



Uždaroji akcinė bendrovė, buveinės adresas Lvovo g. 105A, 08104 Vilnius
Tel.: 8 5 2059895, Faksas: 8 5 2059899
Juridinių asmenų registras, įmonės kodas 302327313, PVM mokėtojo kodas LT100004630711

Užimtumo tarnybai prie Lietuvos Respublikos
Socialinės apsaugos ir darbo ministerijos

(Adresatas (perkančioji/įgaliotoji organizacija))

**PASIŪLYMAS
DĖL TINKLO ĮRANGOS PIRKIMO**

2021-12-01 Nr. PS20211201-01

(Data)

Vilnius

(Sudarymo vieta)

Tiekėjo pavadinimas / <i>Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių pavadinimai/</i>	UAB Fortevento
Tiekėjo adresas / <i>Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių adresai/</i>	Lvovo g. 105A, 08104 Vilnius
Banko sąskaitos Nr.	LT177044060006867877
Asmens, pasirašiusio pasiūlymą, vardas, pavardė, pareigos	Direktorius, Aurelijus Šaltenis
Telefono numeris	+37052059895
Fakso numeris	+37052059899
El. pašto adresas	info@fortevento.lt

1. Šiuo pasiūlymu pažymime, kad susipažinome ir sutinkame su visomis sąlygomis, nustatytomis Užimtumo tarnyba prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos (toliau – Perkančioji organizacija/ Užimtumo tarnyba) **tinklo įrangos** (toliau – prekės) pirkimo, vykdomo **neskelbiamos** apklausos būdu, sąlygose, kituose pirkimo dokumentuose (jų paaškinimuose, papildymuose, jei tokių yra). Teikdami šį pasiūlymą, mes patvirtiname, kad į mūsų siūlomų paslaugų kainą įskaičiuotos visos išlaidos ir kad mes prisiimame riziką už visas išlaidas, kurias teikdami pasiūlymą ir laikydamiesi pirkimo dokumentuose nustatytų reikalavimų, privalėjome įskaičiuoti į pasiūlymo kainą.

2. Pasiūlymas galioja iki termino, nustatyto pirkimo sąlygose.

3. Dokumentų pateikti duomenys yra tikri.

4. Mes siūlome **tinklo įrangą** ir patvirtiname, kad siūlomos paslaugos visiškai atitinka pirkimo dokumentuose nurodytus reikalavimus, kurių pavadinimai ir kaina yra tokie:

1 lentelė

Eil. Nr.	Prekė	Mato vnt.	Perkamas kiekis	Kaina EUR be	Viso kaina EUR be PVM (4x5)
----------	-------	-----------	-----------------	--------------	-----------------------------

				PVM už vienetą	
1	2	3	4	5	6
1.	Wi-Fi prieigos taškai su montavimo įranga ir licencijomis	Vnt.	10	399,00	3990,00
2.	Komutatoriai	Vnt.	2	400,00	800,00
3.	Tinklo vartotojų bei prietaisų autentifikavimo programinė įranga.	Vnt.	12	350,00	4200,00
4.	Tinklo įrangos valdymo ir stebėjimo programinė įranga	Vnt.	12	72,00	864,00
Bendra pasiūlymo kaina be PVM (Eur)					9,854.00
PVM 21 % (Eur)					2,069.34
Bendra pasiūlymo kaina su PVM (Eur)					11,923.34

Pastabos:

1. Finansiniame pasiūlyme privaloma nurodyta tvarka **užpildyti** tik **laisvas** lentelės skiltis.
2. Bendra pasiūlymo kaina nurodoma suapvalinta (pagal aritmetinio apvalinimo taisyklės), paliekant du skaitmenis po kablelio.

Bendra pasiūlymo kaina, Eur su PVM Vienuolika tūkstančių devyni šimtai dvidešimt trys eurai 34 ct

(kaina žodžiais)

Į pasiūlymo kainą įeina visos išlaidos ir visi mokesčiai, taip pat ir 21 % PVM, kuris sudaro 2069,34 du tūkstančiai šešiasdešimt devyni eurai 34 ct (kaina skaičiais ir žodžiais).

(Tais atvejais, kai pagal galiojančius teisės aktus tiekėjui nereikia mokėti PVM, *tiekėjas nurodo teisinį pagrindą, dėl kurio PVM nemoka*).

2 lentelė

Reikalavimai Wi-Fi prieigos taškams.

Eil. Nr.	Parametras	Reikalaujama parametro reikšmė	Pasiūlymo duomenys Privaloma išsamiai aprašyti siūlomą parametą. Pasiūlymai, kuriuose bus įrašyta „Taip/Ne“ arba „Atitinka“ bus atmetti kaip neatitinkantys reikalavimų
1.	Gamintojas modelis	Nurodyti pavadinimą, produkto kodą(-us).	Aruba AP-505
2.	Ryšio standartai	Turi būti palaikoma: • IEEE 802.11b/g; • IEEE 802.11a; • IEEE 802.11n; • IEEE 802.11ac; • IEEE 802.11ax; Bluetooth 5; IEEE 802.15.4 Zigbee.	Palaikomi: • IEEE 802.11b/g; • IEEE 802.11a; • IEEE 802.11n; • IEEE 802.11ac; • IEEE 802.11ax; Bluetooth 5; IEEE 802.15.4 Zigbee.
3.	Radijos	Turi būti palaikoma 802.11ax 5 GHz ir 802.11ax 2,4 GHz 2x2 MIMO.	Palaikoma 802.11ax 5 GHz ir 802.11ax 2,4 GHz 2x2 MIMO.

