HongKe 虹科

# ntopng 应用示例

广州虹科电子科技有限公司
www.hocyber.com

扫描关注

# ntopng 应用示例

| No. | 应用示例 | 描述 | 跳转 |
| --- | --- | --- | --- |
| 1 | **实时流分析** | • 实时展示接口的Flow（会话）统计信息。 | 点击这里 |
| 2 | **主机流量详细分析** | • 实时/回溯分析特定主机流量详细使用情况。 | 点击这里 |
| 3 | **接口流量详细分析** | • 实时/回溯分析特定接口流量详细使用情况。 | 点击这里 |
| 4 | **历史流回溯分析** | • 回溯分析特定定接口或主机的历史Flow, 应用信息。 | 点击这里 |
| 5 | **实时抓包分析** | • 从指定接口实时抓取流量保存为PCAP文件进行详细分析。 | 点击这里 |

# ntopng 应用示例

| No. | 应用示例 | 描述 | 跳转 |
| --- | --- | --- | --- |
| 6 | **全流量回溯分析** | • ntop提供全流量存储回溯分析的功能。 | 点击这里 |
| 7 | **SNMP监控** | • 使用SNMP监控网络设备接口状态和流量。 | 点击这里 |
| 8 | **主机池划分** | • 根据IP、网段、MAC划分逻辑主机池单独生成流量统计信息。 | 点击这里 |
| 9 | **活动监控** | • 监控特定主机可达性或者主机服务可用性或者测试网络带宽。 | 点击这里 |

# ntopng 应用示例

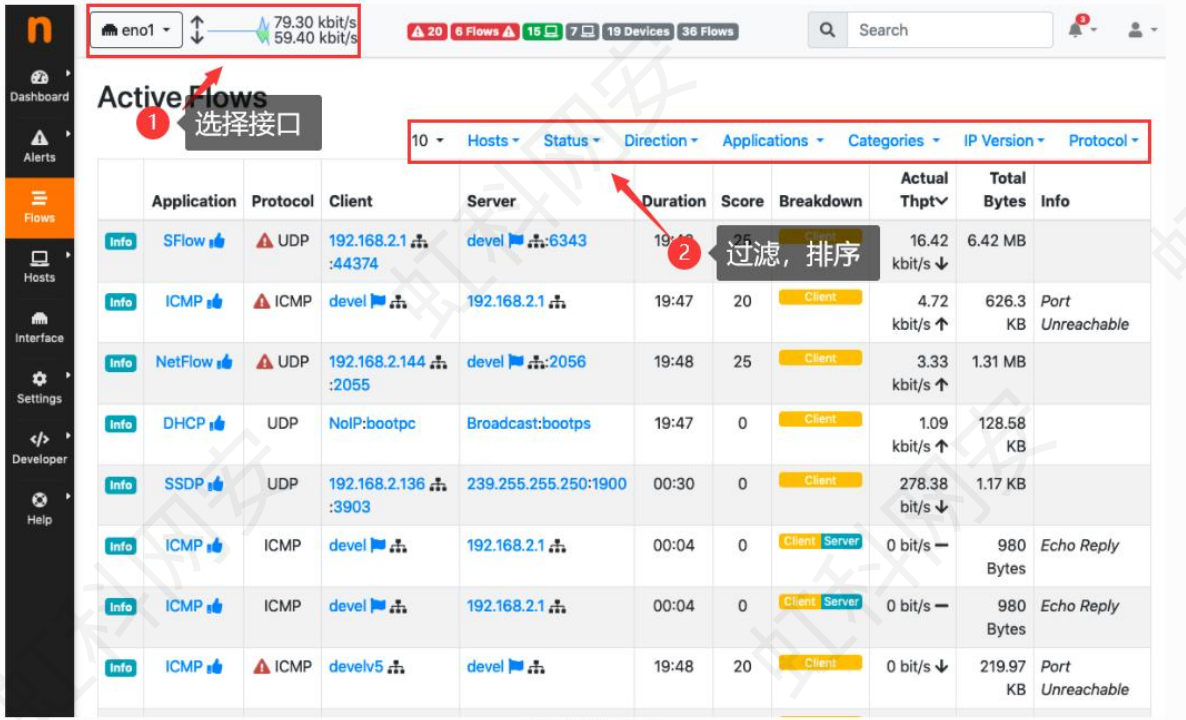
## 实时流分析

[返回主页]

# ntopng 应用示例

- **实时流分析:Flow**

可以选择左侧工具栏中的“Flows”条目来可视化当前活动流量的实时流量信息。可自定义排序方式和过滤显示。



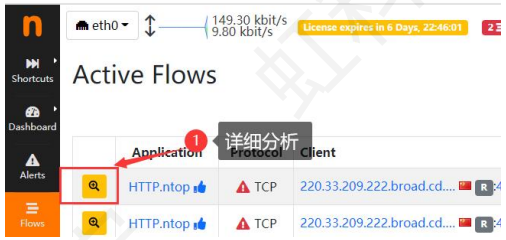

*活动流页面*

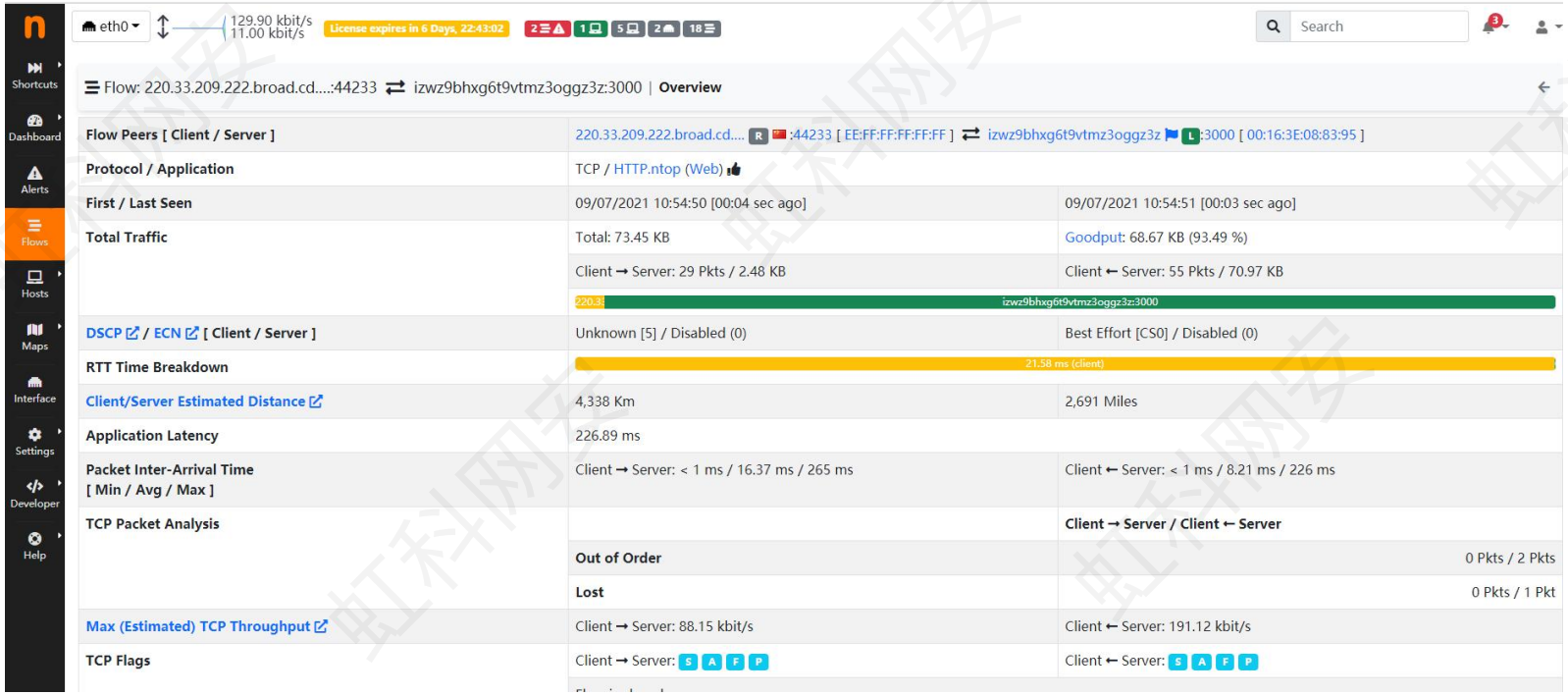
[返回主页]

# ntopng 应用示例

- **实时流分析:Flow**

点击  可以详细分析某个流。




[返回主页]

# ntopng 应用示例

HongKe 虹科

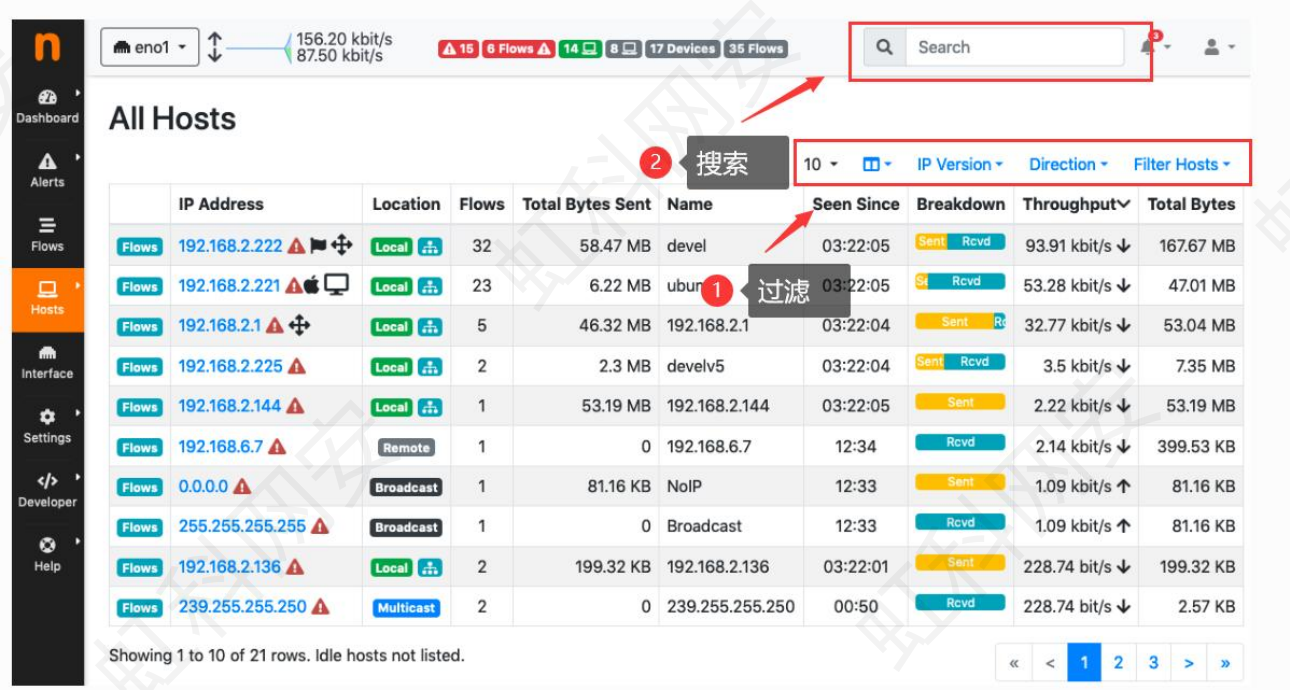
## 主机流量详细分析

[返回主页]

# ntopng 应用示例

- **主机流量分析:Hosts->Hosts**

此页面显示了所有监视网络接口的主机实时流量统计。可以单击列标题以降序（升序）顺序对结果进行排序。表格右上角提供了其他排序选项。点击主机可查看特定主机详细统计信息。




[返回主页]

