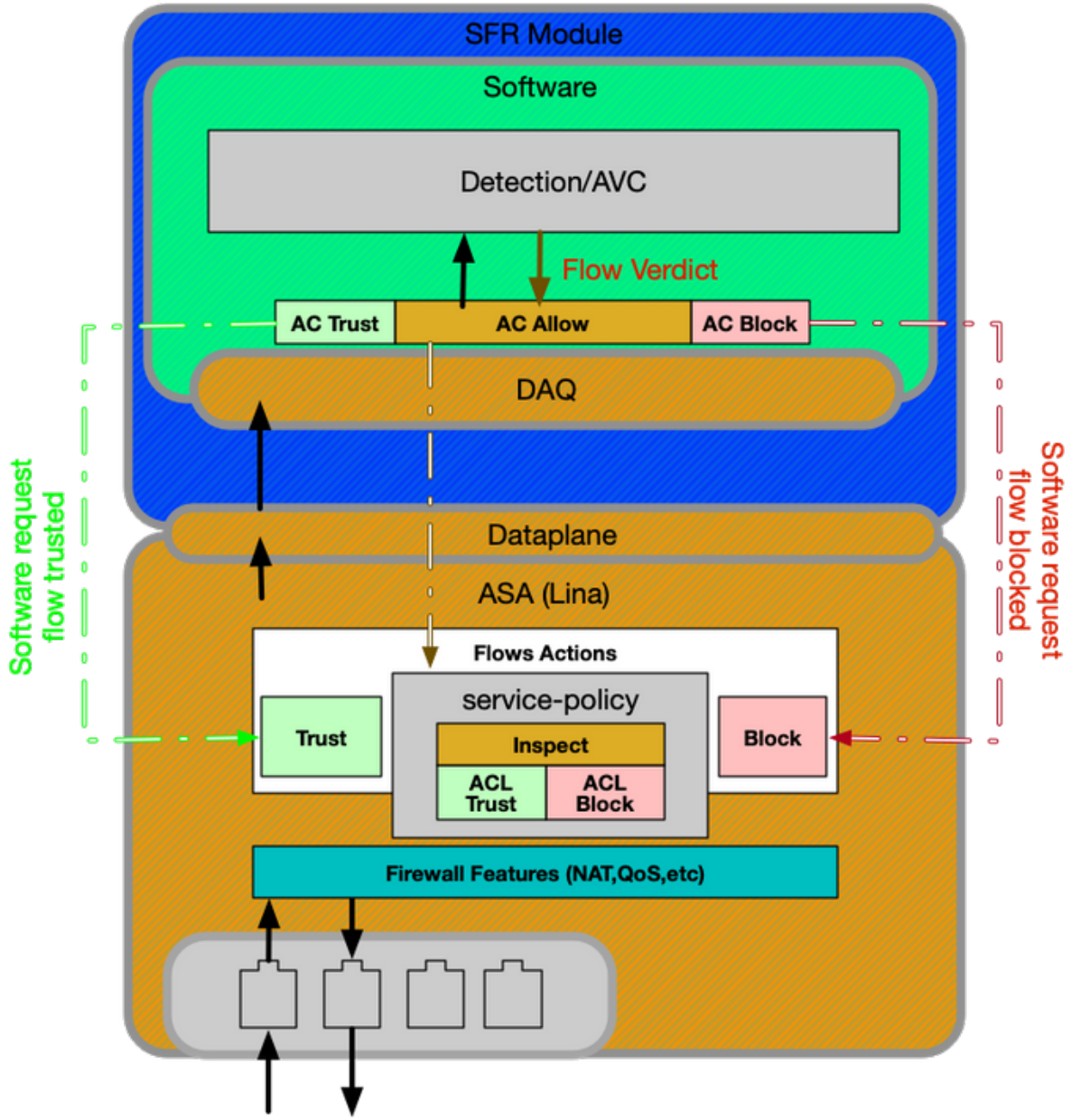
Architectural Overview of the Data Path

The following section looks at the architectural data-path for various Firepower platforms. With the architecture in mind, we will then move on to how to quickly determine whether or not the Firepower device is blocking the traffic flow.

> **Note**: This article does not cover the legacy Firepower 7000 and 8000 series devices, nor the NGIPS (non-FTD) virtual platform. For information on troubleshooting those platforms, please visit our TechNotes page.

ASA with FirePOWER Services (SFR Module) Platform

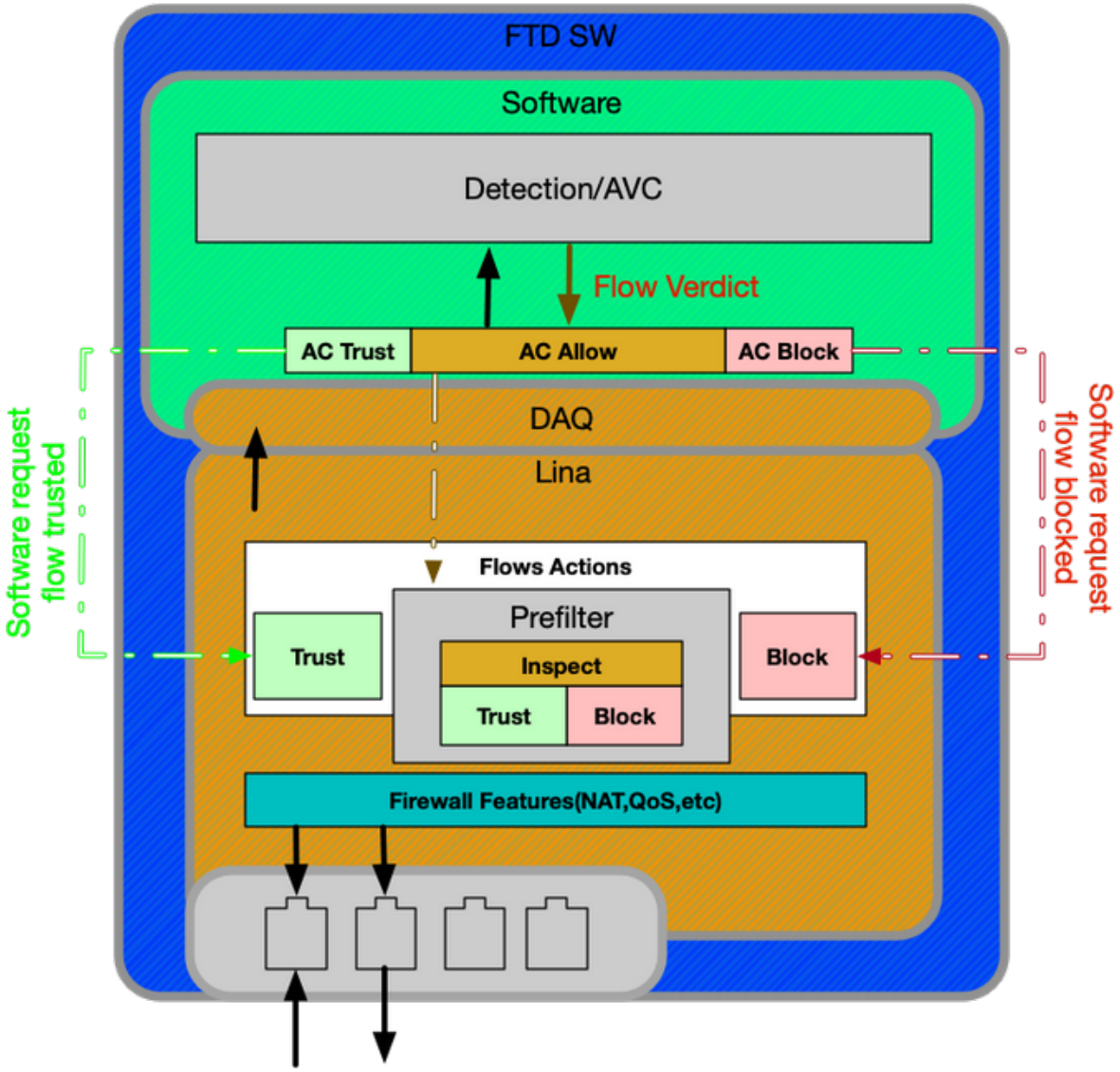
The FirePOWER Services platform is also referred to as SFR module. This is basically a virtual machine which runs on 5500-X ASA platforms.



The service-policy on the ASA determines which traffic is being sent to the SFR module. There is a dataplane layer which is used to communicate with the Firepower Data Acquisition (DAQ) engine, which is used to translate packets in a way which snort can understand.

Firepower Threat Defense on ASA500-X and Virtual FTD Platform

The FTD platform consists of a single image containing both the Lina (ASA) and Firepower code. One major difference between this and the ASA with SFR module platform is that there are more efficient communications between Lina and snort.

