威胁检测

Cisco 的端口扫描检测器是一种威胁检测机制，旨在帮助您检测和阻止所有类型流量中的端口扫描活动，以保护网络免受最终攻击。可以在允许和拒绝的流量中高效检测 Portscan 流量。

端口扫描是一种通常被攻击者用作攻击前奏的网络侦察形式。在端口扫描中，攻击者确定主机支持的网络协议或服务类型，并将特制数据包发送到目标主机。通过检查主机响应时所用的数据包，攻击者通常可以直接或通过推理确定主机上的哪些端口是开放的，以及哪种应用协议正在这些端口上运行。

注释 管理中心 7.2 及更高版本支持访问控制策略中端口扫描检测和防御功能（仅限 Snort 3 设备）。威胁检测仅适用于 Snort 检查的流量。对于发送到威胁防御设备本身的流量，不会考虑威胁检测。

端口扫描检测和预防

检测类型

以下是可阻止主机检测的端口扫描活动的类型。

- **常规端口扫描 (Regular portscan)** - 一对一端口扫描，在这种扫描中，攻击者会使用主机扫描单个目标主机上的多个端口。此选项检测 TCP、UDP 和 IP 端口扫描。
- **诱骗端口扫描 (Decoy portscan)** - 一对一端口扫描，在这种攻击中，攻击者将伪造的源 IP 地址与真实的扫描 IP 地址混合在一起。诱骗端口扫描选项检测 TCP、UDP 和 IP 协议端口扫描。

- **分布式端口扫描 (Distributed portscan)** - 多对一端口扫描，在这种攻击中，多个主机查询单个主机是否有开放端口。这会被用于规避端口扫描检测，因为来自多个主机的所有请求可能看起来都是合法的。分布式端口扫描选项检测 TCP、UDP 和 IP 协议端口扫描。
- **端口清扫 (Port sweep)** - 一对多端口清扫，在这种扫描中，攻击者使用一个或几个主机扫描多个目标主机上的单个端口。这通常发生在新的漏洞攻击中，并且攻击者正在寻找特定的服务。此选项检测 TCP、UDP、ICMP 和 IP 端口清扫。

注释 常规、诱骗和分布式端口扫描不属于常规端口扫描活动并且不会发出警报。

Traffic Selection

- 您可以为 **允许**、**拒绝** 或 **所有** 流量选择端口扫描检测。默认情况下，所选类别中的所有流量都会接受端口扫描检测。
- 您可以指定要监控端口扫描活动的网络。在被监控的网络中，您可以避免某些主机被识别为扫描程序。
- 您还可以避免所有发往目标主机的流量接受端口扫描检测。
- IPv4 和 IPv6 流量都支持端口扫描检测。

检测配置

以下是检测配置选项：

- 配置选项：
  - 协议类型 (Protocol types)：TCP、UDP、IP 和 ICMP
  - 端口计数 (Port count)：为基于 TCP 和 UDP 的扫描访问的端口数
  - 主机计数 (Host count)：为进行基于 TCP、UDP 和 ICMP 的扫描而访问的主机数量
  - 协议计数 (Protocol count)：用于 IP 协议扫描的协议数量
  - 间隔 (Interval)：时间间隔

- 预定义灵敏度级别 (Predefined sensitivity levels) - 您可以使用以下灵敏度级别来调整端口扫描检测：
  - 低 (Low) - 只检测目标主机的否定响应。选择此级别的灵敏度可抑制误报，但请记住，这样可能会遗漏某些类型的端口扫描（慢速扫描、过滤扫描）。

    此级别使用最短的时间窗口进行端口扫描检测。
  - 中 (Medium) - 根据主机的连接数量检测端口扫描，因此可以检测过滤的端口扫描。但是，非常活跃的主机（例如网络地址转换器和代理）可能会生成误报。

