Cisco Systems
МОГУЩЕСТВО СЕТЕВЫХ ТЕХНОЛОГИЙ. сегодня.

ЗАЩИТИТЬ БИЗНЕС. сейчас

(издание III)

РЕШЕНИЯ CISCO ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вы стоите перед выбором, кому доверить решение возникших проблем и сложностей в области обеспечения информационной безопасности Вашей корпоративной сети и ее ресурсов? Вы считаете, что компания Cisco Systems известна только своими сетевыми решениями и технологиями? Вы не знаете, какие решения предлагает компания Cisco в области защиты информации? Вы не знаете, где расположить средства защиты? Вы не знаете, как реагировать на обнаруженные атаки и несанкционированные действия? Вы не знаете, имеют ли продукты компании Cisco сертификаты по требованиям информационной безопасности? Вы не знаете, какому партнеру компании Cisco доверить решение стоящих перед Вами задач?

Надеемся, что чтение данной брошюры будет для Вас не пустым времяпрепровождением и она поможет ответить на все эти и многие другие вопросы.

НАШИ ОТВЕТЫ НА ВАШИ ВОПРОСЫ

ПОЧЕМУ ИМЕННО CISCO SYSTEMS?

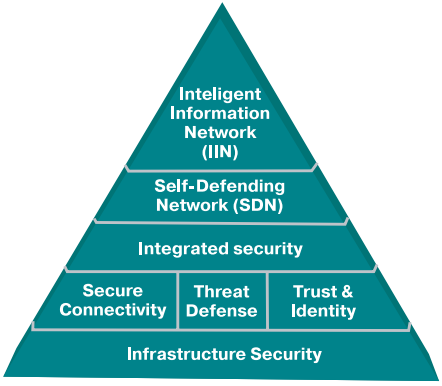
Компания Cisco Systems, признанный лидер в области сетевых решений, предлагает также широкий выбор продуктов в области обеспечения информационной безопасности – от межсетевых экранов и систем предотвращения атак до средств контроля содержимого, защиты приложений и систем персональной защиты серверов и рабочих станций. В каждой из этих областей компания Cisco Systems достигла лидирующих позиций и занимает первые места не только на мировом рынке, но также и в России и странах СНГ.

Такое положение было бы невозможно без исследований и разработок, на которые ежегодно тратится свыше 300 миллионов долларов – больше, чем зарабатывают в год многие другие поставщики рынка информационной безопасности.

Принимая во внимание, что компания Cisco Systems работает во многих странах мира, мы учитываем специфику каждого государства. В России наши решения проходят сертификацию в соответствующих регулирующих органах, например, в Федеральной службе по техническому и экспортному контролю (бывшая Государственная техническая комиссия при Президенте России). В частности, решения компании Cisco имеют свыше 150 сертификатов по требованиям информационной безопасности, что существенно превышает число сертификатов, полученных какой-либо другой компанией (российской или зарубежной), работающей на рынке информационной безопасности.

Работая на территории такой страны, как Россия, невозможно не учитывать различные часовые пояса и огромную территорию, на которой могут располагаться сети наших заказчиков. Несмотря на это, все они могут быть уверены в получении своевременной помощи. Это достигается за счет удаленной круглосуточной технической поддержки и гарантии замены вышедшего из строя оборудования со сроком замены до 4-х часов (в Москве и Санкт-Петербурге) и с отгрузкой в день авторизации замены (для остальных регионов).

СТРАТЕГИЯ CISCO В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Уверенность в том, что бизнес-процессы и ресурсы компании защищены от посягательств злоумышленников и воздействия вредоносных программ, является критическим фактором в современном мире.

Компания Cisco Systems, в отличие от других поставщиков, предлагает своим заказчикам не точечные продукты для защиты отдельных участков корпоративной сети, а комплексное решение, интегрируемое в инфраструктуру предприятия для обеспечения информационной безопасности бизнеса на всех уровнях. Это решение включает в себя не только лучшие в своем классе защитные средства, но также опирается на механизмы, интегрированные в каждую технологию и продукты компании Cisco, будь то беспроводные сети, IP-телефония, системы хранения данных, Metro Ethernet, системы управления и т.п. И, наконец, решение Cisco было бы неполным без квалифицированной помощи высококвалифицированных экспертов, включающихся в процесс построения защищенной сети на всех этапах ее жизненного цикла.

Self-Defending Network (SDN) – стратегия компании Cisco Systems, нацеленная на защиту бизнес-процессов в условиях растущей угрозы со стороны вредоносных программ и злоумышленников, воздействующих на бизнес-процессы изнутри и извне. Учитывая скорость распространения современных угроз, например червей и вирусов, средства защиты компании Cisco Systems строятся на основе проактивного подхода, заключающегося в предвосхищении угроз, а не в борьбе с их последствиями. В основе SDN лежит интеграция механизмов безопасности в сетевую инфраструктуру, в которой все ее элементы – от персонального компьютера до сетевого оборудования – участвуют в процессе обеспечения защищенности, устойчивости и непрерывности бизнеса. Стратегия Self-Defending Network заключается в автоматизации процесса обеспечения информационной безопасности за счет обнаружения угроз, реагирования соответственно уровню критичности, изолирования зараженных или взломанных серверов и рабочих станций и реконфигурации сетевых устройств с целью предотвращения повторных атак.

Дополнительная информация: http://www.cisco.com/go/sdn

ПОСТРОЕНИЕ САМОЗАЩИЩАЮЩЕЙСЯ СЕТИ

Построение самозащищающейся сети зависит от правильного применения совокупности трех основных элементов. Это:

- **Защита от вторжений (Threat Defense)**. Наиболее эффективная защита бизнес-ресурсов от злоумышленников и вредоносных программ достигается только в случае эшелонированной обороны, распределенной по всей сети, а не сосредоточенной в одной точке. Стратегия Threat Defense System интегрирует различные защитные механизмы в маршрутизаторы и коммутаторы, предлагает выделенные защитные устройства для разграничения доступа, отражения атак, контроля контента (включая защиту от спама) и безопасности приложений, а также позволяет защищать конечные устройства, такие как серверы и рабочие станции, от широкого спектра угроз.

  Подробнее о стратегии Threat Defence System смотрите на стр. 7

- **Защищенное взаимодействие (Secure Connectivity)**. Рост филиальной сети, числа надомных работников, возросшая мобильность пользователей требуют обеспечения защиты данных, передаваемых по открытым каналам связи (например, через Интернет). Сохранение конфиденциальности и целостности данных является обязательным элементом современных бизнес-приложений. Это требование достигается за счет стратегии Cisco Secure Connectivity System, которая, используя механизмы шифрования и аутентификации, одинаково эффективно защищает данные, голос и видео, передаваемые как по проводным, так и по беспроводным соединениям. Составной частью Secure Connectivity System являются такие технологии, как IPSec, SSL, SSH, GRE и MPLS.

  Подробнее о стратегии Secure Connectivity Solution смотрите на стр. 39

- **Идентификация и управление доверием (Identity & Trust Management System)**. Прежде чем пользователь, приложение или устройство получат доступ к необходимым ресурсам, они должны быть опознаны средствами защиты. Именно эту задачу на сетевом уровне решают технологии и средства, входящие в стратегию Identity & Trust Management System – Cisco Secure Access Control Server (ACS), Cisco Access Registrar, Cisco Secure User Registration Tool, а также технологию Network Admission Control.

  Подробнее о стратегии Identity & Trust Management System смотрите на стр. 33

THREAT DEFENSE SYSTEM

Стратегия Threat Defense System призвана обеспечить защиту любого элемента инфраструктуры, начиная от пользовательских компьютеров (включая лэптопы) и серверов и заканчивая сетевым оборудованием и целыми сетевыми сегментами, от известных и неизвестных атак. Достигается это за счет проактивного подхода, позволяющего своевременно обнаружить и отразить разнообразные атаки с помощью эшелонированной обороны, включающей ряд технологий и решений, таких как:

Межсетевые экраны (МСЭ)
- Широкий модельный ряд выделенных защитных устройств
- Интегрированные в маршрутизаторы и коммутаторы МСЭ

Системы предотвращения атак (IPS)
- Выделенные устройства обнаружения и предотвращения атак, включая средства защиты от DoS- и DDoS-атак
- Интегрированные в маршрутизаторы, коммутаторы и МСЭ системы IPS и отражения DoS-атак
- Интегрированная в точки беспроводного доступа система обнаружения атак

Защита серверов, ПК и лэптопов
- Эффективная защита компьютера на сетевом и прикладном уровнях
- Всесторонний контроль приложений
- Блокирование утечки информации

Контроль контента
- Контроль доступа к Web-серверам
- Блокирование Интернет-пейджеров (IM) и P2P-сетей
- Аутентификация пользователей при доступе к Web-ресурсам
- Контроль спама
- Защита XML-приложений

Интегрированная защита
- Более ста интегрированных в маршрутизаторы, коммутаторы и точки беспроводного доступа защитных функций и механизмов
- Многофункциональные устройства, объединяющие функции МСЭ, IPS, VPN, сетевого антивируса и т.д.

Дополнительная информация: *http://www.cisco.com/go/tds*

CISCO PIX FIREWALL

Программно-аппаратный межсетевой экран (МСЭ) Cisco Pix Firewall – лидер мирового рынка – обеспечивает многоуровневую защиту, используя широкий набор интегрированных защитных возможностей, включая контроль состояния с помощью алгоритма адаптивной защиты Adaptive Security Algorithm и глубокий анализ сетевых и прикладных протоколов с помощью механизма Deep Packet Inspection.

Широкий спектр моделей Cisco Pix Firewall, ориентированных на защиту различных категорий заказчиков, начиная от надомных пользователей и предприятий малого/среднего бизнеса и заканчивая крупными корпорациями и операторами связи, обеспечивает безопасность, производительность и надежность сетей любого масштаба.

Основные возможности

- Производительность до 1,67 Гбит/сек
- Поддержка технологии VPN
- Встроенная система обнаружения атак
- Фильтрация URL и блокирование ПО для Instant Messaging (IM) и P2P
- Поддержка протокола GTP/GPRS
- Прозрачный МСЭ второго уровня
- «Виртуальные» МСЭ
- Отказоустойчивость (включая поддержание VPN-туннелей)
- Скрытие топологии защищаемой сети с помощью трансляция адресов (NAT) и портов (PAT)
- Контроль всего спектра протоколов для IP-телефонии и мультимедиа – H.323, SIP, SCCP, MGCP, RTSP и т. д.
- Поддержка IPv6

Дополнительная информация: *http://www.cisco.com/go/pix*

МНОГООБРАЗИЕ МОДЕЛЕЙ CISCO PIX FIREWALL

	Pix 501	Pix 506E	Pix 515E	Pix 525	Pix 535
Производительность, Мбит/сек	60	100	190	330	1667
Максимальное число соединений	7500	25 000	130 000	280 000	500 000
Количество одновременно поддерживаемых сессий	19 500	53 000	176 000	625 000	1 000 000
Поддерживаемые физические интерфейсы	1 x 10/100 Ethernet и 4-портовый коммутатор 10/100	2 x 10/100 Ethernet	До 6 x 10/100 Ethernet	До 8 x 10/100/1000 Ethernet	До 10 x 10/100/1000 Ethernet
Поддерживаемые логические интерфейсы VLAN 802.1q	0	0	8	10	24
Производительность VPN (Triple DES / AES-128), Мбит/сек	3/4,5	16/30	135/130*	145/135*	425/495*
Максимальное число VPN-туннелей	10	25	2000*	2000*	2000*

* С VPN Acceleration Card (VAC+).

CISCO FIREWALL SERVICES MODULE

Сервисный модуль FWSM, реализующий функции межсетевого экрана, – это высокопроизводительное интегрированное защитное решение для коммутаторов Catalyst 6500 и маршрутизаторов Cisco 7600. Этот модуль обеспечивает самую высокую в индустрии производительность – 5,5 Гбит/сек (с возможностью увеличения до 20 Гбит/сек), 1 млн одновременно обрабатываемых соединений, 100 000 соединений в секунду. Данное уникальное решение, не имеющее аналогов на рынке, ориентировано на защиту центров обработки данных, операторов связи и штаб-квартир крупных компаний.

Основные возможности

- Базируется на зарекомендовавшей себя временем операционной системе реального времени PixOS
- Поддержка до 4096 VLAN на один модуль
- Создание политик для отдельных VLAN
- Механизм виртуализации (до 100 виртуальных межсетевых экранов)
- Тесная интеграция с модулями обнаружения атак, построения IPSec VPN и работы с SSL
- Защита от подмены MAC/IP-адресов (ARP Spoofing)
- Отказоустойчивость и высокая доступность
- Возможность ограничения использования ресурсов
- Ролевое управление конфигурацией модуля
- Группирование сетевых объектов и сервисов для списков контроля доступа (ACL)
- Масштабирование до 4-х модулей на один коммутатор
- Снижение совокупной стоимости владения за счет интеграции FWSM в уже установленные сети Catalyst 6500

Дополнительная информация: *http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html*

CISCO IOS FIREWALL

Программное обеспечение Cisco IOS Firewall – это межсетевой экран с контролем состояния, интегрированный в операционную систему Cisco IOS и поддерживаемый на широком спектре моделей маршрутизаторов Cisco 800, 1600, 1700, 1800, 2500, 2600, 2800, 3600, 3700, 3800, 7100, 7200, 7400, 7500, 7600 и коммутаторах Catalyst 6500.

