# Remote Worker Agent Training

Diagnose endpoint, Wi-Fi, gateway, ISP, internet, VPN, and application issues from the user perspective.

# Training Goals

Enable operations and support teams to quickly determine whether a remote user issue is caused by the endpoint, Wi-Fi, home network/gateway, ISP, internet path, VPN, or application/service reachability.

In this training we will focus on the NetBeez Remote Worker Agent (RWA).

# Troubleshooting Process

**1.**

**Acquire the right information**

Find the remote worker endpoint, verify the agent status, and review the timeline around the reported issue.

**2.**

**Isolate the failure domain**

Separate endpoint, Wi-Fi, gateway, ISP, internet, VPN, DNS, and application problems using NetBeez data.

**3.**

**Take the correct next step**

Route tickets to the right team with clear evidence, timestamps, and test results or close the ticket.

# Agenda

1. Remote troubleshooting model
2. NetBeez Remote Worker Agent
3. Troubleshooting playbooks

01

# Remote troubleshooting model

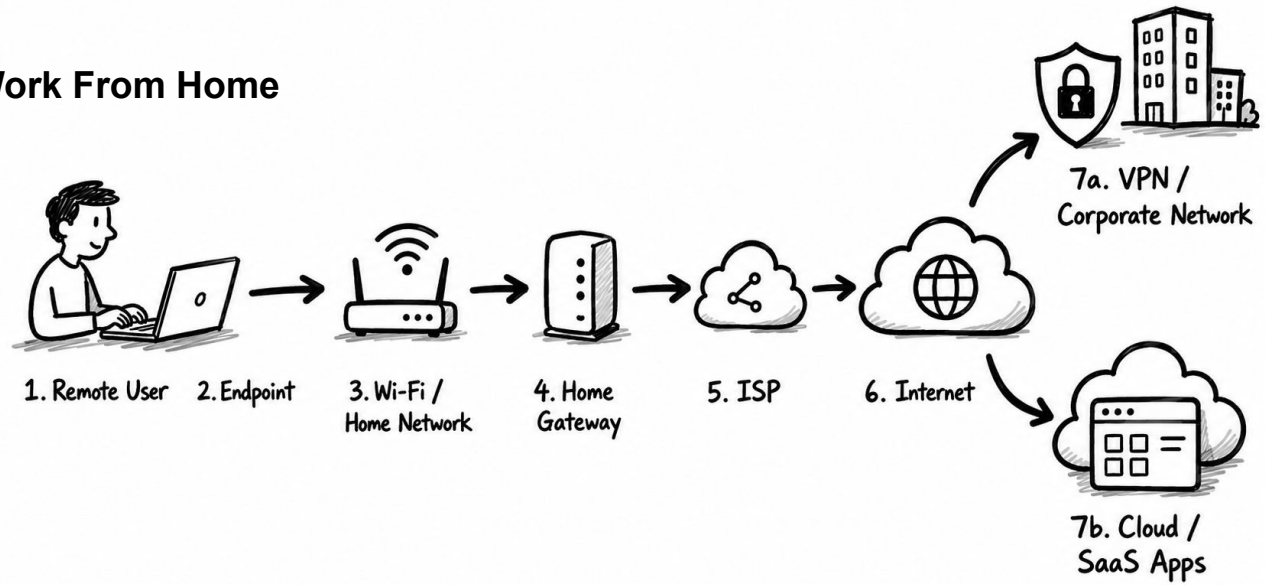
# Why troubleshooting user tickets is hard

