ワンタイムパスワードを使用したRADIUSを備えたASAでのSSH認証失敗のトラブルシューティング

内容

お問い合わせ内容

CiscoSSHスタックが有効になっていると、One-Time Password（OTP；ワンタイムパスワード）を使用したRemote Authentication Dial-In User Service（RADIUS；リモート認証ダイヤルインユーザサービス）による、適応型セキュリティアプライアンス(ASA)ソフトウェアへのセキュアシェル(SSH)アクセスが失敗します。

次のsyslogメッセージが生成されます。

```
Nov 14 2025 16:28:35: %ASA-6-113010: AAA challenge received for user from server .
Nov 14 2025 16:28:35: %ASA-4-109033: Authentication failed for admin user from . Interactive challenge
```

環境

すべての条件が一致すると、症状が現れます。

- シングルコンテキストモードまたはマルチコンテキストモードのASAを使用したファイアウォール1230の保護他のハードウェアプラットフォームも影響を受けます。
- SSH認証にRADIUSサーバが使用されている場合：

<#root>

device#

show run | i aaa

```
aaa-server RAD-OTP protocol radius
aaa-server RAD-OTP (management) host 192.0.2.1
aaa-server RAD-OTP (management) host 192.0.2.2
aaa authentication ssh console RAD-OTP
```

- RADIUSサーバは、認証を正常に行うために有効なOTPコードまたはチャレンジを要求し、要求します。
- CiscoSSHスタックがASAで有効になっている。
- バージョン9.19.1以降では、CiscoSSHスタックはデフォルトで有効になっています。また、no ssh stack ciscoコマンドを使用して、オプションで無効にすることもできます。show sshコマンドを使用して確認します。

<#root>

```
device#

show ssh


ssh secure copy : ENABLED

ciscoSSH stack : DISABLED
```

- バージョン9.23.1以降では、このスタックを無効にしたり検証したりすることはできません。

解決策

症状は内部ラボで再現され、Cisco Bug ID CSCwt57790で追跡されています。

該当するバージョンでは、次のいずれかの回避策オプションを使用してください。

- SSH接続にはローカル認証を使用します。
- RADIUSサーバで、ASAのOTP要件を無効にします。
- 9.23よりも前のリリースでは、no ssh stack ciscoコマンドを使用してCiscoSSHスタックを無効にします。必ず『Cisco Secure Firewall ASAシリーズコマンドリファレンス、Sコマン

ド』を参照して、CiscoSSHスタックを無効にした場合の潜在的な影響を評価してください。

原因

認証失敗の原因はCisco Bug ID CSCwt57790です。

関連コンテンツ

- Cisco Bug ID CSCwi04513
- Cisco Bug ID CSCwt57790
- Cisco Secure Firewall ASAシリーズコマンドリファレンス、コマンド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。