

Техническа спецификация по обособена позиция № 2 с предмет: „Доставка на софтуерно дефинирана мрежа за пренос на данни“

1. Софтуерно дефиниран маршрутизатор тип 1 – 36 броя.

Обща информация	
REQ.1.	Захранване –в диапазона от минимум 100 до 240 VAC
REQ.2.	Работен температурен диапазон от 0° до +40 °C
REQ.3.	Безшумна работа – без вентилатори
REQ.4.	Минимум четири интерфейса 100/1000BASE-T
REQ.5.	Брой USB портове - минимум един, версия 3.0 или по-висока
REQ.6.	Сериен конзолен порт - минимум един
REQ.7.	Минимум 4GB DRAM
REQ.8.	Минимум 4 GB Flash
REQ.9.	Производителност от минимум 500Mbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя
REQ.10.	Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание
REQ.11.	Да поддържа IPv4 и IPv6 WAN транспортни мрежи
REQ.12.	Да поддържа изграждането на SDWAN overlay с използването на IPSec върху различни WAN мрежи – Internet и MPLS
REQ.13.	Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика
REQ.14.	Да поддържа IPsec AH с използване на минимум HMAC-SHA1 алгоритъм
REQ.15.	Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys
REQ.16.	Да поддържа изграждане на GRE тунели до външни системи за сигурност
REQ.17.	Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SDWAN контролерите
REQ.18.	Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати
REQ.19.	Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност
REQ.20.	Да поддържа използване на сертификати от CA на възложителя
REQ.21.	Да поддържа минимум AES-256 GCM алгоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.
REQ.22.	Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация.
REQ.23.	Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.
REQ.24.	Да поддържа автоматично маршрутизиране на ниво приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay
REQ.25.	Да има вграден zone firewall
REQ.26.	Да има application firewall с вградено разпознаване на приложенията
REQ.27.	Да поддържа филтриране на трафика чрез ACL
REQ.28.	Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите.

REQ.29.	Да поддържа управляеми SDWAN IPSec топологии – hub-and-spoke, full mesh и комбинации между двете.
REQ.30.	Да поддържа отделна, виртуална, топология за всеки сегмент
REQ.31.	Да поддържа следните протоколи за интеграция с външни мрежи: <ul style="list-style-type: none"> • Static route • OSPF • BGP
REQ.32.	Да поддържа PIM
REQ.33.	Да поддържа следните видове NAT услуги <ul style="list-style-type: none"> • статичен NAT • симетричен NAT • NAT64 • NAT pools • PAT
REQ.34.	Да поддържа изграждане на SD-WAN IPSec през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay
REQ.35.	Да поддържа QoS: <ul style="list-style-type: none"> • CoS маркиране • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP или подобен алгоритъм • Управление на задръстванията с RED и WRED алгоритми • Traffic policing • Traffic shaping
REQ.36.	Да поддържа packet duplication – изпращане на един пакет по два или повече отделни SDWAN IPSec тунела до приемащия SD-WAN маршрутизатор
REQ.37.	Да поддържа автоматичен избор на най-добрия маршрут до SaaS приложения чрез измерване на закъснението и загубата на пакети до SaaS приложенията през директна Internet връзка и през Internet връзката на централна локация. Да поддържа минимум Microsoft Office 365 и AWS
REQ.38.	Да поддържа минимум следните методи за управление и наблюдение: <ul style="list-style-type: none"> • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • Split DNS • DDOS защита • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика

	<ul style="list-style-type: none"> • Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управление на достъпа чрез RADIUS и TACACS+ системи.
REQ.39.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя;
REQ.40.	Устройството да е окомплектовано с SDWAN лицензи за минимум 100Mbps WAN трафик.
Гаранция и поддръжка:	
REQ.41.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.42.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.43.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.44.	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години

2. Софтуерно дефиниран маршрутизатор тип 2 – 42 броя.

Обща информация	
REQ.45.	Захранване –в диапазона от минимум 100 до 240 VAC
REQ.46.	Работен температурен диапазон от 0° до +40 °C
REQ.47.	Безшумна работа – без вентилатори
REQ.48.	Минимум четири интерфейса 100/1000BASE-T и два интерфейса SFP
REQ.49.	Брой USB портове - минимум един, версия 3.0 или по-висока
REQ.50.	Сериен конзолен порт - минимум един
REQ.51.	Минимум 4GB DRAM
REQ.52.	Минимум 4 GB Flash
REQ.53.	Производителност от минимум 1Gbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя
REQ.54.	Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание
REQ.55.	Да поддържа IPv4 и IPv6 WAN транспортни мрежи
REQ.56.	Да поддържа изграждането на SDWAN overlay с използването на IPSec
REQ.57.	Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика
REQ.58.	Да поддържа IPSec AH с използване на минимум HMAC-SHA1 алгоритъм
REQ.59.	Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys
REQ.60.	Да поддържа изграждане на GRE тунели до външни системи за сигурност
REQ.61.	Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите
REQ.62.	Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати
REQ.63.	Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност
REQ.64.	Да поддържа използване на сертификати от CA на възложителя
REQ.65.	Да поддържа минимум AES-256 GCM алгоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.
REQ.66.	Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация.

