数据流遥测

除使用集成控制面板和 CLI 监控设备外，您还可配置设备将数据发送至遥测收集器。您可使用收集器监控网络中的多台设备。

以下主题说明使用流传输遥测的要求，以及如何设置遥测收集器及其与 Firewall Threat Defense 设备的连接。

关于流式遥测

您可以配置设备将系统运行状况和遥测数据发送到使用 Google 远程过程调用 (gRPC) 收集数据的外部遥测收集器。然后，您就可以使用遥测收集器来监控设备，并与您的自定义遥测解决方案集成。

设备与遥测收集器之间的连接使用双向 TLS (mTLS) 身份验证确保安全。设备与遥测收集器交换证书以验证客户端和服务器身份，并对传输数据进行加密。设备主动向遥测服务器发起连接（拨出模型）。

流式遥测指南

配置流传输遥测时，请牢记以下准则：

- 您只能使用 IPv4 地址。
- 为确保通信安全，Firewall Threat Defense 设备和遥测收集器所用的证书应由同一证书颁发机构 (CA) 签署。为 Firewall Threat Defense 设备创建必要的证书（或重用为 Firewall Threat Defense Web 服务器配置的证书），并下载供遥测收集器使用的证书。
- 每台 Firewall Threat Defense 设备只能连接到一个遥测收集器。但一个收集器可用于多台 Firewall Threat Defense 设备。

- 对于配置为高可用性的设备，您必须在每台设备上单独配置流传输遥测。遥测配置不会从主用设备复制到备用设备。如果需要，您可以将主设备和辅助设备配置为使用不同的遥测收集器。
- Firewall Threat Defense 设备使用以下端口进行流传输遥测：
  - 控制信道：9276（基于 HTTP）
  - 数据信道：8087（基于 HTTP）
  - 端口 9273 和 9276 用于诊断
- 您可以编写远程程序，使用以下 Firewall Threat Defense API 从您的遥测收集器配置 Firewall Threat Defense 设备：
  - /object/internalcertificates
  - /object/externalcacertificates
  - /object/networks
  - /devicesettings/default/telemetrystreamingconfig

启用流式遥测

设置好遥测收集器后，即可配置 Firewall Threat Defense 设备与遥测服务器之间的连接。连接配置完成后，Firewall Threat Defense 设备会自动尝试建立连接；若成功，将按收集器请求的频率传输数据。

开始之前

确保遥测收集器满足设置遥测收集器，第 6 页中所述的要求。

过程

步骤 1 选择**对象** > **证书**，然后点击 + > **添加内部证书**，上传 Firewall Threat Defense 设备用于安全通信的客户端证书。有关详细信息，请参阅上传内部证书和内部 CA 证书。

步骤 2 选择**对象** > **证书**，然后选择 + > **添加受信任 CA 证书**，上传 Firewall Threat Defense 设备用于验证收集器身份的 CA 证书。有关详细信息，请参阅上传受信任的 CA 证书。

步骤 3 选择**对象** > **网络**，然后选择 +，创建用于标识遥测收集器的网络对象。有关详细信息，请参阅配置网络对象和组。

可使用收集器的 IPv4 地址创建主机对象，或使用包含收集器完全限定域名（如 telemetry.domain.com）的 FQDN 对象。FQDN 必须能解析为 IPv4 地址，且您必须配置 DNS 以便正确解析名称。

步骤 4 获取网络对象的 ID。

a) 从更多选项 ⋮ 按钮中选择 **API Explorer** 以访问 API 页面。

b) 在 **NetworkObject**下，选择 **GET /object/networks**。

c) 在**参数**部分的**过滤**字段中，输入对象名称进行过滤。例如，如果您创建的网络对象是 TelemetryCollector，则过滤器为：

name:TelemetryCollector

d) 滚动到 GET /object/networks 部分底部，点击**试用**。

e) 若调用正确，您将收到 200 响应码及有意义的对象正文，如下所示。找到 id 条目并记录其值。在本例中，id 值为 **79ee2ea9-76b7-11ef-9515-f5b34b7d9531**。

```
{
  "items": [
    {
      "version": "p4qjmqtqn5c5e",
      "name": "TelemetryCollector",
      "description": null,
      "subType": "HOST",
      "value": "10.1.1.1",
      "isSystemDefined": false,
      "dnsResolution": "IPV4_AND_IPV6",
      "id": "79ee2ea9-76b7-11ef-9515-f5b34b7d9531",
      "type": "networkobject",
      "links": {
        "self":
"https://ftd1.domain.com/api/fdm/v6/object/networks/79ee2ea9-76b7-11ef-9515-f5b34b7d9531"

      }
    }
```

