Technetic

UAB Technetic, Rugių g. 2, LT-08418 Vilnius, Lietuvos Respublika
Įmonės kodas 302948583, PVM mokėtojo kodas LT100007395612
Telefonas (8-5) 2616990, faksas (8-5) 2121187. www.technetic.lt
A/s LT417300010134056325, AB Swedbank, banko kodas 73000

Valstybinei teismo medicinos tarnybai

PASIŪLYMAS
DĖL TINKLO PERIMETRO APSAUGOS

2016-11-10 Nr.01
Vilnius

Tiekėjo pavadinimas /Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių pavadinimai/	UAB „Technetic“
Tiekėjo adresas /Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių adresai/	Rugių g. 2, Vilnius
Asmens, pasirašiusio pasiūlymą saugiu elektroniniu parašu, vardas, pavardė, pareigos	Gytis Šakys
Telefono numeris	+370 655 40376
Fakso numeris	
El. pašto adresas	gytis@technetic.lt

Pastaba: pildoma, jei tiekėjas ketina pasitelkti subtiekėją (-us)

Subtiekėjo (-ų) pavadinimas (-ai)	
Subtiekėjo (-ų) adresas (-ai)	
Įsipareigojimų dalis (procentais), kuriai ketinama pasitelkti subtiekėją (-us)	

Šiuo pasiūlymu pažymime, kad sutinkame su visomis pirkimo sąlygomis, nustatytomis pirkimo dokumentuose (jų paaiškinimuose, papildymuose).

Mes siūlome šias Prekes:

Eil. Nr.	Prekių pavadinimas, gamintojas, modelis.	Kiekis	Mato vnt.	Vieneto kaina, Eur su PVM	Kaina, Eur be PVM	Kaina, Eur su PVM
1	2	3	4	5	6	7
1.	Astaro unifikuotos tinklo perimetro apsaugos SG330 licencija 12 mėn.	1	Vnt.	8399,00	6941,32	8399,00
					IŠ VISO (bendra pasiūlymo kaina)	

Pasiūlymo kaina Eur su PVM (raštu) Aštuoni tūkstančiai trys šimtai devyniasdešimt devyni Eur 00 cnt.

Technetic

UAB Technetic, Rugių g. 2, LT-08418 Vilnius, Lietuvos Respublika
Įmonės kodas 302948583, PVM mokėtojo kodas LT100007395612
Telefonas (8-5) 2616990, faksas (8-5) 2121187. www.technetic.lt
A/s LT417300010134056325, AB Swedbank, banko kodas 73000

Kartu su pasiūlymu pateikiami šie dokumentai:

Eil.Nr.	Pateiktų dokumentų pavadinimas	Dokumento puslapių skaičius
1.	Techninė specifikacija	18 psl.

Ši pasiūlyme nurodyta informacija yra konfidenciali, perkančioji organizacija šios informacijos negali atskleisti tretiesiems asmenims:

Eil.Nr.	Pateikto dokumento pavadinimas (rekomenduojama pavadinime vartoti žodį „Konfidencialu“)	Dokumentas yra įkeltas šioje CVP IS pasiūlymo lango eilutėje („Prisegti dokumentai“ arba „Kvalifikaciniai klausimai“ prie atsakymo į klausimą)

Pastaba. Tiekėjui nenurodžius, kokia informacija yra konfidenciali, laikoma, kad konfidencialios informacijos pasiūlyme nėra.

Projektų vadovas		Gytis Šakys
(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas)	(Parašas)	(Vardas ir pavardė)

Technetic

UAB Technetic, Rugių g. 2, LT-08418 Vilnius, Lietuvos Respublika
Įmonės kodas 302948583, PVM mokėtojo kodas LT100007395612
Telefonas (8-5) 2616990, faksas (8-5) 2121187. www.technetic.lt
A/s LT417300010134056325, AB Swedbank, banko kodas 73000

Pasiūlymo
1 priedas

Techninė specifikacija

Siūlomas Prekės visiškai atitinka pirkimo dokumentuose nurodytus reikalavimus ir jų savybės tokios:

Eil. Nr.	Parametras	Reikalaujama minimali reikšmė	Atitikimas reikalavimui (nurodyti konkretų techninį parametrą arba aprašymą, arba pateikti nurodytus dokumentus)
		Ugniasienės (paketų filtro) funkcionalumo reikalavimai	
	Taisyklių / Politikos redaktoriui		
1.		Privalo taikyti šiuos veiksmus- priimti/ atmesti / blokuoti	√
2.		IP ir MAC adresais paremtas filtravimas	√
3.		Turi blokuoti pagal kilmės šalį (valstybę): Galimybė nurodyti blokuojamos šalies srauto kryptį (įeinančiam/išeinančiam) srautui Galimybė nustatyti išimtis	√
4.		Registrų įjungimas/išjungimas taisyklei	√
5.		Galimybė aprašyti/įvardinti kompiuterius, tinklus ir servisus (tinklo objektai/paslaugų objektai)	√
6.		Komentarai gali būti pridedami visiems objektams ir saugumo politikoms/nustatymams	√
7.		Turi būti galimybė pridėti komentarus su specialiais simboliais (pav: ä, ö, į, ž)	√
8.		Privaloma galimybė apjungti objektus į grupes	√
9.		Galimybė politikas rūšiuoti pagal spalvines koduotes	√
10.		Galimybė pridėti komentarus kiekvienai taisyklei	√
11.		Reikalavimai laiku paremtoms taisyklėms: vienkartinis aktyvavimas; pasikartojantis aktyvavimas.	√
12.		Taisyklės turi būti taikomos "Vartotojų objektams" su dinaminiais IP adresais: • Nuotoliniu būdu prisijungiantiems vartotojams; • Vartotojams naudojantiems autentifikacijos agentą; • Autentifikacijos agentas turi būti diegiamas kaip „exe" arba „msi" tipo failas.	√
13.		Turi būti integruota naujos kartos ugniasienės technologija leidžianti filtruoti remiantis aplikacija/servisu: • atpažįstamų aplikacijų duomenų bazę turi sudaryti ne mažiau nei 1000 aplikacijų;	√

