Discussion Overview

* Cisco Firepower Next-Generation IPS (NGIPS)
* Cisco Firepower Threat Defense (FTD)
* Cisco Firepower Threat Intelligence Director (TID)
* Cisco Advanced Malware Protection (AMP)
* Covered in the discussions above
  + System Monitoring/Dashboards

Intrusion Policy Overview (NGIPS)

Cisco Firepower Next-Generation IPS (NGIPS) provides network visibility, security intelligence, automation and advanced threat protection.

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Intrusion policies are defined sets of intrusion detection and prevention configurations that inspect traffic for security violations and, in inline deployments, can block or alter malicious traffic. Intrusion policies are invoked by your access control policy and are the system’s last line of defense before traffic is allowed to its destination.

At the heart of each intrusion policy are the intrusion rules. An enabled rule causes the system to generate intrusion events for (and optionally block) traffic matching the rule. Disabling a rule stops processing of the rule.

IPS IDS

What is difference IDS and IPS?

**IPS** stands for intrusion prevention system. An **IPS** is similar to an **IDS**, but it has been designed to address many of an **IDS's** shortcomings.

For starters, an **IPS** sits **between** your firewall and the rest of your network. ... **IPS** systems also differ from **IDS in the** way that they detect attacks.

Cisco Firepower Threat Defense (FTD)

Is an integrative software image combining CISCO ASA and FirePOWER feature into one hardware and software inclusive system. Cisco is a pioneer in the Next Generation Firewall Vendors, where competitors are limited to single platforms.

Cisco Threat Intelligence Director (TID)

Using open industry-standards interfaces, Threat Intelligence Director ingests intelligence from multiple sources. It then facilitates the appropriate monitoring and containment actions. It correlates observations with third-party sources to reduce the total number of alerts you need to review.

Rule categories

* Rule Types
* Rule Conditions
* Rule Responses
* Rules vs Building Blocks
* Creating Custom Rules
* Anomaly Rules
* Creating Anomaly Detection Rules
* Domain and Tenancy Rules

Advanced topics

* Out of the Box Rules
* Local and Global Correlation
* Historical Correlation
* Manage Rules
* Observing behavior
* Test with Counters
* Inactivity tests
* Expensive tests
* Offensive Naming
* False Positives
* Working with Support.

What are rules?

* Rules perform tests on events, flows and offenses to detect unusual activity in your network.
* FMC is capable of generating an extensive number of rule combinations to test against event data, flow data or offenses.
* If all of the conditions of a test are met, the rule may generate a response.
* Tests in each rule can reference building blocks or other rules.
* A rule that is referenced by another rule cannot be disabled or deleted (system checks for dependencies) during modifications.
* Similar rules are grouped together by category, such as audit, exploit, DDoS, Recon and more.

Rules Types

Event Rules

* Test against incoming log source data that is processed in real-time and previously processed data (historical data) by the FMC Event Processor.
* Event rules can perform tests against a single event or event sequences.

Flow Rules

* Test against incoming flow data that is processed by the Flow Processor.
* Flow rules perform test against a single flow or flow sequences.

Common Rules

* Test against event and flow data.

Offenses Rules

* Test the parameters of an offense to trigger more responses
* Do not create new events or offenses.

Domain-Specific Rules

* If a rule has a domain test, you can restrict that rule so that it is applied only to events that are happening within a specific domain

How to Rules work.

FMC Event Collectors

* Gather events from local and remote sources
* Normalize these events
* Classify them into low-level and high level categories

FMC Network Flow Ccollectors

* Read packets from the wire or receive flows from other devices and then converts the network data to flow records.
* Each Event / flow processor processes events or flow data from the FMC event / flow collectors.

The custom rules engine

* Processes event and compares them against defined rule to search for anomalies
* Keeps track of the systems that are involved in incidents that contribute events to offenses.

Rule Conditions

* Each rule might contain functions, building blocks, or tests.
* With functions, you can use building blocks and other rules to create a multi-event, multi-flow or multi-offense function.
* You can connect rule using functions that support Boolean operators, such as OR and AND
* You can also use AND NOT to exclude tests or rules from the rule.

The basic components of rules are tests.

* Tests are performed on log activity events,
* Network activity events,
* Rules
* Offenses
* Tests can be simple (e.g. is it a weekday) or complex (e.g. if X followed by Y within Z timeframe)
* Tests are evaluated in the order in which they appear in a rule
* Ordering test is important for performance
* Tests are evaluated on the EP / FP and / or Console (by the CRE)
* Rules can have Actions and Responses

Rule Responses

* If the tests of a rule match, the rule generates the configured actions and responses:
* Create an Offense
* Dispatch a new event
* Send an email
* Generate system notifications on the dashboard feature
* Add or remove data to reference sets
* Add or remove data to reference data collections
* Generate a response to an external system
* Trigger a scan
* Run a custom action script in response to an event