Cisco IOS Firewall использует эффективный механизм, называемый Context Based Access Control (CBAC), позволяющий контролировать информационные потоки, проходящие через маршрутизатор, на всех уровнях, начиная с сетевого и заканчивая прикладным. На всех уровнях фильтрация осуществляется динамически, основываясь на направлении трафика, состоянии соединения и информации о предыдущих пакетах и сессиях, обработанных маршрутизатором с Cisco IOS Firewall.

Основные возможности

- Поддержка большого числа протоколов, включая мультимедиа
- Поддержка протокола IPv6
- Поддержка различных механизмов аутентификации – RADIUS, TACACS+ и т. д.
- Контроль доступа по времени
- Тесная интеграция с механизмами обнаружения атак, контроля качества (QoS) и построения VPN
- Поддержка различных политик и списков контроля доступа для разных интерфейсов
- Поддержка анализа протоколов на нестандартных портах
- Трансляция сетевых адресов
- Блокирование Java-апплетов
- Поддержка отказоустойчивости за счет динамической смены маршрута на резервный маршрутизатор
- Механизм прозрачности МСЭ (функционирование на канальном уровне)
- Расширенная регистрация событий безопасности

Дополнительная информация: *http://www.cisco.com/go/firewall*

CISCO IDS/IPS

Cisco IDS/IPS является центральным компонентом решений Cisco Systems по отражению атак. На базе данного ПО построены системы обнаружения атак Cisco IDSM-2, Cisco IDS Network Module и Cisco IOS IPS. Наряду с традиционными механизмами в Cisco IDS/IPS используются и уникальные алгоритмы, отслеживающие аномалии в сетевом трафике и отклонения от нормального поведения сетевых приложений. Это позволяет обнаруживать как известные, так и многие неизвестные атаки.

Встроенные технологии корреляции событий безопасности Cisco Threat Response, Threat Risk Rating и Meta Event Generator не только помогают существенно снизить число ложных срабатываний, но и позволяют администраторам реагировать лишь на действительно критичные атаки, которые могут нанести серьезный ущерб ресурсам корпоративной сети.

Основные возможности

- Широкий спектр алгоритмов обнаружения атак (сигнатуры, аномалии, эвристика, отклонения от RFC и т. п.)
- Защита от методов обхода
- Возможность работы одновременно в двух режимах – обнаружения и предотвращения атак
- Обнаружение атак в IP-телефонии
- Обнаружение IM в Web-трафике
- Технология микромодулей T.A.M.E. для каждого типа обнаруживаемых атак
- Автоматический выбор реагирования в зависимости от степени угрозы
- Интеграция с IDS/IPS других производителей с помощью протокола SDEE
- Производительность – 8 Гбит/сек в кластере

Дополнительная информация: *http://www.cisco.com/go/ips*

МНОГООБРАЗИЕ МОДЕЛЕЙ CISCO IDS/IPS

	IDS 4215	IPS 4240	IPS 4255	IDS 4250-XL
Производительность, Мбит/сек	80	250	600	1000
Интерфейс для мониторинга	10/100BASE-Tx	Четыре 10/100/1000 BASE-TX	Четыре 10/100/1000 BASE-TX	Два 1000 BASE-SX с MT-RJ
Опциональный интерфейс для мониторинга	Четыре 10/100BaseTx (всего 5 интерфейсов)	Четыре 10/100/1000BaseTx (всего 8 интерфейсов) или четыре оптических 1000BASE SX	Четыре 10/100/1000BaseTx (всего 8 интерфейсов) или четыре оптических 1000BASE SX	1000BASE-SX (оптика)
Размер шасси	1RU	1RU	1RU	1RU
Дополнительный блок питания	Нет	Нет	Нет	Да
Мониторинг отказов • линии связи • соединения • сервиса • устройства	 Да Да Да Да	 Да Да Да Да	 Да Да Да Да	 Да Да Да Да

CISCO INTRUSION DETECTION SERVICES MODULE

Компания Cisco Systems – единственный производитель в мире, выпускающий решение по обнаружению и предотвращению атак, интегрируемое в коммутаторы локальных сетей. Модуль IDSM-2, разработанный Cisco, устанавливается в шасси коммутатора Catalyst 6500 и обеспечивает мониторинг сетевых соединений, проходящих через него.

Основные возможности

- Базируется на зарекомендовавшем себя временем программном коде системы Cisco IDS/IPS
- Производительность – 600 Мбит/сек, 500 000 одновременно обрабатываемых соединений
- Отсутствие снижения производительности коммутатора
- Отражение атак канального уровня
- Возможность мониторинга неограниченного контроля сетевых сегментов и VLAN
- Мониторинг отказов соединения, сервиса и устройства
- Защищенное обновление сигнатур атак
- Возможность работы в двух режимах – обнаружения и предотвращения атак
- Тесная интеграция с модулями межсетевого экранирования и построения IPSec VPN и обработки SSL
- Единое управление с сенсорами Cisco IDS/IPS, межсетевыми экранами и средствами построения VPN
- Управление с помощью IDS Device Manager или CiscoWorks VPN Security Management Solution

Дополнительная информация: *http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/index.html*

CISCO IDS NETWORK MODULE

Cisco IDS Network Module – единственное на рынке решение для обнаружения атак, предназначенное для интеграции в маршрутизаторы. Этот модуль, устанавливаемый в слот маршрутизаторов Cisco 2600XM, 2691, 2800, 3660, 3700 и 3800, обнаруживает вредоносную активность в трафике, проходящем через периметр удаленного филиала или небольшого офиса.

Основные возможности

- Базируется на зарекомендовавшем себя временем программном коде системы Cisco IDS/IPS
- Производительность – от 10 Мбит/сек для Cisco 2600XM до 45 Мбит/сек для Cisco 3700
- Широкий выбор настраиваемых параметров для каждой сигнатуры атак
- Поддержка трафика VLAN 802.1q
- Интеграция со всеми защитными функциями операционной системы IOS маршрутизатора
- Автоматизированное обновление сигнатур
- Мониторинг отказов соединения, сервиса и устройства
- Разрыв соединения, а также реконфигурация межсетевого экрана, маршрутизатора или коммутатора для блокирования атаки
- Защищенное управление с помощью SSH, SSL и IPSec
- Единое управление с сенсорами Cisco IDS/IPS, межсетевыми экранами и средствами построения VPN
- Управление с помощью IDS Device Manager или CiscoWorks VPN Security Management Solution

Дополнительная информация:
http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_data_sheet09186a008017dc22.html

CISCO ADAPTIVE SECURITY APPLIANCE

Многофункциональный программно-аппаратный комплекс Cisco ASA 5500 предназначен для решения сразу нескольких задач – разграничение доступа к сетевым ресурсам, защиты от атак, защиты взаимодействия с удаленными территориями, блокирования сетевых вирусов и т.п. Это достигается за счет объединения в одном устройстве лучших в своем классе защитных средств – межсетевого экрана Cisco Pix, системы предотвращения атак Cisco IPS и Cisco VPN 3000 Concentrator.

Модульная архитектура Cisco Adaptive Identification and Mitigation (AIM) позволяет наращивать защитные возможности Cisco ASA 5500 новыми функциями – контроль электронной почты и Web-трафика (фильтрация URL), антивирусная защита, антиспам, антифишинг, Network Admission Control и т.п. Этот комплекс незаменим для небольших компаний и удаленных филиалов, неимеющих возможности внедрить несколько самостоятельных защитных устройств.

Основные возможности

- Управление Cisco Adaptive Security Device Manager
- Поддержка VLAN
- Поддержка отказоустойчивых конфигураций (Active/Standby и Active/Active)
- Поддержка Risk Rating, Meta Event Generator
- Поддержка OSPF, PIM, IPv6, QoS
- Поддержка «виртуальных» и прозрачных МСЭ
- Контроль протоколов и приложений (Web, e-mail, FTP, голос и мультимедиа, СУБД, операционных систем, GTP/GPRS, ICQ, P2P и т.п.)
- Защита от атак «переполнение буфера», нарушения RFC, аномалий, подмены адреса

Дополнительная информация: *http://www.cisco.com/go/asa*

МНОГООБРАЗИЕ МОДЕЛЕЙ CISCO ASA 5500

	ASA 5510	ASA 5520	ASA 5540
Производительность МСЭ, Мбит/сек	До 300	До 450	До 650
Производительность МСЭ и отражения атак, Мбит/сек	До 150	До 225 с AIP-SSM-10 До 375 с AIP-SSM-20	До 450 с AIP-SSM-20
Производительность VPN, Мбит/сек	До 170	До 225	До 325
Количество одновременно поддерживаемых сессий	32000/64000*	130000	280000
Число IPSec VPN-туннелей	50/150*	300/750*	500/2000*/5000***
Число SSL VPN-туннелей	50/150*	300/750*	500/1250*/2500***
«Виртуальные» МСЭ	0	2/10**	2/50***
Кластеризация и балансировка VPN	Нет	Да	Да
Поддерживаемые физические интерфейсы	3 Fast Ethernet + 1 порт управления/5 Fast Ethernet*	4 Gigabit Ethernet + 1 Fast Ethernet	4 Gigabit Ethernet + 1 Fast Ethernet
Поддерживаемые логические интерфейсы VLAN 802.1q	0/10*	25	100

Примечание: * – с лицензиями 5510 Security Plus, 5520 VPN Plus и 5540 VPN Plus соответственно

** – при помощи дополнительной лицензии (в базовой комплектации – 2)

*** – с лицензией 5540 VPN Premium

СХЕМА ЛИЦЕНЗИРОВАНИЯ CISCO PIX, CISCO FWSM И CISCO ASA

Лицензирование по числу пользователей

Данный тип лицензии контролирует число пользователей (или других IP-ресурсов), имеющих возможность одновременно «выйти» в Интернет через внешний интерфейс межсетевого экрана. Варианты лицензий – 10, 50 и неограниченное число пользователей. Схема лицензирования применяется только для модели Cisco Pix 501.

Лицензирование по платформе

Тип лицензии	Описание
Restricted (R)	• Ограниченное количество поддерживаемых физических и виртуальных интерфейсов • Нет поддержки отказоустойчивой конфигурации (Failover Active\Standby и Failover Active\Active)) • Нет поддержки «виртуальных» МСЭ и инспекции протокола GTP/GPRS
Unrestricted (UR)	• Отсутствуют любые ограничения, присущие Restricted-лицензии
Failover (FO)	• Обеспечивает возможности, аналогичные Unrestricted-лицензии (за исключением Failover Active\Active) • Предназначен для создания отказоустойчивых конфигураций и использования в паре с МСЭ с Unrestricted-лицензией • Требует применения двух идентичных моделей МСЭ
Failover Active/Active (FO-A/A)	• Включает все возможности Failover-лицензии, а также поддерживает конфигурацию Failover Active\Active • Требует применения двух идентичных моделей МСЭ

Схема лицензирования применяется только для моделей Cisco Pix 515, 515E, 525 и 535.

Лицензирование по функциям шифрования

Данный тип лицензии позволяет активировать функции шифрования, предназначенные для организации VPN и защищенного управления межсетевым экраном.

Тип лицензии	Описание
Restricted (R)	• Ограниченное количество поддерживаемых физических и виртуальных интерфейсов
VPN-None	• Запрещает любые функции шифрования в МСЭ
VPN-DES	• Поддерживает «слабую» криптографию – 512-битный RSA и DSA, 56-битный DES и 56-битный RC4
VPN-3DES/AES	• Поддерживает «сильную» криптографию – 4096-битный RSA, 1024-бтитный DSA, 56-битный DES, 168-битный 3DES, 256-битный AES и 128-битный RC4

Схема лицензирования применяется для любых моделей Cisco Pix. Все модели Cisco ASA 5500 по умолчанию поставляются с лицензией VPN-DES с возможность расширения до VPN-3DES/AES.

Лицензирование по расширенным функциям

Данный тип лицензии позволяет активировать расширенные функции.

Тип лицензии	Описание
Security Context	• Поддерживает возможность создания «виртуальных» межсетевых экранов. Варианты лицензий – 5, 10, 20 и 50 виртуальных «МСЭ»
GTP/GPRS Inspection	• Поддерживает возможность контроля протокола GTP/GPRS

Схема лицензирования применяется только для моделей Cisco ASA 5520 и 5540, а также Cisco Pix 515, 515E, 525 и 535 (для Pix – только для схем лицензирования Unrestricted, Failover и Failover-Active\Active). Для FWSM используется только лицензирование по Security Context.

Дополнительная информация:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a00800b0d85.html

CISCO PIX, FWSM, IOS FIREWALL И ASA 5500: ЧТО ВЫБРАТЬ?

