

Get Next-Generation Firewall protection

Cyberoam NGFW offers Layer 8 (Identity-based) security, App Visibility & Controls, IPS, Web Filtering, VPN, On-appliance Reporting & Bandwidth Controls

NG Cyberoam
Future-Ready Security.



Сyberoam – управляй безопасностью с умом.

AGENDA

1. Профиль компании.
2. Сетевая безопасность на основе решений Cyberoam.
3. Cyberoam и конкуренты.
4. Модельный ряд: Виртуальные и Физические устройства.
5. Центральная Консоль Управления.
6. Лицензирование: выбор компонентов.
7. Аккумуляция положительного эффекта от внедрения решений Cyberoam.

Cyberoam - частная компания, специализирующаяся на сетевой безопасности с глобальным присутствием в более чем 125-ти странах, была основана в 1999 году двумя энтузиастами Хемалем Пателом и Беном Касадо. Руководствуясь концепцией обязательной идентификации пользователя (User Identity-based), как самого уязвимого звена сетевой безопасности и ориентации на эффективные, с точки зрения безопасности и минимизации издержек, решения, компания выросла из подразделения Elitecore Technologies до самостоятельной организации, удовлетворяющей нужды в безопасности и снижении расходов, организации любых размеров – будь то офис из десятка человек или целая корпорация. В настоящий момент, компания состоит из 450+ сотрудников и 4500+ партнеров по всему миру.



“... мы занимаем позиции лидерства на рынке, поэтому для нас важно продолжать следовать рыночной стратегии продвижения инновационных продуктов”.

Hemal Patel

ПРИЗНАНИЕ



СЕРТИФИКАЦИЯ



Компании, выбравшие

Финансовый



Производство



Правительство



Образование



Фармацевтика



Телеком



Введение

Cyberoam рассматривает сеть организации как единый механизм, требующий тщательного контроля и многоуровневой защиты ресурсов от внешних угроз, которым может быть подвержена организация любого масштаба - от малого офиса до крупной организации. Благодаря данному подходу, Cyberoam удовлетворяет требования самых взыскательных заказчиков.

Наиболее распространенными последствиями отсутствия должного уровня защиты сети являются:





Cyberoam awarded **patent** for its **Layer 8 technology**

**Our claim to inventing Identity-based
network security gets validated.**

Ключевая концепция



Модули Безопасности

Межсетевые экраны нового поколения от компании Cyberoam (Cyberoam NGFWs) обладают эффективным набором модулей безопасности, обеспечивающим беспрецедентный уровень защиты ресурсов организаций от различных типов угроз, среди которых:



Система обнаружения шпионского ПО и вредоносного кода, противодействие атакам “Pharming”



Система обнаружения и предотвращения вторжений в сети организации, противостояние DDoS -атакам



Контроль приложений, протоколов, посещаемых ресурсов в сети Интернет

WAF

Файервол для защиты веб-серверов и веб-приложений (WAF).



