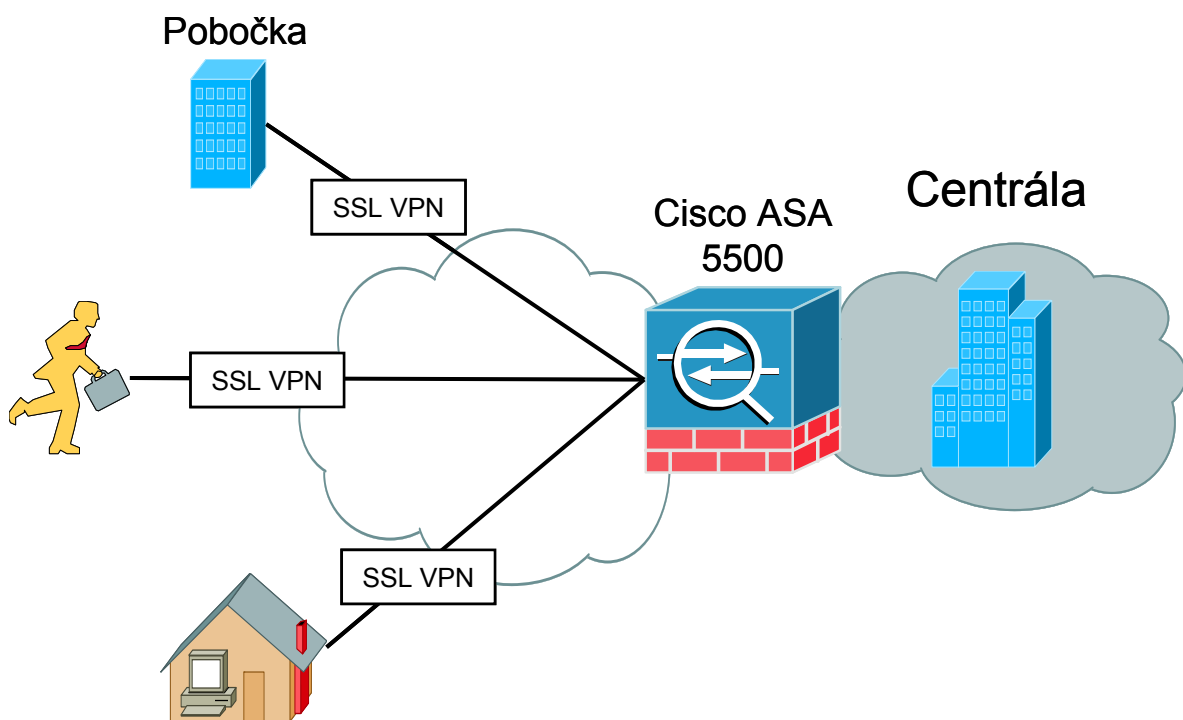


Jednorázová hesla pro zvýšení bezpečnosti vzdáleného přístupu mobilních uživatelů

Jedním z řešení bezpečného vzdáleného přístupu mobilních uživatelů k firemnímu informačnímu systému je použití technologie SSL VPN realizované na platformě Cisco ASA 55xx.



Obrázek 1 Vzdálený přístup mobilních uživatelů pomocí SSL VPN

Zákazníkům se zvýšenými požadavky na bezpečnost nabízí Simac Technik ČR (dlouholetý certifikovaný Cisco Silver Partner) vlastní řešení dvoufaktorové autentizace uživatelů SSL VPN s použitím jednorázových hesel a platformy Cisco ASA 5500. Uživatelé jsou plně pod kontrolou zákazníka v jeho vlastní interní databázi uživatelů (LDAP/MS AD, SQL DB).

Jednorázová hesla se posílají uživatelům pomocí SMS nebo e-mailu.

Technický popis řešení

Jádrem řešení je platforma Cisco ASA 5500 rozšířená o aplikační server (Intel/Linux) a GSM modem pro zaslání SMS.

Použití open-source technologií na aplikačním serveru pro implementaci dvoufaktorové autentizace poskytuje nabízenému řešení dostatečnou flexibilitu na



přizpůsobení řešení specifickým požadavkům zákazníka nejen z hlediska použitého hardwaru, ale i softwarových rozhraní do zákaznického informačního systému.

Implementace dvoufaktorové autentizace SSL VPN

Na obr. 2 je uvedeno funkční schéma použitého řešení dvoufaktorové autentizace externího uživatele, který se chce připojit k internímu informačnímu systému prostřednictvím SSL VPN.