步骤 5 获取内部证书对象的 ID。

a) 在 API Explorer 的**证书**下，选择 **GET /object/internalcertificates**。

b) 在**过滤**字段中按证书名称过滤。例如，若 Firewall Threat Defense 设备的内部证书名为 FTD1Cert，则过滤器为：

name:FTD1Cert

c) 滚动到 GET /object/internalcertificates 部分底部，点击**试用**。

d) 若调用正确，您将收到 200 响应码及有意义的对象正文，如下所示。找到 id 条目并记录其值。在本例中，id 值为 **d874dfa3-7423-11ef-b3a0-09429aedc3d3**。

```
{
  "items": [
    {
      "version": "gr573izgdsj2o",
      "name": "FTD1Cert",
…
       ATTRIBUTES REMOVED
…
      "id": "d874dfa3-7423-11ef-b3a0-09429aedc3d3",
      "type": "internalcertificate",
      "links": {
        "self":
"https://ftd1.domain.com/api/fdm/v6/object/internalcertificates/d874dfa3-7423-11ef-b3a0-09429aedc3d3"

      }
    }
```

步骤 6 获取受信任 CA 证书对象的 ID。

a) 在 API Explorer 的**证书**下，选择 **GET /object/externalcacertificates** 。

b) 在**过滤**字段中按证书名称过滤。例如，若遥测收集器的受信任CA证书名为TelemetryCollectorCert，则过滤器为：

name:TelemetryCollectorCert

c) 滚动到 GET /object/externalcacertificates 部分底部，点击**试用**。

d) 若调用正确，您将收到 200 响应码及有意义的对象正文，如下所示。找到 id 条目并记录其值。在本例中，id 值为 **c3d925b4-7423-11ef-b3a0-bf815c0136ac**。

```
{
  "items": [
    {
      "version": "fkry47nobvcnu",
      "name": "TelemetryCollectorCert",
…
      ATTRIBUTES REMOVED
…
      "id": "c3d925b4-7423-11ef-b3a0-bf815c0136ac",
      "type": "externalcacertificate",
      "links": {
        "self":
"https://ftd1.domain.com/api/fdm/v6/object/externalcacertificates/c3d925b4-7423-11ef-b3a0-bf815c0136ac"

      }
    }
```

步骤 7 配置 Firewall Threat Defense 设备与遥测收集器之间的连接：

a) 在 API Explorer 的 **TelemetryStreamingConfig** 下，选择 **POST /devicesettings/default/telemetrystreamingconfig**。

b) 在**参数**>**正文**下的**值**编辑框中键入以下模板（避免复制隐藏无效字符）。模板中各字段的含义见模板内说明。<> 中的说明为需替换的变量，其他值须保持原样。逗号、圆括号、冒号及 {} 的位置至关重要。

```
{
"name": "<a unique name for the gRPC streaming config API>",
"connectionMode": "DIAL_OUT",
"port": "<port on which the collector is waiting for connections from the
          Threat Defense device, 1-65535. Check the collector configuration
          for the right value.>",
"targetHost": {
    "name": "<name of the network object that identifies the telemetry collector host>",

     "id": "<ID of the network object>",
     "type": "networkobject"
},
"clientCertificate": {
      "name": "<The name of the internal certificate that identifies the Threat Defense
 device>",
      "id": "<ID of the internal certificate object.>",
      "type": internalcertificate
}
"caCertificate": {
      "name": "<The name of the trusted CA certificate for the telemetry collector>",
       "id": "<ID of the trusted CA certificate>",
```

```
      "type": "externalcacertificate"
},
"type": "telemetrystreamingconfig"
}
```

