



Paragon Active Assurance Packet Capture機能の設定手順

ジュニパーネットワークス株式会社

2023/05/10

Non-live packet captureとLive packet capture

- Non-live packet capture

指定したフレーム数までキャプチャ後、キャプチャデータをダウンロード。ダウンロード後にWireshark等でデータの確認が可能。

- NAT配下のTest Agent上でもパケットキャプチャが可能
- リアルタイムでのキャプチャが不可。キャプチャできるサイズが15MBまで。

- Live packet capture

Wiresharkにリアルタイムでキャプチャデータを転送することが可能。

- リアルタイムのトラフィックが確認でき、Non-live packet captureよりも、より多いトラフィックのキャプチャが可能
- NAT配下のTest Agentにはサポートされていない

Non-live packet capture実行手順

1. メニューから“Apps”へ移動し、“Remote Packet Capture”を選択

The image displays two screenshots of the Paragon Active Assurance web interface. The left screenshot shows the main navigation menu with the 'Apps' option highlighted by a red box. The right screenshot shows the 'Applications' page with the 'Remote Packet Capture' option highlighted by a red box. The 'Remote Packet Capture' option includes a description: 'Troubleshoot app problems using remote packet capture and analysis.'

PARAGON ACTIVE ASSURANCE

PARAGON ACTIVE ASSURANCE

Applications


Speedtest
Use browser-based speed tests to simplify customer support.

Remote Packet Capture
Troubleshoot app problems using remote packet capture and analysis.

Non-live packet capture実行手順

2. 各項目を記入し、“Start”をクリック。パケットキャプチャ後、“Download”をクリック。
ダウンロードしたファイルはWireshark等で確認が可能。

Remote packet capture

Capture interfaces:  IPv4 ● TA1: eth1 (192.168.5.2/24)

Frame size (bytes):

Number of frames: Max number of captured frames for 1518 = 9881

Capture filter:

Start

Remote packet capture

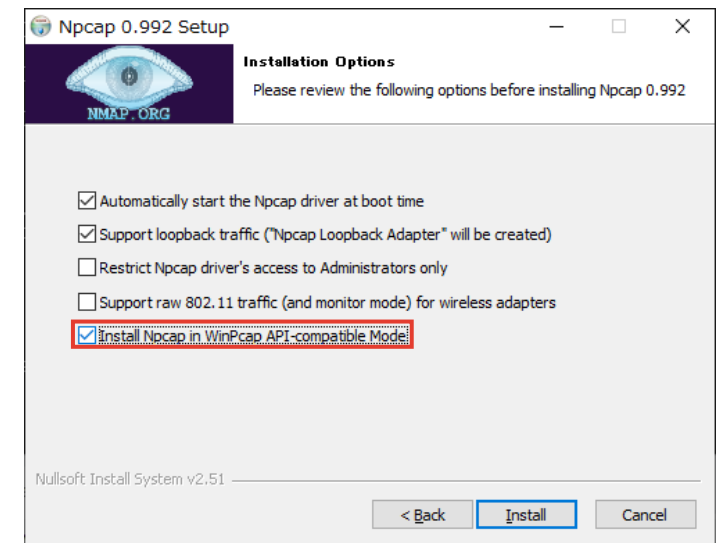
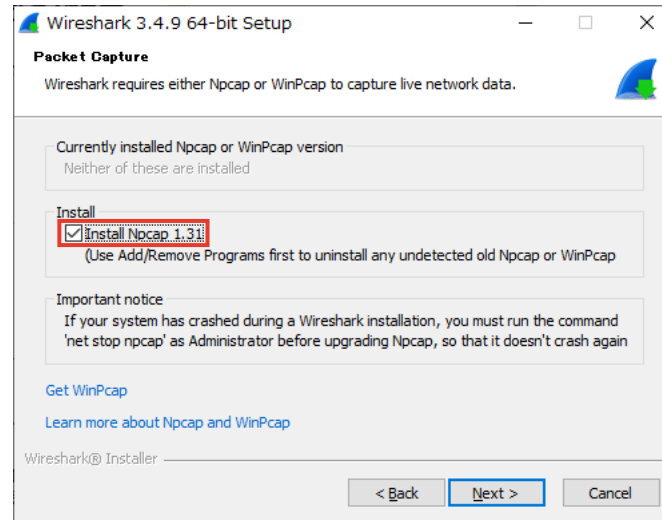
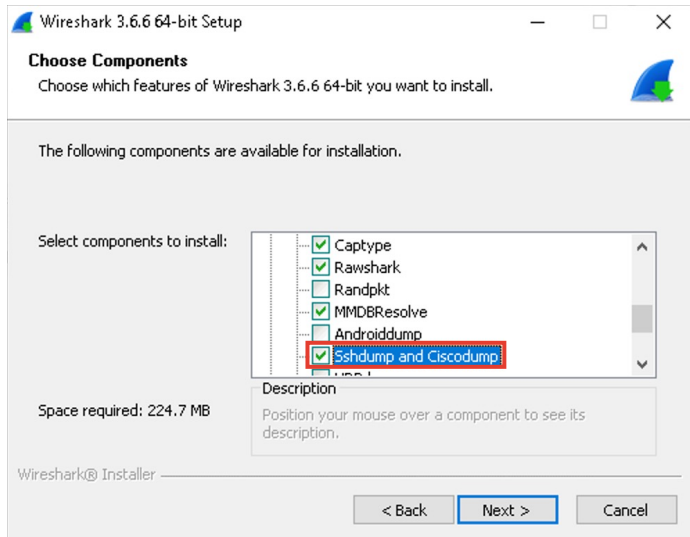
Rerun