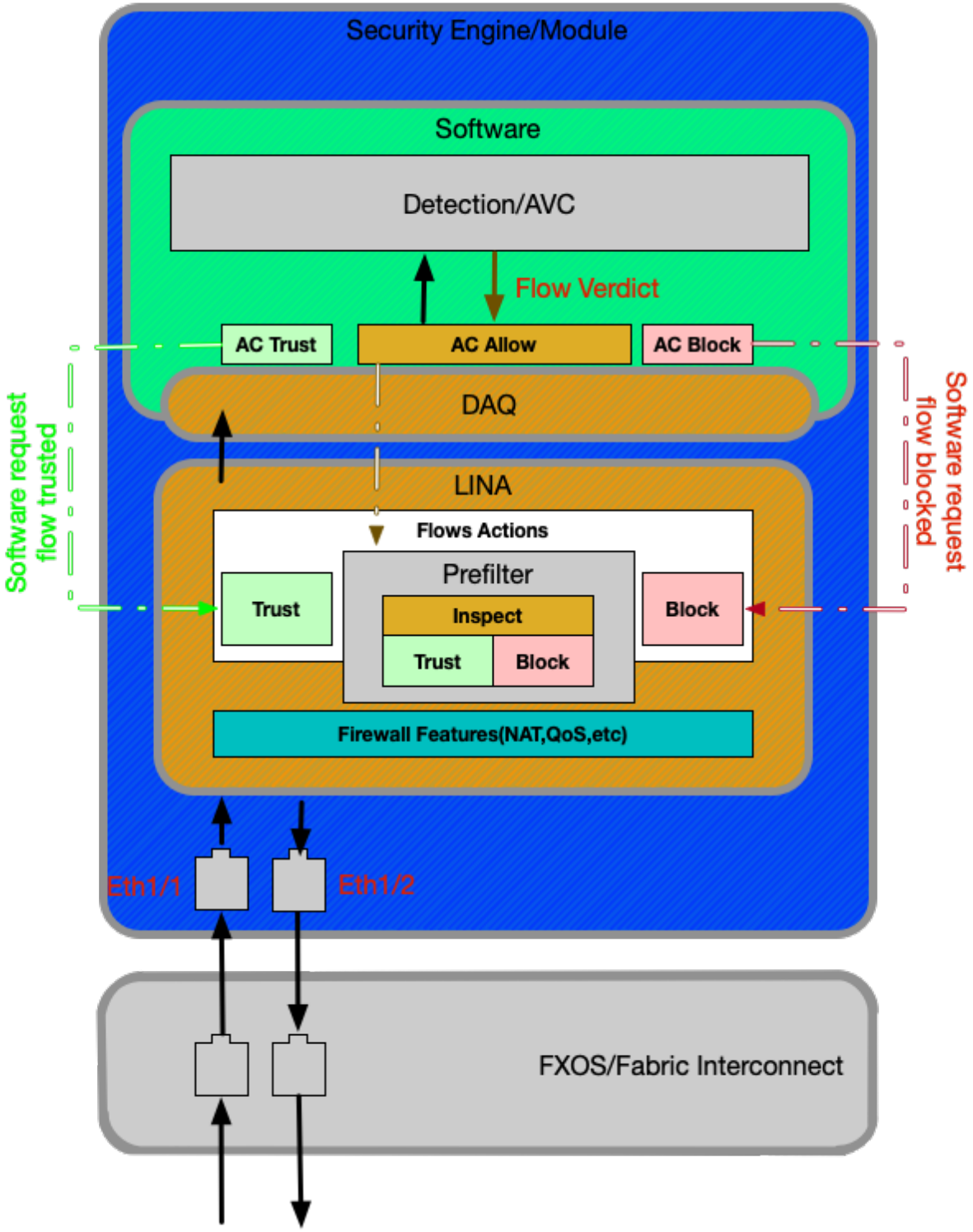


FTD on SSP Platforms

On the Security Service Platforms (SSP) models, the FTD software runs on top of the Firepower eXtensible Operative System (FXOS) platform, which is an underlying Operative System (OS) used to manage the chassis hardware and host various applications known as logical devices.

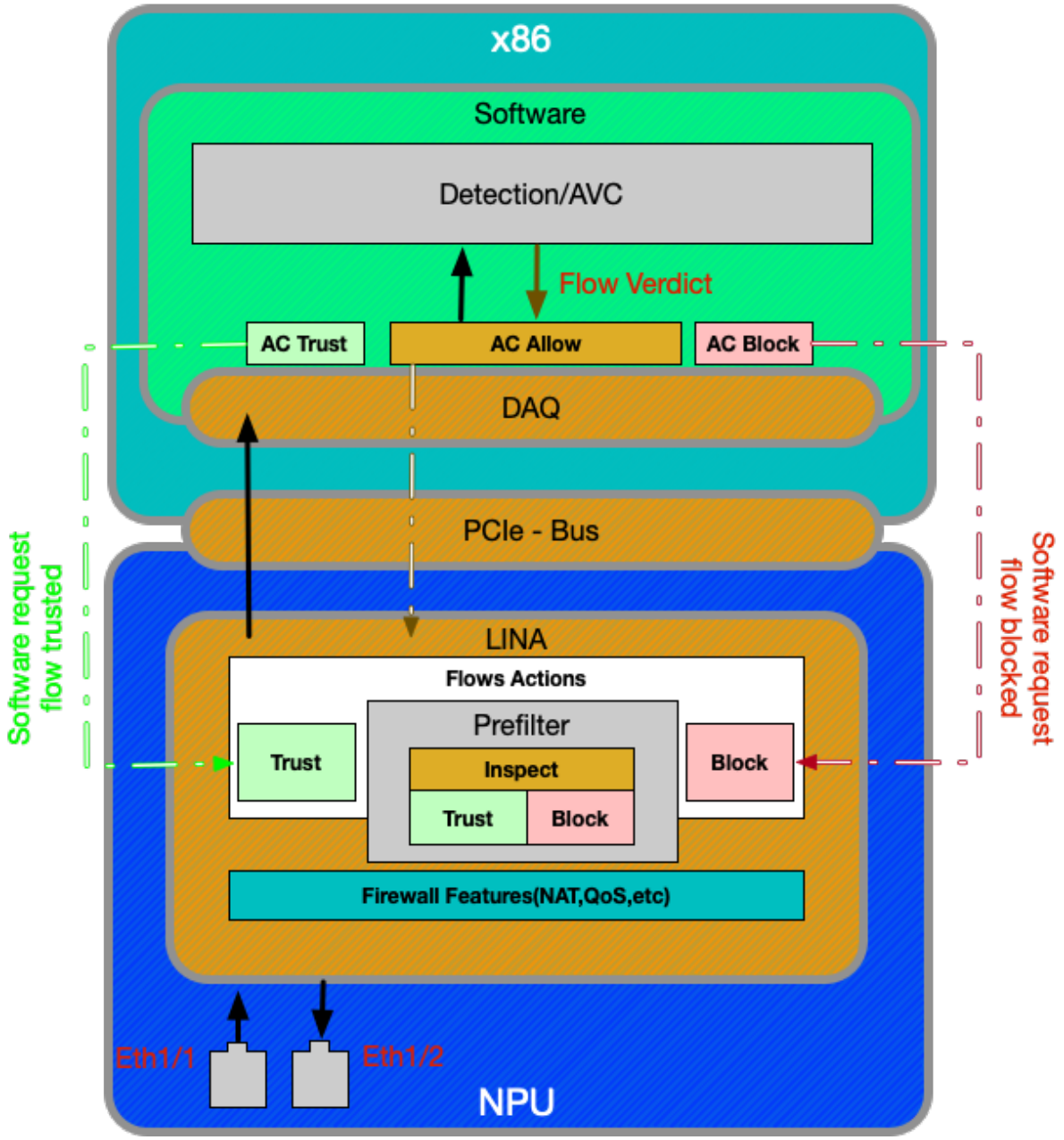
Within the SSP Platform, there are some differences across models, as seen in the diagrams and descriptions below.

Firepower 9300 and 4100 Appliances



On the Firepower 9300 and 4100 platforms, the ingressing and egressing packets are handled by a switch powered by the FXOS firmware (Fabric Interconnect). The packets are then sent to the interfaces assigned to the logical device (in this case, FTD). After that, packet processing is the same as it is on the non-SSP FTD platforms.

Firepower 2100 Appliances



The Firepower 2100 device functions much like the non-SSP FTD platforms. It does not contain the fabric interconnect layer which is present on the 9300 and 4100 models. However, there is a major difference in the 2100 series devices compared to the other devices, and that is the presence of the Application-specific integrated circuit (ASIC). All of the traditional ASA features (Lina) run on the ASIC, and all of the Next-Generation Firewall (NGFW) features (snort, URL filtering, etc) run on the traditional x86 architecture. The way that Lina and Snort communicate on this platform is over a Peripheral Component Interconnect Express (PCIe) via a packet queue, as opposed to the other platforms which use Direct Memory Access (DMA) to queue packets to snort.

