

Connectra

Унифицированный шлюз для удаленного доступа и защиты web-инфраструктуры

Check Point Connectra™ - единственный шлюз удаленного доступа, сочетающий технологии SSL VPN, IPSec VPN, средства предотвращения вторжений с непревзойденным централизованным управлением и высокой гибкостью развертывания решения.

Теперь это решение предлагается с поддержкой шифрования по российскому алгоритму ГОСТ в дополнение к стандартным алгоритмам шифрования SSL. Российские компании получили возможность использовать лидирующее решение для организации защищенного доступа по SSL VPN, интегрируемого в инфраструктуру централизованного управления Check Point в комбинации с шифрованием трафика, использующим российские алгоритмы шифрования.



Решение Connectra позволяет мобильным и удаленным пользователям получить надежный удаленный доступ к корпоративным ресурсам, одновременно обеспечивая защиту сети и ее конечных точек от внешних угроз. Возможность выбора вариантов соединений в сочетании с встроенными средствами предотвращения вторжений и мощным централизованным управлением обеспечивают непревзойденный контроль настройки удаленного доступа и администрирования политик безопасности. Являясь первой линией защиты, Connectra предоставляет комплексную защиту рабочих станций и сетей от шпионского ПО и других вредоносных программ. IT-департаменты могут выбрать, приобрести продукт на аппаратной или программной платформе, или же как виртуальное устройство с превосходной гибкостью развертывания.

Конечные пользователи Connectra будут довольны удобством доступа и интуитивно понятным интерфейсом. SMS-аутентификация устраняет необходимость в хранении и управлении токенами и смарт-картами, когда потребуется двухфакторная аутентификация. Кроме того, благодаря Check Point Endpoint Connect теперь уже не требуется повторная аутентификация при роуминге между сетями. «Тонкий» клиент можно загружать и устанавливать непосредственно с портала Connectra. Конфиденциальность сеансов и защита от утечки данных при подключении с публичных компьютеров обеспечивается Check Point Secure Workspace. При необходимости высококонфиденциального доступа организуется виртуальный сеанс, по завершении которого происходит удаление всех данных сеанса и записей регистрационных журналов активности.

ПРЕИМУЩЕСТВА ПРОДУКТА

Шлюз с централизованным управлением

- Поддержка шифрования по алгоритму ГОСТ
- Не имеющий аналогов шлюз безопасного удаленного доступа, сочетающий технологии SSL VPN и IPSec VPN
- Встроенная система предотвращения вторжений и комплексная защита рабочих станций от шпионского ПО и других вредоносных программ
- Централизованное управление, которое интегрирует внедрение политик безопасности, администрирование клиента и ведение отчетности

Простота и удобство использования

- Check Point Secure Workspace обеспечивает безопасность сеансов и защиту от утечки данных при подключении к сети с общедоступного компьютера или из интернет-киоска
- Непрерывное соединение при роуминге между беспроводными сетями
- Автоматическое сканирование рабочих станций перед предоставлением доступа к сети
- Check Point является первым и единственным производителем, который предоставляет пользователям идентификационные коды в виде SMS-сообщений и устраняет тем самым необходимость в использовании смарт-карт и токенов

Гибкие возможности развертывания

- **Аппаратное устройство** - широкий спектр аппаратных устройств Connectra позволяет максимально удовлетворить требования предприятий по удаленному доступу с наиболее оптимальным соотношением цена/производительность
- **Программное обеспечение** Connectra можно установить на различные платформы на распространенных серверах, сертифицированных Check Point для запуска ОС SecurePlatform™
- **Виртуализированное устройство** - Connectra поддерживается на сервере VMware ESX как виртуализированное устройство, что позволяет снизить операционные расходы для поставщиков услуг управления (MSP), доступа в Интернет (IAP) и телекоммуникационных компаний

ШЛЮЗ С ЦЕНТРАЛИЗОВАННЫМ УПРАВЛЕНИЕМ

ЗАЩИЩЕННЫЙ ДОСТУП ЧЕРЕЗ WEB

Connectra представляет собой шлюз, с помощью которого удаленные пользователи могут получать доступ к ресурсам корпоративной сети через Web. Он обеспечивает доступ на сетевом уровне и через web по протоколу SSL. С помощью интегрированного web-портала Connectra пользователи могут обращаться к web-приложениям и ресурсам, а также получать доступ к разделяемым файлам и электронной почте. Для большего удобства, администраторы могут настраивать дизайн web-портала Connectra, который поддерживает работу на нескольких языках, в том числе на русском.