Capture interface	Captured frames	
TA1:eth1	<div style="width: 100%; height: 15px; background-color: #ccc;"></div> 100/100	Download

Live packet capture実行手順

1. 事前設定

- Wiresharkインストール時に”Sshdump and Ciscodump”を選択し、インストール
- Wiresharkをインストールする端末に [WinPcap](#)またはNpcap を”Install Npcap in WinPcap API-compatible Mode”でインストール



Live packet capture実行手順

1. 事前設定 – 続き

- WiresharkからTest Agentに接続が必要なため、コントロールセンターからLive packet captureを有効にしたいTest Agentに対してWireshark端末のSSH公開鍵を追加

```
$ ssh-keygen -t rsa -f key_file -b 4096 -C "test-agent-key"
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key_file.Your public key has been saved in key_file.pub.
The key fingerprint is:
SHA256:w6gKxgzBDOKFDBmKp9+3Y3a437J0IUiM3/oNQac/a2s test-agent-key
The key's randomart image is:
+---[RSA 4096]-----+
|Bo..                |
|Xo.o                |
|++o o . .          |
| + o + =            |
|o  o * S            |
|+. . o + o         |
|.+. + o.+          |
|.. . o==E+         |
| . o+OB+.          |
+-----[SHA256]-----+

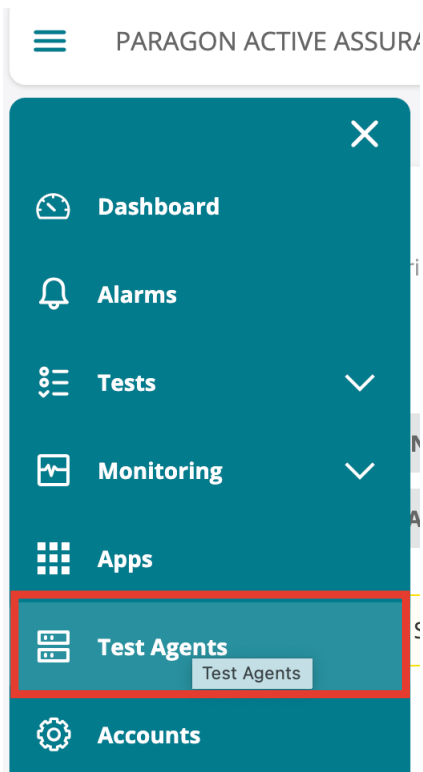
$ ls key_file*
key_file key_file.pub
```

SSH key生成例
"cat key_file.pub"で公開鍵
ファイルの中身を表示し
コピーしておく

Live packet capture実行手順

1. 事前設定 - 続き

- WiresharkからTest Agentに接続が必要なため、コントロールセンターからLive packet captureを有効にしたいTest Agentに対してWireshark端末のSSH公開鍵を追加 - 続き



