Eil. Nr. / No.	Techninėje specifikacijoje nurodyti prekių techniniai parametrai		Technical parameters for parts provided in technical specification		Siūlomų prekių techniniai parametrai ir kiti duomenys / Specifications and other details for suggested parts	Pasiūlymo dokumentai patvirtinantys siūlomos prekės techninius parametrus / Documents which confirms technical specifications of suggested	
						Dokumento pavadinimas / Document name	Pasiūlymo lapo numeris arba nuoroda į gamintojo tinklalapį / Offer sheet number or reference to manufacturer's page
	Rodiklis	**Reikalavimas**	**Indicator**	**Requirement**	***Nurodo Tiekėjas: / Provided by supplier:***		
1.	**Korporatyvinio tinklo ugniasienių aukšto patikimumo sistema (toliau - Sistema) / Corporate Network Firewall High Reliability System (Furth. - System)**						
1.1	Sistemos pavadinimas ir modelis (gamintojo suteiktas numeris (kodas))	Nurodomas sistemos komponentų pavadinimas ir modelis (gamintojo suteiktas numeris (kodas))	System name and model (manufacturer's identification number (code))	Name and model of system components are provided (manufacturer's identification number (code))	*FortiGate 1100E*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	
1.2	Gamintojas (pavadinimas)	Nurodomas sistemos gamintojas	Manufacturer (name)	System manufacturer is provided	*Fortinet*		
1.3	**Sistemos charakteristikos**		**System characteristics**				
1.3.1	Sistemos funkcionalumo aprašymas	Specializuotas identiškai atitinkantis aparatinis–programinis sprendimas, skirtas užtikrinti: vidinio perimetro kontrolę,; įsibrovimų aptikimą ir prevenciją, antivirusinę programinę įrangą; srautų turinio kontrolę. Sprendimą turi sudaryti ne mažiau kaip 2 vienas kitą dubliuojantys įrenginiai, sujungti į aukšto patikimumo sistemą.	Description of system functionality	Specialized identically matching hardware-software solution designed to provide: control of the inner perimeter; intrusion detection and prevention; anti-virus software; Controlling the content of streams. The solution must consist of at least 2 duplicate devices connected in a high-availability system	Specializuotas identiškai atitinkantis aparatinis–programinis sprendimas, skirtas užtikrinti: vidinio perimetro kontrolę,; įsibrovimų aptikimą ir prevenciją, antivirusinę programinę įrangą; srautų turinio kontrolę. Sprendimą turi sudaryti ne mažiau kaip 2 vienas kitą dubliuojantys įrenginiai, sujungti į aukšto patikimumo sistemą.	https://www.fortinet.com/products/next-generation-firewall	
1.3.2	Sistema turi dirbti Aktyvus/Pasyvus (*angl* Active/Passive) ir Aktyvus/Aktyvus (*angl* Active/Active) režimais	Sistema dirba Aktyvus/Pasyvus (*angl* Active/Passive) ir Aktyvus/Aktyvus (*angl* Active/Active) režimais	System must be able to operate in Active / Passive and Active / Active modes	System can operate in Active / Passive and Active / Active modes	Sistema dirba Aktyvus/Pasyvus (*angl* Active/Passive) ir Aktyvus/Aktyvus (*angl* Active/Active) režimais	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_FGCP_ap_aa.htm	
1.3.3	Sutrikus aktyvaus įrenginio veikimui aukšto patikimumo sistema turi automatiškai persijungti į dubliuojantį įrenginį	Sutrikus aktyvaus įrenginio veikimui aukšto patikimumo sistema automatiškai persijungia į dubliuojantį įrenginį	In the event of active device malfunction high-availability system must automatically switch to the backup device	In the event of active device malfunction high-availability system automatically switches to the backup device	Sutrikus aktyvaus įrenginio veikimui aukšto patikimumo sistema automatiškai persijungia į dubliuojantį įrenginį	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_FGCP_failover.htm	
1.3.4	Konfigūracija tarp aukšto patikimumo sistemos įrenginių turi būti automatiškai sinchronizuojama	Konfigūracija tarp aukšto patikimumo sistemos įrenginių automatiškai sinchronizuojama	Configuration between high-availability system devices must be automatically synchronized	Configuration between high-availability system devices is automatically synchronized	Konfigūracija tarp aukšto patikimumo sistemos įrenginių automatiškai sinchronizuojama	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverSyncConfig.htm	
1.3.5	Sistema turi užtikrinti, kad persijungimo metu aktyvios sesijos nenutrūktų	Sistema užtikrina, kad persijungimo metu aktyvios sesijos nenutrūktų	System must ensure that active sessions are not interrupted during the switch between systems	System ensures that active sessions are not interrupted during the switch between systems	Sistema užtikrina, kad persijungimo metu aktyvios sesijos nenutrūktų	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_SessPickupEnabling.htm	
1.3.6	Sistemą sudarantys įrenginiai turi stebėti tinklo prievadų būseną	Sistemą sudarantys įrenginiai stebi tinklo prievadų būseną	Devices that make up the system must be able to monitor status of network ports	Devices that make up the system can monitor status of network ports	Sistemą sudarantys įrenginiai stebi tinklo prievadų būseną	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverLink.htm	
1.3.7	Sistemą sudarantis kiekvienas įrenginys turi stebėti ar yra pasiekiami nurodyti IP adresai (*angl*. track IP). Jei nurodyti IP adresai yra nepasiekiami, sistema turi automatiškai persijungti į dubliuojantį įrenginį	Sistemą sudarantis kiekvienas įrenginys stebi ar yra pasiekiami nurodyti IP adresai (*angl*. track IP). Jei nurodyti IP adresai yra nepasiekiami, sistema automatiškai persijungia į dubliuojantį įrenginį	System must be able to monitor each device for availability of specified IP addresses (track IPs). If specified IP addresses are unavailable, system must automatically switch to the backup device	System can monitor each device for availability of specified IP addresses (track IPs). If specified IP addresses are unavailable, system must automatically switch to the backup device	Sistemą sudarantis kiekvienas įrenginys stebi ar yra pasiekiami nurodyti IP adresai (*angl* track IP). Jei nurodyti IP adresai yra nepasiekiami, sistema automatiškai persijungia į dubliuojantį įrenginį	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-high-availability/HA_failoverRemoteLink.htm	

1.3.8	Turi būti galimybė pagal poreikį pajungti į sistema	Ne mažiau kaip **2** tokius pačius įrenginius	It must be possible to connect higher number of devices to the system as needed	At least **2** identical devices	Ne mažiau kaip **2** tokius pačius įrenginius	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_FGCP_more-than-two.htm	
1.3.9	Kiekviename atskirame įrenginyje įdiegtų 1000Base-T arba 1000Base-SX prievadų skaičius *1000Base-SX prievadai turi būti to paties gamintojo kaip ir įrenginys arba kito gamintojo, oficialiai patvirtinti naudoti ugniasienės gamintojo (tokiu atveju prie pasiūlymo pridedamas ugniasienės gamintojo patvirtinimas)*	Ne mažiau kaip **4**	The number of 1000Base-T or 1000Base-SX ports installed on each individual device *1000Base-SX ports must be from the same manufacturer as the device or another manufacturer, officially approved for use by the firewall manufacturer (in that case the offer should be accompanied by a firewall manufacturer's approval)*	No less than **4**	*16*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.3.10	Kiekviename atskirame įrenginyje įdiegtų 10GBase-SR SFP+ prievadų skaičius *Prievadai turi būti to paties gamintojo kaip ir įrenginys arba kito gamintojo, oficialiai patvirtinti naudoti ugniasienės gamintojo (tokiu atveju prie pasiūlymo pridedamas ugniasienės gamintojo patvirtinimas)*	Ne mažiau kaip **4**	Number of 10GBase-SR SFP + ports installed on each individual device *Ports must be from the same manufacturer as the device or another manufacturer, officially approved for use by the firewall manufacturer (in which case firewall shall be accompanied by firewall manufacturer's approval)*	No less than **4**	*Su FN-TRAN-SFP+SR*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 ir 6 psl.*
1.3.11	Kiekviename atskirame įrenginyje įdiegtų lizdų, kuriuose būtų galima įdiegti 40G prievadus, skaičius	Ne mažiau kaip **2**	Number of sockets installed on each individual device that can accommodate 40G ports	No less than **2**	*2*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.3.12	Kiekviename atskirame įrenginyje įdiegtų atskirų prievadų, skirtų įrenginiams sujungti į aukšto patikimumo sistemą ir komplektuotų reikalingais moduliais, skaičius	Ne mažiau kaip **2**	Number of ports installed in each individual device to connect the devices to a high-reliability system and equipped with required modules	No less than **2**	*2*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.3.13	Kiekviename atskirame įrenginyje įdiegtų papildomų konsolės (angl. Console) prievadų skaičius	Ne mažiau kaip **1**	Number of console ports installed on each individual device	No less than **1**	*1*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.3.14	Kiekviename atskirame įrenginyje įdiegtų papildomų 1000Base-T prievadų, skirtų įrenginiams valdyti, skaičius	Ne mažiau kaip **1**	Number of additional 1000Base-T ports installed on each individual device for device management	No less than **1**	*1*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.3.15	Kiekvieno atskiro įrenginio ugniasienės pralaidumas (angl. Firewall throughput), esant Enterprise mix tipo duomenų srautui arba esant UDP1518 srautui	Ne mažesnė kaip **39** Gbps,esant Enterprise mix tipo duomenų srautui arba ne mažesnė kaip **75** Gbps, esant UDP1518 srautui	Firewall throughput for each individual device with Enterprise mix type traffic or UDP1518 traffic	At least **39 Gbps** for Enterprise mix data traffic or at least **75 Gbps** for UDP1518 traffic	*80 Gbps esant UDP1518*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.3.16	Kiekvieno atskiro įrenginio ugniasienės naudojant aplikacijų protokolų kontrolę (angl. Application Control) ir įsilaužimų kontrolę (angl. Intrusion Prevention System) greitaveika, esant Enterprise mix tipo duomenų srautui	Ne mažesnė kaip **9,5** Gbps	Throughput of each individual device using Application Control and Intrusion Prevention System for Enterprice mix traffic	No less than **9,5** Gbps	*9,8 Gbps*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.3.17	Kiekvieno atskiro įrenginio ugniasienės naudojant programų protokolų kontrolę (angl. Application control) ir įsilaužimų kontrolę (angl. Intrusion prevension system) bei apsaugą nuo virusų, URL filtravimą, Anti-Bot apsaugą greitaveika, esant Enterprise mix tipo arba HTTP 21kB duomenų srautui	Ne mažesnė kaip **7** Gbps	Throughput of each individual device while using Application control, Intrusion prevention, virus protection, URL filtering, Anti-Bot protection for Enterprise mix or HTTP 21 kB traffic	No less than **7** Gbps	*7.1 Gbps*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*

1.3.18	Kiekvieno atskiro įrenginio IPSEC VPN greitaveika, esant idialioms testavimo sąlygoms	Ne mažesnė kaip **10** Gbps	IPSEC VPN performance of each individual device under ideal test conditions	No less than **10** Gbps	*48 Gbps*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.3.19	Kiekviename atskirame įrenginyje veikiančių konkurentinių sesijų skaičius, esant idialioms testavimo sąlygoms	Ne mažiau kaip **8000000**	Number of concurrent sessions running on each individual device under ideal test conditions	No less than **8000000**	*8 000 000*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.3.20	Kiekvienas atskiras įrenginys turi palaikyti naujų sesijų per sekundę, esant idialioms testavimo sąlygoms	Ne mažiau kaip **290000**	Each individual device must support new sessions per second under ideal test conditions	No less than **290000**	*500 000*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.3.21	Kiekviename atskirame įrenginyje veikiančių vienu metu virtualių tinklų (VLAN) skaičius	Ne mažiau kaip **4094**	Number of concurrent virtual networks (VLANs) running on each individual device	No less than **4094**	*4094*	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-system-administration-52/VLANs/VLANs.htm	
1.3.22	Kiekviename atskirame įrenginyje veikiančių loginių savarankiškų virtualių sistemų (domenų) skaičius	Ne mažiau kaip **10**	Number of logical stand-alone virtual systems (domains) which must be configurable on each individual device	No less than **10**	*10*	https://kb.fortinet.com/kb/documentLink.do?externalID=11739	
1.3.23	Kiekvieno atskiro įrenginio ugniasienės vartotojų skaičius neribojamas	Kiekvieno atskiro įrenginio ugniasienės vartotojų skaičius neribojamas	There must be no limit to the number of users per firewall	There is no limit to the number of users per firewall	Kiekvieno atskiro įrenginio ugniasienės vartotojų skaičius neribojamas	https://help.fortinet.com/cli/fos60hlp/60/Content/FortiOS/fortiOS-cli-ref/config/system/resource-limits.htm	
1.3.24	Kiekvienas atskiras įrenginys turi veikti tokiais režimais	Skaidrus (angl. transparent); maršrutizavimo (angl. routing)	Each individual device must operate in these modes:	Transparent; Routing.	Skaidrus (angl. transparent); maršrutizavimo (angl. routing)	https://help.fortinet.com/fos50hlp/54/Content/	
1.3.25	Turi būti galimybė sukonfigūruoti įrenginį taip, kad jis vienu metu, vienoje sistemoje, veiktų visais palaikomais režimais	Yra galimybė sukonfigūruoti įrenginį taip, kad jis vienu metu, vienoje sistemoje, veiktų visais palaikomais režimais	It must be possible to configure device to operate simultaneously in all supported modes on one device	It is possible to configure device to operate simultaneously in all supported modes on one device.	Yra galimybė sukonfigūruoti įrenginį taip, kad jis vienu metu, vienoje sistemoje, veiktų visais palaikomais režimais	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-firewall/Concepts%20-%20WAN%20Opt/Operating%20modes%20and%20VDOMs.htm	
1.3.26	Kiekviename atskirame įrenginyje turi veikti apsauga nuo DoS atakų	Kiekviename atskirame įrenginyje veikia apsauga nuo DoS atakų	Each individual device must have ability to enable DoS attack protection.	Each individual device has ability to enable DoS attack protection.	Kiekviename atskirame įrenginyje veikia apsauga nuo DoS atakų	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Inside%20FortiOS%20DoS%20Protection.htm	
1.3.27	Kiekvienas atskiras įrenginys turi veikti loginio grupavimo protokolą *Turi būti galimybė apjungti į vieną loginį tinklo prievadą nemažiau kaip 8 fizines prievadus. Loginis prievadas gali būti naudojamas kaip L2 arba L3 lygio prievadas*	IEEE 802.3ad arba lygiavertį	Each individual device must run a logical grouping protocol It must be possible to connect at least 8 physical ports to a single logical network port. Logical port can be used as an L2 or L3 level port	IEEE 802.3ad or equivalent.	IEEE 802.3ad arba lygiavertį	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-networking-54/Interfaces/Aggregate%20Interfaces.htm	
1.3.28	Kiekvienas atskiras įrenginys turi palaikyti VLAN žymėjimo (*angl* . tagging) protokolą *VLAN prievadai gali būti kuriamos tinklo prievadams, veikiantiems L2 ir L3 lygyje*	IEEE 802.1q arba lygiavertį	Each individual device must support VLAN tagging protocol VLAN ports can be created for network ports operating at the L2 and L3 levels	IEEE 802.1q or equivalent.	IEEE 802.1q arba lygiavertį	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-system-administration-52/VLANs/VLANs.htm	

1.3.29	Kiekviename atskirame įrenginyje turi veikti vidinio DHCP serverio funkcija	Kiekviename atskirame įrenginyje veikia vidinio DHCP serverio funkcija	It must be possible to configure internal DHCP server in each individual device	It is possible to configure internal DHCP server in each individual device.	Kiekviename atskirame įrenginyje veikia vidinio DHCP serverio funkcija	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Advanced/DHCP%20servers%20and%20relays.htm	
1.3.30	Kiekviename atskirame įrenginyje turi būti palaikoma DHCP Relay funkcija	Kiekviename atskirame įrenginyje yra palaikoma DHCP Relay funkcija	DHCP Relay function must be supported on each individual device	DHCP Relay function is supported on each individual device.	Kiekviename atskirame įrenginyje yra palaikoma DHCP Relay funkcija	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Advanced/DHCP%20servers%20and%20relays.htm	
1.3.31	Kiekviename atskirame įrenginyje turi veikti DHCP ir PPPoE klientai	Kiekviename atskirame įrenginyje veikia DHCP ir PPPoE klientus	It must be possible to configure DHCP or PPPoE clients on each individual device	It is possible to configure DHCP or PPPoE clients on each individual device.	Kiekviename atskirame įrenginyje veikia DHCP ir PPPoE klientus	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-networking-54/Interfaces/PPPoE%C2%A0%20addressing%20mode%20on%20an%20interface.htm	
1.3.32	Kiekviename atskirame įrenginyje turi veikti dinaminio maršrutizavimo protokolai	Statiniai maršrutai (angl. static routes); BGPv4; OSPFv2; OSPFv3	Dynamic routing protocols must be running on each individual device	Static routes; BGPv4; OSPFv2; OSPFv3.	Statiniai maršrutai (angl. static routes); BGPv4; OSPFv2; OSPFv3	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-advanced-routing-52/Routing_Dynamic/Comparison_Protocols.htm	
1.3.33	Kiekviename atskirame įrenginyje turi veikti grakštus BGP ir OSPF perkrovimas (*angl*. graceful restart).	Kiekviename atskirame įrenginyje veikia grakštus BGP ir OSPF perkrovimas (*angl*. graceful restart).	Each individual device must be able to perform graceful restart for BGP and OSPF.	Each individual device is able to perform graceful restart for BGP and OSPF.	Kiekviename atskirame įrenginyje veikia grakštus BGP ir OSPF perkrovimas (*angl* graceful restart).	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverGraceful.htm	
1.3.34	Kiekviename atskirame įrenginyje turi veikti Multicast protokolai	IGMP (versijos 2 ir 3), IGMP proxy arba lygiavertis; PIM-SM arba lygiavertis; PIM-SSM arba lygiavertis	Multicast protocol must be working on each individual device	IGMP (version 2 and 3), IGMP proxy or equivalent; PIM-SM or equivalent; PIM-SSM or equivalent.	IGMP (versijos 2 ir 3), IGMP proxy arba lygiavertis; PIM-SM arba lygiavertis; PIM-SSM arba lygiavertis	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/741750/router-multicast	
1.3.35	Kiekviename atskirame įrenginyje turi veikti politika pagrįstą maršrutizavimas (*angl*. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną, siuntėjo, gavėjo IP adresą, servisą.	Kiekviename atskirame įrenginyje veikia politika pagrįstą maršrutizavimas (*angl*. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną, siuntėjo, gavėjo IP adresą, servisą.	Each individual device must be able to configure Policy Based Routing based on source/destination area, sender, recipient IP address, service, user ID, user group, application	Each individual device can configure Policy Based Routing based on source/destination area, sender, recipient IP address, service, user ID, user group, application.	Kiekviename atskirame įrenginyje veikia politika pagrįstą maršrutizavimas (*angl* Policy based routing) atsižvelgiant į šaltinio/paskirties zoną, siuntėjo, gavėjo IP adresą, servisą.	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-advanced-routing-54/Routing_Advanced_Static/Policy_Routing.htm	
1.3.36	Kiekvienas atskiras įrenginys turi palaikyti IPv6 protokolą	Kiekvienas atskiras įrenginys palaiko IPv6 protokolą	Each individual device must support IPv6 protocol	Each individual device supports IPv6 protocol.	Kiekvienas atskiras įrenginys palaiko IPv6 protokolą	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/IPv6%20in%20FortiOS.htm	
1.3.37	Kiekviename atskirame įrenginyje turi veikti BFD (Bidirectional Forwarding Detection) arba lygiavertis funckionalumas	Kiekviename atskirame įrenginyje veikia BFD (Bidirectional Forwarding Detection) arba lygiavertis funckionalumas	Each individual device must support BFD (Bidirectional Forwarding Detection) or equal functionality	Each individual device supports BFD (Bidirectional Forwarding Detection) or equal functionality.	Kiekviename atskirame įrenginyje veikia BFD (Bidirectional Forwarding Detection) arba lygiavertis funckionalumas	https://kb.fortinet.com/kb/documentLink.do?externalID=FD30260	
1.3.38	Kiekviename atskirame įrenginyje turi veikti adresų transliavimas (angl. NAT)	statinis adresų transliavimas (*angl*. Static NAT); šaltinio adreso transliavimas su portų adresų transliavimu (PAT); paskirties adreso transliavimas su portų adresų transliavimu (PAT)	Each individual device must have Network Address Translation (NAT)	Static NAT; source address translation with port address translation (PAT); destination address translation with port address translation (PAT).	statinis adresų transliavimas (*angl*. Static NAT); šaltinio adreso transliavimas su portų adresų transliavimu (PAT); paskirties adreso transliavimas su portų adresų transliavimu (PAT)	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Dynamic%20NAT.htm	

1.3.39	Kiekviename atskirame įrenginyje turi veikti adresų transliavimas tarp IPv6 ir IPv4 protokolų	Kiekviename atskirame įrenginyje turi veikti adresų transliavimas tarp IPv6 ir IPv4 protokolų	Address translation between IPv6 and IPv4 protocols must be working on each individual device	Address translation between IPv6 and IPv4 protocols is working on each individual device.	Kiekviename atskirame įrenginyje turi veikti adresų transliavimas tarp IPv6 ir IPv4 protokolų	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-firewall-52/Concepts/NAT%2064%20and%20NAT46.htm	
1.3.40	Kiekvienas atskiras įrenginys turi gebėti saugoti nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos)	Kiekvienas atskiras įrenginys geba saugo nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos)	Each individual device must be able to protect against attacks, malicious code (eg viruses, spyware)	Each individual device is able to protect against attacks, malicious code (eg viruses, spyware)	Kiekvienas atskiras įrenginys geba saugo nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos)	https://www.fortiguard.com/learnmore#av	
1.3.41	Kiekvienas atskiras įrenginys turi gebėti, nustačius grėsmę, automatiškai įrašyti paketus, susijusius su grėsme	Kiekvienas atskiras įrenginys geba, nustačius grėsmę, automatiškai įrašyti paketus, susijusius su grėsme	Each individual device must have capability to automatically record threat-related packets upon detection	Each individual device has capability to automatically record threat-related packets upon detection	Kiekvienas atskiras įrenginys geba, nustačius grėsmę, automatiškai įrašyti paketus, susijusius su grėsme	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Enable%20IPS%20packet%20logging.htm	
1.3.42	Kiekvienas atskiras įrenginys turi atpažinti ir kontroliuoti aplikacijas (protokolus) *Tos pačios aplikacijos skirtingos versijos skaičiuojamos kaip viena aplikacija*	Ne mažiau kaip **3000**	Each individual device must recognize and control applications (protocols) Different versions of the same application are counted as one application	No less than **3000**	Daugiau nei 4 000 aplikacijų	https://fortiguard.com/learnmore#ac	
1.3.43	Kiekvienas atskiras įrenginys turi gebėti apsirašyti savo aplikaciją	Kiekvienas atskiras įrenginys geba apsirašyti savo aplikaciją	Each individual device must be able to write down its application	Each individual device can write down its application	Kiekvienas atskiras įrenginys geba apsirašyti savo aplikaciją	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20Application%20&%20IPS%20Signatures.htm	
1.3.44	Kiekvienas atskiras įrenginys turi gebėti kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma	Kiekvienas atskiras įrenginys geba kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma	Each individual device must be able to set individual time for each application after which inactive session is closed	Each individual device can set individual time for each application after which inactive session is closed	Kiekvienas atskiras įrenginys geba kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma	https://help.fortinet.com/cli/fos50hlp/56/Content/FortiOS/fortiOS-cli-ref-56/config/application/list.htm	
1.3.45	Kiekvienas atskiras įrenginys turi gebėti kurti saugumo taisykles, kurios leistų vartotojams jungtis tik prie tam tikros aplikacijos ar aplikacijų grupės, nenurodant serviso/prievado, kuriuo dirba aplikacija, t. y. vartotojas gali prisijungti prie nurodytos aplikacijos nepriklausomai nuo to kokį servisą/prievadą naudoja aplikacija	Kiekvienas atskiras įrenginys geba kurti saugumo taisykles, kurios leistų vartotojams jungtis tik prie tam tikros aplikacijos ar aplikacijų grupės, nenurodant serviso/prievado, kuriuo dirba aplikacija, t. y. vartotojas gali prisijungti prie nurodytos aplikacijos nepriklausomai nuo to kokį servisą/prievadą naudoja aplikacija	Each individual device must have the ability to create security rules that allow users to connect only to a specific application or group of applications without specifying service/port application is running on, i.e. user can connect to specified application regardless of which service/port application uses	Each individual device can create security rules that allow users to connect only to a specific application or group of applications without specifying service/port application is running on, i.e. user can connect to specified application regardless of which service/port application uses.	Kiekvienas atskiras įrenginys geba kurti saugumo taisykles, kurios leistų vartotojams jungtis tik prie tam tikros aplikacijos ar aplikacijų grupės, nenurodant serviso/prievado, kuriuo dirba aplikacija, t. y. vartotojas gali prisijungti prie nurodytos aplikacijos nepriklausomai nuo to kokį servisą/prievadą naudoja aplikacija	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20Application%20&%20IPS%20Signatures.htm	
1.3.46	Kiekvienas atskiras įrenginys turi gebėti riboti prisijungimų iš vieno šaltinio skaičių pagal	siuntėjo IP; gavėjo IP; siuntėjo ir gavėjo IP	Each individual device must have ability to limit number of connections based on provided criteria:	Source IP; Destination IP; Source and Destination IP.	siuntėjo IP; gavėjo IP; siuntėjo ir gavėjo IP	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Security%20Policies/Firewall%20policies.htm	
1.3.47	Kiekvienas atskiras įrenginys, kuriant ugniasienės saugumo taisykles, turi gebėti nurodyti siuntėją, gavėją, servisą/prievadą, aplikaciją, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Servisai/prievadai ir aplikacijos taisyklėse turi būti nurodomi atskiruose laukuose	Kiekvienas atskiras įrenginys, kuriant ugniasienės saugumo taisykles, geba nurodyti siuntėją, gavėją, servisą/prievadą, aplikaciją, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Servisai/prievadai ir aplikacijos taisyklėse yra nurodomi atskiruose laukuose	Each individual device must have ability to specify source, destination, service/port, application, applicable security measures, user, user group when creating firewall rules. Services/ports and applications rules must be referenced in separate fields.	Each individual device has ability to specify source, destination, service/port, application, applicable security measures, user, user group when creating firewall rules. Services/ports and applications rules must be referenced in separate fields.	Kiekvienas atskiras įrenginys, kuriant ugniasienės saugumo taisykles, geba nurodyti siuntėją, gavėją, servisą/prievadą, aplikaciją, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Servisai/prievadai ir aplikacijos taisyklėse yra nurodomi atskiruose laukuose	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Security%20Policies/Firewall%20policies.htm	
1.3.48	Kiekvienas atskiras įrenginys turi gebėti skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones	Kiekvienas atskiras įrenginys geba skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones	Each individual device must have ability to use different security measures for different data traffic.	Each individual device has ability to use different security measures for different data traffic.	Kiekvienas atskiras įrenginys geba skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones	https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/853759	