Для клиент-серверных приложений, не использующих Web, Connectra предлагает защищенный доступ на сетевом уровне через Web с помощью SSL Network Extender™. SSL Network Extender входит в комплект Connectra и представляет собой подключаемый модуль браузера, который осуществляет туннелирование трафика от клиентских приложений по SSL. Он поддерживает любые приложения на базе IP, включая ICMP, TCP и UDP, не требуя сложной настройки для работы каждого из них. SSL Network Extender не нужны даже права администратора на удаленном ПК.

ИНТЕГРИРОВАННЫЕ СРЕДСТВА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Имеющиеся в Connectra интегрированные средства предотвращения вторжений для доступа по SSL VPN помогают обеспечить целостность внутренних приложений. Интегрированные технологии Stateful Inspection, Web Intelligence™ и Application Intelligence™ предлагают защиту от враждебных действий и атак по SSL VPN. Например, Connectra может предотвратить доступ к конфиденциальным данным с помощью атак типа обхода каталогов или внедрения команд SQL, что особенно важно в условиях Extranet. Connectra также позволяет блокировать распространение червей по SSL VPN в случае, когда удаленный пользователь включил туннелирование по SSL VPN для разрешенных приложений. Кроме того, Connectra поставляется с годовой подпиской SmartDefense Services, обеспечивающей актуальность интегрированных средств защиты приложений.

ВСЕОБЪЕМЛЯЮЩАЯ ЗАЩИТА РАБОЧИХ СТАНЦИЙ

Благодаря интеграции с решением Integrity Clientless Security™, Connectra защищает сетевые ресурсы от угроз, исходящих от удаленных ПК, независимо от того, принадлежат они и/или используются сотрудниками или партнерами, клиентами либо другими гостевыми пользователями сети. Этот шлюз осуществляет сетевую политику безопасности для соединений SSL VPN, обеспечивает конфиденциальность сеансов и поддерживает безопасность организации.

- Чтобы гарантировать отсутствие на удаленных компьютерах вредоносных программ, перехватчиков клавиатурного ввода и троянских коней, Connectra выполняет сканирование на наличие этих и других шпионских программ через браузер удаленного пользователя. Благодаря тому, что доступ по SSL VPN предоставляется только после блокирования шпионских программ и выполнения базовых требований безопасности, Connectra позволяет предотвратить присвоение личной информации, хищение паролей и потерю данных. Кроме того, служба SmartDefense™ в режиме реального времени обеспечивает обновление правил проверки безопасности рабочих станций.

- Чтобы обеспечить безопасный доступ даже в неконтролируемой среде (например, аэропорту или интернет-киоски), Connectra предлагает Integrity Secure Workspace, который осуществляет шифрование файлов сеанса (включая электронную почту, присоединенные файлы, файлы cookies и пароли) на удаленном компьютере. Это предотвращает возможность просмотра или похищения конфиденциальной корпоративной информации даже после того, как сеанс завершен и пользователь оставил ПК.
- Connectra может обеспечивать выполнение политики доступа, требующей установки антивирусного программного обеспечения и/или межсетевое экран как условий предоставления доступа пользователям. Пользователи, чьи системы не соответствуют требованиям, получают ссылки на ресурсы для самостоятельного устранения проблем. Когда соответствие восстановлено, им разрешается вход в систему.
- Администраторы также могут с помощью Connectra ограничивать доступ к конкретным ресурсам в зависимости от уровня доверия к компьютеру и пользователю. Например, для одного набора ресурсов можно установить “высокий” уровень чувствительности и разрешать доступ только в случае, если удаленная рабочая станция обеспечивает сильную аутентификацию (например, с помощью электронных ключей) и на ней установлена и работает текущая версия антивирусной программы. Точно так же доступ к другому набору ресурсов можно разрешить только в случае, если используется Integrity Secure Workspace.