示例：

根据本流程中所示的示例值，以下为正确的负载。注意：名称和端口值不由前述步骤决定，您可按需更改。

```
{
"name": "YourCompanyTelemetry",
"connectionMode": "DIAL_OUT",
"port": 50051,
"targetHost": {
   "name": "TelemetryCollector",
   "id": "79ee2ea9-76b7-11ef-9515-f5b34b7d9531",
   "type": "networkobject"
},
"clientCertificate": {
    "name": "FTD1Cert",
    "id": "d874dfa3-7423-11ef-b3a0-09429aedc3d3",
    "type": "internalcertificate"
},
"caCertificate": {
     "name": "TelemetryCollectorCert",
     "id": "c3d925b4-7423-11ef-b3a0-bf815c0136ac",
     "type": "externalcacertificate"
},
"type": "telemetrystreamingconfig"
}
```

c) 滚动到该部分底部，点击**试用**。

d) 查找响应代码 200。若看到其他代码，请修正错误并重试。成功的响应正文应类似如下内容：

```
{
  "version": "jfwu476cue32n",
  "name": "YourCompanyTelemetry",
  "connectionMode": "DIAL_OUT",
  "port": 50051,
  "targetHost": {
    "version": "p4qjmqtqn5c5e",
    "name": "TelemetryCollector",
    "id": "79ee2ea9-76b7-11ef-9515-f5b34b7d9531",
    "type": "networkobject"
  },
  "clientCertificate": {
    "version": "gr573izgdsj2o",
    "name": "FTD1Cert",
    "id": "d874dfa3-7423-11ef-b3a0-09429aedc3d3",
    "type": "internalcertificate"
  },
  "caCertificate": {
    "version": "fkry47nobvcnu",
    "name": "TelemetryCollectorCert",
    "id": "c3d925b4-7423-11ef-b3a0-bf815c0136ac",
    "type": "externalcacertificate"
  },
  "id": "b6dc6f28-76c1-11ef-9515-8ff976794f92",
  "type": "telemetrystreamingconfig",
  "links": {
    "self":
```

"https://ftd1.domain.com/api/fdm/v6/devicesettings/default/telemetrystreamingconfig/b6dc6f28-76c1-11ef-9515-8ff976794f92"

  }
}

下一步做什么

有关如何验证遥测传输是否正常工作，请参阅以下主题：

- 检查遥测流服务状态， 第 10 页
- 验证遥测收集器是否接收到数据， 第 12 页

设置遥测收集器

您需自行提供遥测收集器（现成产品或定制开发），用于从 Firewall Threat Defense 设备接收遥测数据、汇总信息，并以有意义的方式展示，以满足组织的运维需求。以下提供设置遥测收集器、通过 grip 调用从 Firewall Threat Defense 设备运行的 Telegraph 组件收集数据的相关通用信息。

过程

步骤 1 确保您的遥测收集器满足 遥测收集器指南， 第 6 页 中列出的要求。

步骤 2 按照 遥测收集器上的 Proto 定义， 第 7 页 中的说明配置协议定义。

步骤 3 确保遥测收集器能接收并响应 Firewall Threat Defense 设备上运行的 Telegraph 客户端请求，如Firewall Threat Defense 设备与遥测收集器之间的通信， 第 8 页中的介绍。

遥测收集器指南

- 您可以在 Windows、Mac、Linux 或 Unix 服务器上运行遥测客户端。
- 您必须在遥测收集器上安装 Go。最低 Go 版本为 1.20。
- 遥测收集器必须具有 IPv4 地址，并且与使用它的 Firewall Threat Defense 设备之间存在直接或通过代理的正确路由。如果连接丢失，Firewall Threat Defense 设备会每 5 分钟重试一次连接。
- 遥测收集器上的监听端口必须是有效的 TCP 端口 (1-65535)，且未被其他用途占用。
- 遥测收集器上的服务器证书、服务器密钥和 CA 证书必须位于以下路径：
  - 服务器密钥：/root/grpc-certs/keys/server.key
  - 服务器证书：/root/grpc-certs/keys/server.crt
  - CA 证书：/root/grpc-certs/keys/ca.crt

- 当证书过期时，您将在遥测客户端上看到身份验证错误，且流传输将停止。您需要替换证书以更正身份验证问题并恢复传输。
- 消息使用 Prometheus 时间序列格式。您的客户端必须能够处理此格式。
- 不支持以下遥测收集器：https://github.com/CiscoSE/grpc_collector。