1.3.49	Kiekvienas atskiras įrenginys pagal nutylėjimą turi blokuoti visas aplikacijas išskyrus tas, kurios yra apibrėžtos saugumo taisyklėse kaip leistinos	Kiekvienas atskiras įrenginys pagal nutylėjimą blokuoja visas aplikacijas išskyrus tas, kurios yra apibrėžtos saugumo taisyklėse kaip leistinos	By default, each individual device must block all applications except those defined in the firewall rules as allowed	By default, each individual device is blocking all applications except those defined in the firewall rules as allowed.	Kiekvienas atskiras įrenginys pagal nutylėjimą blokuoja visas aplikacijas išskyrus tas, kurios yra apibrėžtos saugumo taisyklėse kaip leistinos	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Security%20Policies/Firewall%20policies.htm	
1.3.50	Kiekvienas atskiras įrenginys turi gebėti suteikti vartotojams prieigą prie aplikacijos/ų (ne serviso/prievado) nepriklausomai nuo to kokiais TCP, UDP prievadais dirba aplikacija	Kiekvienas atskiras įrenginys geba suteikti vartotojams prieigą prie aplikacijos/ų (ne serviso/prievado) nepriklausomai nuo to kokiais TCP, UDP prievadais dirba aplikacija	Each individual device must be able to provide users with access to the application(s) (not service/port), regardless of which TCP, UDP ports the application is running on	Each individual device can provide users with access to the application(s) (not service/port), regardless of which TCP, UDP ports the application is running on.	Kiekvienas atskiras įrenginys geba suteikti vartotojams prieigą prie aplikacijos/ų (ne serviso/prievado) nepriklausomai nuo to kokiais TCP, UDP prievadais dirba aplikacija	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Application_Control/Application%20Control%20Concepts.htm	
1.3.51	Kiekvienas atskiras įrenginys turi gebėti nurodyti prie kokių aplikacijų vartotojui leidžiama jungtis, o prie kokių neleidžiama, net jei aplikacijos dirba tais pačiais TCP, UDP prievadais	Kiekvienas atskiras įrenginys geba nurodyti prie kokių aplikacijų vartotojui leidžiama jungtis, o prie kokių neleidžiama, net jei aplikacijos dirba tais pačiais TCP, UDP prievadais	Each individual device must be able to specify which applications user can connect to and which ones cannot, even if applications are running on the same TCP, UDP ports	Each individual device can specify which applications user can connect to and which ones cannot, even if applications are running on the same TCP, UDP ports	Kiekvienas atskiras įrenginys geba nurodyti prie kokių aplikacijų vartotojui leidžiama jungtis, o prie kokių neleidžiama, net jei aplikacijos dirba tais pačiais TCP, UDP prievadais	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-profiles/Application_Control/Enable%20Application%20Control.htm	
1.3.52	Kiekvienas atskiras įrenginys turi gebėti suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta	Kiekvienas atskiras įrenginys geba suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta	Each individual device must be able to grant access rights only to authenticated users	Each individual device is able to grant access rights only to authenticated users	Kiekvienas atskiras įrenginys geba suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Auth_Intro.htm	
1.3.53	Kiekvienas atskiras įrenginys turi gebėti dinamiškai susieti IP adresą su vartotojų	Kiekvienas atskiras įrenginys geba dinamiškai susieti IP adresą su vartotojų	Each individual device must be able to dynamically associate an IP address with user	Each individual device can dynamically associate an IP address with user	Kiekvienas atskiras įrenginys geba dinamiškai susieti IP adresą su vartotojų	https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/374938/setting-up-your-fortigate-for-fsso	
1.3.54	Kiekvienas atskiras įrenginys turi gebėti suteikti prieigos teises vartotojams, ir/arba vartotojų grupėms.	Kiekvienas atskiras įrenginys geba suteikti prieigos teises vartotojams, ir/arba vartotojų grupėms.	Each individual device must be able to grant access rights to users and/or user groups.	Each individual device has the ability to grant access rights to users and/or user groups.	Kiekvienas atskiras įrenginys geba suteikti prieigos teises vartotojams, ir/arba vartotojų grupėms.	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Security%20Policies/Firewall%20policies.htm	
1.3.55	Kiekvienas atskiras įrenginys turi gebėti nustatyti vartotojų tapatybę, neprašydamas suvesti vartotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz. Active Directory	Kiekvienas atskiras įrenginys geba nustatyti vartotojų tapatybę, neprašydamas suvesti vartotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz. Active Directory	Each individual device must be able to authenticate users without having to enter their username and password but using existing network services eg Active Directory	Each individual device can authenticate users without having to enter their username and password but using existing network services eg Active Directory.	Kiekvienas atskiras įrenginys geba nustatyti vartotojų tapatybę, neprašydamas suvesti vartotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz. Active Directory	https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/374938/setting-up-your-fortigate-for-fsso	
1.3.56	Kiekvienas atskiras įrenginys turi būti integruojamas su Active Directory, LDAP, RADIUS	Kiekvienas atskiras įrenginys yra integruojamas su Active Directory, LDAP, RADIUS	Each individual device must be integrated with Active Directory, LDAP, RADIUS	Each individual device is integrated with Active Directory, LDAP, RADIUS	Kiekvienas atskiras įrenginys yra integruojamas su Active Directory, LDAP, RADIUS	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Servers.htm	

1.3.57	Ugniasienė turi sinchronizuoti vartotojų-ID ir jų IP adresų informaciją. Informacija turi būti renkama tiesiogiai arba per papildomus agentus iš: •Active Directory domain servisų, •Radius accounting šaltinių, •terminalinių serverių. Turi būti papildoma galimybė surinkti informaciją iš Syslog šaltinių tiesiogiai arba naudojant papildomą programinę įrangą, kuri nėra įtraukiama į pasiūlymą. *Vartotojų ID ir IP adresų sinchronizacijai negali būti instaliuojami papildomi agentai klientų kompiuteriuose.* *Šis reikalavimas gali būti įgyvendintas lygiaverčiu funkcionalumu ar pateikiamais sprendimais, kurie nenaudojant papildomų agentų klientų kompiuteriuose sinchronizuotų vartotojų-ID ir jų IP adresų informaciją su Užsakovo turima ir naudojama sistema Aruba ClearPass ir terminaliniuose serveriuose*	Ugniasienė sinchronizuoja vartotojų-ID ir jų IP adresų informaciją. Informacija turi būti renkama tiesiogiai arba per papildomus agentus iš: •Active Directory domain servisų, •Radius accounting šaltinių, •terminalinių serverių. Turi būti papildoma galimybė surinkti informaciją iš Syslog šaltinių tiesiogiai arba naudojant papildomą programinę įrangą, kuri nėra įtraukiama į pasiūlymą.	Firewall must synchronize user IDs and their IP address information. The information must be collected directly or through additional agents from: • Active Directory domain services, • Radius accounting sources • terminal servers. There must be an additional ability to collect information from Syslog sources directly or through the use of additional software that is not included in the offer. *Additional agents cannot be installed on client computers to synchronize user IDs and IP addresses.* *This requirement can be implemented with equivalent functionality or provided solutions that, without the use of additional agents, synchronize user IDs and their IP addresses on client computers with system owned and operated by Customer Aruba ClearPass and terminal servers*	Firewall synchronizes user IDs and their IP address information. The information must be collected directly or through additional agents from: • Active Directory domain services, • Radius accounting sources • terminal servers. There must be an additional ability to collect information from Syslog sources directly or through the use of additional software that is not included in the offer.	Ugniasienė sinchronizuoja vartotojų-ID ir jų IP adresų informaciją. Informacija turi būti renkama tiesiogiai arba per papildomus agentus iš: •Active Directory domain servisų, •Radius accounting šaltinių, •terminalinių serverių. Turi būti papildoma galimybė surinkti informaciją iš Syslog šaltinių tiesiogiai arba naudojant papildomą programinę įrangą, kuri nėra įtraukiama į pasiūlymą.	*https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso* *https://docs.fortinet.com/document/fortigate/6.0.0/handbook/658099/single-sign-on-to-windows-ad* *https://docs.fortinet.com/document/fortigate/6.0.0/handbook/372705/sso-using-radius-accounting-records* *https://docs.fortinet.com/document/fortimanager/6.2.1/new-features/733863/clearpass-sso-identity-connector*	
1.3.58	Kiekviename atskirame įrenginyje vartotojų identifikacijai turi būti palaikomas IPv6 protokolas	Kiekviename atskirame įrenginyje vartotojų identifikacijai yra palaikomas IPv6 protokolas	Each individual device must support IPv6 for user identification	Each individual device has a supported IPv6 protocol for user identification.	Kiekviename atskirame įrenginyje vartotojų identifikacijai yra palaikomas IPv6 protokolas	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-firewall/IPv6/IPv6%20Features/IPv6%20support%20for%20FSSO.htm	
1.3.59	Jei vartotojo tapatybė nebuvo nustatyta skaidriai, vartotojui turi būti parodomas puslapis, kuriame jis turi įvesti tapatybę patvirtinančius duomenis	Jei vartotojo tapatybė nebuvo nustatyta skaidriai, vartotojui turi būti parodomas puslapis, kuriame jis turi įvesti tapatybę patvirtinančius duomenis	If user has not been authenticated in a transparent manner, user must be shown a page where he/she must enter his/her identity details	If user has not been authenticated in a transparent manner, the user is shown a page where he/she must enter his/her identity details.	Jei vartotojo tapatybė nebuvo nustatyta skaidriai, vartotojui turi būti parodomas puslapis, kuriame jis turi įvesti tapatybę patvirtinančius duomenis	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/CaptivePortals.htm	
1.3.60	Kiekvienas atskiras įrenginys turi gebėti kontroliuoti vartotojų, dirbančių terminalinėje aplinkoje (pvz.: Windows Terminal Server) prieigos teises. Įrenginys turi skirti terminalinėje aplinkoje dirbančių vartotojų duomenų srautus ir kontroliuoti kiekvieno vartotojo prieigos teises	Kiekvienas atskiras įrenginys geba kontroliuoti vartotojų, dirbančių terminalinėje aplinkoje (pvz.: Windows Terminal Server) prieigos teises. Įrenginys turi skiria terminalinėje aplinkoje dirbančių vartotojų duomenų srautus ir kontroliuoti kiekvieno vartotojo prieigos teises	Each individual device must be able to control access rights of users working in terminal environment (ex. Windows Terminal Server). Device must allocate data flows to users in terminal environment and control access rights for each user	Each individual device can control access rights of users working in terminal environment (ex. Windows Terminal Server). Device must allocate data flows to users in terminal environment and control access rights for each user.	Kiekvienas atskiras įrenginys geba kontroliuoti vartotojų, dirbančių terminalinėje aplinkoje (pvz.: Windows Terminal Server) prieigos teises. Įrenginys turi skiria terminalinėje aplinkoje dirbančių vartotojų duomenų srautus ir kontroliuoti kiekvieno vartotojo prieigos teises	https://kb.fortinet.com/kb/viewContent.do?externalId=FD35372	
1.3.61	Kiekvienas atskiras įrenginys turi palaikyti vartotojų tapatybės nustatymą naudojant vartotojo skaitmeninį sertifikatą. Nustatant vartotojo tapatybę, turi būti galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse	Kiekvienas atskiras įrenginys palaiko vartotojų tapatybės nustatymą naudojant vartotojo skaitmeninį sertifikatą. Nustatant vartotojo tapatybę, yra galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse	Each individual device must support user authentication with user's digital certificate. When identifying a user, it must be possible to search user's data on multiple authentication servers	Each individual device supports user authentication with user's digital certificate. When identifying a user, it is possible to search user's data on multiple authentication servers.	Kiekvienas atskiras įrenginys palaiko vartotojų tapatybės nustatymą naudojant vartotojo skaitmeninį sertifikatą. Nustatant vartotojo tapatybę, yra galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Certificates.htm	
1.3.62	Kiekvienas atskiras įrenginys turi dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą	Kiekvienas atskiras įrenginys dešifruoja ir tikrina įeinantį ir išeinantį SSL duomenų srautą	Each individual device must decrypt and verify incoming and outgoing SSL traffic	Each individual device decrypts and verifies incoming and outgoing SSL traffic.	Kiekvienas atskiras įrenginys dešifruoja ir tikrina įeinantį ir išeinantį SSL duomenų srautą	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122078/deep-inspection	
1.3.63	Kiekviename atskirame įrenginyje turi būti pasirinktinai nurodoma, kurį duomenų srautą dešifruoti	Kiekviename atskirame įrenginyje yra pasirinktinai nurodoma, kurį duomenų srautą dešifruoti	Each individual device must be able to specify which data stream to decrypt	Each individual device has option of specifying which data stream to decrypt.	Kiekviename atskirame įrenginyje yra pasirinktinai nurodoma, kurį duomenų srautą dešifruoti	https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/853759	

1.3.64	Kiekviename atskirame įrenginyje SSL patikra turi būti atliekama visam SSL duomenų srautui, ne tik HTTPS, SMTPS, POP3S, IMAPS protokolams	Kiekviename atskirame įrenginyje SSL patikra atliekama visam SSL duomenų srautui, ne tik HTTPS, SMTPS, POP3S, IMAPS protokolams	SSL verification must be performed on each individual device for all SSL traffic, not just HTTPS, SMTPS, POP3S, IMAPS protocols	SSL verification is performed on each individual device for all SSL traffic, not just HTTPS, SMTPS, POP3S, IMAPS protocols.	Kiekviename atskirame įrenginyje SSL patikra atliekama visam SSL duomenų srautui, ne tik HTTPS, SMTPS, POP3S, IMAPS protokolams	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122078/deep-inspection	
1.3.65	Kiekviename atskirame įrenginyje SSL patikra turi apimti įsilaužimų, pažeidžiamumų aptikimą ir prevenciją, apsaugą nuo virusų, šnipinėjimo aplikacijų, perduodamų failų kontrolę, perduodamų duomenų turinio kontrolę, URL filtravimą	Kiekviename atskirame įrenginyje SSL patikra apima įsilaužimų, pažeidžiamumų aptikimą ir prevenciją, apsaugą nuo virusų, šnipinėjimo aplikacijų, perduodamų failų kontrolę, perduodamų duomenų turinio kontrolę, URL filtravimą	SSL verification on each individual device must include detection and prevention of hacking, vulnerabilities, virus protection, spyware, file transfer control, data transfer control, URL filtering	SSL verification on each individual device includes detection and prevention of hacking, vulnerabilities, virus protection, spyware, file transfer control, data transfer control, URL filtering.	Kiekviename atskirame įrenginyje SSL patikra apima įsilaužimų, pažeidžiamumų aptikimą ir prevenciją, apsaugą nuo virusų, šnipinėjimo aplikacijų, perduodamų failų kontrolę, perduodamų duomenų turinio kontrolę, URL filtravimą	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-security-profiles/SSL_SSH_Inspection/why_use_ssl_inspection.htm	
1.3.66	Kiekvienas atskiras įrenginys turi dešifruoti TLS1.2 duomenų srautą	Kiekvienas atskiras įrenginys dešifruoja TLS1.2 duomenų srautą	Each individual device must decrypt TLS1.2 data stream	Each individual device decrypts TLS1.2 data stream.	Kiekvienas atskiras įrenginys dešifruoja TLS1.2 duomenų srautą	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-load-balancing/ldb-ssl-tls-version.htm	
1.3.67	Kiekvienas atskiras įrenginys turi inspektuoti TLS1.3 duomenų srautą, atpažinti aplikacijas ir svetaines naudojančias TLS1.3	Kiekvienas atskiras įrenginys inspektuoja TLS1.3 duomenų srautą, atpažįsta aplikacijas ir svetaines naudojančias TLS1.3	Each individual device must inspect TLS1.3 traffic, recognize applications and sites using TLS1.3	Each individual device inspects TLS1.3 traffic, recognize applications and sites using TLS1.3	Kiekvienas atskiras įrenginys inspektuoja TLS1.3 duomenų srautą, atpažįsta aplikacijas ir svetaines naudojančias TLS1.3	https://docs.fortinet.com/document/fortigate/6.2.0/new-features/35927/tls-1-3-support	
1.3.68	Kiekvienas atskiras įrenginys turi riboti prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus	Kiekvienas atskiras įrenginys riboja prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus	Each individual device must be able to limit number of connections based on source, destination IP addresses, services, users	Each individual device can limit number of connections based on source, destination IP addresses, services, users.	Kiekvienas atskiras įrenginys riboja prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/885253/per-ip-traffic-shaper	
1.3.69	Kiekvienas atskiras įrenginys turi gebėti kurti savo įsilaužimų aprašus	Kiekvienas atskiras įrenginys geba kurti savo įsilaužimų aprašus	Each individual device must have the ability to create combined threat prevention descriptions	Each individual device has the ability to create combined threat prevention descriptions	Kiekvienas atskiras įrenginys geba kurti savo įsilaužimų aprašus	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20signature%20keywords.htm	
1.3.70	Kiekvienas atskiras įrenginys turi gebėti atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę	Kiekvienas atskiras įrenginys geba atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę	Each individual device must be able to control access to web resources using a manufacturer-provided URL database	Each individual device can control access to web resources using the URL database provided by the manufacturer	Kiekvienas atskiras įrenginys geba atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-profiles/Web_Filter/FortiGuard%20Web%20Filtering%20Service.htm	
1.3.71	Kiekvienas atskiras įrenginys turi gebėti sukurti leistinų ir draudžiamų URL ir IP sąrašus	Kiekviename atskirame įrenginyje yra galimybė sukurti leistinų ir draudžiamų URL ir IP sąrašus	Each individual device must be able to create lists of allowed and prohibited URLs and IPs	Each individual device can create lists of allowed and blocked URLs and IPs.	Kiekviename atskirame įrenginyje yra galimybė sukurti leistinų ir draudžiamų URL ir IP sąrašus	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-profiles/Web_Filter/Static%20URL%20Filter.htm	
1.3.72	Kiekvienas atskiras įrenginys turi gebėti sukurti ir naudoti savo URL grupes	Kiekvienas atskiras įrenginys geba sukurti ir naudoti savo URL grupes	Each individual device must be able to create and use its own URL groups	Each individual device can create and use its own URL groups.	Kiekvienas atskiras įrenginys geba sukurti ir naudoti savo URL grupes	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Web_Filter/Configuring%20Web%20Filter%20Profiles.htm	
1.3.73	Kiekvienas atskiras įrenginys turi gebėti kurti pažeidžiamumų aprašus	Kiekvienas atskiras įrenginys geba kurti pažeidžiamumų aprašus	Each individual device must be able to create vulnerability profiles	Each individual device can create vulnerability profiles.	Kiekvienas atskiras įrenginys geba kurti pažeidžiamumų aprašus	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20signature%20keywords.htm	

1.3.74	Kiekvienas atskiras įrenginys turi aptikti ir blokuoti Botnet	Kiekvienas atskiras įrenginys aptinka ir blokuoja Botnet	Each individual device must be able to detect Botnet	Each individual device can detect Botnet.	Kiekvienas atskiras įrenginys aptinka ir blokuoja Botnet	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/105208/botnet-c-c-domain-blocking	
1.3.75	Kiekvienas atskiras įrenginys turi palaikyti šifravimo algoritmus	3DES; AES128; AES256.	Each individual device must support provided encryption protocols:	3DES; AES128; AES256.	3DES; AES128; AES256.	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Concepts/Encryption.htm	
1.3.76	Kiekvienas atskiras įrenginys turi palaikyti saugios maišos algoritmus	SHA-1; SHA-256; SHA-384.	Each individual device must support provided secure hash algorithms:	SHA-1; SHA-256; SHA-384.	SHA-1; SHA-256; SHA-384.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/238852/encryption-algorithms	
1.3.77	Kiekvienas atskiras įrenginys turi gebėti siųsti IPv6 duomenų srautą per sukurtą IPSec tunelį tarp skirtingų gamintojo įrenginių	Kiekvienas atskiras įrenginys geba siųsti IPv6 duomenų srautą per sukurtą IPSec tunelį tarp skirtingų gamintojo įrenginių	Each individual device must be able to send IPv6 data traffic via IPSec tunnel between different manufacturer's devices	Each individual device can send IPv6 data traffic via IPSec tunnel between different manufacturer's devices.	Kiekvienas atskiras įrenginys geba siųsti IPv6 duomenų srautą per sukurtą IPSec tunelį tarp skirtingų gamintojo įrenginių	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-IPv6-54/IPv6%20Configuration/IPv6_IPsec_VPN.htm	
1.3.78	Kiekvienas atskiras įrenginys turi palaikyti duomenų srautų ribojimą pagal taikomąją programinę įrangą, vartotoją, siuntėjo, gavėjo IP adresus, tinklo sąsajas	Kiekvienas atskiras įrenginys palaiko duomenų srautų ribojimą pagal taikomąją programinę įrangą, vartotoją, siuntėjo, gavėjo IP adresus, tinklo sąsajas	Each individual device must be able to support data flow restrictions depending on application software, user, source, destination IP addresses, network interface.	Each individual device can support data flow restrictions depending on application software, user, source, destination IP addresses, network interface.	Kiekvienas atskiras įrenginys palaiko duomenų srautų ribojimą pagal taikomąją programinę įrangą, vartotoją, siuntėjo, gavėjo IP adresus, tinklo sąsajas	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-profiles/Application_Control/Enable-Application-Control-NGFW-Policy-Based.htm	
1.3.79	Kiekvienas atskiras įrenginys turi gebėti suteikti prioritetus duomenų paketams	Kiekvienas atskiras įrenginys geba suteikti prioritetus duomenų paketams	Each individual device must be able to give priority to data packets	Each individual device can give priority to data packets.	Kiekvienas atskiras įrenginys geba suteikti prioritetus duomenų paketams	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-traffic-shaping-54/TS_Configuration/TS_Configuring.htm	
1.3.80	Kiekvienas atskiras įrenginys turi gebėti pasirinktam duomenų srautui nustatyti maksimalų pralaidumą	Kiekvienas atskiras įrenginys geba pasirinktam duomenų srautui nustatyti maksimalų pralaidumą	Each individual device must be able to set maximum bandwidth for selected data stream	Each individual device can set maximum bandwidth for selected data stream.	Kiekvienas atskiras įrenginys geba pasirinktam duomenų srautui nustatyti maksimalų pralaidumą	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-traffic-shaping-54/TS_Configuration/TS_Configuring.htm	
1.3.81	Kiekviename atskirame įrenginyje maksimalus arba garantuotas pralaidumas turi būti konfigūruojamas pagal	ugniasienės saugumo taisyklę; vartotojo IP adresą; aplikaciją.	For each individual device, maximum or guaranteed throughput must be configured as per provided criteria:	firewall security rule; user's IP address; application.	ugniasienės saugumo taisyklę; vartotojo IP adresą; aplikaciją.	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-traffic-shaping-54/TS_Configuration/TS_Configuring.htm	
1.3.82	Kiekvienas atskiras įrenginys turi gebėti duomenų srautų valdymo statistiką atvaizduoti grafinių būdu	Kiekvienas atskiras įrenginys geba duomenų srautų valdymo statistiką atvaizduoti grafinių būdu	Each individual device must be capable of graphically displaying traffic management statistics	Each individual device is capable of graphically displaying traffic management statistics.	Kiekvienas atskiras įrenginys geba duomenų srautų valdymo statistiką atvaizduoti grafinių būdu	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-getting-started/using-the-GUI/dashboard.htm	
1.3.83	Kiekvienas atskiras įrenginys turi gebėti kurti saugumo taisykles iš karto tarp kelių saugumo zonų, t. y. sukurti vieną taisyklę, kuri leistų iš 2 ar daugiau zonų jungtis į 2 ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei.	Kiekvienas atskiras įrenginys geba kurti saugumo taisykles iš karto tarp kelių saugumo zonų, t .y. sukurti vieną taisyklę, kuri leistų iš 2 ar daugiau zonų jungtis į 2 ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei.	Each individual device must be able to create security rules for multiple security zones at once, i.e. create a single rule that allows connections from 2 or more zones to 2 or more zones without creating separate rules for each interzone flow control.	Each individual device can create security rules for multiple security zones at once, i.e. create a single rule that allows connections from 2 or more zones to 2 or more zones without creating separate rules for each interzone flow control.	Kiekvienas atskiras įrenginys geba kurti saugumo taisykles iš karto tarp kelių saugumo zonų, t .y. sukurti vieną taisyklę, kuri leistų iš 2 ar daugiau zonų jungtis į 2 ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei.	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/FeatureCatalog-firewall.htm	

1.3.84	Kiekvienas atskiras įrenginys turi gebėti importuoti skaitmeninius sertifikatus SSL sesijų terminavimui / perėmimui ar įrenginio valdymui	Kiekvienas atskiras įrenginys geba importuoti skaitmeninius sertifikatus SSL sesijų terminavimui / perėmimui ar įrenginio valdymui	Each individual device must be able to import digital certificates for SSL session termination/interception or device management	Each individual device can import digital certificates for SSL session termination/interception or device management.	Kiekvienas atskiras įrenginys geba importuoti skaitmeninius sertifikatus SSL sesijų terminavimui / perėmimui ar įrenginio valdymui	https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/378040/importing-the-signed-certificate-to-your-fortigate	
1.3.85	Kiekvienas atskiras įrenginys turi palaikyti CRL (*angl* . Certificate revocation list)	Kiekvienas atskiras įrenginys palaiko CRL (angl. Certificate revocation list)	Each individual device must support CRL (Certificate Revocation List)	Each individual device supports CRL (Certificate Revocation List).	Kiekvienas atskiras įrenginys palaiko CRL (angl. Certificate revocation list)	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/96571/certificate-crl	
1.3.86	Kiekvienas atskiras įrenginys turi palaikyti OCSP (*angl* . Online Certificate Status Protocol) protokolą	Kiekvienas atskiras įrenginys palaiko OCSP (angl. Online Certificate Status Protocol) protokolą	Each individual device must support Online Certificate Status Protocol (OCSP)	Each individual device supports the Online Certificate Status Protocol (OCSP).	Kiekvienas atskiras įrenginys palaiko OCSP (angl. Online Certificate Status Protocol) protokolą	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/59761/vpn-certificate-ocsp-server	
1.3.87	Kiekvienas atskiras įrenginys turi palaikyti 4096 bitų RSA sertifikatus	Kiekvienas atskiras įrenginys palaiko 4096 bitų RSA sertifikatus	Each individual device must support 4096-bit RSA certificates	Each individual device supports 4096-bit RSA certifications.	Kiekvienas atskiras įrenginys palaiko 4096 bitų RSA sertifikatus	https://docs.fortinet.com/document/fortigate/6.2.2/cli-reference/277620/vpn-certificate-setting	
1.3.88	Kiekvienas atskiras įrenginys turi gebėti importuoti tarnybinių stočių viešus, privačius raktus ir sertifikatus *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekvienas atskiras įrenginys geba importuoti tarnybinių stočių viešus, privačius raktus ir sertifikatus	Each individual device must be able to import public, private server keys and certificates *Functionality can be implemented from a central management system*	Each individual device can import public, private server keys and certificates.	Kiekvienas atskiras įrenginys geba importuoti tarnybinių stočių viešus, privačius raktus ir sertifikatus	https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/378040/importing-the-signed-certificate-to-your-fortigate	
1.3.89	Kiekvienas atskiras įrenginys turi gebėti generuoti ir eksportuoti Netflow v9 ar lygiaverčius įrašus apie duomenų srautus. Įrašuose turi būti informacija apie vartotojus ir taikomąją programinę įrangą	Kiekvienas atskiras įrenginys geba generuoti ir eksportuoti Netflow v9 ar lygiaverčius įrašus apie duomenų srautus. Įrašuose turi būti informacija apie vartotojus ir taikomąją programinę įrangą	Each individual device must be able to generate and export Netflow v9 or equivalent data feeds. The records must contain information about users and software application.	Each individual device can generate and export Netflow v9 or equivalent data feeds. The records must contain information about users and software application.	Kiekvienas atskiras įrenginys geba generuoti ir eksportuoti Netflow v9 ar lygiaverčius įrašus apie duomenų srautus. Įrašuose turi būti informacija apie vartotojus ir taikomąją programinę įrangą	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-networking/Troubleshooting/Netflow.htm	
1.3.90	Kiekvieno atskiro įrenginio Įvykių žurnalai turi būti siunčiami į centrinę valdymo tarnybinę stotį	Kiekvieno atskiro įrenginio Įvykių žurnalai yra siunčiami į centrinę valdymo tarnybinę stotį	Event logs for each individual device must be stored locally and sent to a central management server	Event logs for each individual device are stored locally and sent to a central management server.	Kiekvieno atskiro įrenginio Įvykių žurnalai yra siunčiami į centrinę valdymo tarnybinę stotį	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-logging-reporting-54/logs.htm	
1.3.91	Įvykių žurnaluose turi būti galimybė	filtruoti įvykius; fiksuoti administratorių atliekamus veiksmus	Event logs must have the capability	filter events; record actions taken by administrators.	filtruoti įvykius; fiksuoti administratorių atliekamus veiksmus	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-logging-reporting-54/logs.htm	
1.3.92	Kiekvienas atskiras įrenginys turi gebėti nurodytų laiku įvykių žurnalus siųsti į nutolusią darbo vietą/tarnybinę stotį	Kiekvienas atskiras įrenginys geba nurodytų laiku įvykių žurnalus siųsti į nutolusią darbo vietą/tarnybinę stotį	Each individual device must be able to send event logs to a remote workstation/server at a specified time.	Each individual device is able to send event logs to a remote workstation/server at a specified time.	Kiekvienas atskiras įrenginys geba nurodytų laiku įvykių žurnalus siųsti į nutolusią darbo vietą/tarnybinę stotį	https://kb.fortinet.com/kb/documentLink.do?externalID=FD46071	
1.3.93	Kiekviename atskirame įrenginyje turi būti atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginį esant dideliam tinklo aprovimui	Kiekviename atskirame įrenginyje yra atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginį esant dideliam tinklo aprovimui	Each individual device must have separate control and data analysis modules to ensure that device can be operated at high network load	Each individual device has its own control and data analysis modules to control device at high network load.	Kiekviename atskirame įrenginyje yra atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginį esant dideliam tinklo aprovimui	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Other_Profile_Considerations/Conserve%20mode.htm	