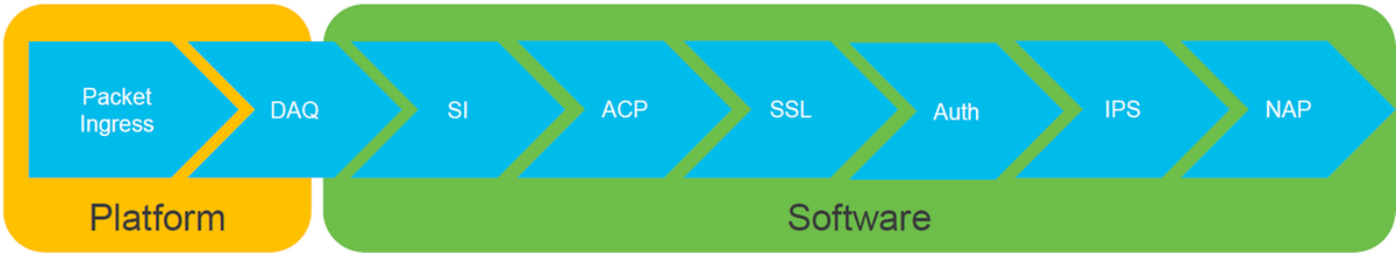
> **Note**: The same methods for troubleshooting the FTD non-SSP platforms will be followed on the FPR-2100 platform.

Recommended Process for Troubleshooting Firepower Data-Path

Now that we have covered how to identify unique traffic as well as the basic data path architecture in Firepower platforms, we now look at the specific places in which packets can be dropped. There

are eight basic components which are covered in the Data Path articles, which can systematically troubleshoot to determine possible packet drops. These include:

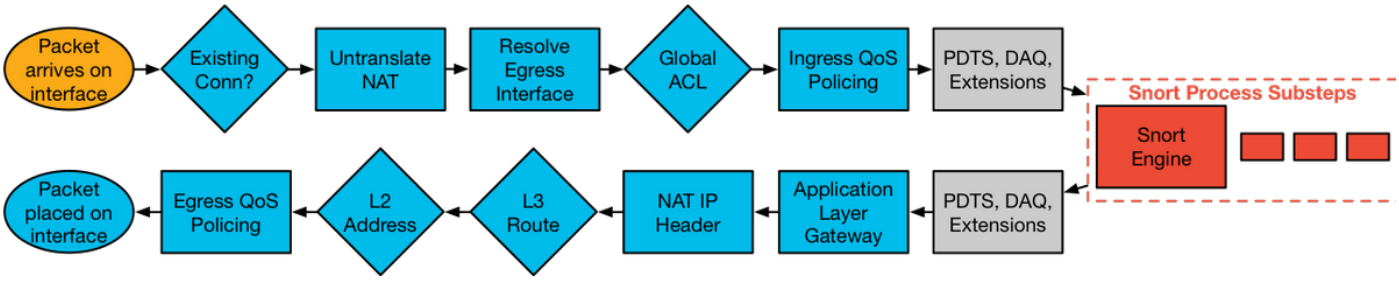
1. Packet Ingress
2. Firepower DAQ Layer
3. Security Intelligence
4. Access Control Policy
5. SSL Policy
6. Active Authentication Features
7. Intrusion Policy (IPS rules)
8. Network Analysis Policy (snort pre-processor settings)



> **Note**: These components are not listed in the exact order of operations in Firepower processing, but are ordered according to our recommended troubleshooting workflow. See illustration below for the actual path of the packet diagram.

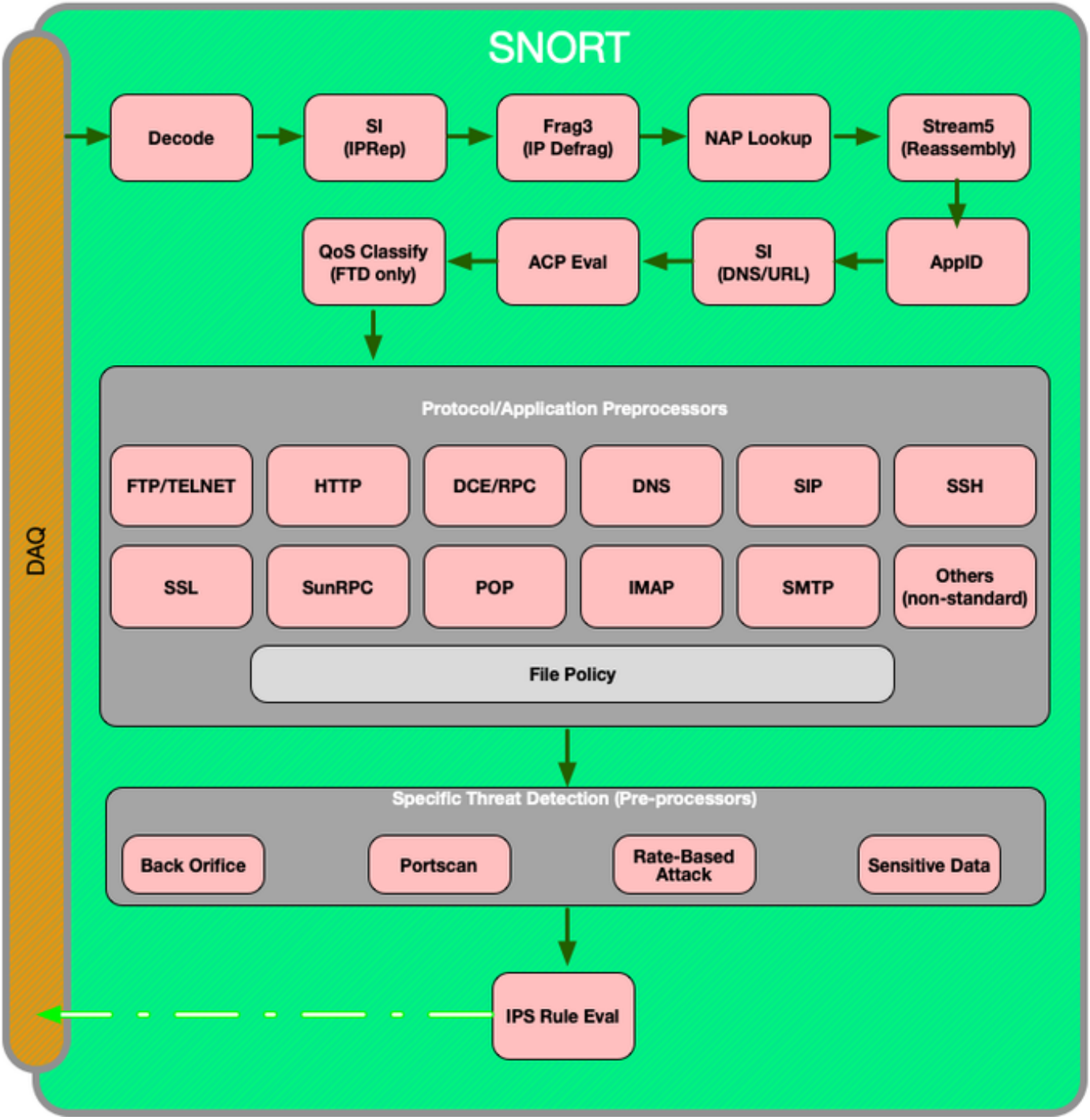
Actual Path of the Packet Through FTD

The illustration below shows the actual path of the packet as it traverses through FTD.



Snort Packet Path

The illustration below shows the path of the packet through the Snort engine.



Packet Ingress and Egress

The first data path troubleshooting step is to make sure that there are no drops occurring at the ingress or egress stage of packet processing. If a packet is ingressing but not egressing, then you can be sure that the packet is being dropped by the device at some place within the data-path.

This article walks through how to troubleshoot packet ingress and egress on Firepower systems.

