www.eset.sk

SECURE AUTHENTICATION

Chráni vašu VPN

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE

Prehľad

Čoraz častejšie používanie vzdialeného prístupu núti firmy hľadať riešenie, ako jednoducho zabezpečiť prístup k citlivým firemným aktívam.

Na trhu je množstvo jednoducho konfigurovateľných a cenovo dostupných VPN, ktoré ponúkajú vzdialený prístup a v niektorých prípadoch Unified Threat Management (UTM) pre malé, stredné aj veľké organizácie.

ESET so svojou technológiou NOD32® zabezpečuje firemnú IT infraštruktúru na všetkých hlavných operačných systémoch. Teraz navyše ponúka spôsob, akým zaviesť silnú autentifikáciu do triedy VPN zariadení. To všetko prostredníctvom jednorazových hesiel (OTP – one-time password), ktoré sú generované jednoducho použiteľnou aplikáciou nachádzajúcou sa v mobilných telefónoch používateľov.

ESET Secure Authentication vám v kombinácii s vašou VPN poskytuje jednoduchý a bezpečný vzdialený prístup – kdekoľvek a kedykoľvek.

Problém

Od firiem a rôznych organizácií sa čoraz viac požaduje, aby poskytovali vzdialený prístup k firemným aplikáciám a údajom – či už od zamestnancov pracujúcich z domu, firemných pobočiek, partnerov alebo zákazníkov. Skutočná sieťová bezpečnosť si vyžaduje množstvo elementov, a mnohé z nich poskytuje rozširujúca sa ponuka VPN riešení.

Statické heslá majú však známu nevýhodu – nie sú bezpečné. Odborníci na bezpečnosť preto odporúčajú doplniť vstavanú autentifikáciu pre VPN zariadenia o ďalší faktor, a zosilniť tak proces autentifikácie.

ESET Secure Authentication je možné integrovať s VPN riešeniami a zaviesť tak dvojfaktorovú autentifikáciu pre silnú ochranu firemnej LAN a dôležitých firemných údajov.

Dvojfaktorová autentifikácia (2FA) je autentifikačná metóda, ktorá si vyžaduje dva od seba nezávislé údaje pre overenie používateľovej identity. 2FA je oveľa silnejšia než tradičná autentifikácia heslom, ktorá si vyžaduje len jeden faktor.

Tento dokument ukazuje, ako sa dá dvojfaktorová autentifikácia pre tieto VPN zariadenia nastaviť rýchlo a jednoducho.

Podrobné manuály pre konkrétne typy VPN si môžete prečítať prostredníctvom odkazov na konci tohto dokumentu. Vyhľadávať môžete tiež v Databáze znalostí ESET podľa názvu vášho VPN zariadenia.

Riešenie

ESET Secure Authentication sa dá jednoducho integrovať do existujúceho VPN riešenia – čím pridáte silnú autentifikáciu bez zásadného zásahu do konfigurácie VPN.

Štandardná autentifikácia pre väčšinu VPN zariadení je založená na LDAP, RADIUS, alebo lokálnej autentifikácii. ESET Secure Authentication používa RADIUS ako externú autentifikačnú metódu pre vaše VPN zariadenie.

Keď správne nastavíte ESET Secure Authentication a vašu VPN, eliminujete tak najslabší článok bezpečnostnej infraštruktúry – používanie statických hesiel, ktoré sa dajú ľahko ukradnúť, uhádnuť, opakovane použiť alebo zdieľať.