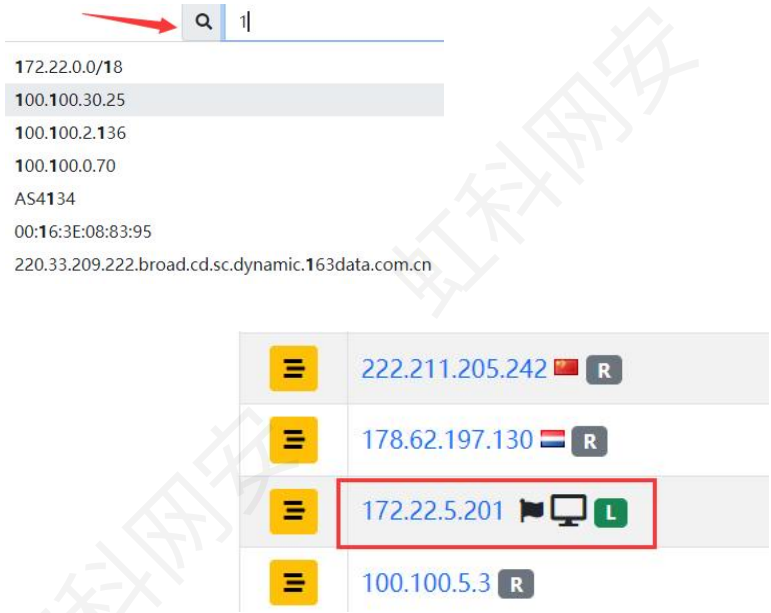
# ntopng 应用示例

- **进入主机详情页面：** 


在Flow，Host->Host或者其他位置搜索栏搜索IP地址可跳转到主机详情页面，或者在任意界面点击感兴趣的IP也能进行跳转。

搜索框提供了一种方便的方式来搜索 ntopng 中的许多流量元素：

- Mac主机（按地址和名称）
- IP地址
- 自治系统
- 动态SNMP 设备

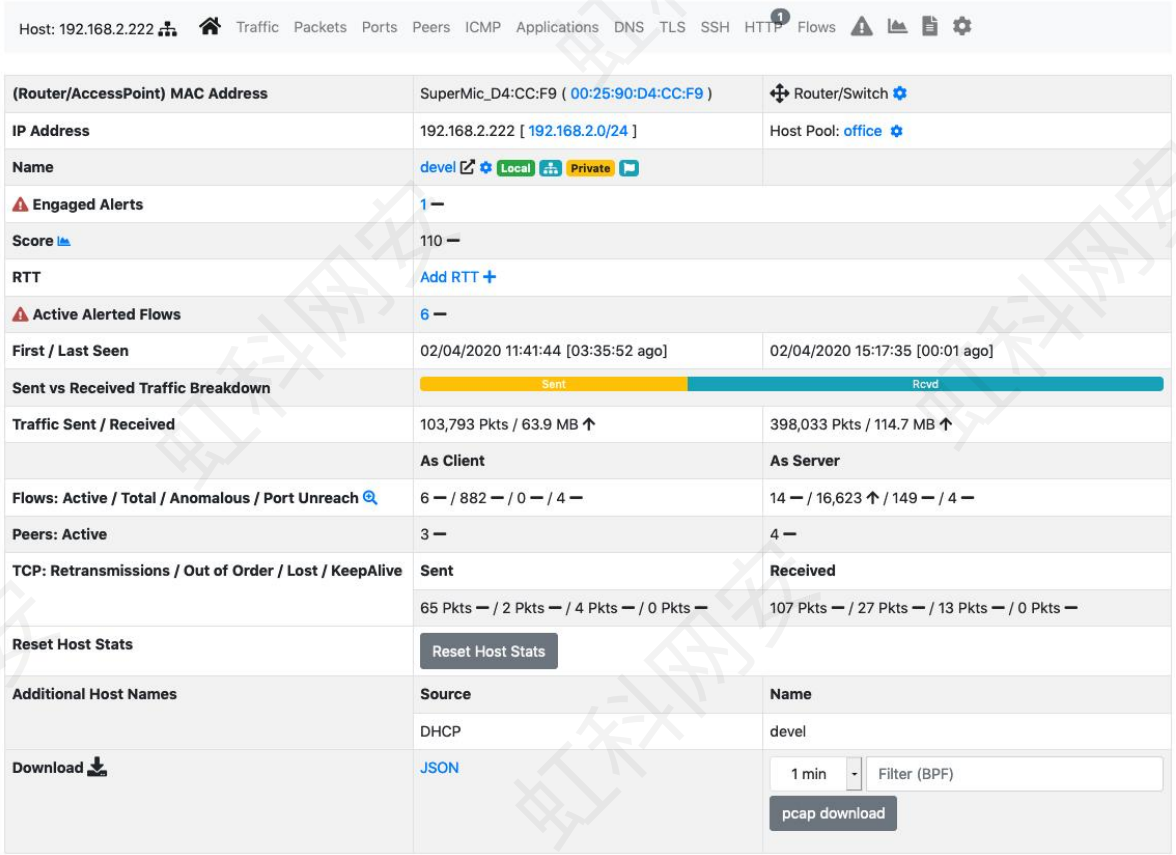



[返回主页]

# ntopng 应用示例

- **主机详情：**


通过上文方法进入主机详细页面后顶部菜单提供了许多选项，可以查看分析指定IP详细历史流量信息，包括应用程序，HTTP，TLS统计，历史流详细等等。

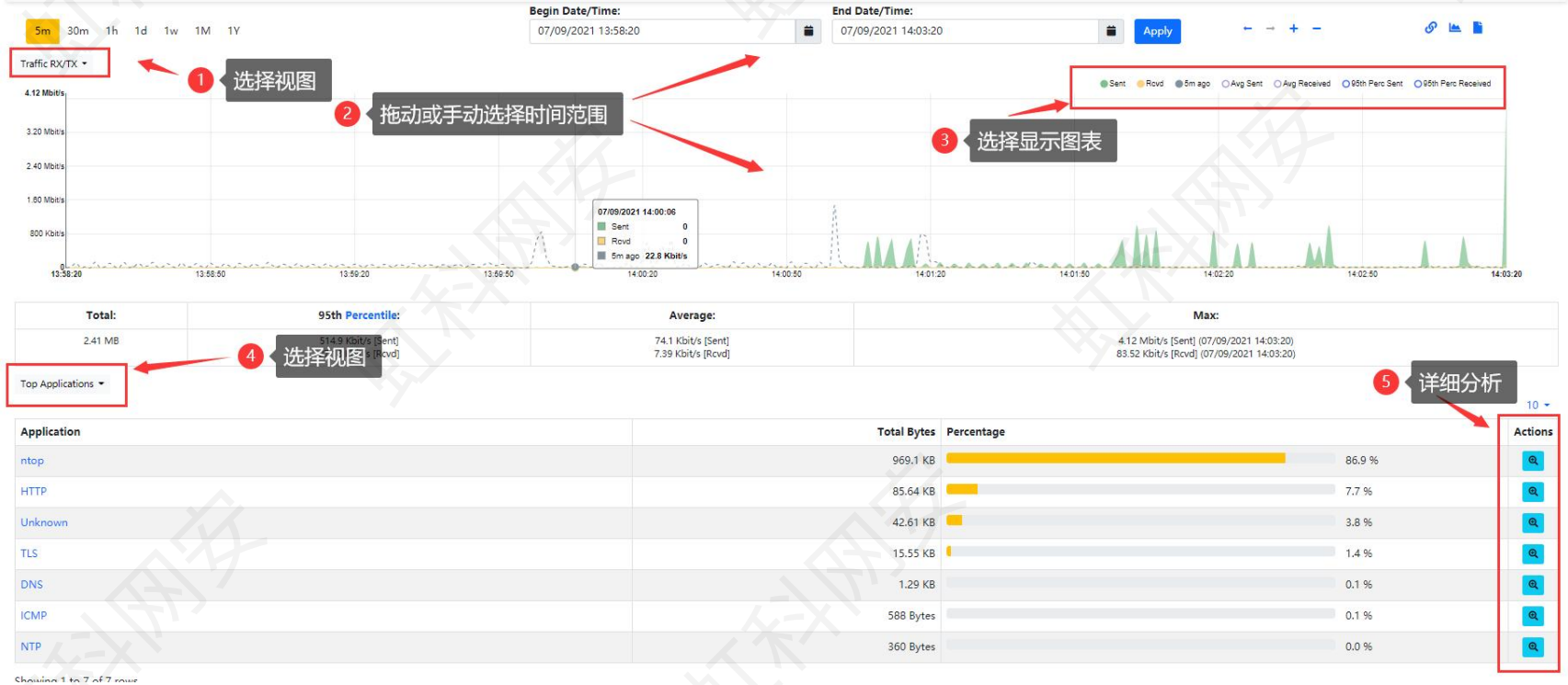



[返回主页]

# ntopng 应用示例

- **主机历史流：主机详细页面->** 

历史流统计页面提供所选主机的历史流量统计信息。用户可以选择基于协议过滤统计数据并以多种格式（例如，字节、数据包、流等）显示数据。（需启用历史流存储功能 *-F=nindex*）




[返回主页]

# ntopng 应用示例

## 接口流量详细分析

[返回主页]

# ntopng 应用示例

- **接口：**

顶部工具栏中的 Interfaces 下拉菜单条目包含列出当前由 ntopng 监控的所有接口。ntopng 中始终存在一个特殊接口，即System Interface。ntopng web GUI 中显示的大部分数据和信息都与当前选择的接口有关。只需单击其名称即可选择列出的任何接口。

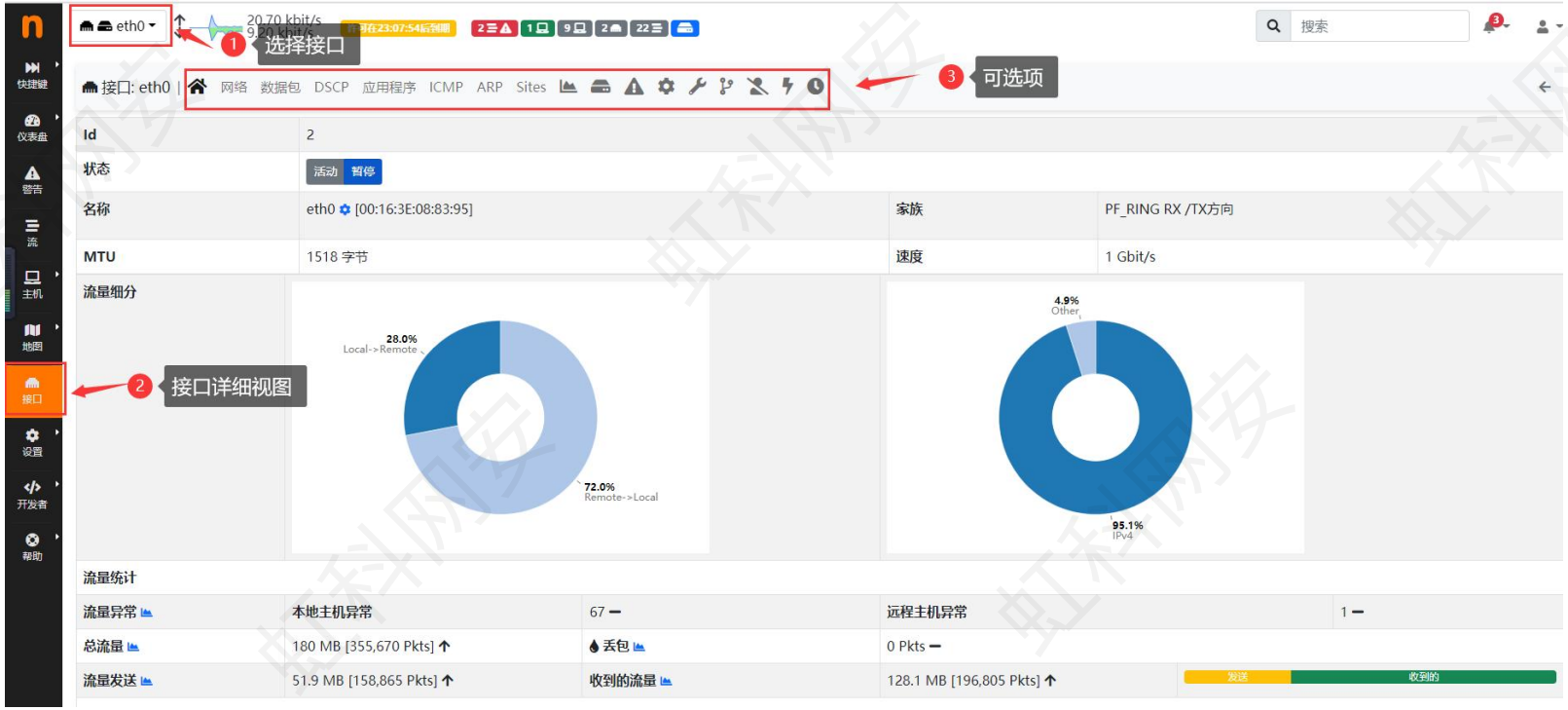

接口下拉菜单

[返回主页]

