ЗАЩИТИТЬ БИЗНЕС. сейчас

(издание VIII)

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 около 500 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 и странах СНГ наши решения проходят сертификацию в соответствующих регулирующих органах. Например, в Российской Федерации это Федеральная служба по техническому и экспортному контролю (бывшая Государственная техническая комиссия при Президенте России) и ФСБ России. В частности, решения компании Cisco имеют свыше 380 сертификатов ФСТЭК, 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, Санкт-Петербурге, Новосибирске, Краснодаре, Тюмени, Казани, Екатеринбурге, Нижнем Новгороде, Самаре, Владивостоке, Сургуте, Киеве и Алматы) и с отгрузкой в день авторизации замены (для остальных регионов). С целью предоставления телефонных консультаций на русском языке в Москве функционирует центр обработки заявок и технического обслуживания (Technical Assistance Center – TAC).

Стремясь предоставить заказчикам Cisco максимальный спектр услуг, в России открыто подразделение Advanced Services, оказывающее услуги технологического консалтинга и проактивной поддержки, в т. ч. и по информационной безопасности. В рамках этого подразделения действует отдел Advisory Services, который, опираясь на информацию о бизнес-задачах заказчиков Cisco, консультирует их по вопросам внедрения новых защищенных услуг, построения современной защищенной сетевой инфраструктуры и увязывания безопасности с бизнесом предприятия.

Все это позволило нам занять первое место на российском рынке информационной безопасности (по данным ежегодного обзора CNews «Средства защиты информации и бизнеса 2008», размещенного по адресу: http://www.cnews.ru/reviews/free/security2008/.
Аналогичный результат достигнут нами и на рынках стран СНГ.

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 не только включает в себя 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 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 6 основных элементов, отражающих эволюцию стратегии Cisco Self-Defending Network (SDN).

1. ***Защищенная сетевая платформа (Secure Network Platform).*** Безопасность давно перестала быть опцией при построении сетей. Она стала неотъемлемой частью и свойством сетей, которые строятся на базе оборудования компании Cisco – маршрутизаторов Cisco ISR и более старших моделей, коммутаторов Catalyst, точек беспроводного доступа и т. д.
2. ***Сетевая безопасность (Network Security).*** Помимо механизмов, интегрированных в сетевое оборудование, компания Cisco предлагает и выделенные защитные устройства, повышающие уровень защищенности корпоративных и операторских сетей – межсетевые экраны Cisco Pix, системы предотвращения атак Cisco IPS и Cisco Guard, средства построения VPN, многофункциональные устройства Cisco ASA и т. д.
3. ***Доверенные оконечные устройства (Trusted End Point).*** Наиболее эффективная защита бизнес-ресурсов от злоумышленников и вредоносных программ достигается только в случае эшелонированной обороны, распределенной по всей сети, включая и оконечные устройства (ПК, лэптопы, принтеры, IP-телефоны и т. д.). Реализуется это за счет технологии Cisco NAC, систем защиты ПК, серверов и лэптопов Cisco Security Agent и т. п.
4. ***Защита и контроль контента (Content Security).*** Обеспечивая сетевую безопасность нельзя забывать и про защиту прикладного уровня, в частности, электронной почты, IM, P2P и т.д. Программно-аппаратные комплексы IronPort E-mail Security Appliance и IronPort Web Security Appliance, а также ряд других систем решают эту задачу.
5. ***Защита приложений (Application Security).*** Помимо защиты на уровне сети, современное предприятие требует защиты и своих бизнес-приложений и баз данных. Компания Cisco предлагает для этой задачи такие системы, как Cisco ACE XML Gateway, и ряд других решений.
6. ***Управление, контроль соответствия, идентификация (Management & Policy Control & Identity).*** Разнообразие защитных и защищаемых систем, различные политики безопасности, большое число требований и стандартов безопасности существенно усложняют задачу управления информационной безопасностью в компании. Cisco Security Manager, Cisco MARS, Cisco Network Compliance Manager, Cisco Secure ACS облегчают ее решение.

CISCO INTEGRATED SERVICES ROUTERS

Cisco Integrated Services Routers (ISR) – лучшие в своем классе маршрутизаторы с интегрированными сервисами и с оптимизированными функциями безопасности для защиты передаваемых данных, голоса и видео. Маршрутизаторы Cisco серии 800, 1800, 2800 и 3800 идеально подходят как для больших компаний с территориально распределенными филиалами, так и для малого офиса.

Маршрутизаторы ISR включают в себя набор защитных технологий и механизмов, предназначенных для построения надежной и защищенной сети в соответствии со стратегией Cisco Self-Defending Network (SDN). Маршрутизаторы ISR хорошо интегрируются с другими компонентами стратегии SDN, такими, как Cisco MARS, Cisco ACS, NAC и т. д.

В маршрутизаторах ISR применяется программное обеспечение Cisco IOS Advanced Security, которое представляет собой набор функций защиты, реализованных в операционной системе Cisco IOS. Благодаря Cisco IOS Advanced Security в каждый маршрутизатор ISR, помимо межсетевого экрана Cisco IOS Firewall, входят подсистема построения VPN (MPLS, DMVPN, Easy VPN), а также подсистема предотвращения атак Cisco IOS IPS, встроенный сервер сертификатов PKI и многие другие защитные подсистемы.

Управление маршрутизаторами Cisco ISR с точки зрения безопасности может осуществляться как с помощью встроенной системы управления Cisco Router and Security Device Manager, так и с помощью системы централизованного управления всеми решениями Cisco по безопасности – Cisco Security Manager. Мониторинг Cisco ISR и сбор сигналов тревоги с них могут быть осуществлены с Cisco MARS, а также иных систем управления событиями безопасности.

Для удовлетворения потребностей рынка в решении VPN, удовлетворяющем требованиям отечественного законодательства, компания Cisco в сотрудничестве с ведущими локальными разработчиками создала модули построения виртуальных частных сетей для маршрутизаторов Cisco ISR, которые использует сертифицированное криптографическое ПО:

- NME-RVPN – ПО компании «С-Терра СиЭсПи» (Россия);
- NME-RVPN ViPNet – ПО компани «Инфотекс» (Россия);
- KazVPN – ПО компании ZorSoft (Казахстан);
- «Булава» – ПО компании НПО «Криптон» (Украина).

