

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

„Доставка на мрежово оборудване за създаване на надеждна и защитена връзка на вътрешната мрежа на изпълнителна агенция „Медицински надзор“ с интернет“.

Навсякъде в настоящата спецификация, където се съдържат и са посочени, определени "Марка", "Тип", "Модел", "Производител" или "Стандарт", да се четат след наименованията, думите "или еквивалент"!!!

2019 г.

I. ОПИСАНИЕ НА НАСТОЯЩАТА ОБЩЕСТВЕНА ПОРЪЧКА

Техническата спецификация е неделима част от Документацията за участие в обществената поръчка за доставка на ново мрежово оборудване за създаване на надеждна и защитена връзка на вътрешната мрежа на изпълнителна агенция „Медицински надзор“ с интернет, наред с договорните условия. Спецификацията е предназначена да поясни и развие изискванията по изпълнение на обществената поръчка.

Предмета на обществената поръчка се изразява в доставка с инсталиране и конфигуриране на ново мрежово оборудване за създаване на надеждна и защитена връзка на вътрешната мрежа на изпълнителна агенция „Медицински надзор“ с интернет.

Цел: Изпълнението на поръчката си поставя като основна цел, успешно инсталиране и конфигуриране на ново мрежово оборудване за създаване на надеждна и защитена връзка на вътрешната мрежа на изпълнителна агенция „Медицински надзор“ с интернет. Специфичните цели на поръчката се изразяват в доставка на посоченото техническо оборудване, съгласно настоящата спецификация включващо добавянето на нови изчислителни ресурси за нуждите на ИАМН чрез закупуване на нов сървър и ъпгрейд на съществуващи, закупуване на ново външно лентово устройство за целите на процесите по архивиране на информация, както и да се осигури надеждна и защитена връзка на вътрешната мрежа на агенцията с Интернет.

Очакван резултат:

- ✓ Изпълнени доставки предмет на обществената поръчка;
- ✓ инсталиране и конфигуриране на мрежово оборудване за създаване на надеждна и защитена връзка на вътрешната мрежа на изпълнителна агенция „Медицински надзор“ с интернет.

Място на изпълнение:

Изпълнителна агенция „Медицински надзор“, с адрес: гр. София, район «Триадица», ул. "Св. Георги Софийски" № 3.

Срок за изпълнение:

Срокът за изпълнение на настоящата поръчка е до 10 (*десет*) календарни дни, след датата на подписване на договора за обществената поръчка и същият включва доставка, инсталиране и конфигуриране на мрежово оборудване за създаване на надеждна и защитена връзка на вътрешната мрежа на изпълнителна агенция „Медицински надзор“ с интернет.

II. ИНФОРМАЦИЯ ЗА ОБЩЕСТВЕНАТА ПОРЪЧКА:

1. Ако не са производители на предлаганото оборудване, участниците трябва да са оторизирани от производителя/ите или от негов официален представител за Р. България да извършва доставка и сервиз за предложеното оборудване (Сървър, Лентово устройство, Компоненти за ъпгрейд на сървъри, Комплексна система за защита, Опорен комутатор).

2. Участниците трябва да са оторизирани от производителя/ите или от негов официален представител за Р. България да извършва продажба и доставка на предложената комплексна система за защита и интернет комутатор.

В случаите когато оторизацията не е от производителя, а от негов официален представител за България, участниците следва да представят документ доказващ, че официалният представител е упълномощен от производителя да издава оторизационни писма от негово име.

За позиция 5. Комплексна система за защита се допуска и оторизационно писмо, издадено от официалния дистрибутор за България.

За доказване изпълнението на горното изискване, към техническото предложение участниците следва да приложат съответните оторизационни документи.

3. Участниците следва да прилагат система за управление на сигурността на информацията съгласно стандарт EN ISO 27001 или еквивалентен, с обхват в областта на доставка и въвеждане в експлоатация на комуникационно и сървърно оборудване, доставка на софтуерни продукти.

За доказване изпълнението на горното изискване, към техническото предложение участниците следва да приложат копие на валиден сертификат за внедрена система за управление на сигурността на информацията, съгласно стандарт EN ISO 27001 или еквивалентен, с обхват в областта на доставка и въвеждане в експлоатация на комуникационно и сървърно оборудване, доставка на софтуерни продукти.