# ntopng 应用示例

- **接口详细：Interface**

单击*Interface*查看当前选择的接口的流量统计信息，顶部菜单提供了许多可选项，包括数据包统计，应用程序统计，历史流量视图，历史警告等等。

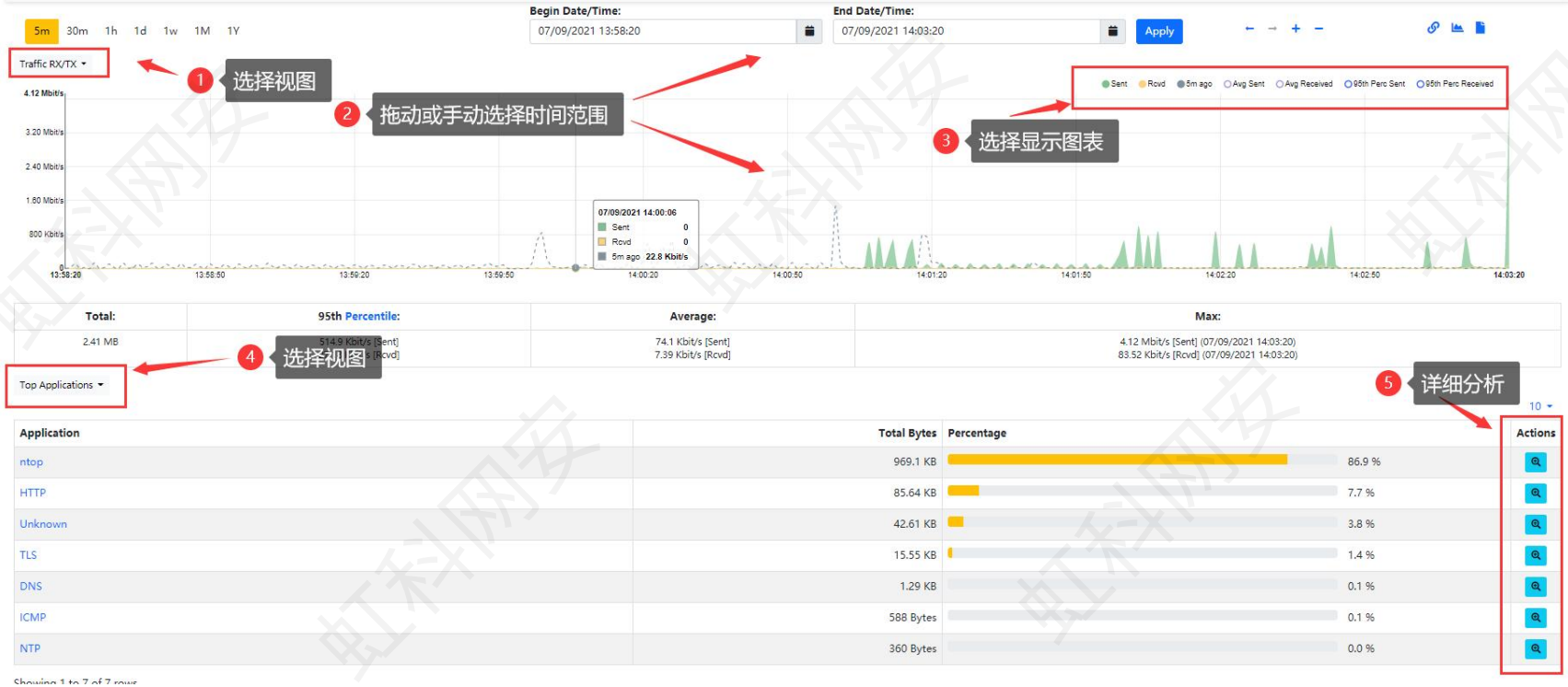



[返回主页]

# ntopng 应用示例

- **接口历史流量视图：Interface->**

统计页面提供所选接口的历史流量统计信息。用户可以选择基于协议过滤统计数据并以多种格式（例如，字节、数据包、流等）显示数据。




[返回主页]

# ntopng 应用示例

HongKe 虹科

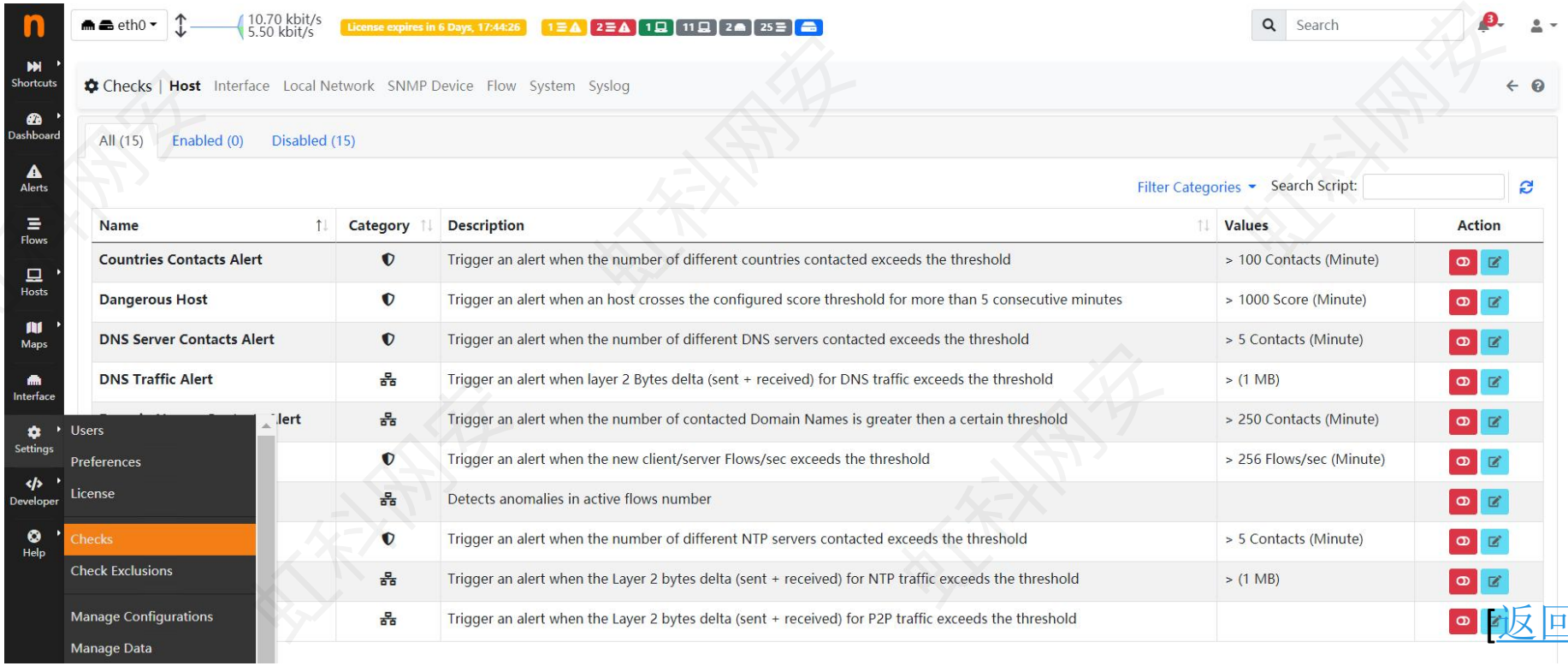
## 警告

[返回主页]

# ntopng 应用示例

- **警报设置： Setting->Checks**

ntopng 警报使用Checks进行评估。对主机、接口、SNMP 设备和其他网络元素执行检查，并可通过设置进行配置。

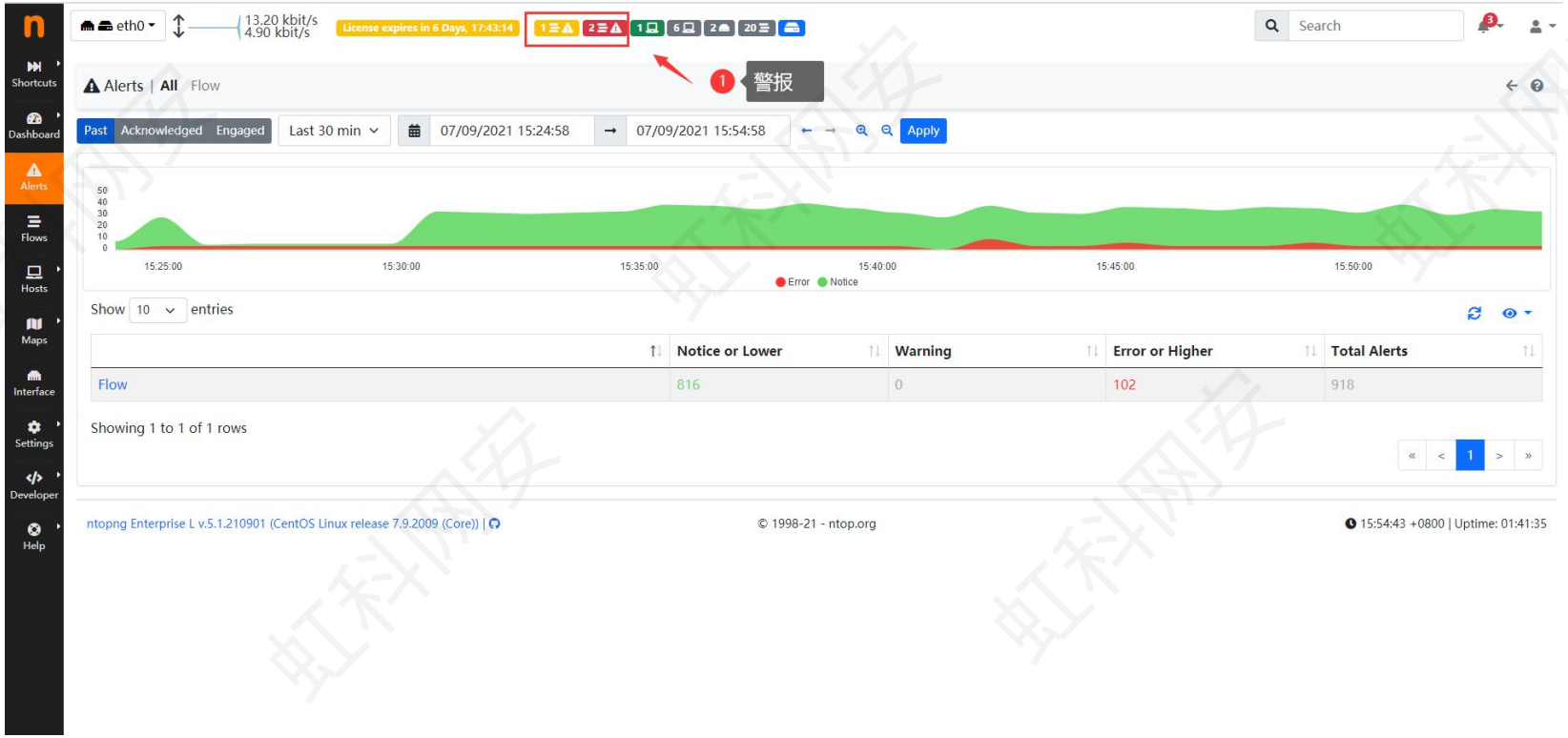



[返回主页]

