NGFW Policy Order of Operations

First Published: May 22, 2018
Last Updated: May 22, 2018

Table of Contents
Policy Order of Operations................................................................. 2
Introduction: Purpose........................................................................ 2
Policy Firewall: Funnel Approach (Threat tornado).............................. 2
    Common Misconceptions: ............................................................... 3
    Firewall Funnel Model: ................................................................. 3
Order of Operations Best Practices..................................................... 4
    Path of the packet and policy checkpoints: ..................................... 6
    Best practices for policy ordering: ................................................ 7
Policy Inheritance: ........................................................................... 7
Threat Policy Diversity: ..................................................................... 8
    Security Intelligence (IP based): .................................................... 8
    Security Intelligence (URL): ......................................................... 8
    Security Intelligence (DNS): ......................................................... 8
    Application Detection: ............................................................... 9
    Malware and File Detection: ....................................................... 9
    Intrusion Prevention: ................................................................. 10
Considering IPS Variables: .............................................................. 10
So why the review of IPS variables? ............................................... 11
Policy Order of Operations

Introduction: Purpose:

In order to avoid potential challenges with both security efficacy as well as device performance it is critical to order the rules within an Access Control Policy correctly. Incorrectly ordering rules, without understanding architectural constraints, may result in poor performance due to unneeded layer 5-7 inspection and may lower the security efficacy of the device. The purpose of this document is to provide a comprehensive understanding of best practices, taking into consideration architectural constraints, around the order in within the Access Control Policy of the Firepower System. After reading this document, you should understand best practices related to order of operations for a policy as well as the architectural considerations that need to be weighed when designing an Access Control Policy.

Policy Firewall: Funnel Approach (Threat tornado):
Common Misconceptions:

The addition of threat monitoring and threat control technologies has had an unexpected side effect in how firewall policies may be implemented. In optimizing firewall policies, it is well understood to optimize as many blocks as possible in the top of the firewall rule stack. What has happened is that some users will think about threat detection as an action that occurs either before or after the firewall rule ACLs. This misconception can lead to poorer performance, or worse the risk of overlooking potential threat scenarios that may be imbedded in traffic that matches an “Allow” access rule.

**Common NGFW Access Policy Misconception**

- NGFW inspects and Controls Layer 2-7 (OSI)
- Many still build FW policies with only Layer 2 and Layer 3 in mind.
- Threat Inspection is generally in L 5-7
- Too easy to think threat inspection happens AFTER L 3-4 controls

Danger! This is not how things work!

Firewall Funnel Model:

The Firewall Funnel Model was created as a way to help firewall and security threat administrators to visualize a consistent approach building and a next generation firewall policy.
NGFW Policies: Efficiently Building Zero-Trust

The above figure models thinking about a firewall access control policy as a funnel. The idea is to remove traffic that either can be blocked or does not require additional threat inspection early. At each lower layer, the model reminds users that progressively fewer traffic patterns need to pass down the funnel. This is especially true for application-based traffic matching (e.g., rules that match on HTTP traffic vs TCP port 80 traffic). The top layer of the funnel evaluates Layer 2-4 traffic only. Once any more is included, such as application detection, URLs, or identity, then additional processes are used to identify these conditions. The top layer is covered by two policy elements, first is the Fast Path policy, where matching is done entirely in hardware and second in the Access Control Policy, where matching is done in software.

As session traffic is mapped to an Access Control rule, additional threat detection capabilities can then be applied to the matching session. This threat inspection can be either the IPS and File/Malware detection engines or both. This means that there are further optimization considerations that can be put in place on an IPS policy (such as Snort Variable configuration or IPS rule selection) that ensures only detection patterns that could occur are being used within the allowed session.

Order of Operations Best Practices:
When designing an Access Control Policy the goal is to ensure that we spend the least amount of time waiting on information to match an Access Control Rule. Additionally, we want to limit the amount of unneeded layer 7 inspection that occurs.

**Example Scenario:**

If we want to block all traffic going to Port 443 we want to ensure this rule is NOT below a rule containing an Application Filter or something we will need to wait for information for.

