28：Intrusion Policy

2019年7月21日　　14:10

目录

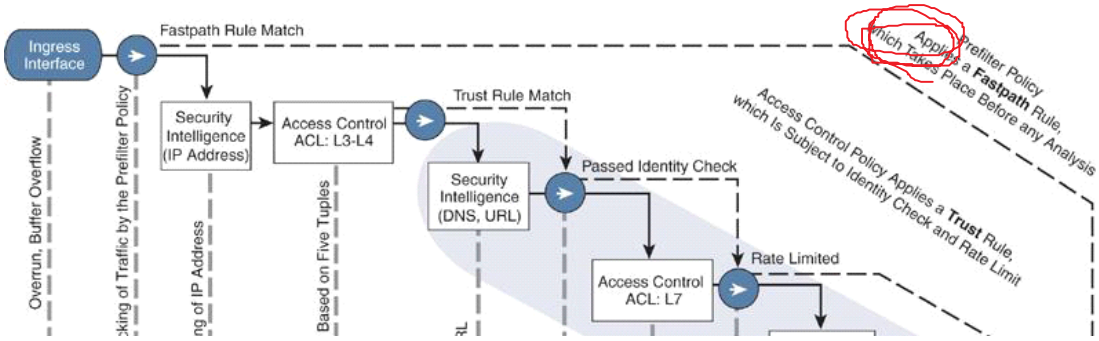
1：官方资料

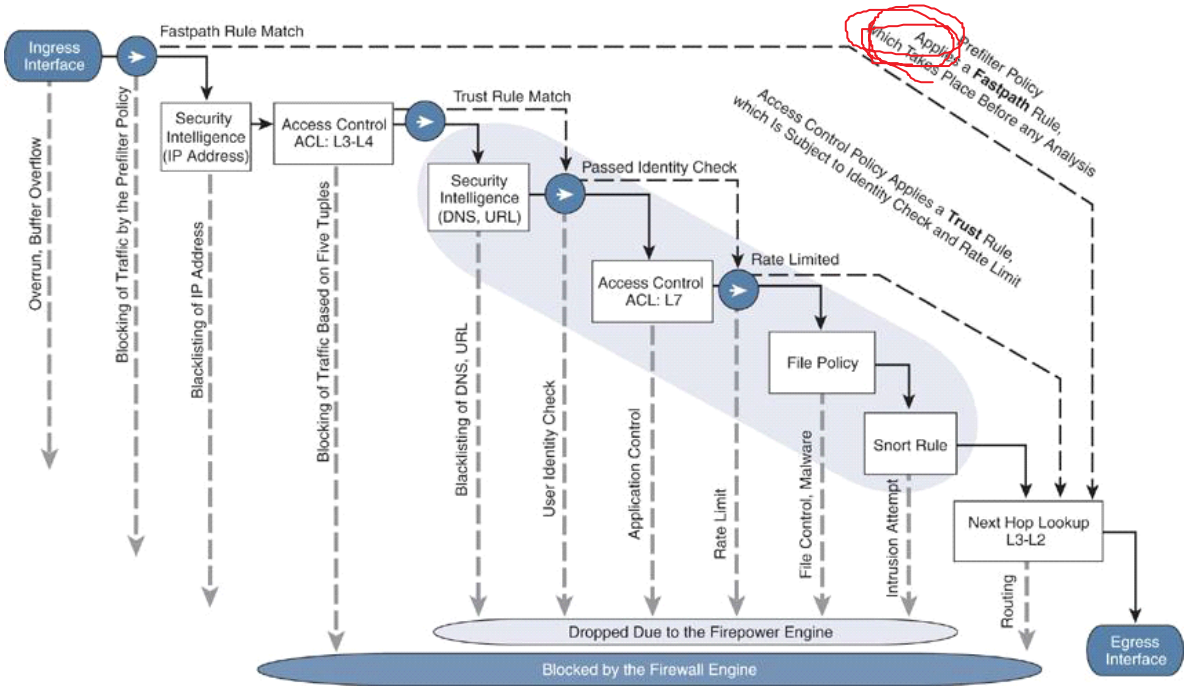
Cisco Live

2：Intrusion Prevention 入侵防御

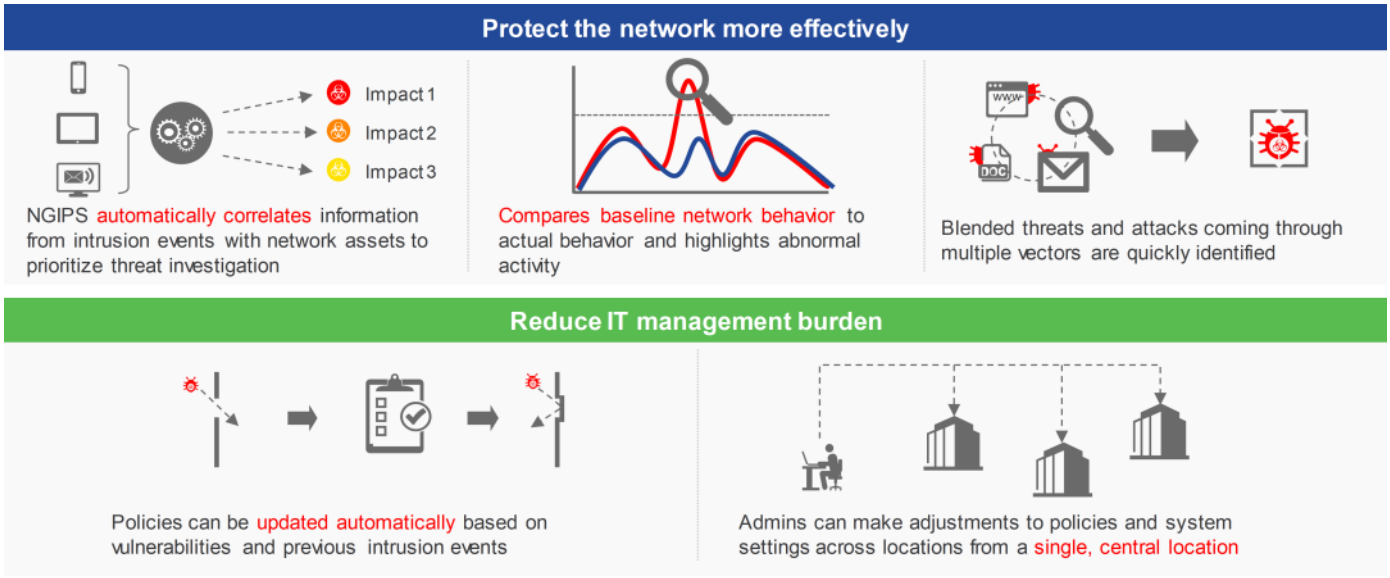
2.1：Firepower NGIPS介绍

- FTD设备使用开源的Snort（IDS/IPS）来执行深度数据包检测Snort可以检测入侵尝试行为。
- Snort规则分析数据包是Firepower引擎检测最后阶段的工作，任何bypass/trust流量都不会被Snort规则约束





