SIA Tet interneta datplūsmas pārvaldības pasākumi un to ietekme

SIA Tet neveic datplūsmas palēninašanu vai ierobežošanu, lai izvairītos no tīkla pārslodzēm. Pat maksimālās noslodzes periodos interneta datplūsma netiek palēnināta vai kavēta nevienam lietojumam.

SIA Tet veic interneta pakalpojumu datplūsmas pārvaldības pasākumus tikai, lai saglabātu tīkla, tīklā sniegto pakalpojumu un galiekārtu integritāti, drošību un nepārtrauktību. Veiktie datplūsmas pārvaldības pasākumi ir sekojoši:

1. Tiek bloķēts Vienkāršā pasta pārsūtīšanas protokola (SMTP) 25. ports privātpersonu pakalpojumu interneta datplūsmām un juridisko personu pakalpojumu ar dinamiskām IP adresēm datplūsmām izejā uz starptautisko tīklu. Tas tiek darīts drošības apsvērumu dēļ, jo 25. porta protokols ir fundamentāli nedrošs un elementāri izmantojams ļaunprātīgos nolūkos. SIA Tet pielietotā 25. porta bloķēšana neierobežo klientam interneta pakalpojuma lietošanu, bloķēšana neliedz galalietotājiem piekļuvi nevienam pakalpojumam, bet aizsargā klientu no IP adreses nonākšanas melnajā sarakstā un no pakalpojumu pārtraukuma. Ja klients izmanto e-pasta serveri ārzemēs, tad to nevarēs izdarīt izmantojot 25.portu, bet izmantojami SMTP porti 587 vai 465.

2. Tiek bloķēts Pārraides vadības protokola (TCP) 53.ports ienākošai datplūsmai no starptautiskā tīkla uz SIA Tet dinamiskajām IP adresēm. Tas tiek darīts drošības apsvērumu dēļ, lai nevarētu Tet klientu kompromitētās galiekārtas izmantot DDoS uzbrukumu organizācijai. Šī 53. porta bloķēšana neļauj izmantot Tet pieslēgumu ar dinamisko IP adresi DNS servera pakalpojumu sniegšanai lietotājiem ārzemēs. Lai izvairītos no šī ierobežojuma, klientam ir jāpieprasa Tet statiska IP adrese. SIA Tet pielietotā 53. porta bloķēšana neierobežo klientam interneta lietošanu, bloķēšana neliedz galalietotājiem piekļuvi nevienam pakalpojumam, bet aizsargā klientu no viņa galiekārtas izmantošanas DDoS uzbrukumos.

3. Tiek bloķēts Lietotāja Datogrammu Protokola UDP (User Datagram Protocol) 1900.ports interneta piekļuves pakalpojumu datplūsmām no dinamiskajām IP adresēm. Tas tiek darīts drošības apsvērumu dēļ, lai ļaundari nevarētu galalietotājiem nezinot to galiekārtas un privāto tīklu iekārtas izmantot DDoS uzbrukumiem. SIA Tet pielietotā UDP 1900.porta bloķēšana neierobežo klientiem interneta lietošanu, bet aizsargā klientus no viņu iekārtu izmantošanas DDoS uzbrukumos. Porta bloķēšana liedz galalietotājam izmantot "Universal Plug and Play" (UPnP) tehnoloģiju publiskajā internetā, kur tā nenodrošina nekādu noderīgu funkcionalitāti.

UPnP tehnoloģija ir paredzēta izmantošanai iekšējos tīklos (LAN) un 1900.porta bloķēšana neietekmē UPnP izmantošanu galalietotāja iekšējā tīklā (LAN).

SIA Tet piemērotie datplūsmas pārvaldības pasākumi nepasliktina interneta piekļuves pakalpojumu kvalitāti, neskar abonentu privātumu un personas datu aizsardzību.

Saskaņā ar valsts kompetento iestāžu lēmumiem Tet klientiem tiek ierobežota piekļuve konkrētām tīmekļa vietnēm (domēna vārdam vai interneta protokola adresei).