# ntopng 应用示例

## 警报查询：Alert

ntopng提供了常见流量异常警告功能，通过左侧菜单选择Alert查看当前和历史所有警告信息。并可根据时间范围，警报类型和危险等级等进行高级的过滤。

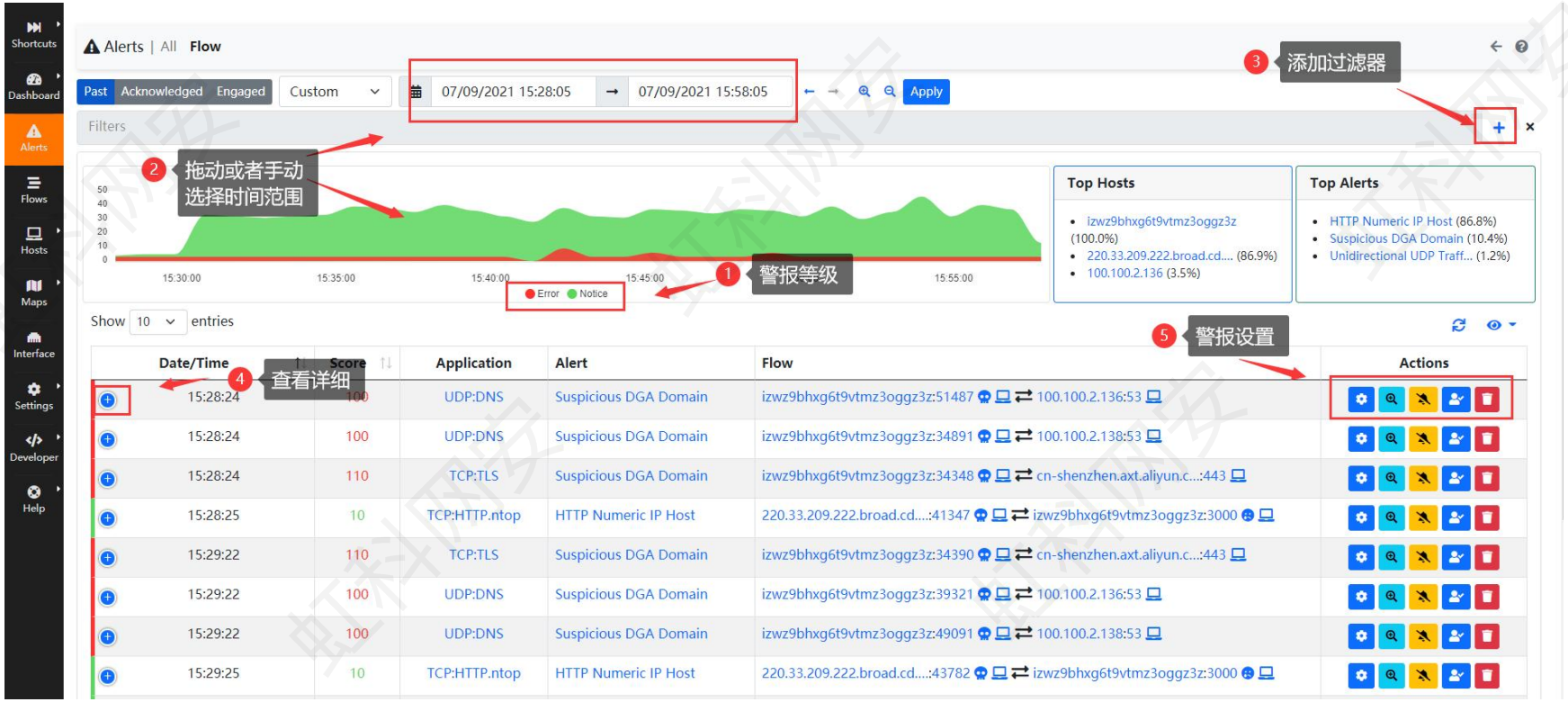



[返回主页]

# ntopng 应用示例

## 警报查询：Alert

通过左侧菜单选择Alert查看当前和历史所有警告信息。并可根据时间范围，警报类型和危险等级等进行高级的过滤。




[返回主页]

# ntopng 应用示例

HongKe 虹科

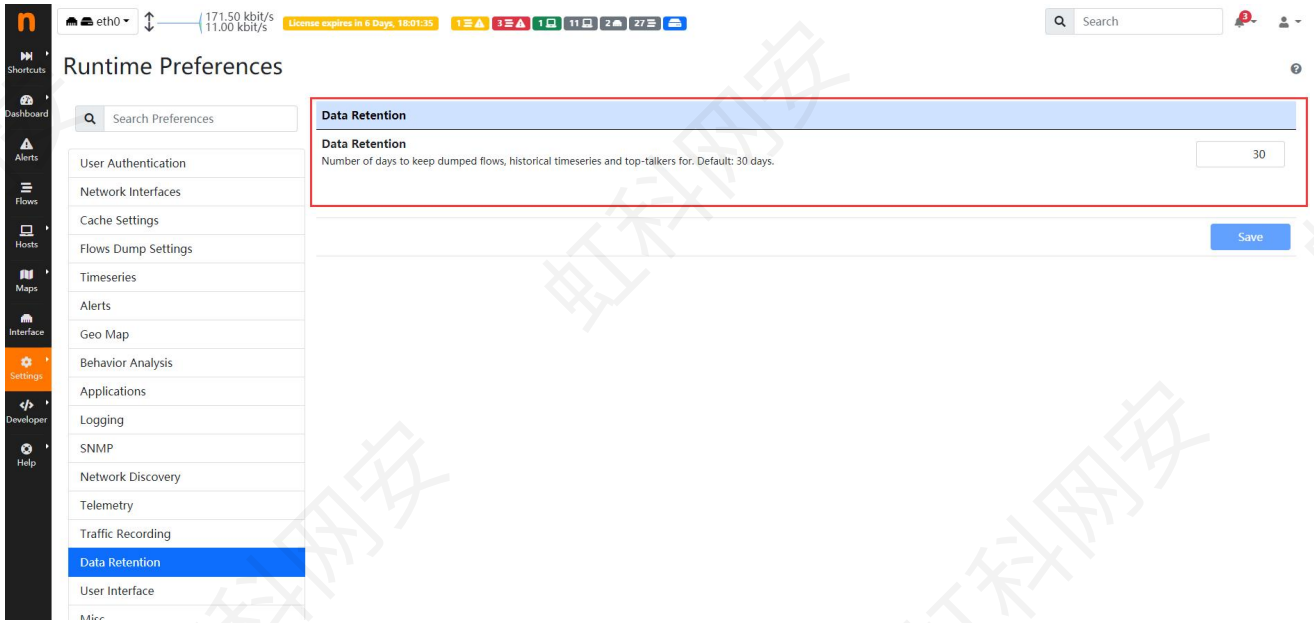
# 历史流回溯分析

[返回主页]

# ntopng 应用示例

- **历史数据存储设置：Setting->Prefrences->Data Retention**

设置数据存储时间将决定历史图表的回溯时长以及*Flow*数据的流存时长。

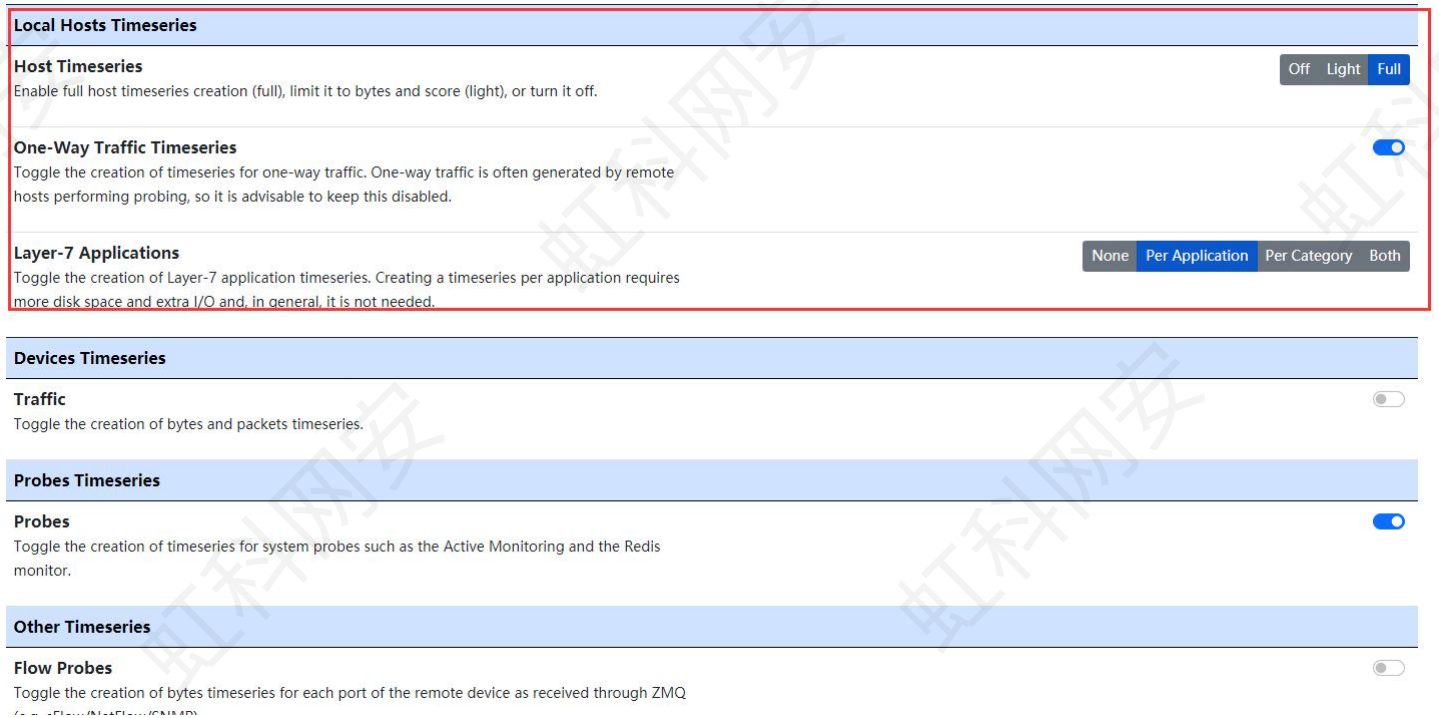



[返回主页]

# ntopng 应用示例

- **时间序列设置：Setting->Prefrences->Timeserise**

时间序列下拉选项中有许多可选项，选择那些模块需要添加时间序列，例如为本地主机添加时间序列设置，这意味着我们可以为每个本地主机单独创建历史图表，只有设置了时间序列，才能生成历史流量时序图。

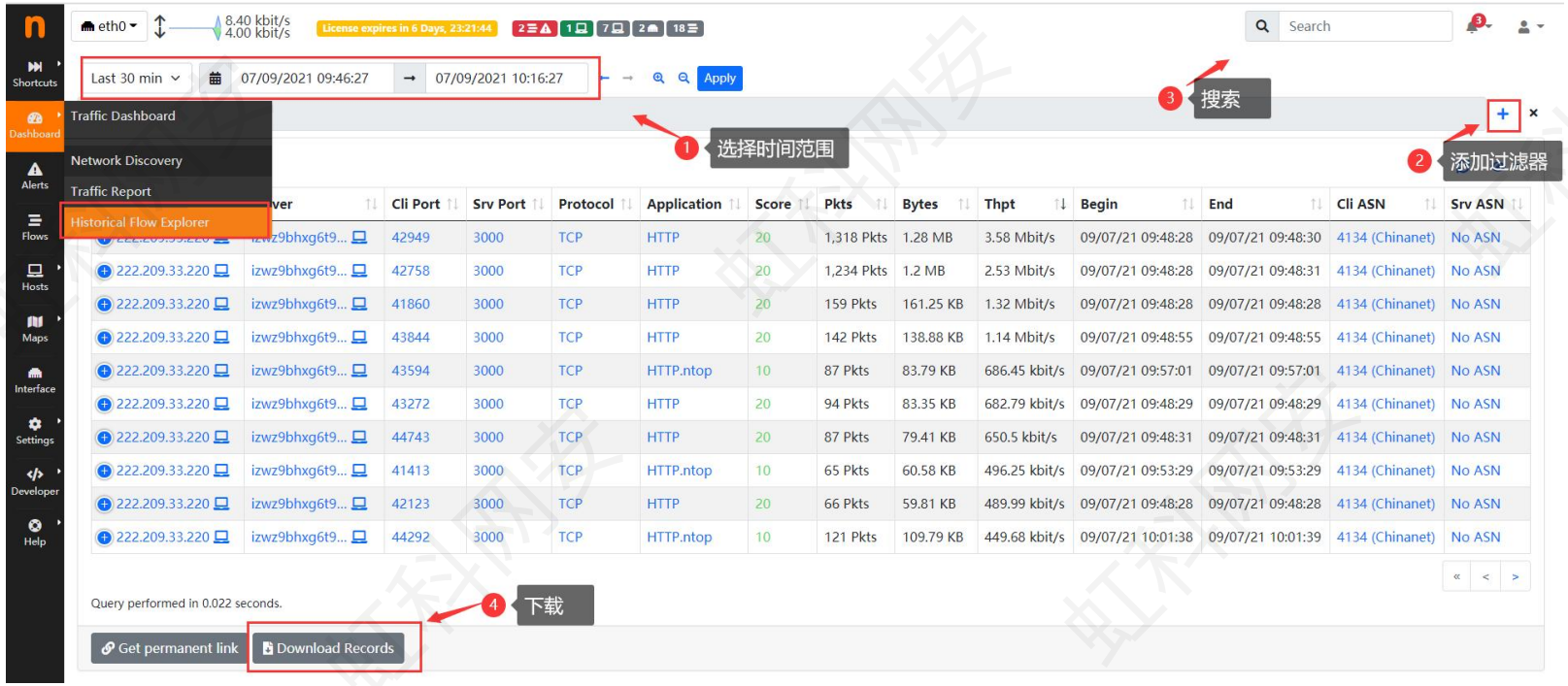



[返回主页]