Let’s take for example an Access Control Policy similar to the below:

Rule 1: Allow Google Drive Traffic and inspect with IPS
Rule 2: Trust Port 22
Rule 3: Block port 443
Rule 4: Block All remaining traffic

The packet flow and packet action with the above Access Control Policy for a TCP connection on destination port 443 would be as follows:

Packet 1: Syn <- Pending Rule 1
Packet 2: Syn-Ack <-Pending Rule 1
Packet 3: Ack <- Pending Rule 1
Packet 4: SSL Client Hello <- Pending Rule 1 looking for Google Certificate or Google Drive URI
   + This may match on the Subject Name Identifier for Google Drive
Packet 5: Rule 3 matched and traffic is blocked.

Notice that in the above packet flow the first 4 packets are not blocked even though we want to block port 443 traffic. Additionally, this traffic cannot just be sent through un-inspected and is sent to the “Intrusion Policy used before Access Control rule is determined” configured in the Advanced Section of the Access Control Policy. This means that we have higher risk for this traffic to impact the network and a higher performance impact than if we blocked the flow based on the first packet.

We should move Rules 3 and Rule 2 above Rule 1 to be more efficient and improve security efficacy.
The general desire is to put you layers 1–4 blocks first, followed by 1–4 trust rules, followed by your layers 5–7 explicitly blocks, followed by your layers 1–7 allow rules, and have your final default action of block. This will reduce the amount of time traffic will spend in inspection pending information for an Access Control Rule to be matched.

Path of the packet and policy checkpoints:

Packets and Policies: Know What’s Happening Where

Optimizing detection also becomes easier when administrators understand the complete path a packet (and the associated flow) takes through Firepower Threat Defense. The above model indicates each of the engines (and their associated configuration policy) that end up doing some form of analysis or control on a packet.

Some key optimization points to note:

- Layer 2–4 traffic that can be matched and either blocked (or allowed as trusted with Fast Path) will handle traffic entirely in hardware.
- Security Intelligence (IP based) is the first detection condition that occurs in the Firepower layer. All of this traffic will be blocked (if set to a block state) and no other additional inspection will occur. This can actually optimize threat monitoring by stopping active threat campaigns without the need for additional threat analysis.
- There is an additional IPS policy that many users do not consider; the Intrusion Policy before Application Detection occurs. This is configured within the
Advanced Tab of the Access Control policy and is performing threat detection on traffic that has not yet matched an application detection flow. Users usually discover this, when attempting to disable an IPS block in a specific IPS policy and finding that Firepower Threat Defense is still blocking the traffic. If that occurs, check the advanced section of the access control policy.

**Best practices for policy ordering:**

1.) Create a, or multiple, Pre-filter block rules for all traffic you wish to block based solely upon OSI layer 1-4 information. *(NOTE: Pay careful consideration to the platform specific considerations and best practices listed below)*

2.) Create one or multiple, pre-filter fast-path rules for all traffic you wish to avoid layer 7 inspection based upon OSI layer 1-3 information *(NOTE: Pay careful consideration to the platform specific considerations and best practices listed below)*

3.) *(Platform Specific)* If needed by platform considerations listed above, create an, or multiple, Access Control block rules for any traffic you wish to block but not offload based on OSI layer 1-4

4.) *(Platform Specific)* If needed by platform considerations listed above, create an, or multiple, Access Control trust rules for any traffic you wish to trust but not offload based on OSI layer 1-4

5.) Create an, or multiple, Access Control block rules for any traffic you wish to explicitly block based on OSI layer 5 and above and place directly following the rules created in best practice 5.

6.) Create an, or multiple, Access Control Allow rules for any traffic you wish to allow and inspect with targeted layer 7 inspection policies based.

7.) Create an, or multiple, Access Control Allow rules for traffic you wish to inspect with generic layer 7 inspection policies.

**Policy Inheritance:**

The Firepower System allows for the inheritance of Access Control Policies as well as Intrusion policies. These features are extremely useful when ensuring best practices in policy order of operations are followed in an environment with diverse Access Control Policies.