1.3.94	Kiekvienas atskiras įrenginys turi būti valdomas	SSHv2; iš centrinės valdymo sistemos	Each individual device must be controlled via:	SSHv2; Central management system.	SSHv2; iš centrinės valdymo sistemos	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-getting-started-52/basic_admin.htm https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-system-administration-52/Central%20Management/central_mgmt.htm	
1.3.95	Turi būti galimybė naudoti IPv6 kiekvieno atskiro įrenginio ir centrinės valdymo tarnybinės stoties sujungimui	Yra galimybė naudoti IPv6 kiekvieno atskiro įrenginio ir centrinės valdymo tarnybinės stoties sujungimui	It must be possible to use IPv6 to connect each individual device to central management server	It is possible to use IPv6 to connect each individual device to the central management server.	Yra galimybė naudoti IPv6 kiekvieno atskiro įrenginio ir centrinės valdymo tarnybinės stoties sujungimui	https://help.fortinet.com/cli/fos60hlp/60/Content/FortiOS/fortiOS-cli-ref/config/system/central-management.htm	
1.3.96	Kiekvieno atskiro įrenginio administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekvieno atskiro įrenginio administratorių prieigos teisės yra kontroliuojamos rolių pagalba	Administrators' permissions for each individual device must be controlled by roles *Functionality can be implemented from a central management system*	Administrators' permissions for each individual device are controlled by roles.	Kiekvieno atskiro įrenginio administratorių prieigos teisės yra kontroliuojamos rolių pagalba	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/294491/administrator-profiles	
1.3.97	Kiekviename atskirame įrenginyje turi būti galimybė kurti administratorių roles *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekviename atskirame įrenginyje yra galimybė kurti administratorių roles	Each individual device must have ability to create administrator roles *Functionality can be implemented from a central management system*	Each individual device can create administrator roles.	Kiekviename atskirame įrenginyje yra galimybė kurti administratorių roles	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/294491/administrator-profiles	
1.3.98	Kiekviename atskirame įrenginyje turi būti galimybė apibrėžti administratoriaus teises *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekviename atskirame įrenginyje yra galimybė apibrėžti administratoriaus teises	Each individual device must have ability to fine-tune administrator privileges *Functionality can be implemented from a central management system*	Each individual device has ability to fine-tune administrator privileges.	Kiekviename atskirame įrenginyje yra galimybė apibrėžti administratoriaus teises	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/294491/administrator-profiles	
1.3.99	Kiekviename atskirame įrenginyje turi būti galimybė sukurti įrenginio naudotoją, kuris turėtų tik skaitymo (*angl* . read-only) teises *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekviename atskirame įrenginyje yra galimybė sukurti įrenginio naudotoją, kuris turėtų tik skaitymo (*angl* . read-only) teises	Each individual device must have ability to create user that has read-only access *Functionality can be implemented from a central management system*	Each individual device can create user that has read-only rights.	Kiekviename atskirame įrenginyje yra galimybė sukurti įrenginio naudotoją, kuris turėtų tik skaitymo (*angl* . read-only) teises	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/294491/administrator-profiles	
1.3.100	Kiekvienas atskiras įrenginys turi gebėti detaliai apibrėžti administratoriaus teises keisti sisteminius įrenginio nustatymus; kurti, keisti saugumo ir NAT taisykles; peržiūrėti įvykių žurnalus *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekvienas atskiras įrenginys geba detaliai apibrėžti administratoriaus teises keisti sisteminius įrenginio nustatymus; kurti, keisti saugumo ir NAT taisykles; peržiūrėti įvykių žurnalus	Each individual device must have the ability to specify administrator privileges to change system settings; to create, change security and NAT rules; access to event logs *Functionality can be implemented from a central management system*	Each individual device can specify administrator privileges to change system settings; to create, change security and NAT rules; access to event logs; right to review reports	Kiekvienas atskiras įrenginys geba detaliai apibrėžti administratoriaus teises keisti sisteminius įrenginio nustatymus; kurti, keisti saugumo ir NAT taisykles; peržiūrėti įvykių žurnalus	https://cookbook.fortinet.com/limited-access-administrator-account/index.html	
1.3.101	Kiekvienas atskiras įrenginys turi gebėti persiųsti operacinę sistemą ir konfigūraciją SCP protokolu *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekvienas atskiras įrenginys geba persiųsti operacinę sistemą ir konfigūraciją SCP protokolu	Each individual device must be able to transfer operating system and configuration using the SCP protocol *Functionality can be implemented from a central management system*	Each individual device can transfer operating system and configuration using the SCP protocol.	Kiekvienas atskiras įrenginys geba persiųsti operacinę sistemą ir konfigūraciją SCP protokolu	https://kb.fortinet.com/kb/documentLink.do?externalID=FD43754	
1.3.102	Kiekviename atskirame įrenginyje turi veikti Syslog protokolas *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekviename atskirame įrenginyje veikia Syslog protokolas	Each individual device must be running Syslog protocol *Functionality can be implemented from a central management system*	Each individual device is running Syslog protocol.	Kiekviename atskirame įrenginyje veikia Syslog protokolas	https://kb.fortinet.com/kb/documentLink.do?externalID=FD44614	

1.3.103	Kiekviename atskirame įrenginyje turi veikti SNMPv3 protokolas	Kiekviename atskirame įrenginyje veikia SNMPv3 protokolas	Each individual device must be running SNMPv3 protocol	Each individual device is running SNMPv3 protocol.	Kiekviename atskirame įrenginyje veikia SNMPv3 protokolas	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Monitoring/SNMP.htm	
1.3.104	Kiekviename atskirame įrenginyje turi veikti NTP (versijos 3 ir 4) laiko sinchronizavimo protokolas *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekviename atskirame įrenginyje veikia NTP (versijos 3 ir 4) laiko sinchronizavimo protokolas	Each individual device must have NTP (version 3 and 4) time synchronization protocol *Functionality can be implemented from a central management system*	Each individual device has NTP (version 3 and 4) time synchronization protocol.	Kiekviename atskirame įrenginyje veikia NTP (versijos 3 ir 4) laiko sinchronizavimo protokolas	https://kb.fortinet.com/kb/viewContent.do?externalId=FD33783	
1.3.105	Kiekvienas atskiras įrenginys turi gebėti keisti įvykių, siunčiamų SYSLOG protokolų, formatą *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekvienas atskiras įrenginys geba keisti įvykių, siunčiamų SYSLOG protokolų, formatą	Each individual device must be able to change format of events sent by SYSLOG protocols *Functionality can be implemented from a central management system*	Each individual device can change format of events sent by SYSLOG protocols.	Kiekvienas atskiras įrenginys geba keisti įvykių, siunčiamų SYSLOG protokolų, formatą	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-whats-new/Top-LogReport-cef.htm	
1.3.106	Kiekvienas atskiras įrenginys turi gebėti automatiškai daryti konfigūracijos kopijas *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekvienas atskiras įrenginys geba automatiškai daryti konfigūracijos kopijas	Each individual device must be able to automatically make configuration copies *Functionality can be implemented from a central management system*	Each individual device can automatically make configuration copies.	Kiekvienas atskiras įrenginys geba automatiškai daryti konfigūracijos kopijas	https://kb.fortinet.com/kb/documentLink.do?externalID=FD39818	
1.3.107	Kiekvienas atskiras įrenginys turi gebėti sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis	Įrenginyje yra galimybė sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis	Device must be able to compare current device configuration with previous configurations	Device can compare current device configuration with previous configurations.	Įrenginyje yra galimybė sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis	https://help.fortinet.com/fmgr/50hlp/56/5-6-8/Content/FortiManager_Admin_Guide/1000_Device%20Manager/1500_Manage_device_configs/0610_Compare_diff_config_files.htm	
1.3.108	Kiekvienas atskiras įrenginys turi gebėti aktyvuoti ankstesnę konfigūraciją	Kiekvienas atskiras įrenginys geba aktyvuoti ankstesnę konfigūraciją	Each individual device must be able to use previous configuration	Each individual device can use previous configuration.	Kiekvienas atskiras įrenginys geba aktyvuoti ankstesnę konfigūraciją	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-getting-started-54/7-Basic-Admin/Firmware/Configuration%20revision.htm	
1.3.109	Kiekvienas atskiras įrenginys turi gebėti matyti aktyvius sujungimus (sesijas)	Kiekvienas atskiras įrenginys geba matyti aktyvius sujungimus (sesijas)	Each individual device must be able to see active connections (sessions)	Each individual device can see active connections (sessions).	Kiekvienas atskiras įrenginys geba matyti aktyvius sujungimus (sesijas)	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-fortiview-54/Consoles/All_Sessions.htm	
1.4	**Įrenginių konstrukcijos reikalavimai**		**Equipment design requirements**				
1.4.1	Kiekvieno atskiro įrenginio konstrukcija	Įrenginys montuojamas į 19” komutacinę spintą, pateikiami su montavimo detalėmis	Design of each individual device	Unit is mounted in a 19" rack provided with mounting parts.	*Montuojamas į 19“ spintą*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.4.2	Kiekvieno atskiro įrenginio aukštis	Ne daugiau kaip **3U**	Height of each individual device	No more than **3U.**	*2 U*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.4.3	Įrenginių elektros maitinimas	230V AC	Device power feed	**230V** AC.	*100 - 240V AC*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*

1.4.4	Kiekviename atskirame įrenginyje įdiegtų kintamosios elektros srovės maitinimo šaltinių skaičius Vienam maitinimo šaltiniui sugedus, įrenginys, nenutraukiant veikimo, turi būti maitinamas iš kito maitinimo šaltinio	Ne mažiau kaip **2** vnt.	Number of AC power supplies installed on each individual device. If one power supply fails, unit must be powered from another power supply without interruption.	No less than **2**.	Dubliuoti maitinimo šaltiniai. Vienam sugedus įrenginys veikia nenutrūkstamai.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	*5 psl.*
1.4.5	Įrenginio elektros tiekimo šaltiniai turi būti sukomplektuoti su elektros tiekimo prijungimo kabeliais	Įrenginio elektros tiekimo šaltiniai sukomplektuoti su elektros tiekimo prijungimo kabeliais	Power supplies for unit must be complete with power supply cables	Power sources for unit are complete with power supply cables.	*Sukomplektuota*	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/8505790d-a81f-11e9-81a4-00505692583a/FortiGate-1100E-Series-ACDC-Supplement.pdf	*2 psl.*
1.4.6	Įrenginys turi būti sukomplektuotas su konsolės prijungimo kabeliu	Įrenginys sukomplektuotas su konsolės prijungimo kabeliu	Unit must be equipped with a console connection cable	Unit is equipped with a console connection cable.	*Sukomplektuota*	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/8505790d-a81f-11e9-81a4-00505692583a/FortiGate-1100E-Series-ACDC-Supplement.pdf	*2 psl.*
1.5	**Sistemos bendrieji reikalavimai**		**General system requirements**				
1.5.1	Siūlomi įrenginiai (toliau – įranga) ir jų sudedamosios dalys turi būti nauji ir nenaudoti. Negalima siūlyti gamykliškai atnaujintos (angl. refurbished) įrangos	Siūlomi įrenginiai (toliau – įranga) ir jų sudedamosios dalys yra nauji ir nenaudoti	Proposed equipment (hereinafter referred to as "equipment") must be new and unused. *Refurbished equipment may not be offered*	Proposed equipment (hereinafter referred to as "equipment") is new and unused.	Siūlomi įrenginiai (toliau – įranga) ir jų sudedamosios dalys yra nauji ir nenaudoti		
1.5.2	Įrangos dokumentacija anglų kalba turi būti pateikiama gamintojo interneto svetainėje	Įrangos dokumentacija anglų kalba pateikiama gamintojo interneto svetainėje	Equipment documentation in English must be available on the manufacturer's website	Equipment documentation in English is available on the manufacturer's website.	Įrangos dokumentacija anglų kalba pateikiama gamintojo interneto svetainėje	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf	
1.5.3	Sistemai turi būti teikiamas techninis aptarnavimas	Sistemai yra teikiamas techninis aptarnavimas	Techical support must be provided to the System	Techical support is provided to the System	Sistemai yra teikiamas techninis aptarnavimas su FG-1100E-BDL-950-36		
1.5.4	Įranga turi būti pateikta su licencijomis, leidžiančiomis techninio aptarnavimo laikotarpiu gauti šiuos aprašų atnaujinimus	Aplikacijų protokolų kontrolės (angl. Application Control); įsilaužimų kontrolės (angl. Intrusion Prevention System); virusų, piktybinių programų (angl. Antivirus); Web filtravimo (angl. Web Filtering)	Equipment must be accompanied by licenses to receive these signatures updates during the maintenance period	Application Control; Intrusion Prevention System; Antivirus; Web Filtering	Aplikacijų protokolų kontrolės (angl. Application Control); įsilaužimų kontrolės (angl. Intrusion Prevention System); virusų, piktybinių programų (angl. Antivirus); Web filtravimo (angl. Web Filtering) Su FG-1100E-BDL-950-36		
1.5.5	Įranga turi gebėti atsisiųsti programinės įrangos atnaujinimus ir pataisymus (*angl*. patch) bei 1.5.4 punkte nurodytus aprašų atnaujinimus iš gamintojo puslapio	Įranga geba atsisiųsti programinės įrangos atnaujinimus ir pataisymus (angl. patch) bei 1.5.4 punkte nurodytus aprašų atnaujinimus iš gamintojo puslapio	Equipment must be able to download software updates, patches and signatures updates referred to clause 1.5.4 from manufacturer's page	Equipment can download software updates, patches and signatures updates referred to clause 1.5.4 from manufacturer's page.	Įranga geba atsisiųsti programinės įrangos atnaujinimus ir pataisymus (angl. patch) bei 1.5.4 punkte nurodytus aprašų atnaujinimus iš gamintojo puslapio	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/817681/fortiguard	
1.5.6	Garantija	Siūlomai įrangai ir visiems pateiktiems techniniams ir programiniams komponentams garantinė priežiūra turi būti atliekama paties įrangos gamintojo arba jo autorizuoto aptarnavimo atstovo. Garantinio aptarnavimo metu turi būti nemokamai atliekami remonto darbai ir nemokamai keičiami sugedę komponentai. Papildomi garantinio remonto ir palaikymo reikalavimai pateikti Techninės specifikacijos 4.12 skyriuje.	Warranty	Offered equipment and all supplied hardware and software components must be under warranty service either by equipment manufacturer or by an authorized service representative. Warranty service must include free repair and replacement of defective components. For additional warranty repair and maintenance requirements, see Section 4.12 of the Technical Specification.	Siūlomai įrangai ir visiems pateiktiems techniniams ir programiniams komponentams garantinė priežiūra turi būti atliekama paties įrangos gamintojo arba jo autorizuoto aptarnavimo atstovo. Garantinio aptarnavimo metu turi būti nemokamai atliekami remonto darbai ir nemokamai keičiami sugedę komponentai. Papildomi garantinio remonto ir palaikymo reikalavimai pateikti Techninės specifikacijos 4.12 skyriuje.		
2.	**Kritinio tinklo ugniasienių aukšto patikimumo sistema (toliau - Sistema) / Critical Network Firewall High Reliability System (Furth. - System)**						

2.1	Sistemos pavadinimas ir modelis (gamintojo suteiktas numeris (kodas))	Nurodomas sistemos komponentų pavadinimas ir modelis (gamintojo suteiktas numeris (kodas))	System name and model (manufacturer's identification number (code))	Name and model of system components are provided (manufacturer's identification number (code))	*FortiGate 600E*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	
2.2	Gamintojas (pavadinimas)	Nurodomas sistemos gamintojas	Manufacturer (name)	System manufacturer is provided	*Fortinet*		
2.3	**Sistemos charakteristikos**		**System characteristics**				
2.3.1	Sistemos funkcionalumo aprašymas	Specializuotas identiškai atitinkantis aparatinis–programinis sprendimas, skirtas užtikrinti: kritinio tinklo kontrolę, įsibrovimų aptikimą ir prevenciją, antivirusinę programinė įrangą srautų turinio kontrolę. Sprendimą turi sudaryti ne mažiau kaip 2 vienas kitą dubliuojantys įrenginiai, sujungti į aukšto patikimumo sistemą	Description of system functionality	Specialized identically matching hardware-software solution designed to provide: control of the inner perimeter; intrusion detection and prevention; anti-virus software; controlling the content of streams. The solution must consist of at least 2 duplicate devices connected in a high-availability system		https://www.fortinet.com/products/next-generation-firewall.html	
2.3.2	Sistema turi dirbti Aktyvus/Pasyvus (*angl* Active/Passive) ir Aktyvus/Aktyvus (*angl* Active/Active) režimais	Sistema dirba Aktyvus/Pasyvus (*angl* Active/Passive) ir Aktyvus/Aktyvus (*angl* Active/Active) režimais	System must be able to operate in Active / Passive and Active / Active modes	System can operate in Active / Passive and Active / Active modes	Sistema dirba Aktyvus/Pasyvus (*angl* Active/Passive) ir Aktyvus/Aktyvus (*angl* Active/Active) režimais	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_FGCP_ap_aa.htm	
2.3.3	Sutrikus aktyvaus įrenginio veikimui aukšto patikimumo sistema turi automatiškai persijungti į dubliuojantį įrenginį	Sutrikus aktyvaus įrenginio veikimui aukšto patikimumo sistema automatiškai persijungia į dubliuojantį įrenginį	In the event of active device malfunction high-availability system must automatically switch to the backup device	In the event of active device malfunction high-availability system automatically switches over to the backup device	Sutrikus aktyvaus įrenginio veikimui aukšto patikimumo sistema automatiškai persijungia į dubliuojantį įrenginį	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_FGCP_failover.htm	
2.3.4	Konfigūracija tarp aukšto patikimumo sistemos įrenginių turi būti automatiškai sinchronizuojama	Konfigūracija tarp aukšto patikimumo sistemos įrenginių automatiškai sinchronizuojama	Configuration between high-availability system devices must be automatically synchronized	Configuration between high-availability system devices is automatically synchronized	Konfigūracija tarp aukšto patikimumo sistemos įrenginių automatiškai sinchronizuojama	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverSyncConfig.htm	
2.3.5	Sistema turi užtikrinti, kad persijungimo metu aktyvios sesijos nenutrūktų	Sistema užtikrina, kad persijungimo metu aktyvios sesijos nenutrūktų	System must ensure that active sessions are not interrupted during the switch between systems	System ensures that active sessions are not interrupted during the switch between systems	Sistema užtikrina, kad persijungimo metu aktyvios sesijos nenutrūktų	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_SessPickupEnabling.htm	
2.3.6	Sistemą sudarantys įrenginiai turi stebėti tinklo prievadų būseną	Sistemą sudarantys įrenginiai stebi tinklo prievadų būseną	Devices that make up the system must be able to monitor status of network ports	Devices that make up the system can monitor status of network ports	Sistemą sudarantys įrenginiai stebi tinklo prievadų būseną	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverLink.htm	
2.3.7	Sistemą sudarantis kiekvienas įrenginys turi stebėti ar yra pasiekiami nurodyti IP adresai (*angl*. track IP). Jei nurodyti IP adresai yra nepasiekiami, sistema turi automatiškai persijungti į dubliuojantį įrenginį	Sistemą sudarantis kiekvienas įrenginys stebi ar yra pasiekiami nurodyti IP adresai (*angl*. track IP). Jei nurodyti IP adresai yra nepasiekiami, sistema automatiškai persijungia į dubliuojantį įrenginį	System must be able to monitor each device for availability of specified IP addresses (track IPs). If specified IP addresses are unavailable, system must automatically switch to the backup device	System can monitor each device for availability of specified IP addresses (track IPs). If specified IP addresses are unavailable, system must automatically switch to the backup device	Sistemą sudarantis kiekvienas įrenginys stebi ar yra pasiekiami nurodyti IP adresai (*angl* track IP). Jei nurodyti IP adresai yra nepasiekiami, sistema automatiškai persijungia į dubliuojantį įrenginį	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-high-availability/HA_failoverRemoteLink.htm	
2.3.8	Turi būti galimybė pagal poreikį pajungti į sistema	Ne mažiau kaip **2** tokius pačius įrenginius	It must be possible to connect higher number of devices to the system as needed	At least **2** identical devices	Ne mažiau kaip **2** tokius pačius įrenginius	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_FGCP_more-than-two.htm	
2.3.9	Kiekviename atskirame įrenginyje įdiegtų 1000Base-T prievadų skaičius	Ne mažiau kaip **8**	Number of 1000Base-T ports installed on each individual device	No less than **8**	Ne mažiau kaip **8**	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*

2.3.10	Kiekviename atskirame įrenginyje įdiegtų 10GBase-SR SFP+ prievadų skaičius *Prievadai turi būti to paties gamintojo kaip ir įrenginys arba kito gamintojo, oficialiai patvirtinti naudoti ugniasienės gamintojo (tokiu atveju prie pasiūlymo pridedamas ugniaisienės gamintojo patvirtinimas)*	Ne mažiau kaip **2**	Number of 10GBase-SR SFP + ports installed on each individual device *Ports must be from the same manufacturer as the device or another manufacturer, officially approved for use by the firewall manufacturer (in which case firewall shall be accompanied by firewall manufacturer's approval)*	No less than **2**	*Ne mažiau kaip 2 su FN-TRAN-SFP+SR*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 ir 6 psl.*
2.3.11	Kiekviename atskirame įrenginyje įdiegtų atskirų prievadų, skirtų įrenginiams sujungti į aukšto patikimumo sistemą ir komplektuotų reikalingais moduliais, skaičius	Ne mažiau kaip **1**	Number of separate ports installed in each individual device to connect devices to a high-reliability system and equipped with the required modules	No less than **1**	*1*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.3.12	Kiekviename atskirame įrenginyje įdiegtų papildomų konsolės (*angl*. Console) prievadų skaičius	Ne mažiau kaip **1**	Number of console ports installed on each individual device	No less than **1**	*1*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.3.13	Kiekviename atskirame įrenginyje įdiegtų atskirų 1000Base-T prievadų, skirtų įrenginiams valdyti, skaičius	Ne mažiau kaip **1**	Number of additional 1000Base-T ports installed on each individual device for device management	No less than **1**	*1*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.3.14	Kiekvieno atskiro įrenginio ugniasienės pralaidumas (angl.Firewall throughput), esant Enterprise mix tipo duomenų srautui arba esant UDP1518 srautui	Ne mažesnė kaip **18** Gbps,esant Enterprise mix tipo duomenų srautui arba ne mažesnė kaip **36** Gbps, esant UDP1518 srautui	Firewall throughput for each individual device with Enterprise mix type traffic or UDP1518 traffic	At least **18 Gbps** for Enterprise mix data traffic or at least **36 Gbps** for UDP1518 traffic	*36 Gbps UDP 1518*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.3.15	Kiekvieno atskiro įrenginio ugniasienės naudojant aplikacijų protokolų kontrolę (angl. Application Control) ir įsilaužimų kontrolę (angl. Intrusion prevention system) greitaveika, esant Enterprise mix tipo duomenų srautui	Ne mažesnė kaip **9,5** Gbps	Throughput of each individual device using Application Control and Intrusion Prevention System for Enterprice mix traffic	No less than **9,5** Gbps	*9.5 Gbps*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.3.16	Kiekvieno atskiro įrenginio ugniasienės naudojant programų protokolų kontrolę (angl. Application control) ir įsilaužimų kontrolę (angl. Intrusion prevension system) bei apsaugą nuo virusų, URL filtravimą, Anti-Bot apsaugą greitaveika, esant Enterprise mix tipo arba HTTP 21kB duomenų srautui	Ne mažesnė kaip **5,8** Gbps	Throughput of each individual device while using Application control, Intrusion prevention, virus protection, URL filtering, Anti-Bot protection for Enterprise mix or HTTP 21 kB traffic	No less than **5,8** Gbps	*7 Gbps*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.3.17	Kiekvieno atskiro įrenginio IPSEC VPN greitaveika, esant idialioms testavimo sąlygoms	Ne mažesnė kaip **4** Gbps	IPSEC VPN performance of each individual device under ideal test conditions	No less than **4** Gbps	*20 Gbps*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.3.18	Kiekviename atskirame įrenginyje veikiančių konkurentinių sesijų skaičius, esant idialioms testavimo sąlygoms	Ne mažiau kaip **4000000**	Number of concurrent sessions running on each individual device under ideal test conditions	No less than **4000000**	*8 000 000*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.3.19	Kiekvienas atskiras įrenginys turi palaikyti naujų sesijų per sekundę, esant idialioms testavimo sąlygoms	Ne mažiau kaip **150000**	Each individual device must support new sessions per second under ideal test conditions	No less than **150000**	*450 000*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.3.20	Kiekviename atskirame įrenginyje veikiančių vienu metuvirtualių tinklų (VLAN) skaičius	Ne mažiau kaip **4094**	Number of concurrent virtual networks (VLANs) running on each individual device	No less than **4094**	*4094*	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-system-administration-52/VLANs/VLANs.htm	

