Traceroute to Private Applications and Internet Destinations Through Secure Access

Contents

Introduction

This document describes the use of traceroute feature to private applications and internet destinations through Secure Access.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Access
- Cisco Secure Client
- Internet Protocol Security (IPSEC) Tunnels
- Remote Access Virtual Private Network (RAVPN)
- Zero Trust Network Access (ZTNA)
- Internet Control Message Protocol (ICMP)
- User Datagram Protocol (UDP)
- Transmission Control Protocol (TCP)
- Secure Web Gateway (SWG)
- Cloud Native Headend (CNHE)
- Carrier-Grade Network Address Translation (CGNAT)

Components Used

The information in this document is based on these software and hardware versions:

- Windows Version 10
- Secure Client Version 5.1.4.74

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Cisco Secure Client now enables users to trace traffic from endpoint to private applications or internet destination by using the ipv4 traceroute command.

The feature currently available on RAVPN and IPSEC Tunnels. This phase does not include ZTNA client based or clientless access.

Traceroute Through Secure Access

Supported Scenarios

- ICMP, UDP, TCP based traceroute from RAVPN client to Internet
- ICMP, UDP, TCP based traceroute from RAVPN client to Private App behind IPSEC Tunnel
- ICMP, UDP, TCP based traceroute from a client in Branch to Internet
- ICMP, UDP, TCP based traceroute from a client in Branch to Private App IPSEC Tunnel

Full Secure Access Deployments

Required Policy Changes

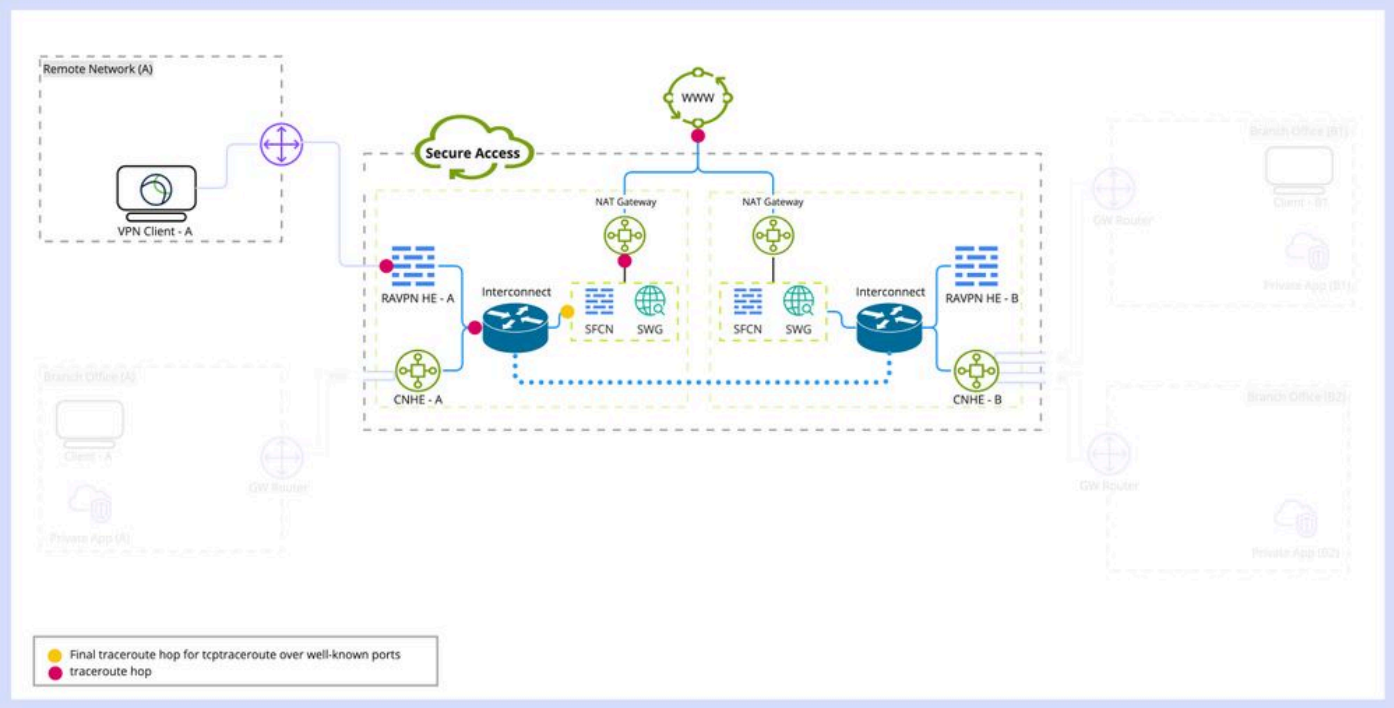
Ensure Protocols and Policies are set properly in Access Policies