		Turi būti galima vienu metu naudoti 2,4 Ghz 802.11ax ir 5 Ghz IEEE 802.11ax standartus.	Galima vienu metu naudoti 2,4 Ghz 802.11ax ir 5 Ghz IEEE 802.11ax standartus.
4.	Duomenų perdavimo sparta	Turi būti palaikoma ne mažesnė kaip 1.2 Gbps sparta naudojant 802.11ax 5 Ghz ir ne mažesnė kaip 0,5 Gbps sparta naudojant 802.11ax 2.4 Ghz	Palaikoma 1.2 Gbps sparta naudojant 802.11ax 5 Ghz ir 0,5 Gbps sparta naudojant 802.11ax 2.4 Ghz
5.	Spindulio formavimas	Turi būti palaikoma spindulio formavimo (angl. beamforming) technologija.	Palaikoma spindulio formavimo (angl. beamforming) technologija.
6.	Antenos	Ne mažiau kaip 2 vidinės antenos	2 vidinės antenos
7.	Kanalų apjungimas	Turi būti palaikomas belaidžio ryšio kanalų apjungtų funkcionalumas (angl. channel bonding). Turi būti palaikomi 80 Mhz pločio apjungti belaidžio ryšio kanalai.	Palaikomas belaidžio ryšio kanalų apjungtų funkcionalumas (angl. channel bonding). 80 Mhz pločio apjungti belaidžio ryšio kanalai.
8.	Laidinio tinklo jungtis	RJ-45,10/100/1000 Mbps, Half/Full Duplex režimai.	RJ-45,10/100/1000 Mbps, Half/Full Duplex režimai.
9.	Kitos jungtys	USB, konsolės, išorinio DC maitinimo jungtys	USB, konsolės, išorinio DC maitinimo jungtys
10.	El. maitinimas	802.3at PoE. Papildomai turi būti galimybė prijungti nuolatinės srovės šaltinį.	802.3at PoE. Galimybė prijungti nuolatinės srovės šaltinį.
11.	Įrenginys turi būti pritaikytas darbui temperatūroje	0 - 50°C	0 - 50°C
12.	Atsparumas aplinkos drėgmei	ne blogiau 5 - 93%	5 - 93%
13.	Energijos sunaudojimas, ne daugiau	16,5 W	16,5 W
14.	Veikimo tipai	Belaidės prieigos taškas turi palaikyti šiuos veikimo tipus: belaidės prieigos taškas, įsibrovimų sistemos sensorius, hibridinis režimas.	Belaidės prieigos taškas palaiko šiuos veikimo tipus: belaidės prieigos taškas, įsibrovimų sistemos sensorius, hibridinis režimas.

15.	Apsaugos priemonės	Turi būti palaikomi šie autentifikavimo protokolai: RADIUS, TACACS + Turi būti palaikomas autentifikavimas per web portalą. Turi būti palaikomas MAC autentifikavimas. Turi būti palaikomas prieigos kontrolės protokolas: 802.1X. Turi būti palaikomi šie prieigos kontrolės metodai: EAP-PEAP (MSCHAPv2) EAP-TLS ir EAP-TTLS;	Palaikomi šie autentifikavimo protokolai: RADIUS, TACACS + Palaikomas autentifikavimas per web portalą. Palaikomas MAC autentifikavimas. Palaikomas prieigos kontrolės protokolas: 802.1X. Palaikomi šie prieigos kontrolės metodai: EAP-PEAP (MSCHAPv2) EAP-TLS ir EAP-TTLS;
16.	RADIUS autorizacijos pakeitimo palaikymas (RFC 3576 arba 5176)	Turi būti palaikoma: RADIUS autorizacijos pakeitimas (RFC 3576 arba 5176)	Palaikoma: RADIUS autorizacijos pakeitimas (RFC 3576 arba 5176)
17.	Duomenų srautų apskaita	RADIUS apskaitos palaikymas	RADIUS apskaitos palaikymas
18.	Virtualūs belaidžiai tinklai (SSID) veikiantys vienu metu, ne mažiau	16	16
19.	Valdymo sąsaja	Saugi WEB/CLI/SNMP sąsaja arba įrenginių valdymo programinė įranga (SSL, SSH ir SNMPv3).	Saugi WEB/CLI/SNMP sąsaja arba įrenginių valdymo programinė įranga (SSL, SSH ir SNMPv3).
20.	Privalomi bevielės prieigos taško veikimo (valdymo) mechanizmai	Autonominis, valdomas bevielės prieigos taško kontrolierio ar jų grupės, debesų tipo valdymas. Jeigu siūlomi bevielės prieigos taškai nepalaiko vieno iš išvardintų režimų, turi būti siūlomi papildomi bevielės prieigos taškai.	Autonominis, valdomas bevielės prieigos taško kontrolierio ar jų grupės, debesų tipo valdymas.
21.	Valdymo funkcijos	Turi būti palaikoma: Automatinis signalo galios reguliavimas; Automatinis kanalo parinkimas ir interferencijos aptikimas; Galios ir spektro analizė – triukšmų aptikimas nuo kitų belaidžių įrenginių; Automatinis klientų perkėlimas į mažiau apkrautus 5GHz kanalus.	Palaikoma: Automatinis signalo galios reguliavimas; Automatinis kanalo parinkimas ir interferencijos aptikimas; Galios ir spektro analizė – triukšmų aptikimas nuo kitų belaidžių įrenginių; Automatinis klientų perkėlimas į mažiau apkrautus 5GHz kanalus.