2.3.21	Kiekviename atskirame įrenginyje veikiančių loginių savarankiškų virtualių sistemų (domenų) skaičius	Ne mažiau kaip **10**	Number of logical stand-alone virtual systems (domains) which must be configurable on each individual device	No less than **10**	*10*	https://kb.fortinet.com/kb/documentLink.do?externalID=11739	
2.3.22	Kiekvieno atskiro įrenginio ugniasienės vartotojų skaičius neribojamas	Kiekvieno atskiro įrenginio ugniasienės vartotojų skaičius neribojamas	There must be no limit to the number of users per firewall	There is no limit to the number of users per firewall	Kiekvieno atskiro įrenginio ugniasienės vartotojų skaičius neribojamas	https://help.fortinet.com/cli/fos60hlp/60/Content/FortiOS/fortiOS-cli-ref/config/system/resource-limits.htm	
2.3.23	Kiekvienas atskiras įrenginys turi veikti tokiais režimais	Skaidrus (*angl* . transparent); maršrutizavimo (angl. routing).	Each individual device must operate in these modes:	Transparent; Routing.	Skaidrus (*angl* . transparent); maršrutizavimo (angl. routing).	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-getting-started-54/2-Installation/2-NAT-Route-vs-Transparent.htm	
2.3.24	Turi būti galimybė sukonfigūruoti įrenginį taip, kad jis vienu metu, vienoje sistemoje, veiktų visais palaikomais režimais	Yra galimybė sukonfigūruoti įrenginį taip, kad jis vienu metu, vienoje sistemoje, veiktų visais palaikomais režimais	It must be possible to configure device to operate simultaneously in all supported modes on one device	It is possible to configure device to operate simultaneously in all supported modes on one device.	Yra galimybė sukonfigūruoti įrenginį taip, kad jis vienu metu, vienoje sistemoje, veiktų visais palaikomais režimais	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-firewall/Concepts%20-%20WAN%20Opt/Operating%20modes%20and%20VDOMs.htm	
2.3.25	Kiekviename atskirame įrenginyje turi būti galimybė įjungti apsaugą nuo DoS atakų.	Kiekviename atskirame įrenginyje yra galimybė įjungti apsaugą nuo DoS atakų.	Each individual device must have ability to enable DoS attack protection.	Each individual device has ability to enable DoS attack protection.	Kiekviename atskirame įrenginyje yra galimybė įjungti apsaugą nuo DoS atakų.	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Inside%20FortiOS%20DoS%20Protection.htm	
2.3.26	Kiekvienas atskiras įrenginys turi veikti loginio grupavimo protokolą *Turi būti galimybė apjungti į vieną loginį tinklo prievadą nemažiau kaip 8 fizines prievadus. Loginis prievadas gali būti naudojamas kaip L2 arba L3 lygio prievadas*	IEEE 802.3ad arba lygiavertį	Each individual device must run a logical grouping protocol *It must be possible to connect at least 8 physical ports to a single logical network port. Logical port can be used as an L2 or L3 level port*	IEEE 802.3ad or equivalent.	IEEE 802.3ad arba lygiavertį	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-networking-54/Interfaces/Aggregate%20Interfaces.htm	
2.3.27	Kiekvienas atskiras įrenginys turi palaikyti VLAN žymėjimo (*angl* . tagging) protokolą *VLAN prievadai gali būti kuriamos tinklo prievadams, veikiantiems L2 ir L3 lygyje*	IEEE 802.1q arba lygiavertį	Each individual device must support VLAN tagging protocol *VLAN ports can be created for network ports operating at the L2 and L3 levels*	IEEE 802.1q or equivalent.	IEEE 802.1q arba lygiavertį	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-system-administration-52/VLANs/VLANs.htm	
2.3.28	Kiekviename atskirame įrenginyje turi veikti vidinio DHCP serverio funkcija	Kiekviename atskirame įrenginyje veikia vidinio DHCP serverio funkcija	It must be possible to configure internal DHCP server in each individual device	It is possible to configure internal DHCP server in each individual device.	Kiekviename atskirame įrenginyje veikia vidinio DHCP serverio funkcija	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Advanced/DHCP%20servers%20and%20relays.htm	
2.3.29	Kiekviename atskirame įrenginyje turi būti palaikoma DHCP Relay funkcija	Kiekviename atskirame įrenginyje yra palaikoma DHCP Relay funkcija	DHCP Relay function must be supported on each individual device	DHCP Relay function is supported on each individual device.	Kiekviename atskirame įrenginyje yra palaikoma DHCP Relay funkcija	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Advanced/DHCP%20servers%20and%20relays.htm	
2.3.30	Kiekviename atskirame įrenginyje turi veikti DHCP ir PPPoE klientai	Kiekviename atskirame įrenginyje veikia DHCP ir PPPoE klientus	It must be possible to configure DHCP or PPPoE clients on each individual device	It is possible to configure DHCP or PPPoE clients on each individual device.	Kiekviename atskirame įrenginyje veikia DHCP ir PPPoE klientus	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-	

2.3.31	Kiekviename atskirame įrenginyje turi veikti dinaminio maršrutizavimo protokolai	Statiniai maršrutai (*angl* . static routes); BGPv4; OSPFv2; OSPFv3.	Dynamic routing protocols must be running on each individual device	Static routes; BGPv4; OSPFv2; OSPFv3.	Statiniai maršrutai (*angl* . static routes); BGPv4; OSPFv2; OSPFv3.	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-advanced-routing-52/Routing_Dynamic/Comparison_Protocols.htm	
2.3.32	Kiekviename atskirame įrenginyje turi veikti grakštus BGP ir OSPF perkrovimas (*angl* . graceful restart)	Kiekviename atskirame įrenginyje veikia grakštus BGP ir OSPF perkrovimas (*angl* . graceful restart).	Each individual device must be able to perform graceful restart for BGP and OSPF.	Each individual device is able to perform graceful restart for BGP and OSPF.	Kiekviename atskirame įrenginyje veikia grakštus BGP ir OSPF perkrovimas (*angl* graceful restart).	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverGraceful.htm	
2.3.33	Kiekviename atskirame įrenginyje turi veikti Multicast protokolai	IGMP (versijos 2 ir 3), IGMP proxy arba lygiavertis; PIM-SM arba lygiavertis; PIM-SSM arba lygiavertis	Multicast protocol must be working on each individual device	IGMP (version 2 and 3), IGMP proxy or equivalent; PIM-SM or equivalent; PIM-SSM or equivalent.	IGMP (versijos 2 ir 3), IGMP proxy arba lygiavertis; PIM-SM arba lygiavertis; PIM-SSM arba lygiavertis	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/741750/router-multicast	
2.3.34	Kiekviename atskirame įrenginyje turi veikti politika pagrįstą maršrutizavimas (angl. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną, siuntėjo, gavėjo IP adresą, servisą	Kiekviename atskirame įrenginyje veikia politika pagrįstą maršrutizavimas (angl. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną, siuntėjo, gavėjo IP adresą, servisą	Each individual device must be able to configure Policy Based Routing based on source/destination area, sender, recipient IP address, service, user ID, user group, application	Each individual device can configure Policy Based Routing based on source/destination area, sender, recipient IP address, service, user ID, user group, application.	Kiekviename atskirame įrenginyje veikia politika pagrįstą maršrutizavimas (angl. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną, siuntėjo, gavėjo IP adresą, servisą	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-advanced-routing-54/Routing_Advanced_Static/Policy_Routing.htm	
2.3.35	Kiekvienas atskiras įrenginys turi palaikyti IPv6 protokolą	Kiekvienas atskiras įrenginys palaiko IPv6 protokolą	Each individual device must support IPv6 protocol	Each individual device supports IPv6 protocol.	Kiekvienas atskiras įrenginys palaiko IPv6 protokolą	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/IPv6%20in%20FortiOS.htm	
2.3.36	Kiekviename atskirame įrenginyje turi veikti BFD (Bidirectional Forwarding Detection) arba lygiavertis funckionalumas	Kiekviename atskirame įrenginyje veikia BFD (Bidirectional Forwarding Detection) arba lygiavertis funckionalumas	Each individual device must support BFD (Bidirectional Forwarding Detection) or equal functionality	Each individual device supports BFD (Bidirectional Forwarding Detection) or equal functionality.	Kiekviename atskirame įrenginyje veikia BFD (Bidirectional Forwarding Detection) arba lygiavertis funckionalumas	https://kb.fortinet.com/kb/documentLink.do?externalID=FD30260	
2.3.37	Kiekviename atskirame įrenginyje turi veikti adresų transliavimas (angl. NAT)	statinis adresų transliavimas (*angl* . Static NAT); šaltinio adreso transliavimas su portų adresų transliavimu (PAT); paskirties adreso transliavimas su portų adresų transliavimu (PAT)	Each individual device must have Network Address Translation (NAT)	Static NAT; source address translation with port address translation (PAT); destination address translation with port address translation (PAT).	statinis adresų transliavimas (*angl* . Static NAT); šaltinio adreso transliavimas su portų adresų transliavimu (PAT); paskirties adreso transliavimas su portų adresų transliavimu (PAT)	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Dynamic%20NAT.htm	
2.3.38	Kiekviename atskirame įrenginyje turi veikti adresų transliavimas tarp IPv6 ir IPv4 protokolų	Kiekviename atskirame įrenginyje veikia adresų transliavimas tarp IPv6 ir IPv4 protokolų	Address translation between IPv6 and IPv4 protocols must be working on each individual device	Address translation between IPv6 and IPv4 protocols is working on each individual device.	Kiekviename atskirame įrenginyje veikia adresų transliavimas tarp IPv6 ir IPv4 protokolų	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-firewall-52/Concepts/NAT%2064%20and%20NAT46.htm	
2.3.39	Kiekvienas atskiras įrenginys turi saugoti nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos)	Kiekvienas atskiras įrenginys saugo nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos)	Each individual device must be able to protect against attacks, malicious code (eg viruses, spyware)	Each individual device is able to protect against attacks, malicious code (eg viruses, spyware)	Kiekvienas atskiras įrenginys saugo nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos)	https://www.fortiguard.com/learnmore#av	
2.3.40	Kiekvienas atskiras įrenginys turi gebėti, nustačius grėsmę, automatiškai įrašyti paketus, susijusius su grėsme	Kiekvienas atskiras įrenginys geba, nustačius grėsmę, automatiškai įrašyti paketus, susijusius su grėsme	Each individual device must have capability to automatically record threat-related packets upon detection	Each individual device has capability to automatically record threat-related packets upon detection	Kiekvienas atskiras įrenginys geba, nustačius grėsmę, automatiškai įrašyti paketus, susijusius su grėsme	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Enable%20IPS%20packet%20logging.htm	
2.3.41	Kiekvienas atskiras įrenginys turi atpažinti ir kontroliuoti aplikacijas (protokolus) *Tos pačios aplikacijos skirtingos versijos skaičiuojamos kaip viena aplikacija*	Ne mažiau kaip **3000**	Each individual device must recognize and control applications (protocols) Different versions of the same application are counted as one application	No less than **3000**	*Daugiau kaip 4000*	https://fortiguard.com/learnmore#ac	

2.3.42	Kiekvienas atskiras įrenginys turi atpažinti ir kontroliuoti industrinių sistemų (angl. Industrial Control Systems) ir SCADA (Supervisory control and data acquisition) aplikacijas (protokolus)	Kiekvienas atskiras įrenginys atpažina ir kontroliuoja industrinių sistemų (angl. Industrial Control Systems) ir SCADA (Supervisory control and data acquisition) aplikacijas (protokolus)	Each individual device must recognize and control Industrial Control Systems and SCADA (Supervisory control and data acquisition) applications (protocols)	Each individual device is able to recognize and control Industrial Control Systems and SCADA (Supervisory control and data acquisition) applications (protocols)	Kiekvienas atskiras įrenginys atpažina ir kontroliuoja industrinių sistemų (angl. Industrial Control Systems) ir SCADA (Supervisory control and data acquisition) aplikacijas (protokolus)	https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/industrial-control-systems	
2.3.43	Kiekvienas atskiras įrenginys turi gebėti apsirašyti savo aplikaciją	Kiekvienas atskiras įrenginys geba apsirašyti savo aplikaciją	Each individual device must be able to write down its application	Each individual device can write down its application	Kiekvienas atskiras įrenginys geba apsirašyti savo aplikaciją	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20Application%20&%20IPS%20Signatures.htm	
2.3.44	Kiekvienas atskiras įrenginys turi gebėti kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma	Kiekvienas atskiras įrenginys geba kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma	Each individual device must be able to set individual time for each application after which inactive session is closed	Each individual device can set individual time for each application after which inactive session is closed	Kiekvienas atskiras įrenginys geba kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma	https://help.fortinet.com/cli/fos50hlp/56/Content/FortiOS/fortiOS-cli-ref-56/config/application/list.htm	
2.3.45	Kiekvienas atskiras įrenginys turi gebėti kurti saugumo taisykles, kurios leistų vartotojams jungtis tik prie tam tikros aplikacijos ar aplikacijų grupės, nenurodant serviso/prievado, kuriuo dirba aplikacija, t. y. vartotojas gali prisijungti prie nurodytos aplikacijos nepriklausomai nuo to kokį servisą/prievadą naudoja aplikacija	Kiekvienas atskiras įrenginys geba kurti saugumo taisykles, kurios leistų vartotojams jungtis tik prie tam tikros aplikacijos ar aplikacijų grupės, nenurodant serviso/prievado, kuriuo dirba aplikacija, t. y. vartotojas gali prisijungti prie nurodytos aplikacijos nepriklausomai nuo to kokį servisą/prievadą naudoja aplikacija	Each individual device must have the ability to create security rules that allow users to connect only to a specific application or group of applications without specifying service/port application is running on, i.e. user can connect to specified application regardless of which service/port application uses	Each individual device can create security rules that allow users to connect only to a specific application or group of applications without specifying service/port application is running on, i.e. user can connect to specified application regardless of which service/port application uses.	Kiekvienas atskiras įrenginys geba kurti saugumo taisykles, kurios leistų vartotojams jungtis tik prie tam tikros aplikacijos ar aplikacijų grupės, nenurodant serviso/prievado, kuriuo dirba aplikacija, t. y. vartotojas gali prisijungti prie nurodytos aplikacijos nepriklausomai nuo to kokį servisą/prievadą naudoja aplikacija	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20Application%20&%20IPS%20Signatures.htm	
2.3.46	Kiekvienas atskiras įrenginys turi gebėti riboti prisijungimų iš vieno šaltinio skaičių pagal	siuntėjo IP; gavėjo IP; siuntėjo ir gavėjo IP	Each individual device must have ability to limit number of connections based on provided criteria:	Source IP; Destination IP; Source and Destination IP.	siuntėjo IP; gavėjo IP; siuntėjo ir gavėjo IP	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Security%20Policies/Firewall%20policies.htm	
2.3.47	Kiekvienas atskiras įrenginys, kuriant ugniasienės saugumo taisykles, turi gebėti nurodyti siuntėją, gavėją, servisą/prievadą, aplikaciją, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Servisai/prievadai ir aplikacijos taisyklėse turi būti nurodomi atskiruose laukuose	Kiekvienas atskiras įrenginys, kuriant ugniasienės saugumo taisykles, geba nurodyti siuntėją, gavėją, servisą/prievadą, aplikaciją, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Servisai/prievadai ir aplikacijos taisyklėse yra nurodomi atskiruose laukuose	Each individual device must have ability to specify source, destination, service/port, application, applicable security measures, user, user group when creating firewall rules. Services/ports and applications rules must be referenced in separate fields.	Each individual device has ability to specify source, destination, service/port, application, applicable security measures, user, user group when creating firewall rules. Services/ports and applications rules must be referenced in separate fields.	Kiekvienas atskiras įrenginys, kuriant ugniasienės saugumo taisykles, geba nurodyti siuntėją, gavėją, servisą/prievadą, aplikaciją, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Servisai/prievadai ir aplikacijos taisyklėse yra nurodomi atskiruose laukuose	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Security%20Policies/Firewall%20policies.htm	
2.3.48	Kiekvienas atskiras įrenginys turi gebėti skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones	Kiekvienas atskiras įrenginys geba skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones	Each individual device must have ability to use different security measures for different data traffic.	Each individual device has ability to use different security measures for different data traffic.	Kiekvienas atskiras įrenginys geba skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones	https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/853759	
2.3.49	Kiekvienas atskiras įrenginys pagal nutylėjimą turi blokuoti visas aplikacijas išskyrus tas, kurios yra apibrėžtos saugumo taisyklėse kaip leistinos	Kiekvienas atskiras įrenginys pagal nutylėjimą blokuoja visas aplikacijas išskyrus tas, kurios yra apibrėžtos saugumo taisyklėse kaip leistinos	By default, each individual device must block all applications except those defined in the firewall rules as allowed	By default, each individual device is blocking all applications except those defined in the firewall rules as allowed.	Kiekvienas atskiras įrenginys pagal nutylėjimą blokuoja visas aplikacijas išskyrus tas, kurios yra apibrėžtos saugumo taisyklėse kaip leistinos	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Security%20Policies/Firewall%20policies.htm	
2.3.50	Kiekvienas atskiras įrenginys turi gebėti suteikti vartotojams prieigą prie aplikacijos/ų (ne serviso/prievado) nepriklausomai nuo to kokiais TCP, UDP prievadais dirba aplikacija	Kiekvienas atskiras įrenginys geba suteikti vartotojams prieigą prie aplikacijos/ų (ne serviso/prievado) nepriklausomai nuo to kokiais TCP, UDP prievadais dirba aplikacija	Each individual device must be able to provide users with access to the application(s) (not service/port), regardless of which TCP, UDP ports the application is running on	Each individual device can provide users with access to the application(s) (not service/port), regardless of which TCP, UDP ports the application is running on.	Kiekvienas atskiras įrenginys geba suteikti vartotojams prieigą prie aplikacijos/ų (ne serviso/prievado) nepriklausomai nuo to kokiais TCP, UDP prievadais dirba aplikacija	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Application_Control/Application%20Control%20Concepts.htm	

2.3.51	Kiekvienas atskiras įrenginys turi gebėti nurodyti prie kokių aplikacijų vartotojui leidžiama jungtis, o prie kokių neleidžiama, net jei aplikacijos dirba tais pačiais TCP, UDP prievadais	Kiekvienas atskiras įrenginys geba nurodyti prie kokių aplikacijų vartotojui leidžiama jungtis, o prie kokių neleidžiama, net jei aplikacijos dirba tais pačiais TCP, UDP prievadais	Each individual device must be able to specify which applications user can connect to and which ones cannot, even if applications are running on the same TCP, UDP ports	Each individual device can specify which applications user can connect to and which ones cannot, even if applications are running on the same TCP, UDP ports	Kiekvienas atskiras įrenginys geba nurodyti prie kokių aplikacijų vartotojui leidžiama jungtis, o prie kokių neleidžiama, net jei aplikacijos dirba tais pačiais TCP, UDP prievadais	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-profiles/Application_Control/Enable%20Application%20Control.htm	
2.3.52	Kiekvienas atskiras įrenginys turi gebėti suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta	Kiekvienas atskiras įrenginys geba suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta	Each individual device must be able to grant access rights only to authenticated users	Each individual device is able to grant access rights only to authenticated users	Kiekvienas atskiras įrenginys geba suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Auth_Intro.htm	
2.3.53	Kiekvienas atskiras įrenginys turi gebėti dinamiškai susieti IP adresą su vartotojų	Kiekvienas atskiras įrenginys geba dinamiškai susieti IP adresą su vartotojų	Each individual device must be able to dynamically associate an IP address with user	Each individual device can dynamically associate an IP address with user	Kiekvienas atskiras įrenginys geba dinamiškai susieti IP adresą su vartotojų	https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/374938/setting-up-your-fortigate-for-fsso	
2.3.54	Kiekvienas atskiras įrenginys turi gebėti suteikti prieigos teises vartotojams, ir/arba vartotojų grupėms.	Kiekvienas atskiras įrenginys geba suteikti prieigos teises vartotojams, ir/arba vartotojų grupėms.	Each individual device must be able to grant access rights to users and/or user groups.	Each individual device has the ability to grant access rights to users and/or user groups.	Kiekvienas atskiras įrenginys geba suteikti prieigos teises vartotojams, ir/arba vartotojų grupėms.	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Security%20Policies/Firewall%20policies.htm	
2.3.55	Kiekvienas atskiras įrenginys turi gebėti nustatyti vartotojų tapatybę, neprašydamas suvesti vartotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz. Active Directory	Kiekvienas atskiras įrenginys geba nustatyti vartotojų tapatybę, neprašydamas suvesti vartotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz. Active Directory	Each individual device must be able to authenticate users without having to enter their username and password but using existing network services eg Active Directory	Each individual device can authenticate users without having to enter their username and password but using existing network services eg Active Directory.	Kiekvienas atskiras įrenginys geba nustatyti vartotojų tapatybę, neprašydamas suvesti vartotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz. Active Directory	https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/374938/setting-up-your-fortigate-for-fsso	
2.3.56	Kiekvienas atskiras įrenginys turi būti integruojamas su Active Directory, LDAP, RADIUS	Kiekvienas atskiras įrenginys yra integruojamas su Active Directory, LDAP, RADIUS	Each individual device must be integrated with Active Directory, LDAP, RADIUS	Each individual device is integrated with Active Directory, LDAP, RADIUS	Kiekvienas atskiras įrenginys yra integruojamas su Active Directory, LDAP, RADIUS	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Servers.htm	
2.3.57	Ugniasienė turi sinchronizuoti vartotojų-ID ir jų IP adresų informaciją. Informacija turi būti renkama tiesiogiai arba per papildomus agentus iš: •Active Directory domain servisų, •Radius accounting šaltinių, •terminalinių serverių. Turi būti papildoma galimybė surinkti informaciją iš Syslog šaltinių tiesiogiai arba naudojant papildomą programinę įrangą, kuri nėra įtraukiama į pasiūlymą. *Vartotojų ID ir IP adresų sinchronizacijai negali būti instaliuojami papildomi agentai klientų kompiuteriuose.* *Šis reikalavimas gali būti įgyvendintas lygiaverčiu funkcionalumu ar pateikiamais sprendimais, kurie nenaudojant papildomų agentų klientų kompiuteriuose sinchronizuotų vartotojų-ID ir jų IP adresų informaciją su Užsakovo turima ir naudojama sistema Aruba ClearPass ir terminaliniuose serveriuose*	Ugniasienė sinchronizuoja vartotojų-ID ir jų IP adresų informaciją. Informacija turi būti renkama tiesiogiai arba per papildomus agentus iš: •Active Directory domain servisų, •Radius accounting šaltinių, •terminalinių serverių. Turi būti papildoma galimybė surinkti informaciją iš Syslog šaltinių tiesiogiai arba naudojant papildomą programinę įrangą, kuri nėra įtraukiama į pasiūlymą.	Firewall must synchronize user IDs and their IP address information. The information must be collected directly or through additional agents from: • Active Directory domain services, • Radius accounting sources • terminal servers. There must be an additional ability to collect information from Syslog sources directly or through the use of additional software that is not included in the offer. *Additional agents cannot be installed on client computers to synchronize user IDs and IP addresses.* *This requirement can be implemented with equivalent functionality or provided solutions that, without the use of additional agents, synchronize user IDs and their IP addresses on client computers with system owned and operated by Customer Aruba ClearPass and terminal servers*	Firewall synchronizes user IDs and their IP address information. The information must be collected directly or through additional agents from: • Active Directory domain services, • Radius accounting sources • terminal servers. There must be an additional ability to collect information from Syslog sources directly or through the use of additional software that is not included in the offer.	Ugniasienė sinchronizuoja vartotojų-ID ir jų IP adresų informaciją. Informacija turi būti renkama tiesiogiai arba per papildomus agentus iš: •Active Directory domain servisų, •Radius accounting šaltinių, •terminalinių serverių. Turi būti papildoma galimybė surinkti informaciją iš Syslog šaltinių tiesiogiai arba naudojant papildomą programinę įrangą, kuri nėra įtraukiama į pasiūlymą.	*https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso* *https://docs.fortinet.com/document/fortigate/6.0.0/handbook/658099/single-sign-on-to-windows-ad* *https://docs.fortinet.com/document/fortigate/6.0.0/handbook/372705/sso-using-radius-accounting-records* *https://docs.fortinet.com/document/fortimanager/6.2.1/new-features/733863/clearpass-sso-identity-connector*	

2.3.58	Kiekviename atskirame įrenginyje vartotojų identifikacijai turi būti palaikomas IPv6 protokolas	Kiekviename atskirame įrenginyje vartotojų identifikacijai yra palaikomas IPv6 protokolas	Each individual device must support IPv6 for user identification	Each individual device has a supported IPv6 protocol for user identification.	Kiekviename atskirame įrenginyje vartotojų identifikacijai yra palaikomas IPv6 protokolas	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-firewall/IPv6/IPv6%20Features/IPv6%20support%20for%20FSSO.htm	
2.3.59	Jei vartotojo tapatybė nebuvo nustatyta skaidriai, vartotojui turi būti parodomas puslapis, kuriame jis turi įvesti tapatybę patvirtinančius duomenis	Jei vartotojo tapatybė nebuvo nustatyta skaidriai, vartotojui turi būti parodomas puslapis, kuriame jis turi įvesti tapatybę patvirtinančius duomenis	If user has not been authenticated in a transparent manner, user must be shown a page where he/she must enter his/her identity details	If user has not been authenticated in a transparent manner, the user is shown a page where he/she must enter his/her identity details.	Jei vartotojo tapatybė nebuvo nustatyta skaidriai, vartotojui turi būti parodomas puslapis, kuriame jis turi įvesti tapatybę patvirtinančius duomenis	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/CaptivePortals.htm	
2.3.60	Kiekvienas atskiras įrenginys turi gebėti kontroliuoti vartotojų, dirbančių terminalinėje aplinkoje (pvz.: Windows Terminal Server) prieigos teises. Įrenginys turi skirti terminalinėje aplinkoje dirbančių vartotojų duomenų srautus ir kontroliuoti kiekvieno vartotojo prieigos teises	Kiekvienas atskiras įrenginys geba kontroliuoti vartotojų, dirbančių terminalinėje aplinkoje (pvz.: Windows Terminal Server) prieigos teises. Įrenginys turi skiria terminalinėje aplinkoje dirbančių vartotojų duomenų srautus ir kontroliuoti kiekvieno vartotojo prieigos teises	Each individual device must be able to control access rights of users working in terminal environment (ex. Windows Terminal Server). Device must allocate data flows to users in terminal environment and control access rights for each user	Each individual device can control access rights of users working in terminal environment (ex. Windows Terminal Server). Device must allocate data flows to users in terminal environment and control access rights for each user.	Kiekvienas atskiras įrenginys geba kontroliuoti vartotojų, dirbančių terminalinėje aplinkoje (pvz.: Windows Terminal Server) prieigos teises. Įrenginys turi skiria terminalinėje aplinkoje dirbančių vartotojų duomenų srautus ir kontroliuoti kiekvieno vartotojo prieigos teises	https://kb.fortinet.com/kb/viewContent.do?externalId=FD35372	
2.3.61	Kiekvienas atskiras įrenginys turi palaikyti vartotojų tapatybės nustatymą naudojant vartotojo skaitmeninį sertifikatą. Nustatant vartotojo tapatybę, turi būti galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse	Kiekvienas atskiras įrenginys palaiko vartotojų tapatybės nustatymą naudojant vartotojo skaitmeninį sertifikatą. Nustatant vartotojo tapatybę, yra galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse	Each individual device must support user authentication with user's digital certificate. When identifying a user, it must be possible to search user's data on multiple authentication servers	Each individual device supports user authentication with user's digital certificate. When identifying a user, it is possible to search user's data on multiple authentication servers.	Kiekvienas atskiras įrenginys palaiko vartotojų tapatybės nustatymą naudojant vartotojo skaitmeninį sertifikatą. Nustatant vartotojo tapatybę, yra galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Certificates.htm	
2.3.62	Kiekvienas atskiras įrenginys turi dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą	Kiekvienas atskiras įrenginys dešifruoja ir tikrina įeinantį ir išeinantį SSL duomenų srautą	Each individual device must decrypt and verify incoming and outgoing SSL traffic	Each individual device decrypts and verifies incoming and outgoing SSL traffic.	Kiekvienas atskiras įrenginys dešifruoja ir tikrina įeinantį ir išeinantį SSL duomenų srautą	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122078/deep-inspection	
2.3.63	Kiekviename atskirame įrenginyje turi būti pasirinktinai nurodoma, kurį duomenų srautą dešifruoti	Kiekviename atskirame įrenginyje yra pasirinktinai nurodoma, kurį duomenų srautą dešifruoti	Each individual device must be able to specify which data stream to decrypt	Each individual device has option of specifying which data stream to decrypt.	Kiekviename atskirame įrenginyje yra pasirinktinai nurodoma, kurį duomenų srautą dešifruoti	https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/853759	
2.3.64	Kiekviename atskirame įrenginyje SSL patikra turi būti atliekama visam SSL duomenų srautui, ne tik HTTPS, SMTPS, POP3S, IMAPS protokolams	Kiekviename atskirame įrenginyje SSL patikra atliekama visam SSL duomenų srautui, ne tik HTTPS, SMTPS, POP3S, IMAPS protokolams	SSL verification must be performed on each individual device for all SSL traffic, not just HTTPS, SMTPS, POP3S, IMAPS protocols	SSL verification is performed on each individual device for all SSL traffic, not just HTTPS, SMTPS, POP3S, IMAPS protocols.	Kiekviename atskirame įrenginyje SSL patikra atliekama visam SSL duomenų srautui, ne tik HTTPS, SMTPS, POP3S, IMAPS protokolams	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122078/deep-inspection	
2.3.65	Kiekviename atskirame įrenginyje SSL patikra turi apimti įsilaužimų, pažeidžiamumų aptikimą ir prevenciją, apsaugą nuo virusų, šnipinėjimo aplikacijų, perduodamų failų kontrolę, perduodamų duomenų turinio kontrolę, URL filtravimą	Kiekviename atskirame įrenginyje SSL patikra apima įsilaužimų, pažeidžiamumų aptikimą ir prevenciją, apsaugą nuo virusų, šnipinėjimo aplikacijų, perduodamų failų kontrolę, perduodamų duomenų turinio kontrolę, URL filtravimą	SSL verification on each individual device must include detection and prevention of hacking, vulnerabilities, virus protection, spyware, file transfer control, data transfer control, URL filtering	SSL verification on each individual device includes detection and prevention of hacking, vulnerabilities, virus protection, spyware, file transfer control, data transfer control, URL filtering.	Kiekviename atskirame įrenginyje SSL patikra apima įsilaužimų, pažeidžiamumų aptikimą ir prevenciją, apsaugą nuo virusų, šnipinėjimo aplikacijų, perduodamų failų kontrolę, perduodamų duomenų turinio kontrolę, URL filtravimą	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-security-profiles/SSL_SSH_Inspection/why_use_ssl_inspection.htm	
2.3.66	Kiekvienas atskiras įrenginys turi dešifruoti TLS1.2 duomenų srautą	Kiekvienas atskiras įrenginys dešifruoja TLS1.2 duomenų srautą	Each individual device must decrypt TLS1.2 data stream	Each individual device decrypts TLS1.2 data stream.	Kiekvienas atskiras įrenginys dešifruoja TLS1.2 duomenų srautą	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-load-balancing/ldb-ssl-tls-version.htm	
2.3.67	Kiekvienas atskiras įrenginys turi inspektuoti TLS1.3 duomenų srautą, atpažinti aplikacijas ir svetaines naudojančias TLS1.3	Kiekvienas atskiras įrenginys inspektuoja TLS1.3 duomenų srautą, atpažįsta aplikacijas ir svetaines naudojančias TLS1.3	Each individual device must inspect TLS1.3 traffic, recognize applications and sites using TLS1.3	Each individual device inspects TLS1.3 traffic, recognize applications and sites using TLS1.3	Kiekvienas atskiras įrenginys inspektuoja TLS1.3 duomenų srautą, atpažįsta aplikacijas ir svetaines naudojančias TLS1.3	https://docs.fortinet.com/document/fortigate/6.2.0/new-features/35927/tls-1-3-support	

