入侵防御性能调整

以下主题介绍如何优化入侵防御性能：

关于入侵防御性能调整

思科提供多项功能，用于提高系统在分析流量中的入侵企图时的性能。您可以执行以下操作：

- 指定事件队列中允许的数据包数量。您还可以在数据流重组前后，启用或禁用对将重建到更大数据流中的数据包进行的检测。
- 覆盖入侵规则中使用的 PCRE 默认匹配和递归限制以检查数据包负载内容。
- 选择使规则引擎在生成多个事件时为每个数据包或数据包流记录多个事件，使您可以收集报告事件之外的信息。
- 在安全和通过数据包及规则延迟阈值将设备延迟保持在可接受水平的需求之间保持平衡。
- 配置设备如何监控和报告其自身性能的基本参数。这样，您可以指定系统更新设备上的性能统计信息的间隔。

可以基于每个访问控制策略配置这些性能设置，他们可应用于该父访问控制策略调用的所有入侵策略。

注释 威胁防御版本 7.7不支持 Snort 2。有关 7.7 之前版本中支持的 Snort 2 功能的信息，请参阅与您的 版本匹配的 防火墙管理中心 指南。

入侵防御性能调整的许可证要求

威胁防御 许可证

IPS

入侵防御性能调整的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

限制入侵的模式匹配

过程

步骤 1 在访问控制策略编辑器中，点击 **高级** （**策略** > **控制** > **编辑** > **更多** > **高级设置**）。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 点击**性能设置 (Performance Settings)** 旁边的 **编辑** ()。

如果显示**视图** ()，则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 点击**性能设置 (Performance Settings)** 弹出窗口中的**模式匹配限制 (Pattern Matching Limits)**。

步骤 4 在**每个数据包要分析的最大模式状态数 (Maximum Pattern States to Analyze Per Packet)** 字段中输入要加入队列的最大事件数的值。

步骤 5 要在 Snort 2 中禁用在数据流重组前后将重建为更大数据流的数据包的检查，请选中**对有待未来重组的流量禁用内容检查 (Disable Content Checks on Traffic Subject to Future Reassembly)** 复选框。重组前后的检测需要更多的处理开销，可能会导致性能下降。

重要事项
在 Snort 3 中，**对未来重组的流量禁用内容检查 (Disable Content Checks on Traffic Subject to Future Reassembly)** 复选框的设置包括：

- 选中 - 表示会在重组前检测 TCP 负载。它包括数据流重组前后的数据包检测。这一过程需要更多的处理开销，并且可能会降低性能。
- 未选中 - 表示在重组后检测 TCP 负载。

步骤 6 点击**确定**。

步骤 7 点击**保存**保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

入侵规则的正则表达式限制覆盖

默认正则表达式限制可确保最低性能级别。覆盖这些限制可能会提高安全性，但也会因允许根据低效的正则表达式对数据包进行评估而严重影响性能。

注意 除非在撰写入侵规则方面很有经验，并且了解衰减模式的影响，否则，不要覆盖默认的PCRE限制。

表 *1:* 正则表达式限制选项

选项	说明
匹配限制状态 (Match Limit State)	指定是否覆盖**匹配限制 (Match Limit)**。您有以下选择： • 选择**默认值 (Default)**，以使用为**匹配限制 (Match Limit)** 配置的值 • 选择 **Unlimited**，以允许不限次数的尝试 • 选择**自定义 (Custom)**，为**匹配限制 (Match Limit)** 指定 1 或更大的值，或指定 0 以彻底禁用 PCRE 匹配评估

选项	说明
匹配限制 (Match Limit)	指定在与 PCRE 正则表达式中定义的模式进行匹配时的尝试次数。
匹配递归限制状态 (Match Recursion Limit State)	指定是否覆盖**匹配递归限制 (Match Recursion Limit)**。您有以下选择： • 选择**默认值 (Default)**，以使用为**匹配递归限制 (Match Recursion Limit)** 配置的值 • 选择**无限制 (Unlimited)**，以允许进行次数不限的递归 • 选择**自定义 (Custom)**，为**匹配递归限制 (Match Recursion Limit)** 指定 1 或更大的值，或指定 0 以彻底禁用 PCRE 递归 注意：为使**匹配递归限制 (Match Recursion Limit)** 具有意义，其值必须小于**匹配限制 (Match Limit)**。
匹配递归限制 (Match Recursion Limit)	指定在根据数据包静载荷对 PCRE 正则表达式进行评估时的递归次数。

