自适应配置文件

以下主题介绍如何配置自适应配置文件：

- 关于自适应配置文件， 第 1 页
- 自适应配置文件的许可证要求， 第 2 页
- 自适应配置文件的要求和前提条件， 第 2 页
- 自适应配置文件更新， 第 2 页
- 自适应配置文件更新和思科 建议规则， 第 3 页
- 自适应配置文件选项， 第 3 页
- 配置自适应配置文件， 第 4 页

关于自适应配置文件

必须启用自适应配置文件才能：

- 执行应用和文件控制，包括恶意软件防护 (AMP)，同时允许入侵规则使用服务元数据。

注意 如配置自适应配置文件， 第 4 页中所述，为了让访问控制规则执行应用和文件控制（包括恶意软件保护 AMP）并让入侵规则使用服务元数据，**必须**启用（默认状态）自适应分析。

- 在被动部署中，通过启用自适应配置文件更新可根据目标主机上的操作系统对 IP 流量进行重整和重组。

注释 在内联部署中，思科建议您不启用自适应配置文件更新，而是配置已启用**规范化 TCP 负载 (Normalize TCP Payload)** 选项的内联规范化预处理器。

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。

自适应配置文件的许可证要求

威胁防御 许可证

IPS

自适应配置文件的要求和前提条件

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

自适应配置文件更新

通常，系统使用网络分析策略中的静态设置预处理和分析流量。通过自适应配置文件，系统可以使用由网络发现检测或从第三方导入的主机信息适应处理行为。

配置文件更新（就像可在网络分析策略中手动配置的基于目标的配置文件一样）有助于以与目标主机上操作系统相同的方式对 IP 数据包进行分片重组并重组数据流。然后入侵规则引擎使用与目标主机所用的相同格式分析数据。

手动配置的基于目标的配置文件应用您选择的默认操作系统配置文件，或绑定到特定主机的配置文件。但是，配置文件更新会根据目标主机的主机配置文件中的操作系统切换到相应的操作系统配置文件。

假设您为 10.6.0.0/16 子网配置配置文件更新，并将默认 IP 分片重组基于目标的策略设置为 Linux。配置设置的防火墙管理中心中有一个包括 10.6.0.0/16 子网的网络映射。

- 当系统检测到来自主机 A（不在 10.6.0.0/16 子网中）的流量时，它使用基于 Linux 目标的策略重组 IP 分片。
- 当系统检测到来自主机 B（在 10.6.0.0/16 子网中）的流量时，它从网络映射检索主机 B 的操作系统数据。系统使用基于该操作系统的配置文件对传送到主机 B 的流量进行分片重组。

自适应配置文件更新和思科 建议规则

自适应配置文件功能是访问控制策略中的高级设置，它全局应用于由该访问控制策略调用的所有入侵策略。思科 建议的规则功能适用于您在其中配置该功能的各个入侵策略。

与 思科 建议的规则一样，配置文件更新 会将规则中的元数据与主机信息进行比较，确定是否应为某个特定主机应用规则。然而，虽然思科 建议的规则为使用该信息的启用或禁用规则提供建议，但配置文件更新 仍会使用这些信息将特定规则应用于特定流量。

思科Firepower建议的规则需要您的互动才能对规则状态执行建议的更改。另一方面，配置文件更新不会修改入侵规则。基于配置文件更新的规则处理在逐包基础上进行。

此外，思科建议的规则可导致启用禁用的规则。相反，配置文件更新仅影响已在入侵策略中启用的规则的应用。配置文件更新 永远不会更改规则状态。

您可以组合使用配置文件更新和思科建议的规则。当部署入侵策略来确定是否纳入某条规则作为应用备选项时，配置文件更新 会使用该规则的规则状态，您是选择接受还是拒绝建议均反映在该规则状态中。您可以同时使用这两个功能来确保您已启用或禁用每个监测网络中最合适的规则，然后应用对特定流量最为有效的已启用规则。

相关主题

关于 Cisco 建议的规则

自适应配置文件选项

启用

以下情况需要启用此选项：

- 访问控制规则，以执行应用和文件控制（包括 AMP）
- 入侵规则，以使用服务元数据

默认情况下，此选项已启用。

注释 要在 Snort 3 中启用自适应配置文件，必须同时选择**启用 (Enable)** 和**启用配置文件更新 (Enable Profile Updates)** 选项。

启用配置文件更新

在被动部署中，通过启用配置文件更新可在网络映射中根据主机使用的操作系统的配置文件对 IP 流量进行重整和重组。

对于 Snort 3，如果启用了自适应配置文件，则必须启用此功能。

自适应配置文件 - 属性更新间隔

在启用配置文件更新后，您可以控制网络映射数据从 防火墙管理中心同步到其托管设备的频率（以分钟为单位）。系统使用该数据确定处理流量时应使用哪些配置文件。增大此选项的值可提升大型网络的性能。

自适应配置文件 - 网络

或者，启用配置文件更新后，您可以通过将配置文件更新限制在逗号分隔的 IP 地址、地址块和网络变量列表中来提高性能。如果使用网络变量，则系统会为您的访问控制策略使用与默认入侵策略相关联的变量集中的变量值。例如，可以输入：**`192.168.1.101, 192.168.4.0/24, $HOME_NET`**。支持 IPv4 和 IPv6。

默认值 (`0.0.0.0/0`) 将自适应配置文件更新应用于所有网络。

相关主题

在识别流量之前检查通过的数据包
变量集

配置自适应配置文件

在被动部署中，思科建议您配置自适应配置文件。在内联部署中，请配置启用**规范化 TCP 负载 (Normalize TCP Payload)** 选项的内联规范化预处理器。

⚠

注意 如本程序中所述，为了让访问控制规则执行应用或文件控制（包括 AMP）并让入侵规则使用服务元数据，**必须**启用（默认状态）自适应分析。

开始之前

访问控制策略必须具有启用主机/服务发现的网络发现策略，或者必须从第三方源导入主机数据。

过程

步骤 1 在访问控制策略编辑器中，点击要修改的策略上的 **编辑** (✎) 。

步骤 2 点击 **更多** > **高级设置**，然后点击 **检测增强设置** 部分旁边的 **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 如自适应配置文件选项，第 3 页中所述，设置自适应配置文件。

步骤 4 点击**确定**。

步骤 5 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。

相关主题

Snort 重新启动场景

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。