

Secure Access RA VPN Authentication Events with Link-Local AAA Server Addresses

Contents

Issue

When testing Secure Access Remote Access (RA) VPN functionality, excessive authentication events are being logged for identities that do not exist in the tenant organization. The authentication logs show more than 10,000 RA VPN authentication events within a 24-hour period, containing AAA errors such as "AAALOG_SERVICE_DOWN" and "AAALOG_SERVER_DOWN". These error messages reference link-local 169.254.x.x addresses as the AAA server, which are not configured in the tenant.

Specific error examples observed in the logs include:

AAALOG_SERVICE_DOWN

AAA authentication server not accessible : server = 169.254.169.79 : user = <user>

AAALOG_SERVER_DOWN

AAA Marking RADIUS server 169.254.169.79 as FAILED

The activity appears to be repeated RADIUS-based authentication attempts against the Secure Access VPN FQDN, creating excessive log noise and raising concerns about external scanning or potential abuse of the VPN service.

Environment

- Cisco Secure Access platform
- Remote Access VPN profile initially configured without certificate authentication
- RADIUS-based authentication configured for RA VPN
- Public VPN tenant configuration with discoverable VPN profiles

Resolution

The resolution involved understanding the authentication flow behavior and implementing certificate-based authentication as a mitigation strategy.

Technical Explanation of Observed Behavior

The excessive authentication events occur due to the technical reasons described in the next sections.

Authentication Flow without Certificate Requirements

When certificate authentication is disabled and RADIUS-based RA VPN authentication is used, the system logs "failed authorization" attempts because the system first checks username identity against the database of users synchronized in Secure Access, and records the "failed authorization" event. These events are expected as a first line of defense but can produce significant log noise when external actors attempt authentication.

Link-Local Address Usage

The 169.254.x.x addresses seen in logs are internal/local-link addresses used by the RA VPN headend to authorize incoming sessions. These addresses represent internal system behavior rather than misconfiguration of AAA servers in the tenant.

VPN Profile Discovery

When a public VPN tenant ID is configured, the VPN profiles are listed in the UI dropdown, which can allow external actors to discover public profiles more easily and target them for authentication attempts.

Immediate Mitigation Steps

1.- Configure certificate-based authentication. Modify the RA VPN profile to require certificate-based authentication. When certificate authentication is required, Secure Access performs a certificate check earlier in the authentication flow. If the certificate is missing, the system produces an error before the standard authentication flow, and the "failed authorization" events are not logged in the same manner.

2.- Validate mitigation effectiveness. Monitor the authentication logs after implementing certificate-based authentication to confirm the reduction in excessive authentication events. Switching to certificate-based authentication successfully mitigated the attacks and reduced log noise.

Long-term Improvements

Two feature requests were created to address the underlying issues:

- Feature Request 1: Add an option to hide or show the tunnel group (VPN profile) list when a public VPN tenant is added, reducing profile discoverability.
- Feature Request 2: Add a configuration option to enable or disable logging of failed RA VPN authorization attempts, providing administrators with control over log verbosity.

Additionally, a public-facing document is created to explain the logged events and authentication behavior to help administrators understand normal system operations.

Cause

The root cause of the excessive authentication events is the combination of discoverable VPN profiles in public tenant configurations and the authentication flow behavior when certificate-based authentication is not required. When RADIUS-based authentication is used without certificate requirements, the system logs all "failed authorization" attempts as part of its security posture, including attempts from external actors who discover the VPN profiles. The link-local addresses in the logs represent normal internal system behavior for the RA VPN headend authorization process, not configuration errors.

Related Content

- [Cisco Technical Support & Downloads](#)