Дополнительная информация: http://www.cisco.com/go/routersecurity, а также на стр. 8 и 10.

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 входят подсистема построения VPN (IPSec, SSL, MPLS, GRE, L2F и L2TP), а также подсистема предотвращения атак Cisco IOS IPS, способная отражать свыше 1400 распространенных атак и методов сетевой разведки, используемых злоумышленниками.

Основные возможности

- Контроль и категорирование 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)
- Технология Flexible Packet Matching
- МСЭ с анализом на прикладном уровне для фильтрации и контроля интернет-пейджеров (IM) и пиринговых приложений (P2P)
- VRF-Aware DNS
- Поддержка технологий EasyVPN и SSL VPN
- Сертификат ФСТЭК

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 IOS TRUST AND IDENTITY

Cisco IOS Trust and Identity – это набор технологий, интегрированных в операционную систему сетевого оборудования компании Cisco – Cisco IOS и включающих в себя механизмы AAA (аутентификация, авторизация и регистрация событий), PKI, Secure Shell (SSH), SSL и 802.1x. Cisco AAA позволяет реализовать инфраструктуру контроля доступа на маршрутизаторах и серверах доступа, Cisco PKI позволяет организовать строгую и надежную аутентификацию, авторизацию и обеспечение конфиденциальности для сетевых приложений, Cisco SSH обеспечивает защищенный доступ к маршрутизаторам, и наконец, Cisco SSL защищает трафик управления между web-браузерами и ресурсами маршрутизатора.

Основные возможности

- Поддержка механизмами AAA широкого спектра приложений и протоколов – 802.11b, Cable&DSL, DialUp, GPRS, IPSec, MPLS, OSP, PDSN, SIP, DCN, VoIP и т. д.
- Локальная поддержка AAA или переадресация запросов на внешние серверы с помощью RADIUS, TACACS+ и Kerberos
- Поддержка протокола DIAMETER
- Интегрированный Cisco IOS Certificate Authority
- Распределение CRL через протокол SCEP
- Совместимость с x.509v3
- Поддержка Certificate-based Access Control (CBAC)
- Поддержка Certificate Auto-Enroll
- Поддержка N-Tier Certificate Chaining

Дополнительная информация: http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html

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, согласно которому защищенная сеть должна строиться на защищенном фундаменте, которым являются маршрутизаторы. Основное предназначение NFP –защита сетевой инфраструктуры, в т. ч. и у операторов связи.

Основные возможности

- Автоматическое отключение опасных команд и функций с помощью механизма AutoSecure
- Контроль загрузки центрального процессора
- Защищенный доступ к устройству при помощи SSHv2, 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 типа «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
- Система анализа и фильтрации пакетов Flexible Packet Matching

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 500, 29xx, 35xx, 37xx, 4500, 4900 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
- Сертификат ФСТЭК

CISCO WIRELESS LAN CONTROLLER

Cisco Wireless LAN Controller – решение, обеспечивающее простоту развертывания и управление функциями защиты в беспроводной сети для компаний любого масштаба. Cisco Wireless LAN Controller может быть выполнен в виде отдельного устройства (Cisco 4400 или Cisco 2000 Series WLAN Controller), в виде модулей, установленных в маршрутизаторы Cisco ISR 2800, 3800 и 3700 (WLCM), а также в виде сервисного модуля, установленного в коммутатор Catalyst 6500 (Wireless Service Module, WiSM). В зависимости от реализации беспроводной контроллер может управлять разным количеством точек беспроводного доступа – от 6 до 300.

Основные возможности

- Поддержка стандартов и протоколов 802.11i (WPA2), Wi-Fi Protected Access (WPA), WEP
- Поддержка различных методов аутентификации по протоколу 802.1x (EAP, PEAP, EAP-TLS, EAP-TTLS, EAP- FAST, Cisco LEAP и SIM)
- Поддержка свыше 20 стандартов безопасности (включая FIPS 140-2, X.509 и т. д.)
- Обнаружение, локализация и блокирование несанкционированно установленных точек доступа
- Встроенная беспроводная система предотвращения атак
- Поддержка 802.11a, 802.11b, 802.11g, 802.11d, 802.11h
- Поддержка Cisco NAC
- Поддержка функции Layer 3 fast secure roaming для WLAN (поддержка Proactive Key Caching, PKC)
- Поддержка SNMPv3
- Поддержка аутентификации пользователей с использованием RADIUS
- Возможность назначения VLAN
- Разграничение доступа с помощью ACL
- Централизованное управление через интуитивно понятный web-интерфейс
- Защищенное управление с помощью HTTPS или SSH
- Терминирование IPSec VPN (для 4400 Series)

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

CISCO ADAPTIVE SECURITY APPLIANCE

Многофункциональный программно-аппаратный комплекс Cisco ASA 5500 предназначен для решения сразу нескольких задач – разграничения доступа к сетевым ресурсам, защиты от атак, защиты взаимодействия с удаленными территориями, блокирования вирусов, червей, шпионского ПО и других вредоносных программ, спамаи атак типа «фишинг». 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 (по мере разработки новых интегрируемых модулей) – 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, не имеющих возможности внедрить несколько отдельных защитных устройств.

