Secure Access Destination Addresses for Split Routing Configuration

Contents

Issue

When deploying Cisco Secure Access (CSA) with Cisco Secure Client (CSC) on Windows endpoints in a Hub-Spoke network architecture, organizations most likely need to configure split routing to allow Spoke site traffic to connect directly to CSA over the local Spoke internet circuit instead of hairpinning through the Hub. This configuration requires knowledge of all Cisco destination addresses used when establishing the CSA tunnel so that routing exceptions (breakout/split routing) can be defined on network devices such as Fortigate firewalls.

The specific requirement is to identify all destination information (IP addresses or URLs) for CSA endpoints used by CSC when establishing TLS/DTLS tunnels, enabling proper configuration of routing policies that bypass the Hub-Spoke VPN tunnel for CSA traffic.

Environment

- Cisco Secure Access (CSA) deployment
- Cisco Secure Client (CSC) on Windows endpoints
- Hub-Spoke network topology with Fortigate firewalls
- TLS/DTLS tunnel connectivity to CSA

Resolution

To configure split routing for Cisco Secure Access connections, the destination information described in the next sections must be configured on the Fortigate device to allow direct connectivity to CSA endpoints.

CSA Destination Domain and Ports

Primary Domain

```
*.vpn.sse.cisco.com
```

Required Ports and Protocols

- **TCP/UDP 443:** Used for TLS/DTLS tunnel establishment
- **UDP 500/4500:** Used for IPsec tunnel establishment
- **TCP 80:** Used for VPN certificate revocation checks

Fortigate Configuration Approach

Configure routing policies on the Fortigate device to direct traffic destined for the CSA domain (*.vpn.sse.cisco.com) and the specified ports through the local Spoke internet circuit rather than through the Hub-Spoke VPN tunnel. This enables the traffic flow outlined in the next code snippets.

Desired Traffic Flow

```
Spoke Site → CSA Tunnel Connection → CSA-mediated Internet Communication
```

Instead of Traffic Flow through Hub Site

```
Spoke Site → Hub Site → CSA Tunnel Connection → CSA-mediated Internet Communication
```

Important Considerations

The CSA connection destinations are dynamically determined during runtime, which means that specific IP addresses cannot be predetermined for static routing configuration. The domain-based approach using *.vpn.sse.cisco.com provides the most reliable method for configuring split routing policies.

Reference the official Cisco Secure Access documentation for the most current destination and port requirements, as these are most likely updated with new software releases.

Cause

In Hub-Spoke network topologies, all internet-bound traffic from Spoke sites typically routes through the Hub site by default. When implementing CSA with CSC, this default routing behavior causes CSA tunnel traffic to hairpin through the Hub site before reaching the CSA endpoints, potentially introducing latency and bandwidth inefficiencies. The dynamic nature of CSA endpoint selection requires domain-based routing policies rather than static IP-based rules to ensure proper split routing functionality.

Related Content

- Cisco Secure Access Documentation - Connection Requirements
- Cisco Secure Access Documentation - Network Configuration
- Cisco Technical Support & Downloads