Управление пропускной способностью канала, приоритезация приложений



Безопасный удаленный доступ по VPN-каналу для пользователей и связи с филиалами



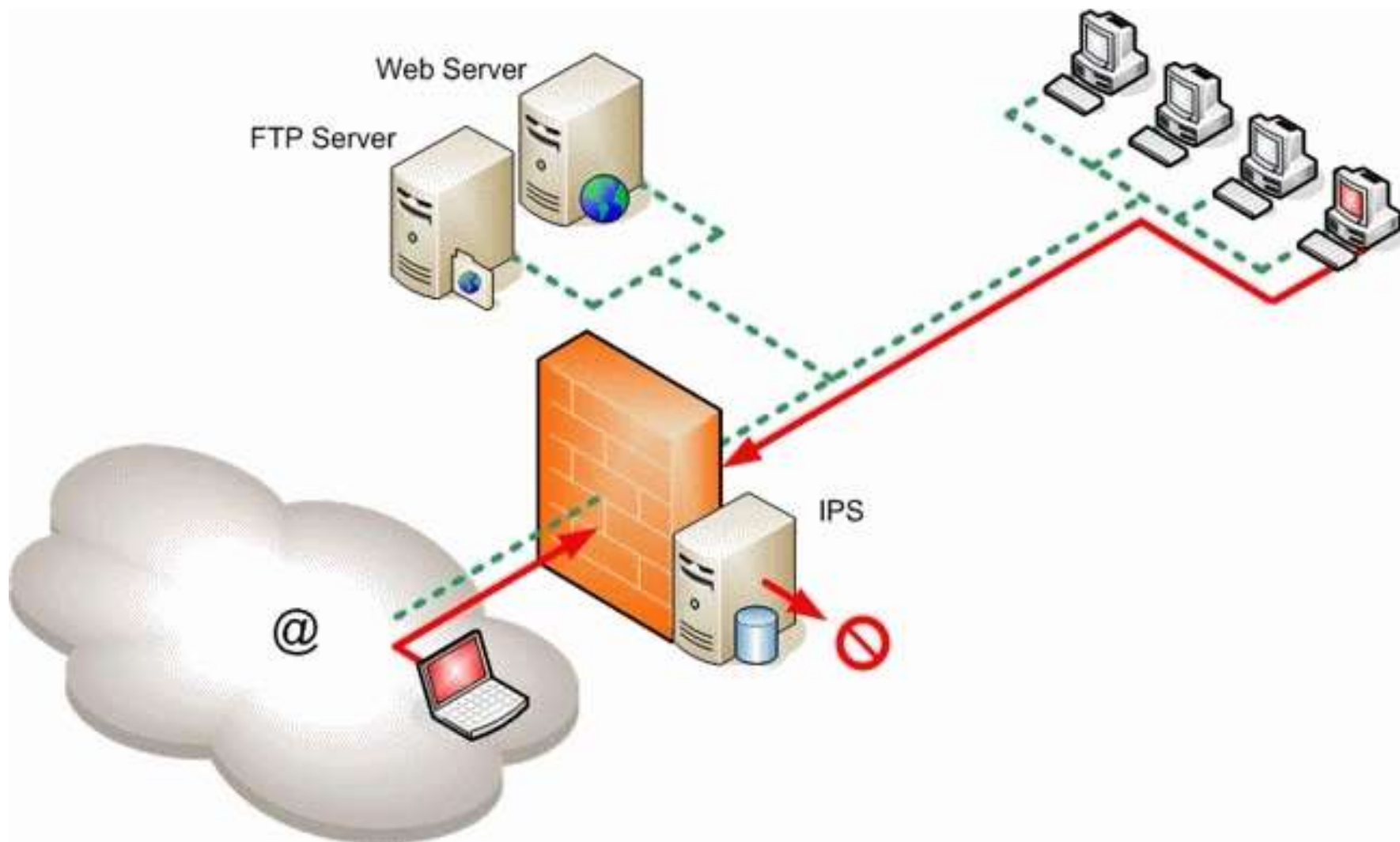
Встроенная система отчетности iView

Обнаружение Вредоносного Кода



Обновление антивирусных сигнатур каждые 30 минут!

Предотвращение Вторжений (IPS)