Основные возможности

- Управление как с помощью Cisco Adaptive Security Device Manager, так и с помощью CLI
- Поддержка до 100 VLAN
- Поддержка отказоустойчивых конфигураций (Active/Standby, Active/Active и LAN-based Failover)
- Поддержка виртуальных и прозрачных МСЭ
- Поддержка Cisco WAAS
- Механизм Syslog to ACL Correlation
- Контроль до 24 сетевых интерфейсов
- Поддержка EIGRP, в т. ч. через NAT, а также OSPF с MD5
- Поддержка multicast
- Встроенный DHCP-сервер и поддержка DHCP Relay
- Встроенный клиент NTPv3
- Локальная или централизованная аутентификация на TACACS+ или RADIUS серверах
- Поддержка SNMPv2 и SNMPv2c
- Поддержка стандарта обмена сигналами тревоги SDEE
- Импорт и экспорт конфигурации с помощью TFTP, HTTP, HTTPS и SCP
- Удаленное управление с помощью SSHv1 или SSHv2
- Хранение различных конфигураций и образов ПО на Compact Flash
- Автоматическое затирание памяти при попытке несанкционированного доступа
- Расширенные функции выявления неисправностей
- Уведомление администратора по e-mail о критических событиях

Дополнительная информация: http://www.cisco.com/go/asa , а также на стр.32, 33

МНОГООБРАЗИЕ МОДЕЛЕЙ CISCO ASA 5500

	5505 Base/Security Plus	5510 Base/Security Plus	5520	5540	5550	5580-20	5580-40
Производительность МСЭ, Мбит/сек	150	300	450	650	1200	5 Гбит/сек (реальный HTTP), 10 Гбит/сек (Jumbo-фреймы)	10 Гбит/сек (реальный HTTP) , 20 Гбит/сек (Jumbo-фреймы)
Производительность МСЭ и отражения атак (МСЭ + модуль IPS), Мбит/сек	Недоступно	До 150 с AIP-SSM-10 До 300 с AIP-SSM-20	До 225 с AIP-SSM-10 До 375 с AIP-SSM-20	До 450 с AIP-SSM-20	Недоступно	Недоступно	Недоступно
Производительность IPS, Мбит/сек	100	170	225	325	425	1 Гбит/сек	1 Гбит/сек
Количество одновременно поддерживаемых сессий	10 000; 25 000*	50 000; 130 000*	280 000	400 000	650 000	1 000 000	2 000 000
Число IPSec VPN-туннелей	10; 25**	250	750	5000	5000	10 000	10 000
Число SSL VPN-туннелей	25	250	750	2500	5000	10 000	10 000
«Виртуальные» МСЭ (включено/максимум)	0/0	0/0 (Base); 2/5 (Security Plus)	2/20	2/50	2/50	2/50	2/50
Кластеризация и балансировка VPN	Нет	Да	Да	Да	Нет	Да	Да
Поддерживаемые физические интерфейсы	8 Fast Ethernet, 2 с поддержкой питания по Ethernet (PoE)	5 Fast Ethernet / 2 Gigabit Ethernet и 3 Fast Ethernet*** + 1 порт управления	1 Gigabit Ethernet + 1 Fast Ethernet	1 Gigabit Ethernet + 1 Fast Ethernet	8 Gigabit Ethernet / 4 SFP Fiber + 1 Fast Ethernet	2-10/100/1000 Management +4-10/100/1000 (with ASA5580-4GE-CU) + 4 GE SR LC (with ASA5580-4GE-FI) +2 10GE SR LC (with ASA5580-2X10GE-SR)	2-10/100/1000 Management +4-10/100/1000 (with ASA5580-4GE-CU) + 4 GE SR LC (with ASA5580-4GE-FI) +2 10GE SR LC (with ASA5580-2X10GE-SR)
Поддержка дополнительного четырехпортового модуля Gigabit Ethernet	Нет	Да	Да	Да	Нет	Не применимо	Не применимо
Поддерживаемые логические интерфейсы VLAN 802.1q	3 (без транкинга); 20	50; 100*	150	200	250	100	100
Слот для SSC / SSM	Да (SSC)	Да (SSM)	Да (SSM)	Да (SSM)	Нет	Да (6-IC)	Да (6-IC)
Форм-фактор	В настольном исполнении	Для монтажа в стойке, 1 RU	Для монтажа в стойке, 1 RU	Для монтажа в стойке, 1 RU	Для монтажа в стойке, 1 RU	Для монтажа в стойке, 4 RU	Для монтажа в стойке, 4 RU

* При помощи дополнительной лицензии.
** При помощи дополнительной лицензии (в базовой комплектации – 2).
*** Доступно с лицензиями Cisco ASA 5510 Security Plus.

МЕЖСЕТЕВОЙ ЭКРАН CISCO ASA

Программно-аппаратный межсетевой экран (МСЭ) Cisco ASA 5500 – 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 ASA 5500, 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 20 Гбит/сек
- Обеспечение отказоустойчивости (в т.ч. для VPN и SIP) в режимах Active/Standby или Active/Active
- Поддержка протокола GTP/GPRS
- Возможность функционирования в прозрачном режиме на канальном уровне (transparent firewall)
- Поддержка до 50 виртуальных межсетевых экранов на одном устройстве
- Отказоустойчивость (включая поддержание VPN-туннелей)
- Скрытие топологии защищаемой сети с помощьютрансляции адресов (NAT) и портов (PAT)
- Контроль всего спектра протоколов для IP-телефонии и мультимедиа – H.323, SIP, SCCP, MGCP, RTSP, TAPI/JTAPI over CTIQBE
- Поддержка IPv6
- Интеграция с CSA для маркирования и приоритезации трафика
- Специальные модули инспекции протоколов (Application Inspection and Control Engine)
- Расширенный анализ Web-трафика (контроль HTTP-команд и методов, обнаружение скрытой передачи данных и т.п.)
- Контроль инкапсулированных протоколов (P2P, IM, GoToMyPC и т.п.)
- Расширенная инспекция и защита унифицированных коммуникаций (TLS Proxy, Phone Proxy, Mobility Proxy, Presence Federation Proxy)
- Расширенный анализ FTP, ESMTP, SNMP, ICMP, Sun RPC и NIS+
- Поддержка фрагментированного и сегментированного трафика
- Поддержка свыше 100 предустановленных политик контроля разных типов приложений
- Различные списки контроля доступа (по интерфейсам, по времени, по пользователям, по группам), включая динамические

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

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 инспекцию трафика на скоростях свыше 10 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 операционной системе 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
- Transparent Firewall NAT/PAT
- Балансировка нагрузки GGSN
- Поинтерфейсный DHCP replay
- BGP stub
- Интеграция с WAAS
- Расширенная инспекция MS-RPC и SIP
- Поддержка RTSP PAT и H.323 GUP
- IOS auto state
- TCP state bypass
- Поддержка регулярных выражений
- Фильтрация HTTPS
- Интеграция с PISA
- Поддержка Virtual Switching System (VSS)

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.