Причины выбора Cisco Pix

- Разделение полномочий по управлению сетью и безопасностью
- Решение для штаб-квартир, центральных офисов компаний и центров обработки данных
- Отказоустойчивость Active/Standby и Active/Active
- Контроль протоколов мобильной связи GTP/GPRS

Причины выбора Cisco FWSM

- Защита центров обработки данных
- Защита операторов связи
- Защита внутренней коммутируемой сети
- Высокая пропускная способность – до 20 Гбит/сек
- Предоставление аутсорсинговых услуг Managed Security Services
- Единая организационная структура управления сетью и безопасностью

Причины выбора Cisco IOS Firewall

- Консолидированное решение для защиты периметра небольших предприятий и домашних пользователей
- Снижение стоимости внедрения в существующую инфраструктуру
- Тесная интеграция с механизмами машрутизации, QoS и другими сетевыми функциями
- Дополнительный уровень защиты

Причины выбора Cisco ASA 5500

- Единое защитное решение для удаленных филиалов (офисов, отделений, терминалов и т.п.) и небольших предприятий
- Снижение совокупной стоимости владения системой защиты
- Централизованное управление всеми защитными механизмами

CISCO IPS 4200, IDSM, NM-IDS, IOS IPS И ASA 5500: ЧТО ВЫБРАТЬ?

Причины выбора Cisco IPS 4200
- Разделение полномочий по управлению сетью и безопасностью
- Решение для штаб-квартир, центральных офисов компаний и центров обработки данных
- Контроль атак в MPLS

Причины выбора Cisco IDSM-2
- Предотвращение атак во внутренней коммутируемой сети
- Единая организационная структура управления сетью и безопасностью

Причины выбора Cisco IOS IPS или Cisco NM-IDS
- Консолидированное решение для защиты периметра небольших предприятий и домашних пользователей
- Снижение стоимости внедрения в существующую инфраструктуру
- Тесная интеграция с механизмами машрутизации, QoS и другими сетевыми функциями
- Необходимость блокирования атак (только для Cisco IOS IPS)
- Дополнительный уровень защиты

Причины выбора Cisco ASA 5500
- Единое защитное решение для удаленных филиалов (офисов, отделений, терминалов и т.п.) и небольших предприятий
- Снижение совокупной стоимости владения системой защиты
- Централизованное управление всеми защитными механизмами

CISCO GUARD и TRAFFIC ANOMALY DETECTOR

Cisco Guard позволяет отражать атаки типа “отказ в обслуживании” (DoS), в т. ч. и распределенные (DDoS), обнаруженные специализированными средствами обнаружения вторжений, в качестве которых могут выступать Cisco Anomaly Traffic Detector, Cisco IDS/IPS 42xx или Arbor Peakflow. Блокирование основано на методе отвода трафика и позволяет отделить вредоносные пакеты от пакетов, несущих полезные данные.

Основные возможности

- Уникальная архитектура Multiverification Process (MVP)
- Отсутствие снижения производительности защищаемой сети
- Скорость обработки трафика – 1,25 млн пакетов в секунду (возможность масштабирования до 10 млн пакетов в секунду путем использования кластеров Cisco Guard)
- Число параллельно обрабатываемых соединений – 1,5 млн
- Возможность поставки в виде выделенного устройства или модуля для коммутатора Cisco Catalyst 6500 или маршрутизатора Cisco 7600
- Защита от одновременной атаки со стороны свыше 100 000 зомби (механизм Zombie Killer)
- Число динамических фильтров – 150 000 (добавление 1000 фильтров в секунду)
- Задержка – менее 1 мсек
- Централизованное управление и интеграция с CiscoWorks SIMS
- Соблюдение необходимого уровня SLA
- Обеспечение услуг аутсорсинга

Дополнительная информация: *http://www.cisco.com/go/guard*, *http://www.cisco.com/go/detector*, *http://www.cisco.com/en/US/products/ps6235/index.html* и *http://www.cisco.com/en/US/products/ps6236/index.html*

CISCO IOS INTRUSION PREVENTION SYSTEM

Программное обеспечение Cisco IOS IPS – это первое в отрасли решение для предотвращения атак, интегрированное в маршрутизаторы и обнаруживающее вредоносную активность в трафике, проходящем через периметр удаленного филиала, небольшого или домашнего офиса. Эта функциональность доступна начиная с IOS 12.3(8)T и поддерживается на маршрутизаторах Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200 и 7301.

Механизм параллельного сканирования Parallel Signature Scanning Engine позволяет снизить влияние механизма инспекции трафика на производительность маршрутизатора даже при увеличении числа проводимых проверок.

Основные возможности

- Базируется на зарекомендовавшем временем программном коде системы Cisco IDS/IPS
- Обнаружение более 740 сигнатур атак в протоколах IP, ICMP, TCP, UDP, DNS, RPC, SMTP, FTP и HTTP
- Интеграция со всеми защитными функциями операционной системы IOS маршрутизатора – IOS Firewall, IOS VPN, Network Admission Control (NAC)
- Технология микромодулей (Signatures Micro-Engine, SME) для каждого типа обнаруживаемых атак
- Возможность блокирования атаки в реальном режиме времени (inline)
- Возможность обновления сигнатур с помощью Signature Definition File (SDF)
- Поддержка уведомления об атаке по протоколу SDEE, syslog и т.д.
- Возможность анализа GRE- или VPN-трафика
- Управление с помощью Security Device Manager (SDM) или CiscoWorks VPN Security Management Solution
- Высокая производительность (до 425 Мбит/сек на Cisco 3845)

Дополнительная информация: *http://www.cisco.com/go/iosips*

CONTENT ENGINE

Устройства Content Engine с программным обеспечением Cisco Application and Content Networking System (ACNS) помогают организациям любого размера снизить опасность, которую несет доступ в Интернет по протоколу HTTP. Content Engine, помимо кэширования данных, решают 3 основные задачи:

- аутентификацию пользователей;
- контроль содержимого Интернет-трафика (HTTP, FTP, HTTPS и т. д.);
- интеграцию с антивирусными решениями по протоколу ICAP (Internet Content Adaptation Protocol).

Основные возможности

- Контроль всех действий сотрудников в сети Интернет
- Методы аутентификации – RADIUS, TACACS+, NTLM, LDAP (включая расширения) и Active Directory
- Фильтрация Web-трафика с помощью Websense, SmartFilter или N2H2
- Прозрачность для пользователей
- Ограничение доступа к сетевым приложениями/ресурсам (например, Web-серверам) на основе имени пользователя или группы, а также по времени
- Обнаружение и блокирование использования Интернет-пейджеров (например, ICQ), P2P-сетей и IRC-чатов
- Ограничение полосы пропускания для отдельных приложений/сервисов
- Перенаправление трафика на антивирусные и фильтрующие серверы TrendMicro, Symantec, SurfControl, Finjan
- Балансировка нагрузки между NTLM/AD-серверами
- Большое число отчетов о деятельности сотрудников в сети Интернет

Дополнительная информация: *http://www.cisco.com/en/US/products/hw/contnetw/index.html*

CONTENT ENGINE NETWORK MODULE

Cisco Content Engine Network Module – единственное на рынке решение для фильтрации Web-трафика и аутентификации пользователей, обращающихся в Интернет, предназначенное для интеграции в маршрутизаторы. Этот модуль, устанавливаемый в слот маршрутизаторов Cisco 2600, 2800, 3700 и 3800, обнаруживает нарушения политики безопасности в трафике, проходящем через периметр удаленного филиала или небольшого офиса.

Основные возможности

- Базируется на зарекомендовавшем себя временем программном коде устройства Cisco Content Engine
- Кэширование и ускорение обработки Web-трафика
- Интеграция со всеми защитными функциями операционной системы IOS маршрутизатора
- Поддержка протокола WCCP (Web Cache Communication Protocol)
- Оптимизация распределения файлов и программного обеспечения большого объема
- 3 модели с жестким диском в 40 или 80 Гбит, а также SCSI-интерфейсом для подключения внешнего дискового массива

Поддерживаемые модели маршрутизаторов

Cisco 2600	Cisco 2600XM	Cisco 2691	Cisco 2811	Cisco 2821
Cisco 2851	Cisco 3725	Cisco 3745	Cisco 3825	Cisco 3845

Дополнительная информация:
http://www.cisco.com/en/US/products/hw/modules/ps2797/products_data_sheet09186a008010fb9f.html

CISCO SERVICE CONTROL ENGINE

Cisco Service Control Engine (SCE) – устройство, ориентированное на операторов связи, и предназначенное для классификации, профилирования и квотирования трафика, в т. ч. и для обнаружения и блокирования атак «отказ в обслуживании», эпидемий червей и вирусов, спама и т.п. Помимо обнаружения и подавления «зомби»-машин, SCE может блокировать и другие нарушения политики безопасности – использование пиринговых сетей, несанкционированное развертывание VoIP-инфраструктуры (например, Skype) и т.п.

Преимущество SCE в том, что нарушения политики безопасности локализуются в границах сети одного оператора связи и не распространяются за ее пределы. Это позволяет защитить абонентов (особенно физических лиц) оператора связи и не возлагать на них бремя ответственности по защите своего подключения к сетям общего пользования с помощью широкополосного доступа.

Использование технологии Stateful Deep Packet Inspection позволяет проникнуть вглубь каждого потока и, например, разрешить передачу одного мегабайтного сообщения электронной почты и блокировать передачу 1000 Кб сообщений.

Основные возможности

- Пропускная способность – до 4 Гбит/сек
- Число одновременно контролируемых абонентов – до 100000
- Число одновременно обрабатываемых потоков – до 2 миллионов
- Поддержка свыше 600 протоколов
- Обеспечение высокой отказоустойчивости
- Поддержка MPLS, VLAN, MPLS VPN, L2TP
- Поддержка DiffServ и ToS
- Переадресация трафика в карантин, уведомление абонентов и перенаправление их в центр поддержки
- Интеграция с биллинговой системой
- Создание политик контроля трафика (используемых протоколов, квот и т. д.) для отдельных абонентов

Дополнительная информация: *http://www.cisco.com/go/servicecontrol*

CISCO AVS 3110 APPLICATION VELOCITY SYSTEM

Cisco AVS 3110 Application Velocity System – программно-аппаратный комплекс для оптимизации и защиты HTML- и XML-приложений. Обычно размещаемый в центрах обработки данных, Cisco AVS 3110 включает в себя ряд компонентов, одним из которых является AppScreen Web Application Firewall, который в реальном режиме времени обрабатывает весь трафика и отражает HTTP/HTTPS-атаки.

Отказ от сигнатурного метода обнаружение атак позволяет обнаруживать многие неизвестные угрозы, направленные на XML- и Web-приложения. Cisco AVS 3110 защищает от атак типа SQL Injection, Cross-Site Scripting, Directory Traversal, загрузки файлов, переполнения буфера, несанкционированного выполнения команд, манипуляции данными в формах, манипуляций с cookie и HTTP-запросами, манипуляций с кодировками и т.п.

В состав Cisco AVS 3110 также входят Condenser Application Accelerator для снижения задержек при доступе к серверам приложений и оптимизации трафика, а также AppScope Monitor для мониторинга производительности HTML\XML-приложений.

Основные возможности

- Поддержка кластеризации для обеспечения высокой доступности
- Использование политик и правил для контроля информационных потоков
- Анализ не только заголовков, но и содержимого HTTP\HTTPS-запроса
- Ведение «белого» и «черного» списка действий
- Генерация уведомлений по SNMP
- Приоритезация атак по степени риска
- Поддержка графических отчетов

Дополнительная информация: *http://www.cisco.com/en/US/products/ps6492/index.html*

CISCO IOS ADVANCED SECURITY

Программное обеспечение Cisco IOS Advanced Security представляет собой набор защитных функций, реализованных в операционной системе Cisco IOS, имеющейся в каждом маршрутизаторе. Помимо Cisco IOS Firewall, в Advanced Security входит подсистема построения VPN (IPSec, MPLS, GRE, L2F и L2TP), а также подсистема предотвращения атак Cisco IOS IPS, способная отражать свыше 740 распространенных атак и методов сетевой разведки, используемых злоумышленниками.

Основные возможности

- Контроль URL
- Обнаружение и отражение атак типа «отказ в обслуживании»
- Поддержка качества обслуживания QoS (в т. ч. и для VPN)
- Ролевое управление доступом для настройки IOS
- Аутентификация и авторизация
- Контроль целостности ПО Cisco IOS
- Поддержка стандарта 802.1x
- Обмен событиями безопасности с другими устройствами по протоколу SDEE (Security Device Event Exchange)
- Поддержка технологии Network Admission Control (NAC)
- Автоматическое отключение опасных команд и функций с помощью механизма AutoSecure
- Встроенный сервер сертификатов PKI
- Поддержка протокола защищенного управления SSHv2
- Поддержка протокола SNMPv3
- Распознавание приложений с помощью технологии Network-Based Application Recognition (NBAR)

Дополнительная информация: *http://www.cisco.com/go/iossecurity*

ПРОИЗВОДИТЕЛЬНОСТЬ ФУНКЦИЙ ЗАЩИТЫ МАРШРУТИЗАТОРОВ С CISCO IOS

	Производительность межсетевого экрана, Мбит/сек	Максимальное число VPN-туннелей	Производительность DES, Мбит/сек	Производительность AES-128, Мбит/сек
Cisco SOHO 90	10	8	1	Не применимо
Cisco 830	20	10	7	2
Cisco 850 ISR	50	5	8	8
Cisco 870 ISR	70	10	30	30
Cisco 1700 с модулем VPN	20	100	15	4,5
Cisco 1800 ISR	100	50	40	40
Cisco 1800 с AIM-VPN/BPII+	100	800	95	95
Cisco 2600XM с AIM-VPN/BPII	50	800	22	22
Cisco 2691 с AIM-VPN/EPII	200	800	150	150
Cisco 2851 ISR	530	300	66	66
Cisco 2851 с AIM-VPN/EPII+	530	1500	145	145
Cisco 3700 с AIM-VPN/HPII	200	2000	190	190
Cisco 3845 ISR	1100	700	180	180
Cisco 3845 с AIM-VPN/HPII+	1100	2500	185	185
Cisco 7200VXR с SA-VAM2+	1605 (802,5 Мбит/сек в каждом направлении)	5000	280	280
Cisco 7301 с SA-VAM2+	1605 (802,5 Мбит/сек в каждом направлении)	5000	379	379

CISCO NETWORK FOUNDATION PROTECTION

Cisco Network Foundation Protection (NFP) – это набор технологий и механизмов, интегрированных в операционную систему Cisco IOS и предназначенных для защиты сетевого устройства, таблиц маршрутизации и ее обновлений, функций управления и данных, проходящих через устройство. В основе NFP лежит принцип, что защищенная сеть должна строиться на защищенном фундаменте, которым являются маршрутизаторы.