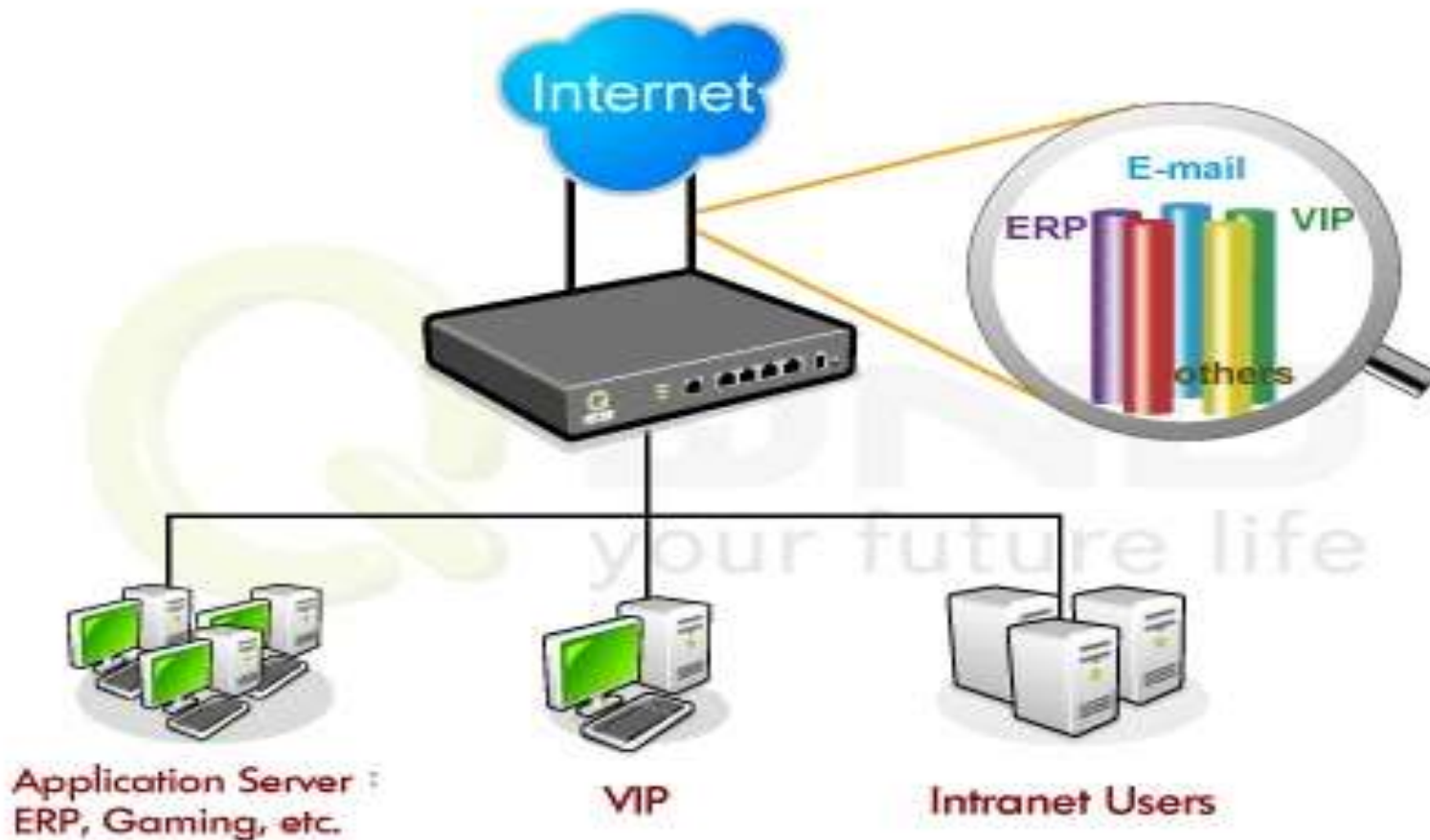


Файервол для защиты Веб-приложений

СYBEROAM WAF ПРОТИВОСТОИТ ВСЕМ АТАКАМ OWASP TOP 10 !