2.2：NGIPS优点



- NGIPS比其他入侵防御系统更有效地保护了网络。
- NGIPS持续扫描网络流量时，会使用有关设备和应用程序的所有信息来更好地分析入侵事件。 NGIPS可以评估每种威胁并确定哪些入侵事件具有影响力，并应立即对其进行调查。威胁关联将资源集中在最有影响力的事件上，最多可将可操作事件减少99%。
- 下一代IPS网络行为分析的网络分析功能可将基准网络行为与实际行为进行比较，并识别超出“正常”容忍度的活动。通过数千个日常安全事件进行筛选几乎是不可能的，并且会导致合法警报被忽略。下一代IPS自动化影响评估可将威胁与主机漏洞情报，网络拓扑和攻击上下文相关联，以减少可操作的安全事件的数量。
- NGIPS通过其多向量关联功能，可以通过关联和列表化各种攻击平面上的可疑行为并整合网络和文件级活动，从而更轻松，更早地识别受感染的主机。
- 除了更有效地保护网络之外，NGIPS还可以通过自动确定适当的IPS规则以抵御环境中所包含的风险来帮助减少IT人员的工作量。此功能不仅可以提高安全性，还可以使组织利用其有限的资源来做更多的事情。
- 所有这些都可以随时随地看到和控制。 NGIPS可以在现场或跨位置远程管理，以确保保护始终是最新的，同时减少了IT人员的工作量。

  T：NGIPS功能可促进威胁发现，威胁分析和威胁管理。如果我设定我某一个主机不会访问哪些主机，但是他产生了访问行为，则被判定为攻击。

2.3：如何将FTD部署为NGIPS（参考3/4）

使用FMC部署三个不同策略

- **Network analysis policy：** 与预处理规则协同使用，对流量执行规范化
- **Intrusion policy：** 该策略使用Snort引擎执行深度数据包检测

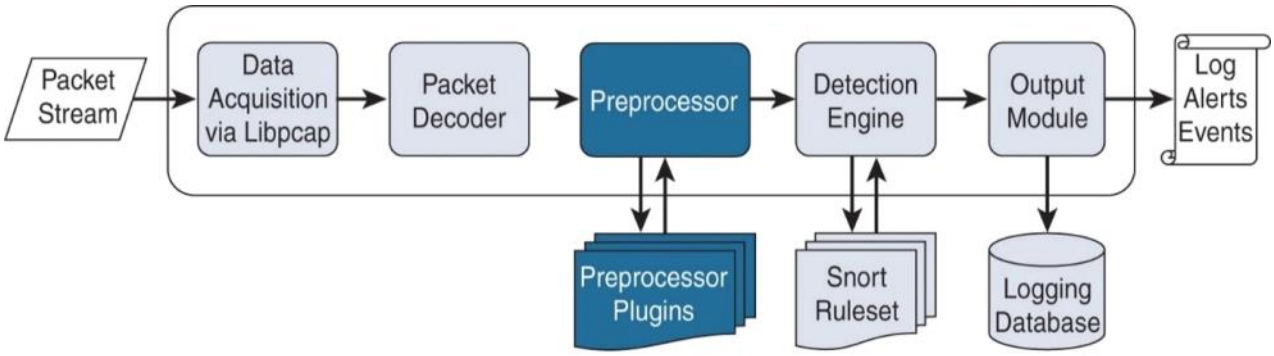
- Access control policy：　调用网络分析策略和IPS策略对数据包进行匹配

3：Network Analysis Policy and Preprocessor

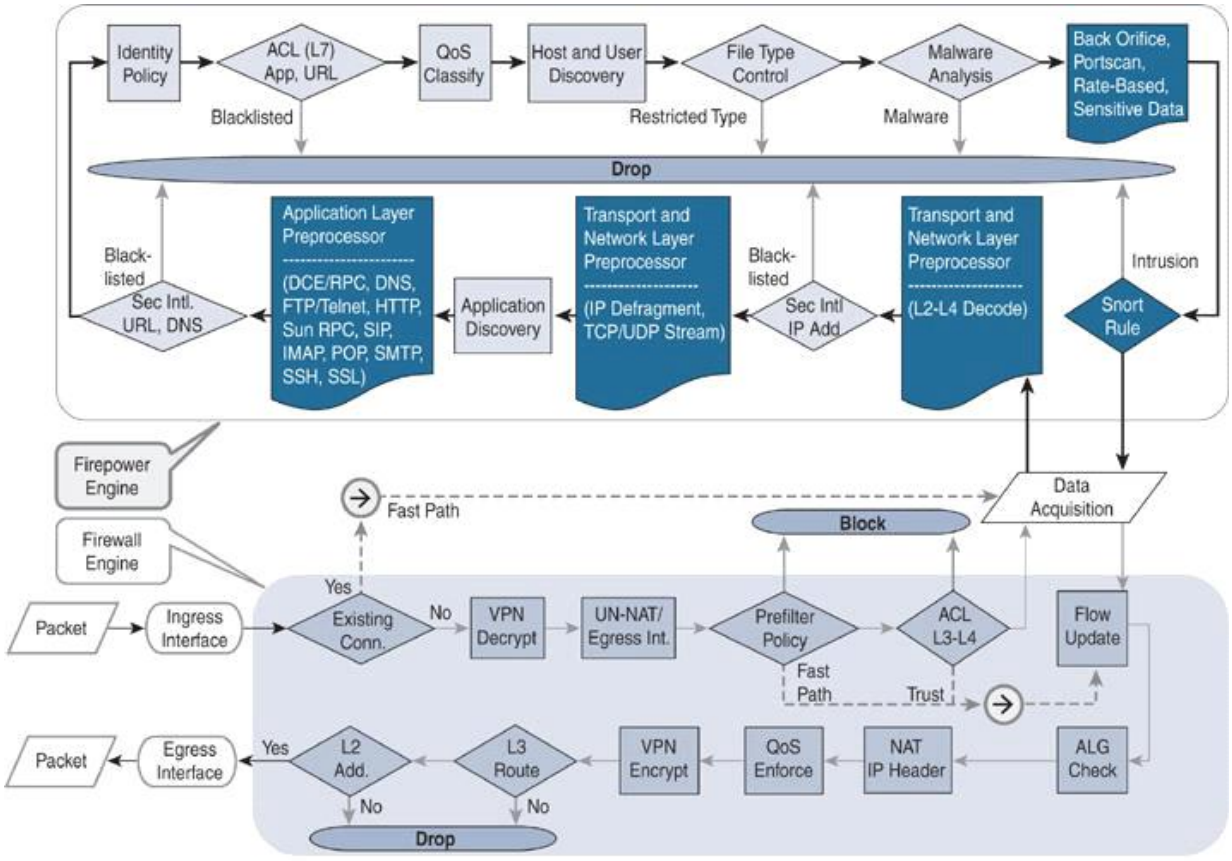
- 执行深度数据包检测前，Snort对数据包进行解码，将其头部和负载简化为Snort引擎可以分析的格式。执行规范化解码的组件=预处理器（Preprocessor），Snort又多种与协议相关的预处理器，可以识别数据包流中的异常情况，检测逃逸计数，并在出现不一致情况（无效/断开异常）丢弃数据包
- 开源Snort预处理器实现和FTD不完全相同，在数据包经历Firepower引擎检查时，Firepower引擎会把不同阶段的流量进行规范化