22.	Suderinamumas	Turi būti suderinama galimybė valdyti belaidės prieigos taškus su belaidžio ryšio prieigos taškų centralizuoto valdymo programine įranga	Suderinama galimybė valdyti belaidės prieigos taškus su belaidžio ryšio prieigos taškų centralizuoto valdymo programine įranga
23.	Montavimas	Laikiklis prieigos taško montavimui prie sienos arba lubų	Laikiklis prieigos taško montavimui prie sienos arba lubų
24.	Garantija	Ne mažiau kaip 5 metai., skaičiuojant nuo įrangos priėmimo-perdavimo akto pasirašymo dienos; Garantinės priežiūros laikotarpiu teikėjas turi garantuoti nemokamą reikalingų dalių tiekimą ir nemokamus remonto darbus bei programinės įrangos atnaujinimas.	5 metai., skaičiuojant nuo įrangos priėmimo-perdavimo akto pasirašymo dienos; Garantinės priežiūros laikotarpiu teikėjas turi garantuoti nemokamą reikalingų dalių tiekimą ir nemokamus remonto darbus bei programinės įrangos atnaujinimas.
25.	Savybės	Visa siūloma įranga turi būti nauja, negalima siūlyti naudotos arba naudotos ir atnaujintos (angl. remarketing/refurbished) įrangos (pateikti deklaraciją)	Nauja, negalima siūlyti naudotos arba naudotos ir atnaujintos (angl. remarketing/refurbished) įrangos (pateikti deklaraciją)

3 lentelė.

Reikalavimai Prieigos komutatoriams.

EilNr	Parametras	Reikalaujama parametro reikšmė	Pasiūlymo duomenys Privaloma išsamiai aprašyti siūlomą parametą. Pasiūlymai, kuriuose bus įrašyta „Taip/Ne“ arba „Atitinka“ bus atmesti kaip neatitinkantys reikalavimų
1.	Gamintojas modelis	Nurodyti pavadinimą, produkto kodą(-us).	Aruba 2530 24G PoE+ Switch
2.	Konstrukcija	1U įrenginys, montuojamas į 19" komutacinę spintą, pateikiamas su montavimo detalėmis, montuojamas horizontaliai.	1U įrenginys, montuojamas į 19" komutacinę spintą, pateikiamas su montavimo detalėmis, montuojamas horizontaliai.
3.	El. maitinimas	220 V AC	220 V AC
4.	Valdymo prievadas	Konsolės prievadas RJ45 arba USB tipo	Konsolės prievadas RJ45 arba USB tipo

5.	10/100/1000BaseT prievadų su automatinio greಿತaveikos atpažinimu ir PoE+ funkcionalumu, ne mažiau (PoE+ arba PoE gali būti naudojama bet kuriame prievade)	24 vnt.	24 vnt.
6.	Bendra komutatoriaus PoE+ galia ne mažiau	240W	240W
7.	SFP 1G prievadų ne mažiau	Ne mažiau 4 vnt.	4 vnt.
8.	MAC adresų lentelės dydis	Ne mažiau kai 16000 įrašų	16000 įrašų
9.	Įrenginio našumas, ne mažiau	55 Gbps, 41 Mpps skaičiuojant 64 baitų paketais. Siūlomi prievadų moduliai turi palaikyti tokio našumo įrenginio vidinę architektūrą.	55 Gbps, 41 Mpps skaičiuojant 64 baitų paketais. Siūlomi prievadų moduliai palaiko tokio našumo įrenginio vidinę architektūrą.
10.	Standartų palaikymas	Naudojami protokolai – STP (IEEE 802.1D), RSTP (IEEE 802.1w), MSTP (802.1s). 802.1s Multiple Spanning tree protokolo palaikymas. IEEE 802.3ad Link Aggregation Control Protocol (LACP) 802.1ab (Link Layer Discovery Protocol) protokolo palaikymas, LLDP-MED (media endpoint discovery). IEEE 802.1v (protocol VLAN), VXLAN	Naudojami protokolai – STP (IEEE 802.1D), RSTP (IEEE 802.1w), MSTP (802.1s). 802.1s Multiple Spanning tree protokolo palaikymas. IEEE 802.3ad Link Aggregation Control Protocol (LACP) 802.1ab (Link Layer Discovery Protocol) protokolo palaikymas, LLDP-MED (media endpoint discovery). IEEE 802.1v (protocol VLAN), VXLAN
11.	Virtualių tinklų ne mažiau	VLAN ir kadų žymėjimo (angl. tagging) palaikymas pilnai turi atitikti 802.1Q standartą ir palaikyti nemažiau 2000 VLAN'ų vienu metu.	VLAN ir kadų žymėjimo (angl. tagging) palaikymas pilnai turi atitikti 802.1Q standartą ir palaikyti nemažiau 2000 VLAN'ų vienu metu.
12.	Virtualių tinklų identifikatorių ne mažiau	4000 VLAN ID	4000 VLAN ID
13.	Maršrutizuojantys protokolai (IPv4/IPv6)	Naudojami protokolai – statinis maršrutizavimas (ne mažiau kaip 250 maršrutų), RIPv1/v2 (10000 maršrutų), RIPng, OSPFv2, OSPFv3, ECMP, PBR	Naudojami protokolai – statinis maršrutizavimas (ne mažiau kaip 250 maršrutų), RIPv1/v2 (10000 maršrutų), RIPng, OSPFv2, OSPFv3, ECMP, PBR

