SOLUTIE DE FILTRARE A CONTINUTULUI TRAFICULUI DE INTERNET

I.D.: 34307268

Data publicarii	05.03.19	Coduri CPV	48200000-0
Termenul limita pentru depunere:	18.03.19		

Descriere: S.N.T.G.N. Transgaz S.A. utilizează o soluţie care asigură filtrarea conţinutului traficului de internet şi monitorizează operaţiunile desfăşurate de utilizatori în timpul navigării acestora pe internetul pus la dispoziţie de către companie. Acesta este este implementată într-o arhitectură distribuită. Soluţia actuală este în funcţiune din anul 2010 şi trebuie înlocuită dar orită: vechimii acesteia (pentru a face faţă noilor tipuri de atacuri informatice) si a creşterii numărului de utilizatori. Soluţia de filtrare a conţinutului traficului de internet trebuie să: - asigure securizarea, monitorizarea şi controlul navigării şi operaţiunilor de download efectuate de utilizatori; - permită aplicarea politicilor de navigare şi al operaţiunilor de download independent de sistemul de operare al staţiilor de lucru şi pentru toate browser-ele utilizate (IE, Edge, GoogleChrome, Firefox, etc.); - se integreze cu Microsoft Active Directory pentru identificarea utilizatorilor (autentificarea utilizatorilor prin SSO folosind IWA) sau a grupurilor de utilizatori şi utilizarea acestora în crearea politicilor de navigare; - să includă posibilitatea activării/dezactivării metodei de identificare a IP-ului de origine: X-Forwarded-For; - sa permită folosirea aceloraşi politici definite mai multor grupuri de utilizatori; - permită crearea de politici de navigare care să controleze accesul la diverse categorii de pagini web pe utilizator, pe grup de utilizatori, pe IP; - permită crearea de politici de navigare pe baza de timp, volum de date accesate; - permită managementul accesului la internet, prin implementarea politicilor de navigare. În urma aplicării politicilor de navigare va fi blocat accesul la pagini web neagreate prin politica companiei sau la pagini web care au conţinut maliţios prin scanarea acestora si filtrarea URL; - să permită inspecţia traficului criptat (HTTPS); - includă posibilitatea filtrării paginilor web pe baza: a) unor categorii ale paginii web (ex. Alcohol, Dating, Gambling, Nudity, Pornography, Travel, etc.); b) reputaţiei acestora; c) unor categorii definite de utilizator; - includă filtre de tip MIME pentru fişierele pe care utilizatorul încearcă să le downloadeze; - includă opţiuni de filtrare pe bază de URL, cuvinte cheie, tipuri de fişiere; - includă mecanisme de blocare a conexiunilor la servicii de web - proxy şi tunelare; - permită blocarea de Java Applets, Cookies, Active X; - permită blocare unor tipuri de fişiere la upload; - permită blocarea site-urilor cu conţinut de malware, phishing, pharming; - determine reputaţia site-urilor accesate în timp real; - permită alocarea lăţimii de bandă pe bază de categorie şi prioritizarea navigării (ex: navigare http/https să aibă prioritate faţă de streaming video/audio); - permită alocarea de cote (zilnice, lunare) bazate pe categorii definite (ex: definire cota de trafic pe grup de utilizatorii AD pentru streaming gen YouTube); - permită un control granular asupra aplicaţiilor de tip social web (ex: aplicaţii/jocuri pe facebook); - includă filtre de tip protocol pe baza cărora să se recunoască şi să filtreze aplicaţii de tip messenger, social media, ftp, etc. - poată distinge între navigarea propriu-zisă pe anumite pagini web şi cereri parazite de navigare (cum ar fi anunţuri de tip Web Advertisments, referiri la platforme de socializare prin componente care apar pe paginile web: Butoane “Share”, “Like” , “Comment” etc.) - permită minim următoarele moduri de navigare: a) fără atenţionare; b) cu atenţionare; c) blocat; - fie administrată dintr-o interfaţă web; - permită definirea de roluri pentru segregarea administrării soluţiei; - Rapoartele în timp real vor permite vizibilitate completă asupra navigării, politicilor aplicate, clasificării conţinutului, aplicaţiilor accesate şi asupra activităţilor desfăşurate de utilizatori; - furnizeze rapoarte asupra activităţii istorice de navigare, lăţimii de bandă utilizate; - permită filtrarea datelor pe baza cărora se creează/rulează rapoarte (ex: Utilizator/IP/Grup/Website/Categorie WEB/Aplicaţie/Politica de navigare/Tip de conţinut, perioadă de timp, etc.); - fie instalată pe echipamente hardware dedicate, iar operaţiunile de filtrare să se execute local; - actualizeze periodic atât module de filtrare a conţinutului (categorii, reputaţii, etc.) cât şi modulele de verificare conţinut maliţios; Cerinţele tehnice de mai sus sunt minimale. Ofertantul poate prezenta orice alte facilităţi suplimentare care să îmbunătăţească şi să eficientizeze soluţia. Scopul acestei soluţii este : - îmbunătăţirea securităţii sistemelor TI din intranetul Transgaz care sunt accesate de utilizatori care accesează pagini web din internet; - scanare anti malware a conţinutului paginilor web pe care utilizatorii Transgaz le accesează; - o gestionare mai eficientă a lărgimii de bandă alocate navigării pe internet;