3.1：开源Snort引擎的预处理器

可以看到预处理器运行在解码数据包后，Snort引擎检查之前



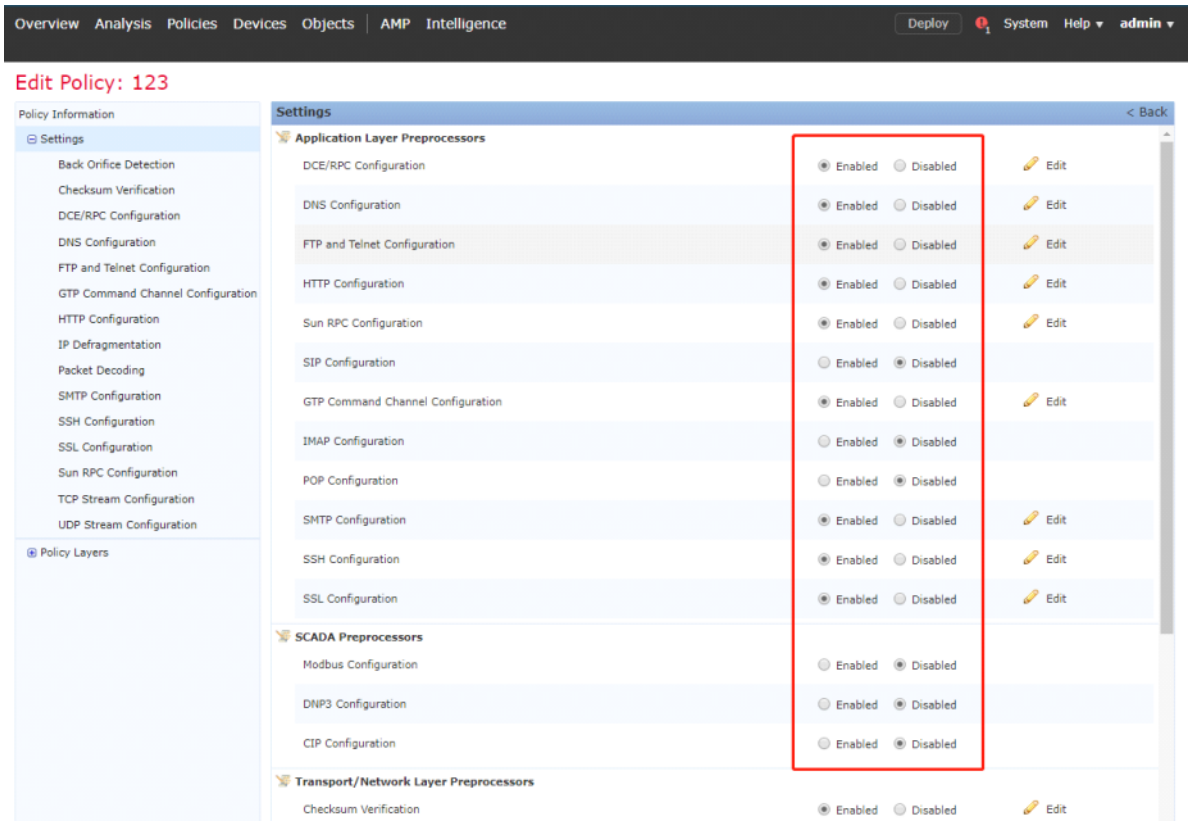
3.2：Firepower-FTD的预处理器运行



Firepower系统上的网络分析策略允许您启用某个预处理器并微调其中的任何细化设置。

预处理器允许Snort对流量进行预处理，解码和规范化，以进行高级检查。 如果您手动禁用了预处理器，但Snort认为该预处理器是必需的，则FTD仍可以在后端使用特定的预处理器，以保护您的网络免受潜在威胁。 但是，网络分析策略配置不会指示FTD何时自动启用必要的预处理器，在视觉上，预处理器设置在FMC GUI上保持禁用状态。

应用层预处理处理器的可以配置各种协议流量的高级设置，包括其他模块的预处理器也都可以



4: Intrusion Prevention policy and snort rules

当数据包使用预处理器进行解码和规范化后，FTD使用IPS规则执行深度包检测。IPS规则是基于Snort规则的语法写的，其中包含漏洞特征。

4.1：Firepower支持来自多个源的Snort规则

- **标准文本规则：**Cisco Talos安全小组在明文文本格式中编写的规则，Snort检测引擎使用这些分析数据包（推荐使用）☆
- **共享对象规则：**Talos使用C语言编写共享对象（Shared object,SO）规则，并为Snort提供编译，SO规则内容不可修改，因为Cisco和第三方之间有约定（推荐使用）☆
- **预处理器规则：**Snort开发团队负责创建这些规则，Firepower引擎使用这些规则解码不同协议的数据包
- **本地规则：**用户在FMC的GUI创建自定义Snort规则。也可以txt编辑规则上传到FMC。Firpower仅支持基于txt的本地规则（不推荐使用，可能会有FTD兼容性问题和性能问题）