Основные возможности

- Автоматическое отключение опасных команд и функций с помощью механизма AutoSecure
- Контроль загрузки центрального процессора
- Защищенный доступ к устройству при помощи SSH, SNMPv3
- Защита от подбора паролей
- Защита от подмены адреса с помощью Unicast Reverse Path Forwarding (uRPF)
- Контроль полосы пропускания с помощью механизма Committed Access Rate (CAR)
- Фильтрация трафика путем применения Remote Triggered Black Hole (RTBH) и Remote Triggered Rate Limiting (RTRL)
- Механизм BGP TTL Security Check
- Контроль целостности обновлений таблиц маршрутизации
- Механизм защиты контура управления Control Plane Policing
- Списки контроля доступа rACL, iACL, VTY Access Control List
- Обнаружение аномалий и атак «отказ в обслуживании» с помощью NetFlow
- Аутентификация администратора с помощью TACACS+/RADIUS и авторизация с помощью RADIUS
- Контроль целостности операционной системы Cisco IOS
- Ролевое управление
- Отслеживание источника атаки с помощью IP Source Tracker

Дополнительная информация: *http://www.cisco.com/go/nfp*

CATALYST INTEGRATED SECURITY (CIS)

Catalyst Integrated Security – набор функций и механизмов, реализованных в каждом коммутаторе Catalyst компании Cisco с целью обеспечения интегрированной защиты внутренней сети. Помимо сегментации локальной сети на непересекающиеся виртуальные подсети (VLAN), семейства коммутаторов Catalyst 2950, 2970, 3550, 3560, 3750, 4500 и 6500 содержат еще несколько десятков возможностей, снижающих вероятность нанесения ущерба сети, построенной на оборудовании компании Cisco Systems.

Основные возможности

- Поддержка списков контроля доступа (ACL) 2–4-го уровней
- Контроль доступа по времени
- Обеспечение доступа неавторизованных пользователей в “гостевую” VLAN
- Поддержка Private VLAN (PVLAN) внутри VLAN
- Защита от подмены MAC- и IP-адресов с помощью IP Source Guard и Dynamic ARP Inspection (DAI)
- Блокирование несанкционированных коммутаторов в сети с помощью механизмов BPDU Guard и Root Guard
- Защита от атак типа «отказ в обслуживании» (MAC Flood, STP loop)
- Защита от атак/червей
- Ограничение полосы пропускания для пользователей / групп пользователей
- Обнаружение и ограничение аномальной активности (Scavenger Class Queuing)
- Защита от перехвата трафика с помощью механизма VLAN, а также DHCP Snooping
- Поддержка стандарта 802.1x
- Уведомление об обнаружении несанкционированного узла в сети

CISCO SECURITY AGENT

Cisco Security Agent (CSA) объединяет различные защитные механизмы и функции в одном решении – предотвращение атак, персональный межсетевой экран, защита от вредоносного кода, контроль целостности, блокирование утечки информации через USB-порты и другие внешние устройства (PCMCIA, CD, Floppy, Zip и др.), ограничение возможностей Интернет-пейджеров (например, ICQ), обнаружение перехватчиков с клавиатуры и т. п.

CSA позволяет отражать широкий спектр нападений – сканирование портов, переполнение буфера, троянцев и червей, DoS-атаки и др. При этом CSA построен по совершенно иному принципу, чем традиционные антивирусы и системы обнаружения атак, и не использует сигнатуры для идентификации несанкционированных действий. Это, в свою очередь, обеспечивает защиту компьютера от неизвестных атак, сигнатуры для которых пока не написаны и отсутствуют в базах традиционных средств защиты.

Основные возможности

- Интеграция с Active Directory, LDAP, NIS
- Автоматическая смена политики контроля в зависимости от имени пользователя и его местоположения в сети
- 2 типа корреляции событий безопасности
- Прозрачность установки, не требующая участия владельца компьютера
- Автоматизация создания политик контроля
- Управление 100 000 агентами с одной консоли управления
- Инвентаризация установленного ПО
- Интеграция с VPN-клиентами компаний Cisco и Check Point
- Интеграция с Network Admission Control (NAC)
- Делегирование отдельных функций управления агентом пользователю

Дополнительная информация: *http://www.cisco.com/go/csa*

IDENTITY & TRUST MANAGEMENT SYSTEM

Стратегия Identity & Trust Management System призвана не допустить появления в сети посторонних пользователей и устройств. Для решения этой задачи компания Cisco Systems предлагает целый ряд технологий и решений.

Контроль доступа с помощью стандарта 802.1x, позволяющего идентифицировать пользователей и устройства, которые пытаются получить доступ к корпоративным ресурсам

Идентификация, аутентификация и авторизация пользователей и устройств с помощью Cisco Secure Access Control Server (ACS) и Cisco Access Registrar, поддерживающих различные протоколы и стандарты – RADIUS, TACACS+, 802.1x, CHAP, PAP и многие другие

Новая технология Network Admission Control (NAC), позволяющая не только авторизовать устройства и пользователей еще на подступах к защищаемым ресурсам, но и изолировать все узлы, не соответствующие политике безопасности (с отсутствующим антивирусом или неактуальной антивирусной базой, неустановленным обновлением или средствами персональной защиты и т. п.) в карантинной сети. О своей поддержке и участии в NAC уже объявили такие компании, как Trend Micro, McAfee, Symantec и IBM (Tivoli), а также Microsoft, Computer Associates, Altiris, Internet Security Systems (ISS), Sophos и многие другие

Стратегия Trust and Identity Solution распространяется на все элементы инфраструктуры – коммутаторы и маршрутизаторы, ПК и IP-телефоны, беспроводные точки доступа и клиентов и т. д.

Дополнительная информация: *http://www.cisco.com/go/ti*

CISCO SECURE ACCESS CONTROL SERVER

Cisco Secure Access Control Server (ACS) – программное или программно-аппаратное решение, предназначенное для централизованного управления доступом корпоративных пользователей через все устройства и защитные решения компании Cisco Systems. При помощи ACS можно управлять доступом на маршрутизаторах и коммутаторах, средствах построения VPN и межсетевых экранах, узлах IP-телефонии и беспроводных точках и клиентах, устройствах хранения и контроля контента, а также для различных типов удаленного доступа (широкополосный, DSL, dialup) и т. д.

Основные возможности

- Поддержка аутентификации LDAP и ODBC, Active Directory и NDS, RADIUS и TACACS+, CHAP и MS-CHAP, PAP и ARA, и т. д.
- Поддержка стандарта 802.1x (режимы EAP-TLS, PEAP, Cisco LEAP, EAP-FAST и EAP-MD5)
- Авторизация команд на устройствах
- Ограничение доступа по времени, числу сессий и другим контролируемым параметрам
- Создание профилей пользователей и групп
- Интеграция с решениями для одноразовых паролей и токенов
- Высокая масштабируемость (свыше 100000 пользователей, тысячи устройств)
- Возможность проверки дополнительных условий перед разрешением доступа в сеть
- Интеграция с Network Admission Control (NAC)
- Интеграция с PKI и поддержка списка отозванных сертификатов (CRL)
- Регистрация всех попыток доступа пользователей
- Генерация отчетов
- Возможность поставки в виде специального устройства с защищенной ОС

Дополнительная информация: *http://www.cisco.com/go/acs*

CISCO ACCESS REGISTRAR

RADIUS-сервер Cisco Access Registrar – централизованная система аутентификации, авторизации и учета абонентов оператора связи, ориентированная на контроль доступа большого числа абонентов, подключающихся к сети оператора связи с помощью различных методов доступа – мобильный (например, CDMA2000 или GPRS), беспроводные корпоративные сети и публичные точки доступа (хотспоты), широкополосный или коммутируемый доступ, SSG и VoIP и т.д.

При поступлении запроса он, в зависимости от типа и содержания, обрабатывается на Cisco Access Registrar или, при необходимости роуминга, пересылается на внешний RADIUS-сервер. При необходимости поступающий запрос обрабатывается с помощью различных сценариев, регистрирующих доступ абонента в базе данных или биллинговой системе, а также накладывающих определенные ограничения, включая блокирование доступа и т.п.маршрутизаторы и обнаруживающее вредоносную активность в трафике, проходящем через периметр удаленного филиала, небольшого или домашнего офиса. Эта функциональность доступна начиная с IOS 12.3(8)T и поддерживается на маршрутизаторах Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200 и 7301.

Механизм параллельного сканирования Parallel Signature Scanning Engine позволяет снизить влияние механизма инспекции трафика на производительность маршрутизатора даже при увеличении числа проводимых проверок.

Основные возможности

- Поддержка LDAP, аутентификации Windows, RADIUS proxy или встроенной высокоскоростной базы пользователей
- Поддержка различных вариантов протокола EAP (LEAP, PEAP, GTC, SIM, EAP-TLS, EAP-FAST, EAP-MD5, EAP Proxy)
- Регистрация попыток доступа в локальном файле или базах данных Oracle или MySQL
- Всесторонний учет всех событий о сессии абонента в локальном файле или базах данных Oracle или MySQL
- Создание групп пользователей
- Интеграция с внешними системами хранения данных и биллинга
- Регистрация всех изменений конфигурации Cisco Access Registrar
- Генерация SNMP для критичных событий
- Поддержка RADIUS SNMP (RFC 2618-21)
- Расширенные механизмы отказоустойчивости
- Возможность создания собственных сценариев обработки запросов на любой стадии

Дополнительная информация*: http://www.cisco.com/en/US/products/sw/netmgtsw/ps411/index.html*

ТЕХНОЛОГИЯ NETWORK ADMISSION CONTROL

Не требующая лицензирования технология Network Admission Control (NAC) позволяет предотвратить доступ к корпоративным ресурсам или сети оператора связи устройств, несоответствующих политике безопасности (заражен вредоносной программой, отсутствует или устарел антивирус, отсутствуют патчи и Service Pack'и, отсутствуют средства защиты и иное программное обеспечение). В случае обнаружения такого несоответствия доступ узла либо блокируется, либо он перенаправляется в карантинную сеть, в которой на узел может быть установлено отсутствующее программное обеспечение.

Контроль соответствия политике безопасности реализуется как можно ближе к возможному источнику нарушения – на маршрутизаторе Cisco или VPN 3000 Concentrator (фаза 1), коммутаторе Catalyst (фаза 2) и других сетевых устройствах (точка беспроводного доступа, межсетевой экран и т.п.), в которые встроена поддержка NAC.

Основные возможности

- Поддержка любых типов доступа (проводной, беспроводной, коммутируемый, широкополосный и т.д.)
- Обеспечение соответствия политике безопасности независимо от желания пользователя
- Поддержка EAP over UDP (фаза 1) и EAP over 802.1x (фаза 2)
- Прозрачность для пользователя
- Поддержка ОС Windows (фаза 1), Linux и Solaris (фаза 2)
- Помещение несоответствующего узла в карантин путем применения списков контроля доступа ACL или URL Redirection (фаза 1), а также VLAN и PACL (фаза 2)
- Решение парадокса «пользователь имеет права доступа в сеть, а его компьютер – нет»
- Интеграция с TrendMicro, Symantec, McAfee, IBM (фаза 1), а также с более чем 100 производителей (Microsoft, ISS, Sophos, Panda, CA и т.д.) в будущем

Дополнительная информация: *http://www.cisco.com/go/nac*

CISCO CLEAN ACCESS

Cisco Clean Access – это решение, предназначенное для автоматического обнаружения, изолирования и лечения инфицированных, уязвимых или несоответствующих политике безопасности узлов, осуществляющих проводной или беспроводной доступ к корпоративным ресурсам.

Будучи одним из компонентов технологии Network Admission Control, Clean Access выполнен в виде отдельного устройства, которое может быть установлено в двух режимах:

- In-band – весь трафик проходит через Cisco Clean Access Server и проверяется каждый раз, когда узел пытается осуществить доступ к защищаемым ресурсам.
- Out-band – трафик перенаправляется на Cisco Clean Access Server только когда узел отсутствует в «белом» списке.