REQ.67.	Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.
REQ.68.	Да поддържа автоматично маршрутизиране на приложения и групи от приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay.
REQ.69.	Да има вграден zone firewall
REQ.70.	Да има application firewall с вградено разпознаване на приложенията
REQ.71.	Да поддържа филтриране на трафика чрез ACL
REQ.72.	Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите
REQ.73.	Да поддържа управляеми IPSec топологии – hub-and-spoke, full mesh и комбинации между двете
REQ.74.	Да поддържа отделна, виртуална, топология за всеки сегмент
REQ.75.	<p>Да поддържа следните протоколи за интеграция с външни мрежи:</p> <ul style="list-style-type: none"> • Static route • OSPF • BGP • VRRP
REQ.76.	Да поддържа 802.1Q
REQ.77.	Да поддържа обединяване на интерфейси в bridge групи
REQ.78.	Да поддържа IGMP v1 и v2
REQ.79.	Да поддържа PIM
REQ.80.	<p>Да поддържа следните видове NAT услуги</p> <ul style="list-style-type: none"> • статичен NAT • динамичен NAT • NAT64 • NAT pools • PAT
REQ.81.	Да поддържа изграждане на SD-WAN през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay
REQ.82.	<p>Да поддържа QoS:</p> <ul style="list-style-type: none"> • CoS маркиране • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP или подобен алгоритъм • Управление на задръстванията с RED и WRED алгоритми • Traffic policing • Traffic shaping
REQ.83.	Да поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор
REQ.84.	Да поддържа автоматичен избор на най-добрия маршрут до SaaS приложения чрез измерване на закъснението и загубата на пакети до SaaS приложенията през директна Internet връзка и през Internet връзката на централна локация. Да поддържа минимум Microsoft Office 365 и AWS
REQ.85.	<p>Да поддържа минимум следните методи за управление и наблюдение:</p> <ul style="list-style-type: none"> • Управление чрез SD-WAN контролерите в това задание

	<ul style="list-style-type: none"> • DHCP клиент • DHCP сървър • DHCP Relay • DNS • Split DNS • DDOS защита • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управление на достъпа чрез RADIUS и TACACS+ системи.
REQ.86.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя;
REQ.87.	Устройството да е окомплектовано с SDWAN лицензи за минимум 1Gbps WAN трафик.
Гаранция и поддръжка:	
REQ.88.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.89.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.90.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.91.	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години

3. Софтуерно дефиниран маршрутизатор тип 3 – 36 броя.

Обща информация	
REQ.92.	Захранване –в диапазона от минимум 100 до 240 VAC
REQ.93.	Работен температурен диапазон от 0° до +40 °C
REQ.94.	Шаси за монтаж в 19“ шкаф
REQ.95.	Два токозахранващи модула
REQ.96.	Минимум четири интерфейса, които поддържат 100/1000BASE-T и SFP
REQ.97.	Брой USB портове - минимум 1
REQ.98.	Конзолен порт - 1
REQ.99.	Минимум 8GB DRAM
REQ.100.	Възможност за добавяне на модул с LTE cat. 6 модем
REQ.101.	Възможност за добавяне на минимум осем 1000Base-T порта
REQ.102.	Производителност от минимум 3Gbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя
REQ.103.	Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание
REQ.104.	Да поддържа IPv4 и IPv6 WAN транспортни мрежи
REQ.105.	Да поддържа изграждането на SDWAN overlay с използването на IPSec
REQ.106.	Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика

REQ.107.	Да поддържа IPsec AH с използване на минимум HMAC-SHA1 алгоритъм
REQ.108.	Да използва уникална двойка ключове за всеки IPsec тунел в мрежата – IPsec pairwise keys
REQ.109.	Да поддържа изграждане на GRE тунели до външни системи за сигурност
REQ.110.	Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите
REQ.111.	Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати
REQ.112.	Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност
REQ.113.	Да поддържа използване на сертификати от CA на възложителя
REQ.114.	Да поддържа минимум AES-256 GCM алгоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.
REQ.115.	Да поддържа изолирането на трафика от определени вътрешни интерфейси чрез използване на VRF, MPLS или подобен протокол за сегментация
REQ.116.	Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация.
REQ.117.	Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPsec тунел.
REQ.118.	Да поддържа автоматично маршрутизиране на приложения и групи от приложения през различни WAN връзки на база динамичните параметрите на IPsec WAN тунелите – packet loss, jitter и delay
REQ.119.	Да има вграден zone firewall
REQ.120.	Да има application firewall с вградено разпознаване на приложенията
REQ.121.	Да поддържа филтриране на трафика чрез ACL
REQ.122.	Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите
REQ.123.	Да поддържа управляеми IPsec топологии – hub-and-spoke, full mesh и комбинации между двете
REQ.124.	Да поддържа отделна, виртуална, топология за всеки сегмент
REQ.125.	<p>Да поддържа следните протоколи за интеграция с външни мрежи:</p> <ul style="list-style-type: none"> • Static route • OSPF • BGP • VRRP
REQ.126.	Да поддържа 802.1Q
REQ.127.	Да поддържа IGMP v2 и v3
REQ.128.	Да поддържа минимум PIM SSM
REQ.129.	Да поддържа PIM rendezvous point
REQ.130.	Да поддържа статичен и динамичен NAT и NAT pool
REQ.131.	Да поддържа изграждане на SD-WAN през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay
REQ.132.	<p>Да поддържа QoS:</p> <ul style="list-style-type: none"> • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP или подобен алгоритъм

	<ul style="list-style-type: none"> • Управление на задръстванията с RED и WRED алгоритми • Traffic policing • Traffic shaping • Автоматичен traffic shaping за всеки VPN тунел съобразно пропускателната способност на WAN връзката, на отдалечения SD-WAN рутер • QoS върху VLAN интерфейси • Премаркиране на DCSP полето на база политики
REQ.133.	Да поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор
REQ.134.	Да има вграден IPS
REQ.135.	Да има вградена Anti Malware защита
REQ.136.	Да има URL филтриране по категории
REQ.137.	Да осигурява декриптиране на SSL и TLS за инспектиране на криптиран трафик
REQ.138.	Да поддържа автоматичен избор на най-добрия маршрут до SaaS приложения чрез измерване на закъснението и загубата на пакети до SaaS приложенията през директна Internet връзка и през Internet връзката на централна локация. Да поддържа минимум Microsoft Office 365 и AWS
REQ.139.	Да поддържа висока надеждност чрез съвместна работа с второ устройство от същия тип и използване на неговите WAN транспортни интерфейси за изграждане на IPSec SDWAN транспортни тунели
REQ.140.	<p>Да поддържа минимум следните методи за управление и наблюдение:</p> <ul style="list-style-type: none"> • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управление на достъпа чрез RADIUS и TACACS+ системи.
REQ.141.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя;
REQ.142.	Устройството да е окомплектовано с SDWAN лицензи за минимум 1Gbps WAN трафик
Гаранция и поддръжка:	
REQ.143.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.144.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.145.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.146.	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години

4. Софтуерно дефиниран маршрутизатор тип 4 – 2 броя.

Обща информация	
REQ.147.	Захранване – в диапазона от минимум 100 до 240 VAC
REQ.148.	Работен температурен диапазон от 0° до +40 °C
REQ.149.	Шаси за монтаж в 19" шкаф
REQ.150.	Два токозахранващи модула
REQ.151.	Минимум шест 1000BaseT и два SFP+ порта.
REQ.152.	Устройството да бъде доставено с четири 10GBASE-SR SFP+ модула
REQ.153.	Брой USB портове - минимум 1,
REQ.154.	Сериен конзолен порт - минимум 1
REQ.155.	Минимум 8GB DRAM
REQ.156.	Производителност от минимум 6Gbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя
REQ.157.	Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание
REQ.158.	Да поддържа IPv4 и IPv6 WAN транспортни мрежи
REQ.159.	Да поддържа изграждането на SDWAN overlay с използването на IPSec
REQ.160.	Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика
REQ.161.	Да поддържа IPSec AH с използване на минимум HMAC-SHA1 алгоритъм
REQ.162.	Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys
REQ.163.	Да поддържа изграждане на GRE тунели до външни системи за сигурност
REQ.164.	Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите
REQ.165.	Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати
REQ.166.	Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност
REQ.167.	Да поддържа използване на сертификати от CA на възложителя
REQ.168.	Да поддържа минимум AES-256 GCM алгоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.
REQ.169.	Да поддържа изолирането на трафика от определени вътрешни интерфейси чрез използване на VRF, MPLS или подобен протокол за сегментация
REQ.170.	Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация.
REQ.171.	Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.
REQ.172.	Да поддържа автоматично маршрутизиране на приложения и групи от приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay
REQ.173.	Да има вграден zone firewall
REQ.174.	Да има application firewall с вградено разпознаване на приложенията
REQ.175.	Да поддържа филтриране на трафика чрез ACL
REQ.176.	Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите
REQ.177.	Да поддържа управляеми IPSec топологии – hub-and-spoke, full mesh и комбинации между двете