		• naujų aplikacijų aprašai turi būti atnaujinami automatiškai; • dinaminis aplikacijų blokavimas remiantis rizikos klase ir produktyvumo indeksacija; • galimybė daryti išimtis remiantis vartotoju/IP/ tinklu.	
14.		Galimybė registruoti taisyklių taikymo aktyvumą registre.	√
		Reikalavimai ugniasienės technologijai	
15.		Išsamus paketų inspektavimas ir paketų filtras paremtas prievadais	√
16.		NAT (Network Address Translation);	√
17.		NAT maskavimas	√
18.		PAT (Port Translation/ Port remapping)	√
19.		SNAT (Source IP/ Port translation)	√
20.		DNAT (Destination IP/Port translation)	√
21.		Pilnas NAT (FullNAT)	√
22.		NoNAT (NAT išimtys)	√
23.		1:1 NAT	√
24.		Bendros taisyklės skirtos: Ping-ICMP (echo, echo reply); Maršruto atsekamumas ICMP ir UDP ; Diagnostinis ICMP;	√
25.		Turi būti integruotos sistemos registrai/ataskaitos.	√
		Reikalavimai VPN technologijai	
	Reikalavimai VPN protokolams		
26.		L2TP per IPSec prisijungimas (Client-to-Site architektūroje)	√
27.		PPTP prisijungimas (Client-to-Site architektūroje)	√
28.		Turi palaikyti Windows IPSec Tunnel modulį	√
29.		Turi palaikyti Apple iPhone klientus	√
30.		Turi palaikyti Cisco klientus	√
31.		Turi palaikyti beklientį VPN: • Veikti HTML5 technologija (naršyklės savybė); • Turi nereikalauti įskiepių (plugin), naršyklės priedėlių (add-on), papildomų aplikacijų; • Turi palaikyti RDP, VNC, Telnet, HTTP/S protokolus; • Automatinio prisijungimo galimybė.	√
32.		SSL VPN prisijungimai (Client-to-Site architektūroje): • Turi dirbti su proksiais ir NAT maršrutizatoriais; • Turi galėti priskirti kliento IP iš adresų sąrašo (pool); • Tunelio modulis (galimybė naudoti visus intraneto servisus);	√

33.		Turi būti galimi išeinantys susijungimai (pvz. prisijungimas prie spausdintuvo nutolusiame biure)	√
34.		SSL VPN prisijungimai (Site-to-Site architektūroje): • Turi dirbti su proksiais ir NAT maršrutizatoriais; • Turi priskirti kliento IP iš adresų sąrašo (pool); • Tunelio modulis (galimybė naudoti visus intraneto servisus); • Prisijungimai į abi kryptis.	√
35.		Automatinis BGP4 nustatymo palaikymas	√
36.		Turi būti numatyta galimybė sukurti "Site-to-site" nutolusių taškų prisijungimą per paprastą techninį įrenginį: • Ši funkcija turėtų būti nustatoma ir valdoma centralizuotai iš saugumo sistemos įrenginio ir turi būti atliekamas 2 lygio tuneliavimas ir duomenų kompresija; • Nuotolinio biuro apjungimui naudojamo techninio įrenginio turi nereikėti konfigūruoti prieš išsiunčiant į nutolusį biurą; • Nuotolinio biuro įrenginys turi palaikyti UMTS/3G USB modemą atsarginės interneto linijos užtikrinimui.	√
37.		Reikalavimai standartiniams IPSec prisijungimams: „Site-to-Site" architektūroje: • IPSec tunelio aprašymas keliems vietiniams/nutolusiems tinklams; • „Site-to-Site" VPN galimybė tarp dviejų sistemų turinčių dinaminius IP abiejose pusėse. „Client-to-Site" architektūroje: • Statinių kliento IP priskyrimas (kiekv. vartotojui); • Kliento IP priskyrimas iš sąrašo (pool).	√
	IPsec Algoritmai		
38.		Turi būti palaikomi šie algoritmai: DES; 3DES; AES/Rijndael (128 Bit); AES/Rijndael (192 Bit); AES/Rijndael (256 Bit); Blowfish; TwoFish; Serpent; SHA1 SHA2 (256, 384, 512 Bit); MD5; IPcomp (IPsec kompresija); DH Grupės 1,2,5,14,15,16 (MODP768/1024/1536/2048/3072/4096).	√