- ICMP allowed for Windows tests

- UDP for Linux and MacOS tests

Expected Hop Details

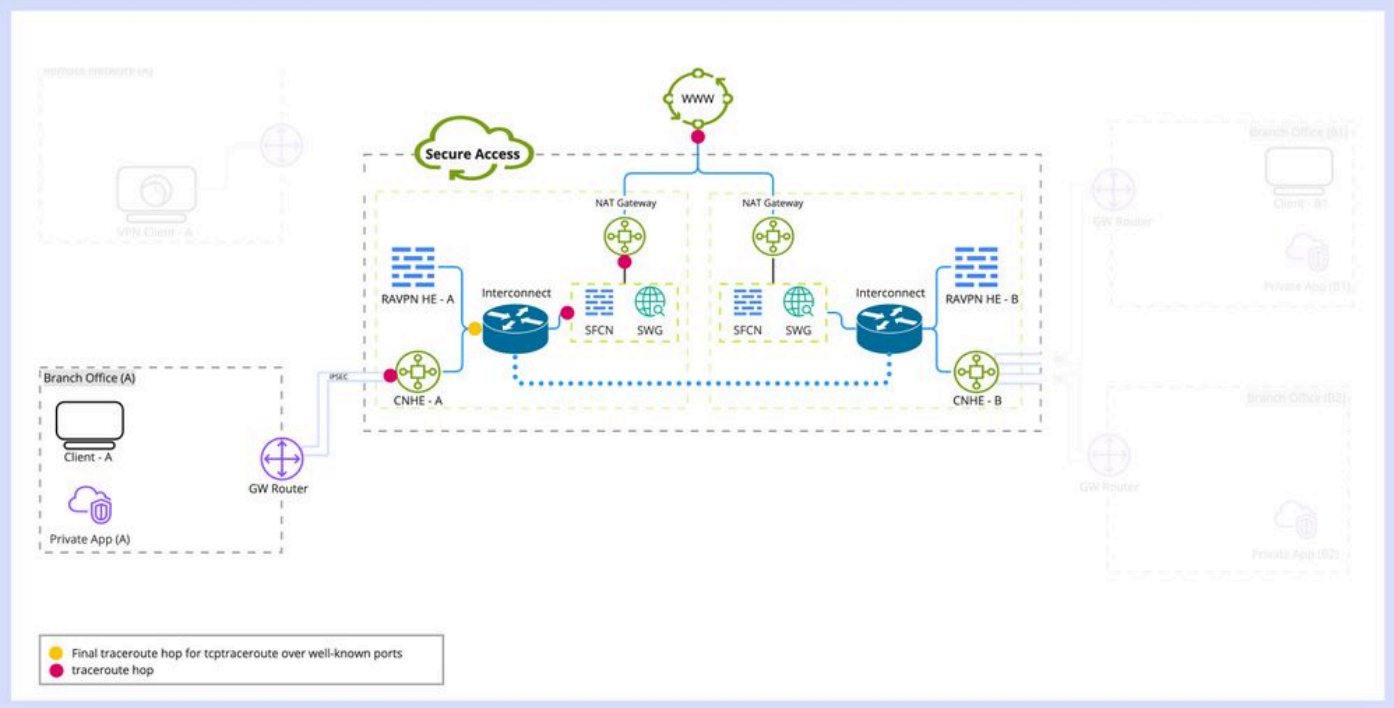
RAVPN Client to Internet



RAVPN Client to Internet

1. **First Hop:** RAVPN headend IP to which client is connected.
2. **Second Hop:** Interconnect service IP (pre-security).
3. **Third Hop:**
    1. **ICMP/UDP based traceroute:** Private IP of Network Address Translation (NAT) Gateway.
    2. **TCP based traceroute:**
        1. **For TCP ports 80, 443, 853, 8080, 8443:** Cisco Secure Firewall Cloud Native (SFCN) proxy IP because SFCN is act as final destinations based on decryption settings in access policies.
        2. When Decryption is not enabled in SFCN, SWG proxy IP is represented as third hop for TCP ports (80, 443).
        3. **TCP traceroute on remaining ports:** Private IP of Network Address Translation (NAT) Gateway.
4. **Fourth Hop and onwards:** Internet nodes involved in the path to the destination, when the traffic is not proxied by Secure Access.