Firepower DAQ Layer

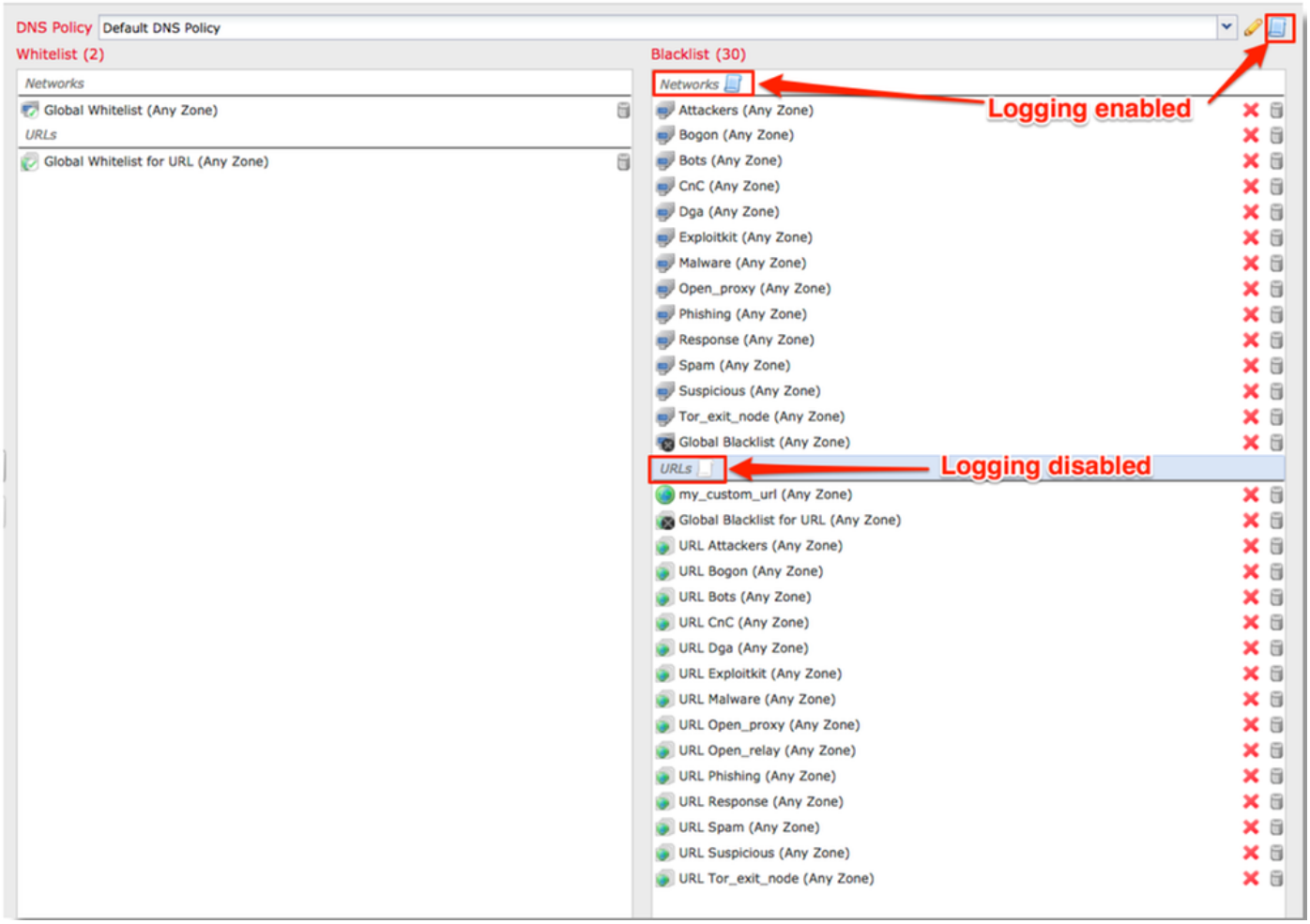
If it has been determined that the packet is ingressing but not egressing, the next step in data path troubleshooting should be at the Firepower DAQ (Data Acquisition) layer to make sure that the traffic in question is being sent to Firepower for inspection and if so, if it is being dropped or modified.

This article looks at how to troubleshoot the initial handling of the traffic by Firepower as well the path it is taking throughout the appliance.

It also covers how the Firepower device can be bypassed altogether to determine whether a Firepower component is responsible for the traffic issue.

Security Intelligence

Security Intelligence is the first component within Firepower to inspect the traffic. Blocks at this level are very easy to determine as long as logging is enabled. This can be determined on the FMC GUI 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.

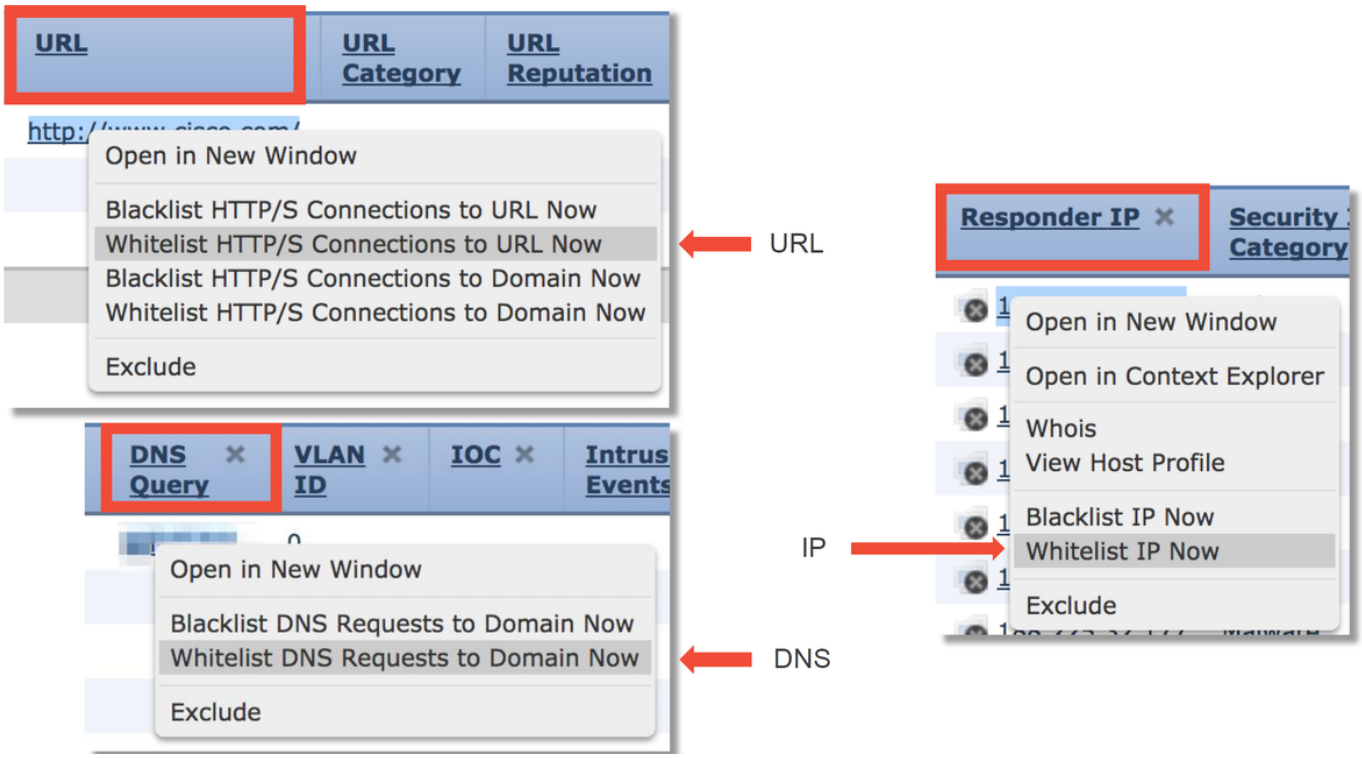


Once logging is enabled, you can view the Security Intelligence Events under **Analysis >**

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 TAC to report on what is being blocked and perhaps have an entry removed from a blacklist.

For in-depth troubleshooting of the Security Intelligence component, please review the relevant data path troubleshooting article.

Access Control Policy

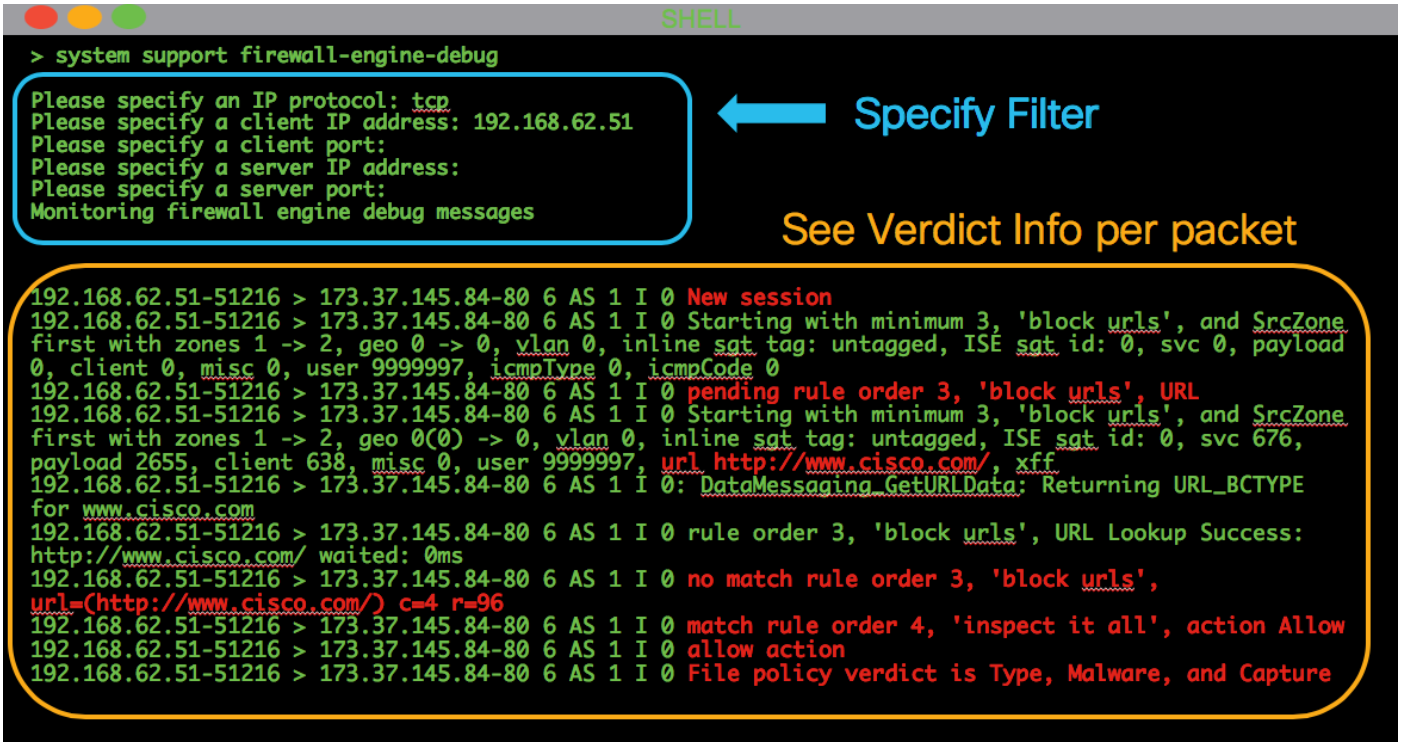
If it has been determined that the Security Intelligence feature is not blocking traffic, the next recommended step is to troubleshoot the Access Control Policy rules to see if a rule with a 'Block' action is dropping the traffic.