ЗАЩИТА ОТ НОВЫХ УГРОЗ

Оперативная доставка обновлений для шлюзов Connectra осуществляется через службу SmartDefense Services, обеспечивающую поддержание инфраструктуры безопасности Check Point в актуальном состоянии. Доставка через эту службу обновлений ПО и новейших рекомендаций по организации мер защиты и политикам безопасности позволяет нашим клиентам идти постоянно на шаг впереди эволюционирующих опасностей. Таким образом, средства предотвращения вторжений и защиты компьютеров конечных пользователей Connectra остаются постоянно на актуальном современном уровне.

МОЩНОЕ ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Управление Connectra может осуществляться централизованно с использованием сервера SmartCenter™ или отдельно через интуитивно понятный интерфейс. Централизованное управление обеспечивает непревзойденный контроль настройки удаленного доступа и администрирования политик безопасности и позволяет обходиться единым хранилищем определений индивидуальных пользователей и групп, сетевых объектов, прав доступа и политик безопасности по всей инфраструктуре безопасности и удаленного доступа. Единые политики доступа распространяются автоматически по всей распределенной среде, что делает возможным безопасное предоставление удаленного доступа из любого места.

Простота и удобство использования

ENDPOINT CONNECT VPN КЛИЕНТ

Check Point Endpoint Connect™ - новый, легкий клиент IPSec VPN для шлюзов Connectra. Endpoint Connect обеспечивает надежный защищенный удаленный доступ к корпоративным ресурсам сети и включен в каждую лицензию Connectra.

Традиционные VPN клиенты требуют повторного соединения и аутентификации и являются неудобными для мобильных пользователей. Endpoint Connect учитывает это – пользователи вводят свои данные повторно лишь при выходе ноутбука из «спящего режима» и при пере-

ходе на другие сети – с корпоративной проводной на беспроводную и GPRS. Подробную информацию по данной компоненте ПО можно найти на странице с описанием Endpoint Connect.

DYNAMICID™ - SMS-АУТЕНТИФИКАЦИЯ

Решение Connectra можно настроить для отправки пользователю одноразового пароля в виде SMS-сообщения на мобильный телефон. Двухфакторная аутентификация через SMS обеспечивает необходимый уровень безопасности, устраняя сложности, связанные с управлением и хранением токенов. Более подробную информацию можно найти на странице с описанием DynamicID.

ГИБКИЕ ВОЗМОЖНОСТИ РАЗВЕРТЫВАНИЯ

Connectra поставляется в виде аппаратного устройства или программного обеспечения для распространенных серверов. Список аппаратных компонентов и устройств приведен на сайте www.opsec.com.

- Аппаратное устройство Connectra: предустановленное программное обеспечение Connectra на сертифицированных аппаратных устройствах Check Point или OPSEC™
- Программное обеспечение Connectra для открытых серверов: Программное решение Connectra позволяет установить защищенную операционную систему Check Point SecurePlatform™
- Connectra поддерживается на сервере VMware ESX как виртуализированное устройство

Connectra устанавливается в демилитаризованной зоне или в доверенной ЛВС (локально-вычислительной сети). Продукт прост в установке и управлении. Поддерживается ряд схем аутентификации, в том числе с использованием LDAP-каталога, RADIUS, SecurID/ACE или внутренней базы данных.

ТЕХНИЧЕСКИЕ СПЕЦИФИКАЦИИ

ГИБКИЙ И НАДЕЖНЫЙ УДАЛЕННЫЙ ДОСТУП

Обеспечивается надежный SSL VPN доступ через браузер без использования клиентского ПО для широкого спектра приложений, а также мобильные IPSec соединения с использованием клиентского ПО для корпоративных пользователей

Удаленный доступ через браузер:

- Поддержка браузеров Internet Explorer, Mozilla и Safari
- Поддержка платформ Windows, Windows Mobile, Mac, iPhone и Linux
- SharePoint, SAP Portal и другие Web-приложения
- Outlook Web Access, Lotus iNotes и другие почтовые приложения
- Встроенный web-интерфейс для серверов POP3/IMAP
- Доступ к файловым серверам Windows (SMB/CIFS) для разделяемых файлов