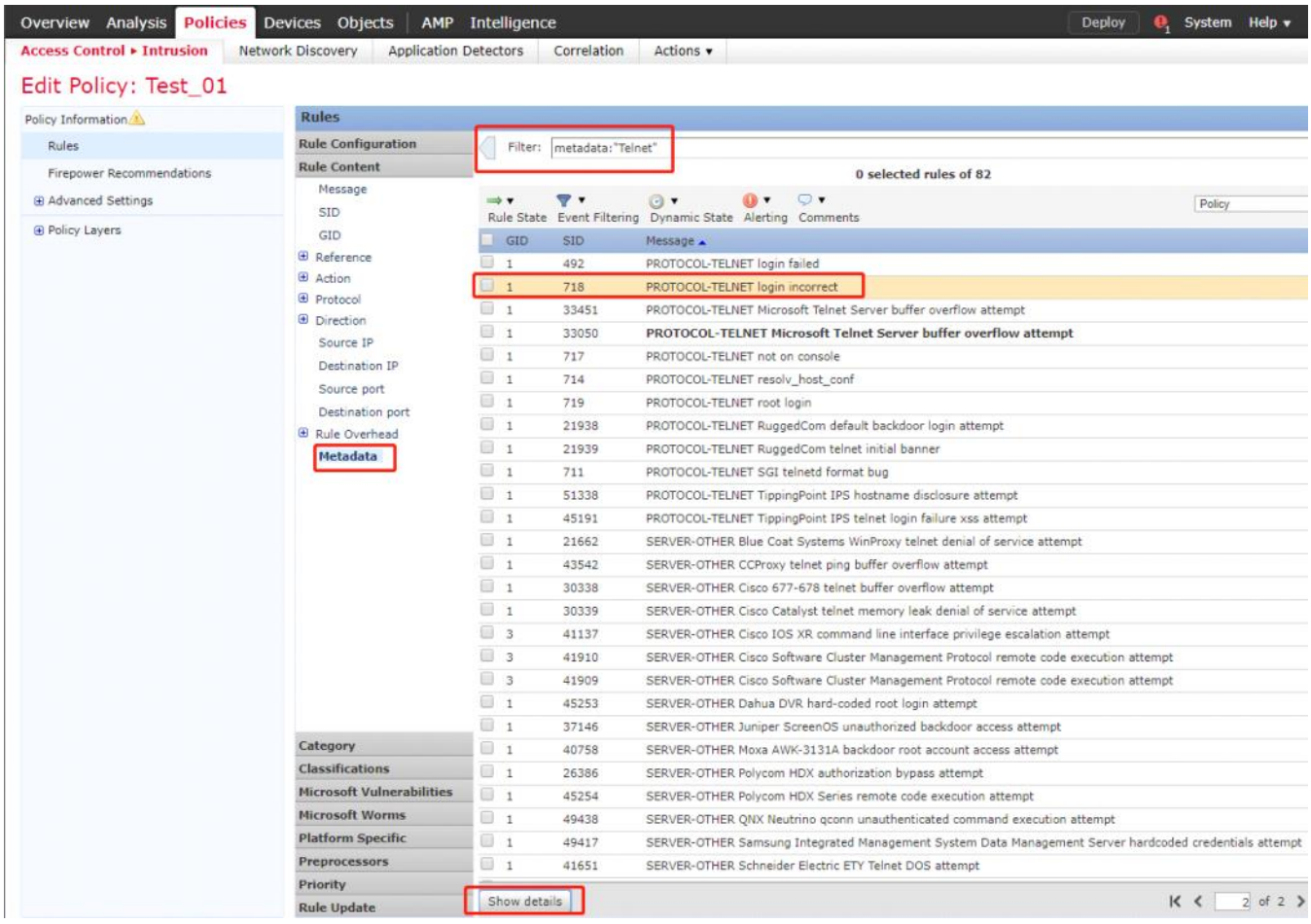
4.2：Snort规则类型

Snort使用唯一的创始者ID（GID）和Snort规则ID（SID）标识一个Rule，根据rule的不同创建者GID和SID编号方案不同

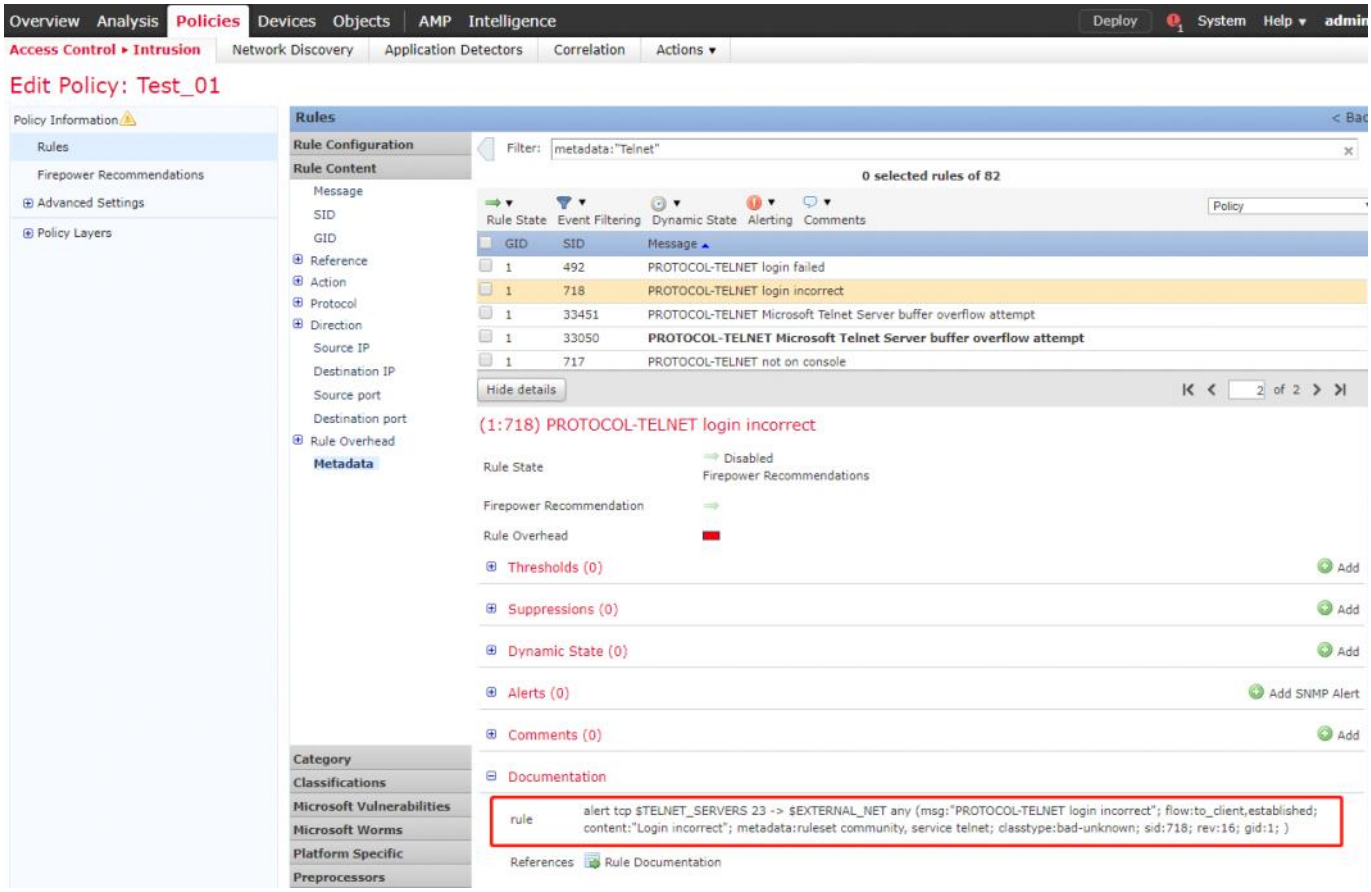
- **Standard text rule** GID is 1. SID is lower than 1,000,000.
- **Shared object rule** GID is 3.
- **Preprocessor rule** GID can be anything other than 1 or 3.
- **Local rule** SID is 1,000,000 or higher.

4.3：筛选Snort规则并举例

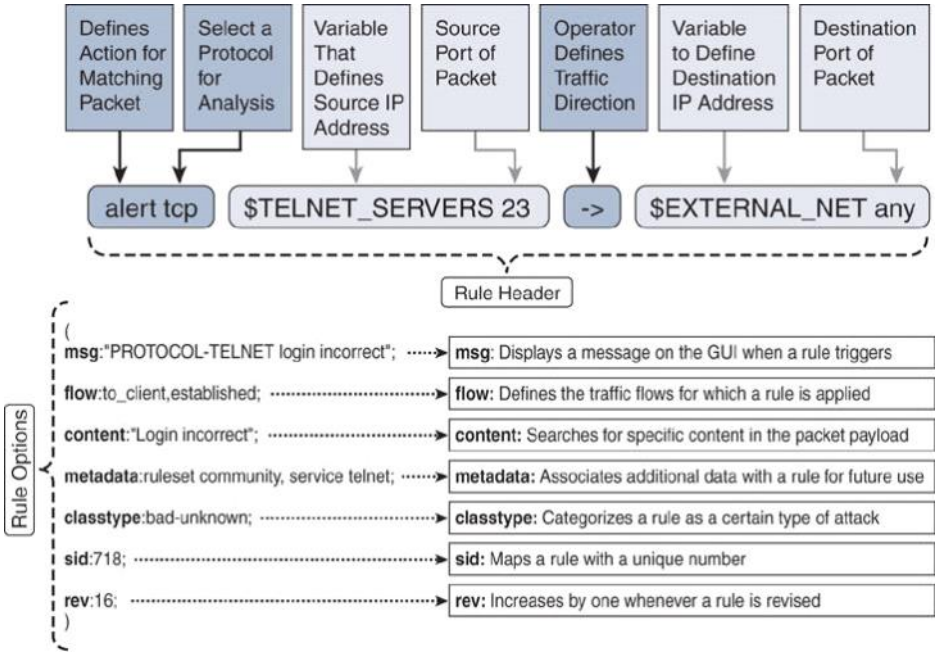
可以进行筛选规则，使用Metadata筛选出和Telnet有关的IPS规则，还可以Show detail查看细节