2.3.68	Kiekvienas atskiras įrenginys turi riboti prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus	Kiekvienas atskiras įrenginys riboja prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus	Each individual device must be able to limit number of connections based on source, destination IP addresses, services, users	Each individual device can limit number of connections based on source, destination IP addresses, services, users.	Kiekvienas atskiras įrenginys riboja prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/885253/per-ip-traffic-shaper	
2.3.69	Kiekvienas atskiras įrenginys turi gebėti kurti savo įsilaužimų aprašus	Kiekvienas atskiras įrenginys geba kurti savo įsilaužimų aprašus	Each individual device must have the ability to create combined threat prevention descriptions	Each individual device has the ability to create combined threat prevention descriptions	Kiekvienas atskiras įrenginys geba kurti savo įsilaužimų aprašus	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20signature%20keywords.htm	
2.3.70	Kiekvienas atskiras įrenginys turi gebėti atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę	Kiekvienas atskiras įrenginys geba atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę	Each individual device must be able to control access to web resources using a manufacturer-provided URL database	Each individual device can control access to web resources using the URL database provided by the manufacturer	Kiekvienas atskiras įrenginys geba atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-profiles/Web_Filter/FortiGuard%20Web%20Filtering%20Service.htm	
2.3.71	Kiekvienas atskiras įrenginys turi gebėti sukurti leistinų ir draudžiamų URL ir IP sąrašus	Kiekviename atskirame įrenginyje yra galimybė sukurti leistinų ir draudžiamų URL ir IP sąrašus	Each individual device must be able to create lists of allowed and prohibited URLs and IPs	Each individual device can create lists of allowed and blocked URLs and IPs.	Kiekviename atskirame įrenginyje yra galimybė sukurti leistinų ir draudžiamų URL ir IP sąrašus	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-profiles/Web_Filter/Static%20URL%20Filter.htm	
2.3.72	Kiekvienas atskiras įrenginys turi gebėti sukurti ir naudoti savo URL grupes	Kiekvienas atskiras įrenginys geba sukurti ir naudoti savo URL grupes	Each individual device must be able to create and use its own URL groups	Each individual device can create and use its own URL groups.	Kiekvienas atskiras įrenginys geba sukurti ir naudoti savo URL grupes	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Web_Filter/Configuring%20Web%20Filter%20Profiles.htm	
2.3.73	Kiekviename atskirame įrenginyje turi būti galimybė kurti pažeidžiamumų aprašus	Kiekviename atskirame įrenginyje yra galimybė kurti pažeidžiamumų aprašus	Each individual device must be able to create vulnerability profiles	Each individual device can create vulnerability profiles.	Kiekviename atskirame įrenginyje yra galimybė kurti pažeidžiamumų aprašus	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20signature%20keywords.htm	
2.3.74	Kiekvienas atskiras įrenginys turi aptikti ir blokuoti Botnet	Kiekvienas atskiras įrenginys aptinka ir blokuoja Botnet	Each individual device must be able to detect Botnet	Each individual device can detect Botnet.	Kiekvienas atskiras įrenginys aptinka ir blokuoja Botnet	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/105208/botnet-c-c-domain-blocking	
2.3.75	Kiekvienas atskiras įrenginys turi palaikyti šifravimo algoritmus	3DES; AES128; AES256.	Each individual device must support provided encryption protocols:	3DES; AES128; AES256.	3DES; AES128; AES256.	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Concepts/Encryption.htm	
2.3.76	Kiekvienas atskiras įrenginys turi palaikyti saugios maišos algoritmus	SHA-1; SHA-256; SHA-384.	Each individual device must support provided secure hash algorithms:	SHA-1; SHA-256; SHA-384.	SHA-1; SHA-256; SHA-384.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/238852/encryption-algorithms	
2.3.77	Kiekvienas atskiras įrenginys turi gebėti siųsti IPv6 duomenų srautą per sukurtą IPSec tunelį tarp skirtingų gamintojo įrenginių	Kiekvienas atskiras įrenginys geba siųsti IPv6 duomenų srautą per sukurtą IPSec tunelį tarp skirtingų gamintojo įrenginių	Each individual device must be able to send IPv6 data traffic via IPSec tunnel between different manufacturer’s devices	Each individual device can send IPv6 data traffic via IPSec tunnel between different manufacturer’s devices.	Kiekvienas atskiras įrenginys geba siųsti IPv6 duomenų srautą per sukurtą IPSec tunelį tarp skirtingų gamintojo įrenginių	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-IPv6-54/IPv6%20Configuration/IPv6_IPsec_VPN.htm	

2.3.78	Kiekvienas atskiras įrenginys turi palaikyti duomenų srautų ribojimą pagal taikomąją programinę įrangą, vartotoją, siuntėjo, gavėjo IP adresus, tinklo sąsajas	Kiekvienas atskiras įrenginys palaiko duomenų srautų ribojimą pagal taikomąją programinę įrangą, vartotoją, siuntėjo, gavėjo IP adresus, tinklo sąsajas	Each individual device must be able to support data flow restrictions depending on application software, user, source, destination IP addresses, network interface.	Each individual device can support data flow restrictions depending on application software, user, source, destination IP addresses, network interface.	Kiekvienas atskiras įrenginys palaiko duomenų srautų ribojimą pagal taikomąją programinę įrangą, vartotoją, siuntėjo, gavėjo IP adresus, tinklo sąsajas	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-profiles/Application_Control/Enable-Application-Control-NGFW-Policy-Based.htm	
2.3.79	Kiekvienas atskiras įrenginys turi gebėti suteikti prioritetus duomenų paketams	Kiekvienas atskiras įrenginys geba suteikti prioritetus duomenų paketams	Each individual device must be able to give priority to data packets	Each individual device can give priority to data packets.	Kiekvienas atskiras įrenginys geba suteikti prioritetus duomenų paketams	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-traffic-shaping-54/TS_Configuration/TS_Configuring.htm	
2.3.80	Kiekvienas atskiras įrenginys turi gebėti pasirinktam duomenų srautui nustatyti maksimalų pralaidumą	Kiekvienas atskiras įrenginys geba pasirinktam duomenų srautui nustatyti maksimalų pralaidumą	Each individual device must be able to set maximum bandwidth for selected data stream	Each individual device can set maximum bandwidth for selected data stream.	Kiekvienas atskiras įrenginys geba pasirinktam duomenų srautui nustatyti maksimalų pralaidumą	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-traffic-shaping-54/TS_Configuration/TS_Configuring.htm	
2.3.81	Kiekviename atskirame įrenginyje maksimalus arba garantuotas pralaidumas turi būti konfigūruojamas pagal	ugniasienės saugumo taisyklę; vartotojo IP adresą; aplikaciją	For each individual device, maximum or guaranteed throughput must be configured as per provided criteria:	firewall security rule; user's IP address; application.	ugniasienės saugumo taisyklę; vartotojo IP adresą; aplikaciją	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-traffic-shaping-54/TS_Configuration/TS_Configuring.htm	
2.3.82	Kiekvienas atskiras įrenginys turi gebėti duomenų srautų valdymo statistiką atvaizduoti grafinių būdu	Kiekvienas atskiras įrenginys geba duomenų srautų valdymo statistiką atvaizduoti grafinių būdu	Each individual device must be capable of graphically displaying traffic management statistics	Each individual device is capable of graphically displaying traffic management statistics.	Kiekvienas atskiras įrenginys geba duomenų srautų valdymo statistiką atvaizduoti grafinių būdu	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-getting-started/using-the-GUI/dashboard.htm	
2.3.83	Kiekvienas atskiras įrenginys turi gebėti kurti saugumo taisykles iš karto tarp kelių saugumo zonų, t. y. sukurti vieną taisyklę, kuri leistų iš 2 ar daugiau zonų jungtis į 2 ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei.	Kiekvienas atskiras įrenginys geba kurti saugumo taisykles iš karto tarp kelių saugumo zonų, t .y. sukurti vieną taisyklę, kuri leistų iš 2 ar daugiau zonų jungtis į 2 ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei.	Each individual device must be able to create security rules for multiple security zones at once, i.e. create a single rule that allows connections from 2 or more zones to 2 or more zones without creating separate rules for each interzone flow control.	Each individual device can create security rules for multiple security zones at once, i.e. create a single rule that allows connections from 2 or more zones to 2 or more zones without creating separate rules for each interzone flow control.	Kiekvienas atskiras įrenginys geba kurti saugumo taisykles iš karto tarp kelių saugumo zonų, t .y. sukurti vieną taisyklę, kuri leistų iš 2 ar daugiau zonų jungtis į 2 ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei.	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/FeatureCatalog-firewall.htm	
2.3.84	Kiekvienas atskiras įrenginys turi gebėti importuoti skaitmeninius sertifikatus SSL sesijų terminavimui / perėmimui ar įrenginio valdymui	Kiekvienas atskiras įrenginys geba importuoti skaitmeninius sertifikatus SSL sesijų terminavimui / perėmimui ar įrenginio valdymui	Each individual device must be able to import digital certificates for SSL session termination/interception or device management	Each individual device can import digital certificates for SSL session termination/interception or device management.	Kiekvienas atskiras įrenginys geba importuoti skaitmeninius sertifikatus SSL sesijų terminavimui / perėmimui ar įrenginio valdymui	https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/378040/importing-the-signed-certificate-to-your-fortigate	
2.3.85	Kiekvienas atskiras įrenginys turi palaikyti CRL (*angl* . Certificate revocation list)	Kiekvienas atskiras įrenginys palaiko CRL (angl. Certificate revocation list)	Each individual device must support CRL (Certificate Revocation List)	Each individual device supports CRL (Certificate Revocation List).	Kiekvienas atskiras įrenginys palaiko CRL (angl. Certificate revocation list)	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/96571/certificate-crl	
2.3.86	Kiekvienas atskiras įrenginys turi palaikyti OCSP (*angl* . Online Certificate Status Protocol) protokolą	Kiekvienas atskiras įrenginys palaiko OCSP (angl. Online Certificate Status Protocol) protokolą	Each individual device must support Online Certificate Status Protocol (OCSP)	Each individual device supports the Online Certificate Status Protocol (OCSP).	Kiekvienas atskiras įrenginys palaiko OCSP (angl. Online Certificate Status Protocol) protokolą	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/59761/vpn-certificate-ocsp-server	
2.3.87	Kiekvienas atskiras įrenginys turi palaikyti 4096 bitų RSA sertifikatus	Kiekvienas atskiras įrenginys palaiko 4096 bitų RSA sertifikatus	Each individual device must support 4096-bit RSA certificates	Each individual device supports 4096-bit RSA certifications.	Kiekvienas atskiras įrenginys palaiko 4096 bitų RSA sertifikatus	https://docs.fortinet.com/document/fortigate/6.2.2/cli-reference/277620/vpn-certificate-setting	

2.3.88	Kiekvienas atskiras įrenginys turi gebėti importuoti tarnybinių stočių viešus, privačius raktus ir sertifikatus *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekvienas atskiras įrenginys geba importuoti tarnybinių stočių viešus, privačius raktus ir sertifikatus	Each individual device must be able to import public, private server keys and certificates *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Each individual device can import public, private server keys and certificates.	Kiekvienas atskiras įrenginys geba importuoti tarnybinių stočių viešus, privačius raktus ir sertifikatus	https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/378040/importing-the-signed-certificate-to-your-fortigate	
2.3.89	Kiekvienas atskiras įrenginys turi gebėti generuoti ir eksportuoti Netflow v9 ar lygiaverčius įrašus apie duomenų srautus. Įrašuose turi būti informacija apie vartotojus ir taikomąją programinę įrangą	Kiekvienas atskiras įrenginys geba generuoti ir eksportuoti Netflow v9 ar lygiaverčius įrašus apie duomenų srautus. Įrašuose turi būti informacija apie vartotojus ir taikomąją programinę įrangą	Each individual device must be able to generate and export Netflow v9 or equivalent data feeds. The records must contain information about users and software application.	Each individual device can generate and export Netflow v9 or equivalent data feeds. The records must contain information about users and software application.	Kiekvienas atskiras įrenginys geba generuoti ir eksportuoti Netflow v9 ar lygiaverčius įrašus apie duomenų srautus. Įrašuose turi būti informacija apie vartotojus ir taikomąją programinę įrangą	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-networking/Troubleshooting/Netflow.htm	
2.3.90	Kiekvieno atskiro įrenginio Įvykių žurnalai turi būti siunčiami į centrinę valdymo tarnybinę stotį	Kiekvieno atskiro įrenginio Įvykių žurnalai yra siunčiami į centrinę valdymo tarnybinę stotį	Event logs for each individual device must be stored locally and sent to a central management server	Event logs for each individual device are stored locally and sent to a central management server.	Kiekvieno atskiro įrenginio Įvykių žurnalai yra siunčiami į centrinę valdymo tarnybinę stotį	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-logging-reporting-54/logs.htm	
2.3.91	Įvykių žurnaluose turi būti galimybė	filtruoti įvykius; fiksuoti administratorių atliekamus veiksmus	Event logs must have the capability	filter events; record actions taken by administrators.	filtruoti įvykius; fiksuoti administratorių atliekamus veiksmus	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-logging-reporting-54/logs.htm	
2.3.92	Kiekviename atskirame įrenginyje turi būti atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginį esant dideliam tinklo aprovimui	Kiekviename atskirame įrenginyje yra atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginį esant dideliam tinklo aprovimui	Each individual device must have separate control and data analysis modules to ensure that device can be operated at high network load	Each individual device has its own control and data analysis modules to control device at high network load.	Kiekviename atskirame įrenginyje yra atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginį esant dideliam tinklo aprovimui	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Other_Profile_Considerations/Conserve%20mode.htm	
2.3.93	Kiekvienas atskiras įrenginys turi būti valdomas	SSHv2; iš centrinės valdymo sistemos	Each individual device must be controlled via:	SSHv2; Central management system.	SSHv2; iš centrinės valdymo sistemos	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-getting-started-52/basic_admin.htm https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-system-administration-52/Central%20Management/central_mgmt.htm	
2.3.94	Turi būti galimybė naudoti IPv6 kiekvieno atskiro įrenginio ir centrinės valdymo tarnybinės stoties sujungimui	Yra galimybė naudoti IPv6 kiekvieno atskiro įrenginio ir centrinės valdymo tarnybinės stoties sujungimui	It must be possible to use IPv6 to connect each individual device to central management server	It is possible to use IPv6 to connect each individual device to the central management server.	Yra galimybė naudoti IPv6 kiekvieno atskiro įrenginio ir centrinės valdymo tarnybinės stoties sujungimui	https://help.fortinet.com/cli/fos60hlp/60/Content/FortiOS/fortiOS-cli-ref/config/system/central-management.htm	
2.3.95	Kiekvieno atskiro įrenginio administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekvieno atskiro įrenginio administratorių prieigos teisės yra kontroliuojamos rolių pagalba	Administrators' permissions for each individual device must be controlled by roles *Functionality can be implemented from a central management system*	Administrators' permissions for each individual device are controlled by roles.	Kiekvieno atskiro įrenginio administratorių prieigos teisės yra kontroliuojamos rolių pagalba	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/294491/administrator-profiles	
2.3.96	Kiekviename atskirame įrenginyje turi būti galimybė kurti administratorių roles *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekviename atskirame įrenginyje yra galimybė kurti administratorių roles	Each individual device must have ability to create administrator roles *Functionality can be implemented from a central management system*	Each individual device can create administrator roles.	Kiekviename atskirame įrenginyje yra galimybė kurti administratorių roles	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/294491/administrator-profiles	
2.3.97	Kiekviename atskirame įrenginyje turi būti galimybė apibrėžti administratoriaus teises *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekviename atskirame įrenginyje yra galimybė apibrėžti administratoriaus teises	Each individual device must have ability to fine-tune administrator privileges *Functionality can be implemented from a central management system*	Each individual device has ability to fine-tune administrator privileges.	Kiekviename atskirame įrenginyje yra galimybė apibrėžti administratoriaus teises	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/294491/administrator-profiles	

2.3.98	Kiekviename atskirame įrenginyje turi būti galimybė sukurti įrenginio naudotoją, kuris turėtų tik skaitymo (*angl* . read-only) teises *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekviename atskirame įrenginyje yra galimybė sukurti įrenginio naudotoją, kuris turėtų tik skaitymo (*angl* . read-only) teises	Each individual device must have ability to create user that has read-only access *Functionality can be implemented from a central management system*	Each individual device can create user that has read-only rights.	Kiekviename atskirame įrenginyje yra galimybė sukurti įrenginio naudotoją, kuris turėtų tik skaitymo (*angl* . read-only) teises	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/294491/administrator-profiles	
2.3.99	Kiekvienas atskiras įrenginys turi gebėti detaliai apibrėžti administratoriaus teises keisti sisteminius įrenginio nustatymus; kurti, keisti saugumo ir NAT taisykles; peržiūrėti įvykių žurnalus *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekvienas atskiras įrenginys geba detaliai apibrėžti administratoriaus teises keisti sisteminius įrenginio nustatymus; kurti, keisti saugumo ir NAT taisykles; peržiūrėti įvykių žurnalus	Each individual device must have the ability to specify administrator privileges to change system settings; to create, change security and NAT rules; access to event logs *Functionality can be implemented from a central management system*	Each individual device can specify administrator privileges to change system settings; to create, change security and NAT rules; access to event logs; right to review reports	Kiekvienas atskiras įrenginys geba detaliai apibrėžti administratoriaus teises keisti sisteminius įrenginio nustatymus; kurti, keisti saugumo ir NAT taisykles; peržiūrėti įvykių žurnalus	https://cookbook.fortinet.com/limited-access-administrator-account/index.html	
2.3.100	Kiekvienas atskiras įrenginys turi gebėti persiųsti operacinę sistemą ir konfigūraciją SCP protokolu *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekvienas atskiras įrenginys geba persiųsti operacinę sistemą ir konfigūraciją SCP protokolu	Each individual device must be able to transfer operating system and configuration using the SCP protocol *Functionality can be implemented from a central management system*	Each individual device can transfer operating system and configuration using the SCP protocol.	Kiekvienas atskiras įrenginys geba persiųsti operacinę sistemą ir konfigūraciją SCP protokolu	https://kb.fortinet.com/kb/documentLink.do?externalID=FD43754	
2.3.101	Kiekviename atskirame įrenginyje turi veikti Syslog protokolas *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekviename atskirame įrenginyje veikia Syslog protokolas	Each individual device must be running Syslog protocol *Functionality can be implemented from a central management system*	Each individual device is running Syslog protocol.	Kiekviename atskirame įrenginyje veikia Syslog protokolas	https://kb.fortinet.com/kb/documentLink.do?externalID=FD44614	
2.3.102	Kiekviename atskirame įrenginyje turi veikti SNMPv3 protokolas	Kiekviename atskirame įrenginyje veikia SNMPv3 protokolas	Each individual device must be running SNMPv3 protocol	Each individual device is running SNMPv3 protocol.	Kiekviename atskirame įrenginyje veikia SNMPv3 protokolas	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Monitoring/SNMP.htm	
2.3.103	Kiekviename atskirame įrenginyje turi veikti NTP (versijos 3 ir 4) laiko sinchronizavimo protokolas *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekviename atskirame įrenginyje veikia NTP (versijos 3 ir 4) laiko sinchronizavimo protokolas	Each individual device must have NTP (version 3 and 4) time synchronization protocol *Functionality can be implemented from a central management system*	Each individual device has NTP (version 3 and 4) time synchronization protocol.	Kiekviename atskirame įrenginyje veikia NTP (versijos 3 ir 4) laiko sinchronizavimo protokolas	https://kb.fortinet.com/kb/viewContent.do?externalId=FD33783	
2.3.104	Kiekvienas atskiras įrenginys turi gebėti keisti įvykių, siunčiamų SYSLOG protokolų, formatą *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekvienas atskiras įrenginys geba keisti įvykių, siunčiamų SYSLOG protokolų, formatą	Each individual device must be able to change format of events sent by SYSLOG protocols *Functionality can be implemented from a central management system*	Each individual device can change format of events sent by SYSLOG protocols.	Kiekvienas atskiras įrenginys geba keisti įvykių, siunčiamų SYSLOG protokolų, formatą	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-whats-new/Top-LogReport-cef.htm	
2.3.105	Kiekvienas atskiras įrenginys turi gebėti automatiškai daryti konfigūracijos kopijas *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Kiekvienas atskiras įrenginys geba automatiškai daryti konfigūracijos kopijas	Each individual device must be able to automatically make configuration copies *Functionality can be implemented from a central management system*	Each individual device can automatically make configuration copies.	Kiekvienas atskiras įrenginys geba automatiškai daryti konfigūracijos kopijas	https://kb.fortinet.com/kb/documentLink.do?externalID=FD39818	
2.3.106	Kiekvienas atskiras įrenginys turi gebėti sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis	Įrenginyje yra galimybė sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis	Device must be able to compare current device configuration with previous configurations	Device can compare current device configuration with previous configurations.	Įrenginyje yra galimybė sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/296380/revision	
2.3.107	Kiekvienas atskiras įrenginys turi gebėti aktyvuoti ankstesnę konfigūraciją	Kiekvienas atskiras įrenginys geba aktyvuoti ankstesnę konfigūraciją	Each individual device must be able to use previous configuration	Each individual device can use previous configuration.	Kiekvienas atskiras įrenginys geba aktyvuoti ankstesnę konfigūraciją	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/702257/configuration-backups	

2.3.108	Kiekvienas atskiras įrenginys turi gebėti matyti aktyvius sujungimus (sesijas)	Kiekvienas atskiras įrenginys geba matyti aktyvius sujungimus (sesijas)	Each individual device must be able to see active connections (sessions)	Each individual device can see active connections (sessions).	Kiekvienas atskiras įrenginys geba matyti aktyvius sujungimus (sesijas)	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-fortiview-54/Consoles/All_Sessions.htm	
2.4	**Įrenginių konstrukcijos reikalavimai**		**Equipment design requirements**				
2.4.1	Kiekvieno atskiro įrenginio konstrukcija	Įrenginys montuojamas į 19” komutacinę spintą, pateikiami su montavimo detalėmis	Design of each individual device	Unit is mounted in a 19" rack provided with mounting parts.	*Montuojamas į 19“ spintą*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.4.2	Kiekvieno atskiro įrenginio aukštis	Ne daugiau kaip **3U**	Height of each individual device	No more than **3U.**	*1 U*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.4.3	Įrenginių elektros maitinimas	230V AC	Device power feed	**230V** AC.	*100 - 240V AC*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.4.4	Kiekviename atskirame įrenginyje įdiegtų kintamosios elektros srovės maitinimo šaltinių skaičius *Vienam maitinimo šaltiniui sugedus, įrenginys, nenutraukiant veikimo, turi būti maitinamas iš kito maitinimo šaltinio*	Ne mažiau kaip **2** vnt.	Number of AC power supplies installed on each individual device. If one power supply fails, unit must be powered from another power supply without interruption.	No less than **2**.	Dubliuoti maitinimo šaltiniai. Vienam sugedus įrenginys veikia nenutrūkstamai.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	*5 psl.*
2.4.5	Įrenginio elektros tiekimo šaltiniai turi būti sukomplektuoti su elektros tiekimo prijungimo kabeliais	Įrenginio elektros tiekimo šaltiniai sukomplektuoti su elektros tiekimo prijungimo kabeliais	Power supplies for unit must be complete with power supply cables	Power sources for unit are complete with power supply cables.	Įrenginio elektros tiekimo šaltiniai sukomplektuoti su elektros tiekimo prijungimo kabeliais	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/186de9b7-1a21-11e9-9685-f8bc1258b856/FortiGate-600E-601E-Supplement.pdf	*2 psl.*
2.4.6	Įrenginys turi būti sukomplektuotas su konsolės prijungimo kabeliu	Įrenginys sukomplektuotas su konsolės prijungimo kabeliu	Unit must be equipped with a console connection cable	Unit is equipped with a console connection cable.	Įrenginys sukomplektuotas su konsolės prijungimo kabeliu	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/186de9b7-1a21-11e9-9685-f8bc1258b856/FortiGate-600E-601E-Supplement.pdf	
2.5	**Sistemos bendrieji reikalavimai**		**General system requirements**				
2.5.1	Siūlomi įrenginiai (toliau – įranga) ir jų sudedamosios dalys turi būti nauji ir nenaudoti. *Negalima siūlyti gamykliškai atnaujintos (angl. refurbished) įrangos*	Siūlomi įrenginiai (toliau – įranga) ir jų sudedamosios dalys yra nauji ir nenaudoti	Proposed equipment (hereinafter referred to as "equipment") must be new and unused. *Refurbished equipment may not be offered*	Proposed equipment (hereinafter referred to as "equipment") is new and unused.	Siūlomi įrenginiai (toliau – įranga) ir jų sudedamosios dalys yra nauji ir nenaudoti		
2.5.2	Įrangos dokumentacija anglų kalba turi būti pateikiama gamintojo interneto svetainėje	Įrangos dokumentacija anglų kalba pateikiama gamintojo interneto svetainėje	Equipment documentation in English must be available on the manufacturer's website	Equipment documentation in English is available on the manufacturer's website.	Įrangos dokumentacija anglų kalba pateikiama gamintojo interneto svetainėje	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	
2.5.3	Sistemai turi būti teikiamas techninis aptarnavimas	Sistemai yra teikiamas techninis aptarnavimas	Techical support must be provided to the System	Techical support is provided to the System	Sistemai yra teikiamas techninis aptarnavimas su FG-600E-BDL-950-36		