Основные возможности

- Независимость от производителя сетевого оборудования (в режиме in-band)
- Интеграция с Kerberos, LDAP, RADIUS, Active Directory, S/Ident и другими методами аутентификации
- Сканирование защищенности ОС Windows, MacOS, Linux, Xbox, PlayStation 2 и КПК с помощью Cisco Clean Access Agent
- Поддержка антивирусов CA, F-Secure, Eset, Лаборатории Касперского, McAfee, Panda, DrWeb, Sophos, Symantec, TrendMicro и других средств защиты компьютера
- Помещение несоответствующего узла в карантин путем применения списков контроля доступа ACL или VLAN
- Создание «белого» списка узлов для ускорения их доступа к ресурсам сети
- Автоматическая установка отсутствующих обновлений, устаревших антивирусных баз или новых версий средств защиты
- Централизованное Web-управление

Дополнительная информация: *http://www.cisco.com/go/cca*

CISCO SECURE USER REGISTRATION TOOL

Cisco Secure User Registration Tool (URT) – инструмент динамической авторизации и аутентификации пользователей, позволяющий динамически назначать пользователям права доступа в определенные VLAN с целью организации доступа только к нужным сервисам и ресурсам. URT связывает пользователей с нужными сетевыми ресурсами, и при попытке получения доступа к ним пользователю автоматически назначается нужная VLAN, тем самым обеспечивается принцип минимума привилегий.

Основное достоинство URT – работа с устройствами, не поддерживающими в данный момент стандарт 802.1x (например, IP-телефоны или ОС Windows 9x, NT и т. п.).

Основные возможности

- Поддержка ОС Windows, Linux и Macintosh
- Поддержка аутентификации LDAP, Active Directory, NDS и RADIUS (например, Cisco Secure ACS)
- Поддержка аутентификации пользователей и устройств (по MAC)
- Привязка VLAN к пользователям, группам или MAC-адресам
- Прозрачность для пользователей
- Высокая масштабируемость и отказоустойчивость
- Регистрация всех попыток доступа
- Помощь в отслеживании физического размещения пользователей
- Поддержка VPS-серверов и технологии VQP/VMPS компании Cisco Systems
- Импорт из CiscoWorks 2000 информации о коммутаторах, доменах VTP и VLAN
- Не требует инсталляции агентов на пользовательские компьютеры
- Поддержка нескольких пользователей на один порт коммутатора

Дополнительная информация: *http://www.cisco.com/go/urt*

SECURE CONNECTIVITY SOLUTION

Стратегия Secure Connectivity Solution призвана обеспечить защищенный доступ к корпоративным ресурсам из любой точки и с помощью любой технологии доступа – как проводной, так и беспроводной. При этом немаловажной является задача защиты трафика для всех типов данных, включая такие критичные к задержкам приложения, как IP-телефония, видео, мультимедиа и т. д. Для решения этой задачи компания Cisco Systems предлагает целый ряд технологий и решений.

Организация защищенного взаимодействия между сетями (Site-to-Site VPN)
- с удаленными филиалами
- с бизнес-партнерами
- с надомными работниками

Организация защищенного удаленного доступа к корпоративным ресурсам (Remote Access VPN)
- для мобильных пользователей
- для надомных пользователей

Защита видео- и голосовых данных
- IP-телефонии
- видеотелефонии
- аудио- и видеоконференций
- контакт-центров

Защита беспроводного взаимодействия между
- точками доступа
- беспроводными клиентами

Различные технологии VPN
- Поддержка IPSec, SSL (WebVPN), MPLS, GRE, VLAN, L2VPN и т.д.

Дополнительная информация: *http://www.cisco.com/go/scs*

CISCO VPN 3000 CONCENTRATOR

Cisco VPN 3000 Concentrator Series – это серия специализированных устройств для построения сетей удаленного доступа на основе технологии виртуальных частных сетей (Virtual Private Networks). Объединяя в себе высокую доступность, производительность, масштабируемость и поддержку современных алгоритмов аутентификации и шифрования, серия Cisco VPN 3000 Concentrator позволяет существенно снизить затраты компании на удаленный доступ к своим ресурсам.

Функциональность WebVPN серии Cisco VPN 3000 Concentrator позволяет установить безопасное VPN-соединение с помощью почти любого Web-браузера, поддерживающего протокол SSL. При этом не требуется установка клиентского ПО на пользовательские компьютеры. Помимо доступа к Web, функция WebVPN позволяет получить доступ к общим ресурсам Windows – электронной почте, файловой системе и многим другим TCP-приложениям типа «клиент–сервер».

Основные возможности

- Обеспечение отказоустойчивости (VRRP, балансировка нагрузки, резервирование модулей шифрования, блоков питания и т. п.)
- Поддержка динамической маршрутизации
- Встроенный пакетный фильтр
- Поддержка протоколов IPSec (UDP и TCP), NAT Transparent IPSec, L2TP, PPTP
- Поддержка Cisco Secure Desktop
- Совместимость с MS PPTP/MPPE/MPPC, MS-CHAPv1/v2, EAP, MS L2TP/IPSec
- Совместимость с Cisco VPN Client, Cisco VPN 3002 Hardware Client, Movian (Certicom) VPN, iPass, Betrusted, RSA Keon, GTE Cybertrust, Entrust и т. д.
- Управление отдельными пользователями и группами
- Поддержка технологии контроля доступа Network Admission Control

Дополнительная информация: *http://www.cisco.com/go/vpn3000*

МНОГООБРАЗИЕ МОДЕЛЕЙ CISCO VPN 3000 CONCENTRATOR

	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3020	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Одновременных пользователей IPSec	До 100	До 100	До 750	До 1500	До 5000	До 10000
Одновременных пользователей WebVPN (SSL)	До 50	До 75	До 200	До 500	До 500	До 500
Туннелей ЛВС–ЛВС	До 100	До 100	До 250	До 500	До 1000	До 1000
Пропускная способность, Мбит/сек	До 4	До 4	До 50	До 50	До 100	До 100
Реализация шифрования	Программная	Программная	Аппаратная	Аппаратная	Аппаратная	Аппаратная
Модули шифрования SEP	0	0	1	1	2	4
Слоты расширения	Нет	4	1	3	2	Нет
Высота шасси	1RU	2RU	2RU	2RU	2RU	2RU
Резервирование блоков питания	Нет	Возможно	Возможно	Возможно	Возможно	Есть
Клиентские лицензии	Не ограничены					

CISCO SECURE DESKTOP

Программное обеспечение Cisco Secure Desktop, входящее в поставку VPN 3000 Concentrator или Cisco WebVPN Service Module, – это ключевой компонент технологии WebVPN компании Cisco Systems, предназначенный для обеспечения защиты конфиденциальной информации во время SSL-сеанса. Cisco Secure Desktop, выполненный в виде небольшого апплета (Java, ActiveX или exe-файл), загружаемого в момент подключения к корпоративной сети по SSL VPN при помощи любого броузера (в т.ч. и из незащищенного Интернет-кафе), позволяет обеспечить безопасность всех обрабатываемых в процессе сеанса данных – файлов, Web-страниц, паролей, электронной почты и т.п. Это обеспечивается за счет создания виртуального раздела (virtual desktop) на диске и шифрование всех данных, загружаемых во время SSL-сеанса для снижения вероятности их кражи, а также контроля всех процессов и обращений к реестру или жесткому диску.

Основные возможности

- Использование различных политик и профилей, базирующихся на типе или расположении узла, пытающегося получить SSL-доступ
- Не требуется административных привилегий
- Прозрачность для пользователя
- Небольшой размер (около 500 Кб)
- По окончании сессии удаление cookie, временных файлов и файла history, кэшированных страниц и паролей, а также других загруженных во время работы данных
- Проверка наличия на узле персонального МСЭ, антивируса, Service Pack'ов перед разрешением защищенного доступа в корпоративную сеть
- Перенаправление пользователя на специальную Web-страницу в случае несоответствия узла требованиям политики безопасности (например, персональный межсетевой экран установлен, но не запущен)
- Интеграция с Microsoft AntiSpyware
- Удаление виртуального раздела осуществляется путем его многократной перезаписи (стандарт DoD 5220.22-M)

CISCO VPN CLIENT

Cisco VPN Client – программное обеспечение, устанавливаемое на персональный компьютер и предназначенное для создания IPSec-туннеля с любым сервером Cisco Easy VPN, в качестве которого может выступать Cisco Pix, Cisco VPN 3000 Concentrator, Cisco ASA 5500 и Cisco IOS.

Основные возможности

- Поддержка на Windows 98, ME, NT, 2000 и XP, Linux, Solaris и MacOS
- Поддержка протоколов IPSec ESP, PPTP, L2TP, L2TP/IPSec, NAT Traversal IPSec, IPSec/TCP, IPSec/UDP
- Поддержка DES, 3DES и AES с MD5 и SHA
- Поддержка токенов Aladdin, ActiveCard, Schlumberger, Gemplus, Datakey и других через MS CAPI
- Поддержка аутентификации XAUTH, LDAP, RADIUS с поддержкой для Active Directory, Kerberos, RSA SecurID, MS-CHAPv2, x509v3
- Отсутствие конфликтов с клиентом Microsoft L2TP/IPSec
- Поддержка протокола Simple Certificate Enrollment Protocol (SCEP)
- Поддержка IKE
- Сжатие передаваемых данных
- Автоматическое обновление до новой версии
- Программный интерфейс API для контроля функционирования VPN Client из других приложений
- Балансировка нагрузки и поддержка резервных VPN-шлюзов
- Централизованное управление с помощью политик (включая списки резервных VPN-шлюзов)
- Встроенный персональный межсетевой экран
- Интеграция с Cisco Security Agent, Sygate, ZoneAlarm

Дополнительная информация: *http://www.cisco.com/go/vpnclient*

CISCO IPSEC VPN SERVICES MODULE

Cisco IPSec VPN Service Module (VPNSM) – специальный модуль, интегрируемый в коммутатор Cisco Catalyst 6500 или маршрутизаторы Cisco 7600 для эффективной организации IPSec и GRE VPN. При этом данный модуль позволяет эффективно организовывать защищенное взаимодействие не только между сетями (Site-to-Site VPN), но и с удаленными пользователями (Remote Access VPN).

Основные возможности

- Производительность – 1,9 Гбит/сек (TripleDES) с возможностью увеличения за счет установки нескольких модулей в одно устройство
- Тесная интеграция с модулями обнаружения атак, межсетевого экранирования и обработки SSL
- Контроль целостности – MD5 и SHA-1
- Управление ключами – IKE, IKE-XAUTH, IKE-CFG-MODE
- Методы аутентификации – X.509, SCEP, RADIUS, TACACS+, CHAP/PAP
- Эффективная интеграция в инфраструктуру IPC (включая VoIP), SAN и т. п.
- Обеспечение отказоустойчивости и надежности VPN-туннелей за счет применения механизмов Stateful Failover для IPSec и GRE, Host-Standby Router Protocol с Reverse Route Injection (HSRP+RRI), Dead Peer Detection (DPD) и др.
- Поддержка PKI от Entrust, VeriSign, Microsoft, Betrusted, Netscape, RSA Keon и др.
- Протоколы маршрутизации – BGP4, RIP и RIP2, OSPF, EIGRP и IGRP, а также ISIS
- Снижение совокупной стоимости владения за счет интеграции VPNSM в уже установленные в сети Catalyst 6500 или Cisco 7600

Дополнительная информация: *http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4221/index.html*

CISCO WEBVPN SERVICE MODULE

Cisco WebVPN Service Module – специальный модуль интегрируемый в коммутатор Cisco Catalyst 6500 или маршрутизаторы Cisco 7600 для эффективной организации SSL VPN. Этот модуль, совместимый с любым поддерживающим SSL броузером (включая FireFox), позволяет организовать эффективное VPN-взаимодействие для удаленных пользователей, подключающихся к корпоративным ресурсам по защищенному каналу.

Основные возможности

- Поддержка до 8000 одновременно подключающихся пользователей и до 32000 одновременно обрабатываемых соединений с возможностью увеличения за счет установки нескольких модулей в одно устройство
- Производительность до 300 Мбит/сек, и 64 шлюзов с возможностью увеличения за счет установки нескольких модулей в одно устройство
- Поддержка виртуализации – до 64 виртуальных SSL VPN контекстов с возможностью увеличения за счет установки нескольких модулей в одно устройство
- Поддержка SSL 3.0, 3.1 и TLS 1.0
- Поддержка Cisco Secure Desktop
- Поддержка виртуальных VRF-контекстов
- Поддержка большого числа приложений через динамически загружаемый SSL-клиент для WebVPN
- Возможность любой порт коммутатора или маршрутизатора сделать SSL VPN-портом
- Поддержка аутентификации RADIUS, Active Directory, NTLM, NIS и Cisco ACS
- Поддержка отказоустойчивости (Active/Active и интеграция с Cisco Content Switching Module)

Дополнительная информация: *http://www.cisco.com/en/US/products/ps6404/index.html*

CISCO SSL SERVICES MODULE

Cisco SSL VPN Service Module (SSM) – специальный модуль, интегрируемый в коммутатор Cisco Catalyst 6500 или маршрутизаторы Cisco 7600 с целью эффективной организации и оптимизации доступа по протоколу SSL для конечных пользователей. Интеграция SSM с Cisco Content Switching Module (CSM) позволяет также обеспечить высокопроизводительное, масштабируемое решение с балансировкой нагрузки между Web-серверами, востребованное, например, при электронном ведении бизнеса.