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 и 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
- Поддержка отказоустойчивости за счет динамической смены маршрута на резервный маршрутизатор
- Механизм прозрачности МСЭ (функционирование на канальном уровне)
- Расширенная регистрация событий безопасности
- Фильтрация и блокирование трафика интернет- пейджеров (IM), пиринговых приложений (P2P) и других сетевых приложений благодаря гибкому анализу на прикладном уровне
- Определяемые пользователем и расширяемые политики проверки объектов протокола HTTP (длина URL, заголовки HTTP и др.)
- Возможность использования конфигурации на основе CPL (Class-based Policy Language) для защиты от уязвимостей и HTTP-атак
- Предотвращение DoS-атак на основе сессионных политик и политики контроля входного потока

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

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

Причины выбора старших моделей Cisco ASA (5550 и выше)

- 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 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 защитыпериметра небольших предприятий идомашних пользователей
- Снижение стоимости внедрения в существующую инфраструктуру
- Тесная интеграция с механизмамимашрутизации, QoS и другими сетевымифункциями
- Дополнительный уровень защиты

Причины выбора младших моделей Cisco ASA (5540 и ниже)

- 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

СХЕМА ЛИЦЕНЗИРОВАНИЯ CISCO ASA 5500 И CISCO FWSM

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 ASA 5505.

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 ASA 5540, 5550 и 5580.

Лицензирование функции UC Proxy

Лицензия UC Proxy позволяет расширить функциональность Cisco ASA 5500 в части контроля и защиты унифицированных коммуникаций. Данная лицензия поддерживает 4 функции.

Тип лицензии	Описание
TLS Proxy	• Расшифрование и инспекция протоколов сигнализации
Phone Proxy	• Терминирование и инспекция SRTP/TLS-трафика
Mobility Proxy	• Обеспечение защищенного взаимодействия с Cisco Unified Mobile Communicator
Presence Federation Proxy	• Защита Presence-решений компаний Cisco и Microsoft

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-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-битный DSA, 56-битный DES, 168-битный 3DES, 256-битный AES и 128-битный RC4

Все модели Cisco ASA 5500 по умолчанию поставляются с лицензией VPN-DES с возможностью расширения до VPN-3DES/AES.

Лицензирование по расширенным функциям

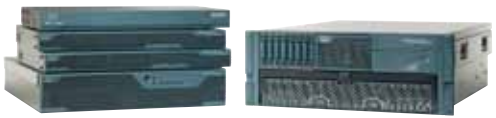
Данный тип лицензии позволяет активировать расширенные функции.

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. 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 IPS



Cisco IPS является центральным компонентом решений Cisco Systems по отражению атак. Наряду с традиционными механизмами в Cisco 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, Risk Rating, Threat 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 (сигна-туры, аномалии, эвристика, отклонения от RFC и т. п.)
- Защита от методов обхода
- Возможность работы одновременно в двух режимах – обнаружения и предотвращения атак
- Обнаружение атак на IP-телефонию и АСУ ТП (SCADA)
- Автоматический выбор реагирования в зависимости от степени угрозы
- Обнаружение атак в инкапсулированном трафике MPLS, GRE, IPv6, Mobile IP-in-IP
- Интеграция с Cisco ASA 5500 и Cisco Secuirty Agent для блокирования атак
- Поддержка нескольких виртуальных сенсоров на одном устройстве
- Интеграция с коммутаторами и маршрутизаторами для блокирования атак путем изменения ACL или ограничения скорости передачи трафика (Rate Limiting)
- Возможность распределения нагрузки между несколькими сенсорами и обеспечение отказоустойчивости
- Выборочное блокирование (не всего IP-адреса, а только атакующего сервиса)
- Поддержка до 255 VLAN на один интерфейс сенсора
- Возможность эффективного предотвращения атак в коммутируемых сетях
- Импорт данных от сканеров безопасности
- Механизм OS Fingerprint для определения релевантности атаки
- Оценка эффективности реагирования на атаку
- Удаленный контроль состояния сенсора
- Специальный универсальный модуль для обнаружения и блокирования атак в любых протоколах на базе TCP
- Модуль обнаружения и блокирования атак в P2P-приложениях и унифицированных коммуникациях

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

МНОГООБРАЗИЕ МОДЕЛЕЙ CISCO IPS

	IPS 4240	IPS 4255	IPS 4260	IPS 4270
Производительность, Мбит/сек	250	500	1000	4 Гбит/сек 2 Гбит/сек
Интерфейс для мониторинга	Четыре 10/100/1000 BASE-TX	Четыре 10/100/1000 BASE-TX	10/100/1000 BASE-TX	4 x 10/100/1000BASE-TX или 4 x 1000BASE-SX
Опциональный интерфейс для мониторинга	Четыре 10/100/1000 BASE-TX (всего 8 интерфейсов) или четыре оптических 1000 BASE-SX	Четыре 10/100/1000 BASE-TX	Четыре 10/100/1000 BASE-TX (всего до 9 интерфейсов) или два 1000 BASE-SX (всего до 4 оптических интерфейсов)	4 x 10/100/1000BASE-TX или 2 x 1000BASE-SX (всего до 16 интерфейсов)
Размер шасси	1RU	1RU	1RU	4RU
Дополнительный блок питания	Нет	Нет	Опционально	Да
Мониторинг отказов				
• **линии связи**	Да	Да	Да	Да
• **соединения**	Да	Да	Да	Да
• **сервиса**	Да	Да	Да	Да
• **устройства**	Да	Да	Да	Да

CISCO IOS INTRUSION PREVENTION SYSTEM

Программное обеспечение Cisco IOS IPS – это первое в отрасли решение для предотвращения атак, интегрированное в операционную систему маршрутизаторов 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 себя программном коде системы Cisco IDS/IPS
- Обнаружение более 1400 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 режиме реального 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 Cisco Security Manager
- Высокая производительность (до 425 Мбит/сек на Cisco 3845)
- Технология Flexible Packet Matching
- МСЭ прикладного уровня для контроля интернет-пейджеров
- Поддержка технологии Distributed Threat Mitigation с помощью системы Cisco MARS
- Поддержка сигнатур того же формата, что и в Cisco IPSv6
- Поддержка технологии Risk Rating
- Поддержка VRF для реализации механизма виртуальных сенсоров

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

CISCO INTRUSION DETECTION SERVICES MODULE

Компания Cisco Systems – один из немногих производителей в мире, выпускающих 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. Основное предназначение этого модуля – защита центров обработки данных, операторов связи и штаб-квартир крупных компаний.