	Reikalavimai vartotojų autentifikavimui		
39.		Vietiniai vartotojai (valdomi ir laikomi saugumo sistemoje)	√
40.		Turi būti galimybė aktyvuoti/deaktyvuoti vietinius vartotojus	√
41.		RADIUS	√
42.		TACACS+	√
43.		LDAP	√
44.		Pagal nustatytą pasidalintą raktą (PSK / Slaptažodis)	√
45.		Vienkartiniai slaptažodžiai: per RADIUS/TACACS/LDAP (išoriniai) integruotas (vidinis: o vienkartinio slaptažodžio aplikacija (angl. OTP) skirta Android ir iOS; o turi būti be papildomos licencijos išoriniam OTP serveriui o Turi būti galimybė pradinius nustatymus atlikti per savitarnos portalą o Turi palaikyti trečių šalių fizinius OTP įrenginius.	√
46.		Sertifikatai (X.509v3): Sertifikatai iš vidinio CA Sertifikatai iš išorinio CA.	√
	Reikalavimai VPN klientams		
47.		IPSec Klientui: • Windows klientų palaikymas (XP,2000); • Windows 64-bit (Vista, Win7); • Linux klientų palaikymas; • Windows CE klientų palaikymas; • Galimybė atsisiųsti konfigūracijos klientą iš vartotojo portalo (reziduojančio saugumo sistemoje); • „Split“ tuneliavimo galimybė; • NAT-Traversal funkcija; • Autentifikacija su: Pasidalintu raktu (Pre-Shared Key (PSK)); Sertifikatais (X.509); Kortelėmis (smartcards); Tokenais; • XAUTH (išplėstinis autentifikacijos palaikymas).	√
48.		SSL VPN Klientui: • Turi būti galimybė atsisiųsti konfigūracijos klientą iš vartotojo portalo (reziduojančio sistemoje); • SSL VPN klientas turi veikti visose dažnai pasitaikančiose operacinėse sistemose (Windows, Linux, Mac OSX, ir kt.); • Turi būti suderinta su 64-bit sistemomis;	√

		• Turi būti įskaičiuota į licencijos kainą arba suteikiamas nemokamai.	
49.		Kiti Klientai: Apple iPhone palaikymas: PPTP; L2TP; IPSec; su automatiškai konfigūruojamu failu; Cisco IPSec kliento palaikymas.	√
Reikalavimai įsiveržimo aptikimo ir prevencijos sistemai, ATP funkcionalumui (IDS/IPS/ATP)			
50.		Turi būti integruota apsauga nuo atsisakymo aptarnauti atakų (DoS)	√
51.		Rankinio pavienių atakų išjungimo galimybė	√
52.		Turi būti nustatymo, besiremiančio pagal atakas į operacines sistemas, galimybė	√
53.		IDS ir IPS nustatymai pagal atakų grupes	√
54.		Aktyvavimas / išjungimas taisyklių grupių vienu pelės paspaudimu	√
55.		IDS/IPS funkcionalumas kiekvienai individualiai sąsajai	√
56.		Galimybė nustatyti išimtis IDS taisyklių taikymui tinklams ir kompiuteriams	√
57.		Anomalijų aptikimas (apsauga nuo nulinės dienos atakų)	√
58.		Prievadų skanavimo aptikimas: Galimybė daryti išimtis.	√
59.		SYN Flood aptikimas: Turi būti numatyta galimybė daryti išimtis; Registrai; Syn Flood normos reguliavimas; Pagal šaltinį (source)/ paskirtį (destination)/ maišytas nustatymas.	√
60.		UDP Flood aptikimas: Turi būti numatyta galimybė daryti išimtis; Registrai; UDP Flood normos reguliavimas; Pagal šaltinį (source)/ paskirtį (destination)/ maišytas nustatymas.	√
61.		ICMP Flood aptikimas: Turi būti numatyta galimybė daryti išimtis; Registrai; ICMP Flood normos reguliavimas; Pagal šaltinį (source)/ paskirtį (destination)/ maišytas nustatymas.	√
62.		Atskiri registrų lygiai IDS ir IPS dalims	√
63.		Atakų aprašų duomenų bazė turi būti nemažiau 8000 aprašų	√
64.		Turi palaikyti dvejetainės sistemos taisykles	√
65.		Turi palaikyti Microsoft Active Protection Programą (MAPP)	√

66.		Turi būti automatiniai šablonų atnaujinimai	√
67.		Administratorius turi galėti konfigūruoti nustatymus serveriui (web serverį, e.pašto serverį) siekiant geriausiai nustatyti IDS/IPS sistemą (kad aktyvuoti automatinį aprašų patikrinimą).	√
68.		Sistema turi galėti aptikti pažengusius pavojus, tokius, kaip botnet tinklai ar komandinius ir kontrolės serverius; Tai turėtų veikti keliais mechanizmais (minimaliai ugniasienės, DNS, IPS, web proksi).	√
Reikalavimai greitųjų žinučių (Instant Messaging (IM)) / Peer to Peer (p2p) protokolų kontrolei realiu laiku			
69.		Sistema turi atpažinti ir blokuoti minimaliai šiuos IM klientus: ICQ, AIM, MSN Messenger; IRC, Yahoo! Messenger, Jabber, Skype	√
70.		Sistema turi galėti blokuoti duomenų siuntimą, tačiau leisti pokalbius (chat) populiariausioms IM aplikacijoms	√
71.		Sistema turi atpažinti sekančius P2P klientus: Bittorrent, Edonkey, Gnutella, WinMX, Winny, Manolito, Ares, Direct Connect	√
72.		Sistema turi galėti blokuoti arba riboti interneto srauto pralaidumą išvardintiems P2P klientams.	√
Reikalavimai interneto (web) turinio saugumo funkcionalumui			
	Integracijai į egzistuojančią aplinką		
73.		Proksi rėžimo galimybė (proksis turi būti galimas konfigūruoti kiekviename kliente)	√
74.		Skaidrus rėžimas (proksio konfigūruoti nebūtina)	√
75.		Skaidrus rėžimas su autentifikacija	√
76.		Prisijungimo portalas (galimybė lokalizuoti).	√
77.		Pilnai skaidrus rėžimas (proksio konfigūruoti nereikia, šaltinio IP adresas peradresuojamas (forward), nėra NAT);	√
78.		Turi būti galimos išimtys šaltinio IP/Tinklams;	√
79.		Reikalavimai vartotojų autentifikacijai skaidriame rėžime: Per Active Directory SSO (NTLM) Autentifikacija vietiniame portale; „Out-of-band“ autentifikacija per klientą	√
80.		Pirminio proksio (Upstream Proxy) palaikymas: • Vartotojų autentifikacija pirminiame proksyje; • Neribotas pirminių proksių skaičius; • Pirminio proksi pasirinkimas remiantis tokias parametrais, kaip šaltinio IP, vartotojas/grupė vartotojų, laikas, domenas, URL.	√
81.		HTTP proksio PAC failų talpinimas: Auto-config kliento per DHCP;	√