It is often best to create and inherit from an Access Control Policy that contains Access Control Rule Sections/Categories for each of the best practices for policy ordering listed above, with the notable exception of Pre-Filter policy, which cannot be inherited. By
creating an Access Control Policy from which you base all others and enforce sections for best practices, you can ensure that others will continue to place rules in optimal locations for performance and efficacy.

Threat Policy Diversity:

Cisco Firepower Threat Defense has a number of detection functions that occur along the inspection path. These include:

*Security Intelligence (IP based):*

Configured in an Access Control Policy, this monitors or blocks on IP address lists. This is usually used for blacklisting active threat campaigns and is usually updated by threat feeds (such as Talos or 3rd party feeds through RSS or the Threat Intel Director in FMC). Since matching happens immediately after hardware accelerated ACLs, this can also be a place to globally whitelist specific IP addresses that may be entirely trusted. Caution, doing so may then exclude that IP from future threat scenarios.

*Security Intelligence (URL):*

Threat based URL monitoring, done after traffic normalization (configured in the network analysis policy pre-processors). This component blocks (or whitelists) traffic based on URLs provided from Cisco Talos, locally configured URL objects (configured on the Objects page within the FMC), or from third-party feeds (say fed from the Threat Intel Director in FMC). Users should note that this capability is distinct from the URL matching that happens in an access control rule. The URL filtering with the access control policy should be thought of as a content categorization and risk reduction filter. This also means that URLs blocked through this engine will not initiate further detections down the inspection path.

*Security Intelligence (DNS):*

Like the IP and URL security intelligence monitor this is a threat focused engine enabled with data from Cisco Talos, locally configured objects or third-party feeds. This component is matching DNS requests to threat feeds. Since almost every connection request requires domain resolution, this is often a way to further reduce additional processing by preventing potentially threat laden sessions from even being initiated.
Application Detection:

Application is not really a threat detection component, but it is a way to start reducing risk. Mindful analysts might regularly review application sessions that are associated with IPS, File and Malware events. If applications are being heavily associated with threat conditions, it may be worth blocking those applications entirely.

(examples from FMC Context Explorer and Dashboard)

The OpenApp ID capability of Firepower Threat Defense also provides a mechanism to further enhancing detection and traffic control. Some uses cases can include matching custom applications or even creating applications on FQDN’s that you may want to include or exclude from further inspection.

Application Detection, as well as Host Profiling, and Passive User Identification are all enabled within the Network Discovery Policy.

Malware and File Detection:

Configured in the Malware and File Policies, this function is processed as a session passes it’s matching Access Control Rule and before being passed to a corresponding IPS policy (if configured in the Access Control Rule). There are two key components to this feature: file control and malware detection/blocking. Since file detection requires
significantly less processing or time than malware detection. Administrators may want to make sure file blocking is used to do risk reduction and performance improvement by blocking unwanted file types from crossing the network boundary and, when possible, be done higher in the access control rule stack.

For both file and malware detection, administrators should consider the traffic stream’s ability to be inspected for files. For example, an access control rule that provides “an allow” for SSL or SSH traffic (by application) will not allow the user to enable a file policy. But if a similar rule on just port TCP/port 22 traffic is enabled then a file policy can be enabled but may not be able actually inspect the traffic being passed.

*Intrusion Prevention:*

Built on the Snort® IPS engine, this is the rules based deep-packet inspection engine. IPS rules are provided by Cisco Talos or can include third-party rules written in the open source Snort® rules language. Administrators can select from default policies provided by Cisco Talos then build on or customize those policies to their environment.

*Considering IPS Variables:*

Every IPS rule uses at least two variables: $HOME_NET and $EXTERNAL_NET. The variables give the IPS a sense of directionality regarding threats across a perimeter. How these are configured greatly effects if you will see more or less events and performance as it can impact the number of sessions that may map to an IPS rule.

Understanding this, can allow you to adjust the variables to either a) reduce event counts (by inspecting fewer flows) or b) show you potentially compromised conditions in your net. You can modify and create your own Variable Sets in the Object Management Page. Just look for “Variable Sets” on the left hand list.