遥测收集器上的 Proto 定义

Firewall Threat Defense 设备使用协议缓冲区来构造数据。遥测收集器上的 proto 定义应包含以下内容。

```
syntax = "proto3";
// Update the go_package option to a local package path
option go_package = "grpcstreaming/grpc_streaming_proto";
package proto;
service GrpcStreamingService {
    rpc DataStream (stream DataResponse) returns (stream DataRequest);
    rpc ControlStream (stream ControlResponse) returns (stream ControlRequest);
}
message ControlResponse {
    string version = 1;
    string ftd_uuid = 2;
    string hostname = 3;
    bool init_streaming = 4;
    repeated string capabilities = 5; // ['metric_streaming']
    // cancel stream acknowledgement
    bool ack = 6;
}
message ControlRequest {
    string version = 1;
    int64 interval = 2;
    repeated string metric_subscriptions = 3;
    // cancel stream
    StreamCancellationMessage cancellation_message = 4;
}
message DataResponse {
    string ftd_uuid = 1;
    repeated Metric metrics = 2;
}
message DataRequest {
    bool ack = 1;
}
message StreamCancellationMessage {
    string collector_uuid = 1;
    bool cancel_stream = 2;
}
message Tag {
    string key = 1;
    string value = 2;
}
message Metric {
    int64 timestamp = 1;
    string metricFamily = 2;
    double value = 3;
    repeated Tag tags = 4;
    string metricType = 5; //Counter | Gauge
}
```

Firewall Threat Defense 设备与遥测收集器之间的通信

为初步建立连接，Firewall Threat Defense 设备会向遥测收集器发送一个 gRPC 请求，其中包含指示 initial_request=True 的有效载荷。该请求还会通告其功能，即“metric_streaming”。

遥测收集器需要确认连接，并通过消息进行响应，其中包括收集器准备好接收流数据的时间间隔。此间隔表示 Firewall Threat Defense 设备应向收集器发送遥测流的预期频率，范围为 1 分钟（60 秒）到 24 小时。获得有效频率后，系统会发送一组初始指标，然后以请求的速率提供其他信息。

以下是用于通信的 RPC 方法：

- 一元 RPC（控制消息），从 Firewall Threat Defense 设备上的 Telegraf 组件发送，用于配置流传输。

  rpc ConfigureMetricStreaming (TelegrafControlMessage) 返回 (CollectorControlMessage)；

- 流 RPC（数据消息），用于在 Firewall Threat Defense 设备上的 Telegraf 和遥测收集器之间实现指标数据的双向流传输。

  rpc BiDirectionalMetricStreaming (stream TelegrafDataMessage) 返回 (stream CollectorDataMessage)；

以下主题更详细地介绍了遥测收集器应从设备接收的消息，以及收集器必须发送到设备的消息。

Telegraf 控制消息（控制通道）

Telegraf 控制消息由 Firewall Threat Defense 设备上的 Telegraf 组件发往收集器，用于启动指标流传输。其中包含设置为 true 的 init_request 标志。

```
message TelegrafControlMessage {
// Indicates the proto version used by the FTD device. First version will be 1.0
    string version;

// Indicates the device id of the sender
    string device_uuid;

// Indicates the device hostname of the sender
    string hostname;

//list of strings indicating the capabilities of FTD. This will be “metric_streaming”
    repeated string capabilities;

// Flag to initiate a collector response for configuring telemetry streaming
    bool init_streaming = 1;
}
```

收集器控制消息（控制通道）

收集器控制消息是收集器对 Telegraf 控制消息的响应，由收集器发送至 Firewall Threat Defense 设备。其中包含间隔参数，即指标批处理的期望频率，范围为 1 分钟（60 秒）至 24 小时。指标订阅组件为可选。

```
message CollectorControlMessage {
// Indicates the proto version used by the target. Current version supported is 1.0
    string version;
// Time interval at which the FTD device should send metric batches
```

```
    int64 interval = 1;
// Set of metric families to subscribe to, the default value is the only supported value.
// Default: "all"
    repeated string metricSubscriptions = 2;
}
```

流取消消息（控制通道）

流取消消息用于取消 Firewall Threat Defense 设备与遥测收集器之间的已有遥测流。Firewall Threat Defense 设备或收集器均可在控制通道上发出此消息。取消请求接收方须回复 ACK 消息。取消完成后，Firewall Threat Defense 设备每 5 分钟重试连接收集器，直至收集器接受新的流传输请求。要永久终止流传输，只需删除 Firewall Threat Defense 设备上的流传输配置。

```
message StreamCancellationMessage {
// Indicates the proto version used by the FTD device. First version will be 1.0
    string version;

// Indicates the device id of the sender
    string device_uuid;
// This flag indicates that the cancel request is true
    bool cancel_request;
}
```

