# VPN brána

V současnosti je použita dvojice VPN bran Interní informace

Požadavkem je renovovat toto připojení a zabezpečit ho v souladu se současnými bezpečnostními normami a dobrou praxí.

Požadujeme modernizaci dvojice VPN bran, které poběží v redundantní režimu active – standby. VPN mají být formou SSL VPN pro mobilní uživatele a IPSec pro přístup do vzdálených lokalit a k partnerům.

U vzdáleného přístupu mobilních uživatelů se očekává kontrola stavu koncového zařízení uživatele (NAC posture validation), který se připojuje pomocí SSL VPN. Tato kontrola bude realizována oproti stávajícím Cisco ISE. Bude požadováno možnost vložení koncového zařízení do karantény při nesplnění bezpečnostních kritérií a možnost změny VPN profilu koncové stanice s využitím funkcionality "change of authorization".

Součástí dodávky musí být i případné licence VPN pro uživatele a to v počtu minimálně pro 150 uživatelů. Řešení musí technicky zvládnout bez zhoršení odezvy minimálně dvojnásobný počet licencovaných uživatelů. Licence nesmí být vázány na fyzickou VPN bránu a v případě přechodu na jiný model stejného výrobce musí být přenositelné.

Součásti dodávky je implementace řešení a to takovým způsobem, aby zde byl soulad s aktuální verzí VKB.

* Řízení provozu
* Autentizace uživatelů a správců systému
* Logovaní
* Autorizace uživatelů a správců systému
* Použité šifrovací a hashovací algoritmy
* Vysoká dostupnost
* Atd.

Z hlediska počtu skupin pro RA VPN přístup jich bude cca. 10. V případě IPSec LAN to LAN tunelů jich bude cca. 5.

Součástí bude implementace VPN klientů na dodané koncové stanice (notebooky), které jsou na bázi Windows OS a Android, v dokumentaci bude potřebná podrobná konfigurace uvedena a navíc také pro operační systémy Linux a iOS . Zde se očekává funkcionalita VPN klientů, která zajistí, aby nebyl povolen žádný uživatelský provoz na síťové úrovni bez sestavené VPN. Po sestavení VPN tunelu se bude veškerý provoz směřovat do tohoto tunelu. Uživatelé následně budou komunikovat a to i včetně Internetové komunikace skrze bezpečnostní prvky, které jsou umístěny v centrální lokalitě.

Nastavené koncové stanice jsou součástí dodávky, jedna se o 4ks administrátorských notebooků a 1ks tabletu v konfiguraci uvedené níže v technických parametrech.

| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| --- | --- | --- |
| Počet zařízení v režimu HA Active-Standby | 2ks |  |
| Propustnost v ideálním prostředí | 900 Mbps |  |
| Propustnost v bežném multiprotokol prostředí | 800 Mbps |  |
| Počet souběžných relací ve stavové tabulce | 250 000 |  |
| Počet nových relací za sekundu | 20 000 |  |
| Počet přenesených packetů za 1s o velikosti 64 bytů | 700 000 |  |
| Propustnost při enkrypci VPN (3DES, AES) | 250 Mbps |  |
| Počet 10/100/1000 rozhraní | 8 |  |
| Počet zdojů DC pro jedno zařízení | 1 |  |
| Podpora IPSec - IKEv1 a IKEv2 | ANO |  |
| Minimální počet souběžný IPSec VPN tunelů pro L2L | 280 |  |
| Minimální počet souběžný SSL VPN tunelů pro remote access | 300 |  |
| Podpora vzdálených SSL VPN typu remote access | ANO |  |
| SSL VPN licence pro 150 uživatelů na minimálně 5 let | ANO |  |
| Pořadavek na podporu operačních systémů pro potřeby remote access SSL VPN klientů | Windows 7/8/10 (32 i 64 bit), Linux (32 i 64 bit), MacOS X (Intel), iOS, Android, Win Phone |  |
| Podpora vysoké dostupnosti v režimu active-standby i active-active | ANO |  |
| Možnost rozšíření o virtuální firewally | ANO, a to až 5 kontextů |  |
| Podpora autetizace pro "remote access" VPN přístupy | TACACS, RADIUS, LDAP, RSA, NT Domain, lokální databáze |  |
| Podpora dynamických směrovacích protokolů | RIPv1 (RFC1058), RIPv2 (RFC2453), OSPFv3 (RFC 2740), EIGRP (RFC 7868) |  |
| Plnohodnotný grafický management | ANO |  |
| Plnohodnotný CLI managment firewallu | ANO |  |
| Integrovaný grafický management jako součást firewallu | ANO |  |
| Podpora ověřování administrátora zařízení pomocí RADIUS a TACACS | ANO |  |
| Možnost přidělování práv administrátorům na úrovni jednotlivých příkazů | ANO |  |
| Logování provozu pomocí syslog | ANO |  |
| Logování provozu pomocí nekterého z těchto protokolů nebo jim podobných NetFlow, Jflow, NetStream, Cflowd, Rflow, AppFlow, sFlow apod. | ANO |  |
| Kontrola stavu koncového zařízení uživatele, který se připojuje pomocí SSL VPN oproti stávajícímu Cisco ISE, možnost vložení koncového zařízení do karantény při nesplnění bezpečnostních kritérií, možnost změny VPN profilu koncové stanice s využitím funkcionality "change of authorization". | ANO |  |
| SNMPv 1,2,3 | ANO |  |
| Minimální počet podporovaných VLAN | 100 |  |
| Podpora IPv6 (filtrování, stavový firewall) | ANO |  |
| IPv6 podpora RA i L2L VPN | ANO |  |
| Podpora IPv4 - NAT, PAT, Dynamický NAT | ANO |  |
| Podpora NAT v IPv6 - NAT64 | ANO |  |
| DHCPv4 a DHCPv6 relay | ANO |  |
| Aplikační inspekce pro protokoly | CTIQBE  DCERPC  DNS over UDP  FTP  GTP  H.323 H.225 and RAS  HTTP  ICMP  ILS (LDAP)  Instant Messaging (IM)  IP Options  MGCP  MMP  NetBIOS Name Server over IP  PPTP  RADIUS Accounting  RSH  RTSP  SIP  SKINNY (SCCP)  SMTP and ESMTP  SNMP  SQL\*Net  Sun RPC over UDP and TCP  TFTP  XDCMP  CTIQBE  DCERPC  DNS over UDP  FTP  GTP  H.323 H.225 and RAS  HTTP  ICMP  ILS (LDAP)  Instant Messaging (IM)  IP Options  MGCP  MMP  NetBIOS Name Server over IP  PPTP  RADIUS Accounting  RSH  RTSP  SIP  SKINNY (SCCP)  SMTP and ESMTP  SNMP  SQL\*Net  Sun RPC over UDP and TCP  TFTP  XDCMP |  |
| Aplikační inspekce pro IPv6 prostředí | DNS FTP HTTP ICMP SIP SMTP IPsec pass-through IPv6 |  |
| Popdora NAT64 pro inspekce | DNS FTP HTTP ICMP |  |
| Podpora na HW, SW a licencí 5 let | ANO |  |
| Zahoření a hardening zařízení dle „best practice“ a VKB | ANO |  |
| Návrh a provedení akceptačních testů | ANO |  |
| Fyzická instalace | ANO |  |
| Konfigurace zařízení dle úvodního popisu | ANO |  |
| Low level a high level design řešení | ANO |  |
| Notebook | 4ks |  |
| Notebook - OS | Windows 10 Professional 64bit CZ |  |
| Notebook - záruka | 5 let NBD onsite, hlášení závady 24/7, záruka garantována výrobcem |  |
| Notebook - CPU | i5 poslední generace |  |
| Notebook - displej | nelesklý, dotykový,13.3- 14", FHD 1920x1080, LED podsvícený |  |
| Notebook - VGA | integrovaná, poslední generace |  |
| Notebook - RAM | 16GB, min. 2 sloty |  |
| Notebook - HDD | SSD 512GB, záruka s notebookem |  |
| Notebook - kamera | ANO |  |
| Notebook - mikrofon | ANO |  |
| Notebook - Bluetooth | 4.2 |  |
| Notebook - WiFi | 2x2, 802.11ac |  |
| Notebook - připojení 4G, LTE (Evropa) | ANO, integrovaná |  |
| Notebook - LAN | 10/100/1000 Ethernet, ne přes redukci |  |
| Notebook - čtečka kontaktních karet pro dvoufázovou autentizaci | integrovaná |  |
| Notebook - TPM čip | ANO |  |
| Notebook - vPro | ANO |  |
| Notebook - klávesnice | CZ, EN, podsvícená |  |
| Notebook - baterie | 65WHr, 3 roky záruka |  |
| Notebook - váha bez adaptéru | max. 1,5 kg |  |
| Notebook - adaptér | 90W, 3 pin |  |
| Notebook - vstup/výstup | HDMI 1.4, USB 3.1, RJ-45, audio in/out - nejsou dovoleny redukce |  |
| Notebook - brašna | ANO, popruh přes rameno |  |
| Tablet | 1ks |  |
| Tablet - OS | min. Google Android 7.1 |  |
| Tablet - CPU | min. 6 jader a frekvence 1.4GHz |  |
| Tablet - úhlopříčka displeje | 7"-8" |  |
| Tablet - rozlišení displeje | 1280x800 |  |
| Tablet - RAM | 3GB |  |
| Tablet - úložiště flash | 16GB |  |
| Tablet - přídavná paměťová karta | SD, SDXC |  |
| Tablet - velikost paměťové karty | 64GB |  |
| Tablet - baterie | 4400mAh, vyjímatelná |  |
| Tablet - připojení | 3G, 4G LTE, WIFI 802.11ac 2.4 a 5GHz, BlueTooth 4.2 |  |
| Tablet - další funkce | GPS, Glonass, pohybový senzor, gyroskop, digitální kompas |  |
| Tablet - fotoaparát | přední i zadní, natáčení videa |  |
| Tablet - nahrávání videa | Full HD |  |
| Tablet - hmotnost | max. 450 g |  |
| Tablet - odolnost | krytí IP68 |  |