威胁检测

威胁检测的 Portscan 检测器是一种机制，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。

端口扫描检测和预防

使用威胁检测识别端口扫描活动。您可以使用系统检测端口扫描，并在发现端口扫描时发出事件。或者，您可以将系统配置为通过自动阻止扫描程序来阻止端口扫描。在阻止端口扫描时，系统会向您发送事件，并在您设置的持续时间段内阻止攻击者。

端口扫描检测的预定义敏感度级别

配置检测设置时，您可以选择以下预定义的灵敏度级别。除“自定义”外，每个级别都为每个协议的端口 (TCP/UDP)、协议 (IP) 或主机 (TCP/UDP/IP/ICMP) 数预设了必须在设定的时间间隔内扫描的值（以秒为单位）。此外，还会启用所有类型的扫描/清扫。

注释 在对端口/协议进行计数时，如果当前数据包中的端口/协议与前一个数据包不同，威胁检测就会让数字递增。例如，如果您有一个应用会随机打开10个端口的连接，那么扫描的端口总数可能会迅速增加，以至于您的端口数会在时间间隔内被超过。系统不会仅对唯一端口进行计数。

超过间隔内的数字可能表示扫描攻击。仅当超出移动时间间隔窗口的端口/协议/主机号时，才会生成端口扫描事件。

- 低- 此级别使用端口扫描检测的最短时间窗口，并为端口/协议/主机加上高计数。因此，您应该只看到最积极的扫描程序的端口扫描事件。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）。有关低灵敏度检测工作原理的更多详细信息，请参阅 在低敏感度级别检测，第 3 页。
  - 间隔 (TCP/UDP/IP/ICMP) - 60 秒。
  - **TCP/UDP portscan 端口数**-120。
  - **TCP/UDP 端口清扫 主机数量**-180。
  - **IP 协议扫描协议数量**-30。
  - **IP 协议扫描主机数**-25。
  - **ICMP 主机扫描主机数**-50。
- 中- 此级别对间隔和端口/协议/主机计数使用中等值。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。将此类主机添加到忽略扫描程序列表。这是默认的敏感度级别，也是一个很好的起点。
  - 间隔 (TCP/UDP/IP/ICMP) - 90 秒。
  - **TCP/UDP portscan 端口数**-90。
  - **TCP/UDP 端口清扫 主机数量**-150。
  - **IP 协议扫描协议数量**-15。
  - **IP 协议扫描主机数**-20。
  - **ICMP 主机扫描主机数**-30。
- 高- 此级别为端口扫描检测使用更长的时间窗口，并为端口/协议/主机提供较低的计数。使用此级别，即使是最不严格的端口扫描/清扫，您也最有可能看到事件，因此您更有可能注意到所有攻击者。另一方面，此级别可能会导致发出大多数端口扫描事件，并可能导致最高数量的误报。
  - 间隔 (TCP/UDP/IP/ICMP) - 600 秒（10 分钟）。
  - **TCP/UDP portscan 端口数**-60。
  - **TCP/UDP 端口清扫主机数量**-100。
  - **IP 协议扫描协议数量**-10。

- **IP 协议扫描主机数**-10。
- **ICMP 主机扫描主机数**-20。

- **自定义**- 如果要配置与某个预定义灵敏度级别不同的任何设置，或者要禁用特定类型的扫描/清扫，级别会自动切换到“自定义”。如果要调整选项，请先选择与所需选项最匹配的级别，然后根据需要编辑值。

在低敏感度级别检测

如果选择低灵敏度级别，系统则跟踪 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（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。

拒绝阈值仅适用于低灵敏度（或同等的自定义设置）；不适用于其他灵敏度级别或同等的自定义设置。

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。

这些条件不适用于内联集中配置的接口上的 UDP/ICMP 连接。

例如，在低灵敏度模式下，端口计数阈值为 120。因此，拒绝计数阈值为 120 的 10%，即 12。以下是在此配置下系统如何发出端口扫描事件的示例：

- 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，因此不会触发端口扫描警报。
- 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，不会触发端口扫描警报。
- 攻击者发起与目标的 134 个端口的连接，目标肯定确认 121 次发起，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，会触发端口扫描警报。