Telegraf 数据消息（数据通道）

Telegraf 数据消息包含从 Firewall Threat Defense 设备发送到收集器的一批指标。其中包含名为 metrics 的重复字段，内含各条 Metric 消息。

```
message TelegrafDataMessage {
    // Batch of metrics sent by Telegraf
    repeated Metric metrics = 1;
}
```

指标消息（数据通道）

遥测数据是从系统各个组件（例如接口、CPU、内存、磁盘使用情况等）收集的指标，这些指标会从 Firewall Threat Defense 设备传输到遥测收集器以进行监控和分析。此数据的格式由协议定义中的指标消息定义。

以下是包含遥测数据的指标消息示例：

```
METRIC=timestamp:1718257445000
metricFamily:"cpu"  value:0.7  tags:{key:"cpu"  value:"CPU))"}  tags:{key:"description"
value:"cpu_utilisation"}  tags:{key:"process"  value:"lina"}  tags:{key:"rcpu"
value:"x86_cpu0"} tags:{key:"uuid"  value:"7eb19498-2519-11ef-a8dd-b74b4d43a7e7"}
metricType:"Gauge"
```

指标消息可以包含以下字段：

- 时间戳（int64 时间戳）— 记录指标的确切时间，以纪元时间表示。
- 指标族（字符串 metricFamily）— 被测量的系统组件或资源，例如“cpu”、“memory”、“disk”、“interface”。
- 值（双精度值）— 指标的数值。对此值的解释取决于指标类型。例如，CPU 利用率百分比。

- 标记（重复的标记）— 有关指标的其他上下文信息。每个标记都是一个键值对，其中键是描述性标签（例如“cpu”、“process”、“interface”），值提供特定详细信息（例如“CPU0”、“lina”、“GigabitEthernet0/0”）。
- 指标类型（字符串 metricType）— 指标的性质。它可以是随时间累积的“计数器”（例如发送的数据包总数），也可以是表示特定时间点值的“计量器”（例如 CPU 使用率）。

收集器数据消息（数据通道）

收集器数据消息须由收集器发回 Firewall Threat Defense 设备，以确认收到 TelegrafDataMessage。其中包括设置为 true 的 ACK 标志，表示成功接收。

```
message CollectorDataMessage {
    // ACK for every metric batch
    bool ack = 1;
}
```

遥测流故障排除

以下主题介绍如何对遥测流进行故障排除。

检查遥测流服务状态

启用遥测流传输后，配置会立即推送到设备。服务将重启并连接到遥测服务器（前提是所有值均正确且存在通往收集器的路径）。

过程

步骤 1 在 API Explorer 中，进入 **TelemetryStreamingConfig**，选择 **GET /operational/telemetrystreamingstatuses**。

步骤 2 点击**试用**。

步骤 3 如果响应代码为 200，请检查响应正文中的**状态**值。

理想的响应是处于 CONNECTED 状态且无错误消息。

如果状态为 DISCONNECTED，请查看错误消息以确定可能的问题。

例如，以下错误表示无法建立连接。此错误示例是由于提供的 IP 地址不适用于遥测连接器而导致的 I/O 超时。这也可能表示您提供了错误的端口值。请注意，错误分为不同类型，并包含自服务启动以来错误发生的次数。

```
"items": [
    {
      "state": "DISCONNECTED",
      "errors": [
        {
          "errorType": "StreamingErrors",
```

```
          "errorMessage": "2024-09-30 19:20:33.575156378 +0000 UTC m=+308552.647839001 :
rpc error: code = Unavailable desc = connection error: desc = \"transport: Error while
dialing: dial tcp 10.1.1.1:50051: i/o timeout\"",
          "errorCount": 3857,
          "type": "telemetryerror"
        }
```