14.	Multicast maršrutizuojantys protokolai	PIM Dense ir Sparse protokolai. IGMPv3 palaikymas, data driven IGMP palaikymas - IP multikastų maršrutizavimas taip pat "IP multicast snooping" mechanizmas.	PIM Dense ir Sparse protokolai. IGMPv3 palaikymas, data driven IGMP palaikymas - IP multikastų maršrutizavimas taip pat "IP multicast snooping" mechanizmas.
15.	Loginis patikimumas	L3 loginio dubliavimo protokolas VRRPv2/v3 (Virtual Router Redundancy Protocol): rezervuotos maršrutizatorių grupės sudarymui.	L3 loginio dubliavimo protokolas VRRPv2/v3 (Virtual Router Redundancy Protocol): rezervuotos maršrutizatorių grupės sudarymui.
16.	IPv6 funkcijos	Turi palaikyti tokias IPv6 savybes: host, Dual Stack (IPv4/IPv6), MLD snooping.	Palaiko tokias IPv6 savybes: host, Dual Stack (IPv4/IPv6), MLD snooping.
17.	Saugumo funkcijos	Access Control Lists (ACL), priskiriami prievadui su galimybe nurodyti L3/L4 parametrus. Komutatoriaus centrinio procesoriaus apsauga (DoS attack prevention). ICMP denial-of-service atakų aptikimas. Prievadų apsauga nuo BPDU atakų ir STP-RG (STP root guard) funkcijos palaikymas. Dinaminė ARP apsauga, apsauga nuo apsimetėlišių DHCP serverių. TACACS+, Radius. Secure Shell (SSHv2). Secure Sockets Layer (SSL). Secure FTP. Vartotojų autentikavimo metodai: IEEE 802.1X,	Access Control Lists (ACL), priskiriami prievadui su galimybe nurodyti L3/L4 parametrus. Komutatoriaus centrinio procesoriaus apsauga (DoS attack prevention). ICMP denial-of-service atakų aptikimas. Prievadų apsauga nuo BPDU atakų ir STP-RG (STP root guard) funkcijos palaikymas. Dinaminė ARP apsauga, apsauga nuo apsimetėlišių DHCP serverių. TACACS+, Radius. Secure Shell (SSHv2). Secure Sockets Layer (SSL). Secure FTP. Vartotojų autentikavimo metodai: IEEE 802.1X,
18.	Valdymo funkcijos, sąsajos	SNMP v1, SNMP v2, SNMP v3, Command Line Interface (CLI), WEB interface. Įrenginys turi turėti REST API sąsają leidžiančią nuskaityti ir keisti įrenginio parametrus Autonominis, centralizuotas lokalus ir debesų tipo valdymas.	SNMP v1, SNMP v2, SNMP v3, Command Line Interface (CLI), WEB interface. Įrenginys turi turėti REST API sąsają leidžiančią nuskaityti ir keisti įrenginio parametrus Autonominis, centralizuotas lokalus ir debesų tipo valdymas.
19.	Srautų stebėjimo funkcijos	RMON, XRMON, sFlow arba NetFlow	RMON, XRMON, sFlow arba NetFlow
20.	Kitos patikimumo funkcijos	Privalo turėti ne mažiau dviejų valdymo programinės įrangos laikmenų (angl.dual flash)	Turi di valdymo programinės įrangos laikmenų (angl.dual flash)

21.	Programinės įrangos atnaujinimas	Turi būti užtikrintas nemokamas visos programinės įrangos naujų versijų pateikimas bei visų reikalingų licencijų palaikymas garantiniu laikotarpiu.	Užtikrintas nemokamas visos programinės įrangos naujų versijų pateikimas bei visų reikalingų licencijų palaikymas garantiniu laikotarpiu.
22.	Surinkimo reikalavimai	Visos siūlomos dalys privalo būti komplektuojamos komutatoriaus gamintojo ir pažymėtos komutatoriaus gamintojo kodais. Visa įranga turi būti gamykliškai nauja „brand new“. Gamykliškai atnaujinti „renew“ / „refurbished“ / „remarked“ komponentai neleistini.	Visos siūlomos dalys komplektuojamos komutatoriaus gamintojo ir pažymėtos komutatoriaus gamintojo kodais. Visa įranga turi būti gamykliškai nauja „brand new“. Gamykliškai atnaujinti „renew“ / „refurbished“ / „remarked“ komponentai neleistini.
23.	Gamintojo katalogas ar jo kopija	Būtina pridėti katalogą, aprašą ar kitą gaminio dokumentą (jo kopiją) arba pateikti nuorodą į elektroninį prekės katalogą (aprašą) gamintojo interneto svetainėje. Visi specifikacijoje reikalaujami techniniai parametrai turi būti kataloge (aprašė).	https://www.arubanetworks.com/products/switches/access/2530-series/
24.	Garantinė techninė priežiūra	Įrangai taikoma gamintojo užtikrinta 5 metų garantija. Reikalavimas privalo būti garantuojamas gamintojo (pateikti tai liudijančią gamintojo dokumentaciją jei tai yra standartinis oficialus gamintojo išipareigojimas arba komplektuoti papildomą gamintojo serviso paketą nurodant pasiūlyme jo kodą ir pavadinimą).	Įrangai taikoma gamintojo užtikrinta 5 metų garantija. Reikalavimas garantuojamas gamintojo https://www.arubanetworks.com/products/switches/access/2530-series/
25.	Sertifikatas	CE (arba lygiavertis) ženklas (pateikti sertifikatą)	CE (arba lygiavertis) ženklas (pateikti sertifikatą)

4 lentelė.

Tinklo vartotojų bei prietaisų autentifikavimo programinė įranga.

Eil. Nr.	Parametras	Reikalaujama parametro reikšmė	Pasiūlymo duomenys Privaloma išsamiai aprašyti siūlomą parametą. Pasiūlymai, kuriuose bus įrašyta „Taip/Ne“ arba „Atitinka“ bus atmesti kaip neatitinkantys reikalavimų
1.	Gamintojas modelis	Nurodyti pavadinimą, produkto kodą(-us).	Aruba ClearPass
2.	Gamintojas	Nurodyti gamintojo ir gamintojo kodą.	

