



BOSNIA AND HERZEGOVINA
MINISTRY OF FINANCE
AND TREASURY

Broj: 01-08/3-02-3-7167-1/ 10
Sarajevo, 16.09.2010. godine

PRAVILNIK PRISTUPA UDALJENIH KORISNIKA IS SISTEMU

1.0. SVRHA PROCEDURE

Svrha ove procedure je da pruži uputstvo za pristup udaljenih korisnika Informacionom sistemu Ministarstva finansija i trezora BiH (u daljem tekstu: IS sistem MFT).
Udaljeni pristup IS sistemu MFT obavlja se na dva načina, i to:

1. preko konekcije „Frame Relay“ ili iznajmljene stalne veze, i
2. preko „IPSec“ ili „L2TP Virtual Private network „(VPN) konekcije.

2.0. OBIM

Ova procedura se primjenjuje na sve zaposlenike i namještenike MFT, lica angažovana po ugovoru, konsultante, privremeno zaposlene i druge zaposlene, uključujući i druge koji koriste usluge pristupa IS sistemu MFT putem konekcije, da pristupe mreži (u daljem tekstu: korisnici).

Ova procedura se odnosi na implementaciju VPN konekcije usmjerene kroz „router“ MFT.

Ova procedura se odnosi na implementaciju VPN konekcije usmjerene kroz „firewall“ MFT.

3.0. PROCEDURA

Korisnici mogu koristiti uslugu konekcije samo ukoliko je ista prethodno odobrena od ovlaštene osobe ispred MFT, a to je voditelj odjela za upravljanje IS sistemom MFT.

3.1. Procedura korištenja konekcije usmjerene kroz „router“ MFT.

3.1.1. Sva oprema spojena na konekciju usmjerenu kroz „router“ predstavlja ekstenziju IS sistema MFT, te stoga dvostruki „tunneling“ **nije dozvoljen**.

Samo jedna mrežna konekcija je dozvoljena, a to podrazumijeva da radna stanica ili laptop (u daljem tekstu: terminal), koji se konektuju na IS sistem MFT **ne smiju imati fizički pristup** Internetu ili nekoj drugoj kompjuterskoj mreži (np. LAN ili WAN mreži).

3.1.2. Korisnik će automatski biti diskonektovan sa IS sistema MFT ukoliko 60 (šezdeset) minuta ne bude aktivan. Da bi se ponovo konektovao na IS sistem MFT korisnik se mora ponovo prijaviti (logirati).

- 3.1.3. Na terminalu, **administratorska prava ima samo** mrežni administrator odjela za upravljanje IS sistemom MFT ili ovlaštena osoba od strane mrežnog administratora (u daljem tekstu: administrator mreže).
- 3.1.4. Servis na strani korisnika postavlja administrator mreže.
- 3.1.5. Za konfiguraciju opremu korištene za uspostavljanje konekcije zadužen je administrator mreže.
- 3.1.6. Za konfiguraciju mrežnih printera korištenih pri konekciji zadužen je administrator mreže.
- 3.1.7. Administrator mreže kod korisnika koji koriste konekciju treba da obezbijedi da terminal posjeduje zadnji "update" AntiVirusnog softvera koji spada u "korporate standard edition" softver.
- 3.1.8. Konekcija je onemogućena sve dok korisnik ne uputi zahtjev administratoru mreže i administrator mreže uspostavi konekciju. Po uspostavljanju konekcije, konekcija je usmjerena kroz "router" 24 (dvadeset i četiri) sata svakog dana u sedmici.
- 3.1.9. Ukoliko korisnik mijenja lokaciju ili ne postoji više potreba za konekcijom, a konekcija mu je omogućena, obavezan je uputiti pismeni zahtjev MFT za dislokaciju ili ukidanje linka. MFT po primitku navedenog zahtjeva obezbjeđuje seljenje ili ukidanje linka navedenog korisnika.
- 3.1.10. Administrator mreže je obavezan da prati preko „log fajla“ sve bitne informacije u vezi sa konekcijama (npr.: nastajanje i trajanje prekida, uočeni pokušaj upada „intrudora“ i dr.) i da redovno informiše svog pretpostavljenog.
- 3.1.11. Korisnici koji koriste konekciju moraju se pridržavati Pravilnika za upotrebu IS sistema MFT broj 01-08-02-1-1562-1/09.

3.2. Procedura korištenja VPN konekcije usmjerene kroz „vatrozid“ MFT.

- 3.2.1. Sva oprema spojena na VPN konekciji je usmjerena kroz „vatrozid“ i predstavlja ekstenziju IS sistema MFT, te stoga dvostruki „tunneling“ **nije dozvoljen**. Samo jedna mrežna konekcija je dozvoljena, a to podrazumijeva da radna stanica ili laptop (u daljem tekstu: terminal), koji se konektuju na IS sistem MFT **ne smiju imati fizički pristup** nekoj drugoj kompjuterskoj mreži (npr. LAN ili WAN mreži).
- 3.2.2. Kada je korisnik aktivno spojen putem VPN konekcije sav saobraćaj od terminala prolazi kroz VPN „tunneling“.
- 3.2.3. VPN "gateway" servis postavlja administrator mreže.
- 3.2.4. Za konfiguraciju terminala kojeg korisnik koristi za uspostavljanje VPN konekcije zadužen je korisnik.
- 3.2.5. Konfiguraciju terminala korisnik konfigurira u skladu sa VPN zahtjevima uspostavljenim IS sistemom MFT, a na temelju parametara dobivenih od administratora mreže.
- 3.2.6. Korisnici koji koriste VPN konekciju moraju obezbijediti da terminal posjeduje zadnji "update" AntiVirusnog softvera koji spada u "korporate standard edition" softver, i to "update" najkasnije dan prije uspostavljanje VPN konekcije.

- 3.2.7. Korisnik je obavezan administratoru mreže pismeno, slanjem e-mail-a, ili eventualno u slučaju hitnosti, najaviti termin i vrijeme kada namjerava da koristi resurse IS sistema MFT, tj. da koristi VPN konekciju.
- 3.2.8. Administrator mreže je obavezan da prati sve bitne informacije u vezi sa VPN konekcijama kroz „log fajlove“ (npr.: nastajanje i trajanje prekida, uočeni pokušaj upada „intrudora“ i dr.) i da redovno informiše svog pretpostavljenog.
- 3.2.9. Korisnik će automatski biti diskonektovan sa IS sistema MFT ukoliko 20 (dvadeset) minuta ne bude aktivan. Da bi se ponovo konektovao na IS sistem MFT korisnik se mora ponovo prijaviti („logirati“).
- 3.2.10. Korisnici koji koriste VPN konekciju moraju se pridržavati Pravilnika za upotrebu IS sistema MFT broj 01-08-02-1-1562-1/09.

4.0. PROVOĐENJE

Ukoliko se korisnik ne pridržava navedenih procedura, njegova upotreba udaljene konekcije će biti ukinuta, a protiv njega će se pokrenuti procedura disciplinske mjere.

5.0. DEFINICIJE

| Termin | Definicija |
|---------------------|--|
| korisnik | lice koja se s udaljene lokacije konektuje na IS sustav MFT |
| terminal | računar ili laptop |
| IS sustav MFT | Informacionom sistemu Ministarstva finansija i trezora BiH |
| VPN konekcija | Virtual Private Network konekcije |
| Administrator mreže | Administrator mreže odjela za upravljanje IS sistemom MFT ili ovlaštena osoba od strane Administratora mreže |

MINISTAR

Dragan Vrankić