Dátum predloženia dokumentu: 19. 9. 2025
Zasadnutie PS štandardizácie číslo:

Identifikácia technickej špecifikácie SSL-VPN

identifikácia SSL-VPN špecifikácie pre zabezpečenie sieťovej komunikácie

Zhrnutie

V tomto dokumente sa predkladajú podklady pre identifikáciu technických špecifikácií SSL-VPN pre zabezpečenie sieťovej komunikácie v súlade s vyhláškou č. 78/2020 Z. z. UPVII o štandardoch pre informačné technológie verejnej správy.

Predmet

Predkladaná špecifikácia je dnes bežne používaná v prostrediach ISVS pre zabezpečenie sieťovej komunikácie.

Špecifikácia protokolu je dostupná na adrese 1. Ultimate Powerful VPN Connectivity - SoftEther VPN Project alebo aj mnohých výrobcov ako napr. Understanding the AnyConnect SSL VPN Connection Flow - Cisco. Takmer všetci výrobcovia sieťových bezpečnostných prvkov implementujú tento protokol VPN pre scenáre client-to-net. Cisco je tu uvedený len ako jeden z príkladov.

Proces

Vzťahy s ostatnými špecifikáciami

SSL-VPN stavia na špecifikáciách

- RFC 8200 - Internet Protocol, Version 6 (IPv6) Specification
- RFC 9110 - HTTP Semantics

OpenVPN je alternatívou k IPSec špecifikácii

- RFC 4301 - Security Architecture for the Internet Protocol

Zhodnotenie

Vhodnosť

Aplikovateľnosť	SSL-VPN slúži na zabezpečenie prenosu údajov na úrovni sieťovej vrstvy ako alternatíva k IPSec. Štandard môže používať VS, HS aj občania. SSL-VPN umožňuje vytvorenie VPN typu site-to-site alebo user-to-site. Výhodou je jednoduchšia správa VPN.
Relevancia	SSL-VPN je už dnes používaný najmä v prostrediach, kde sa kladie dôraz na jednoduchosť správy a sú obmedzené ľudské zdroje.
Prispôsobivosť	Štandard je podporovaný na mnohých platformách. Nie je závislý na zmenách iných technológií.

Dátum predloženia dokumentu: 19. 9. 2025
Zasadnutie PS štandardizácie číslo:

Dopady

Finančný dopad	Prijatie **nemá** finančné dopady, prínosom je zosúladenie legislatívy s praxou.
Organizačný dopad	Prijatie **nemá** vplyv na existujúce postupy.
Strategický dopad	Prijatie je cielené pre **účely VS SR**.
Potreba migrácie	Prijatie **nevyžaduje migráciu** na nové technológie.
Bezpečnostný dopad	Prijatie **nevyžaduje osobitné bezpečnostné opatrenia**.
Dopad na súkromie	Štandard bude používaný na zabezpečenie prenosu údajov na sieťovej úrovni.
Dopad na interoperabilitu	Štandard **nemá** dopad na interoperabilitu.
Dopad na kompatibilitu	Štandard je alternatívou pre IPSec s jednoduchšou správou VPN.
Závislosti	SSL-VPN nemá prídavné závislosti.
Dopad na administratívnu záťaž	Očakáva sa zníženie administratívnej záťaže pre menšie organizácie s obmedzenými ľudskými zdrojmi.

Potenciál

Škálovateľnosť	Špecifikácia aj implementácia štandardu sú otvorené, no vzhľadom na kontext bezpečnosti nie je vhodná ich úprava.
Rozšíriteľnosť	Štandard je už dnes široko používaný vo VS najmä v kontexte client-to-site VPN.
Stabilita	SoftEther štandard existuje od roku 2013, kedy bola vydaná jeho prvá implementácia - Version History (ChangeLog) - SoftEther VPN Project. Ostatní výrobcovia implementujú vlastné formy bez dostupných podrobných špecifikácií.
Údržba	Špecifikácia SoftEther je spravovaná komunitou SoftEther a SoftEther Corporation. GitHub - SoftEtherVPN/SoftEtherVPN: Cross-platform multi-protocol VPN software. Pull requests are welcome. The stable version is available at https://github.com/SoftEtherVPN/SoftEtherVPN_Stable. Ostatní výrobcovia majú rôzny stupeň transparentnosti o detailoch implementácie.

Otvorenosť

Dostupnosť	Dokumentácia špecifikácie SoftEther protokolu je voľne dostupná na adrese 1. Ultimate Powerful VPN Connectivity - SoftEther VPN Project. Táto špecifikácia je základom aj pre iné implementácie výrobcov sieťových bezpečnostných prvkov.
Právne obmedzenia	Špecifikácia SSL-VPN nezanáša žiadne priame obmedzenia. Niektoré obmedzenia môžu byť predmetné v kontexte prvej verzie implementácie „SoftEther 1.0“ s výhradným vlastníctvom Mitsubishi Materials Corporation - About SoftEther VPN Project - SoftEther VPN Project.
Prístupnosť	Špecifikácia aj implementácia sú dostupné bez ďalších obmedzení.

	Detailná špecifikácia implementácií iných výrobcov môže byť zverejnená v rôznom detaile.
Vzájomná spolupráca	

Procesy správy

Otvorené komunikačné kanály	Projekt SoftEther poskytuje otvorené komunikačné kanály.
Hlasovanie o zmenách	Zdrojové kódy implementácie spravuje skupina vývojárov, ktorých zoznam je verejne dostupný GitHub - SoftEtherVPN/SoftEtherVPN: Cross-platform multi-protocol VPN software. Pull requests are welcome. The stable version is available at https://github.com/SoftEtherVPN/SoftEtherVPN_Stable.
Dodržiavanie a transparentnosť	Ktokoľvek (aj mimo komunity) môže otvoriť požiadavku na úpravu.
Otvorenosť zmien	
Podpora	Projekt SoftEther je krytý komunitou a spoločnosťou SoftEther Corporation.

Podmienky trhu

Rozšírenie

Produkty	SoftEther VPN, Cisco AnyConnect, Juniper Secure Connect, a iné.
Dodávatelia	SoftEther, Cisco, Juniper
Kompatibilita	Kompatibilita môže byť v prípade veľkých výrobcov viazaná na „značku“. Kompatibilita SoftEther nie je problematická.
Podiel na trhu v SR	Nie je známe.
Podiel na trhu vo svete	Nie je známe.
Referencie	
Oblasť rozšírenia	

Vyzretosť

Vyzretosť	Štandard je dostatočne vyzretý.
Aktualizácie	Aktualizácie sú zdokumentované.
Známe problémy	Prípadné problémy sú zdokumentované na stránkach projektu.

Opätovná použiteľnosť

Segmentácia	Štandard je použiteľný samostatne na strane klienta aj poskytovateľa VPN.
Kompatibilita	Sú dostupné implementácie na mnohých platformách, dokonca aj mobilných.