Secure Access ZTA Enrollment Communication Errors Due to DNS Configuration Issues

Issue

Users are unable to enroll in the Cisco Secure Access Zero Trust Access (ZTA) system, which was previously functioning correctly and could see Server Connectivity Error. The enrollment process fails with communication errors to enrollment servers, preventing users from completing the ZTA enrollment procedure. This issue affects a large number of users and represents a significant disruption to secure access services.

Environment

- Technology: Solution Support (SSPT - contract required)
- Sub-technology: Cisco Secure Access
- Product Family: SECACCS
- VPN configuration with Default DNS mode enabled
- DNS server configuration pointing to non-responsive server

Resolution

The ZTA enrollment communication errors are resolved by fixing the DNS server configuration issue. The problem occurs when the VPN is configured with Default DNS mode pointing to a DNS server that is not responding to DNS lookups.

Step 1: Identify DNS Configuration Issue

Verify that the VPN Default DNS mode is enabled and check if the configured DNS server is responding to DNS queries. The enrollment servers cannot be reached when DNS resolution fails.

Step 2: Fix DNS Server Problem

Correct the DNS server configuration to ensure it responds properly to DNS lookups. This could involve:

- Updating the DNS server IP address to a working server
- Restarting the DNS service on the configured server
- Verifying network connectivity to the DNS server
- Testing DNS resolution functionality

Step 3: Verify ZTA Enrollment Functionality

After fixing the DNS server problem, test the ZTA enrollment process to confirm that users can successfully enroll. The enrollment functions as expected once DNS resolution is working properly.

Additional Troubleshooting Considerations

If DNS configuration is correct but enrollment issues persist, verify that network devices such as firewalls are not restricting access from user PCs to the Secure Access ZTA enrollment servers. Ensure that all required destinations for ZTNA enrollment are accessible through the network infrastructure.

Cause

The root cause of the ZTA enrollment communication errors is a DNS configuration issue where the VPN Default DNS mode was enabled and pointing to a DNS server that was not responding to DNS lookups. When DNS resolution fails, the ZTA enrollment process cannot communicate with the enrollment servers, preventing users from completing the enrollment procedure successfully.

Related Content

- Cisco Technical Support & Downloads