**Complaints are often vague:**

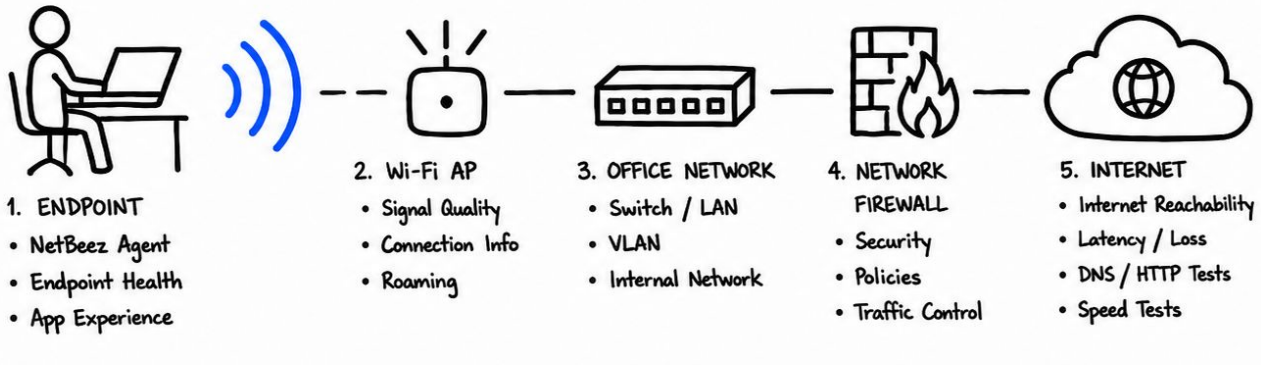
*"internet is slow"* *"VPN is bad"*

*"Teams is choppy"* *"everything is down"*

**Work From Home**




**In Office**



# Remote user failure domains

## Endpoint

CPU/memory, OS, agent status, local device conditions

## Wi-Fi

Signal, SSID/BSSID, local packet loss, roaming, interference

## Gateway

Gateway reachability, local LAN latency/loss, DNS

## ISP / Internet

Public targets, speed, loss beyond gateway, path changes

## VPN

Tunnel state, internal DNS, internal app reachability, VPN gateway

## Application

DNS/HTTP response, SaaS availability, one app vs many apps

# 02

# NetBeez Remote Worker Agent

# What the RWA measures

## Endpoint and agent status

Online/offline state, last check-in, test execution health.

## Wi-Fi and local network

Wi-Fi connection, gateway latency and packet loss.

## Internet experience

Public reachability, path analysis, network speed and DNS.

## VPN and internal reachability

Tests conditioned on VPN state, internal DNS and app targets.

## Application experience

Web and DNS performance to SaaS and internal apps.

# Troubleshooting Method

**Search for the user or device and open the relevant agent view.**

**Use the reported timestamp to identify incidents and alerts.**

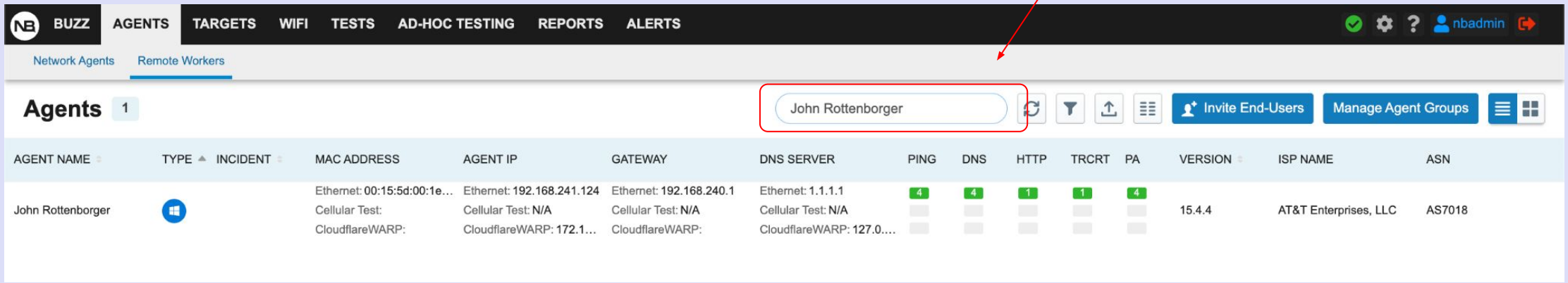
**Verify network path: Wi-Fi, Gateway, ISP, VPN, Path Analysis, App.**