# ntopng 应用示例

- **历史浏览器：*Historical Explorer***

历史浏览器允许提取特定时间段的历史流信息，可以添加多种过滤器根据IP应用程序筛选感兴趣的流量，根据设置最大可存储一年或以上历史数据。

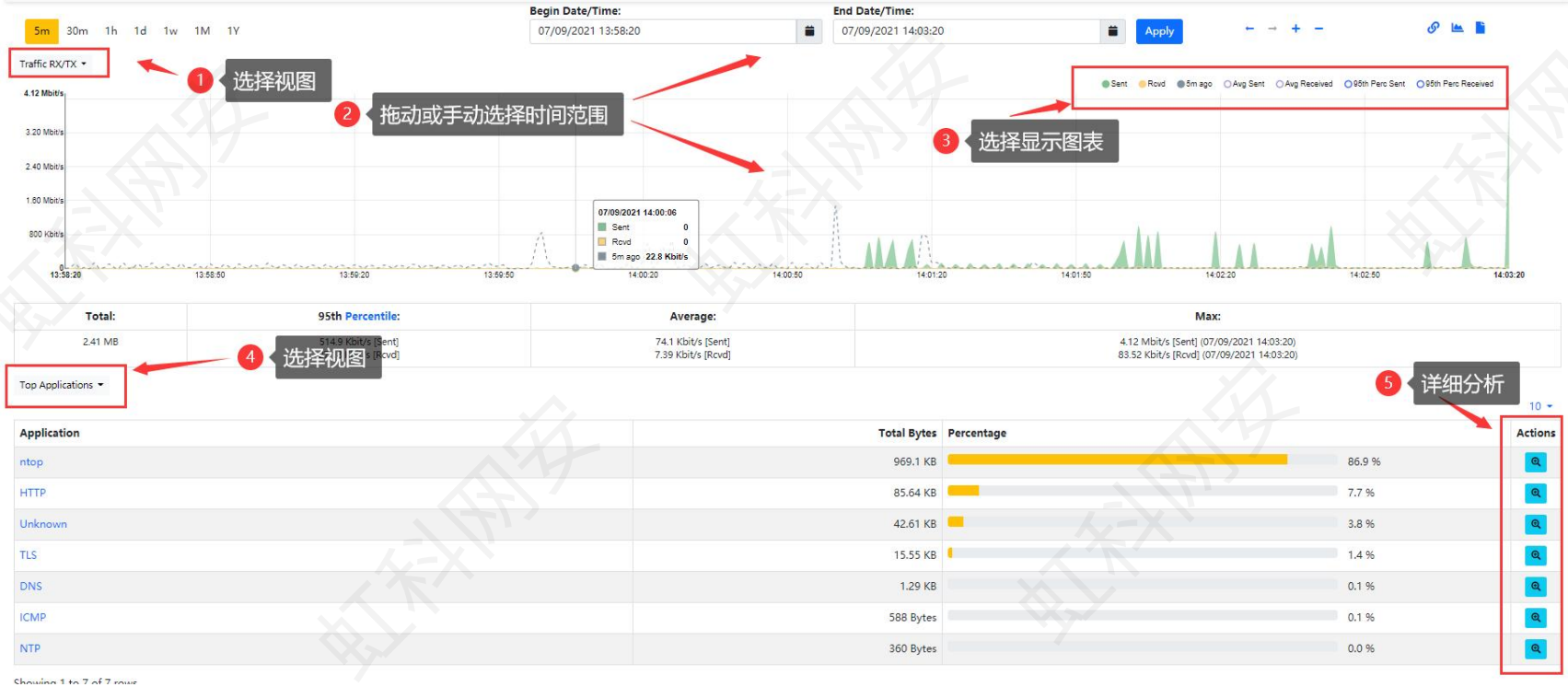



[返回主页]

# ntopng 应用示例

- **接口历史流量回溯分析：**Interface-

接口历史流分析界面，该提供详细的历史流量统计信息。用户可以自由选择需要的分析时间段，基于协议，主机对流量进行过滤分析历史流数据。

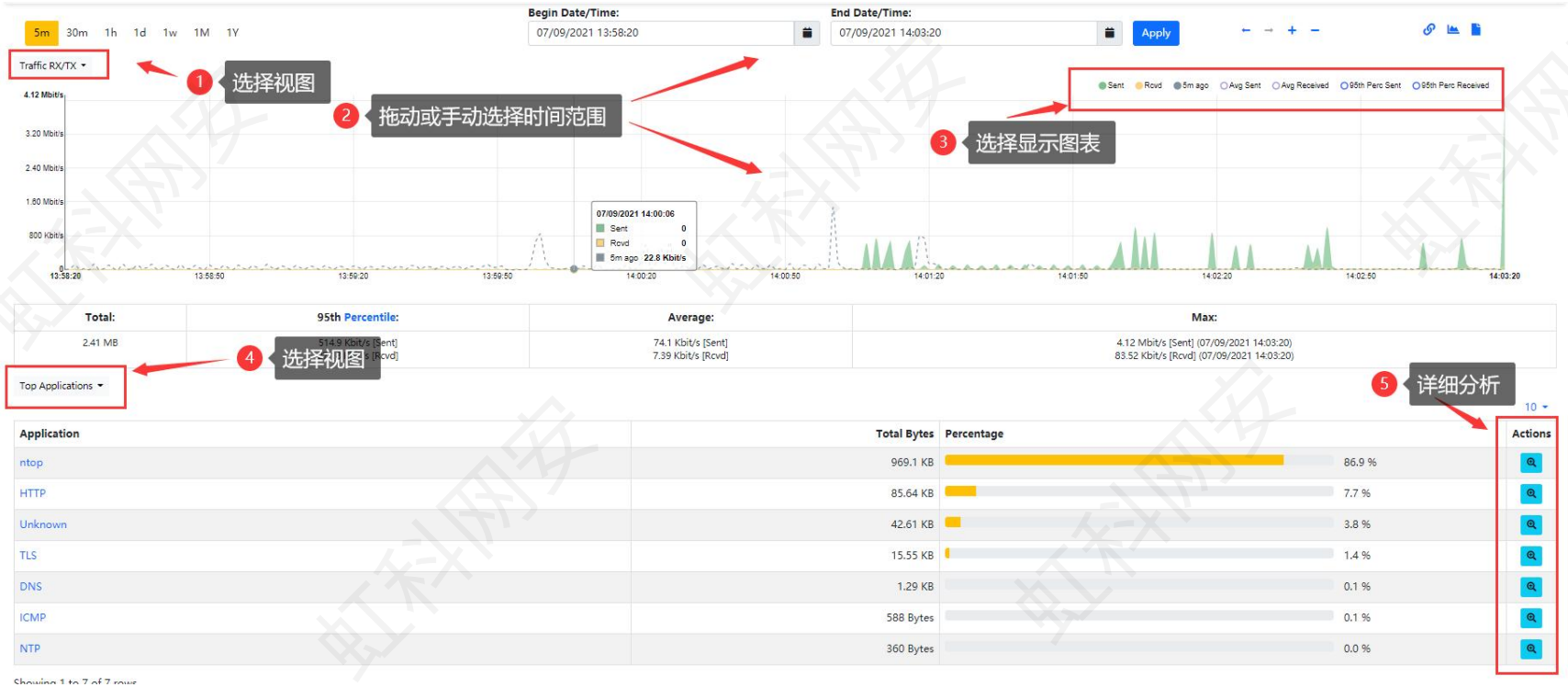



[返回主页]

# ntopng 应用示例

- **主机历史流量回溯分析：**主机详细-> 

在主机详细页面也提供了历史流量分析功能，选择  进行主机级别的历史流量分析，界面与接口历史流量图表基本相同，不同的是这是针对特定*IP*的历史流量分析，




[返回主页]

# ntopng 应用示例

HongKe 虹科

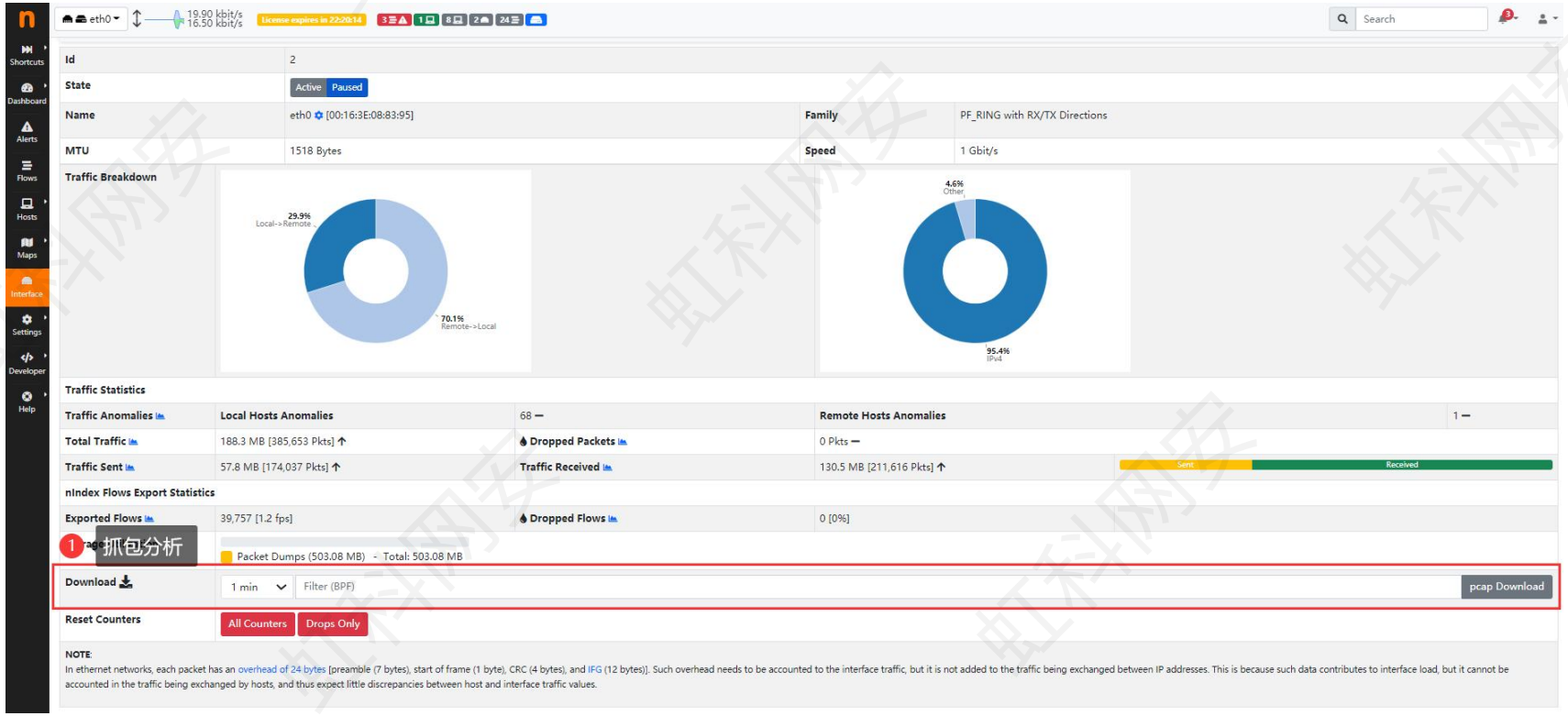
## 实时抓包分析

[返回主页]