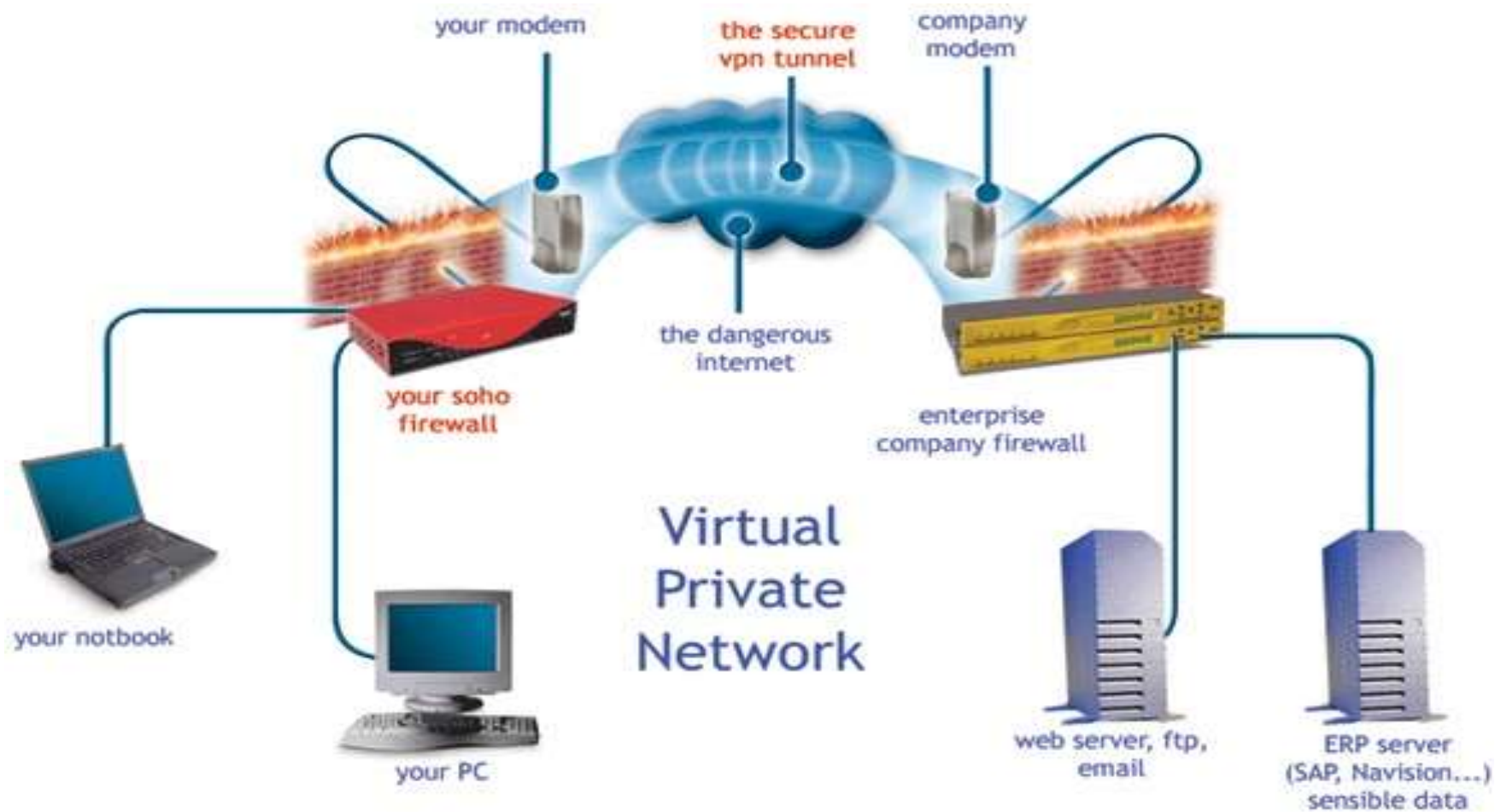


Управление пропускной способностью



QoS Bandwidth Management

Безопасный удаленный доступ



iView – Точка Контроля



Преимущества Cyberoam

1. Контроль доступа к Веб-ресурсам

Конкуренты Cyberoam используют некое абстрактное **«Облако»** для категоризации сайтов, к которому обращаются устройства, в то время как Cyberoam хранит ежедневно обновляемую базу сайтов внутри себя. Облачный же подход чреват созданием иллюзии безопасности и контроля, потому как:

- Большинство веб-ресурсов, принадлежат одновременно к нескольким категориям, что открывает лазейки для пользователей и усложняет контроль. К примеру, Mail.ru принадлежит одновременно к «Поисковым системам, Новостям, Веб-почте», оставив одну из категорий доступной, администратор открывает **Доступ ко всему**.
- Веб-ресурсы содержат встроенные в страницы коды, запускающие рекламные баннеры и небезопасные ссылки, которые невозможно вырезать через «Облако», в результате при закрытой категории **Запрещенные Ресурсы Доступны**.
- Отсутствует возможность создать собственные категории ресурсов и выделить их для отдельной группы пользователей. Другими словами, невозможно разрешить некоторое обучающее видео, вебинар и т.д. на Youtube и закрыть остальные данные, т.е. подход **«Все или Ничего»**.