		Auto-config kliento per DNS.	
82.		Laisvai pasirenkamas proksio „klausymosi“ portas;	√
83.		Failų kešavimas kietajame sistemos diske: Be papildomo licencinio mokesčio; Turi būti ir su skaidriu proksi.	√
	Reikalavimai apsaugos mechanizmui		
84.		Turi būti automatinis virusų šablonų aprašų atnaujinimas	√
85.		Antivirusinė apsauga skirta: • HTTP atsiuntimams; • HTTPS atsisiuntimams; • FTP atsisiuntimams (per naršyklę); • FTP atsisiuntimams (komandinė eilutė/FTP klientas) (skaidrus FTP proksis).	√
86.		Maksimalus skenuojamo failo dydis nustatomas pagal poreikį	√
87.		Saugios paieškos palaikymas populiariausiems paieškos varikliams	√
88.		Web turinio filtro praleidimas (override) (blokuojamiems URL, įskaitant dedikuotą registravimą)	√
89.		Išimčių taikymas: • nurodytiems šaltiniams; • nurodytiems pasiekiamiems taškams (destination); • nurodytiems vartotojams (papildomai su vartotojų autentifikacija).	√
90.		Laisvai nustatomi įspėjimai vartotojams (pavyzdžiui aptiktas virusas)	√
91.		Turi būti integruoti ne mažiau nei du virusų skanavimo varikliai iš skirtingų tiekėjų	√
92.		Skirtingų saugumo profilių konfigūravimas: • Atskyrimas paremtas vietine autentifikacija; • Atskyrimas paremtas LDAP direktorija; • Atskyrimas paremtas AD SSO su NTLM/Kerberos • Atskyrimas paremtas eDirectory SSO direktorija; • Atskyrimas paremtas tinklu (vartotojo IP adresas); • Autentifikacija per RADIUS; • Autentifikacija per TACACS+.	√
93.		Galimybė naudoti paraleliai kelis autentifikacijos būdus, pavyzdžiui kelis Active Directory serverius;	√
94.		Turi būti neribotas profilių skaičius;	√
95.		Turi būti numatyta galimybė naudoti paraleliai įvairius autentifikacijos mechanizmus, paremtus kliento šaltinio IP adresu (pavyzdžiui proksis tinklui	√

		1, LDAP tinklui 2, standartinis proksi rėžimas tinklui 3);	
96.		Reikalavimai filtravimui ir blokavimui: • Pagal failų plėtinius (.exe, .gif,); • Pagal MIME dokumentų tipą (iš serverio): • MIME tipo tikrinimas proksio apžiūra (magic lookup). • Pagal URL kategorijas; • Pagal Java/JavaScript/ActiveX; • Turi būti integruota šnipinėjimo programinę įranga aptinkanti sistema (turi tikrinti įeinantį srautą ir "skambinimą namo" (išeinantį) srautą); • Pagal potencialiai nepageidaujamą aplikaciją; • Pagal baltą sąrašą; • Pagal juodą sąrašą; • Remiantis aplikacijų lygiu (L7 ugniasienė); • Pagal nežinomą (neįtrauktas į kategoriją) tinklalapį; • Filtravimas paremtas laiko parametru arba diena.	√
97.		URL filtro funkcionalumo reikalavimai: • Turi būti daugiau nei 90 skirtingų kategorijų; • URL duomenų bazės užklausos realiu laiku (nėra poreikio duomenų bazės atnaujinimams); • Kategorijų grupės neribotos; • Reputacija paremtas URL blokavimas; • Leisti/blokuoti kategorijas remiantis laiko parametru arba diena; • Globalūs ir vartotojui individuliai nustatomi juodi ir balti sąrašai; • URL filtras juodo sąrašo rėžime (viskas leidžiama išskyrus nepasirinktas kategorijas) arba balto sąrašo rėžimas (viską blokuoti išskyrus pasirinktas kategorijas); • Pasirenkamos išimtys remiantis tokiais parametrais, kaip: Šaltinis/Tikslas/Domenas/Serveris/ Kategorija	√
Reikalavimai elektroninio pašto turinio saugumo funkcionalumui			
	Integracija į egzistuojančią infrastruktūrą		
98.		SMTP prieigos vartų rėžimas (prieigos vartai yra naudojami viduje, kaip perdavėjas ir išorėje, kaip MX)	√
99.		Skaidrus rėžimas (MX įrašo konfigūravimas nėra būtinas)	√