**Update the ticket with findings.**

# Step 1

# Find the RWA

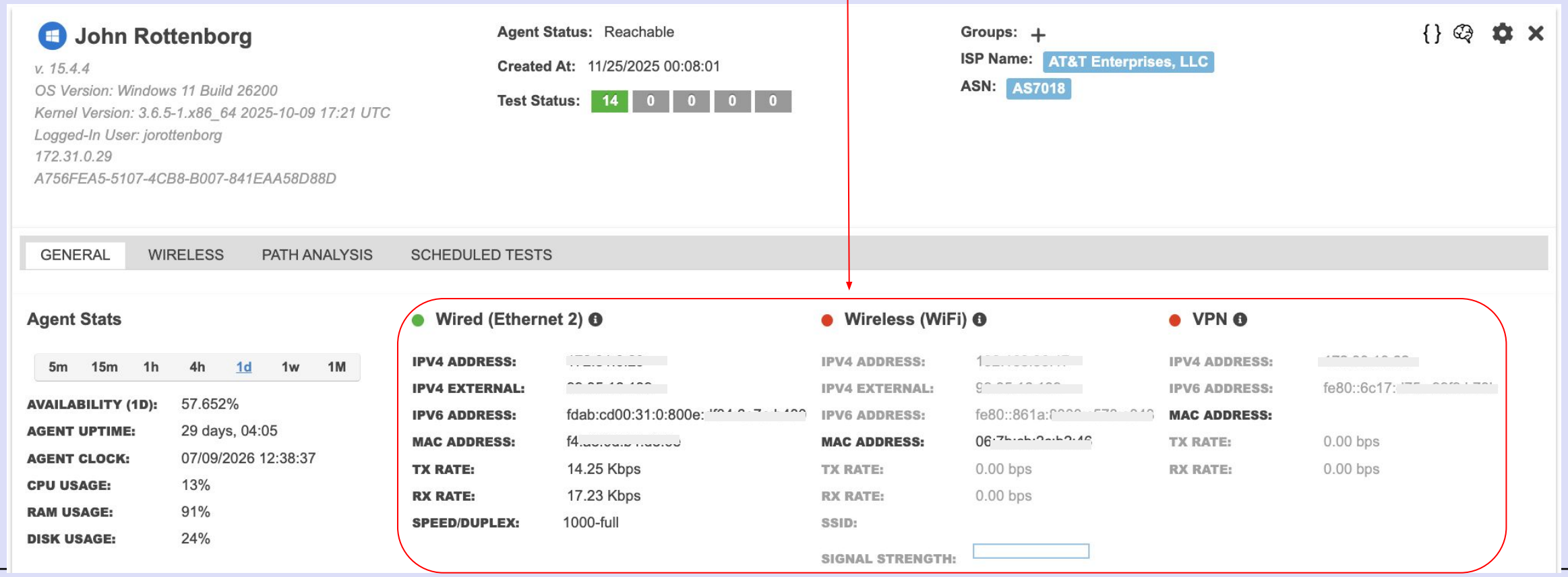
Go to the Agents tab, click on Remote Workers, then use the search box to identify the remote user. You can use the machine name or the logged-in user



# Step 2

# Identify what interfaces are connected

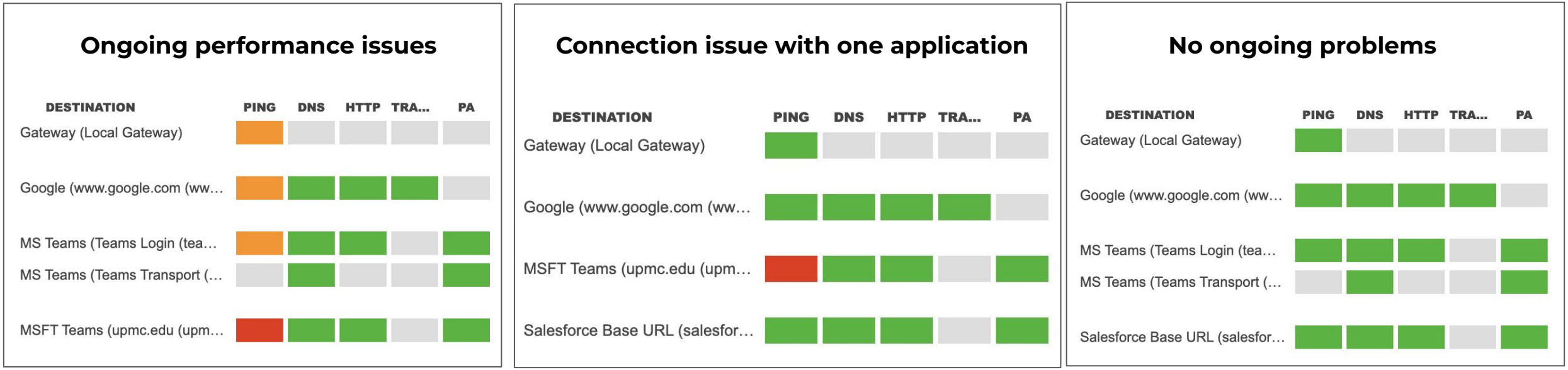
Check what interfaces are connected in the top section of the agent detailed view.



# Step 3

# Check the agent test status

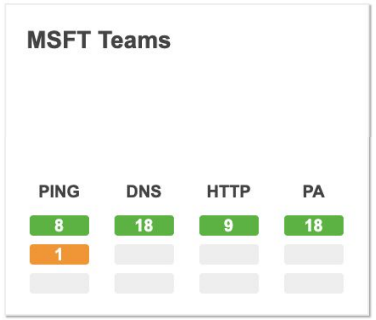
Next, verify the status of the running tests in the main agent details section. Are you troubleshooting an issue in the present or in the past?