# ntopng 应用示例

- **接口抓包分分析：Interface->Home**

在接口详细*Home*页面底部提供实时抓包分析功能，可以设置*BFP*过滤器抓取感兴趣的流量。

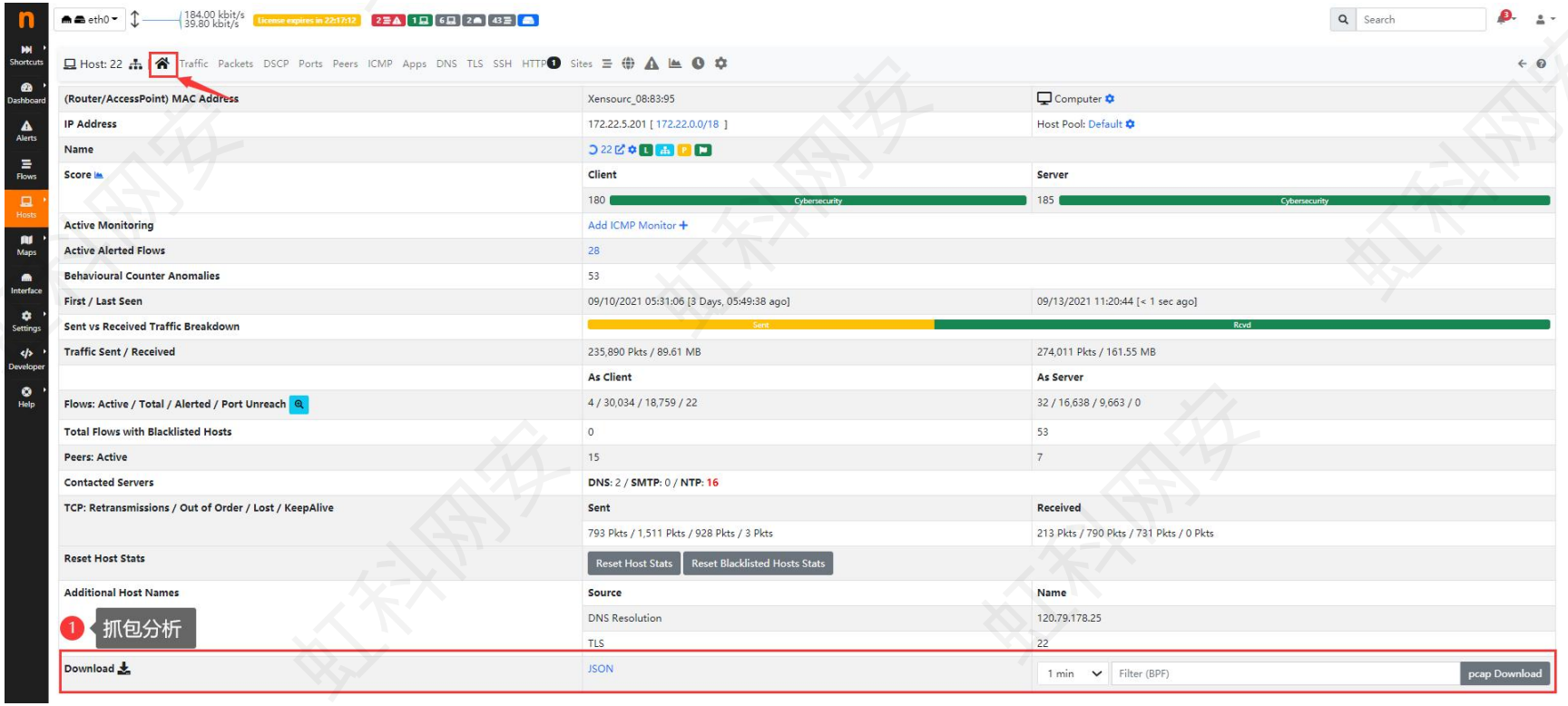



[返回主页]

# ntopng 应用示例

- **主机抓包分分析：主机详情>Home**

在**主机详情**Home页面底部也提供实时抓包分析功能，不同的是这里只抓取该主机IP的流量。




[返回主页]

# ntopng 应用示例

HongKe 虹科

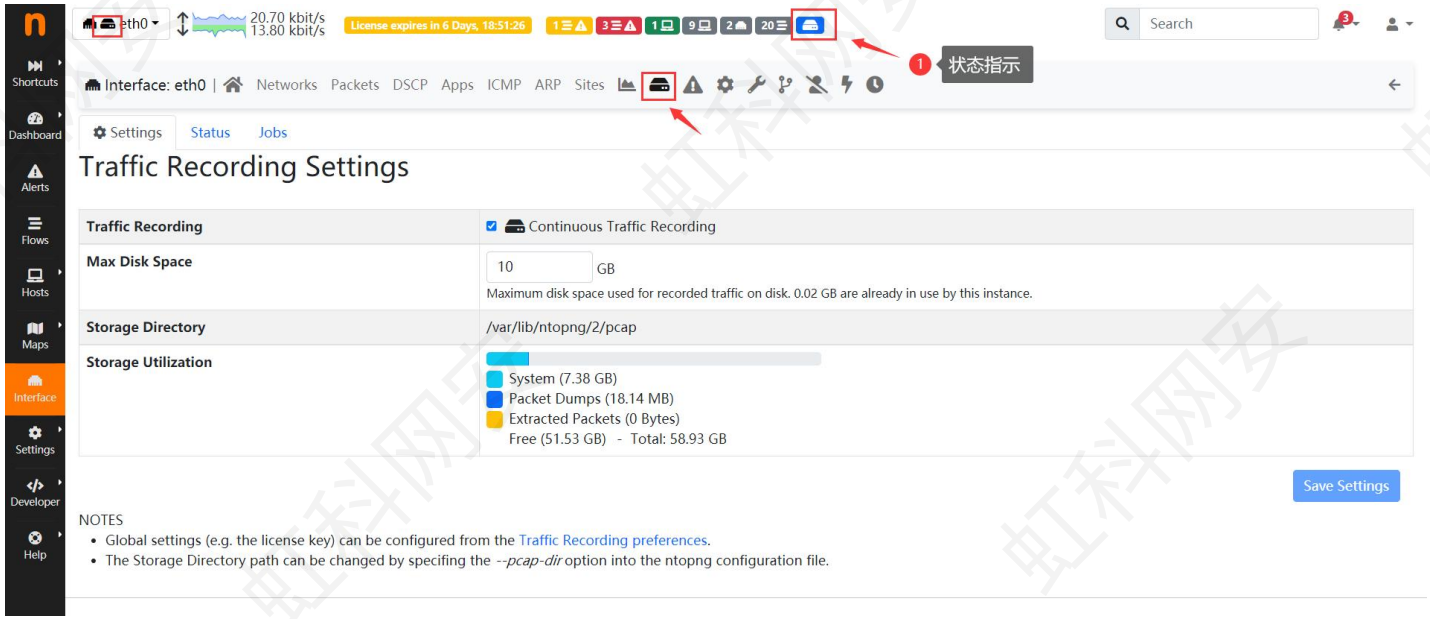
## 全流量回溯分析

[返回主页]

# ntopng 应用示例

- **连续流量记录：Interface->**

当你拥有*n2disk*许可证时，可以起动连续流量记录功能这样将存储所有接口流量，设置最大流量记录空间，当流量超出设置空间时，最开始的流量将被删除。点击保存设置开始记录，设置成功顶部状态指示为蓝色，否则为红色。同时接口处也将增加连续流量记录的图标。

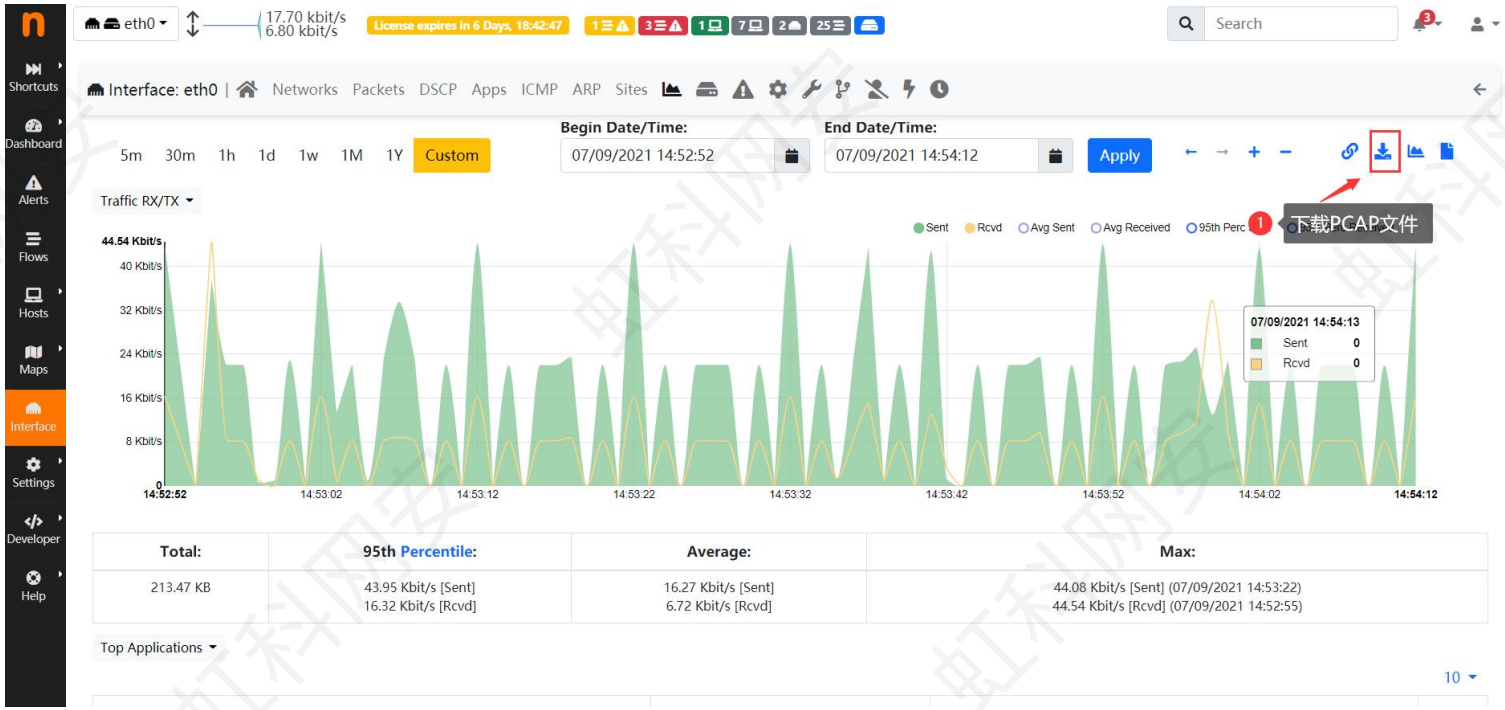



[返回主页]

# ntopng 应用示例

## 全流量回溯分析：Interface

配置成功后可以在接口历史图表，或者主机历史图表选择时间段，下载原始流量PCAP文件。




[返回主页]

# ntopng 应用示例

HongKe 虹科

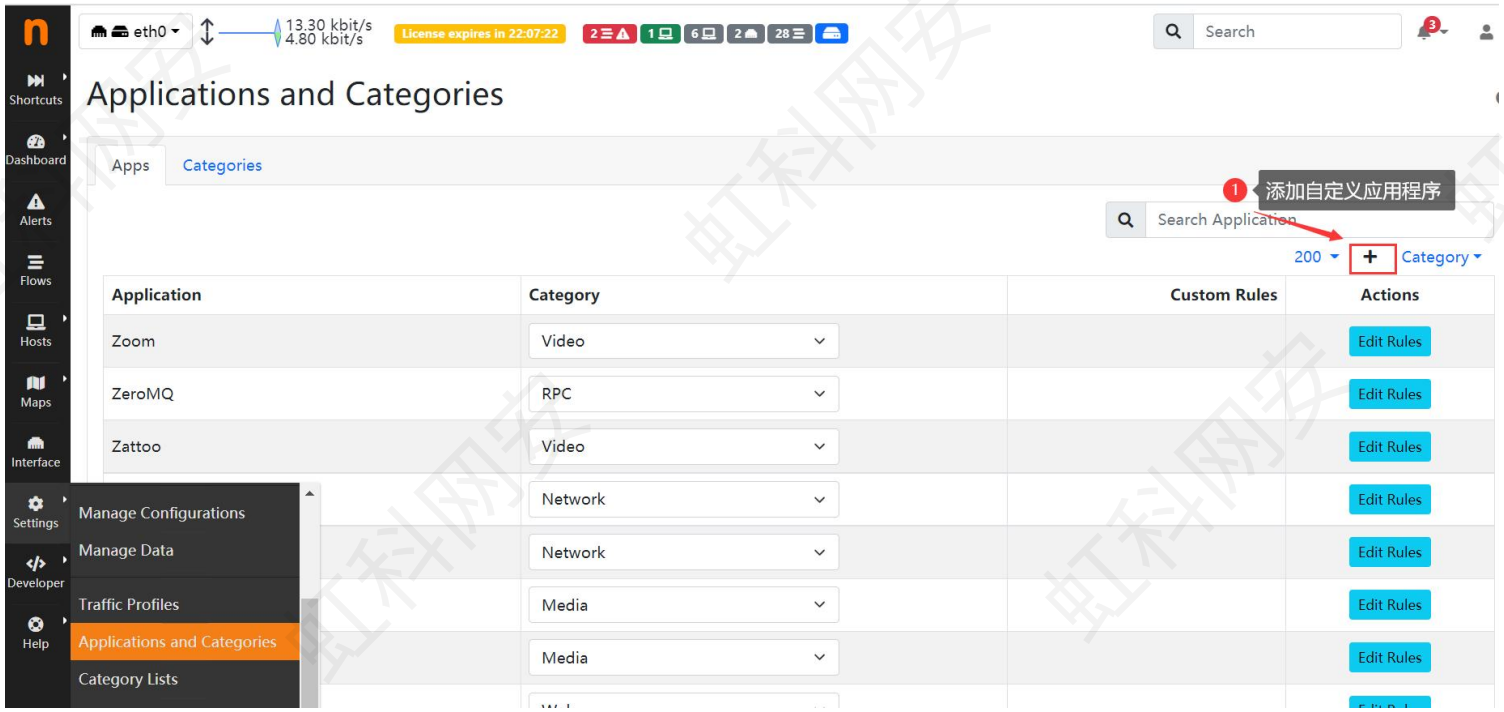
## 自定义应用

[返回主页]

