Troubleshoot MS Teams Issues with Zero Trust Access Profile Configuration

Contents

Issue

Users enrolled in a Zero Trust Access (ZTA) profile for Secure internet access experienced Microsoft Teams call connectivity issues. When users are added to the ZTA profile, Microsoft Teams calls disconnect unexpectedly and other users cannot initiate calls to the affected user. However, calls connect successfully when the affected user initiates the call from their side.

The issue is isolated to users onboarded to the ZTA profile, indicating ZTA policies or routing configurations are impacting Teams call connectivity. Traffic logs show Microsoft Teams traffic from processes like ms-teams.exe to IP addresses in required ranges (such as 52.115.245.30:3480, which is part of 52.112.0.0/14) is being intercepted by the ZTA client rather than going directly to the internet.

Environment

- Cisco Secure Access with Zero Trust Access (ZTA) profile configuration
- ZTA profile configured with "Use ZTA to secure all Internet destinations"
- Microsoft Teams application
- Cisco Secure Client with ZTA capabilities
- Users enrolled in ZTA profile for Secure internet access

Resolution

To resolve the issue, add Microsoft Teams traffic exceptions to the ZTA profile configuration to allow Teams traffic to bypass the ZTA tunnel and connect directly to the internet:

1. Navigate to **Dashboard > End User Connectivity > Zero Trust Access** and locate the affected ZTA

profile.

2. Select the ZTA profile and choose **Edit > Secure Internet Access**.

3. Add these IP ranges and FQDNs to the exceptions list per Microsoft's Official Documentation:

IP Ranges:

```
52.112.0.0/14
52.122.0.0/15
2603:1063::/38
2603:1027::/48
2603:1037::/48
2603:1047::/48
2603:1057::/48
2620:1ec:6::/48
2620:1ec:40::/42
```

FQDNs:

```
*.lync.com
*.teams.cloud.microsoft
*.teams.microsoft.com
teams.cloud.microsoft
teams.microsoft.com
*.keydelivery.mediaservices.windows.net
*.streaming.mediaservices.windows.net
aka.ms
```

4. Add a description for the exceptions, such as:

```
MS Teams exception as per: https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-addre
```

5. Save the configuration changes. Wait few minutes for changes to be applied.

6. Ensure the ZTA client policy is re-synced on affected endpoints. This can require restarting the Zero Trust Access Agent Service or restarting the client device.

7. Test Teams call functionality to confirm that:

- Incoming calls to affected users now connect successfully
- Teams calls no longer disconnect unexpectedly

- Teams traffic bypasses the ZTA tunnel and connects directly to the Internet

---

Note: After implementing the exceptions, Teams traffic does not appear in the Secure Access activity logs, as it bypasses the ZTA tunnel entirely.

Cause

The issue is caused by Microsoft Teams traffic being routed through the ZTA Secure Internet Access tunnel instead of connecting directly to the internet. When the ZTA profile is configured with the "Secure All Internet Destinations" option, it intercepts Teams media traffic, including UDP flows required for real-time communication. This causes connectivity issues, particularly for incoming calls and media streams.

Microsoft recommends bypassing Microsoft Teams traffic from proxy servers and SSL inspection for optimal performance and call quality. When the ZTA configuration is missing the necessary exceptions for Teams traffic the application media flow is processed through the ZTA client rather than taking the direct path required for real-time communication.

Related Content

- Microsoft 365 URLs and IP Address Ranges - Microsoft Teams
- Microsoft Teams Proxy Server Recommendations
- Troubleshoot and Collect Basic Information for Cisco Secure Access
- Cisco Technical Support & Downloads