比如我们查看了GID=1 SID=718的规则，这个规则内容是Telnet登陆不匹配的，



说明了Snort规则1：718，该规则分析$ TELNET_SERVERS变量中的流量以检测潜在的蛮力攻击。
如果您不更改$ TELNET_SERVERS变量的默认值，则Snort会分析来自其他IP地址（与您的真实Telnet服务器一起）的数据包，以获取有效负载中“登录不正确”的内容。



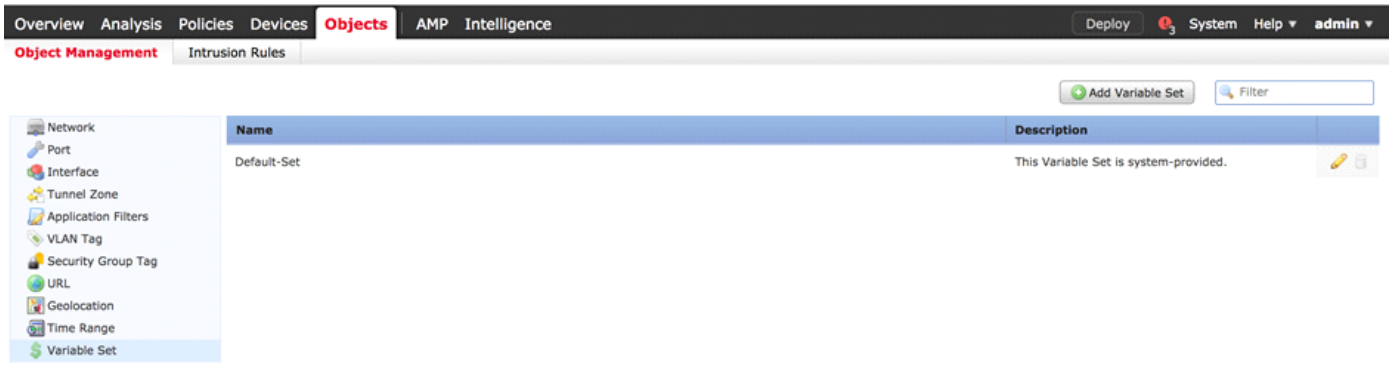
4.4：Snort规则的变量

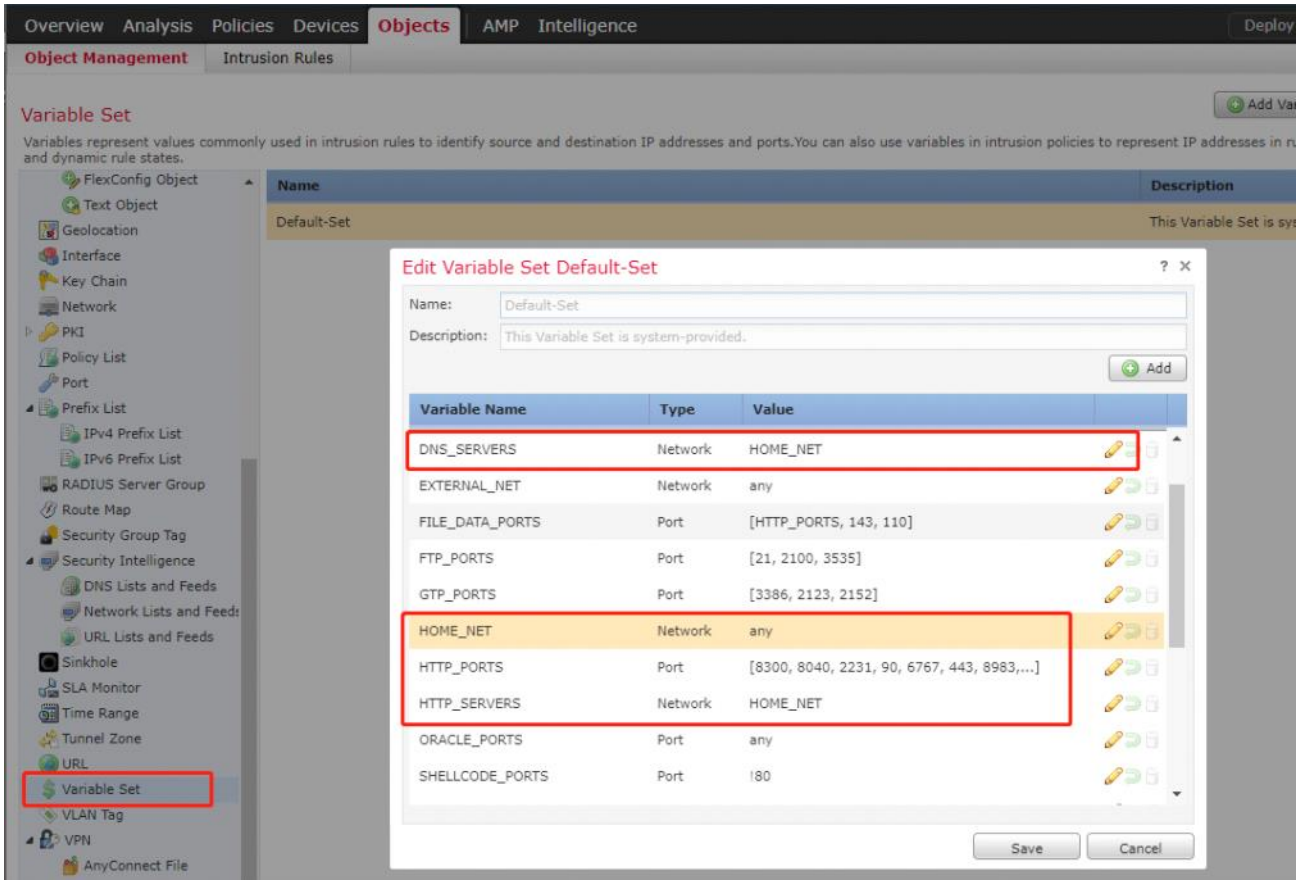
Variable Sets

- Critical componentof IPS tuning
- Associated to intrusion policies in access control policy rules
- Default variable set is provided; custom variable sets can be created
- Support *customized variables* to be used in custom Snort rules

根据网络的实际IP地址填写Snort变量，如果默认值=Any可能会有很多误报（所以填写网络中真实IP地址）

- 比如你还可以填写https服务器的IP地址，DNS服务器的地址，以及telnet/SSH使用的端口（IPS基于此判定是否违规？）
- 填写Home地址包括网络中所有的实际规划真实IP，填写Telnet服务器IP包括所有合法的telnet服务器地址。





Setting *Maximum Active Responses* to a value greater than 0 enables the rules that drop packets to send TCP resets to close the connection. Typically both the client and server are sent TCP resets. With the configuration above, the system can initiate up to 25 active responses (TCP Resets) if it sees additional traffic fr om this connection.