除 I/O 超时外的另一个常见错误是“无到主机的路由”，这表示网络或 Firewall Threat Defense 设备配置中存在路由问题。

有关错误类型的详细信息，请参阅状态错误类别，第 11 页。

状态错误类别

若遥测流传输服务存在错误，无论服务状态是已连接还是已断开，遥测传输状态信息都包括与遇到的问题相关的错误消息。错误消息含发生错误的时间戳、错误代码及描述。

消息分类如下：

中止错误（代码 0）

导致遥测服务中止的错误。若错误持续，请联系思科技术支持。

系统错误（代码 1 – 10）

这些错误通常意味着未配置主机名或 UUID。这意味着遥测流配置未成功。请重新配置。

缓冲区错误（代码 11 – 20）

这些错误与指标缓冲区有关，例如指标转换问题。若错误持续，请联系思科技术支持。

身份验证错误（代码 21-30）

这些错误表示证书存在问题。评估邮件并解决证书问题。

例如，如果证书已过期，您需要上传新的有效证书并重新启用服务。请确保所有证书均由同一证书颁发机构签名。

流传输错误（代码 31-40）

这些错误与 Firewall Threat Defense 设备和遥测收集器之间的连接有关。问题可能包括错误的 IP 地址和端口号，或 DNS 解析问题。它们也可能与路由问题有关。

要进行修复，可能需要重新进行遥测流配置或解决网络中的路由问题。路由/DNS 问题也可能表明存在暂时性问题，例如，您的上游链路或 DNS 服务器发生故障。

无效参数错误（代码 41-50）

这些错误与邮件中返回的错误数据有关。例如，错误的协议版本或越界的间隔频率。这些错误需要修复遥测收集器，而不是 Firewall Threat Defense 设备。请注意，即使出现这些错误，服务状态可能仍为“已连接”。例如，由于间隔频率超出范围（30 秒），而允许的最小值为 1 分钟，因此会发生以下错误。

```
"state": "CONNECTED",
      "errors": [
```

```
        {
          "errorType": "InvalidArgumentErrors",
          "errorMessage": "2024-09-30 19:20:33.575156378 +0000 UTC m=+308552.647839001
 : Possible proto version mismatch or invalid streaming interval - client=192.168.97.90,
 proto version=0.0.1, streaming interval=30s",
          "type": "telemetryerror"
        }
    ],
```

验证遥测收集器是否接收到数据

验证遥测收集器正在接收来自 Firewall Threat Defense 设备的信息。您应能在遥测收集器控制台上看到相关消息和数据。例如：

```
2024/08/19 11:08:58 D! [grpc_client] Streaming interval set to=1m0s
2024/08/19 11:08:58 D! [grpc_client] Starting listener, attempting to listen at address=:50051
 over tcp
2024/08/19 11:08:58 D! [grpc_client] CERT_PATH: /root/grpc-certs/keys
2024/08/19 11:08:58 D! FTD signalling listener running on port=8087
2024/08/19 11:08:58 D! [grpc_client] Collector server started at port=50051
2024/08/19 11:09:24 D! [grpc_client] DataStream RPC invoked
2024/08/19 11:09:24 D! [grpc_client] ControlStream RPC invoked
2024/08/19 11:09:24 D! [grpc_client] Receiving metrics from
device=firepower-7eb19498-2519-11ef-a8dd-b74b4d43a7e7
2024/08/19 11:09:24 D! [grpc_client] ControlStream - received done signal
2024/08/19 11:09:24 D! [grpc_client] RPC
context=&{device:firepower-7eb19498-2519-11ef-a8dd-b74b4d43a7e7 controlStream:0xc000024120
 dataStream:0xc000096020}
2024/08/19 11:14:24 D! [grpc_client] info - received metric batch of count=479 from
device=firepower-7eb19498-2519-11ef-a8dd-b74b4d43a7e7
2024/08/19 11:14:24 D! [grpc_client] METRIC=timestamp:1718257445000  metricFamily:"interface"
  value:35386  tags:{key:"duplex_mode"  value:"FULL"}  tags:{key:"interface"
value:"GigabitEthernet0/0"}  tags:{key:"interface_description"}  tags:{key:"interface_name"
  value:"inside_interface"}  tags:{key:"interface_type"  value:"GigabitEthernet"}
tags:{key:"mac_address"  value:"0050.5683.0a21"}  tags:{key:"uuid"
value:"7eb19498-2519-11ef-a8dd-b74b4d43a7e7"}  tags:{key:"description"  value:"input_packets"}
  metricType:"Counter"
```

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。

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。

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。