100.		Pašto maršruto konfigūravimas: • Prieš-srautinis (upstream) pašto persiuntimas (Smarthost) su autentifikacija; • MX-paremtas maršrutizavimas; • Atskiri pašto prieigos vartai domenui; • Atskiri pašto serveriai domenui.	√
101.		El.pašto persiuntimas su „round robin“	√
102.		TLS palaikymas: • Konfigūruojamas dedikuotam pašto serveriui; • Konfigūruojamas dedikuotam domenui; • TLS sertifikatas gali būti keičiamas. • Galimybė išjungti TLS tam tikriems pašto serveriams	√
103.		Išeinančio el.pašto skaitmeninio pasirašymo galimybė su DKIM	√
104.		SMTP autentifikacija (el.paštas priimamas tik tada jei vartotojas yra autentifikuotas)	√
105.		Keičiamas parašas po laiško turiniu išeinančiam el.paštui.	√
	Apsaugos mechanizmo reikalavimai		
106.		Antivirusinė apsauga skirta SMTP, POP3, POP3S	√
107.		2 ar daugiau integruotos skirtingų gamintojų virusų aptikimo sistemos	√
108.		Kiekviena saugumo opcija gali būti konfigūruojama skirtingai kiekvienam domenui	√
109.		Gaunančiųjų domenų skaičius neribotas	√
110.		Anti persiuntimo (Anti-Relaying) apsauga	√
111.		Reikalavimai Anti-SPAM apsaugai: • Galimi filtro veiksmai “Ištrinti”, “Įspėti”, “Ignoruoti” ir “Karantinuoti”; • Galimybė keisti pridedamą žymę “SPAM” el.pašto pavadinimo laukelyje; • Anti-Spam siuntėjų globalus baltas sąrašas; • Anti-Spam siuntėjo baltas sąrašas kiekvienam el.pašto gavėjui (nustatomas pačio vartotojo); • Anti-Spam siuntėjo juodas sąrašas kiekvienam el.pašto gavėjui (nustatomas pačio vartotojo); • Juodi/Balti sąrašai gali būti keičiami administratoriaus.	√
112.		Antispam apsauga SMTP,POP3, POP3S srautui	√
113.		El.pašto filtravimas turi būti atliekamas remiantis: • Reputacijos duomenų bazės rezultatais realiu laiku; • RBL (Realtime Blackhole Lists);	√

		• Siuntėjas yra DialUp tinkle (privatūs DSL tinklai); • Atvirkštinio DNS tikrinimas; • Gavėjo adreso tikrinimas: Tikrinimas pagal Active Directory; Tikrinimas per SMTP į pašto serverį. • SPF (Sender Policy Framework) tikrinimas; • BATV (Bounce Address Tag Verification); • Įtraukimo į pilką sąrašą galimybė (Greylisting); • Failų plėtinių filtravimas (.exe, .bat., …); • Teksto analizė (raktažodžiai/ekspresijos); • MIME dokumento tipo tikrinimas prisegtam dokumentui; • Neskanuojamų dokumentų blokavimas (pav. Apsaugotų slaptažodžiu pdf); • Pagal maksimalų el.pašto dydį.	
114.		Reikalavimai duomenų nutekėjimo prevencijai el.pašto sraute: • Pagal nustatytą taisyklių sąrašą (kreditinių kortelių numeriai ar pan.) • Turi būti suderinama su reguliariomis išraiškomis (angl. Regular expressions); • Turi būti galimybė nustatyti el.pašto užšifravimo iššaukimą	√
115.		Visas antispam ir antivirus funkcijas turi būti galima išjungti remiantis: tam tikru siuntėjo el.pašto serveriu; tam tikru siuntėju; tam tikru gavėju.	√
	Blokuotų el.laiškų valdymas		
116.		Spam ir infekuoti laiškai turi būti karantinuojami specialioje karantino srityje lokaliai saugumo sistemoje; Galimybė turėti karantiną POP3 srautui; Karantinuoto el.pašto ištrynimas praėjus nustatyto laiko periodui; Spam el.laiškų atmetimas iš karto (atmetimas prieš priimant); El.pašto atmetimas (RBL, BATV, SPF); Galimybė keisti nepageidaujamų ir infekuotų el.laiškų pavadinimo laukelį (subject)/antraštę (header); Galimybė siųsti asmeninę kasdieninę ataskaitą apie blokuotą el.paštą kiekvienam vartotojui atskirai: Viena kasdieninė ataskaita vartotojui, netgi jei vartotojas turi daugiau nei vieną el,pašto adresą sistemoje(konsoliduota ataskaita apie nepageidaujamus el.laiškus);	√

		Galimybė ataskaitos tekstą nustatyti pagal vartotojo poreikius; Turi palaikyti POP3 vartotojus; Ataskaita apie spam gali būti išjungiama pasirinktam el.pašto adresui; Palaikomi vidiniai el.pašto sąrašai; Vartotojas turi galėti išlaisvinti el.paštą iš karantino pats; Vartotojas turi turėti galimybę pats valdyti baltus sąrašus; Vartotojas turi turėti galimybę pats valdyti juodus sąrašus; Vartotojas turi turėti galimybę pats valdyti savo karantiną saugiame web portale (turi reziduoti sistemoje); Administratorius gali nustatyti kokio tipo blokuotus el.laiškus vartotojas gali išlaisvinti; Realiu laiku pasiekiamas el.pašto sąrašas (spool) per internetinę naršyklę: Administratoriui (visus e.laiškus); Vartotojui (jo asmeninius e.laiškus). Administratorius turi galėti valdyti el.paštą karantine (trinti/išlaisvinti).	
117.		Administratorius turi galėti konfigūruoti POP3 žinutę (pvz. rastas virusas) pagal poreikius.	√
	Integruoto el.pašto šifravimo ir dešifravimo funkcijos reikalavimai		
118.		Turi palaikyti OpenPGP; Išorinis PGP raktų serveris; Turi palaikyti S/MIME; Ši funkcija neturi būti licencijuojama atskirai (turi būti be papildomo mokesčio); Automatinis el.pašto šifravimas/dešifravimas; Turi būti integruota CA sertifikatų ir PGP raktų generavimui; Galimybė Importuoti raktus/sertifikatus; Auto importavimo funkcionalumas sertifikatų iš "patikimų išorinių CA; Kiekvienam vartotojui formuojama šifravimo/dešifravimo/pasirašymo politika.	√
119.		PDF failu tipu paremtas el.pašto šifravimas, kai gavėjas neturi PGP arba S/MIME: • Šifravimą turi būti galima atlikti per Outlook priedėlį; • Šifravimas gali būti vykdomas automatiškai susiejus su duomenų nutekėjimo priedėliu.	√