Преимущества Cyberoam

2. Грануляция Политик Безопасности



**GOOD
NEWS!**

- CyberoamOS предоставляет беспрецедентный уровень контроля пользователей, позволяя создавать политики доступа к ресурсам, количеству допустимого времени использования Интернет, гарантированную пропускную способность, фильтрацию протоколов не только под группу пользователей, а под каждого отдельного пользователя. Данный функционал в ограниченном виде присутствует у конкурентов, причем в большинстве случаев процесс чрезмерно сложен и количество правил имеет граничное число.
- В полученных отчетах конкурентов в 90% вместо ID пользователя присутствует только IP-адрес, что значительно усложняет процесс установления инициатора нарушения политик безопасности, использовавший ограничения системы в свою пользу.
- Модули систем противодействия вторжениям (IPS) не обладают необходимым уровнем гибкости, так как могут содержать всего одну единую политику для анализа потока трафика, без возможности кастомизации, что значительно снижает производительность и глубину проверки входящих/исходящих пакетов.

Преимущества Cyberoam

3. Снижение издержек



- Cyberoam позволяет максимально снизить затраты на приобретение и поддержку оборудования, за счет предоставления **наиболее приемлемых цен** на рынке и простоты использования разработанных межсетевых экранов.
- Более **нет необходимости платить за L2TP VPN** для организации безопасного удаленного доступа каждого сотрудника – Cyberoam позволяет построить защищенное соединение без дополнительных плат за лицензии, даже с помощью встроенных в MS Windows VPN-клиентов.
- Многозадачность устройств Cyberoam решает проблему с мониторингом, поддержкой и настройкой множества различных сетевых устройств, а единая консоль управления упрощает сбор информации и управление всем парком межсетевых экранов Cyberoam.

Виртуальные Устройства

Cyberoam позволяет сократить число физических устройств безопасности за счет виртуализации и сократить издержки, связанные с монтажом изделия. Помимо стандартного набора функций виртуальные устройства Cyberoam могут быть установлены между гипервизором и виртуальной серверной фермой, тем самым гарантируя безопасность и защиту данного сегмента.



- CRiV-1C (Поддерживает до 1 vCPU)
- CRiV-2C (Поддерживает до 2 vCPU)
- CRiV-4C (Поддерживает до 4 vCPU)
- CRiV-8C (Поддерживает до 8 vCPU)
- CRiV-12C (Поддерживает до 12 vCPU)

Виртуальные платформы поддерживаемые устройствами Cyberoam:

- VMware ESX/ESXi
- VMware Workstation
- VMware Player
- Hyper-V

ПОПРОБУЙТЕ УЖЕ СЕЙЧАС БЕСПЛАТНЫЕ ВЕРСИИ ВИРТУАЛЬНЫХ УСТРОЙСТВ CYBEROAM !

Физические Устройства

ОБОРУДОВАНИЕ ДЛЯ ПРОВЕДЕНИЯ ПИЛОТНЫХ ЗАПУСКОВ ИМЕЕТСЯ В НАЛИЧИИ НА СКЛАДЕ!



Модельный ряд CR15iNG, CR25iNG, CR35iNG, CR50iNG, CR100iNG, CR200iNG, CR300iNG подойдет малым и средним организациям с количеством пользователей от 20 до 500 человек.



Модельный ряд CR300iNG-XP, CR500iNG-XP, CR750iNG, подойдет средним организациям с количеством пользователей от 500 до 2500 человек.