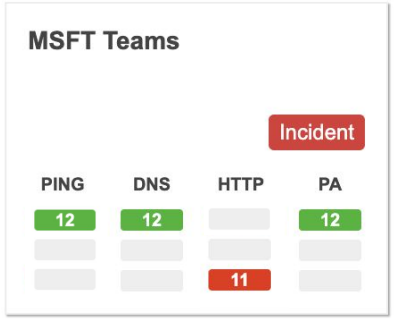
# 03

# Troubleshooting playbooks

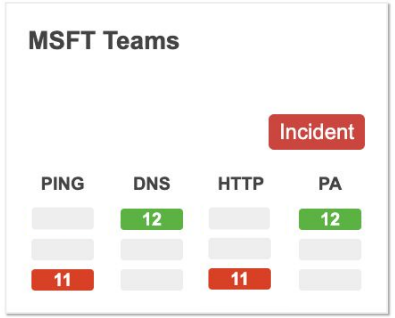
# Playbook: Application or SaaS issue




**Some users** Not an application issues, local agent/network issue

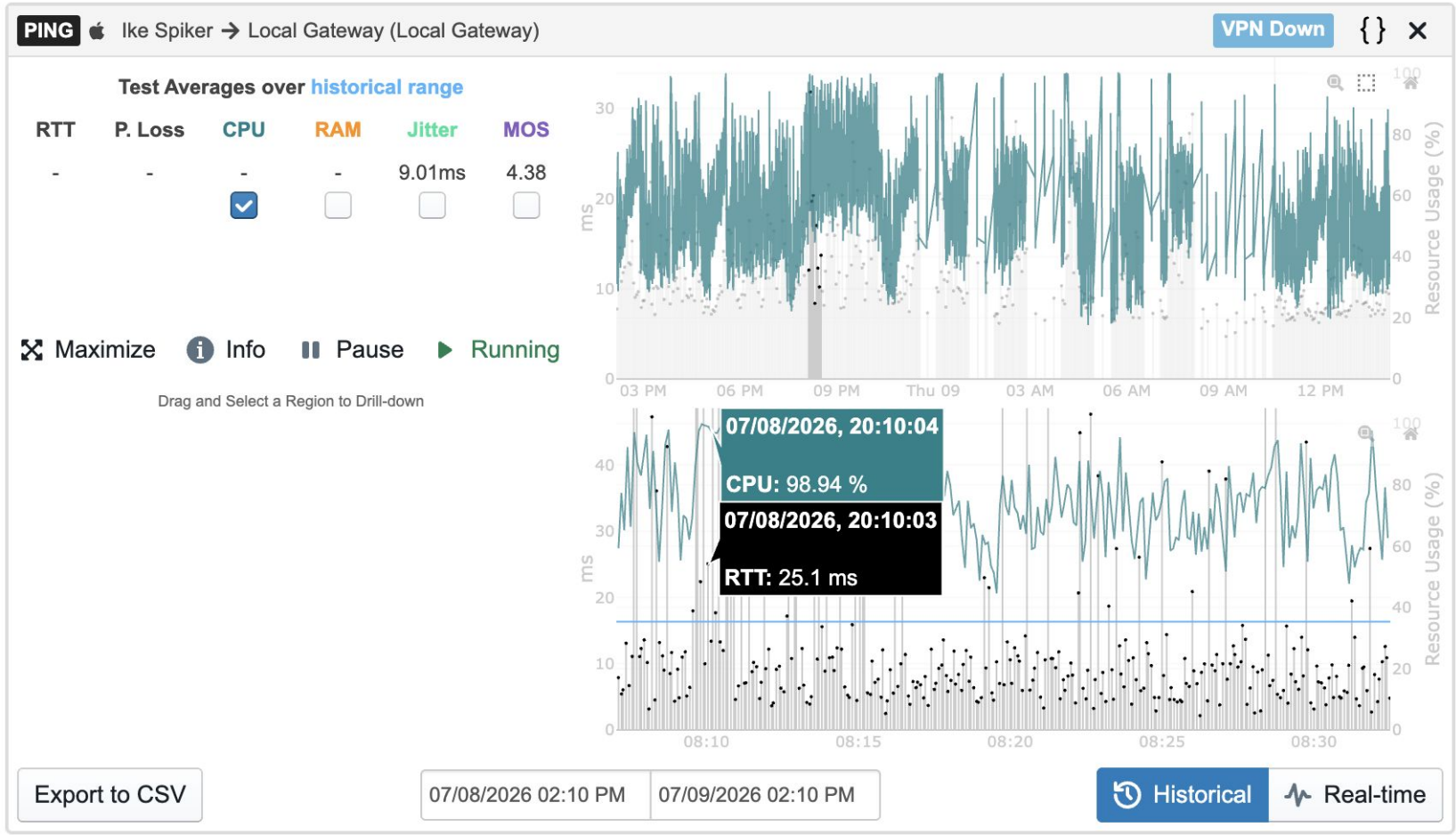



**All HTTP** Problems within the application server or firewall




**All PING and HTTP** Application network reachability

# Playbook: Endpoint is slow




## What to check

Go to the General section, click on a test and check the CPU and RAM utilization by clicking on the radio buttons.