Основные возможности

- Базируется на зарекомендовавшем себя 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

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

CISCO IPS AIM MODULE

Cisco IPS AIM Module – аппаратный модуль для обнаружения атак, предназначенный для интеграции в маршрутизаторы Cisco 1841, 2800 и 3800. Он предназначен для идентификации и блокирования вредоносной активности в трафике, проходящем через периметр удаленного филиала или небольшого офиса.

Cisco IPS AIM Module построен на базе того же ПО, что и обычные сенсоры Cisco IPS 4200 Series и обладает всей их функциональностью, отличаясь только пропускной способностью – до 45 Мбит/сек.

Основные возможности

- Мониторинг различных интерфейсов – T1, T3, DSL, ATM, Fast Ethernet и Gigabit Ethernet
- Собственный процессор для разгрузки маршрутизатора
- Интеграция со всеми защитными функциями операционной системы IOS маршрутизатора
- Различные варианты блокирования атак, в т. ч. путем реконфигурации ACL маршрутизатора
- Автоматизированное обновление сигнатур
- Мониторинг отказов соединения, сервиса и устройства
- Единое управление с сенсорами Cisco IDS/IPS, межсетевыми экранами и средствами построения VPN
- Управление с помощью IDS Device Manager, IPS Manager Express и Cisco Security Manager
- Защищенное обновление сигнатур атак
- Возможность работы в двух режимах – обнаружения и предотвращения атак
- Поддержка VLAM 802.1q

Дополнительная информация: http://www.cisco.com/en/US/products/ps8395/index.html

CISCO IPS 4200, IDSM, IPS-AIM, 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 IPS-AIM

- Консолидированные решения 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), идентифицированные специализированными средствами обнаружения вторжений, в качестве которых могут выступать Cisco Anomaly Traffic Detector, Cisco IDS/IPS 42xx или Arbor Peakflow. Блокирование основано на технологии многоступенчатой проверки, которая позволяет блокировать вредоносные информационные потоки и пропускать те, которые содержат легитимные транзакции, несущие полезные данные.

Основные возможности

- Уникальная архитектура Multiverification Process (MVP)
- Отсутствие снижения производительности защищаемой сети
- Скорость обработки трафика – 3 Гбит/сек (возможность масштабирования до 30 Гбит/сек путем использования кластера из 10 Cisco Guard)
- Число параллельно обрабатываемых соединений – 4,5 млн
- 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 м/сек
- Централизованное управление
- Соблюдение необходимого уровня SLA
- Обеспечение услуг аутсорсинга
- Защита от DoS-атак на IP-телефонию (SIP)
- Технология обнаружения подозрительного трафика путем профилирования нормального поведения в режиме самообучения и обнаружения аномалий
- Поддержка до 500 зон безопасности с различными политиками безопасности (одновременно защищаются до 50 зон)

Дополнительная информация: http://www.cisco.com/en/US/products/ps6235/index.html и http://www.cisco.com/en/US/products/ps6236/index.html

CISCO RUSSIA VPN MODULE

Cisco Russia VPN Module – первое решение компании Cisco, разработанное совместно с российской компанией «С-Терра СиЭсПи» и предназначенное для организации виртуальных частных сетей (VPN) на базе отечественных алгоритмов шифрования. Модуль интегрируется в маршрутизаторы Cisco ISR 2811, 2821, 2851, 3825 и 3845 и использует сертифицированное ФСБ ядро (по классам КС1 и КС2). Программное обеспечение модуля также сертифицировано по ГОСТу Р ИСО 15408 и РД МСЭ.

На базе данного модуля совместно с компаниями Инфотекс и С-Терра было создано решение Russia VPN VipNet Module, которое базируется на программном обеспечении для организации виртуальных частных сетей компании Инфотекс.

Основные возможности

- Поддержка любого IOS Feature Set, начиная с IP Base
- Поддержка IOS 12.4(11)T
- Поддержка IPSec ESP и AH при использовании ГОСТ 28147-89
- Полная совместимость с IKE и IPSec-решениями (RFC 2401-2412)
- Поддержка NAT Transparent IPSec
- Совместимость с разными системами PKI (Microsoft с CryptoPro, Notary-Pro, Валидата, RSA Keon)
- Поддержка сертификатов – LDAPv3, x509v3, PKCS#7, #10 и #12, CRL
- Поддержка IKE при использовании ГОСТ Р 34.10-94, ГОСТ Р 31.10-2001
- Поддержка QoS
- Приоритезация мультимедийного трафика
- Отсутствие обмена данными между модулем и маршрутизатором (для критичных приложений)
- Ограничение предельного уровня нагрузки на CPU для задач шифрования
- Отказоустойчивость за счет автоматического переключения на резервный шлюз
- Перенос IP-адресов отказавшего модуля на резервное устройство (опционально)
- Поддержка протокола DPD (Dead Peer Detection)
- Поддержка резервирования (между модулями в одном маршрутизаторе и между маршрутизаторами)
- Интеграция с другими защитными функциями Cisco ISR – МСЭ, IPS и т. д.