REQ.178.	Да поддържа отделна, виртуална, топология за всеки сегмент
REQ.179.	<p>Да поддържа следните протоколи за интеграция с външни мрежи:</p> <ul style="list-style-type: none"> • Static route • OSPF • BGP • VRRP
REQ.180.	Да поддържа 802.1Q
REQ.181.	Да поддържа IGMP v2 и v3
REQ.182.	Да поддържа минимум PIM SSM
REQ.183.	Да поддържа PIM rendezvous point
REQ.184.	Да поддържа статичен и динамичен NAT и NAT pool
REQ.185.	Да поддържа изграждане на SD-WAN през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay
REQ.186.	<p>Да поддържа QoS:</p> <ul style="list-style-type: none"> • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP или подобен алгоритъм • Управление на задръстванията с RED и WRED алгоритми • Traffic policing • Traffic shaping • Автоматичен traffic shaping за всеки VPN тунел съобразно пропускателната способност на WAN връзката, на отдалечения SD-WAN рутер • QoS върху VLAN интерфейси • Премаркиране на DCSP полето на база политики
REQ.187.	Да поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор
REQ.188.	Да поддържа автоматичен избор на най-добрия маршрут до SaaS приложения чрез измерване на закъснението и загубата на пакети до SaaS приложенията през директна Internet връзка и през Internet връзката на централна локация. Да поддържа минимум Microsoft Office 365 и AWS
REQ.189.	Да поддържа висока надеждност чрез съвместна работа с второ устройство от същия тип и използване на неговите WAN транспортни интерфейси за изграждане на IPSec SDWAN транспортни тунели
REQ.190.	<p>Да поддържа минимум следните методи за управление и наблюдение:</p> <ul style="list-style-type: none"> • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • NTP • SNMP

	<ul style="list-style-type: none"> • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управление на достъпа чрез RADIUS и TACACS+ системи.
REQ.191.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя;
REQ.192.	Устройството да е окомплектовано с SDWAN лицензи за минимум 5Gbps WAN трафик
Гаранция и поддръжка:	
REQ.193.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.194.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.195.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.196.	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години

5. Софтуер за управление на софтуерно дефинирана мрежа

Обща информация	
REQ.197.	Софтуерни контролери за изграждане и управление на SDWAN мрежа с SDWAN маршрутизаторите в това задание
REQ.198.	Инсталация – върху VMWare ESXi на възложителя
REQ.199.	Количество – съгласно изискванията на производителя за постигане на висока надеждност и резервиране на SDWAN контролната система
REQ.200.	Автоматично присъединяване и провизиране на маршрутизаторите в SDWAN средата чрез използване на компонент за оркестриране, който осигурява plug-and-play, zero touch plug&play и подобни решения за автоматизация.
REQ.201.	Управление на маршрутизаторите и техните функции в SDWAN мрежата чрез темплейти
REQ.202.	Управление на услугите и виртуалните топологии в SDWAN мрежата чрез политики
REQ.203.	Управление на транспортната IPSec топология чрез политики
REQ.204.	Динамично управление на различни трафични класове през IPSec транспортната инфраструктура на база параметрите на тунелите – jitter, latency, загуба на пакети
REQ.205.	Управление на IPS, application Firewall, URL Filter и Malware защитата в SDWAN маршрутизаторите с такива функции.
REQ.206.	Наблюдение на SDWAN маршрутизаторите
REQ.207.	Наблюдение на SDWAN IPSec транспортните тунели и техните параметри – минимум up/down, packet loss, jitter и delay
REQ.208.	Наблюдение на трафичните параметри от различни класове приложения, които използват SD-WAN мрежата
REQ.209.	Визуализация на маршрутите за различните класове трафик през SDWAN мрежата
REQ.210.	Изграждане на карта с топологията на SD-WAN мрежата с овърлей върху географска карта на страната.
REQ.211.	Визуализация на пътя на трафичните потоци, на ниво приложения, върху транспортните тунели.
REQ.212.	Преодставяне на информация за QoS на трафичните потоци от приложенията

REQ.213.	Исторически справки за трафичните потоци през SDWAN мрежата
REQ.214.	Web GUI интерфейс
REQ.215.	Role based access controll
REQ.216.	Да поддържа SSO съвместимо с Microsoft ADFS
REQ.217.	Да има REST API за интеграция с външни софтуерни системи
Гаранция и поддръжка:	
REQ.218.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.219.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.220.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.221.	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години

6. Съвместимост на компоненти

Обща информация	
REQ.222.	За постигането на пълна съвместимост и улеснена експлоатация на SDWAN мрежата, предлаганите SDWAN рутери, SFP+ модули и софтуерни компоненти за сигурност трябва да са от един производител.