## Evidence pattern

Prolonged CPU and RAM spikes: **CPU util > 80%** and **RAM > 90%.** Check also if disk is full.

## Support action

Check task manager if the issue is still present and verify process with high CPU utilization

# Playbook: Wi-Fi Metrics


## What to check

Go to the Wireless section and check SSID/BSSID changes, signal strength and link quality

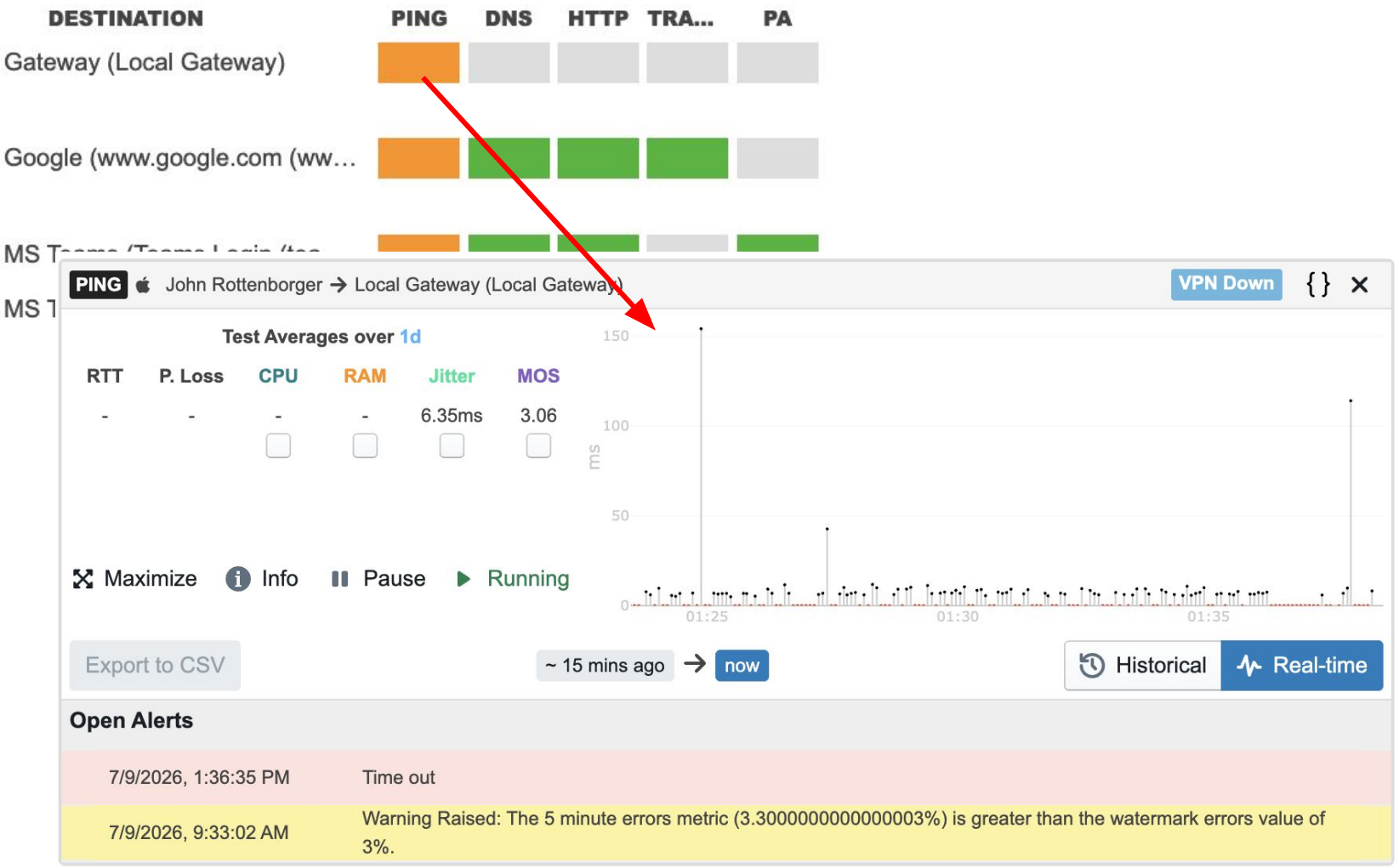
## Evidence pattern

Frequent connect/disconnect events, **signal strength < -70 dBm** or **link quality < 80%**

## Support action

Ask user to move closer to AP, reboot Wi-Fi router if home user, escalate to Wi-Fi team if a office user.

