DEEP PACKET INSPECTION

R&S®PACE 2 plug-in information

NAT/MOBILE TETHERING TRANSPARENCY PLUG-IN

Detecting network address translation (NAT) and the devices behind a NATing device is difficult. Routers, wireless access points or smartphones with enabled tethering option map multiple devices to one publicly exposed IP address. Private and public network areas are separated with NAT. Since multiple network devices with their distinct private IP addresses masquerade as a single public IP address, network resources can be misused. Additionally, NATing can pose a threat to enterprise environments as unauthorized devices such as personal devices are outside the scope of traditional IT security and are able to create an insecure access point to the internal enterprise network.

NAT DETECTION SOLUTION

The NAT/mobile tethering transparency extension is a plug-in of the deep packet inspection (DPI) software R&S®PACE 2 that identifies devices in NAT scenarios using dedicated methods of IP traffic analytics. The plug-in is based on application and operating system (OS) characteristics as well as property fragments of physical devices from the network traffic. The NAT detection plug-in combines multiple heuristic methods to ensure high accuracy and reliability. The heuristic methods include:

- Google QUIC user agent
- TTL
- TCP timestamp

Combining multiple heuristics prevents false positives and enables the identification of various operating systems behind a NATing device with network traffic using the transmission control protocol (TCP) or user datagram protocol (UDP). Through continuous performance and reliability testing, Rohde&Schwarz offers the highest traffic detection rate and the best traffic classification accuracy available on the market. In case of any OS update, there is a dedicated team of software engineers maintaining the advanced extension on a regular basis to ensure a high level of accuracy in detecting NAT and tethering scenarios.

Operating system coverage:

- Windows
- Linux/Android
- macOS
- iOS
- Solaris

KEY FUNCTIONALITIES

- Real-time IP traffic analytics
- Passive detection of NAT & tethering scenarios
- Low memory footprint
- Reliable main device detection & calculation of distinct device count behind a hotspot

NAT DATA MODEL

In addition to detecting NAT and tethering scenarios, presenting the obtained information is of vital importance. The NAT/mobile tethering transparency plug-in provides a central hub to manage gathered information in a well-defined data structure, thereby helping to reduce implementation complexity in the integrated software solution.
The new data model is highly flexible and makes it easy to implement additional methods or integrate new results. The data model ensures optimal data efficiency by allowing all plug-in components to share global information. Global information includes, for example, information about the NAT detection state, main devices, the number of detected devices and device groups, as well as information about currently used heuristic methods. The plug-in immediately reports obtained data and transparently stores its decisions in an easily accessible conclusion tree.

SOLUTION INTEGRATION

The advanced NAT/mobile tethering transparency software component is integrated as a plug-in. It requires the DPI software R&S®PACE 2 as a processing foundation. Both R&S®PACE 2 and the plug-in itself are easy to integrate and simple to manage with no vendor lock-in and open APIs.

ENTERPRISE IT SECURITY

The NAT/mobile tethering transparency plug-in by Rohde&Schwarz is an essential software tool for enterprises that reliably want to detect unauthorized NATing devices. The following use case demonstrates how the plug-in can reveal NATing devices in a specific network.

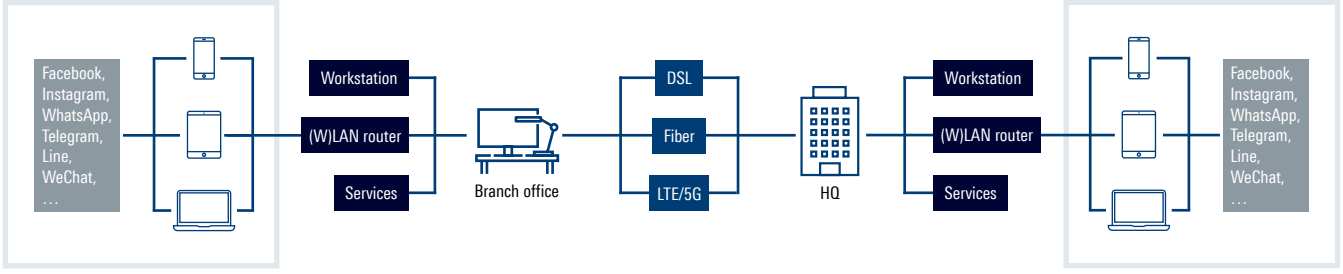
Visibility and control of network data

NATing devices, such as routers or wireless access points, provide a convenient way to share a single IP address between several clients, but they can pose serious security risks. For example, a NAT router connected to an Ethernet port in an enterprise office environment allows several possibly untrusted clients to access network resources. This can create an insecure access point to the internal network. Malicious entities outside the physical protection perimeter could access the internal network and launch an attack. With the Rohde&Schwarz NAT/mobile tethering transparency plug-in, IT administrators can prevent cyberattacks by proactively detecting unauthorized NATing devices within their network.

Key benefits

- Policy-based control of NATing devices
- Detect and prevent security breaches
- Protect sensitive data
- Improve bring-your-own-device management

NAT DEVICES IN AN ENTERPRISE NETWORK



The plug-in in combination with the leading DPI engine R&S®PACE 2 detects NATing and devices behind the corresponding routing device, and the applications used.

ipoque GmbH
A Rohde&Schwarz Company
Augustusplatz 9, 04109 Leipzig
Info: +49 (0)341 59403 0
Email: info.ipoque@rohde-schwarz.com
www.ipoque.com

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

PD 3608.4316.32 | Version 01.00 | March 2020
NAT/Mobile Tethering Transparency Plug-in | Enterprise
Data without tolerance limits is not binding | Subject to change

3608431632

3608.4316.32 01.00 PDP 1 en