$HOME_NET is usually defaulted to the IPv4 Private IP Space. If you have any public IP addresses the IPS may see you will probably want to include those in the $HOME_NET variable. Odds are high, your initial implementation consultant helped you do just this.

$EXTERNAL_NET is usually set on one of two states at most custom sites I’ve seen. It is either: “!”$HOME_NET” (the “!” character is used as a “not” condition in variables and search queries) or “any”. Depending on how this is set on different AC Rules may change what you see.
Most of the IPS rules that monitor for attacks against vulnerabilities are written as 
$EXTERNAL_NET -> $HOME_NET. This means you may get the follow conditions:

<table>
<thead>
<tr>
<th>IPS Rule Setting</th>
<th>$External_NET</th>
<th>$HOME_NET</th>
<th>When exploiting a vuln</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable Setting</td>
<td>! $HOME_NET</td>
<td>&lt;internal IP space&gt;</td>
<td></td>
</tr>
<tr>
<td>Attack 1</td>
<td>Src: Ext_IP</td>
<td>Dst: Int_IP</td>
<td>IPS will inspect</td>
</tr>
<tr>
<td>Attack 2</td>
<td>Src: Int_IP</td>
<td>Dst: Int_IP</td>
<td>IPS will NOT inspect</td>
</tr>
<tr>
<td>Attack 3</td>
<td>Src: Int_IP</td>
<td>Dst: Ext_IP</td>
<td>IPS will NOT inspect</td>
</tr>
</tbody>
</table>

Keep in mind that attack 2 may be an internally exploited asset attacking another internal asset. Which is what we have now seen with threats like WannaCry. Attack 3 may be a scenario where a compromised asset, within your network is now attacking external assets (maybe a mobile user who is unknowing part of a bot-net). A detection of Attack 3 would be an Indication of Compromise and worth finding.

The “easy” way out is making both variables “any”. But this puts unnecessary demand on the IPS engine and can cause more events to be generated than you want.

Indication of Compromise rules provided by Talos are written differently. Since these rules are looking for behaviors from internally devices already compromised and trying to access external threat actors, they are written as $HOME_NET => $EXTERNAL_NET. And in almost every single instance of these rules, that is exactly the condition that is going to occur. This means that detections between internal assets or external to internal assets are just not going to occur. For these rules, having $External_NET as “!/ $HOME_NET” is a good idea.

This means, you can further refine detections within your access control rules based on different variable sets if you want. For Internal user traffic going to and from the Internet, you want $EXTERNAL_NET to be “Not $HOME_NET”. For Access Rules that are controlling Internal-to-Internal Traffic, you may want the variables to have $External_NET set to “any” or to your internal address space. Considering these in your AC Policy rules will give you an even tighter IPS policy, help you capture devices that are already compromised, and potential reduce noise.

**So why the review of IPS variables?**

All of this is shared so that you can consider both the detection conditions and the built-in thinking of directionality in conjunction with event analysis logic. Knowing the variable
conditions of a specific detection point can help prioritize event analysis more effectively, especially when leveraging Impact analysis within the Firepower Management Center. How variables are leveraged should be based on the access control configuration and local threat detection concerns.

Considering Firepower Recommendations:

Firepower Management Center (FMC) offers FTD administrators a capability to recommend IPS rules that match potential vulnerabilities that may exist on hosts within the network. Optimizing this capability, users should consider three important components.

- Networks to Examine selects the IP address(es) that will be considered for IPS rule to Host Vulnerability Mapping. If multiple IPS policies are being used or IPS Policies are built to their specific traffic conditions, then make sure the CIDRs used within this component only align to the IP addresses of Hosts that can actually be inspected within the traffic being monitored by the specific IPS policy.

- Recommendation Threshold informs Firepower Recommendations which IPS rules should be selected. IPS rules are categorized as have a Low, Medium, or High performance impact. Selecting Low would mean only rules that have a Low performance impact will be recommended. Selecting High will include any rule that matches on a vulnerability mapping. Remember, this is not based on an IPS Rule’s priority (which is also labeled Low, Medium, or High).

