Cisco E メール セキュリティ アプライアンス（ESA）の証明書認証アルゴリズムとは何ですか。

目次

概要

Cisco E メール セキュリティ アプライアンス」または「ホストされる」オプションを確認しなさいことを（ESA）によってメールを渡すのに TLS を使用するとき確認しますを使用して証明書確認を「行うことを選択できます。 これは TLS にメールの配信を保護することの重大な一部分であり、この確認がどのように実行されたか知っていることは重要です。

Cisco E メール セキュリティ アプライアンス（ESA）の証明書認証アルゴリズムとは何ですか。

実際に 2 つのアルゴリズムがあります、のための 1 つはオプションを「確認し」、「ホストされる」のための他はオプションを確認します。 通常シナリオのより大きい変化で互換性があるので」オプションが推奨されることをホストされる「確認します。

背景説明

- このドキュメントは AsyncOS 8.0.1 およびそれ以降 バージョンに基づいています。AsyncOS の以前のバージョンは異なる動作が幾分あるかもしれません。
- 他に特に規定がなければ、ワイルドカード一致はサポートされます
- 各アルゴリズムは成功した組合せの後で停止し、それに続くチェックは評価されません
- CLI コマンドは **tlsverify** 「使用を確認しますアルゴリズム」を

定義

- CN: これは Common Name、証明書のサブジェクトの部分です
- SAN: これは X.509 へ認証対象代替名 拡張です。 この資料で使用されたとき、とりわけ SAN フィールドに含まれている DNS名を参照しています。
- メール ドメイン: これは受信者の eメールアドレスのドメイン部分です。 たとえば、「user@example.com」に渡した場合、メール ドメインがである「example.com」が

- MX ホスト名: これらはメール ドメインの MX レコードのホスト名です
- PTR ホスト名: これは ESA がに接続している IP アドレスの DNS PTR ルックアップによって戻るホスト名です
- SMTP ルート ホスト名: SMTP ルートがこの宛先のために設定される場合、これは SMTP ルートで使用されるホスト名です

ホストされるアルゴリズムを確認して下さい

1. 証明書が SAN 属性が含まれている場合、これらだけが使用され、CN が無視される。 CN は証明書に SAN 属性がない場合その時だけ使用されます。 これは RFC 6125 に合致します。
2. 証明書はメール ドメインに対してチェックされます。
3. 証明書はあるかもしれないあらゆる SMTP ルート ホスト名に対してチェックされます。
4. 証明書は MX ホスト名に対してチェックされます。
5. 前のチェックのどれも成功しない場合、確認は失敗します。

アルゴリズムを確認して下さい

1. SAN 属性はメール ドメインに対してチェックされます。
2. CN はメール ドメインに対してチェックされます。 **注:** ワイルドカード一致はサポートされません。
3. SAN 属性は PTR ホスト名に対してチェックされます。
4. 前のチェックのどれも成功しない場合、確認は失敗します。