预防端口扫描的最佳实践

端口扫描预防模式可能会导致流量意外中断。在预防模式下，会在配置的持续时间内阻止主机进一步扫描基于所有协议的网络。请仔细查看检测和防御参数，确保合法流量未被阻止。

在预防模式下配置端口扫描之前，我们强烈建议执行以下操作：

1. 开始在检测模式下使用端口扫描。
2. 观察生成的端口扫描事件。
3. 调整敏感度级别，以及受监控网络、忽略扫描程序列表和忽略目标列表。如果预定义的敏感度级别不适用于您的情况，请根据需要配置自定义设置。

4. 重复此过程，直到消除误报，并且事件速率可以准确反映网络中的端口扫描。确保您熟悉如何阻止已识别的其余扫描程序。

威胁检测的要求和前提条件

型号支持

威胁防御 运行版本 7.2+ 和 Snort 3。

支持的域

任意

用户角色

管理员

访问管理员

网络管理员

威胁检测准则和限制

- 威胁检测仅适用于通过设备的流量。它不适用于定向到设备的流量。
- 威胁检测需要 Snort 3。托管设备的版本必须为 7.2 或更高版本。对于 Snort 2 或版本低于 7.2 的设备，可以通过 NAP 策略配置端口扫描。请注意，威胁检测功能与 NAP 策略中的端口扫描功能不同。如果有非 Snort 3/版本 7.2+ 设备分配给访问控制策略，则不会将威胁检测设置部署到这些不受支持的设备。
- 如果在运行 7.1 或更低版本的设备上的 NAP 策略中配置端口扫描，则在升级到 7.2 时，该配置不会转换为威胁检测功能。您必须手动配置威胁检测。虽然 NAP 和威胁检测 portscan 选项相似，但它们不是一对一匹配。
- 如果配置威胁检测，则NAP策略中的任何端口扫描配置都将被忽略，并且不会在支持威胁检测的设备上进行配置。
- 对于版本 7.2+ 设备，始终忽略 Snort 3 的 NAP 端口扫描功能。要配置端口扫描，必须使用威胁防御设置。
- 在高可用性设置中，端口扫描统计信息不会同步到备用设备。但是，被阻止的主机将同步并继续被阻止，直到持续时间到期，以防发生故障切换。
- 集群：在单个集群节点上进行检测和防御。也就是说，如果节点 B 检测到并阻止来自主机的流量，节点 A 不会注意到该操作，因为端口扫描统计信息不会在集群节点之间同步。

- 对于内联集或配置为等价多路径(ECMP)流量区域一部分的接口，在区域级别完成检测和防护。跨区域的所有接口累积主机的端口扫描统计信息。同样，当主机超过配置的阈值时，会在相应区域的所有接口上被阻止。
- 虽然威胁检测功能生成的端口扫描事件与Snort为端口扫描生成的端口扫描事件相同，但您无需在NAP配置中配置端口扫描（因为这些设置将被忽略），也无需启用端口扫描入侵规则以获取事件。无论您的入侵策略实施如何，威胁检测都能正常工作。

配置端口扫描检测和预防

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。

您可以启用威胁检测以监视端口扫描活动，也可以选择在一段时间内自动阻止扫描程序。

开始之前

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。

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** 窗口中，选择 **端口扫描模式**：

- **禁用**- 关闭威胁检测。该模式为默认模式。您可以点击 **恢复到默认** 以恢复到此未配置状态。
- **检测**- 执行端口扫描检测，但仅在出现问题时发出警报。请勿对潜在的攻击者执行操作。我们建议您最初使用此模式，直到微调威胁检测设置以避免过多的误报。
- **防御**- 执行端口扫描检测并主动阻止已识别的扫描程序，即正在执行端口扫描的主机。

步骤 3 配置 **流量选择** 选项。

流量选择选项确定要监控的网络、监控的连接类型，以及是否应从受监控网络排除任何扫描程序或目标主机。默认情况下，系统会监控所有网络上允许的连接。

- **流量检测**- 选择将监控端口扫描活动的连接类型： **允许**、 **拒绝**或 **所有** 流量。默认为**允许**。
- **监控**- 选择定义要监控端口扫描或清扫活动的网络的网络对象。默认值为任何网络、IPv4 或 IPv6。使用此选项可限制对不受信任网络的扫描。