Основные возможности

- Возможность установки до 4-х модулей в устройство для повышения производительности обработки SSL
- Число соединений в секунду – 2500 с возможностью увеличения до 10 000
- Производительность шифрования – 300 Мбит/сек с возможностью увеличения до 1,2 Гбит/сек
- Число параллельных соединений – 64 000 с возможностью увеличения до 256 000
- Тесная интеграция с модулями обнаружения атак, межсетевого экранирования и построения IPSec VPN
- Оптимизация работы с сертификатами PKI
- Контроль целостности – MD5 и SHA-1
- Протокол установления соединения – SSL 3.0, SSL 3.1/TLS 1.0, SSL 2.0, Session reuse и Session renegotiation
- Аутентификация – RADIUS, TACACS+, PKI
- Поддержка NAT (клиентской и серверной) и PAT
- Обеспечение отказоустойчивости и надежности за счет применения модуля CSM или протокола HSRP
- Расширенные функции мониторинга и статистики
- Снижение совокупной стоимости владения за счет интеграции SSM в уже установленные в сети Catalyst 6500 или Cisco 7600

Дополнительная информация: *http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4156/index.html*

CISCO CONTENT SWITCHING MODULE WITH SSL

Cisco Content Switching Module with SSL (CSM-S) – специальный модуль интегрируемый в коммутатор Cisco Catalyst 6500 или маршрутизаторы Cisco 7600 с целью эффективной балансировки нагрузки между группами серверов (в т.ч. и кэширующих), межсетевых экранов и VPN-шлюзов. При этом распределение потоков происходит даже при использовании шифрования в рамках протокола SSL. В этом случае CSM-S терминирует SSL-трафик, принимает решение о балансировке и при необходимости вновь зашифровывает трафик с помощью SSL.

Основные возможности

- Производительность до 1 млн одновременных соединений и 20000 SSL-соединений с возможностью увеличения за счет установки нескольких модулей в одно устройство
- Поддержка до 165000 новых TCP-cjtbytybq и до 1000 новых SSL-транзакций в секунду с возможностью увеличения за счет установки нескольких модулей в одно устройство
- Возможность балансировки нагрузки между 16000 реальными серверами, 4000 виртуальными серверами и 4000 серверными фермами
- Поддержка Certificate Revocation List (CRL)
- Балансировка на основе различных критериев, в т.ч. URL, cookie и полей заголовка HTTP
- Распределение трафика между IPSec-шлюзами и межсетевыми экранами (включая прозрачные)
- Возможность запроса и аутентификации клиента по сертификатам
- Возможность функционирования в качестве SSL-клиента
- Поддержка NAT и PAT для сервера и клиента
- Встроенная защита от атак «отказ в обслуживании»

Дополнительная информация: *http://www.cisco.com/go/csm-s*

CISCO IOS VPN

Программное обеспечение Cisco IOS VPN, являющееся неотъемлемой частью операционной системы маршрутизаторов, позволяет быстро и эффективно построить виртуальную частную сеть (VPN) для компании любого масштаба и сети любой топологии.

Cisco IOS VPN работает на широком спектре маршрутизаторов Cisco и является идеальным решением для компаний малого и среднего бизнеса, а также для надомных работников, желающих совместить высокий уровень защиты с эффективными возможностями контроля качества обслуживания (QoS), маршрутизации, обработки мультимедиа-трафика и т. п., реализованными в одном устройстве.

Основные возможности

- Эффективная обработка мультимедиа-трафика, включая видео и голос (V3PN)
- Интеграция с механизмами контроля качества (QoS)
- Автоматическая организация VPN с помощью обнаруженных VPN-устройств в удаленных сетях (технология Dynamic Multipoint VPN, DMVPN)
- Интеграция IPSec и MPLS VPN
- Поддержка групп VPN
- Возможность установки аппаратного модуля VPN (AIM-VPN, AS-VAM2 и др.)
- Защищенное управление с помощью Web-консоли управления Cisco Security Device Manager или интерфейса командной строки
- Поддержка различных механизмов аутентификации, включая RADIUS, TACACS+ и PKI
- Возможность выступать в качестве VPN-клиента (EasyVPN Remote)

CISCO PIX VPN

Межсетевые экраны Cisco Pix помимо разграничения доступа к ресурсам корпоративной сети и сети Интернет могут выступать и в качестве IPSec VPN-решения. При этом защита взаимодействия может обеспечиваться как между сетями, так и для удаленных пользователей. VPN-соединения могут аутентифицироваться при помощи различных методов, включая сертификаты PKI X.509v3 и одноразовые пароли, протоколы RADIUS, TACACS+, Kerberos и многие другие.

Встроенная в Cisco Pix и другие решения Cisco Systems, такие как маршрутизаторы Cisco IOS и VPN-концентраторы Cisco VPN 3000 Concentrator Series, технология EasyVPN предлагает легкоуправляемую и масштабируемую архитектуру VPN удаленного доступа, которая реализуется за счет автоматического распределения политик VPN всем подключившимся клиентам.

Основные возможности

- Тесная интеграция с защитными механизмами межсетевого экрана, обеспечивающими многоуровневую защиту
- Возможность выступать в роли аппаратного VPN-клиента (только для Pix 501 и Pix 506E)
- Поддержка широкого спектра VPN-клиентов – от встроенного в ОС Microsoft до ОС для КПК
- Использование алгоритмов DES, TripleDES и AES
- Поддержка протокола SCEP (Simple Certificate Enrollment Protocol)
- Встроенный EasyVPN Server
- Различные механизмы отказоустойчивости VPN-соединений – Cisco IKE keepalive, Dead Peer Detection (DPD) и IPSec Stateful Failover
- Возможность установки VPN-акселератора (VAC+)

Дополнительная информация: *см. раздел о* ***CISCO PIX***

CISCO PIX VPN, VPN 3000, VPN SERVICE MODULE, IOS VPN И ASA: ЧТО ВЫБРАТЬ?

Причины выбора Cisco Pix VPN

- Разделение полномочий по управлению сетью и безопасностью
- Интегрированное решение «среднего» класса

Причины выбора Cisco IPSec VPN SPA или WebVPN Service Module

- Защита центров обработки данных
- Единая организационная структура управления сетью и безопасностью

Причины выбора Cisco IOS VPN

- Организация высокопроизводительной Site-to-Site VPN с расширенными возможностями
- Снижение стоимости внедрения в существующую инфраструктуру
- VPN для WAN-интерфейсов
- Организация VPN без приобретения дополнительных средств защиты
- Интеграция IPSec и MPLS VPN

Причины выбора Cisco ASA 5500

- Организация удаленного доступа с помощью IPSec VPN
- Совместное использование IPSec и SSL VPN
- Совместимость с Cisco VPN 3000
- Единое защитное решение для удаленных филиалов (офисов, отделений, терминалов и т.п.) и небольших предприятий

Причины выбора Cisco VPN 3000 Concentrator

- Организация удаленного доступа с помощью SSL VPN
- Совместное использование IPSec и SSL VPN
- Использование Cisco Secure Desktop

РЕШЕНИЯ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Решения Cisco Systems по управлению позволяют эффективно настраивать, контролировать и обновлять все продукты по информационной безопасности, входящие в стратегию Self-Defending Network и ее составляющие – Threat Defense System, Trust and Identity Management Solution и Secure Connectivity Solution.

Управление политиками контроля
- Создание, модификация и распространение политик контроля на сотни и тысячи средств защиты

Управление обновлениями
- Автоматическое распределение обновлений (включая политики и ПО) по всем средствам защиты

Управление конфигурацией
- Импорт конфигурации с целью ее резервирования
- Автоматическое восстановление конфигурации
- Аудит конфигурации с точки зрения безопасности

Управление событиями безопасности
- Отображение и фильтрация информации о событиях безопасности
- Анализ и корреляция событий безопасности
- Сбор информации о событиях безопасности от решений третьих фирм

Управление статистикой и отчетами
- Анализ статистики
- Генерация отчетов о состоянии защищаемой сети и устройств

Защищенное управление
- Защита взаимодействия между компонентами

Дополнительная информация: *http://www.cisco.com/go/security_management*

CISCOWORKS VPN/SECURITY MANAGEMENT SOLUTION

CiscoWorks VPN/Security Management Solution (VMS) является централизованным инструментом настройки, мониторинга и отладки всех решений по безопасности компании Cisco Systems – средств построения VPN, межсетевых экранов, сетевых и серверных систем предотвращения атак и т. д. Основными компонентами системы являются:

Инструменты управления

- CiscoWorks Management Center for Firewalls,
- CiscoWorks Management Center for IDS Sensors,
- CiscoWorks Management Center for VPN Routers,
- CiscoWorks Management Center for Cisco Security Agents,
- CiscoWorks Auto Update Server.

Инструменты мониторинга

- CiscoWorks Monitoring Center for Security,
- CiscoWorks Monitoring Center for Performance,
- CiscoWorks Resource Manager Essentials.

В отличие от встроенных в каждое защитное устройство собственных систем управления (Cisco Pix Device Manager, Cisco Security Device Manager и Cisco IDS Device Manager) CiscoWorks VMS, имеющий удобный графический Web-интерфейс, позволяет эффективно настраивать и контролировать десятки и сотни средств защиты, что достигается за счет механизма их группирования.

Основные возможности

Управление МСЭ Cisco Pix и Catalyst FWSM

- Управление до 1000 МСЭ Cisco Pix
- Уникальный механизм создания правил Smart Rules, сокращающий время настройки групп межсетевых экранов
- Группирование МСЭ по различным признакам (география, тип, владелец и др.)
- Наследование настроек и правил для групп
- Автоматическое обновление конфигурации и ОС МСЭ
- Периодическая проверка конфигурации удаленных МСЭ

Управление Cisco Security Agent

- Управление до 100 000 агентов CSA
- Создание и настройка политик контроля
- Генерация и распределение дистрибутивов CSA, размещаемых на защищаемых ПК без участия их владельца
- Группирование агентов

Мониторинг средств защиты

- Сбор, отображение, анализ, корреляция событий безопасности
- Посылка уведомлений о событиях безопасности
- Анализ статистики и генерация отчетов

Дополнительная информация: http://www.cisco.com/go/vms

Управление Cisco IDS/IPS, NM-CIDS и IDSM-2

- Управление несколькими сотнями сенсоров с одной консоли
- Задание иерархии сенсоров, содержащей группы и подгруппы
- 5 ролей администраторов, имеющих доступ к консоли управления
- Создание и настройка сигнатур атак
- Настройка вариантов реагирования на обнаруженные нападения
- Доступ к энциклопедии сетевой безопасности, описывающей все атаки

Управление Cisco VPN Router, VPNSM, IOS VPN

- Создание, настройка и распределение защитных политик с помощью Smart Rules
- Настройка отказоустойчивости
- Ролевое управление доступом к консоли
- Импорт конфигурации устройств
- Резервирование и восстановление конфигурации VPN-устройств

Мониторинг производительности

- Мониторинг состояния всех VPN-устройств (включая VPN 3000, SSM, VPNSM и т. д.)
- Анализ статистики и генерация отчетов
- Обнаружение и изоляция проблем

DEVICE MANAGER

Для локального управления возможностями отдельных защитных средств компании Cisco существуют специализированные менеджеры устройств (device manager), осуществляющие весь спектр функций по управлению и мониторингу межсетевыми экранами Cisco Pix и FWSM, маршрутизаторами, системами предотвращения атак (Cisco IPS 4200), многофункциональными устройствами (Cisco ASA 5500).

Основные возможности

- Web-ориентированное управление
- Подсистема помощи при внедрении и настройке устройства защиты (Startup Wizard)
- Создание и применение политик безопасности
- Идентификация и классификация потоков трафика с помощью Modular Policy Framework
- Аудит некорректной конфигурации и рекомендация соответствующих исправлений
- Списки контроля доступа на базе пользователей, групп, времени и т.д.
- Локальная и удаленная аутентификация администраторов
- Ролевое управление настройками средств защиты (16 уровней административного доступа)
- Показ в реальном режиме времени статистики о событиях безопасности, сетевой активности и т.п.
- Защищенное управление с помощью SSL или SSH

Дополнительная информация:
http://www.cisco.com/go/asdm – Adaptive Security Device Manager (для Cisco Pix и ASA 5500)
http://www.cisco.com/go/pdm – Pix Device Manager (для FWSM)
http://www.cisco.com/go/sdm – Router and Security Device Manager (для маршрутизаторов Cisco)
http://www.cisco.com/en/US/products/sw/cscowork/ps4565/ – CiscoView Device Manager

CISCO IP SOLUTION CENTER

Cisco IP Solution Center (ISC) – платформа централизованного управления сетевой инфраструктурой крупных компаний и сервис-провайдеров. В т. ч. ISC управляет и решениями по информационной безопасности – механизмами построения VPN (ЛВС–ЛВС, удаленный доступ, EasyVPN, DMVPN), межсетевыми экранами, сетевой трансляцией адресов (NAT) и качеством сервиса (QoS) на маршрутизаторах с Cisco IOS, МСЭ Cisco Pix и устройствах VPN Concentrator. Эту задачу решает специальное приложение – ISC Security Management.

ISC Security Management предоставляет возможность управления жизненным циклом средств защиты, начиная от создания политик безопасности, активации и аудита защитной услуги и заканчивая оценкой качества предоставления защитной услуги и реконфигурацией используемой политики. Все это позволяет обеспечивать безопасность инфраструктуры без нарушения ее доступности и устойчивости.