3.	Įrenginys	Belaidžių, laidinių tinklų ir nuotolinio prisijungimo prieigos autentifikavimo sprendimas.	Belaidžių, laidinių tinklų ir nuotolinio prisijungimo prieigos autentifikavimo sprendimas.
4.	Licencijos	Ne mažiau kaip 100 įrenginių autentifikavimui vienu metu iskaitant svečių pasijungimus. Visi įrenginiai turi būti profiliuojami. TACACS+ palaikymas Vienu metu ne mažiau kaip 100 vartotojų BYOD įrenginių. Vienu metu ne mažiau kaip 100 vnt įrenginių sveikatos būklės patikrinimui (angl. k. Health check)	100 įrenginių autentifikavimui vienu metu iskaitant svečių pasijungimus. Visi įrenginiai profiliuojami. TACACS+ palaikymas Vienu metu 100 vartotojų BYOD įrenginių. Vienu metu 100 vnt įrenginių sveikatos būklės patikrinimui (angl. k. Health check)
5.	Suderinamumas su hypervizoriais	Siūlomas sprendimas turi veikti debesijos platformoje Microsoft Azure ir taip pat turi būti suderinamas su šiais hypervizoriais: • VMware ESXi; • Microsoft Hyper-V.	Siūlomas sprendimas veikia debesijos platformoje Microsoft Azure ir taip pat turi būti suderinamas su šiais hypervizoriais: • VMware ESXi; • Microsoft Hyper-V.
6.	Aukšto patikimumo išpildymas	Aukšto patikimumo aprašas yra pateiktas Bendrųjų reikalavimų prieigos sistemos visumai 2.d punkte.	Aukšto patikimumo aprašas yra pateiktas Bendrųjų reikalavimų prieigos sistemos visumai 2.d punkte.
7.	Autentifikavimo, prieigos kontrolės protokolai, prieigos kontrolės metodai	Turi būti palaikomi šie autentifikavimo protokolai: • RADIUS; • RADIUS CoA • TACACS+. Turi būti palaikomas autentifikavimas per WEB portalą. Turi būti palaikomas MAC autentifikavimas. Turi būti palaikomas 802.1X. prieigos kontrolės protokolas. • Turi būti palaikomi šie prieigos kontrolės metodai:PEAP (MSCHAPv2); • EAP-TLS. • EAP-FAST • OAuth2 • OSCP • Windows machine authentication	Palaikomi šie autentifikavimo protokolai: • RADIUS; • RADIUS CoA • TACACS+. Palaikomas autentifikavimas per WEB portalą. Palaikomas MAC autentifikavimas. Palaikomas 802.1X. prieigos kontrolės protokolas. • Palaikomi šie prieigos kontrolės metodai:PEAP (MSCHAPv2); • EAP-TLS. • EAP-FAST • OAuth2 • OSCP Windows machine authentication
8.	Autentifikavimo šaltiniai	Turi būti palaikomi šie autentifikavimo šaltiniai: • Microsoft Active Directory; • Integruota SQL duomenų bazė; • Nutolusi Microsoft SQL duomenų bazė	Palaikomi šie autentifikavimo šaltiniai: • Microsoft Active Directory; • Integruota SQL duomenų bazė;

		• LDAP vartotojų duomenų bazė • Tokenų serveris • Kerberos • Microsoft Azure Active Directory • Google G Suite	• Nutolusi Microsoft SQL duomenų bazė • LDAP vartotojų duomenų bazė • Tokenų serveris • Kerberos • Microsoft Azure Active Directory • Google G Suite
9.	Įrenginių profiliavimas	Turi būti palaikomi šie įrenginių profiliavimo metodai: Aktyvūs: • Nmap atidarytų prievadų skenavimas • WMI • SSH • SNMP Pasyvūs: • MAC OUI • DHCP • sFLOW • HTTP User agent • TCP Jeigu siūlomas sprendimas nepalaiko išvardytų reikalavimų, prie sprendimo galima siūlyti papildomą programinę įrangą, kuri kartu su siūlomu sprendimu užtikrintų reikalavimų atitikimą.	Palaikomi šie įrenginių profiliavimo metodai: Aktyvūs: • Nmap atidarytų prievadų skenavimas • WMI • SSH • SNMP Pasyvūs: • MAC OUI • DHCP • sFLOW • HTTP User agent • TCP
10.	RADIUS apskaitos palaikymas (RFC 2866) RADIUS autorizacijos pakeitimo palaikymas (RFC 3576 arba 5176)	Turi būti palaikoma: • RADIUS apskaita (RFC 2866); • RADIUS autorizacijos pakeitimas (RFC 3576 arba 5176).	RADIUS apskaitos palaikymas (RFC 2866) RADIUS autorizacijos pakeitimo palaikymas (RFC 3576 arba 5176)
11.	Įrenginių profiliavimas	Prijungti prie tinklo klientų įrenginiai turi būti profiliuojami. Turi būti nustatomos klientų įrenginių naudojamos operacinės sistemos, jų versijos, įrenginio gamintojas, įrenginio tipas (kompiuteris, mobilus telefonas, spausdintuvas)	Prijungti prie tinklo klientų įrenginiai profiliuojami. Nustatomos klientų įrenginių naudojamos operacinės sistemos, jų versijos, įrenginio gamintojas, įrenginio tipas (kompiuteris, mobilus telefonas, spausdintuvas)
12.	Vartotojų asmeninių įrenginių	Siūlomas sprendimas turi turėti toliau išvardintas galimybes: • Savitarnos portalas, leidžiantis vartotojams prijungti asmeninius	Siūlomas sprendimas turi turėti toliau išvardintas galimybes: • Savitarnos portalas, leidžiantis vartotojams prijungti