Дополнительная информация: http://www.cisco.com/global/RU/products/hw/vpndevc/rvpn/index.shtml

CISCO IPSEC VPN SERVICES MODULE

Cisco IPSec VPN Service Module (VPNSM) – специальный модуль, интегрируемый в коммутатор Cisco Catalyst 6500 или маршрутизатор 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 сети Catalyst 6500 или Cisco 7600

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

CISCO IOS IPSEC/SSL 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 мультимедийного трафика и т. п., реализованными в одном устройстве.

Основные возможности

- Эффективная обработка мультимедийного 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)
- VRF-Aware IPSec MIB
- IPv6 Site-to-Site IPSec VPN
- Поддержка QoS для DMPVN
- Certificate Authority Key Rollover
- Возможность настройки местоположения хранилища сертификатов
- VRF-mode IPSec Stateful High Availability
- Поддержка EasyVPN для Dynamic VTI
- Шифрование multicast-трафика поверх GRE
- Организация SSL VPN (WebVPN) – позволяет обеспечить работу по SSL таких решений, как Clientless Citrix, Microsoft OWA 2003 (2000), CIFS, VoIP

Дополнительная информация: http://www.cisco.com/en/US/products/ps6635/products_ios_protocol_group_home.html

CISCO ASA VPN

Многофункциональные защитные устройства Cisco ASA 5500, помимо предоставления функций межсетевого экрана, предотвращения атак, антивирусной зашиты и др., также обладают всесторонним набором функций организации IPSec и SSL VPN на одной платформе. Объединяя в себе высокую доступность, производительность, масштабируемость и поддержку современных алгоритмов аутентификации и шифрования, Cisco ASA позволяет существенно снизить затраты компании на удаленный доступ к своим ресурсам.

Функциональность WebVPN позволяет установить безопасное VPN-соединение с помощью разных web-браузеров (Internet Explorer, Firefox, Opera и Safari), поддерживающих протокол SSL. При этом не требуется установки 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

- Автоматически загружаемый SSL VPN-клиент при удаленном доступе
- Автоматический контроль и актуализация версии SSL VPN-клиента
- Поддержка Citrix без дополнительно устанавливаемого ПО
- Установка Cisco Secure Desktop при SSL-доступе
- Поддержка QoS для эффективной обработки мультимедийного трафика
- Поддержка динамической маршрутизации OSPF
- Балансировка нагрузки VPN-соединений
- Обеспечение отказоустойчивости, включая Stateful failover
- Поддержка технологии контроля доступа Network Admission Control
- Поддержка от 25 до 5000 одновременных SSL или IPSec-сессий (зависит от модели)
- Поддержка Pocket PC, включая Windows Mobile 5
- Поддержка LDAP и Active Directory
- Централизованное управление для SSL и VPN-функций с единой консоли
- Интеграция с другими защитными функциями Cisco ASA
- Клиент нового поколения Cisco AnyConnect VPN с широкой поддержкой операционных систем (Microsoft Windows Vista, MAC OS X, Linux)
- Создание "умных туннелей" (smart tunnels), предоставляющих приложениям беспрепятственный доступ без дополнительной проверки прав
- Средства оценки состояния защищенности (posture-assessment extensions) удаленного клиента
- Поддержка балансировки нагрузки для WebVPN

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

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

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 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

Причины выбора Cisco IPSec VPN SPA

Защита центров обработки данных

- Единая организационная структура управления сетью и безопасностью

Причины выбора Cisco RVPN

- Требуется поддержка отечественных алгоритмов шифрования
- Требуется наличие сертификата на криптографическую подсистему

CISCO SECURITY AGENT

Cisco Security Agent (CSA) объединяет в одном решении различные защитные механизмы и функции – предотвращение атак, персональный межсетевой экран, защиту от вредоносного кода, контроль целостности, блокирование утечки информации через USB-порты и другие внешние устройства (PCMCIA, CD, Floppy, Zip и т. д.), 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. Это, в свою очередь, обеспечивает защиту компьютера от неизвестных атак, сигнатуры для которых пока не определены 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 – локальная и централизованная (от нескольких агентов)
- 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) и Cisco Security Monitoring, Analysis, and Response System (Cisco MARS)
- Делегирование отдельных функций управления агентом пользователю
- Механизм маркирования трафика приложений (Trusted QoS)
- Функционирование на платформах Windows (серверы; рабочие станции, включая Tablet PC), Linux, Solaris, VMWare
- Возможность контроля утечек информации через различные каналы, включая принтер или буфер обмена
- Контроль загрузки с несанкционированных носителей (CD, дискета, сеть и т. д.) за счет интеграции с технологией Intel AMT
- Интеграция с Cisco IPS 6.0
- Контроль беспроводных интерфейсов
- Возможность реализации мандатного разграничения доступа
- Встроенный сигнатурный антивирус ClamAV
- Автоматическая классификация данных на ПК
- Автоматическое создание и распределение сигнатур для некоторых типов атак
- Интерфейс пользователя на русском языке

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

ТЕХНОЛОГИЯ NETWORK ADMISSION CONTROL

Не требующая лицензирования технология Network Admission Control (NAC) позволяет предотвратить доступ к корпоративным ресурсам или сети оператора связи устройств, не соответствующих 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 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, Cisco ASA 5500, коммутаторе Catalyst или точке беспроводного доступа, в которые встроена поддержка NAC, не требующая дополнительного лицензирования.

NAC Framework рекомендуется к внедрению при условии ее интеграции с технологией Microsoft NAP (Network Access Protection) и использовании в качестве клиентской ОС – MS Windows Vista, а в качестве серверной ОС – MS Windows Server 2008 (Longhorn).

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 и EAP over 802.1x
- Прозрачность для пользователя
- Поддержка ОС Windows, Linux и Solaris
- Помещение несоответствующего узла в карантин путем применения списков контроля доступа ACL или URL Redirection, а также VLAN и PACL
- Решение парадокса «пользователь имеет право доступа в сеть, а его компьютер – нет»
- Мультивендерное решение: интеграция с Altiris, BigFix, IBM, McAfee, Qualys, Symantec, Trend Micro (всего более 70 компаний)
- Поддержка широкого спектра оборудования: маршрутизаторы, коммутаторы, VPN-концентраторы, точки беспроводного доступа
- Интеграция с системами Cisco MARS
- Полная совместимость с системой Microsoft NAP (Network Access Protection)

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

CISCO NAC APPLIANCE и NAC NETWORK MODULE

Cisco NAC Appliance (бывший Cisco Clean Access) – это решение, предназначенное для автоматического обнаружения, изолирования и лечения инфицированных, уязвимых или не соответствующих политике безопасности узлов, осуществляющих проводной или беспроводной доступ к корпоративным ресурсам.