It is recommended to start using the command "firewall-engine-debug" or capture with trace. Commonly, these tools can give you the answer right away and tell you what rule the traffic is

hitting and for what reasons.

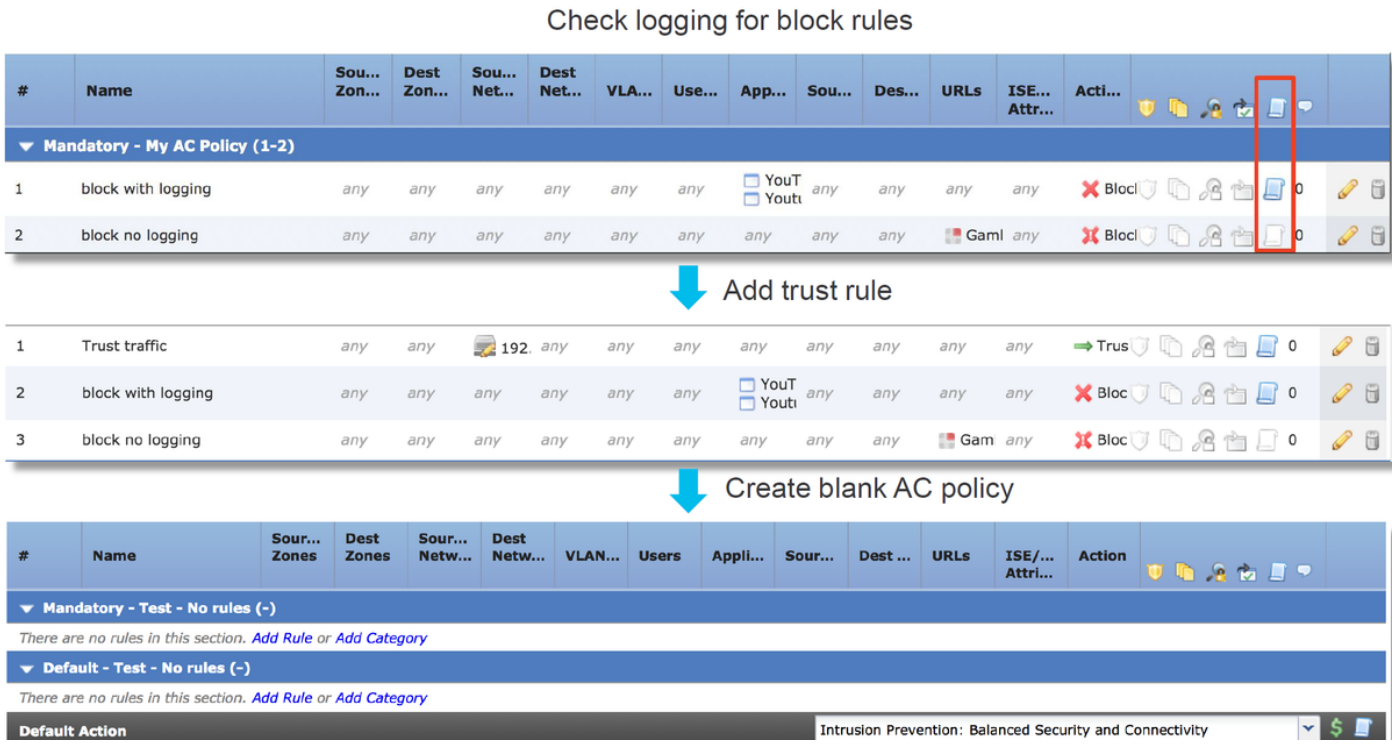
- Run debugging on the Firepower CLI to see which rule is blocking traffic (make sure to enter as many parameters as possible) via the following command: **> system support firewall-engine-debug**
- The debug output can be provided to TAC for analysis

Below is some sample output, depicting rule evaluation for traffic matching an Access Control rule with the action of 'Allow':



If you are unable to determine which Acess Control (AC) rule is being matched, or you are unable to determine if the AC policy is the problem using the tools above, below are some basic steps for troubleshooting the Access Control Policy (note these options are not the first option because they require policy changes/deploys):

- Enable logging for any rules with a 'Block' action
- If you still do not see connection events for the traffic and it is being blocked, next create a Trust rule for traffic in question as a mitigation step
- If the trust rule for the traffic still does not resolve the issue but you still suspect the AC policy is at fault, next, create a new blank Access Control Policy if possible, using a default action other than 'Block All Traffic'

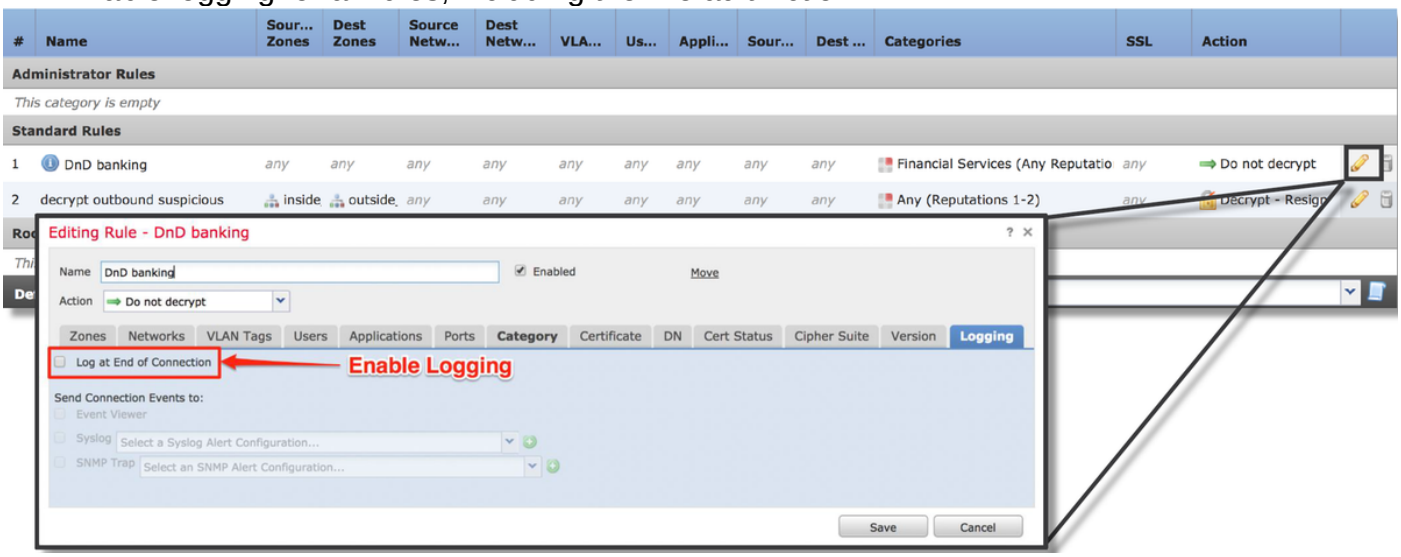


For in-depth troubleshooting of the Access Control Policy, please review the relevant data path troubleshooting article.