Branch Behind IPSEC Tunnel to Internet

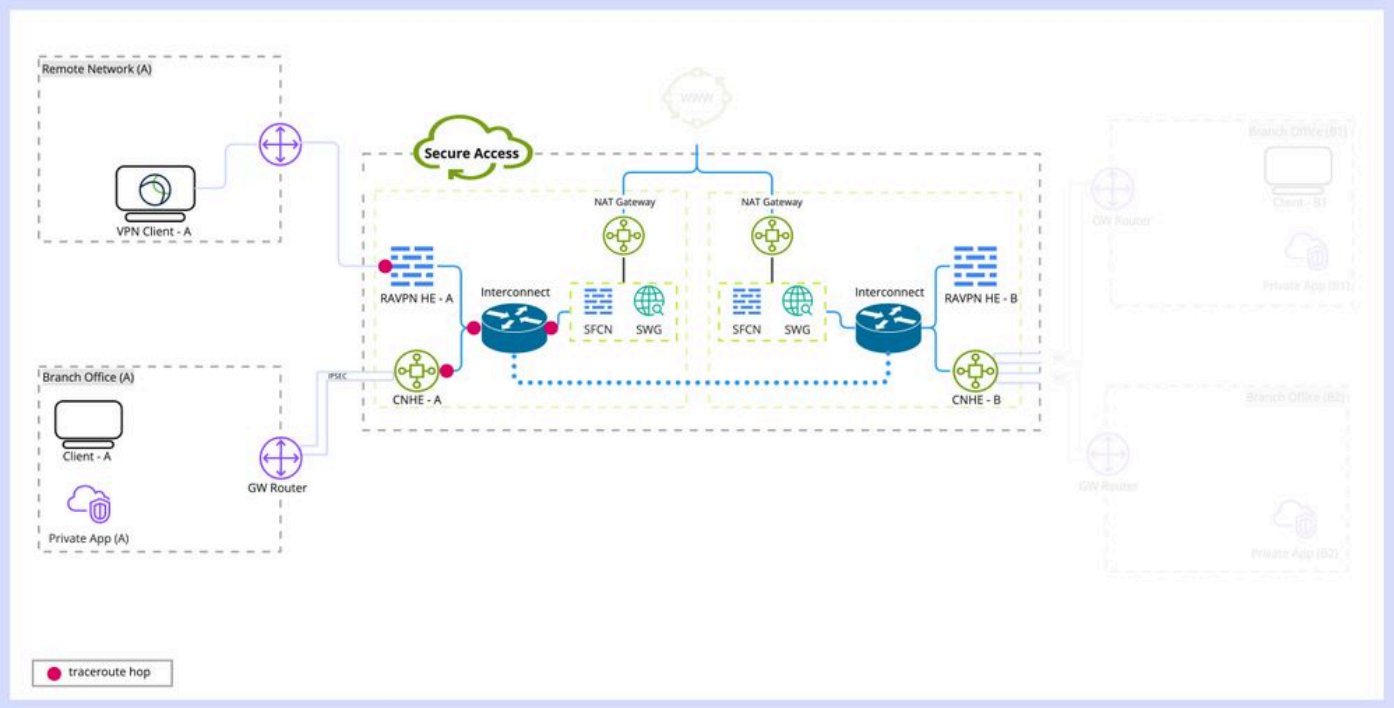


Branch to Internet

1. **First Hop:** CNHE headend IP to which client is connected.
2. **Second Hop:** Interconnect service IP (pre-security)
3. **Third Hop:**
    1. **ICMP/UDP based traceroute**: Private IP of Network Address Translation (NAT) Gateway.
    2. **TCP based traceroute**:
        1. For TCP ports 80, 443, 853, 8080, 8443: Cisco Secure Firewall Cloud Native (SFCN) proxy IP because SFCN is act as final destinations based on decryption settings in access policies.