# Playbook: Gateway or local network issue




### What to check

Go to the General section and open the Gateway target and verify RTT and packet loss (red dots).

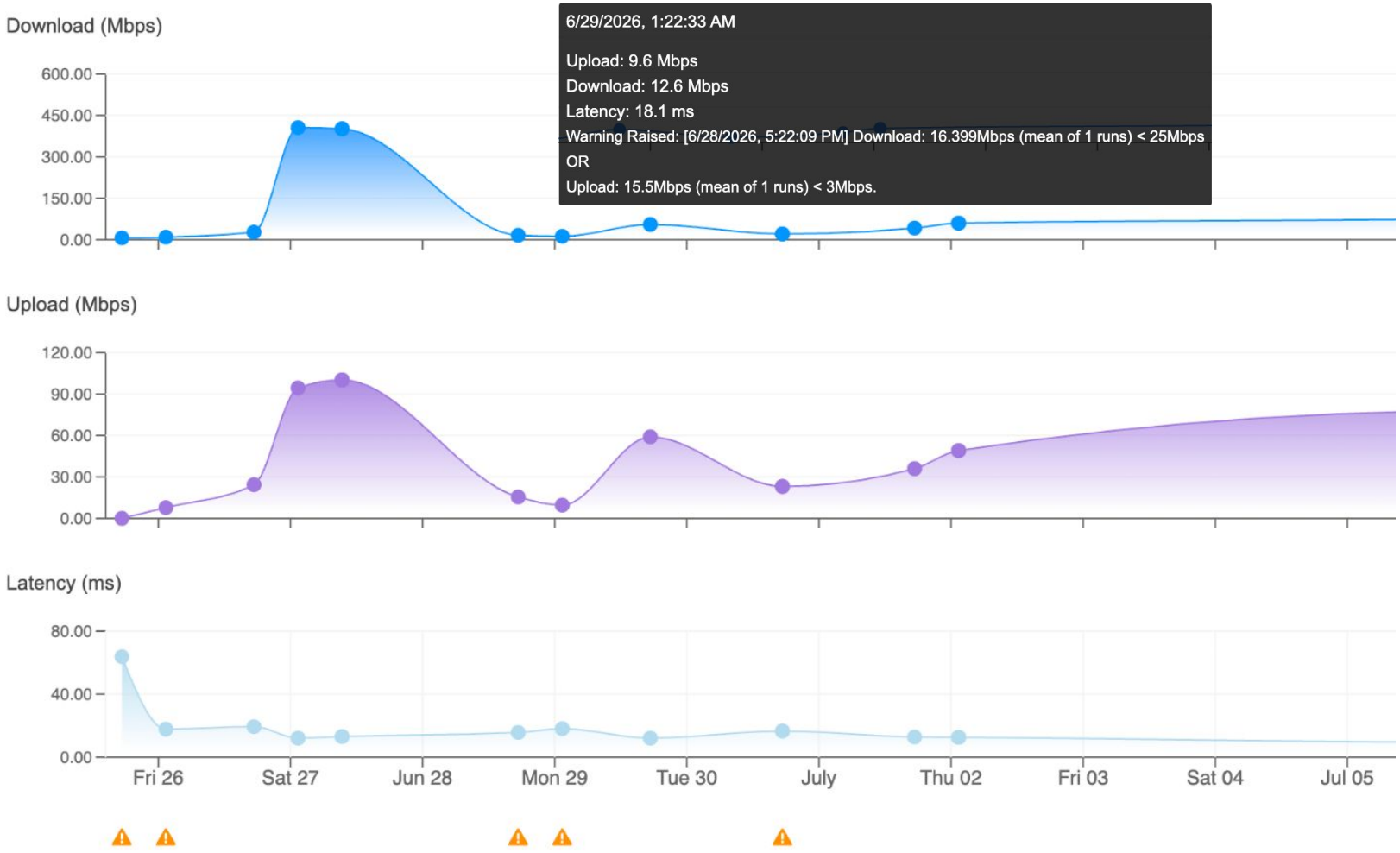
### Evidence pattern

Alerts on high packet loss, high latency, or visually unstable test.