Основные возможности

- Эффективное управление сотнями тысяч политик безопасности и тысячами устройств
- Глобальная политика безопасности автоматически транслируется в команды для разных типов защитных устройств
- Встроенный агент Cisco CNS
- Автоматическое обнаружение новых устройств и применение к ним политик безопасности
- Мониторинг уровня обслуживания SLA
- Анализ топологии и инвентаризация сети
- Открытая и масштабируемая архитектура

Дополнительная информация: *http://www.cisco.com/go/isc*

CISCOWORKS SECURITY INFORMATION MANAGEMENT SOLUTION

CiscoWorks Security Information Management Solution (SIMS) представляет собой масштабируемую и централизованно управляемую систему сбора, анализа и корреляции событий безопасности, получаемых от средств защиты различных производителей (Cisco, Check Point, ISS, NetScreen, Symantec и т. п.), в т. ч. и свободно распространяемых решений. Система CiscoWorks Security Information Management Solution является центральным звеном в управлении информационной безопасностью крупных территориально распределенных сетей, построенных на решениях компании Cisco Systems и других производителей.

В качестве источников данных для SIMS могут выступать межсетевые экраны и маршрутизаторы, сетевые и хостовые системы обнаружения атак, системы построения VPN и Web-сервера, журналы регистрации событий операционных систем Windows и Unix. Также существует возможность подключения своих собственных средств безопасности к SIMS.

Основные возможности

- Агрегирование 20 000 типов сигналов тревоги в 9 категорий
- Объединение связанных событий в одно метасобытие
- Устранение избыточной информации
- Различные виды анализа и сопоставления данных от разнородных средств защиты
- Анализ с точки зрения ценности для бизнеса
- Встроенные и создаваемые пользователем правила корреляции событий
- Расширенные механизмы уведомления
- Более 250 встроенных шаблонов отчетов
- Возможность поставки в виде программно-аппаратного комплекса

Дополнительная информация: *http://www.cisco.com/go/sims*

CISCO MONITORING, ANALYSIS AND RESPONSE SYSTEM (MARS)

Программно-аппаратный комплекс Cisco MARS предназначен для управления угрозами безопасности. В качестве источников информации о них могут выступать – сетевое оборудование (маршрутизаторы и коммутаторы), средства защиты (межсетевые экраны, антивирусы, системы обнаружения атак и сканеры безопасности), журналы регистрации ОС (Solaris, Windows NT, 2000, 2003, Linux) и приложений (СУБД, Web и т.д.) , а также сетевой трафик (например, Cisco Netflow). Cisco MARS поддерживает решения различных производителей – Cisco, ISS, Check Point, Symantec, NetScreen, Extreme, Snort, McAfee, eEye, Oracle, Microsoft и т.д.

Механизм ContextCorrelation™ позволяет проанализировать и сопоставить события от разнородных средств защиты. Визуализация их на карте сети в реальном времени достигается с помощью механизма SureVector™. Данные механизмы позволяют отобразить путь распространения атаки в реальном режиме времени. Автоматическое блокирование обнаруженных атак достигается с помощью механизма AutoMitigate™, который позволяет реконфигурировать различные средства защиты и сетевое оборудование.

Основные возможности

- Обработка до 10000 событий в секунду или свыше 300000 событий Netflow в секунду
- Сигнатурные и «поведенческие» методы обнаружения аномалий и других атак
- Возможность создания собственных правил корреляции
- Эскалация инцидентов (идентификация, реагирование, расследование, контроль, генерация отчетов)
- Уведомление об обнаруженных проблемах по e-mail, SNMP, через syslog и на пейджер
- Ролевое управление через Web-интерфейс
- Визуализация атаки на канальном и сетевом уровнях
- Поддержка Syslog, SNMP, RDEP, SDEE, NetFlow, системных и пользовательских журналов регистрации в качестве источников информации
- Возможность подключения собственных средств защиты для анализа
- Эффективное отсечение ложных срабатываний и шума, а также обнаружение атак, пропущенных отдельными средствами защиты
- Обнаружение аномалий с помощью протокола NetFlow
- Создание и автоматическое обновление карты сети, включая импорт из CiscoWorks и других систем сетевого управления

Дополнительная информация: http://www.cisco.com/go/mars

CISCO SECURITY AUDITOR

Система Cisco Security Auditor предназначена для автоматизированного аудита безопасности сотен сетевых устройств и средств защиты, разбросанных по корпоративной сети или сети оператора связи. Такая проверка позволяет существенно снизить нагрузку на администраторов и гарантировать соответствие сетевых устройств современным требованиям по обеспечению надежной, бесперебойной и защищенной работе.

Cisco Security Auditor может осуществлять свои проверки на соответствие заранее определенной корпоративной политике безопасности, а также лучшим в отрасли стандартам защищенной настройки решений компании Cisco (SAFE, NSA, CIS). По итогам проверки Security Auditor создает отчеты с практическими рекомендациями по устранению обнаруженных уязвимостей и слабостей в настройке сетевого оборудования и средств защиты.

Основные возможности

- Поддержка Cisco Pix, Cisco ASA 5500, маршрутизаторов и коммутаторов Cisco различных серий
- Функционирование под управлением Windows 2000 или Windows 2003
- Web-ориентированное управление (интеграция с LMS 2.5/RME 4.0)
- Поддержка CiscoWorks RME, Common Service DCR и т.д.
- Поддержка браузеров MS Internet Explorer, Netscape Navigator и Mozilla
- Различные варианты отчетов – от высокоуровневых графических до технологических, уровня конкретных устройств
- Импорт устройств из RME, CSV и т.д.
- Организация иерархических групп устройств
- Создание своих политик с помощью Security Policy Description Language (на базе XML)
- Дистанционный и локальный аудит
- Учет веса/рейтинга результатов аудита
- Создание различных отчетов, включая сравнительные

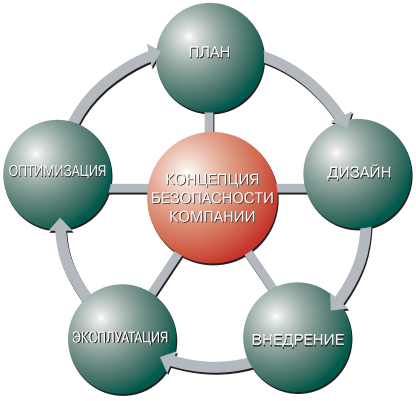
Дополнительная информация: *http://www.cisco.com/en/US/products/ps6263/index.html*

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Далее Вы найдете дополнительную информацию о решениях компании Cisco Systems по информационной безопасности, касающуюся следующих вопросов:

- **Цены, порядок заказа и политика лицензирования**
- **Информация об услугах по внедрению, настройке или аудите решений по защите информации**
- **Авторизованное обучение информационной безопасности**
- **Партнеры компании Cisco Systems и их специализация**
- **Архитектура безопасности SAFE**
- **Сертификация решений по требованиям информационной безопасности**
- **Ссылки на дополнительную информацию на сайте компании Cisco Systems**

ИНФОРМАЦИЯ ОБ УСЛУГАХ



Сложность и масштабность современных сетей определенным образом сказываются на обеспечении их безопасности. Это не такое простое дело, и оно требует квалификации и опыта. Группа консультантов и системных инженеров компании Cisco Systems готова помочь Вам:

- в разработке плана и дизайна защищенного решения;
- во внедрении и настройке средств защиты согласно разработанному дизайну;
- в оптимизации уже внедренных и настроенных средств защиты;
- в поддержке внедренных решений при помощи круглосуточной службы технической поддержки (Technical Assistance Center, TAC);
- в аудите защищенности внедренного решения в соответствии с требованиями архитектуры SAFE.

Помимо высококвалифицированной помощи со стороны компании Cisco Systems, существует возможность обращения к нашим уполномоченным партнерам, которые могут предложить различные услуги, в т. ч. и по аутсорсингу безопасности (Managed Security Service), что особенно актуально в условиях нехватки времени и людей для круглосуточного обеспечения информационной безопасности корпоративных ресурсов.

Дополнительная информация: *http://www.cisco.com/go/securityconsulting*

ВИДЫ УСЛУГ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Все услуги компании Cisco в области информационной безопасности могут быть разделены на 5 категорий, соотносящихся с этапами жизненного цикла защищаемой сети:

1. **Планирование.** На данном этапе осуществляется подготовка и планирование действий в случае наступления инцидентов безопасности. К услугам, предоставляемым на данном этапе, можно отнести:
    - Incident Readiness Assessment
    - IP Telephony Security Review
    - External Security Posture Assessment
    - Internal Security Posture Assessment
    - Wireless Security Posture Assessment
    - Dial-Up Security Posture Assessment
2. **Дизайн.** На данном этапе разрабатывается проект многоуровневой и эшелонированной защиты от злоумышленников, червей, вредоносных программ и других угроз. К услугам, предоставляемым на данном этапе, можно отнести:
    - Incident Readiness Design Development
    - Network Security Design Review
    - Network Security Design Development
3. **Внедрение.** На данном этапе разрабатывает план внедрения средств защиты и настройки защитных мер, предложенных на предыдущем этапе. К услугам, предоставляемым на данном этапе, можно отнести:
    - Network Security Implementation Plan Review
    - Network Security Implementation Engineering
    - Cisco Security Agent Implementation Service
    - Network Admission Control Implementation Service
4. **Эксплуатация.** На данном этапе круглосуточно работающий центр реагирования на инциденты компании Cisco Systems помогает заказчикам обнаруживать и своевременно реагировать на различные угрозы.
5. **Оптимизация.** На данном этапе производится регулярный аудит происходящих в сети изменений и осуществляется оптимизация существующих защитных решений в соответствие с новыми условиями.

ПОДДЕРЖКА ОБОРУДОВАНИЯ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Поддержка оборудования и системного ПО

Для поддержки поставляемых средств защиты и системного программного обеспечения (ОС IOS) компания Cisco предлагает услуги SMARTnet (удаленные и с выездом сервисного инженера на место), включающие в себя:

- Получение основных и промежуточных обновлений программного обеспечения Cisco IOS® через сайт www.cisco.com или на физических носителях
- Постоянный (24x7) авторизованный доступ к сайту www.cisco.com
- Постоянный (24x7) доступ к Центру Технической Поддержки Cisco (Cisco TAC)
  - ✓ через Web-сайт и по электронной почте – для решения проблем низкого приоритета (P3, P4)
  - ✓ по телефону – для решения первоочередных проблем (приоритеты P1 и P2), а также для эскалации критических ситуаций.
- Упреждающая замена запчастей (возможны три варианта, в зависимости от срочности):
  - ✓ SMARTnet 8x5xNBD — гарантированная доставка запчастей на следующий рабочий день, если запрос делается до 15.00 по местному времени.
  - ✓ SMARTnet 8x5x4 — гарантированная доставка запчастей с 9.00 до 17.00 с понедельника по пятницу. Время доставки замены – 4 часа. На территории Российской Федерации услуга доступна только в Москве и Санкт Петербурге.
  - ✓ SMARTnet 24x7x4 — гарантированная доставка запчастей, 24 часа в сутки, 7 дней в неделю. Время доставки замены – 4 часа. На территории Российской Федерации услуга доступна только в Москве и Санкт Петербурге.
- Выделение выездного инженера (только для услуг SMARTnet Onsite), в зависимости от выбранного варианта доставки и существующих ограничений.

Поддержка прикладного ПО

Кроме поддержки оборудования и системного ПО, Cisco также предлагает услуги технической поддержки прикладного программного обеспечения (Software Application Support, SAS), которые включают в себя следующие компоненты:

- Доступ к Web-ресурсам и инструментам Cisco Connection Online (CCO).
- Круглосуточный доступ к Центру Технической Поддержки Cisco (Cisco TAC).
- Предоставление обновлений программного обеспечения (updates, minor upgrades – изменение 3-ей цифры в номере версии).

В качестве опции для некоторых продуктовых линеек возможно также предоставление любых обновлений программного обеспечения (Software Application Support Plus Upgrades, SASU), включая major upgrades (изменение 2-й или 1-й цифры в номере версии).

Поддержка систем обнаружения и предотвращения атак

Для систем обнаружения и предотвращения атак Cisco IPS 4200, модулей Catalyst IDSM-2 и NM-IDS для коммутаторов и маршрутизаторов, а также Cisco IOS IPS компания Cisco предлагает специальные услуги Cisco Services for IPS, которые включают в себя как все составляющие SMARTnet, так и регулярное обновление сигнатур атак.

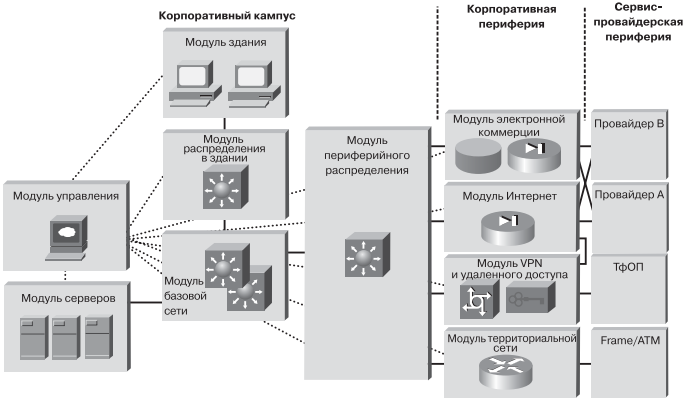
Другие виды технической поддержки

Специально для операторов связи компания Cisco предлагает 2 типа услуг по технической поддержки – удаленной SP Base и с выездом сервисного инженера на место SP Base Onsite. Решения для малого и среднего бизнеса (SMB Solutions) могут поддерживаться в рамках специальной сервисной программы – SMB Support Assistant.