4. Участниците следва да прилагат система за управление на услугите съгласно стандарт EN ISO 20000-1 или еквивалентно/и, с обхват доставка и въвеждане в експлоатация на комуникационно и сървърно оборудване, доставка на софтуерни продукти.

За доказване изпълнението на горното изискване, към техническото предложение участниците следва да приложат копие на валиден сертификат за внедрена система за управление на услугите, съгласно стандарт EN ISO 20000-1 или еквивалентно/и, с обхват доставка и въвеждане в експлоатация на комуникационно и сървърно оборудване, доставка на софтуерни продукти.

Изпълнителят следва да достави, инсталира и конфигурира следното ново оборудване съгласно зададените по-долу минимални технически изисквания:

1. Сървър – 1 брой:

Параметър	Минимални технически изисквания
Шаси	За монтаж в 19" шкаф, максимум 1U
Процесор	Инсталирани 2 броя с минимум 12 ядра, 24 нишки, номинална честота минимум 2.2GHz, с минимум 16.5MB кеш, литография максимум 14 nm, поддръжка на VT-x и VT-d технологии или еквивалентни, поддръжка на Turbo Boost технология или еквивалент
Оперативна памет	Инсталирана минимум 256GB DDR4 2666 MHz честота, ECC, поддръжка на разширение до минимум 3TB
Мрежа	Минимум 8 броя портове 1Gbps Ethernet и минимум 2 броя 16Gb Fibre Channel
Контролер за твърди дискове	Хардуерен контролер с поддръжка на RAID нива 0,1,5,10,50
Твърди дискове	Инсталирани 2 броя SAS 15k rpm HDD с обем минимум 300GB, поддръжка на монтаж на минимум 8 броя дискове, поддръжка на възможност за инсталиране на два броя M.2 SSD дискове на отделна платка, работещи в RAID
Слотове за разширение	Минимум 2 броя PCIe Gen 3

Управление	Наличие на модул за управление с отделен RJ-45 порт 1Gbps, поддръжка на мониторинг на ефективността (performance monitoring), автоматични ъпдейти и планирани ъпдейти;
Захранване	Резервирано захранване 1+1, с мощност максимум 500W всяко
Поддържани операционни системи	Citrix XenServer, Microsoft Windows Server with Hyper-V, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi
Акcesoари	Включени в комплектацията релси за монтаж, захранващи кабели
Гаранция	Минимум 3 години в режим 24x7, с време на реакция следващ работен ден, от производителя

2. Външно лентово устройство - 1 брой:

Параметър	Минимални технически изисквания
Тип технология	LTO-6 със скорост на трансфер минимум 160MB/sec
Интерфейс	SAS 6/12Gbps
Комплектация	Включен HBA SAS 6/12Gbps адаптер, съвместим със сървър Dell R530, минимум 5 броя LTO-6 касетки и минимум 1 брой почистваща касетка, захранващ кабел
Гаранция	Минимум 3 години в режим 8x5, с време на реакция следващ работен ден, от производителя

3. Компоненти за ъпгрейд на съществуващи устройства:

Параметър	Минимални технически изисквания
Памет за сървър Dell R530 със сериен номер 8NHYGD2	1 брой 16GB модул, от производителя на сървъра
Дискове за сървър Dell R530 със сериен номер 8NHYGD2	3 броя 4TB 7.2K rpm SATA 6Gbps за горещ монтаж, от производителя на сървъра
Дискове за дисков масив Dell PowerVault MD3600f със сериен номер F2Q5422	2 броя 600GB SAS 15k rpm за горещ монтаж, от производителя на масива
Дискове за дисков масив Dell PowerVault MD3600f със сериен номер F2Q5422	2 броя 1.8GB SAS 15k rpm за горещ монтаж, от производителя на масива
Компоненти за комутатор QLogic SANbox 5800 със сериен номер 1331F00287	1 брой лиценз за използване на нови 4 порта, 4 броя SFP модули и 5 броя оптични кабели с дължина минимум 2м.

