Secure Access VPN - unable to access Jabber

Contents

Issue

Secure Client users were unable to access internal and private applications such as Jabber and Epic over the Secure Access VPN tunnel when using a private access policy. Users experienced connectivity failures when attempting to reach these critical business applications through the VPN connection. During troubleshooting, unidirectional traffic was observed for Epic resources where ping and TCP SYN traffic was seen egressing the Secure Access VPN tunnel, but return traffic validation issues were identified on the Palo Alto firewall. Additionally, Jabber reachability issues were documented where CUCM FQDNs were resolving via internal DNS while traffic steering was configured for IP-based routing, causing a mismatch in the traffic flow.

Environment

- Cisco Secure Access with VPN tunnel configuration
- Secure Client for VPN connectivity
- Private access policy implementation
- Cisco Unified Communications Manager (CUCM) for Jabber services
- Epic application resources
- Palo Alto firewall for network security
- Internal DNS resolution for CUCM FQDNs

Resolution

The resolution involved multiple configuration changes and troubleshooting steps to restore connectivity to internal applications through the Secure Access VPN tunnel:

Subnet Configuration and Tunnel Modifications

Step 1: Add Additional Subnets to VPN Tunnel

Additional subnets were added to the VPN tunnel configuration for the affected resources. After implementing this change, the resources that were previously inaccessible began loading successfully.

CUCM IP Address Steering Configuration

Step 2: Configure CUCM IP Steering

To resolve the Jabber connectivity issue where CUCM FQDNs were resolving via internal DNS while traffic steering was IP-based, the CUCM IP addresses were steered into Secure Client. This configuration change aligned the DNS resolution with the traffic steering mechanism.

Step 3: Create Access Policy Rule

An access policy rule was created to permit reachability to the CUCM IP addresses. This rule restored proper connectivity to the CUCM infrastructure, enabling Jabber functionality over the VPN tunnel.

Static Routing Configuration

Step 4: Configure Static Routing for CUCM Subnet

Ensure that CUCM IP addresses and the overall CUCM subnet are included in the static routing table for the network tunnel. This configuration ensures proper routing of traffic between the Secure Client user pool and the CUCM infrastructure.

Return Traffic Validation

Step 5: Validate Packet Flow and Return Traffic

Validate the packet flow configuration to confirm that return traffic can reach the Secure Client user pool. This includes reviewing the Palo Alto firewall configuration to ensure proper return-path validation for all internal resources, particularly for Epic connectivity where unidirectional traffic was observed.

Cause

The connectivity issues were caused by multiple configuration gaps in the Secure Access VPN implementation:

- Missing subnet configurations in the VPN tunnel prevented proper routing to internal application resources

- Mismatch between DNS resolution (FQDN-based) and traffic steering configuration (IP-based) for CUCM services caused Jabber connectivity failures
- Incomplete access policy rules that did not permit traffic to CUCM IP addresses
- Missing static routing entries for CUCM subnets in the network tunnel configuration
- Return traffic path validation issues on the Palo Alto firewall affecting bidirectional communication

Related Content

- Cisco Technical Support & Downloads