

Основные характеристики

Решение для комплексного управления

Маршрутизатор поддерживает функции автоматического переключения между WAN-соединениями после отказа (failover) и балансировки нагрузки, что делает данное устройство надежным, защищенным и гибким решением для сетевого управления.

Расширенный функционал VPN

Благодаря расширенному функционалу VPN, включая технологию IPSec Hub and Spoke, можно легко установить защищенное соединение между мобильными пользователями и офисами.

Web-аутентификация

Функция адаптивного портала позволяет легко пройти аутентификацию и авторизацию как сотрудникам, так и гостям.



DSR-500/1000

Гигабитный сервисный маршрутизатор с резервированием WAN портов

Функции

Высокопроизводительная сеть VPN

- Протоколы
 - IPSec, PPTP/L2TP, GRE
- VPN-туннели
 - DES
 - Hub and Spoke

Расширенные сетевые сервисы

- IPv6
- IEEE 802.1Q VLAN
- Мониторинг портов/Управление полосой пропускания
- IGMP Proxy, IGMP snooping
- Фильтрация Web-содержимого
- Web-аутентификация

Отказоустойчивость

- Функция автоматического переключения между WAN-соединениями после отказа и функция балансировки нагрузки

Унифицированные сервисные маршрутизаторы D-Link серии DSR представляют собой высокопроизводительные решения, обеспечивающие защиту сети и предназначенные для удовлетворения растущих потребностей малого и среднего бизнеса.

Возможности комплексного управления

Маршрутизатор DSR-500/1000 оснащен двумя WAN-портами Gigabit Ethernet. Применение функции балансировки нагрузки позволяет распределить исходящий трафик между двумя WAN-интерфейсами и оптимизировать производительность системы, обеспечивая, таким образом, бесперебойную работу сети. Второй WAN-порт может быть настроен как DMZ-порт, что позволяет изолировать серверы от сети LAN. Маршрутизатор DSR-500/1000 поддерживает возможность организации доступа к сети Интернет с помощью USB-модема¹ 3G или 4G². Балансировка нагрузки может быть осуществлена для 3G/4G-соединений, обеспечивая дополнительный уровень резервирования для критически важных данных и приложений резервного копирования.

Web-аутентификация

Функция адаптивного портала позволяет легко пройти аутентификацию и авторизацию как сотрудникам, так и гостям. Пользователи могут быть аутентифицированы с использованием локальной базы данных, RADIUS-сервера, LDAP, Microsoft Windows Active Directory, домена NT и сервера POP3. Одновременно можно настроить максимум четыре сервера.

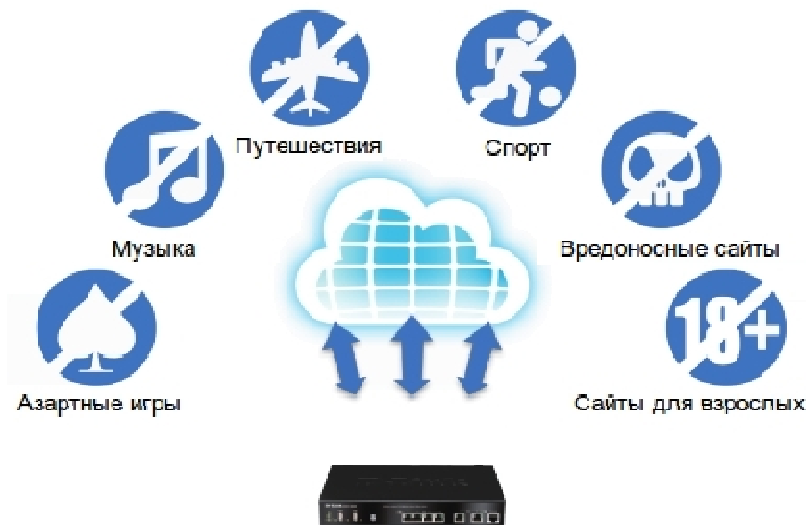
Расширенный функционал VPN

Виртуальная частная сеть (VPN) предоставляет мобильным пользователям и филиалам защищенный канал связи для подключения к корпоративной сети. DSR-500/1000 поддерживает туннели Generic Routing Encapsulation (GRE), обеспечивая мобильным пользователям удаленный доступ к центральной корпоративной базе данных. При создании Site-to-site VPN-туннелей используются протоколы IP Security (IPSec), Point-to-Point Tunneling Protocol (PPTP) или Layer 2 Tunneling Protocol (L2TP), применение которых упрощает процесс подключения удаленных пользователей и филиалов через зашифрованные виртуальные каналы.