### Support action

Ask the wireless user to connect to Ethernet if possible, move closer to the AP, or reboot the home gateway is connected via Ethernet or docking station if a home user

# Playbook: ISP issue




### What to check

Check network speed test data within the agent details view. If no periodic network speed tests are configured, run Ad-Hoc network speed.

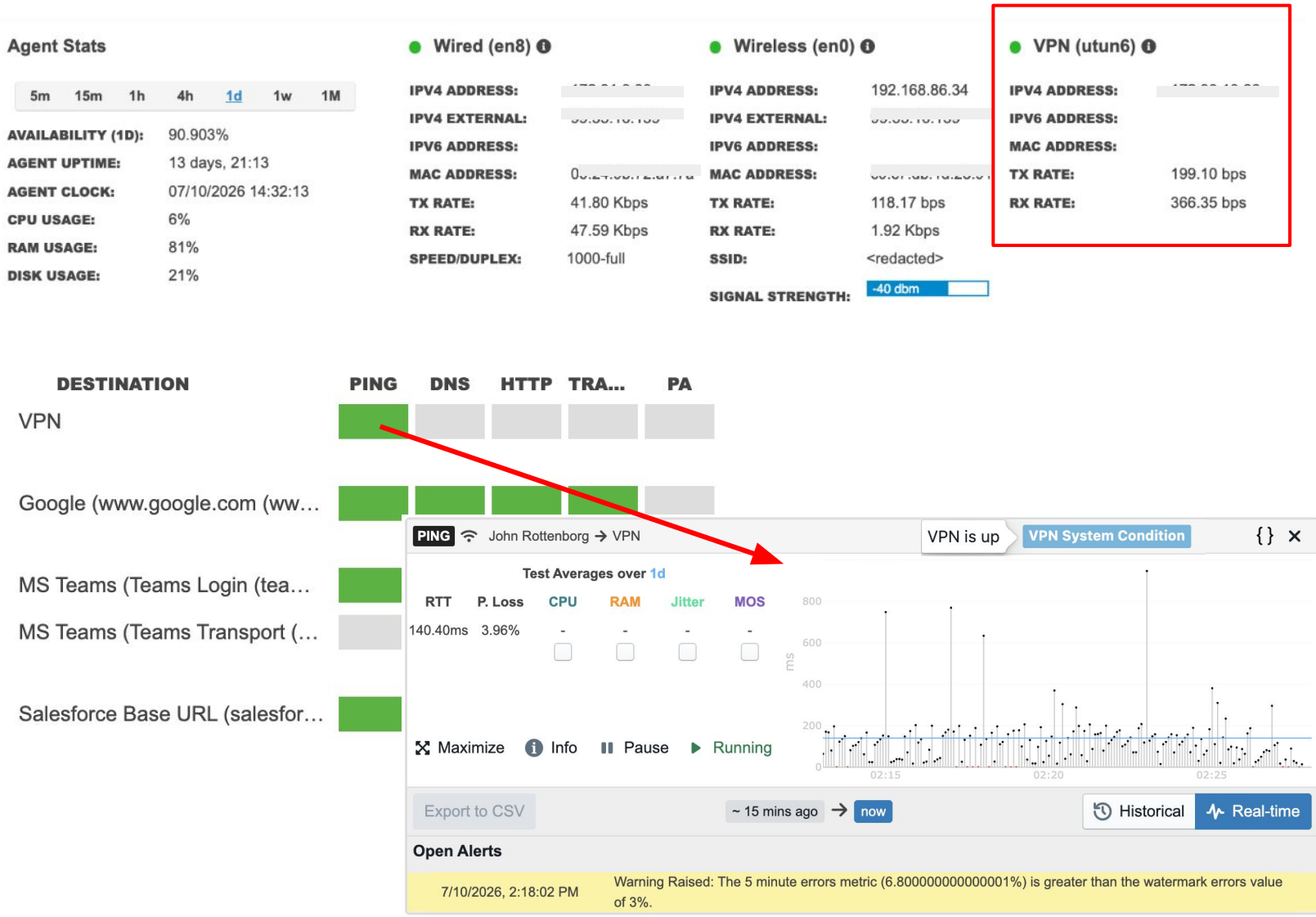
### Evidence pattern

Download speed is less than 25 Mbps or Upload speed is less than 3 Mbps.

### Support action

Home users should either open a ticket with the ISP or use a different connection method if working elsewhere (coffee shop WiFi, mobile device, ...)