相关主题

概述：pcre 关键字

覆盖入侵规则的正则表达式限制

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 点击**性能设置 (Performance Settings)** 旁边的 **编辑** ()。

如果显示**视图** ()，则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 点击**性能设置 (Performance Settings)** 弹出窗口中的**正则表达式限制 (Regular Expression Limits)**。

步骤 4 您可以修改入侵规则的正则表达式限制覆盖，第 3 页中所述的任何选项。

步骤 5 点击**确定**。

步骤 6 点击**保存**保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

每个数据包的入侵事件生成限制

当入侵规则引擎根据规则评估流量时，它会将针对给定数据包或数据包流生成的事件放在事件队列中，然后将队列顶部的事件报告至用户界面。配置入侵事件日志记录限制时，可指定队列中可放置的事件数量及要记录的事件数量，并可选择确定队列中事件顺序的条件。

表 *2:* 入侵事件日志记录限制选项

选项	说明
Maximum Events Stored Per Packet	为给定数据包或数据包流可存储的最多事件数量。
Maximum Events Logged Per Packet	为给定数据包或数据包流记录的事件数量。这不能超过**每个数据包存储的最大事件数量 (Maximum Events Stored Per Packet)** 的值。
事件日志记录的优先排列方式 (Prioritize Event Logging By)	用于确定事件队列内事件排序的值。通过用户界面报告排序最靠前的事件。您可以选择以下选项： • `优先级 (priority)`，按事件的优先级对队列中的事件进行排序。 • `content_length`，按识别出的最长匹配内容对事件进行排序。当事件按内容长度排序时，规则事件始终优先于解码器和预处理程序事件。

限制每个数据包生成的入侵事件

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 点击**性能设置 (Performance Settings)** 旁边的 **编辑** (✎)。

如果显示**视图** (👁)，则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 点击**性能设置 (Performance Settings)** 弹出窗口中的**入侵事件日志记录限制 (Intrusion Event Logging Limits)**。

步骤 4 可以修改每个数据包的入侵事件生成限制，第 5 页中的任何选项。

步骤 5 点击**确定**。

步骤 6 点击**保存**保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

数据包和入侵规则延迟阈值配置

每个访问控制策略都具有基于延迟的设置，这些设置使用阈值来管理数据包和规则处理性能。

数据包延迟阈值用于度量适用的解码器、预处理程序和规则在处理数据包时所需的总时间，并在处理时间超过可配置阈值时停止对数据包的检测。

规则延迟阈值功能可以衡量每个规则处理各个数据包所花费的时间、将超过阈值的规则及一系列相关规则暂停指定的时间（如果处理时间连续超过规则延迟阈值一定次数 [可配置]），以及在暂停到期后恢复规则。

注释 威胁防御版本 7.7不支持 Snort 2。有关 7.7 之前版本中支持的 Snort 2 功能的信息，请参阅与您的 版本匹配的 防火墙管理中心 指南。

基于延迟的性能设置

默认情况下，系统会从已在系统中部署的最新入侵规则更新中获取基于延迟的性能设置。

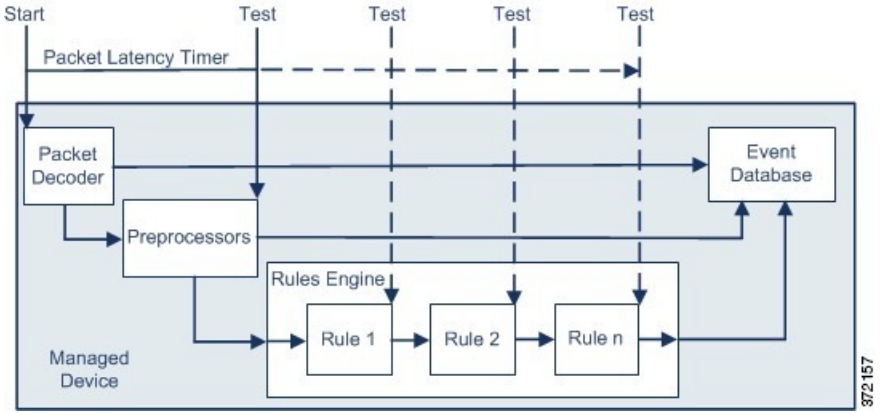
实际应用的延迟设置取决于与访问控制策略关联的网络分析策略 (NAP) 的安全级别。通常，这是指默认 NAP 策略。但是，如果已配置自定义网络分析规则，并且其中任意一个规则指定的 NAP 策略安全级别都高于默认 NAP 策略，则延迟设置取决于自定义规则中安全级别最高的 NAP 策略。如果默认 NAP 策略或任何自定义规则调用自定义 NAP 策略，则评估中使用的安全级别是每个自定义 NAP 策略所基于的系统提供的基本策略。

