

## WATCHGUARD XTM 2050 NEXT-GENERATION FIREWALL



Решение WatchGuard XTM 2050 является высокопроизводительным межсетевым экраном нового поколения (New Generation Firewall - NGFW), которое обеспечивает всеобъемлющую защиту корпоративных сетей и высочайшую производительность. Решение WatchGuard XTM 2050 предназначено для крупных предприятий, головных офисов и центров обработки данных.

Межсетевые экраны WatchGuard NGFW обеспечивают высокую скорость обработки и фильтрации трафика. Кроме того, решения WatchGuard NGFW позволяют управлять приложениями, создавать VPN туннели методом «Drag & Drop», создавать клиентские SSL и IPSec VPN подключения, а также предоставляют обширнейшие возможности по наблюдению за трафиком пользователей, состоянием сети и соблюдением политик безопасности в режиме реального времени.

С решениями WatchGuard NGFW компании могут с высокой точностью контролировать соблюдение политик сетевой безопасности, что способствует уменьшению рисков, связанных с кражами интеллектуальной собственности или конфиденциальных данных.

### УПРАВЛЕНИЕ ПРИЛОЖЕНИЯМИ

- Возможность детализированного контроля над более чем 1 800 приложениями, что обеспечит высокую безопасность и производительность
- Используя более 2 300 сигнатур приложений и сложный анализ на поведенческом уровне, сервис Application Control позволяет увидеть, какие приложения используются в компании, кто их использует и когда
- Сервис Application Control позволяет системным администраторам устанавливать политики безопасности для пользователей и групп пользователей, разграничивая права пользователей относительно отдельных приложений, категорий приложений и отдельных функций приложений

### ПРЕДОТВРАЩЕНИЕ СЕТЕВЫХ АТАК (INTRUSION PREVENTION SYSTEM)

- Идентификация вредоносного программного обеспечения позволяет блокировать или регистрировать весь сомнительный сетевой трафик
- Сканирование сетевого трафика, проходящего по протоколам HTTP, HTTPS, FTP, TCP, UDP, DNS, SMTP и POP3 позволяет блокировать сетевые атаки и вредоносные приложения
- Постоянно обновляемая база данных сигнатур позволяет защищать сеть от новых видов угроз

## ТЕХНИЧЕСКИЕ СПЕЦИФИКАЦИИ ХТМ 2050

ХТМ 2050	
<b>ПРОПУСКНАЯ СПОСОБНОСТЬ</b>	
Пропускная способность МЭ (Гб/с)	20
Пропускная способность VPN (Гб/с)	2
Совокупная пропускная способность ХТМ (Гб/с)	10
Интерфейсы 10/100/1000	16
I/O интерфейсы	1 Serial 1 Management 2 USB
Число поддерживаемых узлов (LAN IPs)	Без ограничений
Количество одновременных сессий (bi-directional)	2 500 000
Количество поддерживаемых VLAN	500
<b>VPN ТУННЕЛИ</b>	
Branch Office VPN	10 000
Mobile VPN (IPSec/ SSL)	20 000
<b>ФУНКЦИИ БЕЗОПАСНОСТИ МЭ НОВОГО ПОКОЛЕНИЯ</b>	
Межсетевой экран	МЭ с запоминанием состояния, глубокий анализ уровня приложений, Proxy на уровне приложений
Proxy на уровне приложений	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3
Защита от угроз	Защита от угроз нулевого дня, блокировка шпионского ПО, DoS/ DDoS атак, фрагментированных и несформированных пакетов, смешанных угроз и много другого
VoIP	H.323, SIP, безопасность установки соединения и сессий
Подписки на дополнительные сервисы безопасности	Application Control, Intrusion Prevention Service, Gateway AntiVirus, Reputation Enabled Defense, spamBlocker, WebBlocker
<b>VPN И АУТЕНТИФИКАЦИЯ</b>	
Шифрование	DES, 3DES, AES 128/192/256-bit
IPSec	SHA-1, MD5, IKE pre-shared key, 3rd party cert
SSL	Тонкий клиент, Web exchange
PPTP	Сервер и транзитный трафик
VPN FailOver	Есть
Single Sign-On	Прозрачная аутентификация Active Directory
XAUTH	Radius, LDAP, Secure LDAP, Windows Active Directory
Другие виды аутентификации пользователей	VASCO, RSA SecurID, Web-based, Local, Microsoft Terminal Services and Citrix

**XTM 2050**

<b>СЕТЕВЫЕ ФУНКЦИИ</b>	
Операционная система	Fireware XTM PRO
Назначение IP адресов	Static, DynDNS, PPPoE, DHCP (server, client, relay)
Маршрутизация	Static, dynamic (BGP4, OSPF, RIP v1/v2), на основе политик
QoS	8 priority queues, diffserv, modified strict queuing
Поддержка VLAN	500 VLANs (bridging, tagging, routed mode)
Отказоустойчивый кластер	Active/passive, active/active с балансировкой нагрузки
NAT	Static, dynamic, 1:1, IPSec traversal, policy-based NAT, virtual IP
Другие функции	Независимые порты, WAN failover, Балансировка нагрузки, Режимы transparent/ drop-in
<b>МЕНЕДЖМЕНТ</b>	
Операционная платформа	WatchGuard System Manager (WSM) v11.5 или выше
Оповещения	SNMP v2/v3, Email, Management System Alert
Поддержка сервера	Логирование и отчеты о состоянии сервера, карантин, WebBlocker, управление
WebUI	Поддержка Windows, Mac, Linux, and Solaris OS
Интерфейс командной строки	Поддержка прямого доступа и скриптов
<b>СЕРТИФИКАЦИЯ</b>	
Содержание опасных веществ	WEEE, RoHS, REACH
Безопасность	ICSA, FIPS, EAL4 +
Охрана труда	NRTL/C, CB, CE