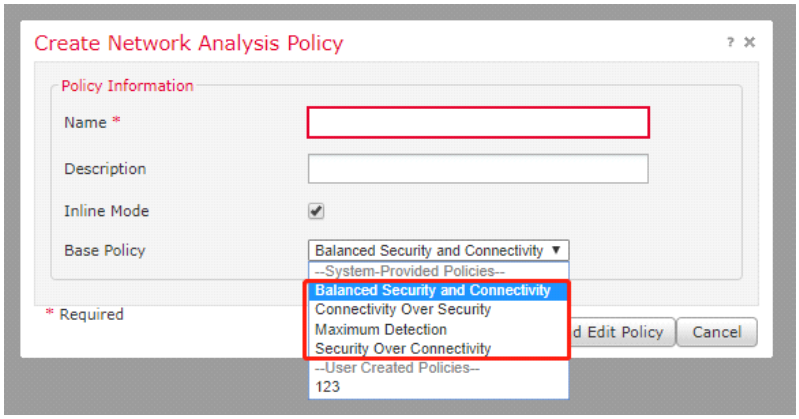
In a production deployment, it is probably best to leave this set to the default. Then no resets are sent, and the malicious system will not know that it has been detected. But for testing and demonstrations, it is generally better to send resets when packets match drop rules.

4.5：IPS策略介绍

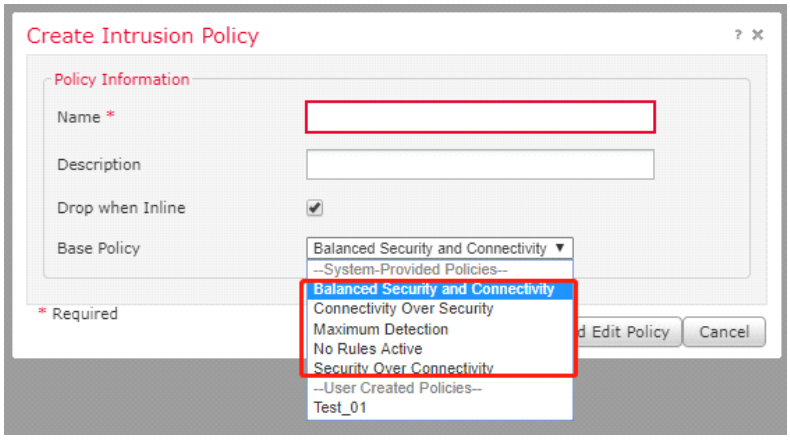
Controls how IDS or IPS inspection is performed on network traffic（控制如何使用IDS/IPS对网络流量进行检查）

- Simple policy inherits settings from 1 of 5 Cisco Talos maintained base policies:（创建的IPS策略会从talos维护的5个基本策略中继承一个）
  a. **Balanced Security and Connectivity** 平衡的安全性和连接性 //Cisco推荐用该策略获取良好的系统性能，不会影响对最新关键漏洞的检测 ☆☆☆
  b. **Connectivity Over Security** – Fewer rules enabled, only most critical rules block 连通信大于安全性 // 启用规则少，把连接速率作优先考虑，只有关键规则会block
  c. **Security Over Connectivity** – More rules enabled, deeper inspection 安全性大于连接性 // 启用更多规则，进行更深入检查，安全性比连接速率和可达性具有更高优先级
  d. **Maximum Detection** – Favors detection over rated throughput 最大检测量 // 优于额定的设备吞吐量的检测机制，安全性比业务连续性具有绝对的优先级。由于最深入的数据包检测行为，终端用户可能会延迟，FTD可能会丢弃一部分合法流量（不推荐）
  e. **No Rules Active** 没有激活的规则！你可以选择该规则以后自定义snort规则。不推荐
- Individual rules can be set to generate events, drop and generate events, or disabled
  （可以为每个规则设置：生成事件，删除和生成事件，或者禁用）
- Layers allow for grouping of settings/rules for easier management （在层次上允许对设置/规则进行分组，简化管理）
- Complex policies can contain multiple layers and multiple levels of inheritance （复杂的策略可以有多个层次和多个继承级别）
- 规则启用越多，设备性能损耗越大

NAP（网络分析策略的四个基本策略类型）



入侵策略的五个基本类型，多出了 no rules active，这个选项意思是里面规则都是禁用的，你可以从头创建入侵策略，或者排查Snort引擎的技术问题

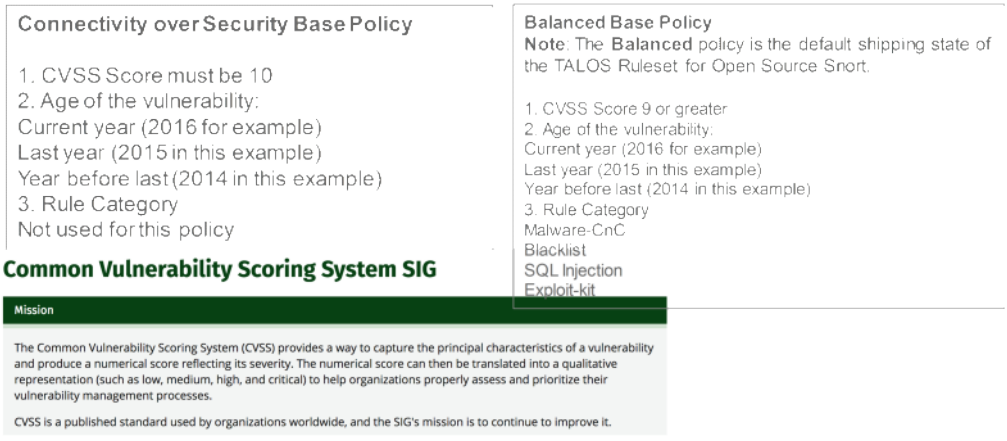


4.6：Default Intrusion policy详解

- 4.5说明了有4种默认的IPS策略，这4种IPS策略默认启用的入侵检测规则数量不一定相同
- Cisco会用漏洞关联的通用安全评分系统（Common vulnerability Scoring System,CVSS）分数来确定一个规则是否应该成为系统策略的一部分（4种默认策略）

规则评分到达指定分数，并且漏洞达到指定年限，则该规则被划入对应的策略类型中

Intrusion Policy	CVSS Score	Age of Vulnerability漏洞年限
Connectivity over Security	10	Current year plus two prior years
Balanced Security and Connectivity	9 or higher	Current year plus two prior years
Security over Connectivity	8 or higher	当前年限加上之前三年
Maximum Detection	7.5 or higher	2005年至今



Security over Connectivity Base Policy

1. CVSS Score 8 or greater

2. Age of the vulnerability:
Current year (2016 for example)
Last year (2015 in this example)
Year before last (2014 in this example)
Year prior (2013 in this example)

3. Rule Category
Malware-CnC
Blacklist
SQL Injection
Exploit-kit
App-detect

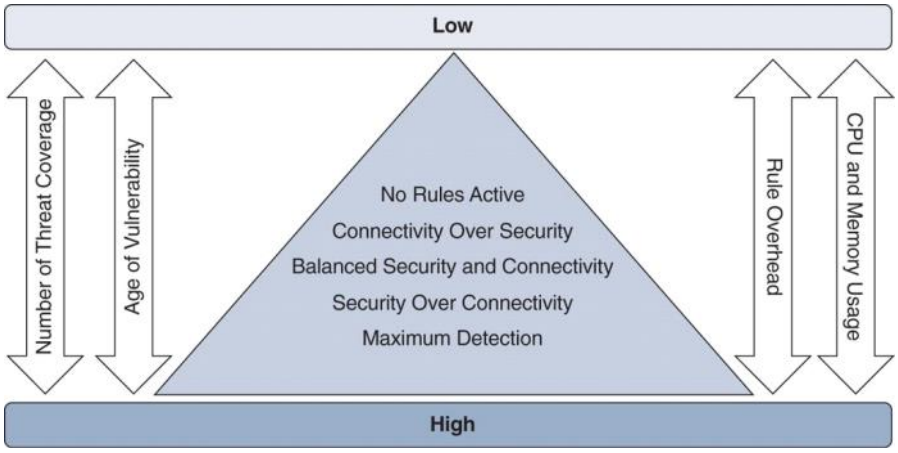
Max-Detect (Maximum Detection) Base Policy:
Note: The "Maximum Detection" policy favors detection over rated throughput. In some situations this policy can and will cause significant throughput reductions. Cisco's Talos continues to recommend the "Balanced Connectivity and Security" policy for most networks, and the "Security Over Connectivity" policy for customers with more rigorous security requirements.