Test Agents

Download

INTERFACE INFO LICENSE INFO

Live packet captureを有効にするTest Agentを選択

Test Agents

Tags

Name	Description	Management IPv4	Management IPv6	Public IP	Applications	Share
<input type="checkbox"/> TA1		172.27.112.6	-	172.27.112.6		
<input type="checkbox"/> TA2		172.27.114.53	-	172.27.114.53		
<input type="checkbox"/> TA3		172.17.0.2	-	172.27.112.142		

Page 1 of 1 |< < > >|

● Ready ● In use ● Offline Test Agent Appliance Test Agent Application

Live packet capture実行手順

1. 事前設定 - 続き

- WiresharkからTest Agentに接続が必要なため、コントロールセンターからLive packet captureを有効にしたいTest Agentに対してWireshark端末のSSH公開鍵を追加 - 続き

TA1
[Click here to add a description]

Load avg: 0 (1 minute)

INTERFACES INTERFACES (METADATA) APPLICATIONS NTP STREAMS LICENSE UTILS GPS LOCATION

PLATFORM INFORMATION **SSH ACCESS**

Info: When adding SSH keys to a Test Agent, an SSH server will be started. Please be aware of the security implications of this.

+ [trash] [refresh]

ADD SSH KEY ×

Name:

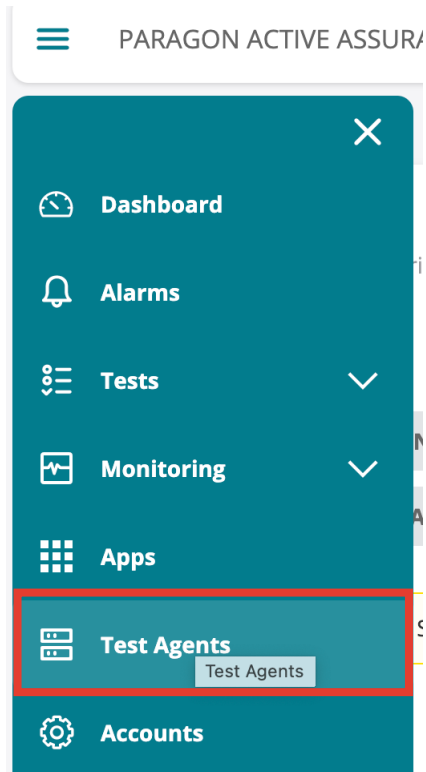
Key:

OK Cancel

任意の名前を記入し、コピーしておいた公開鍵のデータを貼り付けて"OK"

Live packet capture実行手順

2. メニューから“Test Agents”へ移動しTest Agentを選択後、Live remote packet captureを有効にする



Test Agents

Download

INTERFACE INFO LICENSE INFO

Live packet captureを有効にするTest Agentを選択

Test Agents

Clear Tags All Online Offline In use Free

Name	Description	Management IPv4	Management IPv6	Public IP	Applications	Share
<input type="checkbox"/> TA1		172.27.112.6	-	172.27.112.6		
<input type="checkbox"/> TA2		172.27.114.53	-	172.27.114.53		
<input type="checkbox"/> TA3		172.17.0.2	-	172.27.112.142		

Page 1 of 1

Ready In use Offline Test Agent Appliance Test Agent Application

Live packet capture実行手順

2. メニューから“Test Agents”へ移動しTest Agentを選択後、Live remote packet captureを有効にする – 続き

TA1
[Click here to add a description]

Uptime: 4 days 02:31:53
Version: 3.3.1.23
Memory: 26.61% CPU: 2.06%
Load avg: 0 (1 minute) 0.03 (5 minutes) 0 (15 minutes)
Login towards: 172.27.113.169:6000

INTERFACES INTERFACES (METADATA) **APPLICATIONS** NTP STREAMS LICENSE UTILS GPS LOCATION
PLATFORM INFORMATION SSH ACCESS

To understand what an Application is, please refer to the [support documentation](#).

Name	Speedtest	Proxy for management traffic	Capture interface	Connect to interface
eth0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
eth1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Unsaved changes **Save**

wiresharkに接続される
インターフェースを選択
(デフォルトはマネジメントインターフェース)

CONFIGURE SETTINGS FOR LIVE REMOTE PACKET CAPTURE

Capture interface:

Connect to interface
(optional):

Tip: The remote live capture process will be stopped automatically after 24 hours, if not manually stopped before.