Будучи одним из компонентов технологии Network Admission Control, Clean Access выполнен либо в виде сетевого модуля для маршрутизаторов Cisco ISR (для сетей с количеством контролируемых устройств менее 100), либо в виде отдельного устройства (для сетей от 100 устройств), которые могут быть установлены в одном из двух режимов:

- 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.

Преимуществом Cisco NAC Appliance и NAC Network Module является возможность его использования в локальных сетях, построенных на сетевом оборудовании различных производителей (не только Cisco).

Основные возможности

- Независимость от производителя сетевого оборудования (в режиме in-band)
- Интеграция с Kerberos, LDAP, RADIUS, Active Directory, S/Ident и другими методами аутентификации
- Поддержка ОС Windows (включая Vista), MacOS, Linux, Xbox, PlayStation 2, КПК, принтеров, IP-телефонов и т. д.
- Поддержка антивирусов CA, F-Secure, Eset, Лаборатории Касперского, McAfee, Panda, Drweb, Sophos, Symantec, TrendMicro и других средств защиты компьютера (всего 250 производителей)
- 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, новых версий средств защиты или актуализация устаревших антивирусных баз
- Централизованное web-управление
- Поддержка русского языка
- Проведение прозрачного аудита

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

NAC GUEST SERVER и NAC PROFILER

NAC Guest Server – решение, специально предназначенное для управления всем жизненным циклом гостевого доступа, начиная от создания временной учетной записи и настроек доступа и заканчивая автоматическим блокированием доступа при истечении заранее заданного времени. При этом все операции осуществляется не ИТ-персоналом, а любым сотрудником, вплоть до секретаря компании.

NAC Profiler – решение, предназначенное для поиска, инвентаризации, профилироваия, поддержки истории и мониторинга поведения IP-устройств, отличных от персональных компьютеров, лэптопов и серверов – принтеры, IP-телефоны, IP-видеокамеры, управляемые ИБП, POS-терминалы, системы контроля доступа, медицинские устройства и т. п.

Основные возможности NAC Guest Server

- Гостевой доступ с аутентификацией и без нее
- Интеграция с NAC Appliance и WLAN Controller
- Детали доступа могут быть распечатаны, отправлены по e-mail или через SMS
- Наличие портала управления жизненным циклом удаленного доступа
- Ограничение доступа по времени, полосе пропускания, IP–адресам, доменам и т. п.
- Наличие API для подключения внешних систем
- Интеграция с Active Directory

Основные возможности NAC Profiler

- Сбор информации об устройствах посредством SNMP, Netflow, DHCP
- Защита от атак MAC Spoofing, port swapping, аномалии аутентификации и т. п.
- Автоматическое включение неуправляемых IP-устройств в список исключений Cisco NAC Appliance Manager
- Снижение времени на инвентаризацию сети на несколько порядков
- Поддержка широкого спектра типов IP-устройств

Дополнительная информация: http://www.cisco.com/go/nacguestserver и http://www.cisco.com/go/nac

CISCO SECURE SERVICES CLIENT

Cisco Secure Services Client – программный клиент, обеспечивающий единую аутентификацию пользователей и устройств, подключающихся к различным узлам проводной и беспроводной сети. Cisco Secure Services Client (ранее называвшийся Meetinghouse AEGIS SecureConnect) обеспечивает простоту управления, надежную защиту и позволяет снизить совокупную стоимость владения беспроводной инфраструктурой.

Основные возможности

- Аутентификация на основе стандарта 802.1X (проводные и беспроводные сети)
- Поддержка Ethernet, 802.11a, 802.11b и 802.11g
- Поддержка аутентификации на основе протокола EAP (EAP-MD5, EAP-TLS, Cisco LEAP, EAP-FAST, PEAP)
- Поддержка EAP-TTLS (PAP, CHAP, MSCHAP, MSCHAPv2, EAP-MD5)
- Поддержка методов аутентификации EAP-PEAP (EAP-MSCHAPv2, EAP-GTC)
- Поддержка Wi-Fi-протоколов шифрования (WPA, WPA2, WPA-PSK, WPA2-PSK, WEP)
- Гибкий выбор пользовательских аутентификационных данных (пароли, одноразовые пароли, токены RSASecurID, сертификаты X.509)
- Поддержка работы со смарт-картами различных производителей (Axalto, Gemplus, SafeNet iKey, Aladdin)
- Возможность автоматического назначения пользователю необходимой VLAN
- Поддержка различных профилей выбираемых автоматически и вручную
- Поддержка технологии единого входа (single sign-on,SSO) для пользователей сетей Novell и Windows
- Интеграция с Cisco Network Admission Control (NAC)
- Совместимость с Cisco Secure ACS и Microsoft IAS
- Совместимость с сертифицированными Wi-Fi-альянсом устройствами
- Защита от изменения корпоративных настроек
- Автоматизация управления с помощью скриптов

Дополнительная информация: http://www.cisco.com/en/US/products/ps7034/index.html

CISCO SECURE DESKTOP

Программное обеспечение Cisco Secure Desktop, входящее в поставку Cisco ASA 5500, Cisco ISR 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 браузера (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 шифрования 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)
- Поддержка широкого спектра предустановленных приложений (Trend Micro, Microsoft, IBM, Symantec, Лаборатория Касперского, Dr.Web, Eset, Panda, McAfee и т. д.)
- Возможность создания собственных проверок

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 могут выступать Cisco Pix, Cisco VPN 3000 Concentrator, Cisco ASA 5500 и Cisco IOS.