4. Интернет комутатор – 1 брой:

Параметър	Минимални технически изисквания
-----------	---------------------------------

Вид	Управляем
Ниво на комутатора	L2
Електрическо захранване	100-240 VAC, 50-60 Hz
Монтаж	Монтиране в комуникационен шкаф
Регулаторни изисквания	UL 60950-1 Second Edition, CAN/CSA-C22.2 No. 60950-1 Second Edition, EN 60950-1 Second Edition, IEC 60950-1 Second Edition, AS/NZS 60950-1 47CFR Part 15 (CFR 47) Class A, AS/NZS CISPR22 Class A, CISPR22 Class A, EN55022 Class A, ICES003 Class A, VCCI Class A, EN61000-3-2, EN61000-3-3, KN22 Class A, CNS13438 Class A EN55024, CISPR24, EN300386, KN24
Етернет портове	24x 10/100/1000 0BASE-T ports, RJ45 конектори
Uplink интерфейси	4x 1000BASE-T SFP-based ports, два от които да са съвместими с наличните SFP модули: Atop, SFP 1.256, 1310 nm, LX 20 KM DMI (APS31123CDL20)
Пропускателна способност	41 Mpps
Капацитет на предаване (Forwarding bandwidth)	28 Gbps
Капацитет за маршрутизиране/превключване	56 Gbps
VLAN	Maximum active VLANs: 64 VLAN IDs available: 4094 Стандарт: IEEE 802.1Q VLAN
L2 мрежови стандарти	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3az, IEEE 802.3ae, IEEE 802.3af, IEEE 802.3at, IEEE 802.1ax, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.3x, IEEE 802.1ab, IEEE 802.3ad, IEEE 802.3ah
L3 мрежови стандарти	RFC 1256 - Internet Control Message Protocol (ICMP) Router Discovery, RFC 792 - ICMP, RFC 791 - IP, RFC 793 - TCP, RFC 768 - UDP
IPv6	Да поддържа IPv6
Сигурност	802.1X; 802.1x Disable per-VLAN MAC learning Multidomain/AAA command authorization Port-based ACLs SSH, Kerberos, and SNMPv3; SPAN TACACS+/ RADIUS/MAC authentication MAC address/Web notification Bridge Protocol Data Unit (BPDU) Spanning-tree Root Guard (STRG) IGMP filtering Dynamic VLAN assignment
Методи за управление	SNMP, web UI, Bluetooth for over-the-air access, Virtual Stacking, DHCP, Internet Group Management Protocol (IGMP), Trivial File Transfer Protocol (TFTP), RMON, TCP
Портове за управление	USB mini-Type B (console) port USB Type A port и RJ-45 Console Port

Гаранция	Минимум 3 години
----------	------------------

5. Комплексна система за защита – 1 брой:

Комплексната система за защита (система от тип Next Generation Firewall) трябва да осигурява защита на мрежата и компютрите от вируси и хакерски атаки. Тя трябва да се реализира чрез хардуерни и софтуерни компоненти и следва да включва 2 броя хардуерни модули (основно и резервно) и всички необходими софтуерни лицензи за осигуряване на описаните по-долу минимални изисквания.

5.1. Общи параметри на хардуерните компоненти (основен и резервен):

Параметър	Технически изисквания
Електрическо захранване	И двата компонента да имат възможност за монтиране на втори захранващ модул, като основния компонент да е оборудван с два захранващи модула
Параметри на захранването	100-240 VAC, 50-60 Hz
Form factor	1U Rack Mountable
Регулаторни изисквания	FCC Class A, CE, LVD, RoHS, TUV/GS, VCCI Class A, MSIP/KCC Class A, UL, WEEE, REACH,
Интерфейси	2 x 2.5-GbE SFP 2 x 2.5-GbE 6 x 1-GbE 1 GbE Management 1 Console
USB портове	2
Управление	CLI, SSH, Web UI, Централизирана мениджмънт конзола за управление на устройството/а, REST APIs
Отказоустойчивост (High availability)	Active/Passive with State Sync и възможност за Active/Active При отпадане на основното устройство, резервното трябва автоматично да поеме неговите функции.
Logging	Analyzer, Local Log, Syslog
Интеграция	LDAP integration
IP address assignment	Static, DHCP, PPPoE, L2TP and PPTP client, Internal DHCP server, DHCP Relay
NAT	IPv6 NAT Load Balancing NAT Policies – 512 NAT Mode of Operation One-to-One NAT NAT with DHCP Client NAT with PPPoE Client NAT with L2TP client NAT with PPTP client Enhanced NAT Modes Inbound NAT Load Balancing
L2 функционалност	Layer-2 QoS L2 bridge, wire/virtual wire mode, tap mode
L3 функционалност	Dynamic routing (RIP/OSPF/BGP) Policy-based routing (ToS/metric and ECMP)

