

Параметри за конфигурација на IPSec VPN

09/21/2023 20:31:58

[FAQ Article Print](#)

Category:	VDC::Edge Gateway	Votes:	0
State:	public (all)	Result:	0.00 %
Language:	mk	Last update:	15:40:18 - 10/08/2021

Keywords

edge ipsec

Symptom (public)

Параметри за конфигурација на IPSec VPN на Edge Gateway со друг уред.

Problem (public)

Solution (public)

Доколку се воспоставува Site-to-Site IPSec tunnel со користење на IKE верзија 1, параметри кои се користат за воспоставување на IPSec VPN меѓу Edge Gateway и друг уред се:

The IKE Phase 1 parameters:

- IKE Version: 1
- Main mode
- Encryption: AES 256
- Digest: SHA-1
- Diffie-Helman Group: DH2 (MODP1024 bits)
- Pre-shared secret (To be exchanged separately)
- SA lifetime of 28800 seconds (eight hours) with no Kbytes rekeying
- ISAKMP aggressive mode disabled

The IKE Phase 2 parameters:

- Encryption: AES 256
- Digest: SHA-1
- ESP tunnel mode
- Diffie-Helman Group: DH2 (MODP1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no Kbytes rekeying

Доколку се воспоставува Site-to-Site IPSec tunnel со користење на IKE верзија 2, параметри кои се користат за воспоставување на IPSec VPN меѓу Edge Gateway и друг уред се:

The IKE Phase 1 parameters:

- IKE Version: 2
- Main mode
- Encryption: AES 256
- Digest: SHA-256
- Diffie-Helman Group: DH14 (MODP2048 bits)
- Pre-shared secret (To be exchanged separately)
- SA lifetime of 28800 seconds (eight hours) with no Kbytes rekeying
- ISAKMP aggressive mode disabled

The IKE Phase 2 parameters:

- Encryption: AES 256
- Digest: SHA-256
- ESP tunnel mode
- Diffie-Helman Group: DH14 (MODP2048 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no Kbytes rekeying