	autentifikavimas	įrenginius prie saugaus kompiuterinio tinklo; Integruota sertifikatų išdavimo ir valdymo tarnyba, skirta sertifikatų išdavimui vartotojų asmeniniams įrenginiams. Jeigu siūlomas sprendimas nepalaiko išvardytų reikalavimų, prie sprendimo galima siūlyti papildomą programinę įrangą, kuri kartu su siūlomu sprendimu užtikrintų reikalavimų atitikimą.	asmeninius įrenginius prie saugaus kompiuterinio tinklo; Integruota sertifikatų išdavimo ir valdymo tarnyba, skirta sertifikatų išdavimui vartotojų asmeniniams įrenginiams.
13.	Svečių autentifikavimas	Siūloma sprendimas turi palaikyti toliau išvardintas svečių autentifikavimo galimybes: - Svečių autentifikavimas naudojant WEB portalą; - Svečių autentifikavimo užklausų siuntimas (SMS arba elektroniniai laiškais) tinklo administratoriui; - Tinklo administratorius turi turėti galimybę patvirtinti svečio užklausas. - Svečių autentifikavimas naudojant socialinių tinkle prisijungimo duomenis: Facebook, LinkedIn ir kiti. Jeigu siūlomas sprendimas nepalaiko išvardytų reikalavimų, prie sprendimo galima siūlyti papildomą programinę įrangą, kuri kartu su siūlomu sprendimu užtikrintų reikalavimų atitikimą.	Siūloma sprendimas palaiko toliau išvardintas svečių autentifikavimo galimybes: - Svečių autentifikavimas naudojant WEB portalą; - Svečių autentifikavimo užklausų siuntimas (SMS arba elektroniniai laiškais) tinklo administratoriui; - Tinklo administratorius turi turėti galimybę patvirtinti svečio užklausas. - Svečių autentifikavimas naudojant socialinių tinkle prisijungimo duomenis: Facebook, LinkedIn ir kiti.
14.	Vartotojų įrenginių sveikatos būklės patikrinimo galimybė	Galimybė	Yra
15.	Valdymo sąsaja, autentifikavimo užklausų statistika	Turi būti: - Grafinė WEB sąsaja; - Grafinis statistikos atvaizdavimas su visais vartotojais ir įrenginiais prisijungusiais ar besijungiančiais į duomenų tinklą; - Autentifikavimo istorinių duomenų kaupimas.	Yra: - Grafinė WEB sąsaja; - Grafinis statistikos atvaizdavimas su visais vartotojais ir įrenginiais prisijungusiais ar besijungiančiais į duomenų tinklą;

			Autentifikavimo istorinių duomenų kaupimas.
16.	REST API sąsaja	Siūlomas sprendimas turi turėti REST API sąsają, papildomai integracijai su kliento sistemomis.	Siūlomas sprendimas turi REST API sąsają, papildomai integracijai su kliento sistemomis.
17.	Trečių šalių programinės įrangos integracija	Siūlomas sprendimas turi palaikyti integraciją su trečių šalių sprendimais: MDM sistemomis MS Intune, MobileIron, Airwatch; Ugniasienėmis	Siūlomas sprendimas palaiko integraciją su trečių šalių sprendimais: MDM sistemomis MS Intune, MobileIron, Airwatch; Ugniasienėmis
18.	Plėtimas ir aukštas patikimumas	Turi būti užtikrintas aukštas patikimumas (angl. high availability) prijungiant antrą virtualų įrenginį.	Užtikrintas aukštas patikimumas (angl. high availability) prijungiant antrą virtualų įrenginį.
19.	Garantija	Ne mažiau kaip 3 metų gamintojo ar gamintojo autorizoto garantinio aptarnavimo garantija, skaičiuojant nuo įrangos priėmimo-perdavimo akto pasirašymo dienos. Garantinės priežiūros laikotarpiu gamintojas turi garantuoti nemokamą reikalingų dalių tiekimą ir nemokamus remonto darbus. Garantinės priežiūros laikotarpiu gamintojas turi garantuoti programinės įrangos atnaujinimus, klaidų šalinimus bei pagalbą sprendžiant siūlomos programinės įrangos sutrikimus. Garantinių paslaugų tiekimo laikas 24 (dvidešimt keturios) valandos per parą ir 7 (septynios) dienos per savaitę. Reakcijos į incidentus laikas ne ilgiau kaip 2 (dvi) valandos.	3 metų gamintojo ar gamintojo autorizoto garantinio aptarnavimo garantija, skaičiuojant nuo įrangos priėmimo-perdavimo akto pasirašymo dienos. Garantinės priežiūros laikotarpiu gamintojas turi garantuoti nemokamą reikalingų dalių tiekimą ir nemokamus remonto darbus. Garantinės priežiūros laikotarpiu gamintojas turi garantuoti programinės įrangos atnaujinimus, klaidų šalinimus bei pagalbą sprendžiant siūlomos programinės įrangos sutrikimus. Garantinių paslaugų tiekimo laikas 24 (dvidešimt keturios) valandos per parą ir 7 (septynios) dienos per savaitę. Reakcijos į incidentus laikas ne ilgiau kaip 2 (dvi) valandos.

5 lentelė. Tinklo įrangos valdymo ir stebėjimo programinė įranga.

Eil. Nr.	Parametras	Reikalaujama parametro reikšmė	Pasiūlymo duomenys Privaloma išsamiai aprašyti siūlomą parametrą. Pasiūlymai, kuriuose bus įrašyta „Taip/Ne“ arba „Atitinka“ bus atmesti kaip neatitinkantys reikalavimų
1.	Gamintojas modelis	Nurodyti pavadinimą, produkto kodą(-us).	Aruba Centra
2.	Įrenginys	Tinklo įrangos valdymo programinės įrangos licencija arba prenumerata.	Tinklo įrangos valdymo programinės įrangos prenumerata.
3.	Tipas	Valdymo programinė įranga turi būti „debesijos“ tipo. Jeigu siūloma valdymo programinė įranga tokio funkcionalumo neturi, galima siūlyti kitą sprendimą patalpintą virtualioje aplinkoje bei į pasiūlymą įtraukti visus su tokiu sprendimo įgyvendinimu susijusius kaštus. Toks sprendimas turi užtikrinti aukšto patikimumo bei saugaus prisijungimo iš bet kur reikalavimus.	Valdymo programinė įranga „debesijos“ tipo.
4.	Gamintojas	Nurodyti.	Aruba
5.	Programinės įrangos aprašymas	Užtikrina visų siūlomų tinklo įrenginių centralizuotą valdymą ir stebėjimą.	Užtikrina visų siūlomų tinklo įrenginių centralizuotą valdymą ir stebėjimą.
6.	Orkestravimas	Sistema turi orkestruoti dinaminį šifruotų ryšių (tunelių) užmezgimą, atliktų šifravimo raktų atnaujinimą tarp prieigos valdiklių bei VPN koncentratorių. Sistema turi užtikrinti dinaminę maršrutų sklaidą tarp skirtingų Užsakovo lokacijų.	Sistema orkestruoja dinaminį šifruotų ryšių (tunelių) užmezgimą, atliktų šifravimo raktų atnaujinimą tarp prieigos valdiklių bei VPN koncentratorių. Sistema turi užtikrinti dinaminę maršrutų sklaidą tarp skirtingų Užsakovo lokacijų.
7.	Gedimų indikavimas	Sistema mašininio mokymosi ir dirbtinio intelekto pagalba turi gebėti atpažinti ir informuoti apie galimus gedimus tinklo infrastruktūroje	Sistema mašininio mokymosi ir dirbtinio intelekto pagalba turi gebėti atpažinti ir informuoti apie galimus gedimus tinklo infrastruktūroje