In wireshark when you add the remote interfaces use the IP address of the selected connect interface as host and 2002 for port. The default connect interface is the management interface.

Note, that you can select only a single remote interface in wireshark at a time for capturing.

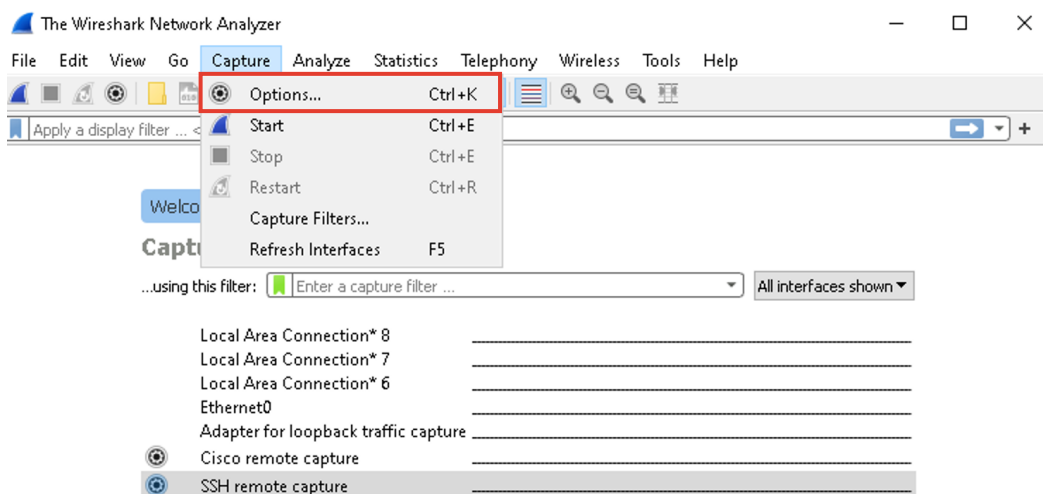
Ok Cancel

キャプチャを行いたいインターフェースを選択

最後に“Save”をクリック

Live packet capture実行手順

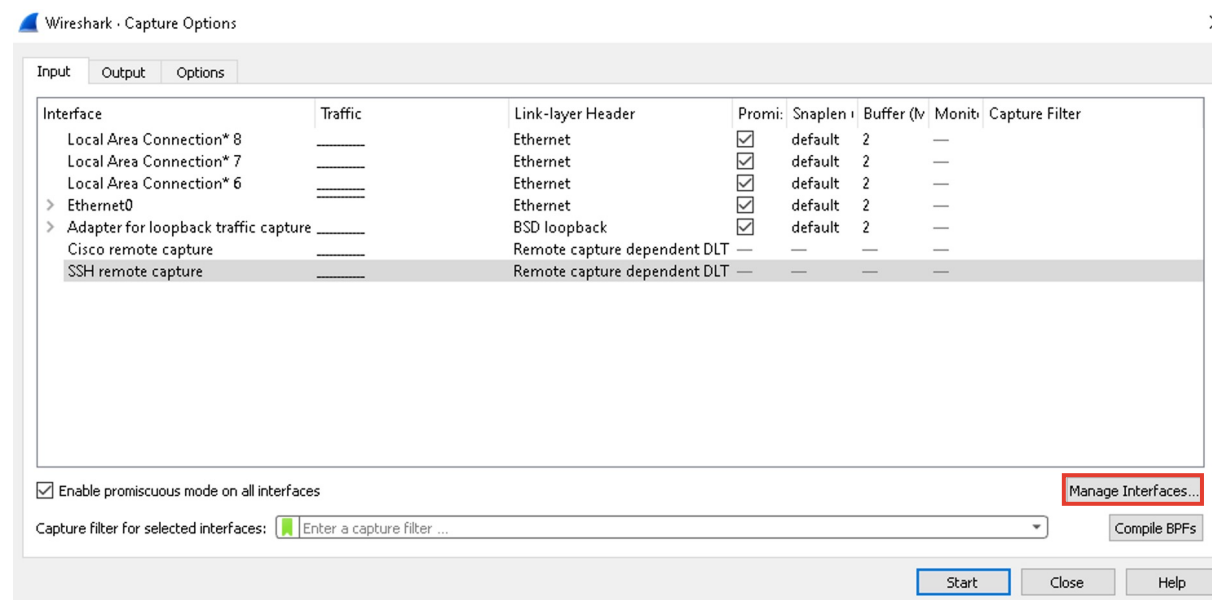
3. WiresharkにRemote Interfaceを設定



Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.6.7 (v3.6.7-0-g4a304d7ec222). You receive automatic updates.



