Standard připojení k síti Internet

Verze 1.12

Změny:

Datum vydání	Verze	Změna proti předchozí verzi	Změnil (jméno)
21.6.2006	0.80	První draft	Libor Šmíd
29.6.2006	1.00	Úprava do finální verze	Milan Zapletal
15.8.2006	1.10	Doplněna kapitola 3.2	Libor Šmíd
16.7.2015	1.11	Úprava celého dokumentu	Milan Zapletal
3.1.2016	1.12	Úprava dokumentu	Jan Boháč

Obsah

Odstr

1. Úvod

Tento dokument popisuje základní konfiguraci připojení ČSSZ do prostředí internetu.
Standard definuje způsob komunikace koncových stanic, serverů a infrastrukturních služeb s internetem. V dokumentu nejsou řešeny přístupy aplikačních serverů umístěných v DMZ. K tomu účelu slouží projektová dokumentace k IKR-DMZ.
Tento dokument patří mezi schválené standardy ČSSZ a je pro dodavatele ČSSZ závazný.

2. Proxy TMG

Připojení uživatelů k síti internet je realizováno prostřednictvím proxy serverů na bázi produktu Microsoft Forefront Threat Management Gateway 2010. Celá soustava je postavena redundantně v lokalitách (Křížová 25, Trojská 13) a skládá se ze dvou upstream proxy v DMZ, dvou downstream proxy a mgmt serverů v core. Na straně klienta je používám Internet explorer, který je pomocí doménové skupinové politiky směrován na content switch, předřazený před oba downstream proxy servery. Ten rozkládá zátěž mezi lokalitami Trojská 13, ústředím Křížová 25 a současně zajišťuje redundantnost provozu. To znamená, že v případě vypnutí (nedostupnosti) jedné z downstream proxy se webový provoz přesměruje na druhou lokalitu. Proxy soustava zajišťuje přístup pro webové aplikace na stránky v Internetu, Govbone a CMS. Nikoliv tedy na webové aplikace v interních doménách *.cssz.cz.

2.1 Rozdělení přístupů

Neomezený webový přístup do Internetu je nastaven pro skupiny uživatelů z řad pracovníků IT, vedoucích zaměstnanců a managementu. Řízení přístupu se provádí přiřazením uživatelských účtů do patřičných bezpečnostních skupin v Active Directory.
Omezený webový přístup do Internetu je nastaven pro povolené domény a destinace všem zbylým uživatelům přihlášeným v doméně cssz.cz.
Speciální webové přístupy do Internetu pro aplikace, wifi, update serverů jsou nastaveny jako anonymní. Pravidly jsou rozčleněny podle zdrojových adres a cílových destinací formou domén, url adres nebo IP adres.

3. Firewall

Privátní síť ČSSZ je od ostatních externích sítí, včetně Internetu oddělena dvojicí clusterovaných firewallů na bázi produktu SecurePlatform NG od firmy CheckPoint. Firewallová soustava je tvořena dvojicí modulů pracujících v režimu sdílené zátěže. Jsou řízeny jedním SmartCenter serverem, který zároveň slouží jako úložiště monitorovacích logů.

Firewall na základě definovaných pravidel zabezpečuje komunikaci mezi následujícími síťovými rozhraními:

1. Eth0 - síť privátní ČSSZ
2. Eth1 - síť Govbone (MPSV, MFCR)
3. Eth2 - síť demilitarizované zóny (DMZ)
4. Eth3 - propojení nutné v režimu sdílené zátěže
5. Eth4 – GovNet (nevyužívá se)
6. Eth5 - síť Internet

3.1 DMZ infrastrukturní služby

Demilitarizované zóny na obou lokalitách slouží jako bezpečnostní perimetr pro aplikační, webové a poštovní služby publikované do Internetu:

- SMTP služby – poštovní Trend Micro servery
- DNS služby – DNSEC servery
- Webové služby - LPS portál, PCBO objednávky
- Aplikační služby – App GŘ MFCR
- PKI služby – Publikační server crl pro VPN
- Proxy služby – Upstraem proxy servery
- Citrix – Netscaler servery
- Symantec – LU servery

3.2 Přístup na Internet z aplikační vrstvy

Přístup na Internet z vrstvy aplikačních serverů je možný pouze prostřednictvím B2B kanálu zakončeném na aktivním prvku Cisco ASA v DMZ. Provoz z aplikačních serverů do Internetu je jednosměrný a je omezen na destinace, které jsou zaneseny v pravidlech na firewallech.