1. CVSS Score of 7.5 or greater

2. Age of the Vulnerability:
2005 or greater

3. Rule Category
Malware-CnC
Exploit-kit

入侵策略的检测范围和处理开销的关联图。可以看到威胁覆盖范围越大，FTD资源利用率越高



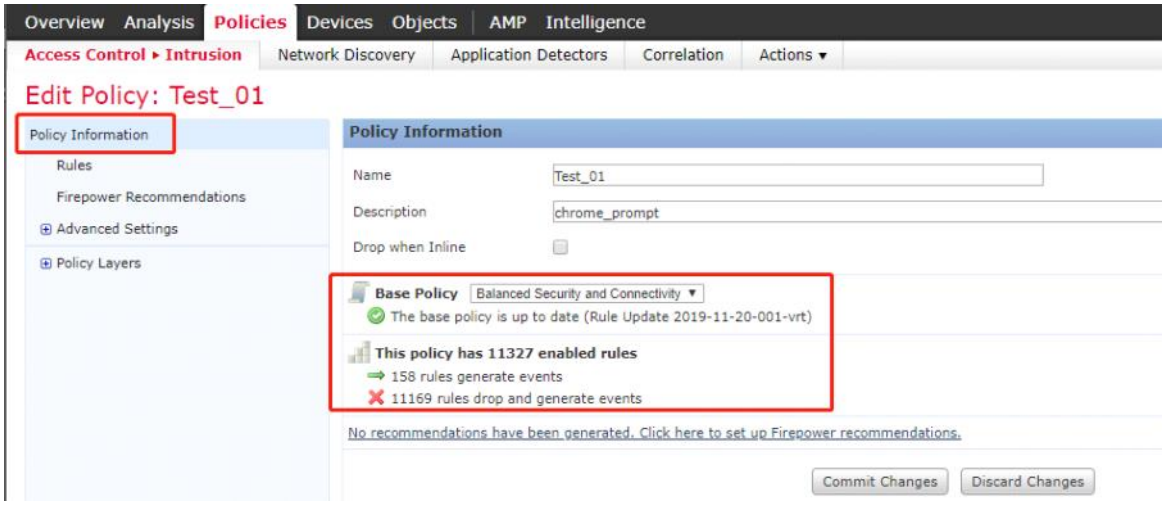
Cisco会周期性发布规则更新，FMC可以通过计划任务从云自动更新规则集，也可以手动下载再传给FMC。

Intrusion Policy	Total Number of Enabled Rules	Rules to Generate Events	Rules to Drop and Generate Events
No Rules Active	0	0	0
Connectivity over Security	459	9	450
Balanced Security and Connectivity	7142	84	7058
Security over Connectivity	10,069	235	9834
Maximum Detection	5533	39	5494

Intrusion Policy	Number of Enabled Preprocessors
Connectivity over Security	15
Balanced Security and Connectivity	15
Security over Connectivity	17
Maximum Detection	18

- Maximum Detection（最大化检测）不意味着启用最多的入侵规则，而是启用最深入的数据包分析，也意味着启用更多的预处理器
- Security over Connectivity（安全性重于连通性）启用最多的入侵规则

可以在你部署的IPS策略中查看启用多少调入侵规则，以及规则集的更新时间



5：威胁指数 Impact Flag

6：Snort Language

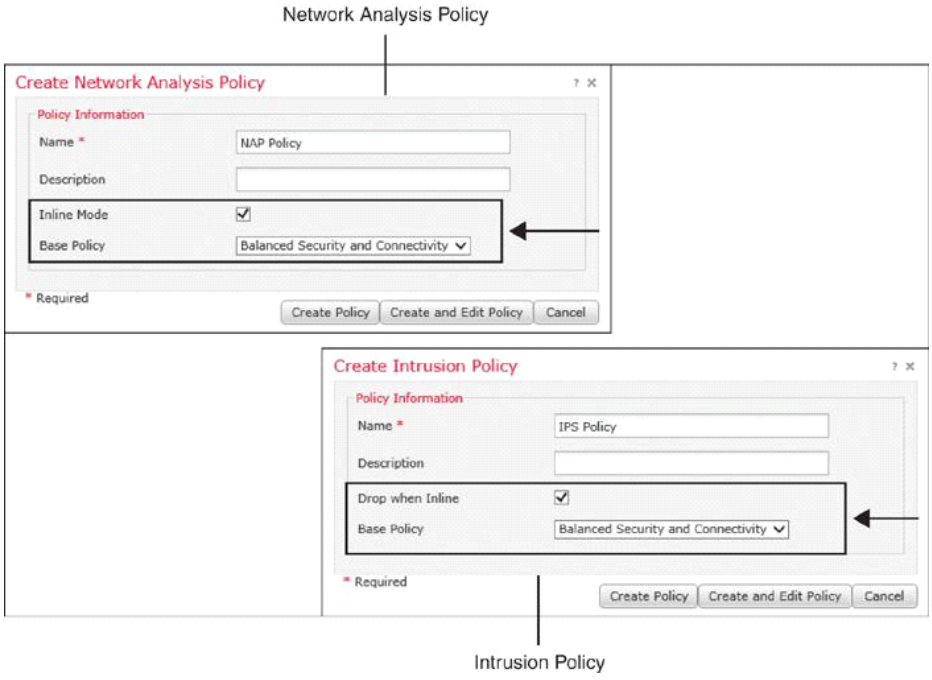
7：Best Practices for Intrusion Policy Deployment