2.5.4	Įranga turi būti pateikta su licencijomis, leidžiančiomis techninio aptarnavimo laikotarpiu gauti šiuos aprašų atnaujinimus	Aplikacijų protokolų kontrolės (angl. Application Control); įsilaužimų kontrolės (angl. Intrusion Prevention System); virusų, piktybinių programų (angl. Antivirus); Web filtravimo (angl. Web Filtering)	Equipment must be accompanied by licenses to receive these signatures updates during the maintenance period	Application Control; Intrusion Prevention System; Antivirus; Web Filtering	Aplikacijų protokolų kontrolės (angl. Application Control); įsilaužimų kontrolės (angl. Intrusion Prevention System); virusų, piktybinių programų (angl. Antivirus); Web filtravimo (angl. Web Filtering) su FG-600E-BDL-950-36		
2.5.5	Įranga turi gebėti atsisiųsti programinės įrangos atnaujinimus ir pataisymus (*angl* . patch) bei 2.5.4 punkte nurodytus aprašų atnaujinimus iš gamintojo puslapio	Įranga geba atsisiųsti programinės įrangos atnaujinimus ir pataisymus (angl. patch) bei 2.5.4 punkte nurodytus aprašų atnaujinimus iš gamintojo puslapio	Equipment must be able to download software updates, patches and signatures updates referred to clause 2.5.4 from manufacturer's page	Equipment can download software updates, patches and signatures updates referred to clause 2.5.4 from manufacturer's page.	Įranga geba atsisiųsti programinės įrangos atnaujinimus ir pataisymus (angl. patch) bei 2.5.4 punkte nurodytus aprašų atnaujinimus iš gamintojo puslapio	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/817681/fortiguard	
2.5.6	Garantija	Siūlomai įrangai ir visiems pateiktiems techniniams ir programiniams komponentams garantinė priežiūra turi būti atliekama paties įrangos gamintojo arba jo autorizuoto aptarnavimo atstovo. Garantinio aptarnavimo metu turi būti nemokamai atliekami remonto darbai ir nemokamai keičiami sugedę komponentai. Papildomi garantinio remonto ir palaikymo reikalavimai pateikti Techninės specifikacijos 4.12 skyriuje.	Warranty	Offered equipment and all supplied hardware and software components must be under warranty service either by equipment manufacturer or by an authorized service representative. Warranty service must include free repair and replacement of defective components. For additional warranty repair and maintenance requirements, see Section 4.12 of the Technical Specification.	Siūlomai įrangai ir visiems pateiktiems techniniams ir programiniams komponentams garantinė priežiūra turi būti atliekama paties įrangos gamintojo arba jo autorizuoto aptarnavimo atstovo. Garantinio aptarnavimo metu turi būti nemokamai atliekami remonto darbai ir nemokamai keičiami sugedę komponentai. Papildomi garantinio remonto ir palaikymo reikalavimai pateikti Techninės specifikacijos 4.12 skyriuje.		
3.	**Tinklo ugniasienė (toliau - Ugniasienė) / Network Firewall (Furth. - System)**						
3.1	Ugniasienės pavadinimas ir modelis (gamintojo suteiktas numeris (kodas))	Nurodomas ugniasienės pavadinimas ir modelis (gamintojo suteiktas numeris (kodas))	System name and model (manufacturer's identification number (code))	Name and model of system components are provided (manufacturer's identification number (code))	*FortiGate 60F*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	
3.2	Gamintojas (pavadinimas)	Nurodomas ugniasienės gamintojas	Manufacturer (name)	System manufacturer is provided	*Fortinet*		
3.3	**Ugniasienės charakteristikos**		**System characteristics**				
3.3.1	Ugniasienės funkcionalumo aprašymas	Specializuotas identiškai atitinkantis aparatinis–programinis sprendimas, skirtas užtikrinti: vidinio perimetro kontrolę, įsibrovimų aptikimą ir prevenciją, antivirusinę programinę įrangą, srautų turinio kontrolę.	Description of firewall functionality	Specialized identically matching hardware-software solution designed to provide: control of the inner perimeter; intrusion detection and prevention; anti-virus software; controlling the content of streams.	Specializuotas identiškai atitinkantis aparatinis–programinis sprendimas, skirtas užtikrinti: vidinio perimetro kontrolę, įsibrovimų aptikimą ir prevenciją, antivirusinę programinę įrangą, srautų turinio kontrolę.	https://www.fortinet.com/products/next-generation-firewall	
3.3.2	Ugniasienė turi dirbti aukšto patikimumo sistemoje su tokio pat tipo įrenginiais Aktyvus/Pasyvus (*angl* . Active/Passive) ir Aktyvus/Aktyvus (*angl* . Active/Active) režimais	Ugniasienė dirba aukšto patikimumo sistemoje su tokio pat tipo įrenginiais Aktyvus/Pasyvus (*angl* Active/Passive) ir Aktyvus/Aktyvus (*angl* Active/Active) režimais	Firewall must be able to operate in Active / Passive and Active / Active modes	Firewall can operate in Active / Passive and Active / Active modes	Ugniasienė dirba aukšto patikimumo sistemoje su tokio pat tipo įrenginiais Aktyvus/Pasyvus (*angl* . Active/Passive) ir Aktyvus/Aktyvus (*angl* . Active/Active) režimais	https://docs.fortinet.com/document/fortigate/6.4.6/administration-guide/062403/introduction-to-the-fgcp-cluster	
3.3.3	Ugniasienei dirbant aukšto patikimumo sistemoje turi galioti lentelės 1.3.3-1.3.9 ir 2.3.3-2.3.9 punktuose nurodyti reikalavimai	Ugniasienei dirbant aukšto patikimumo sistemoje galioja lentelės 1.3.3-1.3.9 ir 2.3.3-2.3.9 punktuose nurodyti reikalavimai	When firewall is operating in a high-reliability system, requirements specified in items 1.3.3-1.3.9 and 2.3.3-2.3.9 of the table must apply.	When firewall is operating in a high-reliability system, requirements specified in items 1.3.3-1.3.9 and 2.3.3-2.3.9 of the table applies.	*Žiūrėti lentelės 1.3.3-1.3.9 ir 2.3.3-2.3.9 punktus*	*Žiūrėti lentelės 1.3.3-1.3.9 ir 2.3.3-2.3.9 punktus*	*Žiūrėti lentelės 1.3.3-1.3.9 ir 2.3.3-2.3.9 punktus*
3.3.4	Ugniasienėje įdiegtų 10/100/1000Base-T prievadų su automatiniu greitaveikos parinkimu skaičius	Ne mažiau kaip **5**	Number of 10/100 / 1000Base-T ports with automatic speed selection installed in the System	No less than **5**	*10*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	*5 psl.*
3.3.5	Ugniasienėje įdiegtų papildomų konsolės (*angl* Console) prievadų skaičius	Ne mažiau kaip **1**	Number of console ports installed on device	No less than **1**	*1*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	*5 psl.*

3.3.6	Ugniasienėje įdiegtų USB prievadų skaičius	Ne mažiau kaip **1**	Number of USB ports installed in the system	No less than **1**	*1*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	*5 psl.*
3.3.7	Ugniasienės pralaidumas (angl. Firewall throughput), esant Enterprise mix tipo duomenų srautui arba esant UDP1518 srautui	Ne mažesnė kaip **1,6** Gbps, esant Enterprise mix tipo duomenų srautui, arba ne mažesnė kaip **4** Gbps, esant UDP1518 srautui	Firewall throughput of the firewall device with Enterprise mix type traffic or UDP1518 traffic	At least **1,6 Gbps** for Enterprise mix data traffic or at least **4 Gbps** for UDP1518 traffic	*10 Gbps UDP 1518*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	*5 psl.*
3.3.8	Ugniasienės, naudojant programų protokolų kontrolę (angl. Application control) ir apsaugą nuo įsibrovimų (angl. Intrusion prevension system IPS), apsaugą nuo virusų, URL filtravimą, Anti-Bot apsaugą greitaveika, esant Enterprise mix tipo arba HTTP 21kB duomenų srautui	Ne mažesnė kaip **700** Mbps	Throughput of the firewall while using Application control, Intrusion prevention, virus protection, URL filtering, Anti-Bot protection for Enterprise mix or HTTP 21 kB traffic	No less than **700** Mbps	*700 Mbps*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	*5 psl.*
3.3.9	Ugniasienės IPSEC VPN greitaveika, esant idialiomis testavimo sąlygoms	Ne mažesnė kaip **1,2** Gbps	IPSEC VPN performance of each individual device under ideal test conditions	No less than **1,2** Gbps	*6,5 Gbps*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	*5 psl.*
3.3.10	Ugniasienėje veikiančių konkurentinių sesijų skaičius, esant idialiomis testavimo sąlygoms	Ne mažiau kaip **125000**	Number of concurrent sessions running on the device under ideal test conditions	No less than **125000**	*700 000*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	*5 psl.*
3.3.11	Ugniasienė turi palaikyti naujų sesijų per sekundę, esant idialiomis testavimo sąlygoms	Ne mažiau kaip **8000**	System must support new sessions per second under ideal test conditions	No less than **8000**	*35 000*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	*5 psl.*
3.3.12	Ugniasienėje veikiančių vienu metu virtualių tinklų (VLAN) skaičius	Ne mažiau kaip **300**	Number of concurrent virtual networks (VLANs) running on the device	No less than **300**	*4094*	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-system-administration-	
3.3.13	Ugniasienės vartotojų skaičius neribojamas	Ugniasienės vartotojų skaičius neribojamas	There must be no limit to the number of users per firewall	There is no limit to the number of users per firewall	Ugniasienės vartotojų skaičius neribojamas	https://help.fortinet.com/cli/fos60hlp/60/Content/FortiOS/fortiOS-cli-ref/config/system/resource-limits.htm	
3.3.14	Ugniasienė turi veikti tokiais režimais	Skaidrus (*angl* . transparent); maršrutizavimo (angl. routing).	Firewall must operate in these modes:	Transparent; Routing.	Skaidrus (*angl* . transparent); maršrutizavimo (angl. routing).	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-getting-started-54/2-Installation/2-NAT-Route-vs-Transparent.htm	
3.3.15	Ugniasienėje turi veikti apsauga nuo DoS atakų.	Ugniasienėje veikia apsauga nuo DoS atakų.	Firewall must have ability to enable DoS attack protection.	Firewall has ability to enable DoS attack protection.	Ugniasienėje veikia apsauga nuo DoS atakų.	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Inside%20FortiOS%20DoS%20Protection.htm	

3.3.16	Ugniasienėje turi veikti loginio grupavimo protokolą *Turi būti galimybė apjungti į vieną loginį tinklo prievadą nemažiau kaip 8 fizines prievadus. Loginis prievadas gali būti naudojamas kaip L2 arba L3 lygio prievadas*	IEEE 802.3ad arba lygiavertį	Firewall must run a logical grouping protocol *It must be possible to connect at least 8 physical ports to a single logical network port. Logical port can be used as an L2 or L3 level port*	IEEE 802.3ad or equivalent.	IEEE 802.3ad arba lygiavertį	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-networking-54/Interfaces/Aggregate%20Interfaces.htm	
3.3.17	Ugniasienė turi palaikyti VLAN žymėjimo (*angl* . tagging) protokolą *VLAN prievadai gali būti kuriamos tinklo prievadams, veikiantiems L2 ir L3 lygyje*	IEEE 802.1q arba lygiavertį	Firewall must support VLAN tagging protocol *VLAN ports can be created for network ports operating at the L2 and L3 levels*	IEEE 802.1q or equivalent.	IEEE 802.1q arba lygiavertį	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-system-administration-52/VLANs/VLANs.htm	
3.3.18	Ugniasienėje turi veikti vidinio DHCP serverio funkcija	Ugniasienėje veikia vidinio DHCP serverio funkcija	It must be possible to configure internal DHCP server on the device	It is possible to configure internal DHCP server on the device.	Ugniasienėje veikia vidinio DHCP serverio funkcija	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Advanced/DHCP%20servers%20and%20relays.htm	
3.3.19	Ugniasienėje turi būti palaikoma DHCP Relay funkcija	Ugniasienėje yra palaikoma DHCP Relay funkcija	DHCP Relay function must be supported on the device	DHCP Relay function is supported on the device.	Ugniasienėje yra palaikoma DHCP Relay funkcija	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Advanced/DHCP%20servers%20and%20relays.htm	
3.3.20	Ugniasienėje turi veikti DHCP ir PPPoE klientai	Ugniasienėje veikia DHCP ir PPPoE klientus	It must be possible to configure DHCP or PPPoE clients on the device	It is possible to configure DHCP or PPPoE clients on the device.	Ugniasienėje veikia DHCP ir PPPoE klientus	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-networking-54/Interfaces/PPPoE%C2%A0%20addressing%20mode%20on%20an%20interface.htm	
3.3.21	Ugniasienėje turi veikti dinaminio maršrutizavimo protokolai	Statiniai maršrutai (*angl* . static routes); BGPv4; OSPFv2; OSPFv3.	Dynamic routing protocols must be running on the firewall	Static routes; BGPv4; OSPFv2; OSPFv3.	Statiniai maršrutai (*angl* . static routes); BGPv4; OSPFv2; OSPFv3.	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-advanced-routing-52/Routing_Dynamic/Comparison_Protocols.htm	
3.3.22	Ugniasienėje turi veikti grakštus BGP ir OSPF perkrovimas (*angl* . graceful restart).	Ugniasienėje veikia grakštus BGP ir OSPF perkrovimas (*angl* . graceful restart).	Firewall must be able to perform graceful restart for BGP and OSPF.	Firewall is able to perform graceful restart for BGP and OSPF.	Ugniasienėje veikia grakštus BGP ir OSPF perkrovimas (*angl* . graceful restart).	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverGraceful.htm	
3.3.23	Ugniasienėje turi veikti Multicast protokolai	IGMP (versijos 2 ir 3), IGMP proxy arba lygiavertis; PIM-SM arba lygiavertis; PIM-SSM arba lygiavertis	Multicast protocol must be working on the firewall	IGMP (version 2 and 3), IGMP proxy or equivalent; PIM-SM or equivalent; PIM-SSM or equivalent.	IGMP (versijos 2 ir 3), IGMP proxy arba lygiavertis; PIM-SM arba lygiavertis; PIM-SSM arba lygiavertis	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/741750/router-multicast	
3.3.24	Ugniasienėje turi veikti politika pagrįstą maršrutizavimas (*angl* . Policy based routing) atsižvelgiant į šaltinio/paskirties zoną, siuntėjo, gavėjo IP adresą, servisą	Ugniasienė veikia politika pagrįstą maršrutizavimas (*angl* . Policy based routing) atsižvelgiant į šaltinio/paskirties zoną, siuntėjo, gavėjo IP adresą, servisą	Firewall must be able to configure Policy Based Routing based on source/destination area, sender, recipient IP address, service.	Firewall can configure Policy Based Routing based on source/destination area, sender, recipient IP address, service.	Ugniasienė veikia politika pagrįstą maršrutizavimas (*angl* . Policy based routing) atsižvelgiant į šaltinio/paskirties zoną, siuntėjo, gavėjo IP adresą, servisą	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-advanced-routing-54/Routing_Advanced_Static/Policy_Routing.htm	

3.3.25	Ugniasienė turi palaikyti IPv6 protokolą	Ugniasienė palaiko IPv6 protokolą	Firewall must support IPv6 protocol	Firewall supports IPv6 protocol.	Ugniasienė palaiko IPv6 protokolą	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/IPv6%20in%20FortiOS.htm	
3.3.26	Ugniasienėje turi veikti BFD (Bidirectional Forwarding Detection) arba lygiavertis funckionalumas	Ugniasienė veikia BFD (Bidirectional Forwarding Detection) arba lygiavertis funckionalumas	Firewall must support BFD (Bidirectional Forwarding Detection) or equal functionality	Firewall supports BFD (Bidirectional Forwarding Detection) or equal functionality.	Ugniasienė veikia BFD (Bidirectional Forwarding Detection) arba lygiavertis funckionalumas	https://kb.fortinet.com/kb/documentLink.do?externalID=FD30260	
3.3.27	Ugniasienėje turi veikti adresų transliavimas (*angl* . NAT)	statinis adresų transliavimas (*angl* . Static NAT); šaltinio adreso transliavimas su portų adresų transliavimu (PAT); paskirties adreso transliavimas su portų adresų transliavimu (PAT).	Firewall must have Network Address Translation (NAT)	Static NAT; source address translation with port address translation (PAT); destination address translation with port address translation (PAT).	statinis adresų transliavimas (*angl* . Static NAT); šaltinio adreso transliavimas su portų adresų transliavimu (PAT); paskirties adreso transliavimas su portų adresų transliavimu (PAT).	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Dynamic%20NAT.htm	
3.3.28	Ugniasienėje turi veikti adresų transliavimas tarp IPv6 ir IPv4 protokolų	Ugniasienėje veikia adresų transliavimas tarp IPv6 ir IPv4 protokolų	Address translation between IPv6 and IPv4 protocols must be working on the device	Address translation between IPv6 and IPv4 protocols is working on the device.	Ugniasienėje veikia adresų transliavimas tarp IPv6 ir IPv4 protokolų	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-firewall-52/Concepts/NAT%2064%20and%20NAT46.htm	
3.3.29	Ugniasienė turi gebėti saugoti nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos)	Ugniasienė geba saugoti nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos)	Firewall must be able to protect against attacks, malicious code (eg viruses, spyware)	Firewall is able to protect against attacks, malicious code (eg viruses, spyware)	Ugniasienė geba saugoti nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos)	https://www.fortiguard.com/learnmore#av	
3.3.30	Ugniasienė turi gebėti, nustačius grėsmę, automatiškai įrašyti paketus, susijusius su grėsme	Ugniasienė geba, nustačius grėsmę, automatiškai įrašyti paketus, susijusius su grėsme	Firewall must have capability to automatically record threat-related packets upon detection	Firewall has capability to automatically record threat-related packets upon detection	Ugniasienė geba, nustačius grėsmę, automatiškai įrašyti paketus, susijusius su grėsme	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Enable%20IPS%20packet%20logging.htm	
3.3.31	Ugniasienė turi atpažinti ir kontroliuoti aplikacijas (protokolus) *Tos pačios aplikacijos skirtingos versijos skaičiuojamos kaip viena aplikacija*	Ne mažiau kaip **3000**	Firewall must recognize and control applications (protocols) *Different versions of the same application are counted as one application*	No less than **3000**	*Daugiau kaip 4000*	https://fortiguard.com/learnmore#ac	
3.3.32	Ugniasienė turi būti gebėti apsirašyti savo aplikaciją	Ugniasienė geba apsirašyti savo aplikaciją	Firewall must be able to write down its application	Firewall can write down its application	Ugniasienė geba apsirašyti savo aplikaciją	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20Application%20&%20IPS%20Signatures.htm	
3.3.33	Ugniasienė turi gebėti kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma	Ugniasienė geba kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma	Firewall must be able to set individual time for each application after which inactive session is closed	Firewall can set individual time for each application after which inactive session is closed	Ugniasienė geba kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma	https://help.fortinet.com/cli/fos50hlp/56/Content/FortiOS/fortiOS-cli-ref-56/config/application/list.htm	
3.3.34	Ugniasienė turi gebėti kurti saugumo taisykles, kurios leistų vartotojams jungtis tik prie tam tikros aplikacijos ar aplikacijų grupės, nenurodant serviso/prievado, kuriuo dirba aplikacija, t. y. vartotojas gali prisijungti prie nurodytos aplikacijos nepriklausomai nuo to kokį servisą/prievadą naudoja aplikacija	Ugniasienė geba kurti saugumo taisykles, kurios leistų vartotojams jungtis tik prie tam tikros aplikacijos ar aplikacijų grupės, nenurodant serviso/prievado, kuriuo dirba aplikacija, t. y. vartotojas gali prisijungti prie nurodytos aplikacijos nepriklausomai nuo to kokį servisą/prievadą naudoja aplikacija	Firewall must have the ability to create security rules that allow users to connect only to a specific application or group of applications without specifying service/port application is running on, i.e. user can connect to specified application regardless of which service/port application uses	Firewall can create security rules that allow users to connect only to a specific application or group of applications without specifying service/port application is running on, i.e. user can connect to specified application regardless of which service/port application uses.	Ugniasienė geba kurti saugumo taisykles, kurios leistų vartotojams jungtis tik prie tam tikros aplikacijos ar aplikacijų grupės, nenurodant serviso/prievado, kuriuo dirba aplikacija, t. y. vartotojas gali prisijungti prie nurodytos aplikacijos nepriklausomai nuo to kokį servisą/prievadą naudoja aplikacija	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20Application%20&%20IPS%20Signatures.htm	

3.3.35	Ugniasienė turi gebėti riboti prisijungimų iš vieno šaltinio skaičių pagal	siuntėjo IP; gavėjo IP; siuntėjo ir gavėjo IP	Firewall must have ability to limit number of connections based on provided criteria:	Source IP; Destination IP; Source and Destination IP.	siuntėjo IP; gavėjo IP; siuntėjo ir gavėjo IP	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Security%20Policies/Firewall%20policies.htm	
3.3.36	Ugniasienė, kuriant ugniasienės saugumo taisykles, turi gebėti nurodyti siuntėją, gavėją, servisą/prievadą, aplikaciją, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Servisai/prievadai ir aplikacijos taisyklėse turi būti nurodomi atskiruose laukuose	Ugniasienė, kuriant ugniasienės saugumo taisykles, geba nurodyti siuntėją, gavėją, servisą/prievadą, aplikaciją, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Servisai/prievadai ir aplikacijos taisyklėse yra nurodomi atskiruose laukuose	Firewall must have ability to specify source, destination, service/port, application, applicable security measures, user, user group when creating firewall rules. Services/ports and applications rules must be referenced in separate fields.	Firewall has ability to specify source, destination, service/port, application, applicable security measures, user, user group when creating firewall rules. Services/ports and applications rules must be referenced in separate fields.	Ugniasienė, kuriant ugniasienės saugumo taisykles, geba nurodyti siuntėją, gavėją, servisą/prievadą, aplikaciją, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Servisai/prievadai ir aplikacijos taisyklėse yra nurodomi atskiruose laukuose	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Security%20Policies/Firewall%20policies.htm	
3.3.37	Ugniasienė turi gebėti skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones	Ugniasienė geba skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones	Firewall must have ability to use different security measures for different data traffic.	Firewall has ability to use different security measures for different data traffic.	Ugniasienė geba skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones	https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/853759	
3.3.38	Ugniasienė pagal nutylėjimą turi blokuoti visas aplikacijas išskyrus tas, kurios yra apibrėžtos saugumo taisyklėse kaip leistinos	Ugniasienė pagal nutylėjimą blokuoja visas aplikacijas išskyrus tas, kurios yra apibrėžtos saugumo taisyklėse kaip leistinos	By default, firewall must block all applications except those defined in the firewall rules as allowed	By default, firewall is blocking all applications except those defined in the firewall rules as allowed.	Ugniasienė pagal nutylėjimą blokuoja visas aplikacijas išskyrus tas, kurios yra apibrėžtos saugumo taisyklėse kaip leistinos	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Security%20Policies/Firewall%20policies.htm	
3.3.39	Ugniasienė turi gebėti suteikti vartotojams prieigą prie aplikacijos/ų (ne serviso/prievado) nepriklausomai nuo to kokiais TCP, UDP prievadais dirba aplikacija	Ugniasienė geba suteikti vartotojams prieigą prie aplikacijos/ų (ne serviso/prievado) nepriklausomai nuo to kokiais TCP, UDP prievadais dirba aplikacija	Firewall must be able to provide users with access to the application(s) (not service/port), regardless of which TCP, UDP ports the application is running on	Firewall can provide users with access to the application(s) (not service/port), regardless of which TCP, UDP ports the application is running on.	Ugniasienė geba suteikti vartotojams prieigą prie aplikacijos/ų (ne serviso/prievado) nepriklausomai nuo to kokiais TCP, UDP prievadais dirba aplikacija	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Application_Control/Application%20Control%20Concepts.htm	
3.3.40	Ugniasienė turi gebėti nurodyti prie kokių aplikacijų vartotojui leidžiama jungtis, o prie kokių neleidžiama, net jei aplikacijos dirba tais pačiais TCP, UDP prievadais	Ugniasienė geba nurodyti prie kokių aplikacijų vartotojui leidžiama jungtis, o prie kokių neleidžiama, net jei aplikacijos dirba tais pačiais TCP, UDP prievadais	Firewall must be able to specify which applications user can connect to and which ones cannot, even if applications are running on the same TCP, UDP ports	Firewall can specify which applications user can connect to and which ones cannot, even if applications are running on the same TCP, UDP ports	Ugniasienė geba nurodyti prie kokių aplikacijų vartotojui leidžiama jungtis, o prie kokių neleidžiama, net jei aplikacijos dirba tais pačiais TCP, UDP prievadais	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-profiles/Application_Control/Enable%20Application%20Control.htm	
3.3.41	Ugniasienė turi gebėti suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta	Ugniasienė geba suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta	Firewall must be able to grant access rights only to authenticated users	Firewall is able to grant access rights only to authenticated users	Ugniasienė geba suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Auth_Intro.htm	
3.3.42	Ugniasienė turi gebėti dinamiškai susieti IP adresą su vartotojų	Ugniasienė geba dinamiškai susieti IP adresą su vartotojų	Firewall must be able to dynamically associate an IP address with user	Firewall can dynamically associate an IP address with user	Ugniasienė geba dinamiškai susieti IP adresą su vartotojų	https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/374938/setting-up-your-fortigate-for-fsso	
3.3.43	Ugniasienė turi gebėti suteikti prieigos teises vartotojams, ir/arba vartotojų grupėms.	Ugniasienė geba suteikti prieigos teises vartotojams, ir/arba vartotojų grupėms.	Firewall must be able to grant access rights to users and/or user groups.	Firewall has the ability to grant access rights to users and/or user groups.	Ugniasienė geba suteikti prieigos teises vartotojams, ir/arba vartotojų grupėms.	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/Security%20Policies/Firewall%20policies.htm	