        2. When Decryption is not enabled in SFCN, SWG proxy IP is represented as third hop for TCP ports (80, 443).
        3. TCP traceroute on remaining ports: Private IP of Network Address Translation (NAT) Gateway.
4. **Fourth Hop and onwards:** Internet nodes involved in the path to the destination, when the traffic is not proxied by Secure Access.

RAVPN Client to Private Application

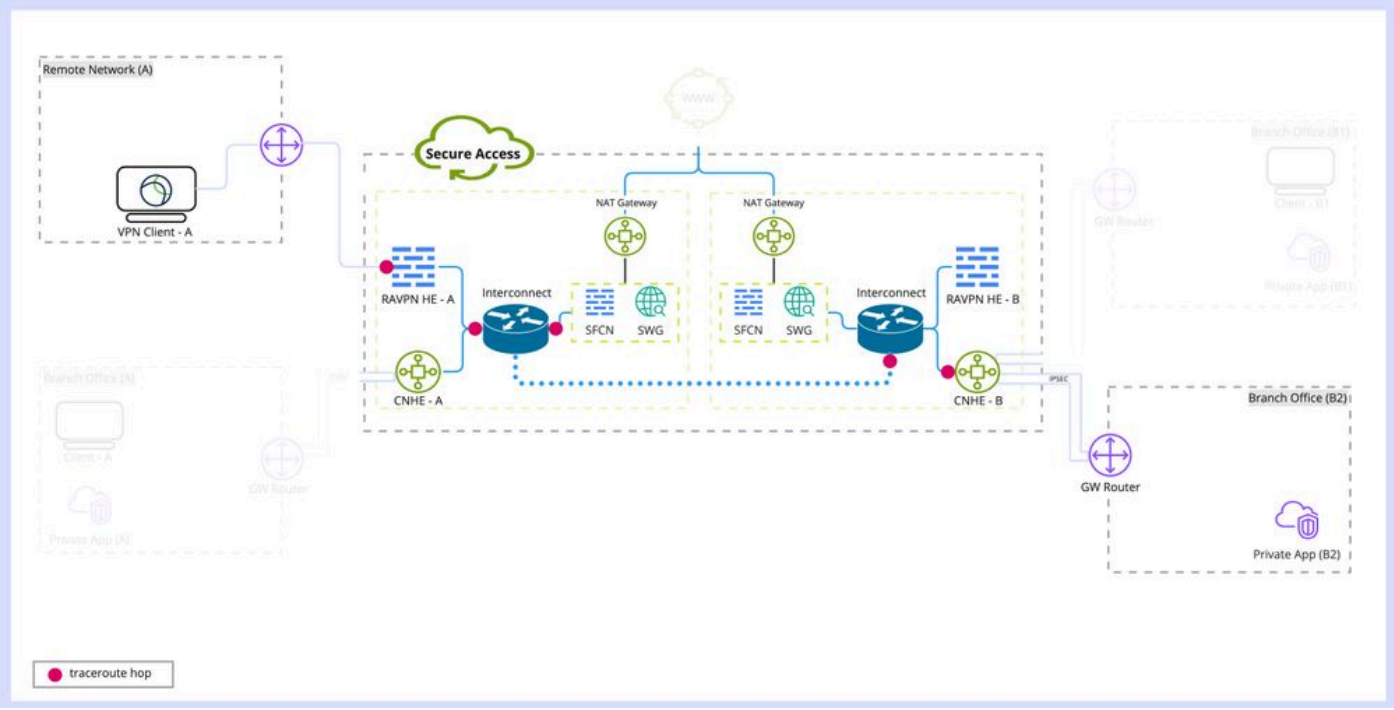
RAVPN Client and Private Application are connected to the same VEDC (Virtual Edge Data Center).