7.1：普通最佳实践

A. 使用TCP五元组匹配数据包（源目端口/IP以及协议号），并且使用ACP匹配五元组，而不适用IPS规则。基于Snort的入侵规则是进行高级深度数据包检测的，“专款专用”

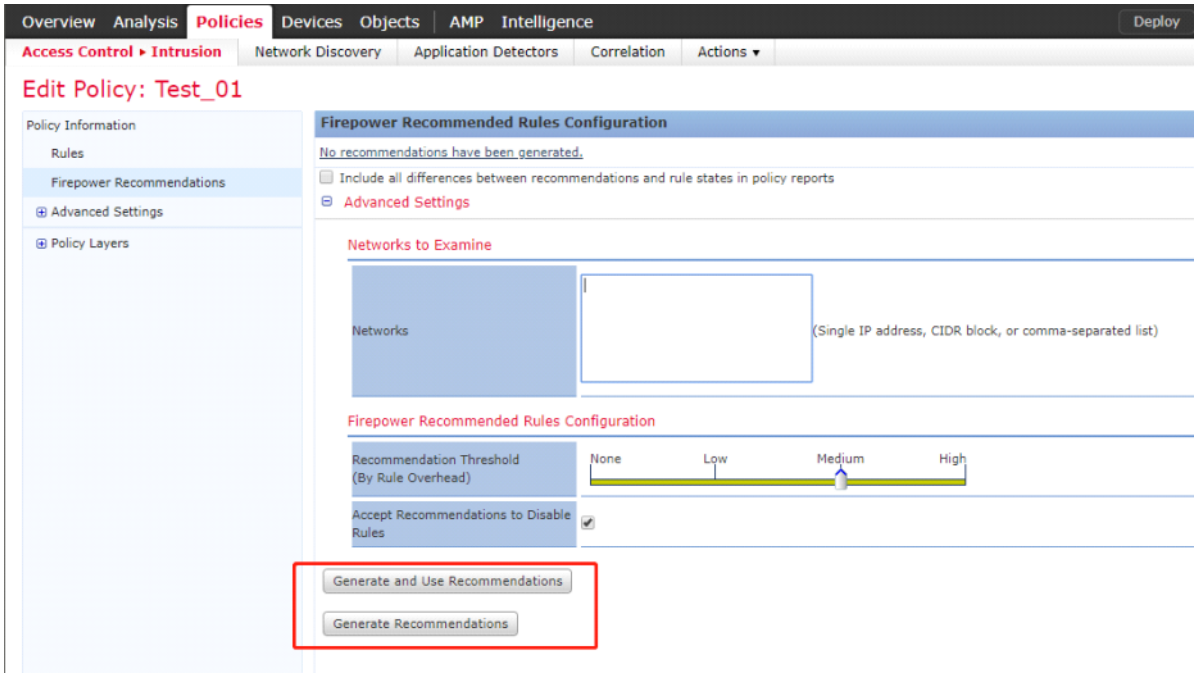
B. 使用Balanced Security and Connectivity作为默认策略（作为新建IPS的基线策略/父策略）

C. 若希望FTD阻塞违反入侵规则的流量，则创建IPS策略时必须选中inline mode 和Drop when inline选项（分别是网络分析策略和IPS规则使用）

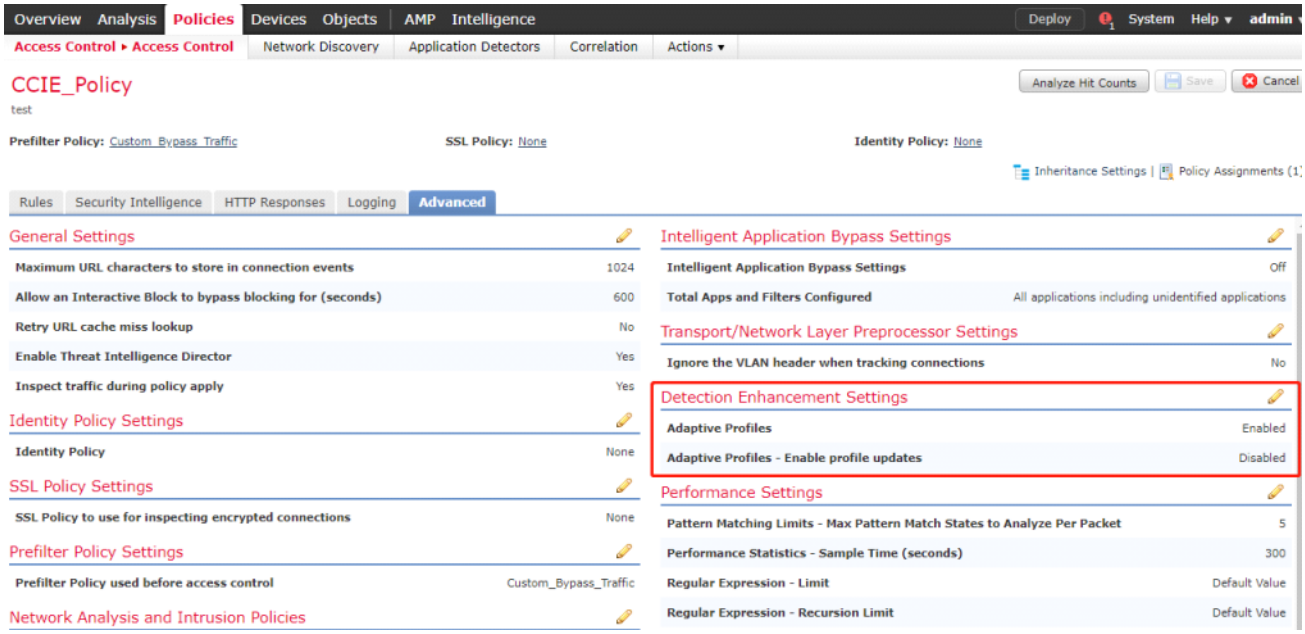


D. 入侵策略中启用Firepower推荐特性，该特性可以与network discovery结合使用，用以确定网络中运行的操作系统，服务和应用相关的入侵规则（规则里匹配了比较细的应用条件）

E. ☆☆生成Firepower推荐的入侵规则配置时，要定义网络来检查并设置推荐门限值，为优化系统性能一定要设置为中等或低等，该功能会根据你的Firepower发现网络中的应用，主机，服务，操作系统等生成推荐的入侵规则（需要谨慎配置☆ 最好balance默认即可，看客户要求把。）



F. 启用Adaptive Profiles和Enable Profile Update（开启自适应文件更新）特性来使用服务元数据，并让FTD只能的将启用的ips规则应用到相关流量上（开需要谨慎☆



备注：启用Firepower推荐特性和启用Adaptive profiles updates特性有区别。

同时开启E和F这两个特性可以让FTD设备启用或禁用与网络上运行主机应用和服务相关的入侵规则，然后将启用的入侵规则应用在这些主机的相关流量上。

Firepower推荐特性	Adaptive profiles updates特性
推荐特性根据发现的应用和主机，来启用和禁用入侵规则	将规则元数据与主机的应用程序和操作系统进行比较，并确定FTD设备是否应将某个规则应用于该主机的某些流量。
如果规则与网络中的主机和应用程序有关，则可以启用该被禁用的规则。	不更改禁用规则的状态。 仅适用于入侵策略中已启用的规则。
在入侵策略中进行配置	在访问控制策略ACP中配置

G. 在网络分析策略NAP中，inline Normalizatoin（在线规范化）预处理器上启用Normalize TCP Paload（规范化TCP负载），这样确保重传数据的一致性（谨慎配置☆

7.2：取决于部署模型的最佳实践

- 如果要通过阻止入侵尝试来防止网络攻击，则需要将FTD部署为BTIW，BTIW需要使用在线接口对inline-pair。（参考16章）
- 如果FTD只是用来检测攻击的，比如IDS模式，可以考虑部署inline tap mode，而不是passive-mode，这样可以实施的切换到inline-mode阻断流量
- 如果一定要部署passive mode，需要确保ACP访问控制策略的高级选项中，开启Adaptive profiles选项。该选项让FTD设备可以根据服务流量，客户端应用流量和主机流量的元数据，动态的自动调整入侵规则

8：IPS场景化示例

虚无缥缈的东西都不实在

- IPS规则可以实现，客户定义网络中哪些是WEB服务器，WEB服务器的服务端口有哪些
- 以及DNS服务器的IP地址，Telnet服务器的IP地址，以及内网中有哪些合法的IP网段
    - 当网络中定义了WEB服务器=172.18.18.222，服务端口=443时，所有客户端访问流量都是正常的

- 但如果网络中出现客户端访问10.10.10.10的Https服务4443时，IPS会报错，还可以block流量，因为这个地址不属于合法的https服务器，并且端口也是不合规的。