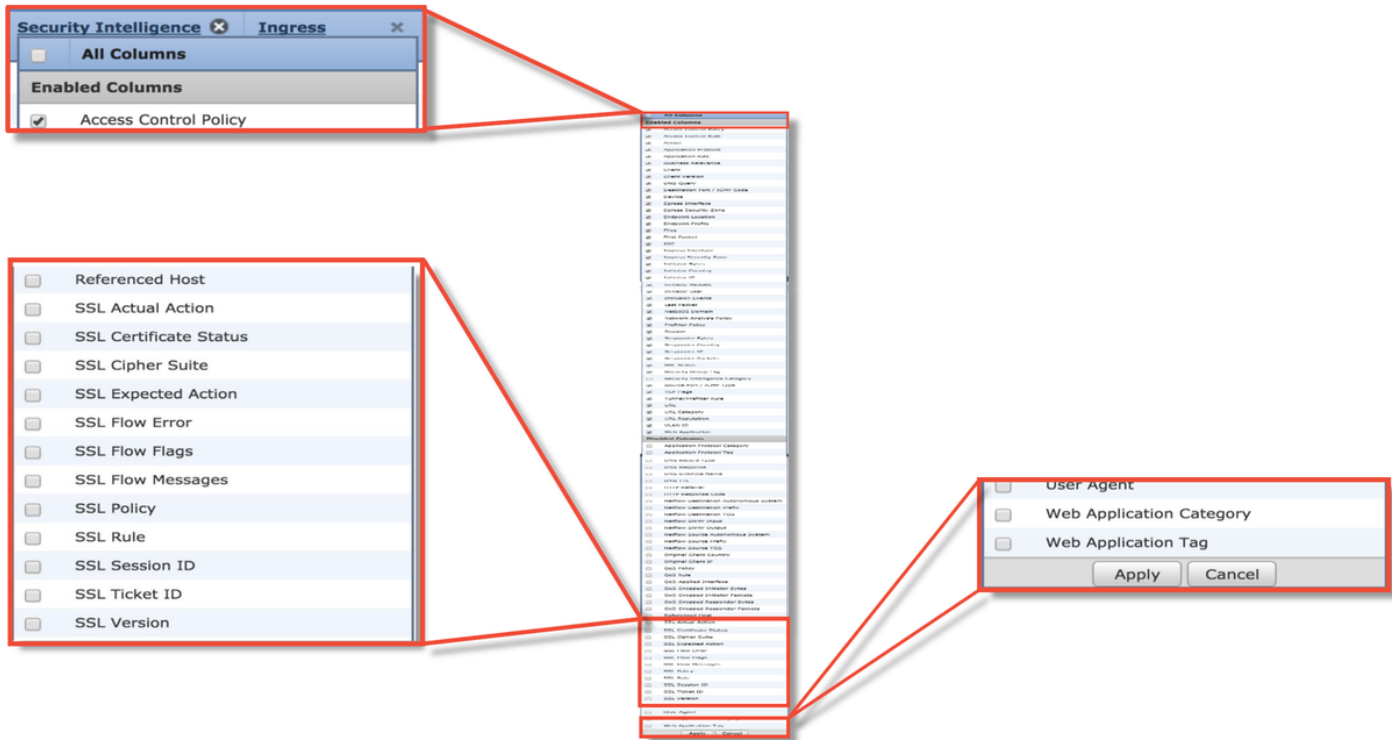
SSL Policy

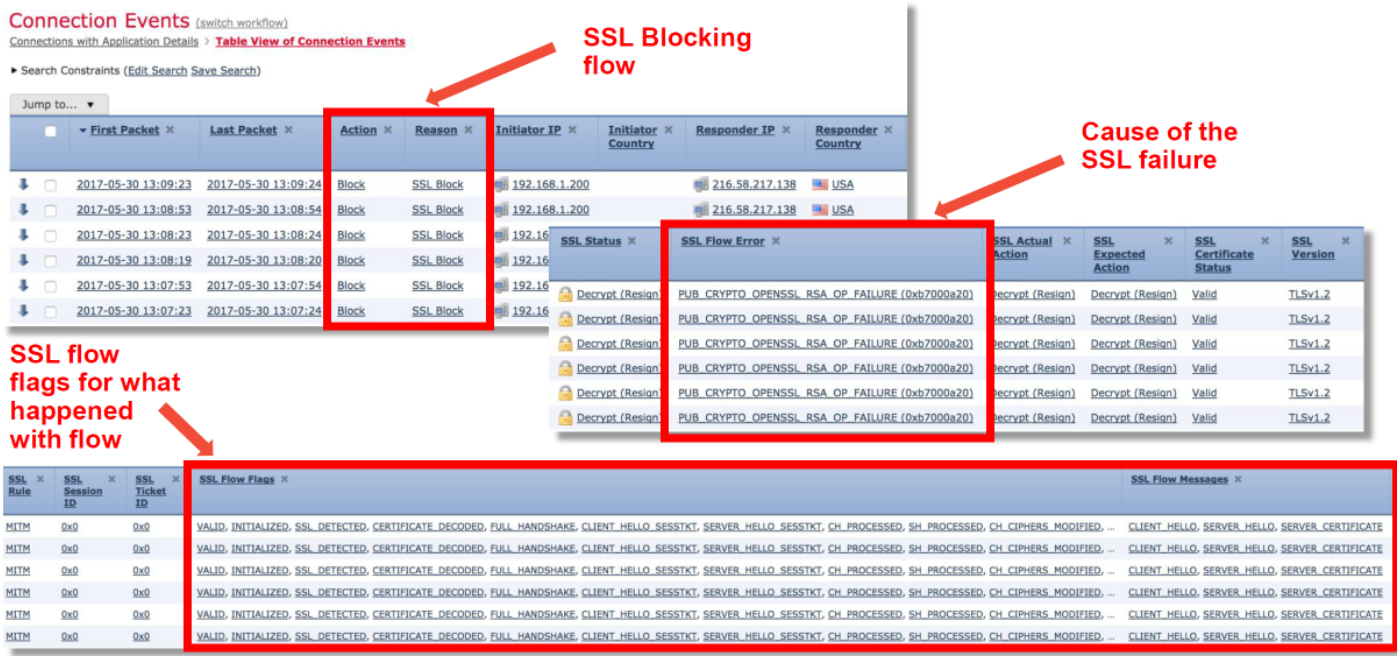
If SSL Policy is being used, it is possible that it may be blocking traffic. Below are some basic steps for troubleshooting the SSL Policy:

- Enable logging for all rules, including the 'Default Action'



- Check the Undecryptable Actions tab to see if an option is set to block traffic
- In the Connection events section, check all the fields with 'SSL' in the name
  Most are disabled by default and need to be enabled in the Connection Events viewer by clicking on the cross next to any column name





- Create a blank SSL policy with Do not Decrypt as the Default Action as a mitigation step
- Remove the SSL Policy from the Access Control Policy as a mitigation step
  This is set in the Advanced tab

It SSL Policy is suspected of dropping traffic, the connection events along with the policy configuration can be sent to TAC.

For more in-depth troubleshooting of the SSL Policy, please review the relevant data path troubleshooting article.

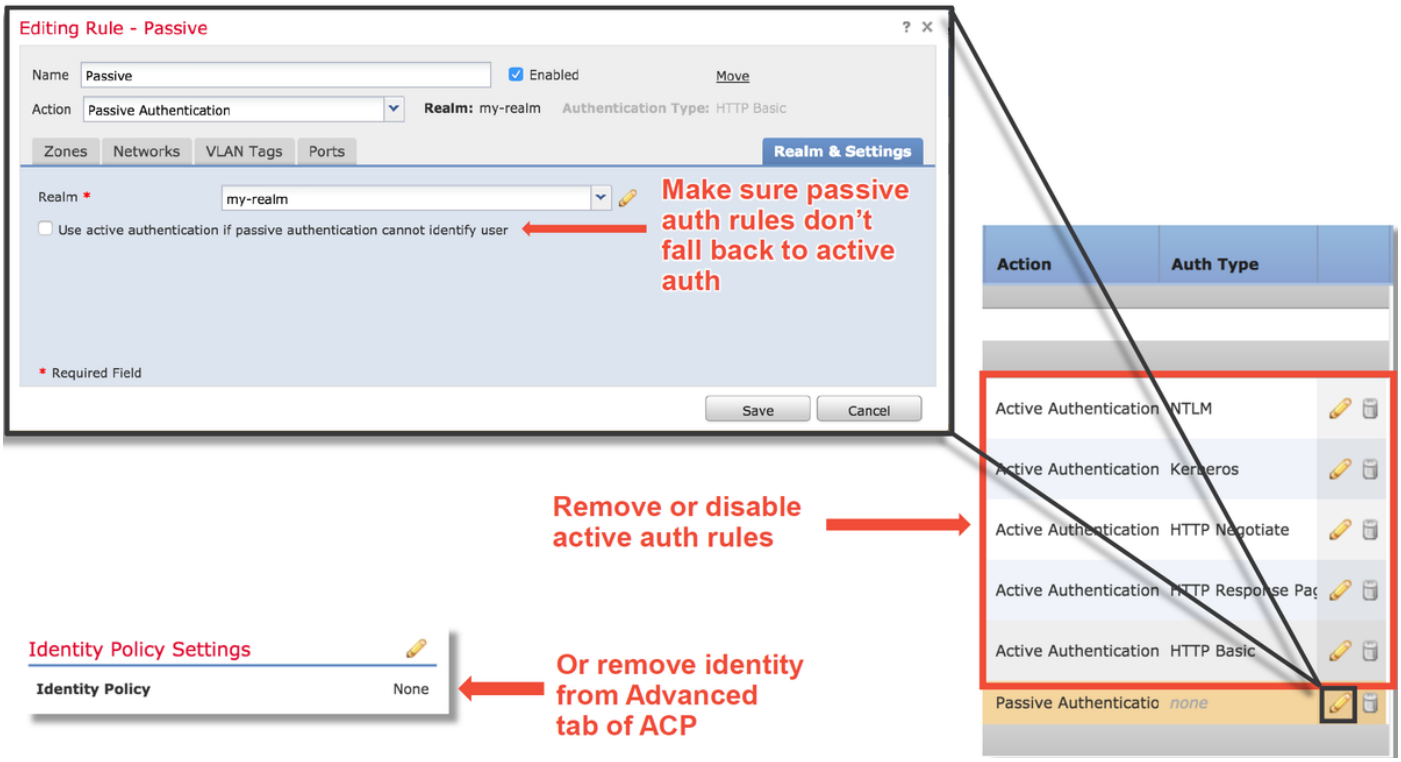
Active Authentication

When used in an Identity Policy, Active Authentication has the ability to drop traffic which should