# ntopng 应用示例

- **自定义应用程序：Setting->Applications and Categories**

要启用启用此功能，ntopng 配置文件应该添加 –ndpi-protocols=/var/lib/ntopng/protos.txt选项启动。如果您已经有 protos 文件，请将其移动到/var/lib/ntopng/protos.txt并运行，然后在Setting->Applications and Categories点击添加。




[返回主页]

# ntopng 应用示例

- **自定义应用程序：Setting->Applications and Categories**

通过单击 +或者 Edit Rules 按钮，可以直接从 GUI 编辑应用程序规则并添加新协议。需要注意的是，规则和新协议只会在 ntopng 重新启动后创建和应用。目前支持根据IP，网段，端口和字符串匹配规则。


[返回主页]

# ntopng 应用示例

HongKe 虹科

## SNMP监控

[返回主页]

# ntopng 应用示例

- **启动SNMP时间序列：Setting->Preferences->SNMP**

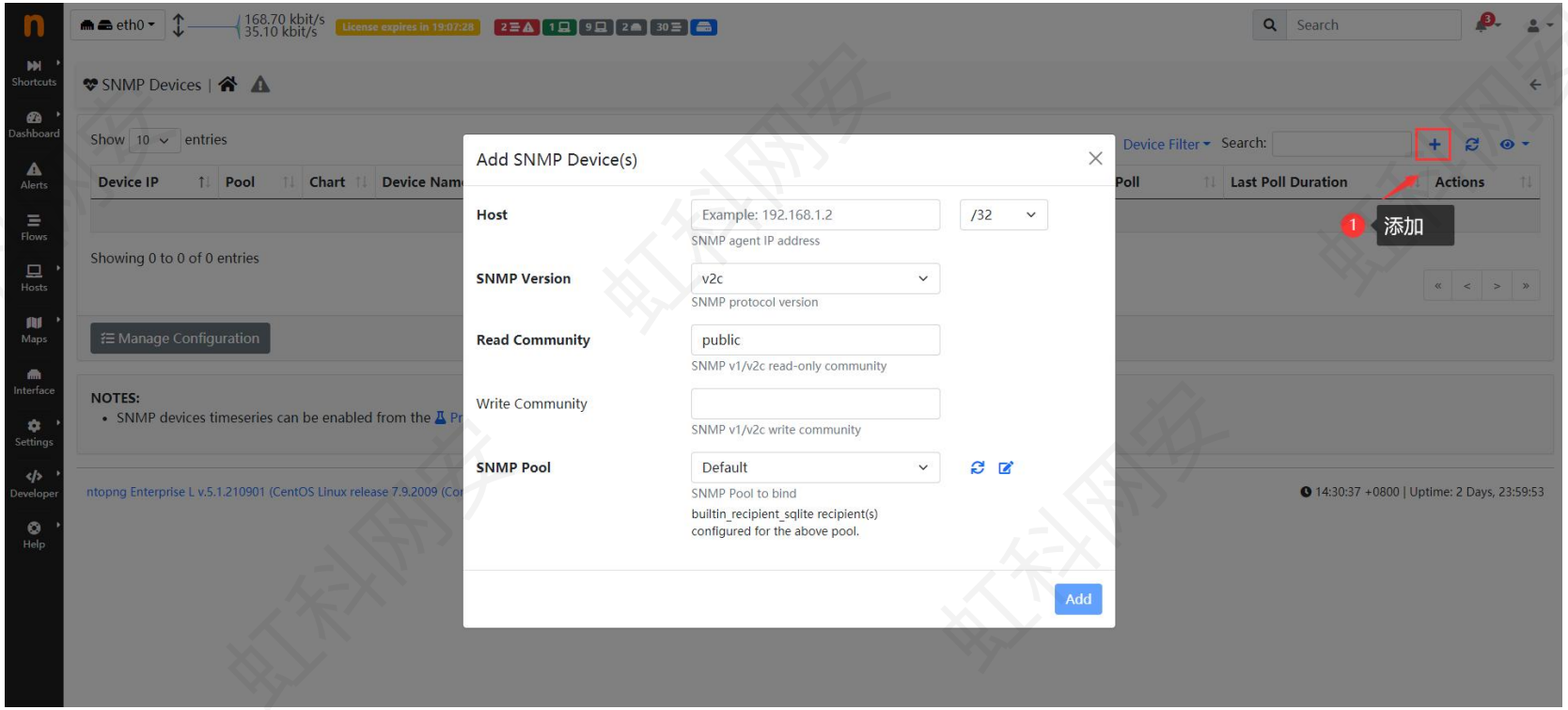
在首选项->SNMP中可以设置启用SNMP时间序列，这将为每个SNMP接口创建时序表。


[返回主页]

# ntopng 应用示例

- **添加SNMP设备：Shortcuts->SNMP**

在SNMP监控界面点击添加即可添加SNMP设备。

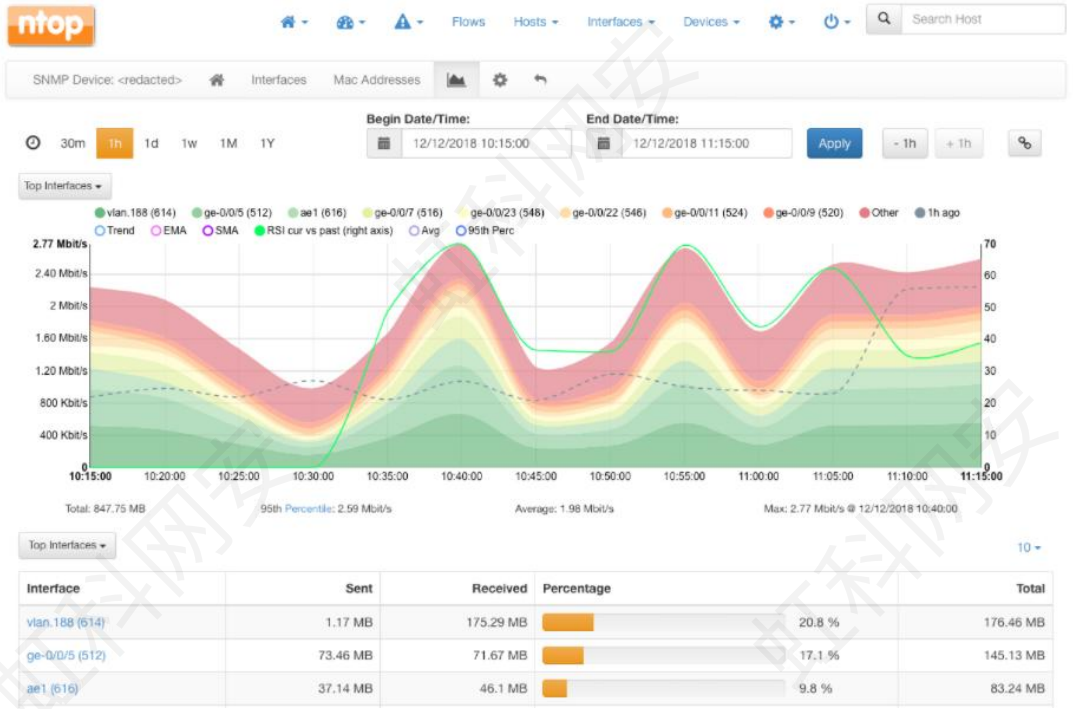



[返回主页]

# ntopng 应用示例

- **SNMP历史图表：**

最有用的历史图表将显示特定时间范围内最高接口流量速度的堆叠图表。在图表正下方，还显示了同一时间范围内的接口总数。

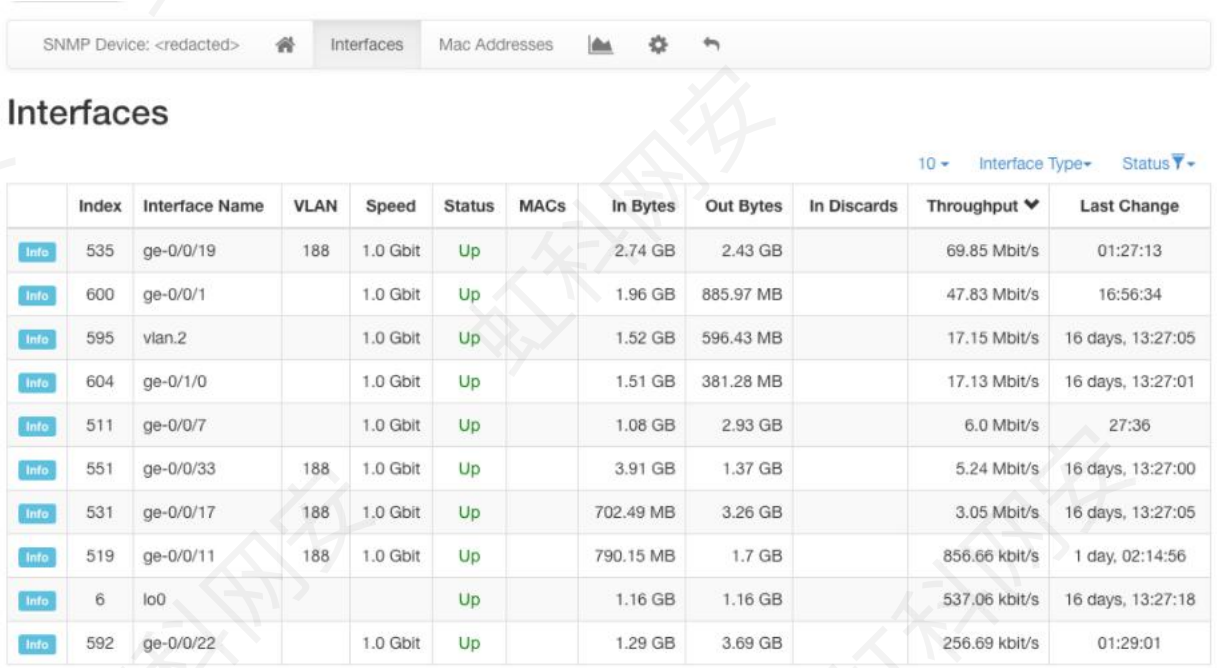



[返回主页]

# ntopng 应用示例

- **SNMP接口列表：**

设备接口状态现在显示在动态加载的分页表中。




| | Index | Interface Name | VLAN | Speed | Status | MACs | In Bytes | Out Bytes | In Discards | Throughput | Last Change |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Info | 535 | ge-0/0/19 | 188 | 1.0 Gbit | Up | | 2.74 GB | 2.43 GB | | 69.85 Mbit/s | 01:27:13 |
| Info | 600 | ge-0/0/1 | | 1.0 Gbit | Up | | 1.96 GB | 885.97 MB | | 47.83 Mbit/s | 16:56:34 |
| Info | 595 | vlan.2 | | 1.0 Gbit | Up | | 1.52 GB | 596.43 MB | | 17.15 Mbit/s | 16 days, 13:27:05 |
| Info | 604 | ge-0/1/0 | | 1.0 Gbit | Up | | 1.51 GB | 381.28 MB | | 17.13 Mbit/s | 16 days, 13:27:01 |
| Info | 511 | ge-0/0/7 | | 1.0 Gbit | Up | | 1.08 GB | 2.93 GB | | 6.0 Mbit/s | 27:36 |
| Info | 551 | ge-0/0/33 | 188 | 1.0 Gbit | Up | | 3.91 GB | 1.37 GB | | 5.24 Mbit/s | 16 days, 13:27:00 |
| Info | 531 | ge-0/0/17 | 188 | 1.0 Gbit | Up | | 702.49 MB | 3.26 GB | | 3.05 Mbit/s | 16 days, 13:27:05 |
| Info | 519 | ge-0/0/11 | 188 | 1.0 Gbit | Up | | 790.15 MB | 1.7 GB | | 856.66 kbit/s | 1 day, 02:14:56 |
| Info | 6 | lo0 | | | Up | | 1.16 GB | 1.16 GB | | 537.06 kbit/s | 16 days, 13:27:18 |
| Info | 592 | ge-0/0/22 | | 1.0 Gbit | Up | | 1.29 GB | 3.69 GB | | 256.69 kbit/s | 01:29:01 |

[返回主页]