# Playbook: VPN




## What to check

Make sure the VPN interface is up and that the VPN target is running.

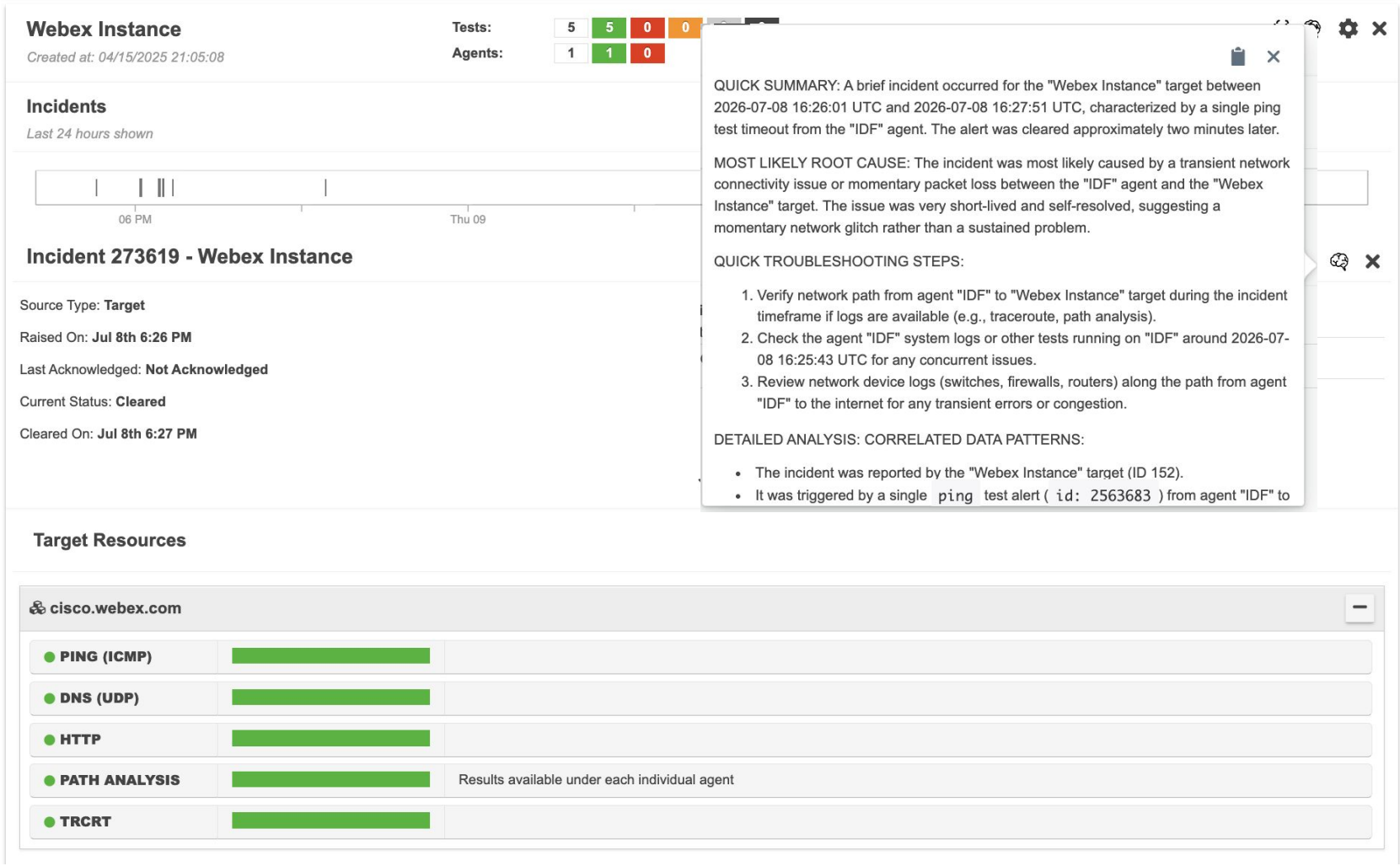
## Evidence pattern

Find any performance issues on the ping tests across the VPN, including alerting for RTT or packet loss.

## Support action

If available, run an iperf test across the tunnel to check how much traffic can pass. You will need a NetBeez agent or iperf server on the far end side of the tunnel (enterprise side).

# Incidents AI for root cause analysis




## What to check

It's possible to query the AI function when an incident is triggered (either Agent or Target)

## Evidence pattern

Reviews events and data included in the root cause analysis.

## Support action

Verify accuracy of AI analysis by reviewing the supporting facts and data

https://netbeez.net