- **忽略扫描程序**-从受监控网络的范围内选择定义应忽略的主机或网络的网络对象。例如，如果您设置了自己的扫描仪来测试网络，则可以豁免扫描仪的地址，以避免不必要的地址报告。请勿包含受监控网络外部的地址，因为这些地址已被忽略。
- **忽略目标**-选择定义应作为目标忽略的主机或网络（即端口扫描或清扫的受害者）的网络对象。

步骤 4 点击 **配置** 选项卡，然后选择扫描灵敏度级别。

预定义的敏感度级别**低**、**中**和**高**将端口扫描选项设置为越来越严格的值。例如，如果选择“低”，预计会看到更少的端口扫描事件，并且比选择“中”或“高”时更容易漏掉攻击者。另一方面，如果选择“高”，您可能会看到更多事件，也可能会出现更多误报。默认级为“中”。有关级别的信息，请参阅端口扫描检测的预定义敏感度级别，第 1 页。

选择级别时，您可以在协议部分中看到相关值：**TCP**、**UDP**、**IP**和 **ICMP**。如果更改任何预设值或禁用某种类型的扫描，灵敏度模式会自动更改为“**自定义**”。

在每个协议部分中，选项包括：

- **间隔**- 超出为端口扫描或端口清扫配置的值的时间范围（以秒为单位）。例如，如果选择 90 秒和 60 作为 TCP 端口扫描端口数，则扫描程序需要在 90 秒内尝试主机上的 60 个端口，才会被视为端口扫描。仅当超过指定间隔内的端口、协议或主机数（对于端口清扫）时，系统才会生成事件。

  您可以指定 30-600 秒之间的范围。时间段越长，主机被识别为扫描程序的可能性就越大。
- **端口扫描** (TCP/UDP) - 选择是否监控单个主机的端口扫描，并指定在间隔内必须扫描的端口数，才能计为端口扫描攻击。允许的范围为 1-256。
- **端口清扫** (TCP/UDP) - 选择是否针对多个主机监控端口清扫，并指定在间隔内必须为给定端口扫描多少主机才能计为端口清扫攻击。允许的范围为 1-256。
- **协议扫描** (IP) - 选择是否监控单个主机的协议扫描，并指定在间隔内必须扫描的协议数，才能计为协议扫描攻击。允许的范围为 1-255。
- **协议扫描** (IP) - 选择是否监控多个主机的协议扫描，并指定在间隔内必须为给定协议扫描多少主机才能计为协议扫描攻击。允许的范围为 1-256。
- **主机清扫** (ICMP) - 选择是否针对多个主机监控 ICMP 主机清扫，并指定在间隔内必须扫描的主机数，才能将其计为主机清扫攻击。允许的范围为 1-256。

步骤 5 如果选择了防护模式，请点击 **防护** 选项卡并配置选项。

在预防模式下，会在配置的持续时间内自动阻止主机进一步扫描基于所有协议的网络。请仔细查看检测和防御参数，确保合法流量未被阻止。

- **排除**-从受监控网络的范围内选择定义应从自动阻止中排除的主机或网络的网络对象。即使这些主机违反了您的扫描检测参数，系统也不会阻止它们。
- **持续时间**-应阻止自动阻止的扫描程序主机通过设备发送任何类型的流量的时长（以秒为单位）。持续时间结束后，主机会自动清除，并且可以再次通过设备发送流量。允许的范围为600-2592000 秒。默认值为 3600 秒（1 小时）。

如果需要手动取消阻止主机，请通过SSH连接到阻止主机的防火墙，并使用**clear threat-detection portscan attacker** 命令。

步骤 6 点击 **确定** 以保存威胁检测设置。

步骤 7 点击**保存 (Save)** 保存访问控制策略。

下一步做什么

部署配置更改；请参阅 部署配置更改。

监控威胁检测

以下主题介绍如何监控端口扫描活动

查看端口扫描警报

端口扫描活动会通过现有端口扫描特定入侵事件来发出警报。会生成生成器ID (GID) 为 122 且 Snort ID 为 1 至 27 的入侵事件。对于这些事件，在事件消息中会附加 *(port_scan)* 字符串。事件包括数据包信息以及包含触发警报的统计信息的数据包数据。