    默认情况下，灵敏度级别会被设为**中 (Medium)**。

此级别使用较长的时间窗口进行端口扫描检测。

- 高 (High) - 根据时间窗口检测端口扫描，这意味着，可以检测基于时间的端口扫描。此级别使用更长的时间周期进行端口扫描检测。
- 自定义 (Custom) - 用于自定义灵敏度级别。如果编辑现有的预配置灵敏度级别，则会自动选择**自定义 (Custom)** 选项。

- 您可以微调阈值，也可以启用或禁用不同类型的扫描。

阻止配置

以下是配置防御的相关选项：

- 您可以选择阻止已确定为正在执行端口扫描活动的主机。
- 基于持续时间的阻止，并在持续时间到期后自动取消阻止主机。
- 您可以避免主机因端口扫描活动而被阻止。

有关配置端口扫描检测和防御的详细信息，请参阅配置端口扫描检测和预防 ， 第 3 页。

配置端口扫描检测和预防

端口扫描可被配置为进行检测或防御。默认情况下，只能对允许的流量执行端口扫描检测。

开始之前

要从访问控制策略编辑器配置端口扫描检测和防御，则要满足以下前提条件：

- 管理中心 和托管设备必须运行 7.2.0 或更高版本。
- Snort 3 必须已启用。

注释 当您将设备从 Snort 3 移至 Snort 2 时，端口扫描会被禁用。但是，您可以使用 NAP 和入侵策略在使用 Snort 2 的设备上配置端口扫描。

过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的**更多**下拉箭头中点击**高级设置**。然后，点击**威胁检测**旁边的 **编辑**（ ）。

步骤 2 在**威胁检测 (Threat Detection)** 窗口中，您可以选择**检测 (Detection)** 或**防御 (Prevention)** 作为**端口扫描模式 (Portscan mode)**。

步骤 3 如果选择**检测 (Detection)**：

1. 在 **流量选择 (Traffic Selection)** 选项卡下，您可以选择对 **允许 (Permitted)**、**拒绝 (Denied)** 或 **所有 (All)** 流量。
2. 在**监控 (Monitor)**、**忽略扫描程序 (Ignore Scanner)** 和**忽略目标 (Ignore Target)** 字段中，可以选择要考虑（监控）进行端口扫描检测的 IP 或网络、要作为攻击者忽略的 IP 或网络，以及要作为目标主机忽略的 IP 或网络。

   注释 端口扫描配置不支持 FQDN、通配符掩码、any、any-ipv4 和 any-ipv6 网络对象。这些对象不会显示在**监控 (Monitor)**、**忽略扫描程序 (Ignore Scanner)**、**忽略目标 (Ignore Target)** 和**排除 (Exclude)** 字段下。

3. 在**配置 (Configuration)** 选项卡下，您可以选择预配置的灵敏度级别 - **低 (Low)**、

   中 (Medium)、**高 (High)** 和**自定义 (Custom)**，以便调整扫描后检测。选择**自定义 (Custom)** 选项以自定义灵敏度级别。
4. 在不同的协议类型（TCP、UDP、IP 和 ICMP）下，您可以设置访问的主机数量、访问的端口数量、使用的协议数量（用于 IP 协议）以及间隔。

步骤 4 您可以选择**防御 (Prevention)** 端口扫描模式，以阻止主机进一步扫描网络或发起攻击。在**排除 (Exclude)** 下的**预防 (Prevention)** 选项卡中，您可以选择免除阻止 IP 或网络，还可以设置阻止主机的**持续时间 (Duration)**。

步骤 5 要将端口扫描设置恢复为默认（禁用）状态，请点击**恢复默认设置 (Revert to Defaults)** 选项。

步骤 6 点击**确定 (OK)** 以保存端口扫描检测和防御设置。

步骤 7 单击 **Save** 保存策略。

注释 端口扫描配置更改会作为 AC 策略审核日志报告的一部分提供。

下一步做什么

部署配置更改；请参阅 部署配置更改。

改进了低灵敏度检测

您可以在低灵敏度级别跟踪 TCP、UDP 和 ICMP 初始数据包的否定响应。仅当不成功的连接数超过拒绝阈值（例如，低灵敏度时为 10%）且端口/IP 协议计数超过配置的阈值时，才会触发警报。这可以减少误报。