be allowed if something goes wrong. The active authentication feature itself can directly impact all HTTP/HTTPS traffic because if it is determined that we need to authenticate a user, all of this happens over the HTTP protocol only. This means that active authentication should not impact other network services (such as DNS, ICMP, etc) unless you have specific Access Control rules that block based on user, and users are unable to authenticate through the active authentication services on the FTD. However, this would not be a direct problem of the active authentication feature, but a result of users not being able to authenticate and having a policy that blocks unauthenticated users.

A quick mitigation step would be to disable any rule within the Identity Policy with the action of 'Active Authentication'.

Also, make sure that any rules with 'Passive Authentication' action do not have the 'Use active authentication if passive authentication cannot identify user' option checked.



More more in-depth troubleshooting of the Active Authentication, please review the relevant data path troubleshooting article.

Intrusion Policy

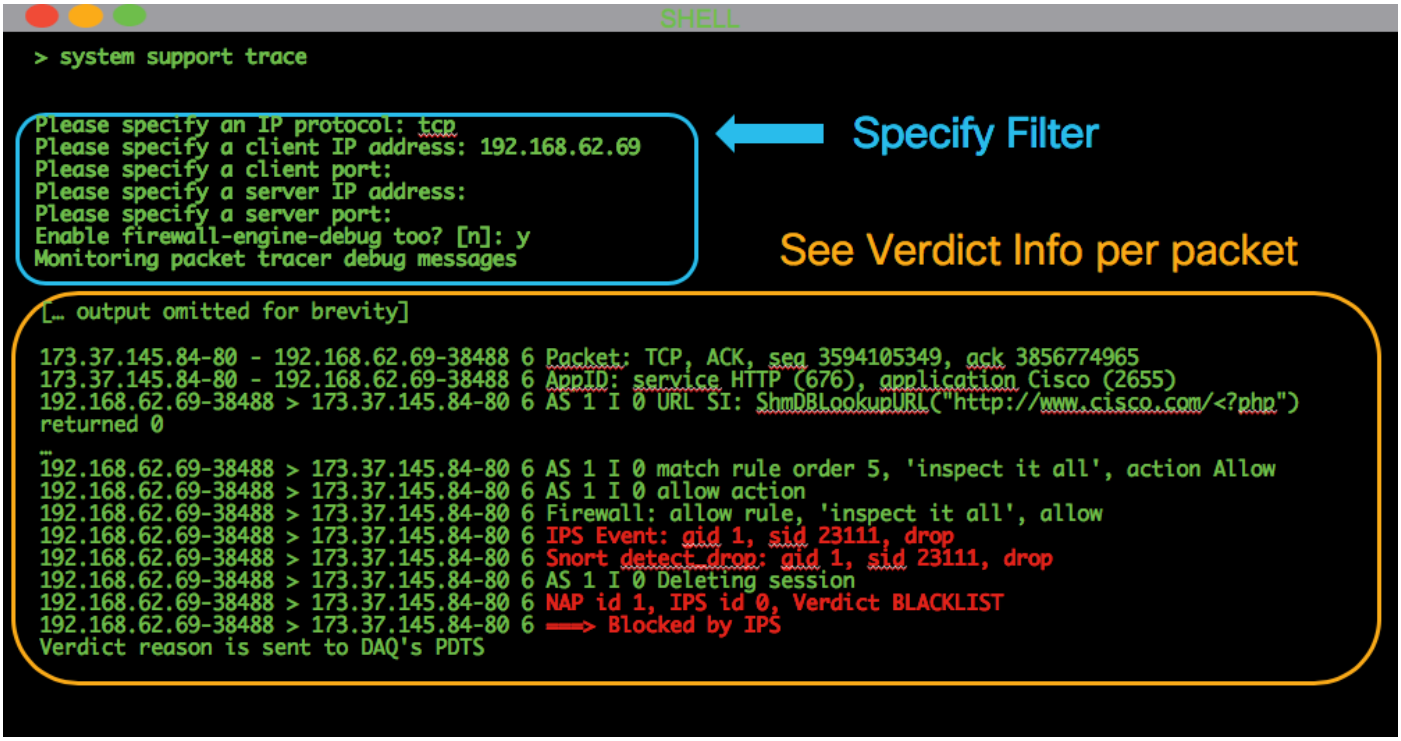
An Intrusion Policy might be dropping traffic or causing network latency. An Intrusion Policy can be used in one of the following three places within the Access Control Policy:

- In an Access Control Rule, within the "Inspection" tab
- In the Default Action
- In the Advanced tab, in the **Network Analysis and Intrusion Policies** > **Intrusion Policy used before Access Control rule is determined** section

To see whether an Intrusion Policy rule is blocking traffic, navigate to the **Analysis > Intrusions > Events** page in the FMC. The **Table View of Intrusion Events** view provides information about the hosts involved in the events. Please see the relevant data path troubleshooting article on information pertaining to event analysis.

The first recommended step to determining if an Intrusion Policy Signature (IPS) is blocking the traffic would be to utilize the **> system support trace** feature from the CLI of the FTD. This debug command works in a similar fashion as firewall-engine-debug, and it also gives you the option to enable firewall-engine-debug alongside the trace.

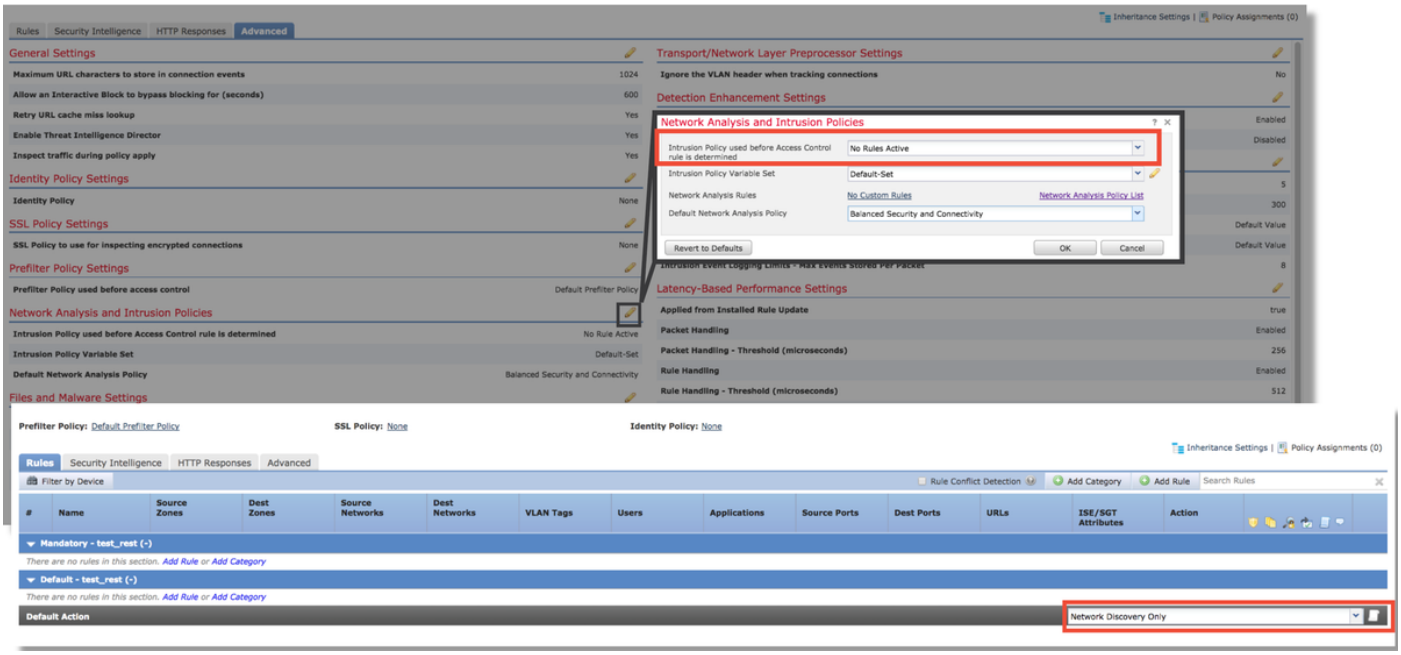
The illustration below shows an example of using the system support trace tool where the result showed that a packet was blocked due to an Intrusion rule. This gives you all of the details such as the GID (Group Identifier), SID (Signature Identifier), NAP (Network Analysis Policy) ID and IPS ID so you can see exactly what policy/rule is blocking this traffic.



