e-SERVICE PANTEON.NET® e-ARCHIVE

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

Purpose

This document is describing the requirements needed for the establishment of the VPN connection with the firewall of the business network **Panteon.net®**.

Technical description

1.1 Technical requirements for the establishment of the VPN connection

VPN connection is implemented with the use of IKE technology for the establishment of the connection and IPSEC technology for the data encryption. The identification of the remote firewall is being executed by the common password. The establishment of the VPN connection is requiring the reconciliation of parameters for the phase IKE and the reconciliation of parameters for the phase IPSEC.

Requirements for the phase IKE (PHASE1):

Algorithm for encryption:	3DES or AES-256
Algorithm for the assurance of integrity:	MD5 or SHA1 or SHA256
Diffie-Hellman group:	group2 (1024 bits) or group5 (1536)
IKE SA life cycle:	1440 minutes

Requirements for the phase IPSEC (PHASE2):

Algorithm for encryption:	3DES or AES-256
Algorithm for the assurance of integrity:	MD5 or SHA1 or SHA256
Enhanced confidentiality (Perfect Forward Secrecy):	YES
Diffie-Hellman group:	group2 (1024 bits) or group5 (1536)
IPSEC SA life cycle:	7200 seconds
Data compression:	possible

The common password is being always agreed personally or via telephone.

1.2 Technical requirements for establishment of VPN connection with VPN client

Security rules policy on side of the remote user firewall which have to be enabled for access and proper activity of SecuRemote client:

1. **A client is in LAN network, located behind the firewall which is executing masking (NAT). Required rules on a firewall:**
   a. enabled protocol UDP on port 500 (IKE) towards internet
   b. enabled protocol TCP on port 500 (IKE over TCP) towards internet
   c. enabled protocol UDP on port 2746 (encrypted data)
   d. enabled protocol UDP on port 4500 (for IKE and IPSEC – NAT-T)
   e. enabled protocol TCP on port 264 (transfer of basic data for encryption establishment)

2. **A client is connecting directly on Internet and uses »personal firewall«. Required rules:**
   a. enabled protocol UDP on port 500 (IKE)
   b. enabled protocol ESP (50)
   c. enabled protocol TCP on port 264 (transfer of basic data for encryption establishment)

1.3 Limitations for establishment of VPN connection with SecuRemote VPN client

1. **Only on MS Windows 32 bit operating systems is possible to install a Checkpoint SecuRemote VPN client**

Implementation

Based on the form »Establishment of the VPN connection with the remote network« data required for the establishment of the remote VPN connection are obtained.
Fulfilled form **Establishment of VPN connection with remote network** or **Establishment of VPN connection with SecuRemote VPN client** send to address:

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

or FAX 05/6397 632