如果同时存在允许和阻止的流量，则根据允许和阻止的流量之间的差异计算拒绝端口或主机的数量。在仅阻止流量的情况下，不考虑拒绝阈值。

注意 当在内联集模式下配置威胁防御时，此解决方案不适用于 UDP 和 ICMP 连接。

示例

假设在低灵敏度的威胁防御中启用了端口扫描。

配置的端口计数阈值 = 120

计算出的拒绝计数阈值 = 120 的 10% = 12

攻击者发起与目标的 131 个端口的连接，目标肯定确认所有发起。端口计数 = 131，大于阈值，但由于没有否定确认，因此不会触发警报。

攻击者发起与目标的 131 个端口的连接，目标肯定确认 121 次发起，否定确认 10 次。

端口计数 = 131，大于阈值，但拒绝端口计数 = 10，小于拒绝阈值；因此不会触发警报。

例如，攻击者向目标的 134 个端口发起连接，目标肯定会确认 121 次发起并否定确认 13 次。端口计数 = 134，大于阈值，拒绝端口计数 = 13 也高于拒绝阈值。因此，在这种情况下会触发警报。

警报 - 端口扫描活动

在配置端口扫描后，将生成特定于端口扫描的入侵策略事件，而无论是否存在或配置 IPS 策略或事件。

端口扫描活动会通过现有端口扫描特定 IPS 事件来发出警报。会生成生成器 ID (GID) 为 122 且 Snort ID 为 1 至 27 的 IPS 事件。对于这些事件，在事件消息中会附加 *(port_scan)* 字符串。

要在 管理中心中查看这些事件，请转至 **分析** > **入侵** > **事件**。

从 NAP 策略进行端口扫描升级

运行 7.2.0 或更高版本的设备不支持基于 Snort 3 网络分析策略 (NAP) 的端口扫描功能。

对于运行 7.2.0 或更高版本的设备，您必须使用访问控制策略（“高级设置”(Advanced settings) 选项卡）来配置端口扫描。

升级到 7.2.0（或更高版本）Snort 3 设备后，将从访问控制策略端口扫描设置（而不是 NAP 策略）中挑选和部署端口扫描配置设置，因此，如果您尚未将 NAP 端口扫描配置迁移到 AC 策略端口扫描，那么您的设备将在下次部署时丢失端口扫描配置。

下表显示了可应用于运行 Snort 3 或 Snort 2 引擎的版本 7.2.0 或更高版本以及版本 7.1.0 或更早版本的端口扫描配置。

FMC	FTD	端口扫描配置
FMC 7.0 或 7.1	Snort 2 设备	Snort 2 NAP 策略中的配置适用。
	Snort 3 设备	Snort 3 NAP 策略中的配置适用。

FMC	FTD	端口扫描配置
FMC 7.2.0	Snort 2 设备	Snort 2 NAP 策略中的配置适用。
	Snort 3 设备（7.1.0 及更早版本）	Snort 3 NAP 策略中的配置适用。
	Snort 3 设备（7.2.0 及更高版本）	访问控制策略中的配置适用。

通过端口扫描支持访问控制策略的功能

以下功能支持使用端口扫描的访问控制策略：

- **审核日志和增量预览 (Audit Logs and Delta Preview)** - 端口扫描信息在 AC 策略审核日志和部署预览下可用。
- **导入和导出 (Import and Export)** - 您可以导入或导出包含端口扫描配置的 AC 策略。
- **域 (Domains)** – 可以为全局和分叶域中的 AC 策略配置端口扫描。
- **PDF 报告生成 (PDF Report Generation)** – AC 策略报告还包含已配置的端口扫描设置。
- **回滚 (Rollback)** – 您可以回滚到包含端口扫描配置的配置的已部署版本。

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。