Фильтрация Web-содержимого

Фильтрация Web-содержимого помогает администраторам осуществлять мониторинг, управление и контроль использования сотрудниками предоставленного им доступа к сети Интернет. Статическая фильтрация Web-содержимого позволяет удалить опасные объекты, такие как Java-апплеты, объекты ActiveX, файлы cookie, или блокировать URL-адреса по ключевому слову. Динамическая фильтрация Web-содержимого, требующая приобретения лицензии, позволяет администраторам фильтровать содержимое по списку категорий. DSR-500/1000 поддерживает несколько серверов глобальных индексов с миллионами URL-адресов и информацией в реальном времени о Web-сайтах, что позволяет увеличить производительность и обеспечить максимальную доступность сервиса.

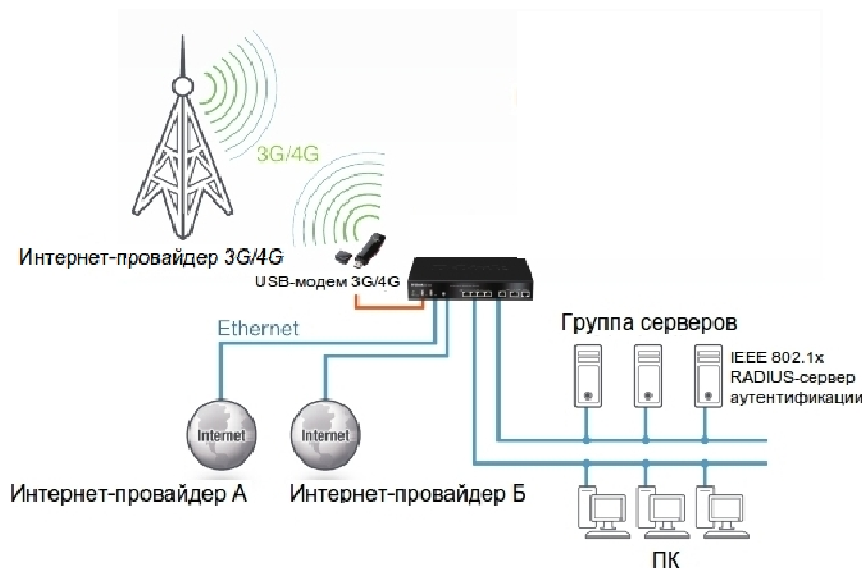
Фильтрация Web-содержимого для HTTP/HTTPS



Организация защищенной VPN-сети



Dual-WAN для резервного подключения к сети Интернет



Технические характеристики		
Модель	DSR-500	DSR-1000
Аппаратная версия	B1	
Аппаратное обеспечение		
Интерфейсы	<ul style="list-style-type: none"> • 2 порта WAN 10/100/1000Base-T • 4 порта LAN 10/100/1000Base-T • Порт USB 2.0 • Консольный порт с разъемом RJ-45 	<ul style="list-style-type: none"> • 2 порта WAN 10/100/1000Base-T • 4 порта LAN 10/100/1000Base-T • 2 порта USB 2.0 • Консольный порт с разъемом RJ-45
Индикаторы	<ul style="list-style-type: none"> • Питание/Статус • USB • LAN/WAN (Скорость/Статус) 	
Кнопки	<ul style="list-style-type: none"> • Кнопка Reset 	
Разъем питания	<ul style="list-style-type: none"> • Разъем для подключения питания (постоянный ток) 	
Производительность ³		
Пропускная способность межсетевого экрана ⁴	• 950 Мбит/с	• 950 Мбит/с
Пропускная способность VPN ⁵	• 200 Мбит/с	• 250 Мбит/с
Количество параллельных сессий	• 50 000	• 100 000
Количество новых сессий в секунду	• 500	• 1000
Политики межсетевого экрана	• 600	• 600