120.		Automatizuotas paraštės (footer) pridėjimas el.pašte: „Patikrinta nuo virusų“ paraštė; Legal disclaimer.	√
121.		Neturi būti apribojimų konkurenciniams el.pašto prisijungimams.	√
Reikalavimai web aplikacijų saugumo funkcionalumui (atvirkštinis proksi (reverse proxy))			
122.		Atvirkštinis Proksio funkcionalumas (aplikacijų lygio prieigos vartai)	√
123.		Turi būti realizuotas HTTPS palaikymas: • HTTP iš naršyklės->HTTPS į galutinę sistemą (backend); • HTTPS iš naršyklės->HTTPS į galutinę sistemą (backend); • HTTPS iš naršyklės->HTTP į galutinę sistemą (HTTPS offlaoding); • SAN (Subject Alt. Name) sertifikatų palaikymas; • Tarpinių CA sertifikatų palaikymas; • Galimybė pačių pasirašytų sertifikatų generavimas įrenginyje.	√
124.		Autentifikacijos perkėlimas (angl. Offloading): • Autentifikacija per bazinę autentifikaciją proksyje; • Prisijungimo rekvizitų perdavimas į galinį (angl. Backend) serverį (per bazinę autorizaciją) • OTP palaikymas • Autentifikacija turi būti konfigūruojama serveriui/URL	√
125.		Turi būti integruotas URL stiprinimo variklis: • Informacija gali būti nuskaitoma iš sitemap.xml; • Automatiškai/periodiškai.	√
126.		Turi būti atliekama gilių nuorodų (deep linking) pateikimo kontrolė	√
127.		Direktorijos sankirtos (Directory traversal) prevencija	√
128.		Apsauga nuo SQL injekcijų	√
129.		Formų stiprinimo apsauga	√
130.		Apsauga nuo tarptinklinių scenarijų atakų (XSS);	√
131.		Dviguba antivirusinė apsauga;	√
132.		Reputacija paremtas blokavimas (TOR tinklai, anonymazeriai...)	√
133.		Sausainukų (Cookie) pasirašymas su skaitmeniniu parašu	√
134.		Automatinis serverio skanavimas web serverio identifikavimui	√
135.		Apkrovos balansavimas lankytojų išskirstymui per kelis serverius	√

136.		Pilna visų veiksmų registrų transakcija.	√
		Papildomai reikalavimai	
	Reikalavimai Valdymui / Administravimui		
137.		Valdymas internetinės naršyklės pagalba be papildomos programinės įrangos įdiegimo; Komunikacija turi būti šifruojama per HTTPS; HTTPS sertifikatas gali būti pakeistas.	√
138.		IOS palaikymas valdymo konsolei	√
139.		Automatinis administratoriaus atjungimas („log off“) po nustatyto laiko intervalo	√
140.		Web paremtos konsolės meniu paieška	√
141.		Galimybė nustatyti pagal poreikius pagrindinį meniu langą	√
142.		Turi būti galimybė matyti konfigūracijos pakeitimus	√
143.		Turi būti numatyta galimybė spausdinti konfigūracija (XML, PDF)	√
144.		Turi būti numatyta galimybė importuoti/eksportuoti sąrašus	√
145.		Turi būti numatyta galimybė klonuoti objektus	√
146.		Turi būti numatyta galimybė paraleliai naudoti administravimo įrankius keliems administratoriams: • skaitymo/įrašymo rėžimas tuo pačiu metu; • spausdinama konfigūracija (XML, PDF); • konfigūracijų pakeitimo sekimas (tracking).	√
147.		Turi būti rolėmis paremtas administravimas: Rolės nustatomos pagal poreikį; Tik skaitymo rėžimo rolė.	√
148.		Instrukcijos/ Pagalba “online”: • Administravimo instrukcija; • Elektroninė instrukcija sistemoje; • Kontekstui jautri “online” pagalba; • Galimybė atlikti paiešką “online” pagalboje.	√
	Galimybė centralizuotai valdyti keletą sistemų vienu metu		
149.		Kelių atskirų ir geografiškai nutolusių saugumo sistemų valdymas tuo pačiu metu iš vieno valdymo centro (turi nereikalauti papildomos licencijos centralizuoto valdymo programinei įrangai); Centrinė kontrolės konsolė turi turėti grafinius būsenos indikatorius: resursų būsena; licencijos būsena; atakų ataskaita; versijos būsena; atnaujinimų aktyvavimas; Rolėmis paremtas administravimas	√