		Inbound/outbound load balancing Asymmetric routing
WAN функционалност		Secure SD-WAN SD-WAN Groups – 38 SD-WAN members – 76 Performance probes - 44
Характеристика на портовете	на	<ul style="list-style-type: none"> - Port security - Jumbo frames - Port mirroring - Link aggregation (static and dynamic) - Port redundancy
VLAN		VLAN interfaces – 256 VLAN trunking Spanning Tree Protocol RSTP (Rapid Spanning Tree Protocol)
Маршрутизиращи протоколи (Routing protocols)		BGP, OSPF, RIPv1/v2, static routes, policy-based routing
Качество на услугите (QoS)		Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p
Автентикация (Authentication)		LDAP (multiple domains), XAUTH/RADIUS, SSO, internal user database, Terminal Services, Common Access Card (CAC)
Автентикация на потребителите (User Authentication)	на (User)	SSO Users - 20 000 Terminal Servers Supported -5 SSO Agents - 9 Non-SSO Users(Web, L2TP, GVC, SSLVPN) - 1 500 RADIUS Accounting Clients -1 500 Authentication Partitioning
VoIP		Full H323, SIP, Enable/Disable H.323 Transformations, Enable/Disable SIP Transformations, Advanced QoS and Monitoring
Стандарти		TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3
VPN		Site-to-Site VPN Policies Remote Access (GroupVPN) MD5/SHA1 authentication DES/3DES AES Support for AES-128, AES-192, AES-256 Manual Key IKE using pre-shared secrets IKE using certificates IKEv2 XAUTH Authentication Main Mode Aggressive Mode Customizable Phase 1/Phase2 NAT Traversal DHCP Relay RIPv2 advertising Netbios pass through

	SNMP VPN MIB L2TP Server User-definable Local Networks using Groups "User-definable Destination Networks (Using Groups)" User-definable local IKE identities User-definable peer identities NAT and Rules Policies per VPN Zone Remote Access VPN Per User/Group Policies Policy on the tunnel Remote Access IP Pooling Secondary IPSec Gateway / Redundant Peer Gateway Per Tunnel Access Control using User Groups Route Based VPN VPN Tunnel Redundancy
Site-to-Site - VPN Policies (Unnumbered)	500
Site-to-Site - VPN Tunnel Interface (Number)	32
IPSec VPN clients	50
SSL VPN Clients	2
DPI Signatures	10 000
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography
Route-based VPN	RIP, OSPF, BGP
DNS функционалност	DNS security
DHCP	DHCP server
IPv6	IPv6 addresses on interfaces IPv6 DHCP Prefix Delegation IPv6 6rd (Rapid Deployment) BGP IPv6 Support IPv6 Backend Support IPv6 Wire Mode support IPv6 NAT Load Balancing
Wireless Security	802.11 Wireless Support -Via Access Point WEP, WEP on Demand - Via Access Point WPA - Via Access Point MAC Filtering WifiSec Support (IPSEC Security for Wireless) Wireless Guest Services Max Guest Logins Per Wireless Zone – 1 500 WLAN to LAN Bridging Wireless Intrusion Detection/Protection Access Points Supported - 256 Access Points per physical Interface - 256 WWAN Failover (4G/LTE)

5.2. Производителност на защитната стена:

Параметър	Технически изисквания
Firewall inspection throughput (RFC 2544)	3.0 Gbps
Firewall Performance 1280 Byte	2 500 Mbps
Threat Prevention throughput	1.5 Gbps
IPS throughput	1.4 Gbps
Malware throughput	1.3 Gbps
VPN throughput	1.45 Gbps
VPN Performance (AES)	1300 Mbps
IMIX Performance	700 Mbps
Connections per second	14,000/sec

5.3. Наблюдение и управление:

Да има следната функционалност:

- Централизирана мениджмънт конзола за управление на устройството/а, Web UI, CLI, REST APIs, SNMPv2/v3
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat Security Analytics Platform
- Enhanced logging
- Bandwidth management

6. Функционални изисквания на компонентите за защита:

6.1. Комплексната защитна стена трябва да включва:

- Stateful packet inspection - Целият трафик на мрежата се проверява, анализира и привежда в съответствие с правилата за достъп до защитната стена
- Gateway Anti-Virus
- Anti-Spyware
- Intrusion Prevention
- Application Intelligence
- Control Service subscription
- Content Filtering Service subscription - Цялостното филтриране на съдържанието. Рейтингите на уебсайтове.
- TLS/SSL decryption and inspection. Сканиране на трафика до откриване, дешифриране и проверява за кибератаки по всички портове.
- SSH inspection - Проверка на пакети на SSH дешифрира и проверява преминаването на данни през SSH тунел, за да се предотвратят атаки, които използват SSH.
- DDoS attack protection (UDP/ICMP/SYN flood)
- IPv4/IPv6
- Biometric authentication for remote access
- DNS proxy
- REST APIs
- Sandbox функционалност- Много слойно решение за откриване и спиране на нулеви заплахи и да разполага с инспекция на паметта в реално време – защита от „Нулеви“ и непознати нови кибер заплахи. Открива и блокира зловреден софтуер, който не се проявява или се крие, чрез криптиране. Да може да блокира съмнителни файлове за проверка, докато не се установи дали не съдържа вируси. Да може да сканира Windows и Android устройства.

- Идентификация и управление на приложения
- HTTP/HTTPS Web content filtering
 - URL filtering
 - Proxy avoidance
 - Keyword blocking
 - Policy based filtering (exclusion/inclusion)
 - HTTP header insertion
 - Bandwidth manage CFS rating categories
 - Unified policy model with app control
 - Content Filtering Client
- Web caching

6.2. Изисквания за защита на електронната поща:

Комплексната защитна стена трябва да осигурява многослойна (поне дву-степенна) антиспам и антивирусна защита на електронната поща със следните изисквания:

6.2.1. Слой 1 – Първо ниво на защита със следните минимални изисквания:

- Gateway/портал защита за електронна поща срещу вируси, шпионски софтуер, троянски кон, фишинг, adware, spyware и друг злонамерен код
- Проверка както на входяща, така и на изходяща електронна поща. Антиспам, антифишинг сканиране и защита от вируси с прилагане на различни методи на защита
- Автоматично обновяване на антивирусните дефиниции
- Карантиране на съмнителни писма в “Junk” пощенски кутии, която функционалност да се управлява от администраторите
- Използване на списъци за блокиране на писма от конкретни адреси и домейни.
- Интеграция с LDAP включваща повече от един LDAP сървъри

6.2.2. Слой 2 – Второ ниво на защита (ниво Microsoft Exchange пощенски кутии) със следните минимални изисквания:

- Сканиране на съобщенията при транзитно преминаване (входяща и изходяща поща) или пребиваване в пощенската кутия
- Защита в реално време за електронна поща срещу вируси, шпионски софтуер, троянски кон, фишинг, adware, spyware и други злонамерени атаки.
- Защита от непоискани имейли / спам
- Защита от нежелано съдържание или нежелани прикачени файлове
- Предпазва от заразяване на пощенските кутии по всяко време чрез непрекъснато сканиране за нови атаки, които може да са пропуснати от защитите от първо ниво, като например от имейл gateway/портал
- Защиатава от „нулев ден“ заплахи
- Обновяване на дефиниции
- Използване на предварително зададени правила, редовни изрази, критерии за прикачване, вярно писане на файлове и др.
- Следи за репутацията на файловете
- Прилагане на базата на Microsoft Active Directory® за опростяване управлението на политиките.
- Отдалечена инсталация, централизирана конфигурация на политиките на сървърна група, известия, сигнали, за издаване по разписание на консолидиран отчет.
- Интеграцията с Microsoft System Center Operations Manager