Модули браузера на основе Java для доставки приложений по требованиям:

- Платформы Windows, Mac и Linux
- FTP, Jabber IM, RDP, SSH, Telnet, эмуляция терминала

Модули браузера для доставки приложений по требованиям:

- Поддержка платформ Windows, Mac и Linux
- SSL Network Extender в составе Connectra
 - Поддержка приложений: приложения на базе TCP, включая Citrix, MS RDP, Outlook, FTP и др.
 - Сетевые средства: все приложения на базе IP

НЕПРЕВЗОЙДЕННАЯ МОБИЛЬНОСТЬ

Непрерывное подключение к сети при переключении между сетями

Endpoint Connect - VPN клиент для ноутбуков и ПК

- SSL / IPSec клиент для платформ Windows 2000, XP и Vista
- Двухфакторная аутентификация с PKI, SecureID и SoftID
- Поддержка режима Office Mode (эффект присутствия в офисе)
- Встроенное сканирование рабочих станций на выполнение базовых требований безопасности и на наличие шпионских программ
- Автоматический выбор режима соединения (IPSec или SSL)
- Автоматическое восстановление связи при переключении между сетями
- Поддержка приложений на базе IP

SecureClient Mobile - VPN клиент для смартфонов и КПК

- Поддержка платформ Pocket PC 2003, Windows Mobile 5.x и 6.x
- Двухфакторная аутентификация с PKI, SecureID, SoftID
- SSL туннель с поддержкой роуминга и персональным межсетевым экраном
- Поддержка режима Office Mode (эффект присутствия в офисе)
- Контроль WAP, Bluetooth и другой периферии
- Интеграция с Outlook Mobile, установление туннеля по требованию для сохранения энергии
- Поддержка приложений на базе IP

Комплексная защита конечных точек сети

Защита рабочих станций по требованию, дополнительно - сканирование рабочих станций на выполнение базовых требований безопасности и на наличие шпионских программ

- Проверка подключаемых рабочих станций на соответствие корпоративной политике безопасности
- Обнаруживает наличие регистраторов клавиатурного ввода, троянских коней и другого шпионского ПО
- Пользователям, не прошедшим проверку, предлагаются ссылки на необходимые для восстановления ресурсы

Secure Workspace – устанавливает конфиденциальную VPN сессию даже при подключении с общественных компьютеров:

- Создает защищенное виртуальное окружение, изолированное от основной операционной системы
- Шифрует и удаляет всех данных сеанса и записей регистрационных журналов активности по завершении виртуального сеанса

ВСТРОЕННЫЕ СРЕДСТВА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Web Intelligence:

- Обеспечивает защиту от вредоносного кода в Web-приложениях
- Блокирует червей, различные атаки (например, на переполнение буфера), SQL-инъекции и др

Application Intelligence:

- Защищает трафик, переносимый по туннелям VPN, создаваемым SNX, Endpoint Connect и SecureClient Mobile
- Защита, включающая FTP, почтовые и другие IP-протоколы

ВЫСОКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ

ClusterXL (в составе Connectra) обеспечивает балансировку нагрузки и обеспечение высокой доступности

ПОВЫШЕННАЯ МАСШТАБИРУЕМОСТЬ

Connectra может поддерживать одновременно до 10 тысяч пользователей (модель Connectra 9072), а также работать на серверах высокой плотности

ОТКРЫТАЯ АРХИТЕКТУРА

Открытая архитектура позволяет использовать Connectra NGX R66 в качестве программно-аппаратного комплекса, программного обеспечения на открытом сервере или на платформе VMware.