# ntopng 应用示例

HongKe 虹科

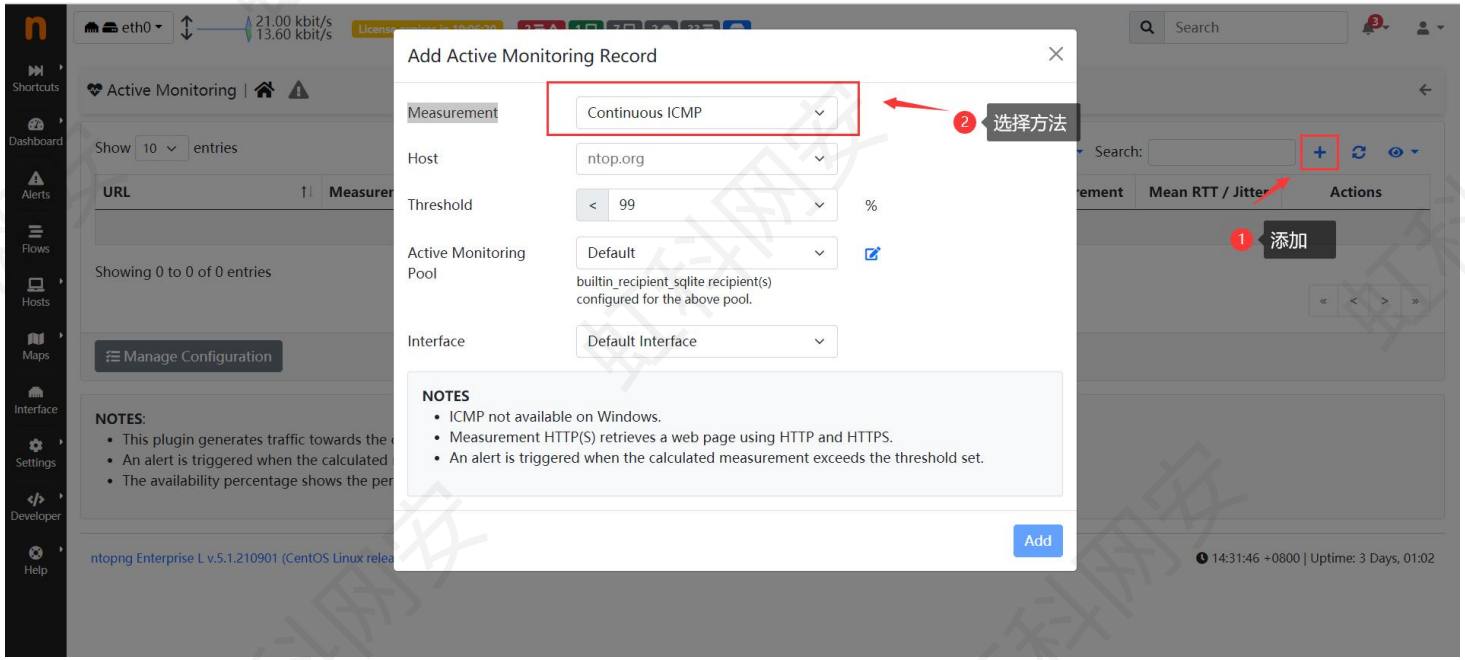
## 活动监控



[返回主页]

# ntopng 应用示例

- 添加活动监控：Shortcuts->SNMP



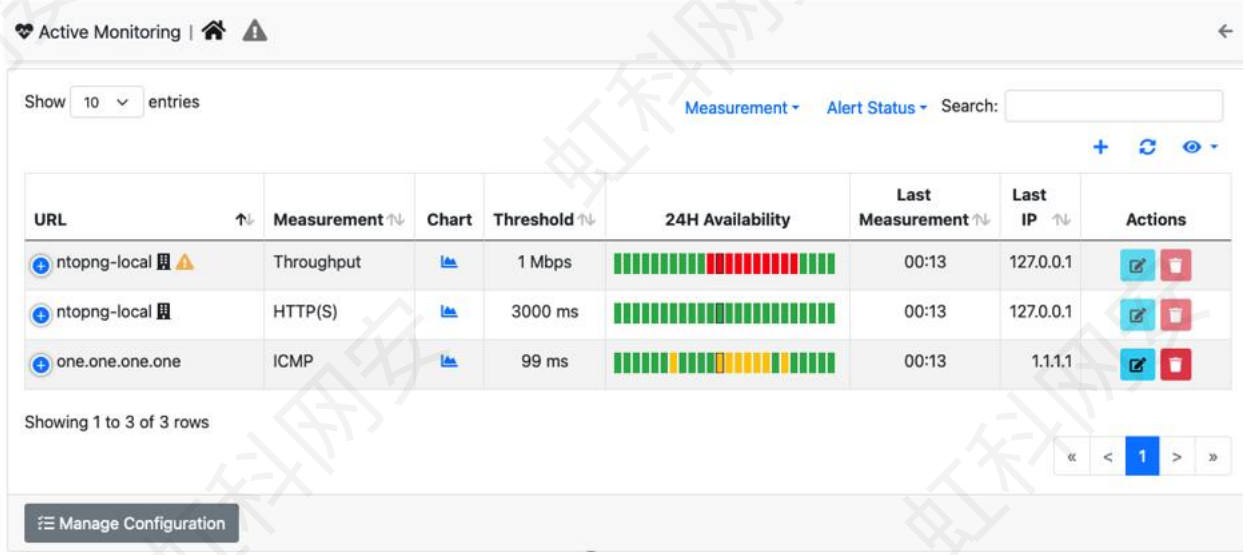

[返回主页]

# ntopng 应用示例

- **活动监控： Shortcuts-> Active Monitoring**

活动监视器每分钟探测配置主机以检查：

- ICMP ：检查主机 IP 可达性
- HTTP 和 HTTPS：检查主机 Web 服务器的功能
- Speedtest：检查互联网带宽




[返回主页]

# ntopng 应用示例

HongKe 虹科

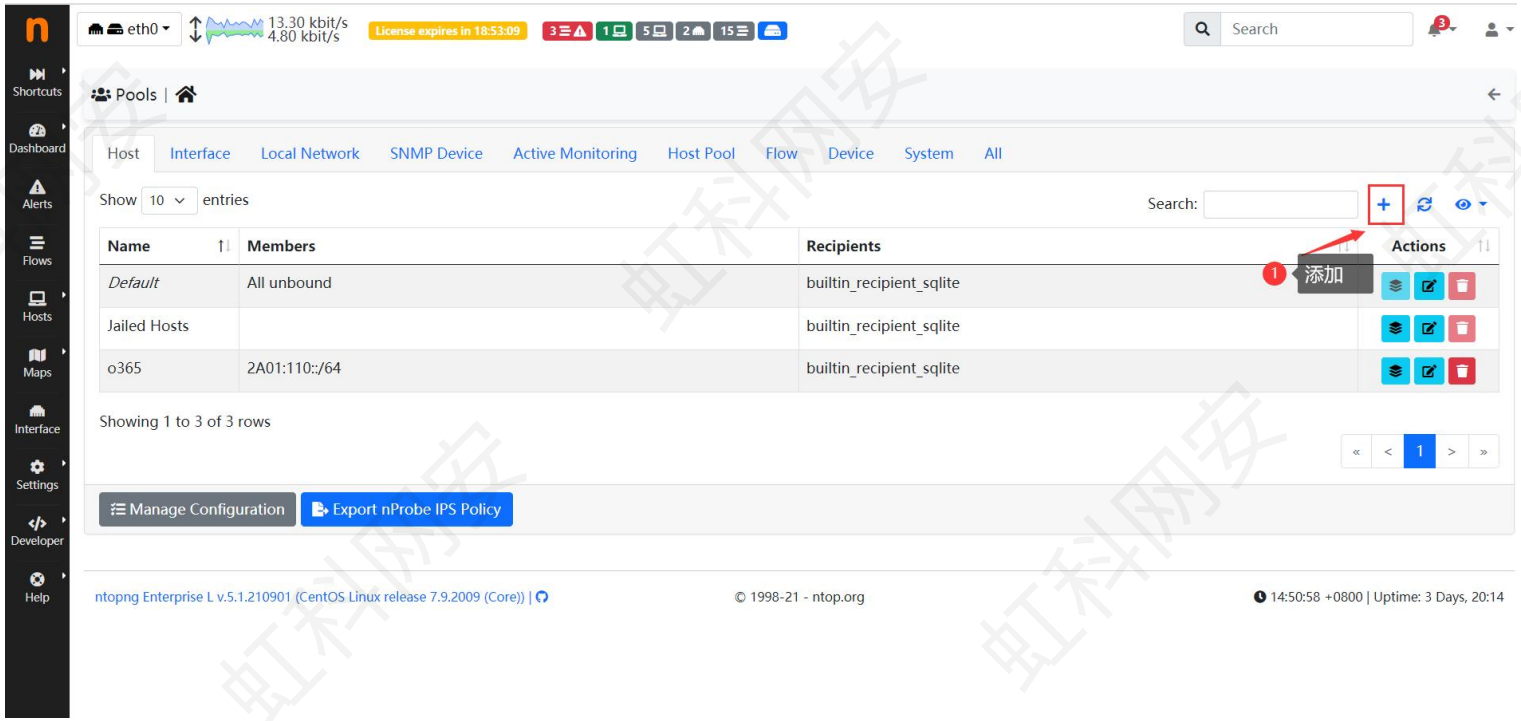
## 主机池划分

[返回主页]

# ntopng 应用示例

- **主机池划分： Shortcuts-> Pools**

主机池是主机的逻辑组，可以根据IPv4/IPv6网段，MAC地址等划分自定义主机池，对每个主机池生成单独的流量统计信息，可以在，Shortcuts-> Pools 点击 + 添加主机池。

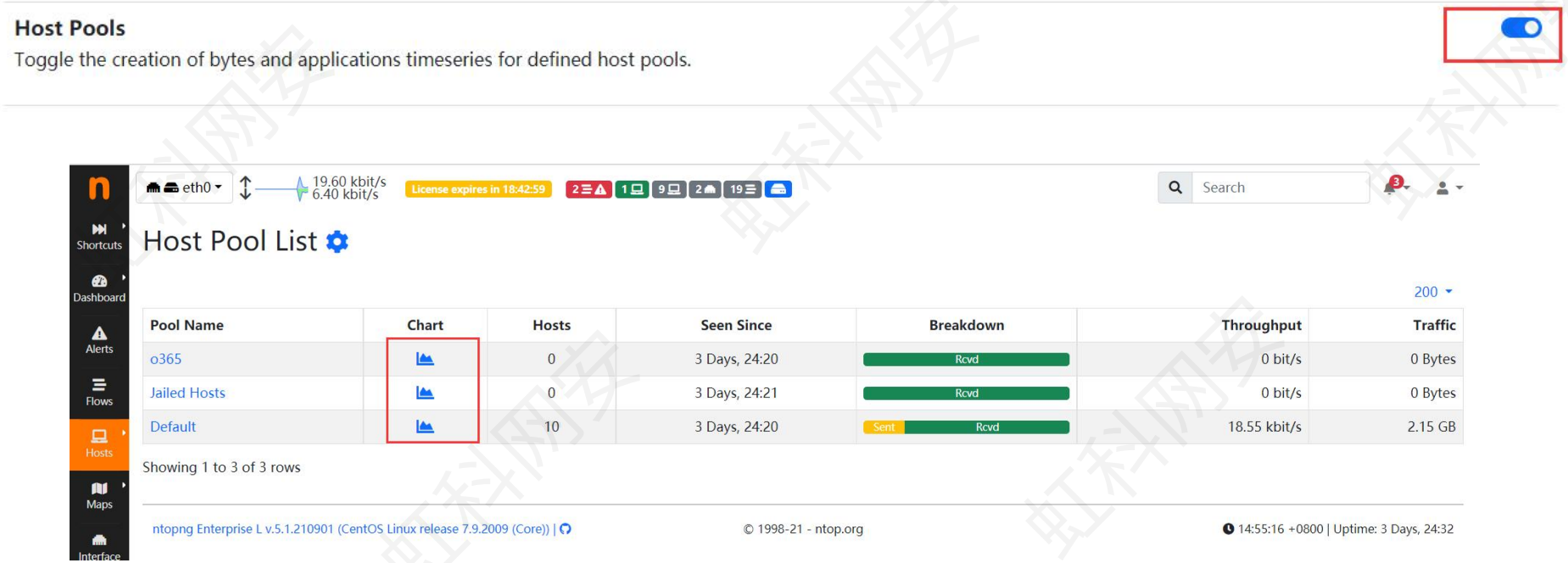



[返回主页]

# ntopng 应用示例

- **主机池添加时间序列： Settings-> Preferences->Timeserise**

为主机池添加时间序列可以为每个主机池创建历史流量时序视图，可在Hosts->Host Pool查看主机池流量使用详细，点击主机名或者历史图表 查看更多详细统计信息。




[返回主页]