Výhody

ESET Secure Authentication ponúka nasledujúce výhody v kombinácii s vaším VPN zariadením:

- Výrazne vyššia úroveň bezpečnosti vďaka dvom nezávislým faktorom pre autentifikáciu
- Menšie riziko z málo komplexných a slabých hesiel
- Minimálny čas potrebný na zaškolenie a podporu používateľov
- Jednoduché zavedenie vo vašej sieti

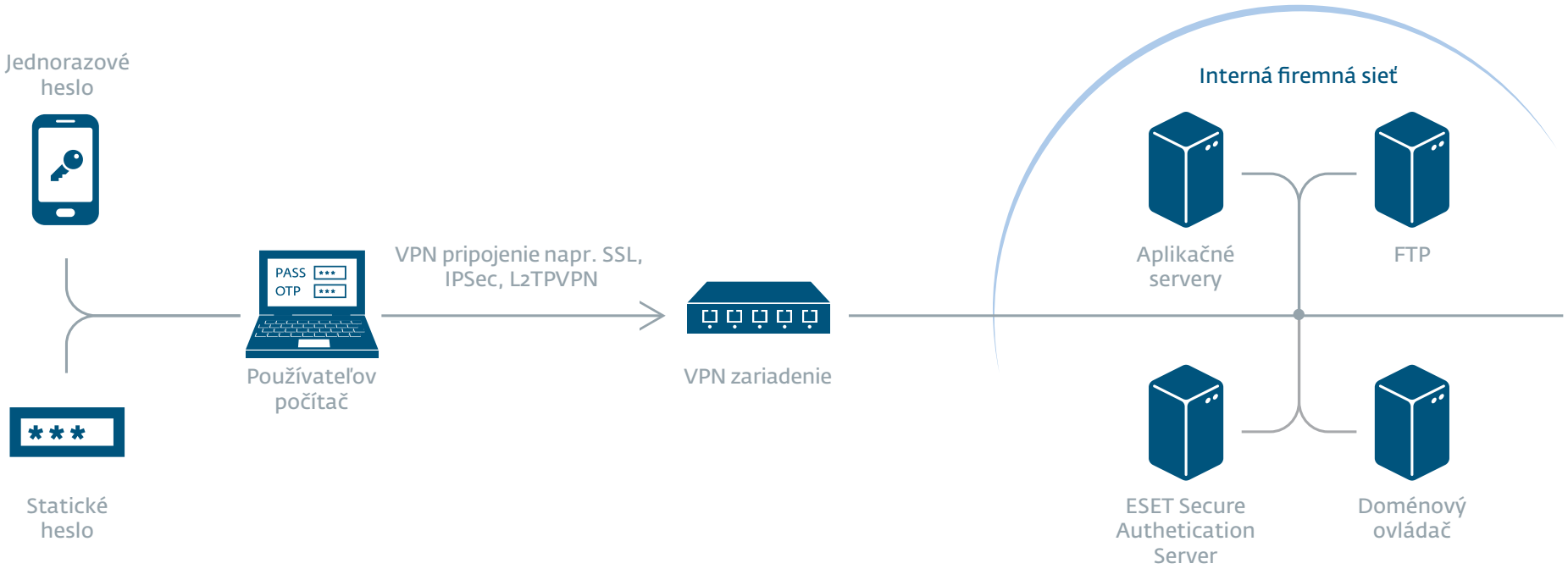
Ako funguje 2FA s ESET Secure Authentication?

Dvojfaktorová autentifikácia vyžaduje použitie autentifikačnej služby tretej strany. Autentifikačná služba pozostáva z dvoch častí:

- ESET Secure Authentication RADIUS Server vo windowsovej sieti, na ktorom môže administrátor používať Active Directory Users and Computers (ADUC) na konfiguráciu používateľových nastavení pre 2FA.
- Mobilná aplikácia (pre rôzne mobilné operačné systémy) bežiaca na používateľovom mobilnom telefóne, ktorá sa použije na generovanie OTP pri každom autentifikačnom pokuse. Ako alternatíva: OTP je možné nechať si zaslať cez SMS správu.