	Connectra 270	Connectra 3070	Connectra 9072
Версия ПО Connectra	R66	R66	R66
Производительность			
Максимальное число одновременно работающих пользователей SSL	100	1 000	10 000
Максимальное число одновременно работающих пользователей IPSec	100	1 000	10 000
Ускорение оборудования SSL/IPSec	Нет	Нет	Да
Интерфейсы			
Встроенные интерфейсы	4 GbE (медный кабель)	10 GbE (медный кабель)	10 GbE (медный кабель)
Оптические интерфейсы	нет	нет	2 x 10 GbE Fiber (SR/LR) (single mode) 4 x 1 GbE Fiber SR (single mode)
Число сетей VLAN	256	256	256
Емкость устройства хранения данных			
Размер	160 Гб	160 Гб	2 x 160 Гб
Тип	Встроенный	Встроенный	Вынимаемый, возможность «горячей замены»
Размеры			
Корпус	1U	1U	2U
Габаритные размеры (стандартные)	16,8 x 10 x 1,73 дюйма	17,4 x 15 x 1,73 дюйма	17 x 20 x 3,46 дюйма
Габаритные размеры (метрические)	429 x 255 x 44 мм	443 x 381 x 44 мм	431 x 509,5 x 88 мм
Масса	3,7 кг (8,1 фунта)	6,5 кг (14,3 фунта)	16,5 кг (36,3 фунта)
Питание			
Двойные источники питания с возможностью «горячей замены»	Нет	Нет	Да
Входное питание	65 Вт (макс.)	250 Вт (макс.)	400 Вт (макс.)
Условия окружающей среды	Температура: от 5 до 40°C, влажность: от 10 до 85% без конденсации, высота над уровнем моря: 2500 м		
Соответствие стандартам	UL 60950; FCC часть 15, подчасть В, класс А; EN 55024; EN 55022; VCCI V-3 AS/NZS 3548:1995; CNS 13438 класс А (испытания успешно проведены; ожидается утверждение государственными органами); KN22, серия KN61000-4, ТТА; IC-950; ROHS		

Технические характеристики ПО

ПО Connectra - программное решение для открытых серверов. Операционная система SecurePlatform™ и программы Connectra устанавливаются менее чем за 10 минут.

ПО Connectra и SecurePlatform тестируются на совместимость с широким спектром аппаратных платформ. Информацию об этом можно найти на странице сайта: Connectra Hardware Compatibility (<http://www.checkpoint.com/services/techsupport/hcl/connectra.html>).

Минимальные требования к аппаратному обеспечению для установки ПО Connectra	
Процессор	Intel Celeron 2.4Гц
Память	512Мб
Дисковое пространство	10Гб на жестком диске

Технические характеристики виртуального устройства

Connectra поддерживается на сервере VMware ESX как виртуализированное устройство

Данная конфигурация сертифицирована Check Point и рекомендуется к использованию с SecurePlatform

Память (минимальный размер)	512Мб
Гостевая операционная система	RHEL 5.0 (32-bit)
Адаптер SCSI, поддерживаемый гостевой ОС	LSI Logic
Минимальное свободное место на диске	12 Гб

АДРЕСА И ТЕЛЕФОНЫ CHECK POINT

Международная штаб-квартира

5 Ha'Soleim Street, Tel Aviv 67897, Israel | Телефон: +972-3-753-4555 | Факс: +972-3-624-1100 | Эл. почта: info@checkpoint.com

Представительство в России и СНГ

Check Point Software Technologies (Russia) ООО | 109240, Москва, ул. Николаямская, д.13, стр.17 | Тел./факс: +7 495 967 7 444 | <http://rus.checkpoint.com>

©2003-2009 Check Point Software Technologies Ltd. Все права сохранены. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, логотип Check Point, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, Firewall-1, Firewall-1 GX, Firewall-1 SecureServer, FloodGate-1, Full Disk Encryption, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, логотип puresecurity, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartL.SM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, логотип totalsecurity, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs и логотип Zone Labs представляют собой товарные знаки или зарегистрированные товарные знаки компании Check Point Software Technologies Ltd. или ее подразделений. ZoneAlarm принадлежит компании Check Point Software Technologies, Inc. Все другие упоминаемые здесь названия продуктов являются товарными знаками или зарегистрированными товарными знаками соответствующих владельцев. Продукты, описанные в данном документе, защищены патентами США № 5 606 668, 5 835 726, 5 987 611, 6 496 935, 6 873 988, 6 850 943 и 7 165 076, а также могут быть защищены иными патентами США или других стран либо патентными заявками.