8.	Belaidžio tinklo padengimo stebėjimas	Turi būti funkcionalumas parodantis valdomų prieigos taškų kuriamą belaidžio ryšio padengimą (Heatmap) realiu laiku.	Funkcionalumas parodantis valdomų prieigos taškų kuriamą belaidžio ryšio padengimą (Heatmap) realiu laiku.
9.	Suderinamumas su tinklo įranga	Siūlomas sprendimas turi integruotis su siūlomu vartotojų autentifikavimo sprendimu, komutatoriais ir prieigos taškais.	Siūlomas sprendimas integruojasi su siūlomu vartotojų autentifikavimo sprendimu, komutatoriais ir prieigos taškais.
10.	Tinklo topologija	Siūlomas sprendimas turi gebėti atvaizduoti sistemoje įtrauktus įrenginius vizualiai, atvaizduojant komutatorių, belaidės prieigos taškų ir kitų stebimų įrenginių tarpusavio fizinius sujungimus.	Siūlomas sprendimas geba atvaizduoti sistemoje įtrauktus įrenginius vizualiai, atvaizduojant komutatorių, belaidės prieigos taškų ir kitų stebimų įrenginių tarpusavio fizinius sujungimus.
11.	Orkestruojamų VPN sujungimų stebėjimas	Siūlomas sprendimas turi turėti galimybę atvaizduoti perkančiosios organizacijos tinklo VPN tunelius tarp užsakovo duomenų centro ir padalinių.	Siūlomas sprendimas turi galimybę atvaizduoti perkančiosios organizacijos tinklo VPN tunelius tarp užsakovo duomenų centro ir padalinių.
12.	Belaidės prieigos klientų prisijungimų parametrų stebėjimas	Siūlomas sprendimas turi stebėti ir atvaizduoti perkančiosios organizacijos išigijamų belaidės prieigos taškų siunčiamą informaciją susietą su belaidės prieigos klientų kokybinių parametrų stebėjimu: autentikacija, autorizacija, DHCP, DNS.	Siūlomas sprendimas stebi ir atvaizduoti perkančiosios organizacijos išigijamų belaidės prieigos taškų siunčiamą informaciją susietą su belaidės prieigos klientų kokybinių parametrų stebėjimu: autentikacija, autorizacija, DHCP, DNS.
13.	Saugūs valdymo protokolai	Sprendimo komunikacija su tinklo įranga turi būti paremta tik saugiais valdymo protokolais: SSH arba SNMPv3, arba HTTPS.	Sprendimo komunikacija su tinklo įranga paremta tik saugiais valdymo protokolais: SSH arba SNMPv3, arba HTTPS.

14.	API sąsaja	Siūlomas sprendimas turi turėti API sąsają, papildomai integracijai su kliento sistemomis.	Siūlomas sprendimas turi API sąsają, papildomai integracijai su kliento sistemomis.
15.	Konfigūravimas	Sprendimas turi palaikyti: • Centralizuotą tinklo įrenginių prievadų, prieigos taisyklių, VLAN, QoS konfigūravimą per sprendimo grafinę sąsają, be tiesioginio tinklo administratoriaus jungimosi į konfigūruojamus įrenginius; • Konfigūracijos šablonų konfigūravimą; • Konfigūracijų valdymas: konfigūracijos turi būti audituojamos ir registruojamos. • Suderinamo tinklo įrangos programinės įrangos atnaujinimų diegimas pagal laiko grafikus.	Sprendimas palaiko: • Centralizuotą tinklo įrenginių prievadų, prieigos taisyklių, VLAN, QoS konfigūravimą per sprendimo grafinę sąsają, be tiesioginio tinklo administratoriaus jungimosi į konfigūruojamus įrenginius; • Konfigūracijos šablonų konfigūravimą; • Konfigūracijų valdymas: konfigūracijos turi būti audituojamos ir registruojamos. Suderinamo tinklo įrangos programinės įrangos atnaujinimų diegimas pagal laiko grafikus.
16.	Automatizuoti pranešimai	Sprendime turi būti galimybė konfigūruoti išpėjamuosius pranešimus pagal tam tikrus tinklo įrenginių parametrus gautus iš tinklo įrenginių apie: CPU, RAM, prievadų utilizavimo lygį, VPN tunelio būseną. Išpėjimai apie įvykius, turi būti išsiunčiami per elektroninį pašta.	Sprendime yra galimybė konfigūruoti išpėjamuosius pranešimus pagal tam tikrus tinklo įrenginių parametrus gautus iš tinklo įrenginių apie: CPU, RAM, prievadų utilizavimo lygį, VPN tunelio būseną. Išpėjimai apie įvykius, turi būti išsiunčiami per elektroninį pašta.
17.	Tinklo įrenginių parametrų atvaizdavimas	Sprendime turi būti ši funkcija: • Grafikų piešimą pagal tinklo įrenginių parametrus: CPU, RAM, prievadų ir radijo dažnių utilizavimo lygį, VPN	Sprendime yra ši funkcija: Grafikų piešimą pagal tinklo įrenginių