3.3.44	Ugniasienė turi gebėti nustatyti vartotojų tapatybę, neprašydamas suvesti vartotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz. Active Directory	Ugniasienė geba nustatyti vartotojų tapatybę, neprašydamas suvesti vartotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz. Active Directory	Firewall must be able to authenticate users without having to enter their username and password but using existing network services eg Active Directory	Firewall can authenticate users without having to enter their username and password but using existing network services eg Active Directory.	Ugniasienė geba nustatyti vartotojų tapatybę, neprašydamas suvesti vartotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz. Active Directory	https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/374938/setting-up-your-fortigate-for-fsso	
3.3.45	Ugniasienė turi būti integruojama su Active Directory, LDAP, RADIUS	Ugniasienė yra integruojama su Active Directory, LDAP, RADIUS	Firewall must be integrated with Active Directory, LDAP, RADIUS	Firewall is integrated with Active Directory, LDAP, RADIUS	Ugniasienė yra integruojama su Active Directory, LDAP, RADIUS	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Servers.htm	
3.3.46	Ugniasienė turi sinchronizuoti vartotojų-ID ir jų IP adresų informaciją. Informacija turi būti renkama tiesiogiai arba per papildomus agentus iš: •Active Directory domain servisų, •Radius accounting šaltinių, •terminalinių serverių. Turi būti papildoma galimybė surinkti informaciją iš Syslog šaltinių tiesiogiai arba naudojant papildomą programinę įrangą, kuri nėra įtraukiama į pasiūlymą. *Vartotojų ID ir IP adresų sinchronizacijai negali būti instaliuojami papildomi agentai klientų kompiuteriuose.* *Šis reikalavimas gali būti įgyvendintas lygiaverčiu funkcionalumu ar pateikiamais sprendimais, kurie nenaudojant papildomų agentų klientų kompiuteriuose sinchronizuotų vartotojų-ID ir jų IP adresų informaciją su Užsakovo turima ir naudojama sistema Aruba ClearPass ir terminaliniuose serveriuose*	Ugniasienė sinchronizuoja vartotojų-ID ir jų IP adresų informaciją. Informacija turi būti renkama tiesiogiai arba per papildomus agentus iš: •Active Directory domain servisų, •Radius accounting šaltinių, •terminalinių serverių. Turi būti papildoma galimybė surinkti informaciją iš Syslog šaltinių tiesiogiai arba naudojant papildomą programinę įrangą, kuri nėra įtraukiama į pasiūlymą.	Firewall must synchronize user IDs and their IP address information. The information must be collected directly or through additional agents from: • Active Directory domain services, • Radius accounting sources • terminal servers. There must be an additional ability to collect information from Syslog sources directly or through the use of additional software that is not included in the offer. *Additional agents cannot be installed on client computers to synchronize user IDs and IP addresses.* *This requirement can be implemented with equivalent functionality or provided solutions that, without the use of additional agents, synchronize user IDs and their IP addresses on client computers with system owned and operated by Customer Aruba ClearPass and termianl servers*	Firewall synchronizes user IDs and their IP address information. The information must be collected directly or through additional agents from: • Active Directory domain services, • Radius accounting sources • terminal servers. There must be an additional ability to collect information from Syslog sources directly or through the use of additional software that is not included in the offer.	Ugniasienė sinchronizuoja vartotojų-ID ir jų IP adresų informaciją. Informacija turi būti renkama tiesiogiai arba per papildomus agentus iš: •Active Directory domain servisų, •Radius accounting šaltinių, •terminalinių serverių. Turi būti papildoma galimybė surinkti informaciją iš Syslog šaltinių tiesiogiai arba naudojant papildomą programinę įrangą, kuri nėra įtraukiama į pasiūlymą.	*https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso* *https://docs.fortinet.com/document/fortigate/6.0.0/handbook/658099/single-sign-on-to-windows-ad* *https://docs.fortinet.com/document/fortigate/6.0.0/handbook/372705/sso-using-radius-accounting-records* *https://docs.fortinet.com/document/fortimanager/6.2.1/new-features/733863/clearpass-sso-identity-connector*	
3.3.47	Ugniasienėje vartotojų identifikacijai turi būti palaikomas IPv6 protokolas	Ugniasienėje vartotojų identifikacijai yra palaikomas IPv6 protokolas	Firewall must support IPv6 for user identification	Firewall has a supported IPv6 protocol for user identification.	Ugniasienėje vartotojų identifikacijai yra palaikomas IPv6 protokolas	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-firewall/IPv6/IPv6%20Features/IPv6%20support%20for%20FSSO.htm	
3.3.48	Jei vartotojo tapatybė nebuvo nustatyta skaidriai, vartotojui turi būti parodomas puslapis, kuriame jis turi įvesti tapatybę patvirtinančius duomenis	Jei vartotojo tapatybė nebuvo nustatyta skaidriai, vartotojui turi būti parodomas puslapis, kuriame jis turi įvesti tapatybę patvirtinančius duomenis	If user has not been authenticated in a transparent manner, user must be shown a page where he/she must enter his/her identity details	If user has not been authenticated in a transparent manner, the user is shown a page where he/she must enter his/her identity details.	Jei vartotojo tapatybė nebuvo nustatyta skaidriai, vartotojui turi būti parodomas puslapis, kuriame jis turi įvesti tapatybę patvirtinančius duomenis	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/CaptivePortals.htm	
3.3.49	Ugniasienė turi gebėti kontroliuoti vartotojų, dirbančių terminalinėje aplinkoje (pvz.: Windows Terminal Server) prieigos teises. Įrenginys turi skirti terminalinėje aplinkoje dirbančių vartotojų duomenų srautus ir kontroliuoti kiekvieno vartotojo prieigos teises	Ugniasienė geba kontroliuoti vartotojų, dirbančių terminalinėje aplinkoje (pvz.: Windows Terminal Server) prieigos teises. Įrenginys turi skiria terminalinėje aplinkoje dirbančių vartotojų duomenų srautus ir kontroliuoti kiekvieno vartotojo prieigos teises	Firewall must be able to control access rights of users working in terminal environment (ex. Windows Terminal Server). Device must allocate data flows to users in terminal environment and control access rights for each user	Firewall can control access rights of users working in terminal environment (ex. Windows Terminal Server). Device must allocate data flows to users in terminal environment and control access rights for each user.	Ugniasienė geba kontroliuoti vartotojų, dirbančių terminalinėje aplinkoje (pvz.: Windows Terminal Server) prieigos teises. Įrenginys turi skiria terminalinėje aplinkoje dirbančių vartotojų duomenų srautus ir kontroliuoti kiekvieno vartotojo prieigos teises	https://kb.fortinet.com/kb/viewContent.do?externalId=FD35372	
3.3.50	Ugniasienė turi palaikyti vartotojų tapatybės nustatymą naudojant vartotojo skaitmeninį sertifikatą. Nustatant vartotojo tapatybę, turi būti galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse	Ugniasienė palaiko vartotojų tapatybės nustatymą naudojant vartotojo skaitmeninį sertifikatą. Nustatant vartotojo tapatybę, yra galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse	Firewall must support user authentication with user's digital certificate. When identifying a user, it must be possible to search user's data on multiple authentication servers	Firewall supports user authentication with user's digital certificate. When identifying a user, it is possible to search user's data on multiple authentication servers.	Ugniasienė palaiko vartotojų tapatybės nustatymą naudojant vartotojo skaitmeninį sertifikatą. Nustatant vartotojo tapatybę, yra galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Certificates.htm	

3.3.51	Ugniasienė turi dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą	Kiekvienas atskiras įrenginys dešifruoja ir tikrina įeinantį ir išeinantį SSL duomenų srautą	Firewall must decrypt and verify incoming and outgoing SSL traffic	Firewall decrypts and verifies incoming and outgoing SSL traffic.	Kiekvienas atskiras įrenginys dešifruoja ir tikrina įeinantį ir išeinantį SSL duomenų srautą	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122078/deep-inspection	
3.3.52	Ugniasienėje turi būti pasirinktinai nurodoma, kurį duomenų srautą dešifruoti	Ugniasienėje yra pasirinktinai nurodoma, kurį duomenų srautą dešifruoti	Firewall must be able to specify which data stream to decrypt	Firewall has option of specifying which data stream to decrypt.	Ugniasienėje yra pasirinktinai nurodoma, kurį duomenų srautą dešifruoti	https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/853759	
3.3.53	Ugniasienėje SSL patikra turi būti atliekama visam SSL duomenų srautui, ne tik HTTPS, SMTPS, POP3S, IMAPS protokolams	Ugniasienėje SSL patikra atliekama visam SSL duomenų srautui, ne tik HTTPS, SMTPS, POP3S, IMAPS protokolams	SSL verification must be performed on the firewall for all SSL traffic, not just HTTPS, SMTPS, POP3S, IMAPS protocols	SSL verification is performed on the firewall for all SSL traffic, not just HTTPS, SMTPS, POP3S, IMAPS protocols.	Ugniasienėje SSL patikra atliekama visam SSL duomenų srautui, ne tik HTTPS, SMTPS, POP3S, IMAPS protokolams	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122078/deep-inspection	
3.3.54	Ugniasienėje SSL patikra turi apimti įsilaužimų, pažeidžiamumų aptikimą ir prevenciją, apsaugą nuo virusų, šnipinėjimo aplikacijų, perduodamų failų kontrolę, perduodamų duomenų turinio kontrolę, URL filtravimą	Ugniasienėje SSL patikra apima įsilaužimų, pažeidžiamumų aptikimą ir prevenciją, apsaugą nuo virusų, šnipinėjimo aplikacijų, perduodamų failų kontrolę, perduodamų duomenų turinio kontrolę, URL filtravimą	SSL verification on the firewall must include detection and prevention of hacking, vulnerabilities, virus protection, spyware, file transfer control, data transfer control, URL filtering	SSL verification on the firewall includes detection and prevention of hacking, vulnerabilities, virus protection, spyware, file transfer control, data transfer control, URL filtering.	Ugniasienėje SSL patikra apima įsilaužimų, pažeidžiamumų aptikimą ir prevenciją, apsaugą nuo virusų, šnipinėjimo aplikacijų, perduodamų failų kontrolę, perduodamų duomenų turinio kontrolę, URL filtravimą	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-security-profiles/SSL_SSH_Inspection/why_use_ssl_inspection.htm	
3.3.55	Ugniasienė turi dešifruoti TLS1.2 duomenų srautą	Ugniasienė dešifruoja TLS1.2 duomenų srautą	Firewall must decrypt TLS1.2 data stream	Firewall decrypts TLS1.2 data stream.	Ugniasienė dešifruoja TLS1.2 duomenų srautą	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-load-balancing/ldb-ssl-tls-version.htm	
3.3.56	Ugniasienė turi inspektuoti TLS1.3 duomenų srautą, atpažinti aplikacijas ir svetaines naudojančias TLS1.3	Ugniasienė inspektuoja TLS1.3 duomenų srautą, atpažįsta aplikacijas ir svetaines naudojančias TLS1.3	Firewall must inspect TLS1.3 traffic, recognize applications and sites using TLS1.3	Firewall inspects TLS1.3 traffic, recognize applications and sites using TLS1.3	Ugniasienė inspektuoja TLS1.3 duomenų srautą, atpažįsta aplikacijas ir svetaines naudojančias TLS1.3	https://docs.fortinet.com/document/fortigate/6.2.0/new-features/35927/tls-1-3-support	
3.3.57	Ugniasienė turi riboti prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus	Ugniasienė riboja prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus	Firewall must be able to limit number of connections based on source, destination IP addresses, services, users	Firewall can limit number of connections based on source, destination IP addresses, services, users.	Ugniasienė riboja prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/885253/per-ip-traffic-shaper	
3.3.58	Ugniasienė turi gebėti kurti savo įsilaužimų aprašus	Ugniasienė geba kurti savo įsilaužimų aprašus	Firewall must be able to create its own intrusion profiles	Firewall is able to create its own intrusion profiles	Ugniasienė geba kurti savo įsilaužimų aprašus	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20signature%20keywords.htm	
3.3.59	Ugniasienė turi gebėti atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę	Ugniasienė geba atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę	Firewall must be able to control access to web resources using a manufacturer-provided URL database	Firewall can control access to web resources using the URL database provided by the manufacturer	Ugniasienė geba atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-profiles/Web_Filter/FortiGuard%20Web%20Filtering%20Service.htm	
3.3.60	Ugniasienė turi gebėti sukurti leistinų ir draudžiamų URL ir IP sąrašus	Ugniasienėje yra galimybė sukurti leistinų ir draudžiamų URL ir IP sąrašus	Firewall must be able to create lists of allowed and prohibited URLs and IPs	Firewall can create lists of allowed and blocked URLs and IPs.	Ugniasienėje yra galimybė sukurti leistinų ir draudžiamų URL ir IP sąrašus	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-profiles/Web_Filter/Static%20URL%20Filter.htm	
3.3.61	Ugniasienė turi gebėti sukurti ir naudoti savo URL grupes	Ugniasienė geba sukurti ir naudoti savo URL grupes	Firewall must be able to create and use its own URL groups	Firewall can create and use its own URL groups.	Ugniasienė geba sukurti ir naudoti savo URL grupes	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Web_Filter/Configuring%20Web%20Filter%20Profiles.htm	

3.3.62	Ugniasienė turi gebėti kurti pažeidžiamumų aprašus	Ugniasienė geba kurti pažeidžiamumų aprašus	Firewall must be able to create vulnerability profiles	Firewall can create vulnerability profiles.	Ugniasienė geba kurti pažeidžiamumų aprašus	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20signature%20keywords.htm	
3.3.63	Ugniasienė turi aptikti ir blokuoti Botnet	Ugniasienė aptinka ir blokuoja Botnet	Firewall must be able to detect Botnet	Firewall can detect Botnet.	Ugniasienė aptinka ir blokuoja Botnet	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/105208/botnet-c-c-domain-blocking	
3.3.64	Ugniasienė turi palaikyti šifravimo algoritmus	3DES; AES128; AES256	Firewall must support provided encryption protocols:	3DES; AES128; AES256.	3DES; AES128; AES256	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Concepts/Encryption.htm	
3.3.65	Ugniasienė turi palaikyti saugios maišos algoritmus	SHA-1; SHA-256; SHA-384.	Firewall must support provided secure hash algorithms:	SHA-1; SHA-256; SHA-384.	SHA-1; SHA-256; SHA-384.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/238852/encryption-algorithms	
3.3.66	Ugniasienė turi gebėti siųsti IPv6 duomenų srautą per sukurtą IPSec tunelį tarp skirtingų gamintojo įrenginių	Ugniasienė geba siųsti IPv6 duomenų srautą per sukurtą IPSec tunelį tarp skirtingų gamintojo įrenginių	Firewall must be able to send IPv6 data traffic via IPSec tunnel between different manufacturer's devices	Firewall can send IPv6 data traffic via IPSec tunnel between different manufacturer's devices.	Ugniasienė geba siųsti IPv6 duomenų srautą per sukurtą IPSec tunelį tarp skirtingų gamintojo įrenginių	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-IPv6-54/IPv6%20Configuration/IPv6_IPsec_VPN.htm	
3.3.67	Ugniasienė turi palaikyti duomenų srautų ribojimą pagal taikomąją programinę įrangą, vartotoją, siuntėjo, gavėjo IP adresus, tinklo sąsajas	Ugniasienė palaiko duomenų srautų ribojimą pagal taikomąją programinę įrangą, vartotoją, siuntėjo, gavėjo IP adresus, tinklo sąsajas	Firewall must be able to support data flow restrictions depending on application software, user, source, destination IP addresses, network interface.	Firewall can support data flow restrictions depending on application software, user, source, destination IP addresses, network interface.	Ugniasienė palaiko duomenų srautų ribojimą pagal taikomąją programinę įrangą, vartotoją, siuntėjo, gavėjo IP adresus, tinklo sąsajas	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-profiles/Application_Control/Enable-Application-Control-NGFW-Policy-Based.htm	
3.3.68	Ugniasienė turi gebėti suteikti prioritetus duomenų paketams	Ugniasienė geba suteikti prioritetus duomenų paketams	Firewall must be able to give priority to data packets	Firewall can give priority to data packets.	Ugniasienė geba suteikti prioritetus duomenų paketams	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-traffic-shaping-54/TS_Configuration/TS_Configuring.htm	
3.3.69	Ugniasienė turi gebėti pasirinktam duomenų srautui nustatyti maksimalų pralaidumą	Ugniasienė geba pasirinktam duomenų srautui nustatyti maksimalų pralaidumą	Firewall must be able to set maximum bandwidth for selected data stream	Firewall can set maximum bandwidth for selected data stream.	Ugniasienė geba pasirinktam duomenų srautui nustatyti maksimalų pralaidumą	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-traffic-shaping-54/TS_Configuration/TS_Configuring.htm	
3.3.70	Ugniasienėje turi gebėti pasirinktam duomenų srautui nustatyti garantuotą pralaidumą	Ugniasienėje geba pasirinktam duomenų srautui nustatyti garantuotą pralaidumą	Firewall must be able to set maximum bandwidth for selected data stream	Firewall can set maximum bandwidth for selected data stream.	Ugniasienėje geba pasirinktam duomenų srautui nustatyti garantuotą pralaidumą	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-traffic-shaping-54/TS_Configuration/TS_Configuring.htm	
3.3.71	Ugniasienėje maksimalus arba garantuotas pralaidumas turi būti konfigūruojamas pagal	ugniasienės saugumo taisyklę; vartotojo IP adresą; aplikaciją	Maximum or guaranteed throughput must be configured as per provided criteria on the firewall:	firewall security rule; user's IP address; application.	ugniasienės saugumo taisyklę; vartotojo IP adresą; aplikaciją	https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-getting-started/using-the-GUI/dashboard.htm	

3.3.72	Ugniasienėje turi gebėti duomenų srautų valdymo statistiką atvaizduoti grafinių būdu	Ugniasienėje turi gebėti duomenų srautų valdymo statistiką atvaizduoti grafinių būdu	Firewall must be capable of graphically displaying traffic management statistics	Firewall is capable of graphically displaying traffic management statistics.	Ugniasienėje turi gebėti duomenų srautų valdymo statistiką atvaizduoti grafinių būdu	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/FeatureCatalog-firewall.htm	
3.3.73	Ugniasienė turi gebėti kurti saugumo taisykles iš karto tarp kelių saugumo zonų, t. y. sukurti vieną taisyklę, kuri leistų iš 2 ar daugiau zonų jungtis į 2 ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei.	Ugniasienė geba kurti saugumo taisykles iš karto tarp kelių saugumo zonų, t .y. sukurti vieną taisyklę, kuri leistų iš 2 ar daugiau zonų jungtis į 2 ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei.	Firewall must be able to create security rules for multiple security zones at once, i.e. create a single rule that allows connections from 2 or more zones to 2 or more zones without creating separate rules for each interzone flow control.	Firewall can create security rules for multiple security zones at once, i.e. create a single rule that allows connections from 2 or more zones to 2 or more zones without creating separate rules for each interzone flow control.	Ugniasienė geba kurti saugumo taisykles iš karto tarp kelių saugumo zonų, t .y. sukurti vieną taisyklę, kuri leistų iš 2 ar daugiau zonų jungtis į 2 ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei.	https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/378040/importing-the-signed-certificate-to-your-fortigate	
3.3.74	Ugniasienė turi gebėti importuoti skaitmeninius sertifikatus SSL sesijų terminavimui / perėmimui ar įrenginio valdymui	Ugniasienė geba importuoti skaitmeninius sertifikatus SSL sesijų terminavimui / perėmimui ar įrenginio valdymui	Device must be able to import digital certificates for SSL session termination/interception or device management	Firewall can import digital certificates for SSL session termination/interception or device management.	Ugniasienė geba importuoti skaitmeninius sertifikatus SSL sesijų terminavimui / perėmimui ar įrenginio valdymui	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/96571/certificate-crl	
3.3.75	Ugniasienė turi palaikyti CRL (*angl*. Certificate revocation list)	Ugniasienė palaiko CRL (angl. Certificate revocation list)	Firewall must support CRL (Certificate Revocation List)	Firewall supports CRL (Certificate Revocation List).	Ugniasienė palaiko CRL (angl. Certificate revocation list)	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/96571/certificate-crl	
3.3.76	Ugniasienė turi palaikyti OCSP (*angl*. Online Certificate Status Protocol) protokolą	Ugniasienė palaiko OCSP (angl. Online Certificate Status Protocol) protokolą	Firewall must support Online Certificate Status Protocol (OCSP)	Firewall supports the Online Certificate Status Protocol (OCSP).	Ugniasienė palaiko OCSP (angl. Online Certificate Status Protocol) protokolą	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/59761/vpn-certificate-ocsp-server	
3.3.77	Ugniasienė turi palaikyti 4096 bitų RSA sertifikatus	Ugniasienė palaiko 4096 bitų RSA sertifikatus	Firewall must support 4096-bit RSA certificates	Firewall supports 4096-bit RSA certifications.	Ugniasienė palaiko 4096 bitų RSA sertifikatus	https://docs.fortinet.com/document/fortigate/6.2.2/cli-reference/277620/vpn-certificate-setting	
3.3.78	Ugniasienė turi gebėti importuoti tarnybinių stočių viešus, privačius raktus ir sertifikatus Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos	Ugniasienė geba importuoti tarnybinių stočių viešus, privačius raktus ir sertifikatus	Firewall must be able to import public, private server keys and certificates *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Firewall can import public, private server keys and certificates.	Ugniasienė geba importuoti tarnybinių stočių viešus, privačius raktus ir sertifikatus	https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/378040/importing-the-signed-certificate-to-your-fortigate	
3.3.79	Ugniasienė turi gebėti generuoti ir eksportuoti Netflow v9 ar lygiaverčius įrašus apie duomenų srautus. Įrašuose turi būti informacija apie vartotojus ir taikomąją programinę įrangą	Ugniasienė geba generuoti ir eksportuoti Netflow v9 ar lygiaverčius įrašus apie duomenų srautus. Įrašuose turi būti informacija apie vartotojus ir taikomąją programinę įrangą	Device must be able to generate and export Netflow v9 or equivalent data feeds. The records must contain information about users and software application.	Device can generate and export Netflow v9 or equivalent data feeds. The records must contain information about users and software application.	Ugniasienė geba generuoti ir eksportuoti Netflow v9 ar lygiaverčius įrašus apie duomenų srautus. Įrašuose turi būti informacija apie vartotojus ir taikomąją programinę įrangą	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-networking/Troubleshooting/Netflow.htm	
3.3.80	Ugniaisienės įvykių žurnalai turi būti kaupiami lokaliai ir siunčiami į centrinę valdymo tarnybinę stotį	Ugniaisenės įvykių žurnalai yra kaupiami lokaliai ir siunčiami į centrinę valdymo tarnybinę stotį	Event logs for the firewall must be stored locally and sent to a central management server	Event logs for the firewall are stored locally and sent to a central management server.	Ugniaisenės įvykių žurnalai yra kaupiami lokaliai ir siunčiami į centrinę valdymo tarnybinę stotį	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-logging-reporting-54/logs.htm	
3.3.81	Įvykių žurnaluose turi būti galimybė	filtruoti įvykius; fiksuoti administratorių atliekamus veiksmus.	Event logs must have the capability	filter events; record actions taken by administrators.	filtruoti įvykius; fiksuoti administratorių atliekamus veiksmus.	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-logging-reporting-54/logs.htm	
3.3.82	Ugniasienė turi gebėti nurodytų laiku įvykių žurnalus siųsti į nutolusią darbo vietą/tarnybinę stotį	Ugniasienė geba nurodytų laiku įvykių žurnalus siųsti į nutolusią darbo vietą/tarnybinę stotį	Firewall must be able to send event logs to a remote workstation/server at a specified time.	Firewall is able to send event logs to a remote workstation/server at a specified time.	Ugniasienė geba nurodytų laiku įvykių žurnalus siųsti į nutolusią darbo vietą/tarnybinę stotį	https://kb.fortinet.com/kb/documentLink.do?externalID=FD46071	

3.3.83	Ugniasienėje turi būti atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginį esant dideliam tinklo aprovimui	Ugniasienėje yra atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginį esant dideliam tinklo aprovimui	Firewall must have separate control and data analysis modules to ensure that device can be operated at high network load	Firewall has its own control and data analysis modules to control device at high network load.	Ugniasienėje yra atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginį esant dideliam tinklo aprovimui	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Other_Profile_Considerations/Conserve%20mode.htm	
3.3.84	Ugniasienė turi būti valdomas	SSHv2; iš centrinės valdymo sistemos.	Firewall must be controlled via:	SSHv2; Central management system.	SSHv2; iš centrinės valdymo sistemos.	https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-getting-started-52/basic_admin.htm ir https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-system-administration-52/Central%20Management/central_mgmt.htm	
3.3.85	Turi būti galimybė naudoti IPv6 kiekvieno atskiro įrenginio ir centrinės valdymo tarnybinės stoties sujungimui	Yra galimybė naudoti IPv6 kiekvieno atskiro įrenginio ir centrinės valdymo tarnybinės stoties sujungimui	It must be possible to use IPv6 to connect firewall to central management server	It is possible to use IPv6 to connect firewall to the central management server.	Yra galimybė naudoti IPv6 kiekvieno atskiro įrenginio ir centrinės valdymo tarnybinės stoties sujungimui	https://help.fortinet.com/cli/fos60hlp/60/Content/FortiOS/fortiOS-cli-ref/config/system/central-management.htm	
3.3.86	Ugniasienės administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Ugniasienės administratorių prieigos teisės yra kontroliuojamos rolių pagalba	Administrators' permissions of firewall must be controlled by roles *Functionality can be implemented from a central management system*	Administrators' permissions of firewall are controlled by roles.	Ugniasienės administratorių prieigos teisės yra kontroliuojamos rolių pagalba	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/294491/administrator-profiles	
3.3.87	Ugniasienėje turi būti galimybė kurti administratorių roles *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Ugniasienėje yra galimybė kurti administratorių roles	Firewall must have ability to create administrator roles *Functionality can be implemented from a central management system*	Firewall can create administrator roles.	Ugniasienėje yra galimybė kurti administratorių roles	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/294491/administrator-profiles	
3.3.88	Ugniasienėje turi būti galimybė apibrėžti administratoriaus teises *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Ugniasienėje yra galimybė apibrėžti administratoriaus teises	Firewall must have ability to fine-tune administrator privileges *Functionality can be implemented from a central management system*	Firewall has ability to fine-tune administrator privileges.	Ugniasienėje yra galimybė apibrėžti administratoriaus teises	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/294491/administrator-profiles	
3.3.89	Ugniasienėje turi būti galimybė sukurti įrenginio naudotoją, kuris turėtų tik skaitymo (*angl*. read-only) teises *Funkcionalumas gali būti realizuotas iš centrinės valdymo sistemos*	Ugniasienėje yra galimybė sukurti įrenginio naudotoją, kuris turėtų tik skaitymo (*angl*. read-only) teises	Firewall must have ability to create user that has read-only access *Functionality can be implemented from a central management system*	Firewall can create user that has read-only rights.	Ugniasienėje yra galimybė sukurti įrenginio naudotoją, kuris turėtų tik skaitymo (*angl* read-only) teises	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/294491/administrator-profiles	
3.3.90	Ugniasienė turi gebėti detaliai apibrėžti administratoriaus teises keisti sisteminius įrenginio nustatymus; kurti, keisti saugumo ir NAT taisykles; peržiūrėti įvykių žurnalus *Funkcionalumas gali būti realizuotas iš centrinės valdymo tarnybinės sistemos*	Ugniasienė geba detaliai apibrėžti administratoriaus teises keisti sisteminius įrenginio nustatymus; kurti, keisti saugumo ir NAT taisykles; peržiūrėti įvykių žurnalus	Firewall must have the ability to specify administrator privileges to change system settings; to create, change security and NAT rules; access to event logs *Functionality can be implemented from a central management system*	Firewall can specify administrator privileges, to change system settings; to create, change security and NAT rules; access to event logs; right to review reports	Ugniasienė geba detaliai apibrėžti administratoriaus teises keisti sisteminius įrenginio nustatymus; kurti, keisti saugumo ir NAT taisykles; peržiūrėti įvykių žurnalus	https://cookbook.fortinet.com/limited-access-administrator-account/index.html	
3.3.91	Ugniasienė turi gebėti persiųsti operacinę sistemą ir konfigūraciją SCP protokolu *Funkcionalumas gali būti realizuotas iš centrinės valdymo tarnybinės sistemos*	Ugniasienė geba persiųsti operacinę sistemą ir konfigūraciją SCP protokolu	Firewall must be able to transfer operating system and configuration using the SCP protocol *Functionality can be implemented from a central management system*	Firewall can transfer operating system and configuration using the SCP protocol.	Ugniasienė geba persiųsti operacinę sistemą ir konfigūraciją SCP protokolu	https://kb.fortinet.com/kb/documentLink.do?externalID=FD43754	