RAVPN Client to Same VEDC

1. **First hop:** RAVPN headend IP to which client is connected.
2. **Second Hop:** Interconnect service IP (pre-security)
3. **Third Hop:** Interconnect service IP (post-security)
4. **Fourth Hop:** CNHE service IP behind which Private App is hosted.
5. **Fifth hop onwards:** belongs to environment involved in reaching private application.

RAVPN Client and Private application are connected to the different VEDC (Virtual Edge Data Center).



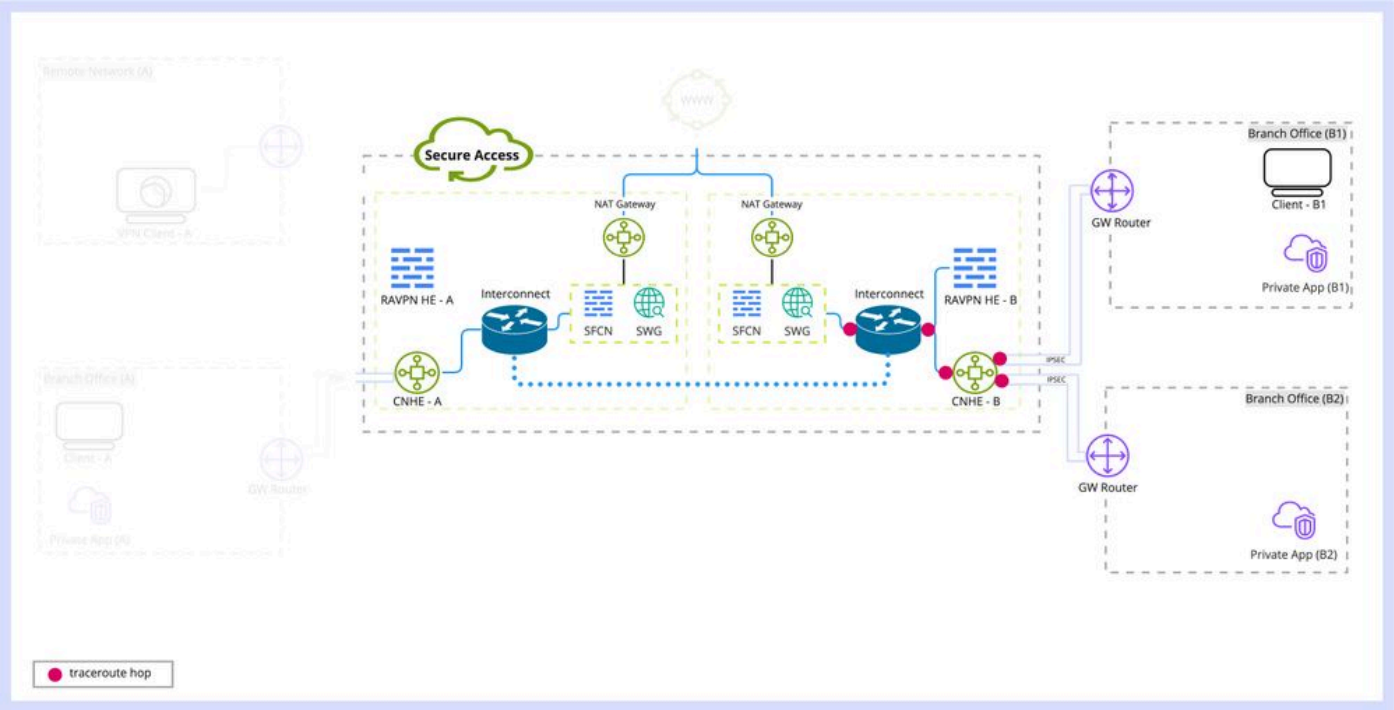
RAVPN Client to Different VEDC

1. **First hop:** RAVPN headend IP to which client is connected.