- Филтриране на съдържание в Microsoft Exchange Server 2016, 2019 като същевременно поддържа хоствани, виртуализирани среди на Microsoft Hyper-V® и VMware® виртуализирани Exchange сървъри.
- Анализира подробно състоянието на защита Microsoft Exchange.
- Да има способността за търсене и анализ на данни от карантина.
- 64-битов поддръжка
- Дава възможност за бързи актуализации на Micro Definitions Benefits
- Управление на множество пощенски сървъри MS Exchange през една конзола

6.2.3. Поддръжка:

Да е осигурена 24x7 поддръжка от производителя и да включва:

- Актуализации на софтуера и фърмуера
- Достъп до телефон или Web-базирана система при необходимост от консултации, свързани с базово конфигурирани или основни проблеми.
- Подмяна на хардуер, при излизане от строя на хардуерен модул.
- Срок на лиценз – 12 месеца

7. Опорен комутатор – 1 брой:

Параметър	Минимални технически изисквания
Вид	Управляем
Ниво на комутатора	L3
Електрическо захранване	100-240 VAC, 50-60 Hz
Монтаж	Монтиране в комуникационен шкаф
Етернет портове	28x Gigabit Ethernet: <ul style="list-style-type: none"> - 24x RJ-45 Ports - 4x Combo Ports (RJ-45 + SFP)
Пропускателна способност	41 Mpps
Капацитет за маршрутизиране/превключване	56 Gbps
L2 функционалност	Стандарти: 802.1d, 802.1w, 802.1s, IEEE 802.3ad Voice VLAN Layer 2 DHCP Relay IGMP versions 1, 2, and 3 snooping Loopback Detection Jumbo frames
VLAN	Брой активни VLANs: 4096 Стандарт: IEEE 802.1Q VLAN
Големина на адресната таблица	16 000
L3 функционалност	IPv4 routing IPv6 routing CIDR Layer 3 DHCP Relay L3 UDP Relay DHCP Server
Сигурност	SSH, SSL/TLS, IEEE 802.1X (Authenticator role) STP BPDU Guard, STP Root Guard, IP Source Guard Dynamic ARP Inspection, IP/MAC/Port Binding Филтрация по MAC адреси Уеб базирана автентикация

	DHCP snooping L2 PVE, Port security Storm control RADIUS/TACACS+ DoS prevention ACLs
Система за поддържане качеството на услугите (QoS)	Weighted Round-Robin (WRR) 802.1p/CoS 802.1p VLAN priority based Класификация и маркиране на ACLs
Мрежови стандарти	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad LACP, IEEE 802.3z Gigabit Ethernet, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w RSTP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, RFC 768, RFC 783, RFC 791, RFC 792, RFC 793, RFC 813, RFC 879, RFC 896, RFC 826, RFC 854, RFC 855, RFC 856, RFC 858, RFC 894, RFC 919, RFC 922, RFC 920, RFC 950, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1157, RFC 1350, RFC 1533, RFC 1541, RFC 1624, RFC 1700, RFC 1867, RFC 2030, RFC 2616, RFC 2131, RFC 2132, RFC 3164, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 2576, RFC 4330, RFC 1213, RFC 1215, RFC 1286, RFC 1442, RFC 1451, RFC 1493, RFC 1573, RFC 1643, RFC 1757, RFC 1907, RFC 2011, RFC 2012, RFC 2013, RFC 2233, RFC 2618, RFC 2665, RFC 2666, RFC 2674, RFC 2737, RFC 2819, RFC 2863, RFC 1157, RFC 1493, RFC 1215, RFC 3416
Методи за управление	Web UI, (HTTP/HTTPS), SNMP, CLI Отдалечено наблюдение Port и VLAN mirroring Актуализация на фърмуера Автоматично конфигуриране
Гаранция	Минимум 3 години