Live packet capture実行手順

3. WiresharkにRemote Interfaceを設定 - 続き

The image shows two overlapping dialog boxes from Wireshark. The larger one is titled "Manage Interfaces" and has three tabs: "Local Interfaces", "Pipes", and "Remote Interfaces". The "Remote Interfaces" tab is active, showing a table with columns "Show" and "Host / Device URL". Below the table are a "+" button (highlighted with a red box), a "-" button, and a "Remote Settings" button. At the bottom of the dialog are "OK", "Cancel", and "Help" buttons, with the "OK" button highlighted by a red box. A green callout box points to the "OK" button with the text: "Remote Interfaceを追加後、'OK'をクリック".

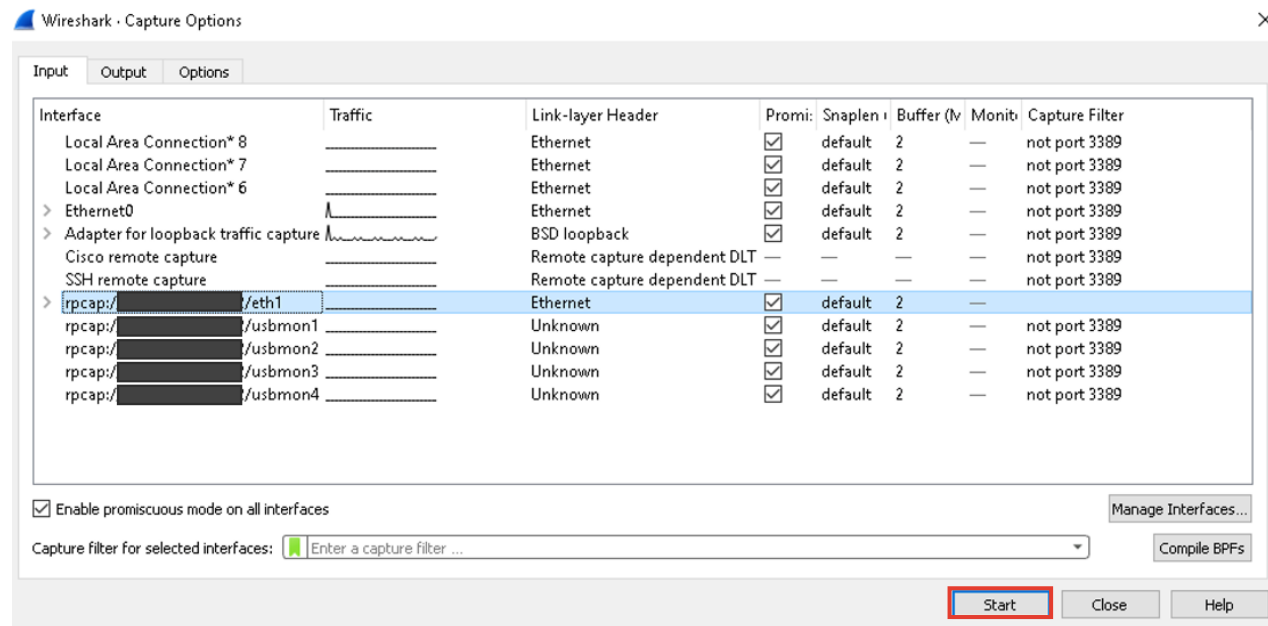
The smaller dialog box is titled "Remote Interface" and contains the following fields:

- Host: [dropdown menu]
- Port: 2002
- Authentication section with two radio buttons: "Null authentication" (selected) and "Password authentication".
- Username: [text input]
- Password: [text input]
- Buttons: "OK" (highlighted with a red box) and "Cancel".

A green callout box points to the Host field with the text: "'Connect to Interface'に設定したインターフェースのIPアドレスをHostに記入".

Live packet capture実行手順

4. WiresharkでLive packet captureを開始
※開始から24時間後に自動的に停止してしまうので注意





THANK YOU

JUNIPER
NETWORKS

Driven by
Experience™