2. **Second Hop:** Interconnect service IP (pre-security) of VEDC to which client is connected.
3. **Third Hop:** Interconnect service IP of one of the VEDC's where the security enforcement is being done.
4. **Forth Hop:** Interconnect service IP (post-security) of VEDC to which Private Application is connected.
5. **Fifth Hop:** CNHE service IP behind which Private App is hosted.
6. **Sixth hop onwards:** belongs to environment involved in reaching private application.

Branch Behind IPSEC Tunnel to Private Application

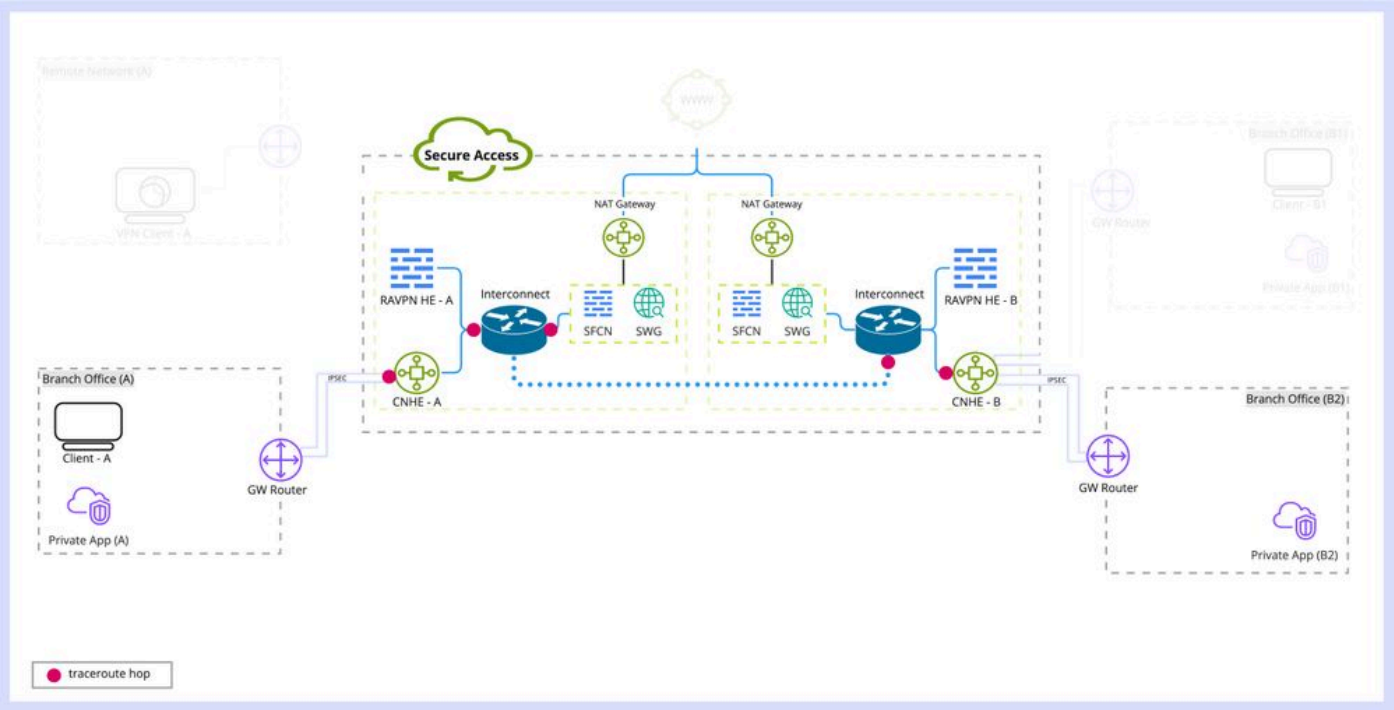
CNHE Branch Client and Private application are connected to the same VEDC (Virtual Edge Data Center).