不论有效阈值和/或网络分析配置直接在策略中继承还是配置，上述情况均成立。

数据包延迟阈值

数据包延迟阈值度量所需时间，而不仅是处理时间，目的是为了更准确地反映规则在处理数据包时实际所需的时间。然而，延迟阈值功能是基于软件实现的延迟管理功能，并不能实施严格的定时功能。

性能与源自延迟阈值的延迟优势的权衡取舍在于未经检查的数据包可能包含攻击。解码器处理开始时，每个数据包的计时器开始计时。计时器会持续计时，直到数据包的所有处理工作结束或处理时间在计时测试点超过阈值。



如上图所示，数据包延迟计时在以下测试点测试：

- 在所有解码器和预处理器的处理完成之后且在规则处理开始之前
- 在每条规则的处理之后

如果处理时间在任何测试点超出阈值，数据包检测将停止。

提示 总的数据包处理时间不包括常规的 TCP 数据流或 IP 分片重组时间。

对于由处理数据包的解码器、预处理器或规则所触发的事件，数据包延迟阈值不会对其产生影响。只有当数据包已完全处理完毕，或当数据包处理因超过了延迟阈值而终止时（以先出现者为准），任何适用的解码器、预处理器或规则才会触发事件。如果丢弃规则在内联部署中检测到入侵，则丢弃规则将触发事件并将数据包丢弃。

注释 只有当数据包的处理因超出数据包延迟阈值而停止后，才会根据规则评估数据包。本可触发事件的规则无法触发该事件，同时，丢弃规则无法丢弃该数据包。

通过停止对要求过长处理时间的数据包进行的检查，数据包延迟阈值可提高被动和内联部署模式下的系统性能，并可缩短内联部署中的延迟。例如，这些性能优势可以在以下情形中发挥出来：

- 无论是被动式部署还是内嵌式部署，多个规则连续检测数据包都需要大量时间
- 对于内联式部署，网络性能不佳（例如，当有人下载超大文件时）期间，数据包处理变慢。

在被动式部署中，停止数据包的处理可能无助于恢复网络性能，这是因为，只不过转至处理下一数据包而已。

数据包延迟阈值说明

默认情况下，用于数据包处理的基于延迟的性能设置会被禁用。您可以选择将其启用。但是，思科建议您不要更改阈值设置的默认值。

仅当您选择指定自定义值时，以下信息才适用。

表 *3:* 数据包延迟阈值选项

选项	说明
阀值（微秒）(Threshold [microseconds])	指定数据包检测停止的时间，以微秒为单位。

启用数据包延迟阈值

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 点击**基于延迟的性能设置 (Latency-Based Performance Settings)** 旁边的 **编辑** ()。

如果显示**视图** ()，则表明设置继承自祖先策略，或者您没有修改设置的权限。

步骤 3 在**基于延迟的性能设置 (Latency-Based Performance Settings)** 弹出窗口中，点击**数据包处理 (Packet Handling)**。

步骤 4 选中 **Enabled** 复选框。

步骤 5 点击**确定**。

步骤 6 点击**保存**保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

配置数据包延迟阈值

默认情况下，用于数据包处理的基于延迟的性能设置会被禁用。您可以选择将其启用。但是，思科建议您不要更改阈值设置的默认值。

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 点击**基于延迟的性能设置 (Latency-Based Performance Settings)** 旁边的 **编辑** ()。

系统 () > **监控** > **统计信息**

步骤 3 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 4 在**基于延迟的性能设置 (Latency-Based Performance Settings)** 弹出窗口中，点击**数据包处理 (Packet Handling)**。

