

Umbrella Proxy Blocks Ninja Application Connectivity

Contents

Issue

Users are unable to run a remote system using a downloaded setup file when connected through Cisco Umbrella. The application fails to function under Umbrella protection, specifically affecting access to the remote system. The same remote system works perfectly without any issues when the Cisco Umbrella proxy is disabled.

Troubleshooting attempts included testing with a separate policy where the system security and destination were set to ANY, but the issue persisted. Additionally, routing the traffic through Zero Trust Access (ZTA) was attempted, yet the problem remained unchanged. Traffic was allowed through Secure Access on TCP/443, but connections were still blocked on the endpoint.

Environment

- Cisco Umbrella with proxy functionality enabled
- Zero Trust Access (ZTA) configuration
- Secure Access policies configured for TCP/443 traffic

Resolution

The resolution involves excluding specific NinjaOne-related domains from the Umbrella proxy to allow direct connectivity for the remote access application.

Step 1: Identify Affected Domains

Analysis of the packet capture and HAR files reveals that these NinjaOne-related domains are being affected by the Umbrella proxy:

- ninjarmm.net
- ninjarmm.com
- app.ninjarmm.com
- ninjaone.com
- agent-app.ninjaone.com

Step 2: Configure Domain Exemptions

Exclude the identified domains from both Secure Web Gateway (SWG) Internet Security policies and ZTA internet traffic steering. This configuration change allows these domains to bypass the Umbrella proxy and establish direct connections.



Note: A Do Not Decrypt (DND) list configuration has been observed as ineffective for resolving this issue. Traffic steering and exemption is the recommended approach.

Step 3: Apply Configuration Changes

Implement the domain exemptions in the Umbrella configuration to exclude the NinjaOne-related traffic from proxy processing. This allows the remote access application to establish direct connections to the required services.

Step 4: Validate Resolution

Test the remote access application functionality after applying the exemptions to ensure proper connectivity is restored while maintaining Umbrella protection for other traffic.

Cause

The issue occurs because NinjaOne remote access applications reject proxied connections when traffic is routed through the Cisco Umbrella proxy. The application requires direct connectivity to specific NinjaOne domains to function properly. When these connections are proxied through Umbrella, the remote access service cannot establish the necessary communication channels, resulting in application failure even when security policies are configured to allow the traffic.

Related Content

- [Cisco Technical Support & Downloads](#)