If you are unable to determine that IPS is blocking from trace output, but you suspect that it is IPS dropping due to a custom Intrusion Policy, you can replace the Intrusion Policy with a "Balanced Security and Connectivity" policy or a "Connectivity over Security" policy. These are Cisco-provided Intrusion Policies. If making that change, resolves the issue, then the custom Intrusion Policy used prior can be troubleshot by TAC. If a default Cisco policy is used already you can try changing the default to a less secure one as these have fewer rules, so it may help narrow the scope. For example, if traffic is blocked and you are using a balanced policy, then you switch to connectivity over security policy and the problem goes away, it's likely that there was a rule in the balanced policy dropping the traffic that is not set to drop in the connectivity over security policy.

The following changes can be made within the Access Control Policy to eliminate all Intrusion Policy inspection block possibilities (it is recommended to make as fewer changes as possible as to not alter your security efficacy, so making targetted AC rules for the traffic in question is recommended, as opposed to disabling IPS in the entire policy):

- In all the Access Control rules (or just the rule(s) that specific traffic is matching that is impacted), remove the Intrusion Policy from the Inspection tab
- In the Advanced tab, in the **Network Analysis and Intrusion Policies** > **Intrusion Policy used before Access Control rule is determined** section, choose the "No Rules Active" policy.



If that still does not resolve the issue, move ahead to troubleshooting the Network Analysis Policy.

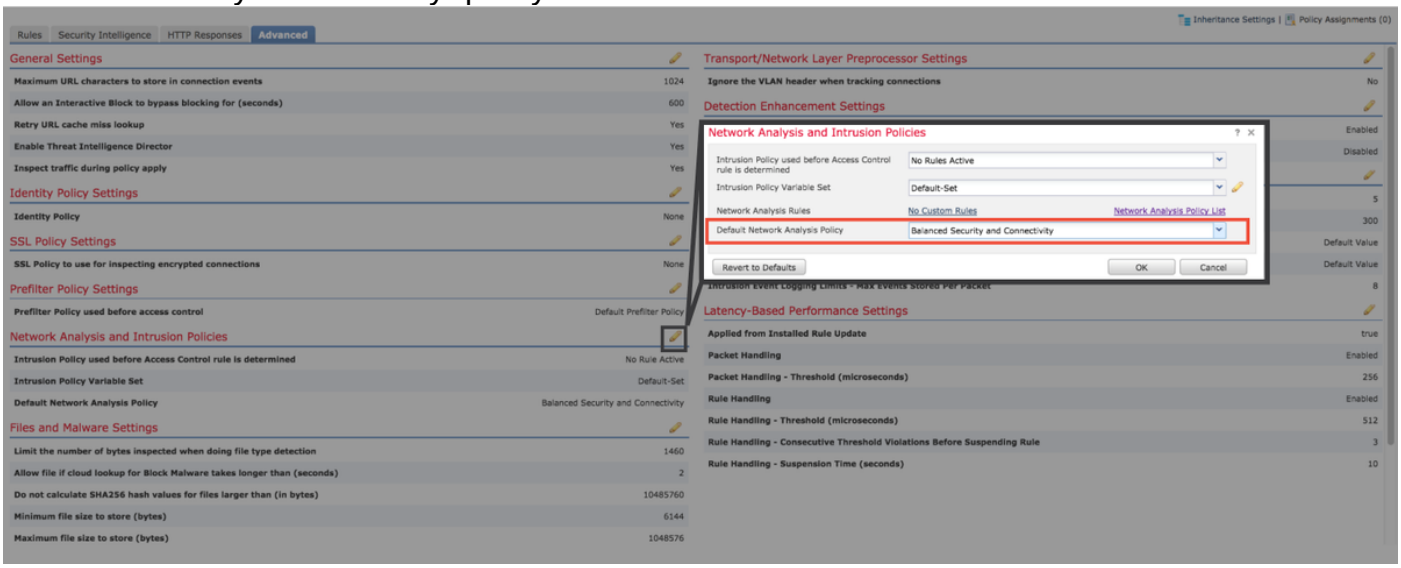
More more in-depth troubleshooting of the Intrusion Policy feature, please review the relevant data path troubleshooting article.

Network Analysis Policy

The Network Analysis Policy (NAP) contains Firepower pre-processor settings, some of which can drop traffic. The first recommended step for troubleshooting this is the same as for the IPS troubleshooting, which is to use the **> system support trace** tool to try to find what in snort is blocking the traffic. See the "Intrusion Policy" section above for more information about this tool and example usage.

To quickly mitigate possible issues with the NAP, the following steps can be performed:

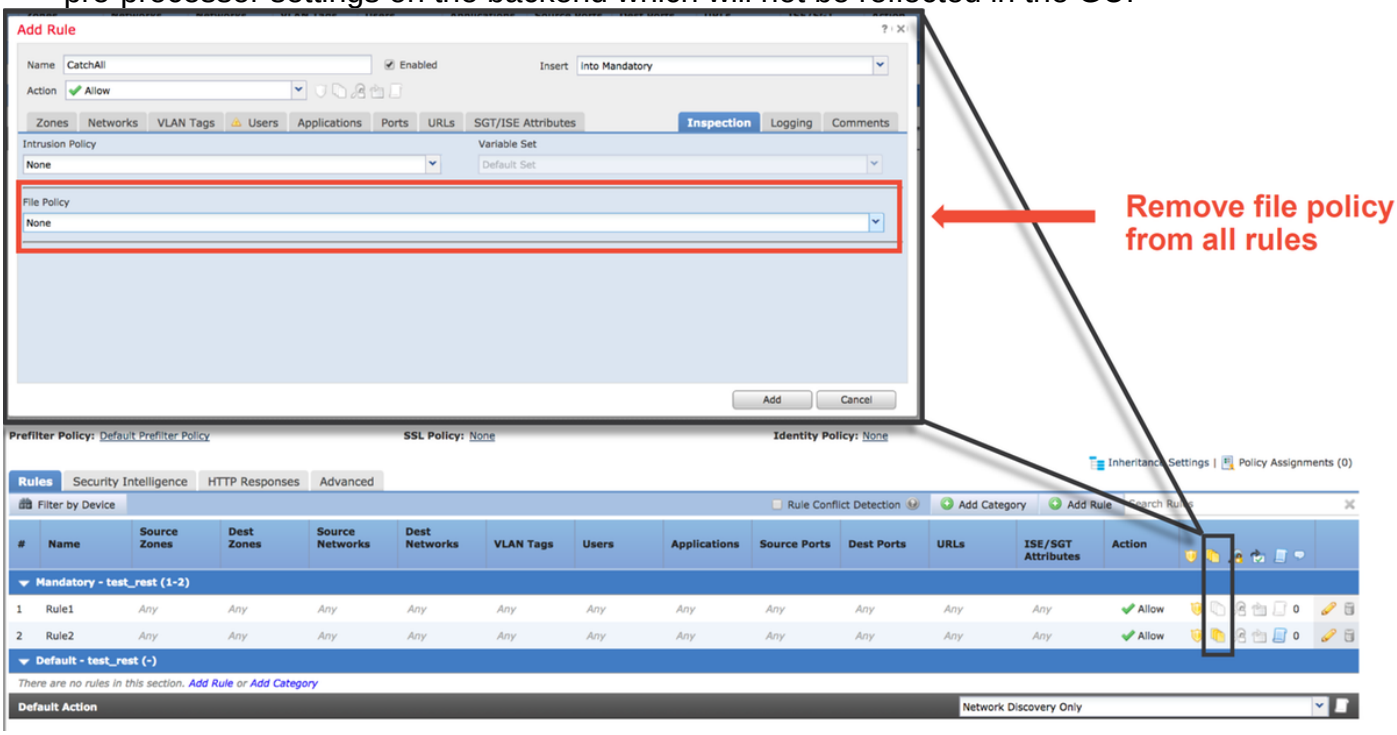
- If a custom NAP is being used, replace it with a "Balanced Security and Connectivity" or "Connectivity over Security" policy



- If any "Custom Rules" are being used, make sure to set the NAP to one of the defaults

mentioned above

- If any Access Control rules use a File Policy, temporarily remove it as a File Policy can enable pre-processor settings on the backend which will not be reflected in the GUI



More in-depth troubleshooting of the Network Analysis Policy feature can be reviewed in this article.

Related Information

Links to Firepower documentation

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html