系统会默认选择**已安装规则的更新 (Installed Rule Update)**。我们建议使用此默认设置。

显示的值未反映出自动设置。

步骤 5 如果您选择指定自定义值：

- 选中**启用 (Enabled)** 复选框，然后查看数据包延迟阈值说明，第 7 页以了解最低的**阈值 (Threshold)** 设置。
- 您必须在“数据包处理”(Packet Handling) 选项卡和“规则处理”(Rule Handling) 选项卡中指定自定义值。

步骤 6 点击**确定**。

步骤 7 点击**保存**保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

规则延迟阈值

规则延迟阈值度量所需时间，而不仅是处理时间，目的是为了更准确地反映规则在处理数据包时实际所需的时间。然而，延迟阈值功能是基于软件实现的延迟管理功能，并不能实施严格的定时功能。

性能与源自延迟阈值的延迟优势的权衡取舍在于未经检查的数据包可能包含攻击。计时器测量每次根据一组规则处理数据包所用的处理时间。每当规则处理时间超过指定的规则延迟阈值时，系统将使计数器递增。如果连续超过阈值的次数达到指定数值，则系统将采取以下操作：

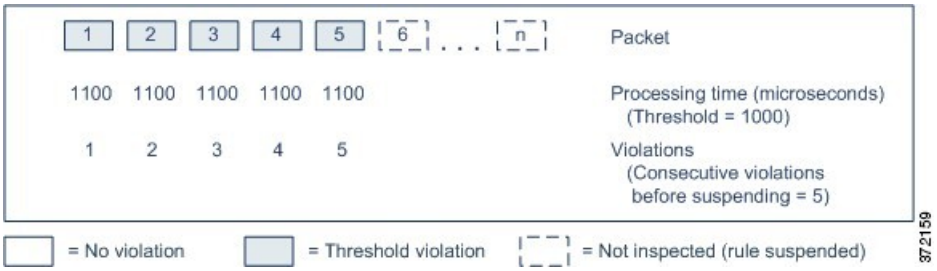
- 在指定时期内暂停规则
- 触发一个事件，指示已暂停规则
- 在暂停到期后重新启用规则
- 触发一个事件，指示已重新启用规则

在已暂停规则组或违反规则的情况不再连续时，系统将使计数器归零。在暂停规则前允许某些连续违反规则的情况，可以使您忽略对性能的影响可以忽略不计的偶然违反规则的情况，转而将重点放在反复超过规则延迟阈值的、更重大的规则影响上。

下面的示例显示了五个连续的规则处理时间，它们并未导致规则暂停。

在上面的示例中，处理前三个数据包中的每个数据包所需的时间都超过了 1000 毫秒的规则延迟阈值，因此违规计数器随着每次违规都会递增。处理第四个数据包并未超过阈值，因此违规计数器复位为零。第五个数据包超过了阈值，因此违规计数器从一重新开始。

下面的示例显示了五个连续的规则处理时间，它们导致了规则暂停。



在第二个示例中，处理五个数据包中的每个数据包所需的时间都超过了1000毫秒的规则延迟阈值。由于对于指定的五次连续违规，每个数据包 1100 毫秒的规则处理时间都超过了 1000 毫秒的阈值，因此该规则组被暂停。不会针对已暂停的规则对任何后续数据包（在该图中表示为数据包 6 至 n）进行检查，直到暂停到期为止。如果在重新启用规则后出现更多数据包，则违规计数器将再次从零开始。

规则延迟阈值处理对处理该数据包的规则所触发的入侵事件没有影响。对于在该数据包中检测到的任何入侵，无论规则处理时间是否超过阈值，规则都会触发事件。如果检测到入侵的规则是内联部署中的丢弃规则，则该数据包将被丢弃。当某一丢弃规则检测到导致该规则被暂停的某一数据包中存在入侵时，该丢弃规则将触发一个入侵事件，该数据包将被丢弃，并且该规则以及所有相关规则都将被暂停。

注释 不会针对已暂停的规则对数据包进行评估。本来能够触发某一事件的规则在被暂停后将无法触发该事件，并且对于丢弃规则，也将无法丢弃数据包。

规则延迟阈值处理可以同时改善被动部署和内联部署中的系统性能，并可通过暂停花费最长时间处理数据包的规则，缩短内联部署中的延迟。不会再次针对已暂停的规则来评估数据包，直到可配置的时间到期为止，为已过载设备提供恢复时间。例如，这些性能优势可以在以下情形中发挥出来：