		Centrinis ataskaitų serveris	
	Reikalavimai atsarginėms kopijoms ir atstatymui		
150.		Turi būti numatyta galimybė nuotoliniu būdu generuoti atsargines kopijas ir atsisiųsti jas per internetinę naršyklę; Galimybė automatiškai generuoti atnaujinimus per el.paštą; Komentarų pridėjimo funkcija atsarginėms kopijoms; Galimybė valdyti kelias atsargines kopijas vienoje saugumo sistemoje; Turi būti numatyta galimybė užšifruoti ir slaptažodžiu apsaugoti atsargines kopijas; Turi būti numatyta galimybė įkelti ir atstatyti atsargines kopijas per internetinę naršyklę; Turi būti numatyta galimybė įkelti ir atstatyti atsargines kopijas iš USB atmintinės; Galimybė sukurti „apkarpytą“ atsarginę kopiją šablono naudojimo tikslais	√
	Reikalavimai atnaujinimo mechanizmui		
151.		Visi atnaujinimai turi būti pateikiami iš sprendimo gamintojo;	√
152.		Visus atnaujinimus (įskaitant stambius atnaujinimus) turi būti galima atsisiųsti iš interneto ir atnaujinimų serverio;	√
153.		Atnaujinimai turėtų būti atsiunčiami automatiškai ir laikomi saugumo sistemos kietajame diske;	√
154.		Šablonų aprašymų atnaujinimai turi būti atsiunčiami ir įdiegiami automatiškai;	√
155.		„Firmware“ ir aprašų šablonų įkėlimas gali būti atliekamas pagal iš anksto sudarytą grafiką;	√
156.		Sistemos pataisos turi būti įdiegiamos vienu pelės klavišo paspaudimu.	√
	Reikalavimai integruotoms saugumo sistemoje ataskaitoms		
157.		Turi būti pateikiama grafinė informacija apie įrangą (CPU, kietąjį diską, tinklą...);	√
158.		Turi būti pateikiama grafinė informacija apie atakas (IPS, Virusus, Prievadų skanavimą...);	√
159.		Turi būti pateikiama grafinė informacija realiu laiku apie pralaidumą: • Aplikacijų atpažinimas L7; • Vaizdavimas lentelėje ar diagramoje;	√

		• Galimybė blokuoti ar valdyti pralaidumą iškarto iš monitoringo lango.	
160.		Turi būti pateikiama grafinė informacija apie naršymo srautą (Top 10 tinklalapių, persiųstų MB kiekį...);	√
161.		Turi būti pateikiama grafinė informacija apie el.pašto srautą (persiųstų MB kiekį, top siuntėjai);	√
162.		Turi būti pateikiama informacija apie nutolusių prisijungimų srautą (sesijos, dabartinį vartotoją,...);	√
163.		Turi būti pateikiama detalizuota ataskaita realiu laiku apie web srautą: paremta domenais; paremta vartotojais; paremta lankomu tinklalapiu; paremta kategorija; paremta skyriumi (departamentu); paremta paieškos variklių užklausomis; galimybė naudoti kelis filtrų kriterijus; galimybė išsaugoti filtro kriterijų; automatinės ataskaitos el.paštu.	√
164.		Turi būti automatiškai siunčiama administratoriui įvykių santrauka nurodyto laiko periodui tokiais intervalais: kasdien kas savaitę kas mėnesį	√
165.		Galimybė daryti išimtis ataskaitoms, kad išvengti nepageidaujamos informacijos;	√
166.		„Flash" technologija paremtos ataskaitos: Galimybė išjungti/įjungti.	√
167.		Ataskaitų informacijos anonimizavimo (maskavimo) galimybė (web ir e.pašto) (vartotojo vardas/IP adresas, pašto domenas ir pašto adresai turėtų būti uždengiami). Atrakinimas šios informacijos turėtų vykti dviejų slaptažodžių pagalba.	√
	Reikalavimai tinklui/LAN/WAN		
168.		Turi palaikyti DSL: • Integruotas PPPoE; • Integruotas PPPoA; • Integruotas VDSL; • Galimybė persijungti prie DSL rankiniu būdu; • Automatinio persijungimo funkcija.	√
169.		UMTS/3G palaikymas USB tipo modemams	√
170.		Turi būti galima skaidriai integruoti į L3 aplinką (skaidrus rėžimas/bridging rėžimas); Gali būti aktyvuojama prievadui; Prievadų apjungimo (bundeling) viename skirstytuve (switch).	√
171.		Turi palaikyti IPv6: • Ugniasienei/Paketų filtrui;	√

		• HTTP proksiui; • SMTP proksiui; • DNS, DHCP ir PPPoE; • Valdymui ir galutinio vart. portalui; • SNMP ir NTP; • IDS/IPS sistemai; • Turėtų tuneliuoti IPv6 adresus per IPv4; • Tunelio „brokerio“ galimybės.	
172.		Maršrutizavimas pagal politiką (maršrutizavimas paremtas paskirties tašku (destination)/šaltinio portu arba šaltinio IP adresu;	√
173.		Pilnas palaikymas VLAN žymėjimo (Tagging)(IEEE 802.1q);	√
174.		Turėtų palaikyti iki 99 šalutinių sąsajų (alias interfaces) (keletą IP adresų ant vienos sąsajos);	√
175.		Turėtų palaikyti proksi ARP;	√
176.		Prievadų agregacijos (IEEE802.3ad) palaikymas: • skirtas susijungimams į kelis komutatorius (switches) (aukštas patikimumas); • skirtas prievadų susiejimui viename komutatoriuje; • (aukšto patikimumo tinklas).	√
177.		Turėtų būti automatinis apkrovos balansavimas į kelis WAN sujungimus;	√
178.		Daugiau nei 8 WAN „uplink“ palaikymas;	√
179.		Turi būti galimas rankinis apkrovos balansavimas paremtas taisyklėmis;	√
180.		Vienas adreso objektas visoms sąsajoms;	√
181.		Prioritetas pagal nustatytą eilę;	√
182.		„Pasvertas“ (weighted) apkrovos balansavimas;	√
183.		UMTS/3G tik apkrovos balansavimui;	√
	WAN apkrovos balansavimas:		
184.		WAN „failover“ reikalavimai: • Automatinis „failover“ dedikuotam WAN portui, jei WAN sujungimas nebefunkcionuoja (turi būti įdiegtas diagnozavimo mechanizmas); • Automatinis „failover“ IPSec tuneliui.	√
185.		Dinaminis maršrutizavimas per OSPF: Atviro teksto/MD 5 autentifikacija; Srities tipas normalus, Stub, NSSA; prisijungusių išdalinimas; statinių išdalinimas;	√
186.		BGP4 palaikymas: Leisti keletą autonominių sistemų; Griežtas IP adresų sutapimas; Keleto kelių maršrutizavimas.	√