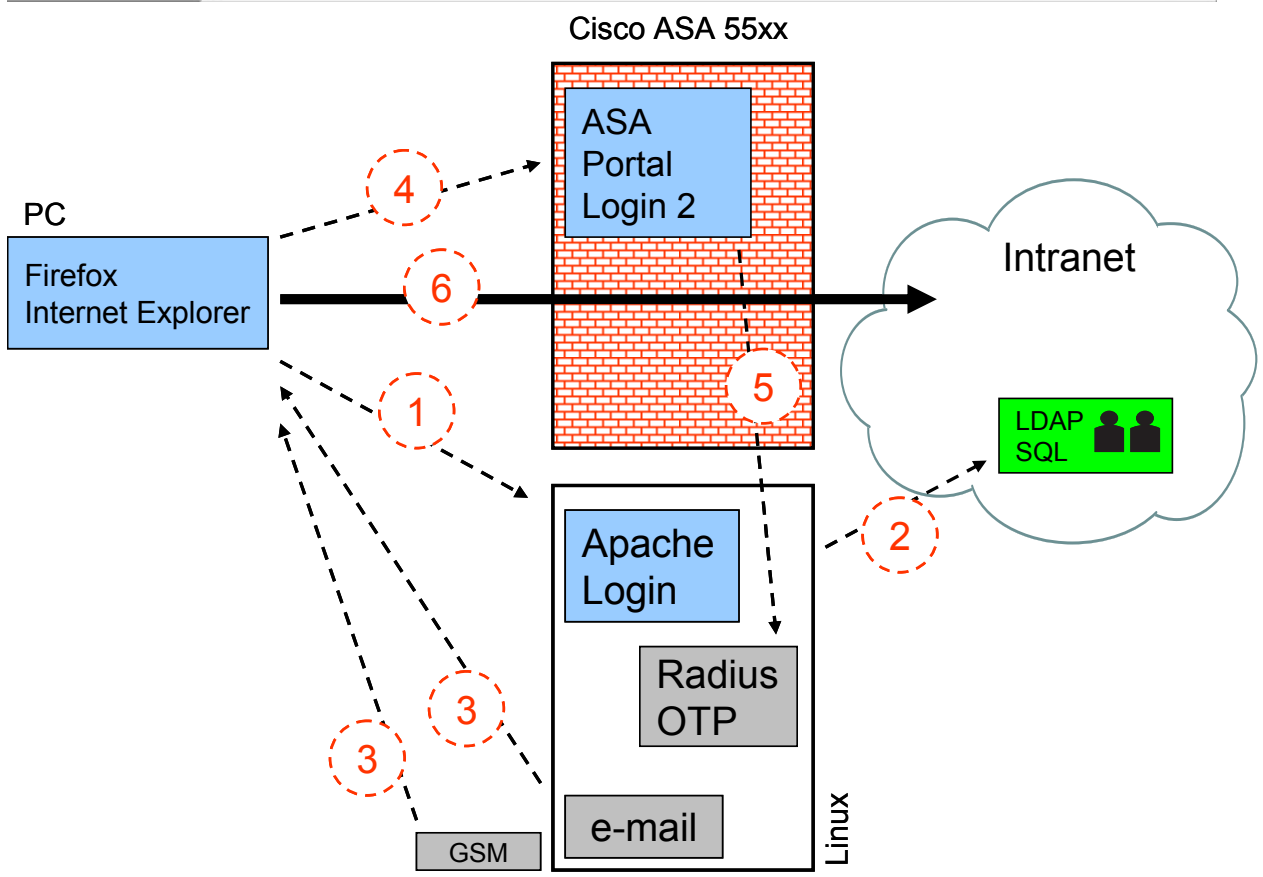
Uživatel SSL VPN potřebuje na svém počítači webový prohlížeč (Firefox s Java pluginem nebo Internet Explorer).

Aplikační server (Linux, v dolní části obrázku) poskytuje služby:

- webového serveru (Apache 2.x) pro primární přihlášení,
- RADIUS serveru pro autentizaci SSL VPN pomocí jednorázového hesla (OTP),
- odesílání e-mailových zpráv (SMTP),
- odesílání SMS zpráv pomocí GSM modemu.

Uživatelské účty pro vzdálený přístup jsou administrovány zákazníkem v jeho interní databázi uživatelů (LDAP, SQL databáze).

Sekundární autentizace uživatelů je realizována na Cisco ASA 55xx prostřednictvím ASA portálu.



Obrázek 2 Implementace dvoufaktorové autentizace



Přihlášení vzdáleného uživatele probíhá v několika krocích

1. Uživatel se ze svého počítače přihlásí pomocí webového prohlížeče na WWW server (Apache). Používá při tom jméno a heslo definované administrátorem v databázi uživatelů. Tato primární autentizace je implementována pomocí standardních modulů web serveru Apache.
2. Po zadání přihlašovacích údajů je uživatel ověřen v zákaznickově databázi uživatelů, odkud se načítají parametry uživatelského přihlášení - platnost jména, e-mailová adresa a/nebo telefonní číslo pro zaslání SMS.
3. Systém vygeneruje jednorázové heslo, které se posílá uživateli podle nastavených parametrů (e-mail, SMS). Pokud uživatel po uplynutí předdefinované doby nedostane zprávu s jednorázovým heslem, může iniciovat odeslání nového jednorázového hesla.
4. Po potvrzení příjmu jednorázového hesla je uživatel přesměrován na webový portál Cisco ASA 55xx, kde se znovu autentizuje, nyní s použitím svého jména a jednorázového hesla.
5. Cisco ASA 55xx pro autentizaci používá RADIUS server na aplikačním serveru.
6. Po úspěšné sekundární autentizaci může uživatel používat služby definované v Cisco ASA portálu. Obsah portálu může být přizpůsoben podle identity uživatele.

Flexibilita řešení

Nabízené řešení rozšiřuje standardní možnosti SSL VPN na platformě Cisco ASA 5500 o dvoufaktorovou autentizaci s použitím jednorázových hesel. Díky použitým technologiím lze řešení snadno integrovat s existující zákaznickou infrastrukturou ICT. Součástí dodávky systému je i jeho přizpůsobení specifickým požadavkům zákazníka.

Simac Technik ČR

Simac Technik ČR, a.s. je systémový integrátor poskytující služby v ICT prostředí. Systémová integrace v podání naší společnosti je o komplexním řešení potřeb zákazníků, které integruje infrastrukturu, bezpečnost, management a aplikace.

Kontaktní informace firmy

Simac Technik ČR, a.s.
Radlická 740/113c
Avenir Business Park, budova B
158 00 Praha 5
Tel.: +420 283 061 281
Fax: +420 283 061 280

Silver Certified Partner





info@simac.cz
www.simac.cz