- 匆忙编写的、大部分未经测试的规则需要大量的处理时间
- 在网络性能较差（如有人下载极大文件）的时段内，将导致数据包检查缓慢

规则延迟阈值说明

默认情况下，数据包和规则处理的基于延迟的性能设置由最新部署的入侵规则更新自动填充，我们建议您不要更改默认设置。

仅当您选择指定自定义值时，本主题中的信息才适用。

如果规则处理数据包时所用时间超过**暂停规则前连续超出阈值的次数 (Consecutive Threshold Violations Before Suspending Rule)** 所指定的连续次数的**阈值 (Threshold)**，则规则延迟阈值就会按**暂停时间 (Suspension Time)** 指定的时间暂停规则。

可启用规则 134:1，当规则已暂停时生成事件；并启用规则 134:2，在启用已暂停规则时生成事件。

表 *4:* 规则延迟阈值选项

选项	说明
阈值	指定规则在检查数据包时不应超出的时间，以微秒为单位。
暂停规则前连续超出阈值的次数 (Consecutive Threshold Violations Before Suspending Rule)	指定在暂停规则之前，规则可按超过为**阈值 (Threshold)** 设置的时间检查数据包的连续次数。
暂停时间 (Suspension Time)	指定暂停一组规则的秒数。

配置规则延迟阈值

默认情况下，数据包和规则处理的基于延迟的性能设置由最新部署的入侵规则更新自动填充，我们建议您不要更改默认设置。

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 点击**基于延迟的性能设置 (Latency-Based Performance Settings)** 旁边的 **编辑** (✎)。

如果显示**视图** (👁)，则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 在**基于延迟的性能设置 (Latency-Based Performance Settings)** 弹出窗口中，点击**规则处理 (Rule Handling)**。

系统会默认选择**已安装规则的更新 (Installed Rule Update)**。我们建议使用此默认设置。

显示的值未反映出自动设置。

步骤 4 如果您选择指定自定义值：

- 可以按规则延迟阈值说明，第 11 页中所述配置任何选项。
- 您必须在“数据包处理”(Packet Handling) 选项卡和“规则处理”(Rule Handling) 选项卡中指定自定义值。

步骤 5 点击**确定**。

步骤 6 点击**保存**保存策略。

下一步做什么

- 如果要生成事件，请启用延迟规则 134:1 和 134:2。
- 部署配置更改；请参阅 部署配置更改。

入侵性能统计信息日志记录配置

采样时间（秒）和最小数据包数量

当过了所指定的性能统计数据更新之间的秒数时，系统验证其已分析的数据包是否到达指定数量。如果到达，则系统更新性能统计数据。否则，系统等待，直到其分析的数据包到达指定的数量。

注意 为采样时间配置非常低的值（例如 1 秒）可能会对设备造成巨大影响；设备上记录的性能统计信息可能会导致磁盘空间问题并影响设备的运行。因此，我们建议您不要配置非常低的值。

故障排除选项：日志会话/协议分布

支持部门可能要求您在故障排除调用期间记录协议分布、数据包长度和端口统计信息。

注意 除非有支持人员的指示，否则请勿启用**记录会话/协议分发**。

故障排除选项：摘要

支持部门可能要求您在故障排除调用期间将系统配置为仅在 Snort 进程关闭或重新启动时计算性能统计数据。要启用此选项，也必须启用 **Log Session/Protocol Distribution** 故障排除选项。

注意 除非有支持人员的指示，否则请勿启用**摘要**。

配置入侵性能统计信息日志记录

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)**，然后点击**性能设置 (Performance Settings)** 旁边的**编辑** (✎) 。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

如果显示**视图** (👁)，则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 点击出现的弹出窗口中的**性能统计信息 (Performance Statistics)**。

步骤 3 如 入侵性能统计信息日志记录配置，第 12 页中所述修改 **采样时间** 或 **最少数据包数量**。

注意
为 **采样时间** 配置非常低的值（例如 1 秒）可能会对设备造成巨大影响；设备上记录的性能统计信息可能会导致磁盘空间问题并影响设备的运行。因此，我们建议您不要配置非常低的值。

步骤 4 或者，展开 **Troubleshoot Options** 部分并修改这些选项（仅当支持部门要求这样做时）

步骤 5 点击**确定**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。