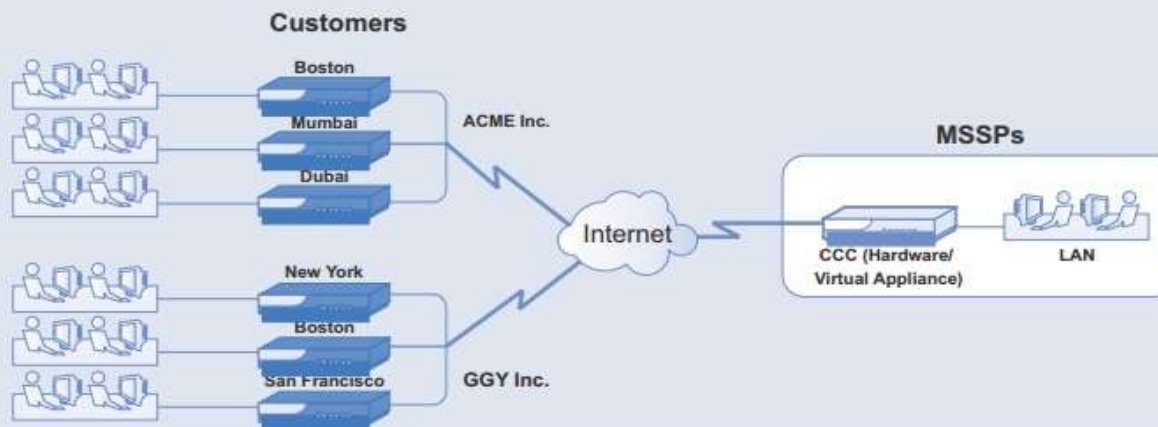
Модельный ряд CR1000iNG-XP, CR1500iNG-XP, CR2500iNG, CR2500iNG-XP подойдет крупным организациям с количеством пользователей в несколько тысяч человек.

Гбит

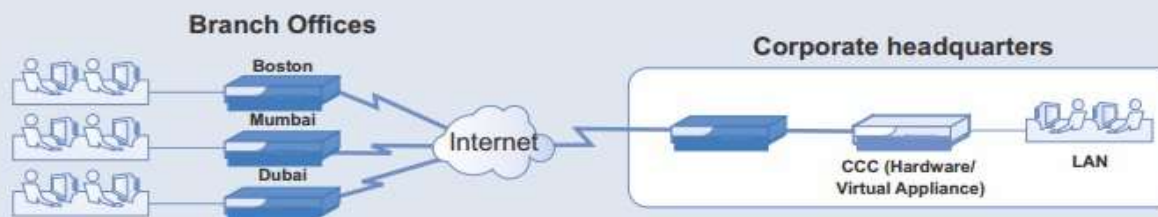
Центральная Консоль Управления



Cyberoam Central Console Deployment- MSSP



Cyberoam Central Console Deployment- Distributed Enterprise



Лицензирование

Перечень Подписок Безопасности

Comprehensive Value Subscription

- Anti Malware
- Anti Spam
- Web and Application Filter
- WAF
- Intrusion Prevention System
- 24x7 Support
- hardware warranty and RMA fulfillment

Total Value Subscription

- Anti Malware
- Anti Spam
- Web and Application Filter
- Intrusion Prevention System
- 8x5 Support
- hardware warranty and RMA fulfillment

Security Value Subscription

- Anti Malware
- Web and Application Filter
- Intrusion Prevention System
- 8x5 Support
- hardware warranty and RMA fulfillment

СВЯЖИТЕСЬ С НАМИ ДЛЯ ВЫБОРА ОПТИМАЛЬНОГО ВАРИАНТА!

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР НА ТЕРРИТОРИИ КАЗАХСТАНА

TOO «UNIFIED TECHNOLOGIES & TELECOMMUNICATIONS COMPANY»

ТЕХНИЧЕСКИЙ ЭКСПЕРТ

АБДУЛЛАЕВ ГАРИК

тел: +7 (727) 248-33-13, 225-02-80

моб: +7 701 887 79 27

e-mail: AG@UTTCCOM.UA

**ЗАКАЗАТЬ ПРОБНУЮ ВЕРСИЮ ИЛИ СОГЛАСОВАТЬ ПИЛОТНЫЙ ЗАПУСК
МОЖНО, СВЯЗАВШИСЬ ПО УКАЗАННЫМ ВЫШЕ КОНТАКТАМ**