Дополнительная информация: *http://www.cisco.com/go/smartnet*

АРХИТЕКТУРА SAFE

Главная цель архитектуры Cisco Systems для безопасности корпоративных сетей (SAFE) состоит в том, чтобы предоставить заинтересованным сторонам информацию о современном опыте проектирования и развертывания защищенных сетей. SAFE призвана помочь тем, кто проектирует сети и анализирует требования к сетевой безопасности. SAFE исходит из принципа глубокоэшелонированной обороны сетей от внешних атак. Этот подход нацелен не на механическую установку межсетевого экрана и системы обнаружения атак, а на анализ ожидаемых угроз и разработку методов борьбы с ними. Эта стратегия приводит к созданию многоуровневой системы защиты, при которой прорыв одного уровня не означает прорыва всей системы безопасности. SAFE основывается на продуктах компании Cisco Systems и ее партнеров.



Архитектура Cisco SAFE с максимальной точностью моделирует функциональные потребности современных корпоративных сетей и решает следующие задачи (в порядке приоритетности):

- Безопасность и борьба с атаками на основе политик.
- Внедрение мер безопасности по всей инфраструктуре (а не только на специализированных устройствах защиты).
- Безопасное управление и отчетность.
- Аутентификация и авторизация пользователей и администраторов для доступа к критически важным сетевым ресурсам.
- Обнаружение атак на критически важные ресурсы и подсети.
- Поддержка новых сетевых приложений.

Основные достоинства Cisco SAFE

- Обеспечивает основу для построения безопасных, доступных, интегрированных сетей.
- Открытая модульная структура.
- Упрощает разработку, внедрение и управление сетевой безопасностью.
- Обеспечивает масштабируемость решений.
- Позволяет эффективное поэтапное внедрение.
- Использует лучшие продукты и услуги сетевой безопасности благодаря интеграции решений экосистемных партнеров.
- Архитектура Cisco SAFE, дополняемая лучшими экосистемными партнерами, продуктами и услугами, позволяет пользователям внедрять надежные, безопасные сети в эпоху Интернет-экономики.

Дополнительная информация

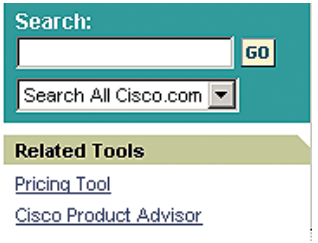
На сайте Cisco Systems подробно описываются различные аспекты реализации архитектуры SAFE:

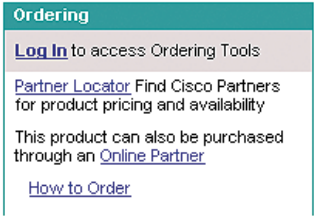
- безопасность крупных компаний, а также предприятий малого и среднего бизнеса,
- безопасность IP-телефонии, беспроводных сетей,
- отражение червей и атак канального уровня,
- особенности внедрения систем обнаружения атак и средств построения VPN и т. д.

Дополнительная информация: *http://www.cisco.com/go/safe*

ЦЕНЫ, ПОРЯДОК ЗАКАЗА И ПОЛИТИКА ЛИЦЕНЗИРОВАНИЯ

Информация о ценах может быть получена из меню “Pricing Tool” раздела “Related Tools” на странице с описанием выбранного решения. Данное меню доступно только для зарегистрированных пользователей сайта www.cisco.com. В некоторых случаях данное меню может быть недоступно, и вместо него отображается раздел “Ordering” (“Заказ”), в котором всю необходимую информацию можно получить у партнеров компании Cisco Systems.





Перейдя по указанной в разделе “Ordering” ссылке, Вы попадаете в форму поиска партнеров “Partner Locator” (“Поиск партнера”). Мы рекомендуем Вам перейти на вкладку “Advanced Search” (“Расширенный поиск”), на которой Вы вводите всю интересующую Вас информацию:

- Страна, в которой работает партнер.
- Регион или город (если необходимо).
- Уровень сертификации (если необходимо).
- Специализация. Мы рекомендуем обращаться к партнерам, имеющим соответствующую специализацию по информационной безопасности, – VPN Security, VPN/Security Services или Security VPN/Firewall Express. Выбрать данные типы специализации можно в полях Technology Specialization, Other Specialization и Additional Partner Programs соответственно.

Коды продуктов для составления спецификации указаны в разделе “Product Ordering Information” на странице с описанием выбранного решения.

АВТОРИЗОВАННОЕ ОБУЧЕНИЕ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Cisco Learning Partner – это партнеры компании Cisco Systems, которые проводят авторизованное обучение по утвержденным программам и курсам. В данных учебных центрах:

- используются различные формы обучения: очная, заочная (дистанционная), индивидуальная;
- преподавательский состав представлен инструкторами, имеющими звания CCSI (Certified Cisco Systems Instructor), имеющими большой опыт практической работы в разработке и обслуживании сетей в России и за рубежом, а также квалификационное звание CCIE (Cisco Certified Internetwork Expert);
- осуществляется подготовка к сдаче квалификационных экзаменов по программе Cisco Career Certification.

По информационной безопасности компания Cisco Systems предлагает две сертификации, ценящиеся во всем мире:

- Cisco Certified Internetwork Expert (CCIE Security);
- Cisco Certified Security Professional (CCSP).

Для получения указанных статусов необходима сдача соответствующего экзамена и прохождение ряда курсов, которые читаются на территории России в авторизованных учебных центрах компании Cisco Systems, а также в сетевых академиях Cisco Systems (Cisco Networking Academy).

Дополнительная информация: *http://www.cisco.com/go/securitytraining*

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ

В мире и России существует множество российских и международных стандартов и требований по информационной безопасности – Sarbanes Oxley Act, ISO 17799, GLBA (Gramm-Leach-Bliley Act), HIPAA, Базель II, Руководящие документы Федеральной службы по техническому и экспортному контролю (бывшая Государственная техническая комиссия при Президенте России), «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», ГОСТ Р ИСО/МЭК 15408 и другие. Решения Cisco Systems по информационной безопасности соответствуют основным требованиям этих стандартов и рекомендаций. Во многих случаях это подтверждается соответствующими сертификатами.

В России компания Cisco Systems сертифицировала свои межсетевые экраны Cisco Pix и Catalyst FWSM, маршрутизаторы с ОС Cisco IOS, коммутаторы Cisco Catalyst, системы обнаружения атак Cisco IDS 42xx и Catalyst IDSM-2, Cisco Security Agent, а также система управления CiscoWorks VPN/Security Management Solution на соответствие техническим условиям, руководящим документам и заданиям по безопасности.

Общее число выданных Федеральной службой по техническому и экспортному контролю (ФСТЭК) компании Cisco Systems сертификатов превысило 150, что существенно превышает число сертификатов, полученных какой-либо другой компанией (российской или зарубежной), работающей на рынке информационной безопасности.

Дополнительная информация: *http://www.cisco.com/go/securitycert*

ПАРТНЕРЫ CISCO SYSTEMS ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С целью оказания помощи нашим заказчикам при внедрении, настройке и эксплуатации средств обеспечения информационной безопасности компания Cisco Systems уполномочила ряд своих партнеров на решение этих задач. Для уверенности в качестве предоставляемых услуг были введены несколько специализаций, подтверждающих уровень компетенции компании-партнера (в порядке возрастания):

- Security VPN/Firewall Express,
- VPN Security,
- VPN Security Services.

Подробную информацию о партнерах, имеющих данный статус, можно получить на сайте компании Cisco Systems в разделе «Partner Locator» («Поиск партнера»), для чего необходимо перейти на вкладку «Advanced Search» («Расширенный поиск»), на которой Вы вводите всю интересующую Вас информацию:

- Страна, в которой работает партнер.
- Регион или город (если необходимо).
- Уровень сертификации (если необходимо).
- Специализация. Мы рекомендуем обращаться к партнерам, имеющим соответствующую специализацию по информационной безопасности, – VPN Security, VPN/Security Services или Security VPN/Firewall Express. Выбрать данные типы специализации можно в полях Technology Specialization, Other Specialization и Additional Partner Programs соответственно.

Дополнительная информация: *http://www.cisco.com/go/partnerlocator/* и
http://www.cisco.com/en/US/partner/partners/index.html

ССЫЛКИ НА ДОПОЛНИТЕЛЬНУЮ ИНФОРМАЦИЮ НА САЙТЕ CISCO

Компания Cisco Systems предлагает большой спектр решений в сфере информационной безопасности. С целью ускорения доступа к информации о них в данном разделе приведены дополнительные ссылки на разделы сайта Cisco Systems, в которых описаны решения и инициативы в этой области (другие ссылки можно найти в данной брошюре на страницах с описанием каждого продукта).

http://www.cisco.com/securitynow	**– Подход Cisco Systems к защите бизнеса**
http://www.cisco.com/go/security	**– Все о решениях Cisco по информационной безопасности**
http://www.cisco.com/go/ibns	**– Инициатива Identity Based Networking Services**
http://www.cisco.com/go/outbreak	**– Решения Cisco Systems по отражению и локализации вирусных эпидемий**
http://www.cisco.com/go/prevention	**– Решения Cisco Systems по предотвращению атак**
http://www.cisco.com/go/routersecurity	**– Все о безопасности маршрутизаторов Cisco**
http://www.cisco.com/go/v3pn	**– Voice and video enabled VPN**
http://www.cisco.com/go/dmvpn	**– Dynamic Multipoint VPN**
http://www.cisco.com/go/mpls	**– MPLS VPN**
http://www.cisco.com/go/ipsec	**– Cisco IPSec VPN**
http://www.cisco.com/go/sslvpn	**– Решения Cisco Systems в области SSL VPN**
http://www.cisco.com/go/ssl	**– Решения Cisco Systems по управлению SSL-трафиком**
http://www.cisco.com/go/easyvpn	**– Easy VPN**
http://www.cisco.com/go/ipcsecurity	**– Решения Cisco Systems по защите IP-телефонии**
http://www.cisco.com/go/psirt	**– Cisco Security Advisories and Notices**
http://www.cisco.com/go/ipsalert	**– IPS Alert Center**
http://www.ciscowebtools.com/spb/	**– Cisco Security Policy Builder**
http://www.cisco.com/go/solutiondesigner	**– Cisco Security Solution Designer**
http://www.cisco.com/go/advisor	**– Cisco Security Product Advisor**
http://www.cisco.com/go/midsizedsecurity	**– Решения Cisco по безопасности для малых и средних предприятий**
http://www.cisco.com/go/theft	**– Решение Cisco по предотвращению утечки информации**
http://tools.cisco.com/MySDN/Intelligence/home.x	**– MySDN: Achieve Security Through Intelligence**

По результатам опроса компании Ernst&Young, проведенного в России, только 40% компаний уверены, что могут обнаружить атаки на свои ресурсы! А это значит, что оставшиеся 60% могут даже и не знать о том, что они подверглись нападению со стороны злоумышленников или вредоносных программ. Но мы надеемся, что Вы не из их числа. Для полной уверенности Вы можете проверить свою сеть «на прочность», обратившись к нам или одному из наших партнеров с целью проведения аудита безопасности (дополнительную информацию об этом смотрите на стр. 60).

Если у Вас все хорошо и нет проблем с информационной безопасностью, то мы искренне рады за Вас. Тогда просто посмотрите нашу брошюру с самого начала и, возможно, Вы найдете для себя что-то новое и полезное.

КОНТАКТЫ

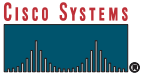
Связаться с нами можно различными способами:

- По телефону:
  - ✓ В Москве – +7 (095) 961-1410
  - ✓ В Санкт-Петербурге – +7 (812) 346-7733
  - ✓ В Алматы – +7 (3272) 58-4658
  - ✓ В Киеве – +7 (38044) 490-3600

- По электронной почте – *security-request@cisco.com*

- Через форму обратной связи на нашем сайте – *http://www.cisco.com/global/RU/contacts/feedback.shtml*

Составитель: Алексей Лукацкий



Cisco Systems
Россия, 113054 Москва
бизнес центр “Риверсайд Тауэрз”
Космодамианская наб., 52
Стр. 1, 4-й этаж
Тел.: +7 (095) 961 14 10
Факс: +7 (095) 961 14 69
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099 Алматы
бизнес центр “Самал 2”
Ул. О. Жолдасбекова, 97
блок А2, этаж 14
Тел.: +7 (3272) 58 46 58
Факс: +7 (3272) 58 46 60
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004 Киев
бизнес центр “Горайзон Тауэрз”
Ул. Шовковична, 42-44, этаж 9
Тел.: (044) 490 36 00
Факс: (044) 490 56 66
Internet: www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the **Cisco Connection Online Web site at http://www.cisco.com.**
//www.cisco.ru.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China (PRC) • Colombia • Costa Rica • Czech Republic • Denmark England • Finland • France • Germany • Greece • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxemburg • Malaysia Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Russia • Saudi Arabia • Scotland • Singapore South Africa • Spain • Sweden • Switzerland • Taiwan, ROC • Thailand • Turkey • United Arab Emirates • United States • Venezuela