		tunelių kokybinių parametrų atvaizdavimas.	parametrus: CPU, RAM, prievadų ir radijo dažnių utilizavimo lygį, VPN tunelių kokybinių parametrų atvaizdavimas.
18.	Belaidžio tinklo saugumo funkcijos	Sprendimas turi aptikti nesankcionuotai prie tinklo prijungtus belaidės prieigos taškus.	Sprendimas aptinka nesankcionuotai prie tinklo prijungtus belaidės prieigos taškus.
19.	Garantija	Ne mažiau kaip 3 metų gamintojo ar gamintojo autorizoto garantinio aptarnavimo garantija, skaičiuojant nuo įrangos priėmimo-perdavimo akto pasirašymo dienos. Garantinės priežiūros laikotarpiu gamintojas turi garantuoti nemokamą reikalingų dalių tiekimą ir nemokamus remonto darbus. Garantinės priežiūros laikotarpiu gamintojas turi garantuoti programinės įrangos atnaujinimus, klaidų šalinimus bei pagalbą sprendžiant siūlomos programinės įrangos sutrikimus. Garantinių paslaugų tiekimo laikas 24 (dvidešimt keturios) valandos per parą ir 7 (septynios) dienos per savaitę. Reakcijos į incidentus laikas ne ilgiau kaip 2 (dvi) valandos.	3 metų gamintojo ar gamintojo autorizoto garantinio aptarnavimo garantija, skaičiuojant nuo įrangos priėmimo-perdavimo akto pasirašymo dienos. Garantinės priežiūros laikotarpiu gamintojas turi garantuoti nemokamą reikalingų dalių tiekimą ir nemokamus remonto darbus. Garantinės priežiūros laikotarpiu gamintojas turi garantuoti programinės įrangos atnaujinimus, klaidų šalinimus bei pagalbą sprendžiant siūlomos programinės įrangos sutrikimus. Garantinių paslaugų tiekimo laikas 24 (dvidešimt keturios) valandos per parą ir 7 (septynios) dienos per savaitę. Reakcijos į incidentus laikas ne ilgiau kaip 2 (dvi) valandos.
20.	Suderinamumas	Turi būti to paties gamintojo, kaip ir siūlomi tinko įrenginiai bei pilnai suderinama su siūlomais tinklo komutatoriais.	To paties gamintojo, kaip ir siūlomi tinko įrenginiai bei pilnai suderinama su

			siūlomais tinklo komutatoriais.
--	--	--	---------------------------------

5. Vykdam sutartį pasitelksiu šiuos subteikėjus (subteikėjus, subrangovus)*:

Eil. Nr.	Subrangovo (-ų), subteikėjo (-ų) ar subteikėjo (-ų) pavadinimas (-ai)	Subrangovo (-ų), subteikėjo (-ų) ar subteikėjo (-ų) adresas (-ai)	Įsipareigojimų dalis (nurodant konkrečius pagal sutartį prisiimamus įsipareigojimus), kuriai ketinama pasitelkti subteikėją (-us)

*Pildyti tuomet, jei tiekėjas ketina pasitelkti subrangovą (-us), subteikėją (-us) ar subteikėją (-us)

6. Kiti su pasiūlymu pateikiami dokumentai:

Eil. Nr.	Pateiktas dokumentas ir/ar informacija	Ar nurodytame dokumente pateikiama informacija yra konfidenciali informacija (komercinė paslaptis)** Taip/Ne)

**Tokią informaciją sudaro, visų pirma, komercinė (gamybinė) paslaptis ir konfidencialieji pasiūlymų aspektai. Informacija, kurią viešai skelbti įpareigoja Lietuvos Respublikos įstatymai, negali būti paslaugų teikėjo nurodoma kaip konfidenciali.

Nurodant konfidencialią informaciją, rekomenduojama vadovautis Viešųjų pirkimų tarnybos išaiškinimu, kuris paskelbtas Viešųjų pirkimų tarnybos internetinėje svetainėje, adresu: <http://vpt.lrv.lt/lt/naujienos/kaip-turi-buti-suprantamas-konfidencialumas-viesuosiuose-pirkimuose>

Atkreiptinas dėmesys, kad vadovaudamasi Viešųjų pirkimų įstatymu, Perkančioji organizacija paskelbs sudarytą pirkimo sutartį ir laimėtojo pasiūlymą. Todėl paslaugų teikėjas turi būti atidus, rengdamas savo pasiūlymą, ir tuo atveju, jei pasiūlyme yra konfidenciali informacija, teikiant pasiūlymą ją aiškiai nurodyti. **Tiekėjas negali nurodyti, kad konfidencialus yra pasiūlymo įkainis, kaina arba, kad visas pasiūlymas yra konfidencialus.** Tiekėjui nenurodžius, kokia informacija yra konfidenciali, laikoma, kad konfidencialios informacijos pasiūlyme nėra.

7. Laimėjimo atveju už sutarties vykdymą skiriame atsakingą (sutarties projekto 8.6 papunktis) ir sutartį pasirašantįjį asmenį (-is):

Eil. Nr.	Pateikiami duomenys	Asmuo, atsakingas už sutarties vykdymą	Asmuo, pasirašantis sutartį
1.	Vardas, pavardė, pareigos	Verslo spendimų pardavimo vadovas	Generalinis direktorius
2.	Atstovavimo pagrindas***	-	-
3.	Telefonas	+37068580465	+37052059895
4.	Faksas	+37052059899	+37052059899
5.	El. paštas	karolis.marcinkevicius@fortevento.lt	aurelijus.saltenis@fortevento.lt

***duomenys (Eil. Nr. 2) pateikiami tik sutartį pasirašančiojo asmens, t. y. veikiantis pagal įmonės įstatus (nuostatus); jei sutartį pasirašys įgaliotas asmuo, nurodoma, kad veikiantis pagal įgaliojimą (data, numeris).

Generalinis direktorius

(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas)

(Parašas)

Aurelijus Šaltenis

(Vardas ir pavardė)