V momente, keď je zavedená 2FA, používateľ musí vložiť svoje statické heslo a taktiež platné OTP, aby získal prístup. OTP je šesťmiestny číselný kód z aplikácie na používateľovom mobilnom telefóne, ktorý môže byť vygenerovaný bez pripojenia telefónu do siete. Statické heslo sa prepošle cez VPN do back-endu (doménový ovládač) pre overenie jeho platnosti. OTP sa zašle na ESET Secure Authentication Server v rámci siete, kde sa overí. Ak sú obe heslá platné, používateľ sa autorizuje.

Vaša VPN s ESET Secure Authentication



Technická špecifikácia

Štandardný postup

RADIUS autentifikácia s ESET Secure Authentication funguje nasledovne:

1. Vzdialený používateľ inicializuje spojenie k VPN.
2. VPN získa používateľovo ID, statické heslo, jednorazové heslo (OTP) a pošle tieto údaje na ESET Secure Authentication RADIUS server.
3. Server posunie tieto údaje službe ESET Secure Authentication Core Authentication Service.
4. Authentication Service autentifikuje statické heslo voči Active Directory (AD) a OTP voči skrytým dátam uloženým pod používateľovým AD účtom.
5. VPN zariadenie potom povolí autorizovanému používateľovi prístup do firemnej siete.

VPN autentifikácia s ESET Secure Authentication

Hlavným účelom VPN je zvýšiť bezpečnosť vzdialeného prístupu do siete. Vie zabezpečiť autentifikáciu oproti externej službe pomocou protokolu RADIUS – toto umožňuje službe ESET Secure Authentication RADIUS Server fungovať ako back-end služba pre vašu VPN.

Používatelia sú autentifikovaní najprv prostredníctvom ESET Secure Authentication Servera, ktorý môže byť prepojený na back-ende s Active Directory. ESET Secure Authentication v podstate funguje medzi VPN a Active Directory.

To znamená, že ESET Secure Authentication dostane všetky požiadavky na autentifikáciu z vašej VPN. OTP a autentifikačné požiadavky sú overené pomocou ESET Secure Authentication RADIUS Servera. Server odošle statické heslo back-endu (RADIUS Server alebo Active Directory) na verifikáciu, ak je to požadované. Po úspešnej verifikácii sa zašle akceptačná správa RADIUS ACCESS-ACCEPT na VPN pre autentifikačnú odpoveď.

Predpoklady pre zabezpečenie VPN s ESET Secure Authentication

VPN predpoklady

VPN s fungujúcim nastavením je základným predpokladom pre implementáciu riešenia ESET Secure Authentication. Je dôležité, aby VPN fungovala správne skôr, ako začnete s inštaláciou ESET Secure Authentication.

Active Directory

Active Directory musí byť vopred nakonfigurované, bude slúžiť ako back-end pre overovanie statických hesiel používateľov k jednotlivým účtom. Používateľské účty musia byť tiež vytvorené v Active Directory.

ESET Secure Authentication Server

ESET Secure Authentication musí byť nainštalovaný v doménovom prostredí. ESET Secure Authentication obsahuje vlastný RADIUS server, takže má všetko, čo potrebujete pre pridanie 2FA do vašej VPN.

Integračné manuály

V našej databáze znalostí nájdete manuály pre:

Barracuda

Cisco ASA ipsec

Cisco ASA

Citrix Access Gateway

Citrix Netscaler

F5 Firepass

Check Point Software

Fortinet Fortigate

Juniper

Microsoft RRAS

Microsoft RRAS with NPS

OpenVPN Access Server

Palo Alto

Sonicwall

O spoločnosti ESET
ESET je globálnym výrobcom bezpečnostných riešení pre firmy a domácich používateľov. Hlavné sídlo sa nachádza v Bratislave a pobočky po celej Európe, Ázii, Austrálii, Latinskej Amerike a Severnej Amerike. Produktom ESETu dôveruje viac než 100 miliónov IT profesionálov a používateľov po celom svete. Výskumné a vývojové centrá ESET prinášajú bezpečnostné inovácie pre zákazníkov v 180 krajinách.