Гигабитный сервисный маршрутизатор с резервированием WAN портов

Сеть			
Тип интернет-соединения	<ul style="list-style-type: none"> • Статический/Динамический IP-адрес <ul style="list-style-type: none"> • PPPoE/L2TP/PPTP • Multiple PPPoE • Russian PPTP/L2TP (Dual Access) <ul style="list-style-type: none"> • Russian PPPoE (Dual Access) <ul style="list-style-type: none"> • 3G/4G² 		
Межсетевой экран	<ul style="list-style-type: none"> • Статический маршрут • Динамический маршрут: RIP v1/v2, OSPF, OSPFv3 <ul style="list-style-type: none"> • Dynamic DNS • Маршрутизация между VLAN <ul style="list-style-type: none"> • NAT, PAT • Фильтрация Web-содержимого: статический URL-адрес, ключевые слова, Dynamic WCF (требуется лицензия) • Система предотвращения вторжений (IPS): пакет сигнатур, входящий в комплект ПО <ul style="list-style-type: none"> • Аутентификация: внутренняя база данных, RADIUS, POP3, LDAP, AD, домен NT 		
Сетевые функции	<ul style="list-style-type: none"> • Сервер/Клиент DHCP <ul style="list-style-type: none"> • DHCP Relay • IEEE 802.1Q VLAN • VLAN (на основе порта) • IP Multicast: IGMP Proxy, IGMP Snooping <ul style="list-style-type: none"> • IPv6 • Функция автоматического переключения между WAN-соединениями после отказа (Route Failover) <ul style="list-style-type: none"> • Балансировка нагрузки (Outbound Load Balancing) • Резервирование 3G/4G² 		
Виртуальная частная сеть (VPN)	<table border="0" style="width: 100%;"> <tr> <td style="width: 50%; vertical-align: top;"> <ul style="list-style-type: none"> • VPN-туннели: 95 • IPSec-туннели: 35 • PPTP/L2TP-туннели: 25 <ul style="list-style-type: none"> • GRE-туннели: 15 • Методы шифрования: DES, NULL • Сервер IPSec/PPTP/L2TP <ul style="list-style-type: none"> • IPSec NAT Traversal • Обнаружение недействующих узлов • IP Encapsulating Security Payload (ESP) <ul style="list-style-type: none"> • IP Authentication Header (AH) • VPN Tunnel Keep Alive <ul style="list-style-type: none"> • Hub and Spoke </td> <td style="width: 50%; vertical-align: top;"> <ul style="list-style-type: none"> • VPN-туннели: 155 • IPSec-туннели: 70 • PPTP/L2TP-туннели: 25 <ul style="list-style-type: none"> • GRE-туннели: 20 • Методы шифрования: DES, NULL • Сервер IPSec/PPTP/L2TP <ul style="list-style-type: none"> • IPSec NAT Traversal • Обнаружение недействующих узлов • IP Encapsulating Security Payload (ESP) <ul style="list-style-type: none"> • IP Authentication Header (AH) • VPN Tunnel Keep Alive <ul style="list-style-type: none"> • Hub and Spoke </td> </tr> </table>	<ul style="list-style-type: none"> • VPN-туннели: 95 • IPSec-туннели: 35 • PPTP/L2TP-туннели: 25 <ul style="list-style-type: none"> • GRE-туннели: 15 • Методы шифрования: DES, NULL • Сервер IPSec/PPTP/L2TP <ul style="list-style-type: none"> • IPSec NAT Traversal • Обнаружение недействующих узлов • IP Encapsulating Security Payload (ESP) <ul style="list-style-type: none"> • IP Authentication Header (AH) • VPN Tunnel Keep Alive <ul style="list-style-type: none"> • Hub and Spoke 	<ul style="list-style-type: none"> • VPN-туннели: 155 • IPSec-туннели: 70 • PPTP/L2TP-туннели: 25 <ul style="list-style-type: none"> • GRE-туннели: 20 • Методы шифрования: DES, NULL • Сервер IPSec/PPTP/L2TP <ul style="list-style-type: none"> • IPSec NAT Traversal • Обнаружение недействующих узлов • IP Encapsulating Security Payload (ESP) <ul style="list-style-type: none"> • IP Authentication Header (AH) • VPN Tunnel Keep Alive <ul style="list-style-type: none"> • Hub and Spoke
<ul style="list-style-type: none"> • VPN-туннели: 95 • IPSec-туннели: 35 • PPTP/L2TP-туннели: 25 <ul style="list-style-type: none"> • GRE-туннели: 15 • Методы шифрования: DES, NULL • Сервер IPSec/PPTP/L2TP <ul style="list-style-type: none"> • IPSec NAT Traversal • Обнаружение недействующих узлов • IP Encapsulating Security Payload (ESP) <ul style="list-style-type: none"> • IP Authentication Header (AH) • VPN Tunnel Keep Alive <ul style="list-style-type: none"> • Hub and Spoke 	<ul style="list-style-type: none"> • VPN-туннели: 155 • IPSec-туннели: 70 • PPTP/L2TP-туннели: 25 <ul style="list-style-type: none"> • GRE-туннели: 20 • Методы шифрования: DES, NULL • Сервер IPSec/PPTP/L2TP <ul style="list-style-type: none"> • IPSec NAT Traversal • Обнаружение недействующих узлов • IP Encapsulating Security Payload (ESP) <ul style="list-style-type: none"> • IP Authentication Header (AH) • VPN Tunnel Keep Alive <ul style="list-style-type: none"> • Hub and Spoke 		
Управление			
Управление полосой пропускания	<ul style="list-style-type: none"> • Управление максимальной полосой пропускания • Управление приоритетной полосой пропускания: <ul style="list-style-type: none"> - QoS на основе порта - 3 класса 		
Управление системой	<ul style="list-style-type: none"> • Web-интерфейс • Командная строка • SNMP v1, v2c, v3 		
Функции USB			
Функции USB	<ul style="list-style-type: none"> • USB-модем¹ • Принт-сервер⁶ • Встроенный сервер Samba 		

