ＶＰＮ装置への攻撃を
どのように防御できるか？

なぜ、多くの VPN アプライアンス
がハッキングされてしまったのか？

解決できるソリューションは
存在するのか？

SmatSecret VPN について

多くの VPN アプライアンス（UTM）では、個別証明書を発行して利用するリモートアクセス環境を構築するには別途、証明書発行管理サーバーなどを用意する必要があり膨大な費用が必要になります。

また、クライアント証明書毎に固定の仮装 IP アドレスを割り振る機能も持ち合わせていないために、ユーザ毎のセキュリティポリシーを適応させる事ができません。

現状の UTM で実装されているリモートアクセス VPN では、
ユーザ ID/パスワード認証
共通の PSK 認証
共通の証明書認証

などが利用されていますが、それらの多くは利用者本人に成り済ます事が可能です。

なぜなら、利用者が本当に利用者のデバイスから通信しているかを厳密に確認してはいないからです。

その結果、多くの UTM で VPN の不正利用が発生しました。

昨今ニュースになった VPN への不正進入は、
https://koneta.nifty.com/koneta_detail/1141008008526_1.htm
https://www.itmedia.co.jp/business/articles/2009/06/news009.html

また、著名なパロアルトやシスコの VPN アプリケーションにも
脆弱性見つかり不正アクセスが発生しました。
https://cybersecurity-info.com/news/vulnerability-vpn/

- Palo Alto Networks (CVE-2019-1579)
- Fortinet (CVE-2018-13379)
- Pulse Secure (CVE-2019-11510)

SmatSecret VPN について

SSL VPN 装置での脆弱性は 2019 から指摘されていました。
しかし、UTM の運用管理を適切に実施しないまま、脆弱性のパッチの適用などを実施しないデバイスはまだ世界の至る所に存在しています。

実際、Fortinet の被害の影響も大きなインシデントでした。
https://active.nikkeibp.co.jp/atcl/act/19/00100/011500003/

このようなインシデントは一部脆弱性と安易な認証方法を採用した結果と言えます。

上記の認証方法では、利用者に紐づいたデバイスであると、信頼できる要素とは言えません。

結果として、セキュリテイレベルが低くても良いとは思っていない顧客層も利用せざるを得ないことになっています。

セキュリティクリアランスを考慮するのであれば、利用者とデバイスを完全に関連づける事が義務付けされます。

本当に、本人が利用しているデバイスから VPN を接続しているのか？
このことは非常に重要であることは明白です。

こうした紐付けは、ナショナルセキュリティの世界では必然のこととして利用されています。しかし民間で利用する VPN では社員一人舞に異なる個別証明書を持たせることは現状の UTM には負荷が大きすぎ実装されてはいません。

そうです、多くの VPN は、全て安易なログイン認証を利用していルのです。

その結果、多くの不正利用を止める事ができない状況になっているのです。

SmartSecret VPN ではそうした問題の根本的な回避を目指して設計されました。
本製品には、ナショナルセキュリテイで利用されている技術を応用しています。