3.3.92	Ugniasienėje turi veikti Syslog protokolas *Funkcionalumas gali būti realizuotas iš centrinės valdymo tarnybinės sistemos*	Ugniasienėje veikia Syslog protokolas	Firewall must be running Syslog protocol *Functionality can be implemented from a central management system*	Firewall is running Syslog protocol.	Ugniasienėje veikia Syslog protokolas	https://kb.fortinet.com/kb/documentLink.do?externalID=FD44614	
3.3.93	Ugniasienėje turi veikti SNMPv3 protokolas	Ugniasienėje veikia SNMPv3 protokolas	Firewall must be running SNMPv3 protocol	Firewall is running SNMPv3 protocol.	Ugniasienėje veikia SNMPv3 protokolas	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Monitoring/SNMP.htm	
3.3.94	Ugniasienėje turi veikti NTP (versijos 3 ir 4) laiko sinchronizavimo protokolas *Funkcionalumas gali būti realizuotas iš centrinės valdymo tarnybinės sistemos*	Ugniasienėje veikia NTP (versijos 3 ir 4) laiko sinchronizavimo protokolas	Firewall must have NTP (version 3 and 4) time synchronization protocol *Functionality can be implemented from a central management system*	Firewall has NTP (version 3 and 4) time synchronization protocol.	Ugniasienėje veikia NTP (versijos 3 ir 4) laiko sinchronizavimo protokolas	https://kb.fortinet.com/kb/viewContent.do?externalId=FD33783	
3.3.95	Ugniasienė turi gebėti keisti įvykių, siunčiamų SYSLOG protokolų, formatą *Funkcionalumas gali būti realizuotas iš centrinės valdymo tarnybinės sistemos*	Ugniasienė geba keisti įvykių, siunčiamų SYSLOG protokolų, formatą	Firewall must be able to change format of events sent by SYSLOG protocols *Functionality can be implemented from a central management system*	Firewall can change format of events sent by SYSLOG protocols.	Ugniasienė geba keisti įvykių, siunčiamų SYSLOG protokolų, formatą	https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-whats-new/Top-LogReport-cef.htm	
3.3.96	Ugniasienė turi gebėti automatiškai daryti konfigūracijos kopijas *Funkcionalumas gali būti realizuotas iš centrinės valdymo tarnybinės sistemos*	Ugniasienė geba automatiškai daryti konfigūracijos kopijas	Firewall must be able to automatically make configuration copies *Functionality can be implemented from a central management system*	Firewall can automatically make configuration copies.	Ugniasienė geba automatiškai daryti konfigūracijos kopijas	https://kb.fortinet.com/kb/documentLink.do?externalID=FD39818	
3.3.97	Ugniasienė turi gebėti sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis	Įrenginyje yra galimybė sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis	Firewall must be able to compare current device configuration with previous configurations	Firewall can compare current device configuration with previous configurations.	Įrenginyje yra galimybė sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/702257/configuration-backups	
3.3.98	Ugniasienė turi gebėti aktyvuoti ankstesnę konfigūraciją	Ugniasienė geba aktyvuoti ankstesnę konfigūraciją	Firewall must be able to use previous configuration	Firewall can use previous configuration.	Ugniasienė geba aktyvuoti ankstesnę konfigūraciją	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-getting-started-54/7-Basic-Admin/Firmware/Configuration%20revision.htm	
3.3.99	Ugniasienė turi gebėti matyti aktyvius sujungimus (sesijas)	Ugniasienė geba matyti aktyvius sujungimus (sesijas)	Firewall must be able to see active connections (sessions)	Firewall can see active connections (sessions).	Ugniasienė geba matyti aktyvius sujungimus (sesijas)	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-fortiview-54/Consoles/All_Sessions.htm	
3.4	**Ugniasienės konstrukcijos reikalavimai**		**Equipment design requirements**				
3.4.1	Elektros maitinimas	230V AC	Device power feed	**230V** AC.	*100-240V AC*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	*6 psl.*
3.4.2	Elektros tiekimo šaltinis turi būti sukomplektuotas su elektros tiekimo prijungimo kabeliu	Elektros tiekimo šaltinis sukomplektuotas su elektros tiekimo prijungimo kabeliais	Power supplies for unit must be complete with power supply cables	Power sources for unit are complete with power supply cables.	Elektros tiekimo šaltinis sukomplektuotas su elektros tiekimo prijungimo kabeliais	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/1a50676a-0748-11eb-96b9-00505692583a/FG-FWF-40F-3G4G-60F-Series-QSG.pdf	*14 psl.*

3.4.3	Ugniasienė turi būti sukomplektuota su konsolės prijungimo kabeliu	Ugniasienė sukomplektuota su konsolės prijungimo kabeliu	Firewall must be equipped with a console connection cable	Firewall is equipped with a console connection cable.	Ugniasienė sukomplektuota su konsolės prijungimo kabeliu	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/1a50676a-0748-11eb-96b9-00505692583a/FG-FWF-40F-3G4G-60F-Series-QSG.pdf	*14 psl.*
3.5	**Ugniasienės bendrieji reikalavimai**		**General system requirements**				
3.5.1	Siūloma ugniasienė (toliau – įranga) ir jos sudedamosios dalys turi būti naujos ir nenaudotos. *Negalima siūlyti gamykliškai atnaujintos (angl. refurbished) ugniasienės*	Siūloma ugniasienė ir jos sudedamosios dalys yra naujos ir nenaudotos	Proposed firewall (hereinafter referred to as "equipment") must be new and unused. *Refurbished equipment must not be offered*	Proposed firewall (hereinafter referred to as "equipment") is new and unused.	Siūloma ugniasienė ir jos sudedamosios dalys yra naujos ir nenaudotos		
3.5.2	Įrangos dokumentacija anglų kalba turi būti pateikiama gamintojo interneto svetainėje	Įrangos dokumentacija anglų kalba pateikiama gamintojo interneto svetainėje	Equipment documentation in English must be available on the manufacturer's website	Equipment documentation in English is available on the manufacturer's website.	Įrangos dokumentacija anglų kalba pateikiama gamintojo interneto svetainėje	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	
3.5.3	Ugniasienei turi būti teikiamas techninis aptarnavimas	Ugniasienei yra teikiamas techninis aptarnavimas	Techical support must be provided to Firewall	Techical support is provided to Firewall	Ugniasienei yra teikiamas techninis aptarnavimas		
3.5.4	Įranga turi būti pateikta su licencijomis, leidžiančiomis techninio aptarnavimo laikotarpiu gauti šiuos aprašų atnaujinimus	Aplikacijų protokolų kontrolės (angl. Application Control); įsilaužimų kontrolės (angl. Intrusion Prevention System); virusų, piktybinių programų (angl. Antivirus)	Equipment must be provided with licenses to receive these specification updates during maintenance	Application Control; Intrusion Prevention System; viruses, malware (Antivirus).	Aplikacijų protokolų kontrolės (angl. Application Control); įsilaužimų kontrolės (angl. Intrusion Prevention System); virusų, piktybinių programų (angl. Antivirus)		
3.5.5	Įranga turi būti pateiktos su licencijomis, leidžiančiomis techninio aptarnavimo laikotarpiu gauti šiuos aprašų atnaujinimus	Aplikacijų protokolų kontrolės (angl. Application Control)	Equipment must be provided with licenses to receive these specification updates during maintenance	Application Control.	Aplikacijų protokolų kontrolės (angl. Application Control)		
3.5.6	Ugniaisienė turi gebėti atsisiųsti programinės įrangos atnaujinimus ir pataisymus (*angl*. patch) bei 3.5.4 ir 3.5.5 punktuose nurodytus aprašų atnaujinimus iš gamintojo puslapio	Ugniasienė geba atsisiųsti programinės įrangos atnaujinimus ir pataisymus (angl. patch) bei 3.5.4 ir 3.5.5 punktuose nurodytus aprašų atnaujinimus iš gamintojo puslapio	Firewall must be able to download software updates, patches and signatures updates referred to clauses 3.5.4 and 3.5.5 from the manufacturer's website.	Firewall is able to download software updates, patches and signatures updates referred to clauses 3.5.4 and 3.5.5 from the manufacturer's website.	Ugniasienė geba atsisiųsti programinės įrangos atnaujinimus ir pataisymus (angl. patch) bei 3.5.4 ir 3.5.5 punktuose nurodytus aprašų atnaujinimus iš gamintojo puslapio	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/817681/fortiguard	
3.5.7	Garantija	Siūlomai įrangai ir visiems pateiktiems techniniams ir programiniams komponentams garantinė priežiūra turi būti atliekama paties įrangos gamintojo arba jo autorizuoto aptarnavimo atstovo. Garantinio aptarnavimo metu turi būti nemokamai atliekami remonto darbai ir nemokamai keičiami sugedę komponentai. Papildomi garantinio remonto ir palaikymo reikalavimai pateikti Techninės specifikacijos 4.12 skyriuje.	Warranty	Offered equipment and all supplied hardware and software components must be under warranty service either by equipment manufacturer or by an authorized service representative. Warranty service must include free repair and replacement of defective components. For additional warranty repair and maintenance requirements, see Section 4.12 of the Technical Specification.	Siūlomai įrangai ir visiems pateiktiems techniniams ir programiniams komponentams garantinė priežiūra turi būti atliekama paties įrangos gamintojo arba jo autorizuoto aptarnavimo atstovo. Garantinio aptarnavimo metu turi būti nemokamai atliekami remonto darbai ir nemokamai keičiami sugedę komponentai. Papildomi garantinio remonto ir palaikymo reikalavimai pateikti Techninės specifikacijos 4.12 skyriuje.		
4.	**Tinklo ugniasienių centrinė valdymo sistema (toliau – Sistema) / Central Network Firewall Management System (Furth. - System)**						
4.1	Sistemos pavadinimas ir modelis (gamintojo suteiktas numeris (kodas))	Nurodomas sistemos pavadinimas ir modelis (gamintojo suteiktas numeris (kodas))	System name and model (manufacturer's identification number (code))	Name and model of system components are provided (manufacturer's identification number (code))	*FortiManager ir FortiAnalyzer*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	
4.2	Gamintojas (pavadinimas)	Nurodomas sistemos gamintojas	Manufacturer (name)	System manufacturer is provided	*Fortinet*		
4.3	**Sistemos charakteristikos**		**System characteristics**				

4.3.1	Sistemos funkcionalumo aprašymas	Specializuotas vieno gamintojo programinis sprendimas, skirtas valdyti ugniasienes, įskaitant logines savarankiškas virtulias sistemas (domenus), nurodytas techninės specifikacijos 1-3 dalyse, kaupti įvykių pranešimus iš ugniasienių, juos analizuoti, koreliuoti bei generuoti ataskaitas.	Description of system functionality	Specialized single-vendor software solution for managing firewalls, including logical stand-alone virtual systems (domains), as specified in Parts 1 to 3 of the technical specification, for collecting, analyzing, correlating, and generating reports of event messages from firewalls.	Specializuotas vieno gamintojo programinis sprendimas, skirtas valdyti ugniasienes, įskaitant logines savarankiškas virtulias sistemas (domenus), nurodytas techninės specifikacijos 1-3 dalyse, kaupti įvykių pranešimus iš ugniasienių, juos analizuoti, koreliuoti bei generuoti ataskaitas.	*https://www.fortinet.com/products/management/fortimanager ir https://www.fortinet.com/products/management/fortianalyzer*	
4.3.2	Sistemos valdomų įrenginių skaičius	Ne mažiau kaip **50**	Number of devices controlled by the system	No less than **50**	*Ne mažiau kaip 50 su FMG-VM-10-UG x5*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	*4 psl.*
4.3.3	Sistemos darbo terpė	Sistema diegiama į virtualią Užsakovo infrastruktūrą. Turi būti palaikomos VMware ESXi 6.5 ir naujesnės versijos	System work environment	System is installed in customer's virtual infrastructure. VMware ESXi 6.5 and later must be supported	Sistema diegiama į virtualią Užsakovo infrastruktūrą. Turi būti palaikomos VMware ESXi 6.5 ir naujesnės versijos	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	*4 psl.*
4.3.4	Sistema turi apdoroti žurnalinių įvykių per parą	Ne mažiau kaip **5GB**	Ammount of processed log events on a daily basis by the system	No less than **5GB**	*6 GB su FAZ-VM-GB5*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	*4 psl.*
4.3.5	Sistema turi saugoti istorinių įvykių pranešimų	Ne mažiau kaip **3TB**	Ammount of log events saved by the system	No less than **3TB**	*3 TB su FAZ-VM-GB5*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	*4 psl.*
4.3.6	Sistema turi atlikti šias funkcijas	centralizuotas įrenginių konfigūracijų valdymas; centralizuotas įrenginių įvykių žurnalų kaupimas; įvykių žurnalų peržiūra; centralizuotas valdomų įrenginių statistikos kaupimas; ataskaitų generavimas.	System must perform these functions:	centralized management of device configurations; centralized collection of device event logs; review of event logs; centralized collection of statistics on managed installations; report generation.	centralizuotas įrenginių konfigūracijų valdymas; centralizuotas įrenginių įvykių žurnalų kaupimas; įvykių žurnalų peržiūra; centralizuotas valdomų įrenginių statistikos kaupimas; ataskaitų generavimas.	*https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf ir https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf*	
4.3.7	Prisijungimas prie sistemos turi būti vykdomas naudojant	SSHv2; HTTPS.	Connection to the system must be made using:	SSHv2; HTTPS.	SSHv2; HTTPS.	*https://help.fortinet.com/fmgr/cli/5-6-2/Document/0600_Using-the-CLI/0415_Connecting-to-CLI%20-%20SSH.htm https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/643984/connecting-to-the-gui https://docs.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/965071/connecting-to-the-fortianalyzer-cli-using-ssh https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/643984/connecting-to-the-gui*	

4.3.8	Sistema turi gebėti surinkti, analizuoti, koreliuoti įvykių pranešimus.	Sistemas geba surinkti, analizuoti, koreliuoti įvykių pranešimus.	System must be able to collect, analyze and correlate event messages.	System is able to collect, analyze and correlate event messages.	Sistemas geba surinkti, analizuoti, koreliuoti įvykių pranešimus.	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/401159/types-of-logs-collected-for-each-device	
4.3.9	Sistema turi gebėti generuoti ataskaitas.	Sistema turi galimybę generuoti ataskaitas.	System must be able to generate reports.	System is able to generate reports.	Sistema turi galimybę generuoti ataskaitas.	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/136416/reports	
4.3.10	Sistema turi gebėti atlikti paiešką tarp įvykių pranešimų.	Sistema geba atlikti paiešką tarp įvykių pranešimų.	System must be able to search for event messages.	System is able to search for event messages.	Sistema geba atlikti paiešką tarp įvykių pranešimų.	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/368629/filtering-messages	
4.3.11	Sistema turi gebėti atvaizduoti įvykius realiu bei istorinius įvykius.	Sistema geba atvaizduoti įvykius realiu bei istorinius įvykius.	System must be able to display real and historical events.	System is able to display real and historical events.	Sistema geba atvaizduoti įvykius realiu bei istorinius įvykius.	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/294662/viewing-historical-and-real-time-logs	
4.3.12	Sistemoje paruoštų skirtingų ataskaitų šablonų skaičius	Ne mažiau kaip **20**	Number of different report templates prepared in the system	No less than **20**	*61*	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/002854/list-of-report-templates	
4.3.13	Sistema turi gebėti kurti savo ataskaitų šablonus.	Sistema geba kurti savo ataskaitų šablonus.	System must be able to create its own report templates.	System is able to create its own report templates.	Sistema geba kurti savo ataskaitų šablonus.	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/222636/creating-report-templates	
4.3.14	Sistema turi gebėti automatizuoti ataskaitų generavimą	Sistema geba automatizuoti ataskaitų generavimą	System must be able to automate report generation	System is able to automate report generation	Sistema geba automatizuoti ataskaitų generavimą	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/377901/scheduling-reports	
4.3.15	Ataskaitos turi būti pateikiamos ne mažiau kaip vienu iš šių formatų	PDF; HTML; CSV; XML	Reports must be submitted in at least one of these formats:	PDF; HTML; CSV; XML	PDF; HTML; CSV; XML	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/435266/viewing-completed-reports	
4.3.16	Sistema turi gebėti sugeneruotą ataskaitą išsiųsti nurodytu elektroninio pašto adresu	Sistema geba sugeneruotą ataskaitą išsiųsti nurodytu elektroninio pašto adresu	System must be able to send generated report to the specified e-mail address	System is able to send generated report to the specified e-mail address	Sistema geba sugeneruotą ataskaitą išsiųsti nurodytu elektroninio pašto adresu	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/108255/creating-output-profiles	
4.3.17	Sistema turi gebėti realiu laiku pateikti informaciją apie valdomo įrenginio perduodamus duomenų srautus	Sistema geba realiu laiku pateikti informaciją apie valdomo įrenginio perduodamus duomenų srautus	System must be able to provide real-time information on data flows transmitted by the controlled device	System is able to provide real-time information on data flows transmitted by the controlled device	Sistema geba realiu laiku pateikti informaciją apie valdomo įrenginio perduodamus duomenų srautus	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/294662/viewing-historical-and-real-time-logs	

4.3.18	Sistema turi gebėti pateikti informaciją apie duomenų srautus pagal šalis	Sistema geba pateikti informaciją apie duomenų srautus pagal šalis	System must be able to provide information on data flows by country	System is able to provide information on data flows by country	Sistema geba pateikti informaciją apie duomenų srautus pagal šalis	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/85344/fortiview-dashboards	
4.3.19	Sistema turi gebėti pateikti informaciją apie labiausiai naudojamas taisykles	Sistema geba pateikti informaciją apie labiausiai naudojamas taisykles	System must be able to provide information on the most commonly used rules	System is able to provide information on the most commonly used rules	Sistema geba pateikti informaciją apie labiausiai naudojamas taisykles	https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/397218/policy-hit-count	
4.3.20	Sistema turi gebėti pateikti informaciją apie dažniausiai lankomas svetaines, svetainių grupes	Sistema geba pateikti informaciją apie dažniausiai lankomas svetaines, svetainių grupes	System must be able to provide information about the most visited sites, groups of sites	System is able to provide information about the most visited sites, groups of sites	Sistema geba pateikti informaciją apie dažniausiai lankomas svetaines, svetainių grupes	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/85344/fortiview-dashboards	
4.3.21	Sistema turi gebėti parodyti geografinį grėsmių atvaizdavimą	Sistema geba parodyti geografinį grėsmių atvaizdavimą	System must be able to display a geographical representation of threats	System is able to display a geographical representation of threats	Sistema geba parodyti geografinį grėsmių atvaizdavimą	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-	
4.3.22	Sistemoje turi būti galimybė persiųsti visus sukauptus įvykių pranešimus į kitą įvykių pranešimo kaupimo stotį CEF formatu	Sistemoje yra galimybė persiųsti visus sukauptus įvykių pranešimus į kitą įvykių pranešimo kaupimo stotį CEF formatu	System must be able to forward all accumulated event messages to another event message storage station in CEF format	Systemis able to forward all accumulated event messages to another event message storage station in CEF format	Sistemoje yra galimybė persiųsti visus sukauptus įvykių pranešimus į kitą įvykių pranešimo kaupimo stotį CEF formatu	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/621804/log-forwarding	
4.3.23	Sistema turi gebėti atvaizduoti realiu laikų valdomų įrenginių parametrus	CPU apkrovimą; RAM panaudojimą.	System must be able to display parameters of real-time controlled devices	CPU load; RAM usage.	CPU apkrovimą; RAM panaudojimą.	https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/284439/view-system-dashboard-for-managed-logging-devices	
4.3.24	Duomenų apsikeitimas tarp sistemos ir valdomų įrenginių turi būti šifruojamas	Duomenų apsikeitimas tarp sistemos ir valdomų įrenginių yra šifruojamas	Data exchange between the system and managed devices must be encrypted	Data exchange between the system and managed devices is encrypted	Duomenų apsikeitimas tarp sistemos ir valdomų įrenginių yra šifruojamas	*https://docs.fortinet.com/document/fortimanager/6.4.3/cli-reference/772079/global#global* *https://docs.fortinet.com/document/fortianalyzer/6.4.3/cli-reference/849211/global#global*	
4.3.25	Sistema turi gebėti jungti valdomus įrenginius į skirtingas grupes	Sistema geba jungti valdomus įrenginius į skirtingas grupes	System must be able to connect managed devices to different groups	System is able to connect managed devices to different groups	Sistema geba jungti valdomus įrenginius į skirtingas grupes	https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/551924/add-device-groups	
4.3.26	Sistema turi gebėti skirtingos įrenginių (fizinių ir virtualių) grupėms priskirti atskirus administratorius	Sistemoje geba skirtingos įrenginių (fizinių ir virtualių) grupėms priskirti atskirus administratorius	System must be able to assign individual administrators to different groups of devices (physical and virtual)	System is able to assign individual administrators to different groups of devices (physical and virtual)	Sistemoje geba skirtingos įrenginių (fizinių ir virtualių) grupėms priskirti atskirus administratorius	https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/858351/creating-administrators	
4.3.27	Sistemoje turi būti užtikrinta, kad administratorius gali matyti ir valdyti tik jam priskirtus įrenginius	Sistemoje yra užtikrinta, kad administratorius gali matyti ir valdyti tik jam priskirtus įrenginius	System must ensure that administrator can only see and manage the devices assigned to him	System ensures that administrator can only see and manage the devices assigned to him	Sistemoje yra užtikrinta, kad administratorius gali matyti ir valdyti tik jam priskirtus įrenginius	https://docs.fortinet.com/document/fortimanager/6.4.3/administration-	

4.3.28	Sistema turi gebėti kurti bendrus objektus ir saugumo taisykles, kurios yra naudojamos keliems įrenginiams	Sistema geba kurti bendrus objektus ir saugumo taisykles, kurios yra naudojamos keliems įrenginiams	System must be able to create common objects and security rules that are used for multiple devices	System is able to create common objects and security rules that are used for multiple devices	Sistema geba kurti bendrus objektus ir saugumo taisykles, kurios yra naudojamos keliems įrenginiams	https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/304425/firewall-policy-objects	
4.3.29	Administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba	Administratorių prieigos teisės yra kontroliuojamos rolių pagalba.	Administrators' access rights must be controlled by roles	Administrators' access rights is controlled by roles	Administratorių prieigos teisės yra kontroliuojamos rolių pagalba.	https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/392019/permissions	
4.3.30	Sistemoje turi būti galimybė kurti roles	Sistemoje yra galimybė kurti roles	System must be able to create roles	System is able to create roles	Sistemoje yra galimybė kurti roles	https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/675151/creating-administrator-profiles	
4.3.31	Administratorių tapatybės nustatymas turi būti atliekamas	lokaliai; RADIUS; LDAP; TACACS+.	Administrators must be authenticated:	locally; RADIUS; LDAP; TACACS+.	lokaliai; RADIUS; LDAP; TACACS+.	https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/123103/authentication	
4.3.32	Sistemoje turi būti kaupiami visų valdomų įrenginių įvykių žurnalai	Sistemoje turi būti kaupiami visų valdomų įrenginių įvykių žurnalai	Event logs for all managed devices must be stored in the system	Event logs for all managed devices is stored in the system	Sistemoje turi būti kaupiami visų valdomų įrenginių įvykių žurnalai	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/401159/types-of-logs-collected-for-each-device	
4.3.33	Sistema turi gebėti generuoti bendras ataskaitas ir kiekvienam įrenginiui individualias ataskaitas	Sistema geba generuoti bendras ataskaitas ir kiekvienam įrenginiui individualias ataskaitas	System must be able to generate general reports and individual reports for each device	System is able to generate general reports and individual reports for each device	Sistema geba generuoti bendras ataskaitas ir kiekvienam įrenginiui individualias ataskaitas	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/227385/reports-settings-tab	
4.3.34	Sistemos įvykių žurnaluose turi būti fiksuojami administratorių atliekami veiksmai, laikas kada buvo atliktas veiksmas	Sistemos įvykių žurnaluose turi būti fiksuojami administratorių atliekami veiksmai, laikas kada buvo atliktas veiksmas	System event logs must record actions performed by administrators and time when action was performed	Sistemos įvykių žurnaluose turi būti fiksuojami administratorių atliekami veiksmai, laikas kada buvo atliktas veiksmas	Sistemos įvykių žurnaluose turi būti fiksuojami administratorių atliekami veiksmai, laikas kada buvo atliktas veiksmas	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/401159/types-of-logs-collected-for-each-device	
4.3.35	Turi turėti galimybę apjungti dvi tokias pats sistemas į aukšto patikimumo sistemą, veikiančią Aktyvus/Pasyvus (angl. Active/Passive) režimu	Yra galimybė apjungti dvi tokias pats sistemas į aukšto patikimumo sistemą, veikiančią Aktyvus/Pasyvus (angl. Active/Passive) režimu	System must be able to combine two identical systems into a high-reliability system operating in Active / Passive mode	System is able to combine two identical systems into a high-reliability system operating in Active / Passive mode	Yra galimybė apjungti dvi tokias pats sistemas į aukšto patikimumo sistemą, veikiančią Aktyvus/Pasyvus (angl. Active/Passive) režimu	*https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/568591/high-availability* *https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/506748/high-availability*	

4.3.36	Turi būti galimybė iš sistemos eksportuoti sistemos ir sistemos valdomų įrenginių taisykles.	Yra galimybė iš sistemos eksportuoti sistemos ir sistemos valdomų įrenginių taisykles	It must be possible to export system and system-managed device rules from the system.	It is possible to export system and system-managed device rules from the system.	Yra galimybė iš sistemos eksportuoti sistemos ir sistemos valdomų įrenginių taisykles	*https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/112240/backing-up-the-system https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/304008/creating-backup-adoms ir https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/112240/backing-up-the-system*	
4.3.37	Sistemoje turi gebėti valdomiems įrenginiams centralizuotai įdiegti dinaminius atnaujinimus (antivirusus, IPS, pažeidžiamumų aprašus) iš lokaliai saugomos duomenų bazės.	Sistema geba valdomiems įrenginiams centralizuotai įdiegti dinaminius atnaujinimus (antivirusus, IPS, pažeidžiamumų aprašus) iš lokaliai saugomos duomenų bazės	System must be able to centrally install dynamic updates (antivirus, IPS, vulnerability descriptions) from a locally stored database on managed devices.	System is able to centrally install dynamic updates (antivirus, IPS, vulnerability descriptions) from a locally stored database on managed devices.	Sistema geba valdomiems įrenginiams centralizuotai įdiegti dinaminius atnaujinimus (antivirusus, IPS, pažeidžiamumų aprašus) iš lokaliai saugomos duomenų bazės	https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/431186/operating-as-an-fds-in-a-closed-network	
4.3.38	Sistemos realizavimas	Įrenginių valdymo sistema ir žurnalinių įvykių kaupimo bei apdorojimo sistema gali būti realizuotos, naudojant bendrą sistemą arba skirtingas sistemas, išlaikant nurodytus funkcionalumo reikalavimus	System implementation	Device management system, log event storage and processing system can be implemented using a common system or different systems, while maintaining specified functionality requirements.	*Įrenginių valdymo sistema ir žurnalinių įvykių kaupimo bei apdorojimo sistemai realizuota, naudojant skirtingas FortiManager ir FortiAnalyzer sistemas, išlaikant nurodytus funkcionalumo reikalavimus*	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	
4.4	**Sistemos bendrieji reikalavimai**		**General system requirements**				
4.4.1	Sistemos dokumentacija anglų kalba turi būti pateikiama gamintojo interneto svetainėje	Sistemos dokumentacija anglų kalba pateikiama gamintojo interneto svetainėje	System documentation in English must be available on the manufacturer's website	System documentation in English is available on the manufacturer's website.	Sistemos dokumentacija anglų kalba pateikiama gamintojo interneto svetainėje	*https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf*	
4.4.2	Sistemai turi būti teikiamas techninis aptarnavimas	Sistemai yra teikiamas techninis aptarnavimas	System must be serviced	System is serviced.	Sistemai yra teikiamas techninis aptarnavimas su FC1-10-LV0VM-248-02-36 ir FC2-10-M3004-248-02-36		
4.4.3	Sistema turi būti pateikta su visom licencijom, užtikrinančiomis visų įrenginių, įskaitant virtualias sistemas (domenus), administravimą, bei leidžiančiomis techninio aptarnavimo laikotarpiu gauti programinės įrangos atnaujinimus ir pataisymus (angl. patch) atnaujinimus	Sistema yra pateikta su visom licencijom, užtikrinančiomis visų įrenginių, įskaitant virtualias sistemas (domenus), administravimą, bei leidžiančiomis techninio aptarnavimo laikotarpiu gauti programinės įrangos atnaujinimus ir pataisymus (*angl* . patch) atnaujinimus	System must be accompanied by all licenses to administer all devices, including virtual systems (domains), and to allow software updates and patches to be obtained during maintenance.	System is accompanied by all licenses to administer all devices, including virtual systems (domains), and to allow software updates and patches to be obtained during maintenance.	Sistema yra pateikta su visom licencijom, užtikrinančiomis visų įrenginių, įskaitant virtualias sistemas (domenus), administravimą, bei leidžiančiomis techninio aptarnavimo laikotarpiu gauti programinės įrangos atnaujinimus ir pataisymus (*angl* patch) atnaujinimus		
4.4.4	Sistema turi turėti galimybę atsisiųsti programinės įrangos atnaujinimus ir pataisymus (*angl* . patch) iš gamintojo puslapio	Ugniasienė turi galimybę atsisiųsti programinės įrangos atnaujinimus ir pataisymus (*angl* . patch) iš gamintojo puslapio	System must be able to download software updates and patches from the manufacturer's site	System is able to download software updates and patches from the manufacturer's site	Ugniasienė turi galimybę atsisiųsti programinės įrangos atnaujinimus ir pataisymus (*angl* . patch) iš gamintojo puslapio	https://docs.fortinet.com/document/fortimanager/6.4.3/upgrade-guide/262607/upgrading-fortimanager-firmware	