Branch Client to Branch private app in same VEDC

1. **First hop:** CNHE headend IP to which client is connected.
2. **Second Hop:** Interconnect service IP (pre-security)
3. **Third Hop:** Interconnect service IP (post-security)
4. **Fourth Hop:** CNHE service IP behind which Private App is hosted.
5. **Fifth hop onwards:** belongs to environment involved in reaching private application.

CNHE Branch Client and Private application are connected to the different VEDC (Virtual Edge Data Center).



Branch to Private App in different VEDC

1. **First Hop:** CNHE headend IP to which client is connected.
2. **Second Hop:** Interconnect service IP (pre-security) of VEDC to which client is connected.
3. **Third Hop:** Interconnect service IP of one of the VEDC's where the security enforcement is being done.
4. **Forth Hop:** Interconnect service IP (post-security) of VEDC to which Private Application is connected.
5. **Fifth Hop:** CNHE service IP behind which Private App is hosted.
6. **Sixth Hop onwards:** belongs to environment involved in reaching private application.

Reporting and Activity Search

- Packet Flow related First Hop (RAVPN, CNHE) not shown in activity search
- Firewall activity search have entries related to traceroute provided logging is enabled

Frequently Asked Questions (FAQ)

Q. Why traceroute is not displaying the last hop (private application), while ping to private application is working properly?

A. Some implementations of traceroute (ex: ubuntu) tries with UDP packets, which can not be allowed in some networks. It is recommended to try with ICMP by providing ICMP option explicitly.

Q. Why traceroute with UDP shows different routes comparted to ICMP?

A. traceroute shows different hops as each protocol can go through different routes

Q. Why traceroute shows incomplete list of hops for tcptraceroute over standard web-ports?

A. SFCN and/or SWG terminates TCP sessions over stand web-ports, hence tcptraceroute over standard web-ports is always incomplete.

Q. Why traceroute shows repeating hops beyond Secure Access?

A.

1. ECMP load-balanced paths of unequal hop length.

2. Involvement of NAT and/or Tunnels, where multiple hops handling TTL value of a packet, but using same source IP while generating ICMP Error packets.

Q. How to do we know which protocol is being used for traceroute (ICMP, UDP)

A.

1. Windows always uses ICMP for traceroute.

2. Linux and MacOS uses UDP for traceroute by default. (-I option can be used to switch to ICMP traceroute)

Q. Why we are not seeing class-E (240.0.0.0/4) in tracert, CGNAT range (100.64.0.0/10) in TCP traceroute output in Windows, but we are seeing it in Linux and MacOS?

A. In lab testing we observed the following:

1. Windows tracert drops ICMP responses received from class-E subnet (240.0.0.0/4).

2. Windows tracertcp drop ICMP responses received from CGNAT subnet (100.64.0.0/10).

Related Information

- **Secure Access Help Center (User Guide)**
- **Technical Support & Documentation - Cisco Systems**