要查看端口扫描事件，请转至 **分析** > **入侵** > **事件**。

无论入侵策略或 NAP 配置如何，Portscan 都会发出这些事件。仅当扫描程序的数量超过为关联协议配置的时间间隔内为各种类型的扫描或清扫而配置的端口/协议/主机数时，才会发出事件。一旦达到阈值，来自一个主机的端口扫描就会在每个设置的间隔内生成一个事件。如果同一主机在同一间隔内启动新的端口扫描，则不报告任何事件。

下表显示了可能的事件。

表 *1:* 端口扫描事件

端口扫描类型	入侵事件
TCP 常规、欺骗、分布式扫描	122:1 (port_scan) TCP 端口扫描
TCP 端口清扫	122:3 (port_scan) TCP 端口清扫
IP 常规、欺骗、分布式协议扫描	122:9 (port_scan)IP 协议 SCA
IP 协议清扫	122:11 (port_scan) IP 协议扫描
UDP 常规、欺骗、分布式扫描	122:17 (port_scan) UDP 端口扫描
UDP 端口清扫	122:19（port_scan）UDP 端口清扫
ICMP 扫描	122:25 (port_scan) ICMP 扫描

监控防火墙上的端口扫描

要监控端口扫描，请登录设备 CLI 并使用以下命令。

- **show threat-detection portscan** ［**attacker** | **target** | **shun**］

  显示扫描仪的 IP 地址、已避开（阻止）的扫描仪以及已成为扫描或清扫目标的主机。

- **show threat-detection portscan statistics** ［**host** ［*ipv4_address* | *ipv6_address*］］［**protocol** {**tcp** | **udp** | **ip** | **icmp**} ］

  显示与端口扫描系统相关的统计信息。您可以指定主机、协议或主机和协议，以将输出过滤为所需的信息。

- **clear threat-detection portscan** ［**attacker** | **target** | **shun**］［*ipv4_address mask* | *ipv6_address/prefix* ］

  手动取消阻止扫描程序（攻击者）或识别的目标。输入不带参数的命令，以清除所有攻击者、目标或避开的主机。

- **clear threat-detection portscan statistics** ［**host** ［*ipv4_address* | *ipv6_address*］］［**protocol** {**tcp** | **udp** | **ip** | **icmp**} ］

  清除与端口扫描相关的统计信息，以便您可以更清楚地查看通过此设备扫描的当前状态。输入不带参数的 命令以清除所有统计信息。或者，指定主机、协议或主机和协议，以将重置限制为指定项目。

取消阻止主机

如果在防御模式下配置威胁检测，并且系统阻止了您知道不是攻击者的主机，则可以在持续时间到期后自动取消阻止主机之前手动取消阻止该主机。

要手动取消阻止主机，请登录到主机被阻止的设备 CLI，然后输入 **clear threat-detection portscan attacks** 命令。例如：

```
> clear threat-detection portscan attacker 10.2.0.100 255.255.255.255
1 tracker object deleted and 1 shun entry removed
```

考虑将主机 IP 添加到防护配置中的“排除”列表。

威胁检测的历史记录

功能	管理中心最低版本	威胁防御最低版本	说明
改进了低灵敏度检测。	7.4	7.4	在低灵敏度级别运行时，识别端口扫描和清扫的方法已得到改进。更改是自动的；没有新的配置设置。

功能	管理中心最低版本	威胁防御最低版本	说明
改进了端口扫描检测。	7.2	7.2 运行 Snort 3	通过改进的端口扫描检测器，您可以轻松地配置系统以检测或防止端口扫描。您可以细化要保护的网络，设置灵敏度等。对于运行 Snort 2 的设备以及运行版本 7.1 及更早版本的设备，请继续使用网络分析策略进行端口扫描检测。 新增/修改的屏幕：我们向访问控制策略的高级选项卡添加了 **威胁检测**。 新增/修改的命令： **clear threat-detection portscan**、 **show threat-detection portscan**。

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。