187.		Apkrovos balansavimas prisijungimams į serverio susivienijimą (pool) su įdiegtu tikrinimo mechanizmu.	√
188.		DHCP palaikymas: • Turi būti integruotas DHCP serveris; • Statinis išdavimas (static lease); • Turi būti integruotas DHCP persiuntimas (relay).	√
	Bevielio ryšio (wifi) palaikymas		
189.		Integruotas wifi kontroleris (suderinama su to pačio gamintojo wifi prieigos taškais (AP)); Skaičius palaikomų AP neturi būti ribojamas pagal licenciją; AP turi būti prijungiami prie sistemos „plug and play“ principu; Spartaus „roaming“ (802.11r) palaikymas Wifi kliento srauto apdorojimas: Zonų atskyrimas (srautas turi eiti pro saugumo sistemą analizei); Kliento izoliavimas; SSID maskavimas; Realaus laiko klientų ir AP monitoringas; Integruotas portalas svečiams/vidiniams vartotojams (HotSpot); Naudojimo sąlygų nustatymas (terms of use acceptance); Prisijungimas gali būti suteiktas pagal galiojimo laiką, laiko kvotą, duomenų atsisiuntimą.	√
	Paslaugos užtikrinimas (QoS) / Pralaidumo valdymo reikalavimai		
190.		Turi būti srauto parinkėjas, kad aprašyti srauto būklę; Turi palaikyti TOS bitus; Turi palaikyti DSCP bitus; Pralaidumas nustatomas per sąsają; Garantuotas pralaidumo užtikrinimas; Pralaidumo ribojimas: • paremtas L7 aplikacijomis; • vienu paspaudimu aplikacijų srauto valdymas. VoIP/transliacijos (streaming) palaikymas.	√
	Proksis / Aplikacijų lygio prieigos vartai		
191.		Turi būti integruotas DNS proksis: • DNS serverio persiuntimas (forwarding); • Išskirto (split) DNS palaikymas (persiuntimas domenų į vidinius DNS serverius);	√

		• Galimybė aprašyti vieną hostą ir jiems priklausančius IP adresus; • Turi būti integruotas DynDNS, FreeDNS, Zoneedit, NameCheap, dfDNS irEasyDNS klientai.	
192.		Turi būti integruotas „ident“ proksis;	√
193.		„Generic“ proksis (papildomoms aplikacijoms);	√
194.		Turi būti integruotas H.323: Skaidrus H.323; H.323 Gatekeeper; H.323 tam tikriems klientams.	√
195.		Integruotas SIP / VoIP: Skaidrus SIP; SIP tam tikriems šaltiniams/gavėjams;	√
196.		Integruotas SOCKS Proksis: • Turi būti SOCKS vartotojų autentifikacija su RADIUS; • Turi būti SOCKS vartotojų autentifikacija su TACACS+; • Turi būti SOCKS vartotojų autentifikacija su LDAP; • Turi būti SOCKS vartotojų autentifikacija su eDirectory; • Turi būti SOCKS vartotojų autentifikacija su vietiniais vartotojais.	√
	Papildomi reikalavimai		
197.		Prisijungimas prie Direktorijos serviso vartotojų administravimui (naršymo profiliai, VPN vartotojas): • Microsoft ADS; • Vietinis LDAP; • Integruota naršyklė skirta ADS/LDAP grupėms; • Novell eDirectory; • Integruota naršyklė skirta eDirectory grupėms; • Apple OpenDirectory; • TACACS+; • RADIUS.	√
	Reikalavimai registrui ir įspėjimo pranešimams		
198.		Registras turi būti galimas keliuose išoriniuose Syslog serveriuose;	√
199.		Registras centriniame ataskaitų serveryje;	√
200.		Atskiri registrų failai skirtingiems moduliams;	√
201.		Registrų failų užklausos mechanizmas;	√

202.		Įspėjimo pranešimas per SNMP Trap: SNMPv2 ir SNMPv3 palaikymas;	√
203.		Įspėjimo pranešimas per el.paštą;	√
204.		Įspėjimų pranešimų konfigūravimas kiekvienam individualiam įspėjimui;	√
205.		SNMP MIB atsisiuntimo galimybė per GUI.	√
206.		Programinės įrangos, saugumo modulių (kurie turi būti periodiškai atnaujinami), virusų ir įsiveržimo šablonų duomenų bazės atnaujinimai internetu turi būti užtikrinti ne mažiau kaip 1 metus.	√
207.		Turi būti užtikrinta 8 val. penkias dienas per savaitę techninis palaikymas (telefonu, el.paštu).	√
208.		Garantija įrangai suteikiama 1 metams	√

Projektų vadovas		Gytis Šakys
(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas)	(Parašas)	(Vardas ir pavardė)