Solución de problemas de MS Teams con configuración de perfil de acceso de confianza cero

Contenido

Problema

Los usuarios inscritos en un perfil de acceso de confianza cero (ZTA) para el acceso seguro a Internet experimentaron problemas de conectividad de llamadas de Microsoft Teams. Cuando se agregan usuarios al perfil ZTA, las llamadas de Microsoft Teams se desconectan inesperadamente y otros usuarios no pueden iniciar llamadas al usuario afectado. Sin embargo, las llamadas se conectan correctamente cuando el usuario afectado inicia la llamada desde su lado.

El problema se aísla para los usuarios incluidos en el perfil ZTA, lo que indica que las políticas ZTA o las configuraciones de routing están afectando a la conectividad de las llamadas de los equipos. Los registros de tráfico muestran que el tráfico de Microsoft Teams de procesos como ms-team.exe a direcciones IP en rangos requeridos (como 52.115.245.30:3480, que es parte de 52.112.0.0/14) está siendo interceptado por el cliente ZTA en lugar de ir directamente a Internet.

Entorno

- Configuración del perfil de Cisco Secure Access con acceso de confianza cero (ZTA)
- Perfil ZTA configurado con "Utilizar ZTA para proteger todos los destinos de Internet"
- aplicación Microsoft Teams
- Cisco Secure Client con funciones ZTA
- Usuarios inscritos en el perfil ZTA para acceso seguro a Internet

Resolución

Para resolver el problema, agregue excepciones de tráfico de Microsoft Teams a la configuración del perfil ZTA para permitir que el tráfico de Teams pase por alto el túnel ZTA y se conecte directamente a Internet:

1. Navegue hasta Panel > Conectividad del usuario final > Acceso de confianza cero y localice el perfil ZTA afectado.

2. Seleccione el perfil ZTA y elija Edit > Secure Internet Access.

3. Agregue estos rangos de IP y FQDN a la lista de excepciones de la Documentación Oficial de Microsoft:

Intervalos IP:

```
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
```

FQDN:

```
*.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. Añada una descripción para las excepciones, como:

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

5. Guarde los cambios de configuración. Espere unos minutos a que se apliquen los cambios.

6. Asegúrese de que la política de cliente ZTA se vuelva a sincronizar en los terminales afectados. Esto puede requerir el reinicio del servicio Agente de acceso de confianza cero o el reinicio del dispositivo cliente.

7. Los equipos de pruebas llaman a la funcionalidad para confirmar que:

- Las llamadas entrantes dirigidas a los usuarios afectados se conectan ahora correctamente
- Las llamadas de equipo ya no se desconectan inesperadamente
- El tráfico de los equipos omite el túnel ZTA y se conecta directamente a Internet

---


Nota: Después de implementar las excepciones, el tráfico de Teams no aparece en los registros de actividad de Secure Access, ya que omite por completo el túnel ZTA.

Causa

El problema se debe a que el tráfico de Microsoft Teams se enruta a través del túnel de acceso seguro a Internet ZTA en lugar de conectarse directamente a Internet. Cuando el perfil ZTA se configura con la opción "Secure All Internet Destinations" (Proteger todos los destinos de Internet), intercepta el tráfico multimedia de Teams, incluidos los flujos UDP necesarios para la comunicación en tiempo real. Esto provoca problemas de conectividad, especialmente en el caso de las llamadas entrantes y las transmisiones de medios.

Microsoft recomienda omitir el tráfico de Microsoft Teams de los servidores proxy y la inspección SSL para obtener un rendimiento y una calidad de llamada óptimos. Cuando la configuración ZTA no cuenta con las excepciones necesarias para el tráfico de los equipos, el flujo de medios de la aplicación se procesa a través del cliente ZTA en lugar de tomar la ruta directa requerida para la comunicación en tiempo real.

Contenido relacionado

- Direcciones URL e intervalos de direcciones IP de Microsoft 365 - Microsoft Teams
- Recomendaciones del servidor proxy de Microsoft Teams
- Solución de problemas y recopilación de información básica para Cisco Secure Access
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).