- Accept Recommendation to Disable Rules can provide a significant reduction of IPS rules that will be enabled within an IPS policy, as it will disable any IPS rule that does not map to a potential vulnerability on hosts within the network. The often-unexpected side-effect is that many of the IPS rules within the Firepower system do not contain a vulnerability mapping and thus would be disabled when this item is checked. For example, IPS in the “Indication of Compromise” category are almost entirely devoid of a CVE or vulnerability reference. These and other detections are based on finding either already compromised hosts, potential policy violations, or other risk factors that be expressing themselves in the network.
There are two ways to optimize for this, and many organizations may want to use both. The first is for internal-to-internal detection conditions, users may want to either disable this action, or create an IPS policy layer within the IPS policy to enable specific policy considerations.

The other action is to leave this item unchecked on externally facing traffic. Since most of indication of compromise (and other similar rules) are based on an $HOME_NET to $EXTERNAL_NET (ie. Internal to External) traffic pattern, keeping this item un-checked will insure Cisco’s recommendations for indications of compromise are not automatically disabled.

If users choose to leave this item checked within a perimeter IPS policy, users can identify most of these rules by searching from them within the IPS Policy configuration engine by using the search filter: metadata:"impact_flag red"

Architectural Considerations:

The architecture you are leveraging has an impact on how best to design the order of operations of your Access Control Policy. In each architecture, Pre-filter fast-path traffic may or may not be offloaded to an ASIC and may or may not be serviced by a process sharing resources with layer 7 inspection. Predominantly the impact to best practices for Access Control order of operations is related to what traffic should be pre-filter fast-pathed and what traffic should be marked Access control policy trust. Below is a listing of the three commonly used architectures of FTD, their platform specific considerations and best practices.

NG 4100/9300:
Special Platform Considerations:

- Pre-filter fast path rules can and will be flow-offloaded (send to ASIC). **Warning:** This should not be used for short lived flows, such as DNS, as the cost of initial fast-path session establishment is computationally expensive.
- Traditional Firewalling and Layer 7 inspection share the same compute resources. Overutilization of one can impact the other.
- LACP and Layer 2 handled by FXOS and managed in Chassis Manager.

Platform Specific best practices:

- Only pre-filter fast-path long lived flows that should avoid Layer 7 inspection. These would be flows like backups, database replications, etc that transmit large amounts of data over a single connection.
- Do not pre-filter fast-path traffic that is short lived, such as DNS, as ASIC session creation may impact the speed of this type of traffic. This traffic should be marked trust in the Access Control policy (Assuming Security Intelligence is enabled)
NG 2100:

**Special Platform Considerations:**

- Pre-filter fast path rules will **NOT** be flow-offloaded (sent to ASIC). They will be handled by the LINA process and occur on the ASIC the LINA process is running on.
- Traditional Firewalling and Layer 7 inspection do **NOT** share the same compute resources.

**Platform Specific best practices:**

- Pre-filter fast-path any traffic that you wish to avoid Layer 7 inspection and only receive traditional ASA inspection. Traffic serviced by this will not count against the traffic that layer 7 engines can process.
vFTD/ASA 5500-X FTD

Special Platform Considerations:

- Pre-filter fast path rules will **NOT** be flow-offloaded (sent to ASIC). They will be handled by the LINA process.
- Traditional Firewalling and Layer 7 inspection share the same compute resources on the same kernel. This includes fast-path flows being serviced by the LINA process.
Platform Specific best practices:

- Pre-filter fast-path any traffic that you wish to avoid Layer 7 inspection and only receive traditional ASA inspection. This traffic will be processed more quickly avoiding layer 7 detection, but will still be utilizing resources from the same pool as the layer 7 engine.

How does this impact order of operations?

As described above, dependent on the platform we need to be careful of what traffic is included in our pre-filter policy and select traffic that plays to the strengths of each platform. This information is indicated in the Best practices for policy ordering section above.

Legal Information:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.
All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.