Ver	Datum	Avtor	Opis	Podjetje
6	31.03.2014	Gregor Kosmina	Verzija 1.07.SI	Panteon Group d.o.o.

Namen

Dokument opisuje zahteve potrebne za vzpostavitev VPN povezave s požarno pregrado poslovnega omrežja Panteon.net®.

Tehnični opis

1.1 Tehnične zahteve za vzpostavitev VPN povezave med požarnima pregradama (site-to-site VPN)

VPN povezava se izvede med požarno pregrado Panteon.net in požarno pregrado oddaljenega partnerja. VPN povezava je izvedena z uporabo IKE tehnologije za vzpostavitev povezave in IPSEC tehnologijo za šifriranje podatkov. Identifikacija oddaljene požarne pregrade se izvaja s skupnim geslom. Vzpostavitev VPN povezave zahteva uskladitev parametrov za IKE fazo in uskladitev parametrov za IPSEC fazo.

Zahteve za IKE fazo (FAZA1):

Algoritem za šifriranje:	3DES ali AES-256
Algoritem za zagotovitev integritete:	MD5 ali SHA1 ali SHA-256
Diffie-Hellman skupina:	group2 (1024 bitov) ali group5 (1536)
IKE SA življenski čas:	1440 minut

Zahteve za IPSEC fazo (FAZA2):

Algoritem za šifriranje:	3DES ali AES-256
Algoritem za zagotovitev integritete:	MD5 ali SHA1 ali SHA-256
Poudarjena zaupnost (Perfect Forward Secrecy):	DA
Diffie-Hellman skupina:	group2 (1024 bitov) ali group5 (1536)
IPSEC SA življenski čas:	7200 sekund
Stiskanje podatkov (compression):	možno

Skupno geslo se vedno dogovori osebno oz. po telefonu.

1.2 Tehnične zahteve za vzpostavitev VPN povezave z VPN odjemalcem

Pravila varnostne politike na strani požarne pregrade oddaljenega uporabnika, ki morajo biti omogočena za dostop in pravilno delovanje VPN odjemalca:

1. **Odjemalec se nahaja v LAN omrežju za požarno pregrado, ki izvaja maskiranje (NAT). Potrebna pravila na požarni pregradi :**
   a. omogočen protokol UDP na vratih 500 (IKE) proti internetu
   b. omogočen protokol TCP na vratih 500 (IKE over TCP) proti internetu
   c. omogočen protokol UDP na vratih 2746 (šifrirani podatki)
   d. omogočen protokol UDP na vratih 4500 (za IKE in IPSEC - NAT-T)
   e. omogočen protokol TCP na vratih 264 (prenos osnovnih podatkov za vzpostavitev šifriranja)

2. **Odjemalec se povezuje na internet direktno in uporablja "personal firewall". Potrebna pravila:**
   a. omogočen protokol UDP na vratih 500 (IKE)
   b. omogočen protokol ESP (50)
   c. omogočen protokol TCP na vratih 264 (prenos osnovnih podatkov za vzpostavitev šifriranja)

1.3 Omejitve za vzpostavitev VPN povezave z VPN odjemalcem

1. **Checkpoint SecureRemote VPN odjemalca je možno instalirati le na MS Windows 32 bit operacijske sisteme**

Izvedba

Na osnovi obrazca »Vzpostavitev VPN povezave z oddaljenim omrežjem (site-to-site)« ali obrazca »Vzpostavitev VPN povezave s SecuRemote odjemalcem« se pridobijo podatki potrebni za vzpostavitev oddaljene VPN povezave.

Izpolnjen dokument **Vzpostavitev VPN povezave z oddaljenim omrežjem** ali **Vzpostavitev VPN povezave z VPN odjemalcem** pošljite na naslov:

Panteon Group d.o.o
g. Gregor Kosmina
gregor@panteongroup.com

ali na FAX 05/6397 632