Основные возможности

- Поддержка 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 ANYCONNECT CLIENT

Cisco AnyConnect Client – новое поколение VPN-клиента Cisco, который предназначен для защищенного подключения к корпоративным ресурсам по протоколу SSL. Отличительной особенностью Cisco AnyConnect Client является возможность его автоматической загрузки на компьютер, который до этого не имел VPN-клиента. Эта возможность позволяет открыть защищенный доступ к своим корпоративным ресурсам клиентам, партнерам и консультантам.

Основные возможности

- Поддержка TLS (HTTPS) и DTLS
- Полный доступ к сетевым ресурсам
- Поддержка чувствительных к задержкам приложений (например, голосовые) за счет протокола DTLS
- Поддержка Windows 2000 / XP (x86/x64) / Vista (x86/x64) / Mobile 5.0 Pocket PC Edition / Mac OS X 10 / Linux Intel
- Возможность удаленной загрузки и настройки для снижения нагрузки на пользователя
- Возможность запуска до процедуры входа в сеть (для Windows 2000 / XP)
- Поддержка Proxy Auto-Configuration
- В качестве VPN-концентратора удаленного доступа может выступать Cisco ASA или Cisco ISR
- Возможность инсталляции в виде стандартного приложения (standalone) или при удаленном доступе к защищаемым ресурсам
- Отсутствие перезагрузки после инсталляции
- Автоматическая загрузка в виде ActiveX или Java
- Доступ при удаленном подключении к порталу, персонализирующему язык, RSS-новости, закладки, приложения, внутренние каталоги
- Обеспечение доступа к Web-ориентированным и стандартным приложениям
- Поддержка SAML Single Sign-On
- Поддержка русского языка на портале

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

IRONPORT E-MAIL SECURITY APPLIANCE

IronPort E-mail Security Appliance (ESA) – программно-аппаратный комплекс, предназначенный для всестороннего контроля и защиты электронной почты. Построенный на базе масштабируемой и защищенной операционной системы AsyncOS, IronPort ESA позволяет не только защитить корпоративную почту от спама и вредоносного кода (вирусов, червей, фишинга и т. д.), но и обеспечить ее целостность, конфиденциальность, маркировку и защиту от подмены.

Основные возможности

- Обширная база знаний SenderBase, позволяющая отслеживать спам и вредоносный код по 150 различным параметрам
- Механизм Reputation Filters для эффективной фильтрации входящей почты
- Механизм контроля почты CASE (Context Adaptive Scanning Engine) позволяет проверять не только содержимое сообщения (включая Web-ссылки), но и его структуру и отправителя
- Механизм Outbreak Filters для обнаружения вредоносного кода, для которого еще отсутствуют сигнатуры в антивирусе
- Поддержка DKIM и DomainKeys
- Интегрированные антивирусные движки McAfee и Sophos
- Анализ текста в свыше 390 форматах файлов
- Анализ метаданных в файлах
- Обнаружение внедренных объектов в файлах MS Office
- Контроль соответствия требованиям различных стандартов
- Блокирование просмотра контролируемых сообщений администратором системы
- Различные варианты реагирования – блокирование, карантин, запрет вложений и т. д.
- Маркировка исходящей почты для ее однозначной идентификации
- Защита от подмены сообщений
- Кластеризация устройств IronPort ESA для масштабируемости
- Интеграция с LDAP и Active Directory
- Централизованное управление с помощью E-Mail Security Monitor
- Поддержка SNMP, syslog
- Проверка SPF и SIDF
- Шифрование e-mail с помощью IronPort PXE

Дополнительная информация: http://www.ironport.com/products

IRONPORT WEB SECURITY APPLIANCE

IronPort Web Security Appliance (WSA) –программно-аппаратный комплекс, предназначенный для всестороннего контроля и защиты Web-трафика. Построенный на базе масштабируемой и защищенной операционной системы AsyncOS, IronPort WSA позволяет не только защитить Web-трафика от вредоносного кода (вирусов, червей и т. д.), но и предотвратить посещение сотрудниками сайтов, не нужных для выполнения служебных обязанностей.

Основные возможности

- Обширная база знаний SenderBase, позволяющая отслеживать вредоносный код и нарушающие политику безопасности сайты по 150 различным параметрам
- Механизм Web Reputation Filters для эффективной фильтрации Web-трафика
- Одновременный контроль до 100 000 TCP-соединений, 10M HTTP транзакций в час, 1 Гбит/сек
- Большая база URL, используемая для фильтрации – 52 категории, 21 миллион сайтов, 3,5 миллиарда Web- траниц
- Автоматическое обновление базы URL
- Создание политик контроля по пользователям или группам
- Интеграция с LDAP и Active Directory
- Поддержка механизма исключений
- Встроенная система обнаружения вредоносного кода и рекламного ПО
- Механизм контроля Dynamic Vectoring & Streaming (DVS) позволяет параллельно сканировать поток разными «движками» с целью ответа на вопросы относительно анализируемого Web-трафика «Кто?», «Откуда?», «Что?» и «Как?»
- Обнаружение HTTP-трафика, передаваемого в обход 80 порта
- Возможность функционирования в режиме «только мониторинг» или «мониторинг и блокирование»
- Централизованное управление с помощью Web Security Monitor
- Расширенная система генерации отчетов
- Экспорт отчетов в различные форматы
- Поддержка SNMP, syslog
- Внедрение в виде прокси, «прозрачного» коммутатора или путем интеграции по протоколу WCCP

Дополнительная информация: http://www.ironport.com/products

CONTENT SECURITY AND CONTROL SECURITY SERVICES MODULE

Content Security and Control Security Services Module (CSC-SSM) – модуль расширения для Cisco ASA 5500, обеспечивающий защиту от вредоносных программ и контроль содержимого. Модуль CSC-SSM (Anti-X) включает в себя такие функции, как антивирус, антиспам, механизм защиты от программ-шпионов, блокирование подозрительных файлов, фильтрация и блокирование URL и др. В модуле CSC-SSM для защиты от вредоносного кода используются технологии Trend Micro – одного из лидеров рынка защиты от вредоносного ПО. Реализованный в модуле CSC-SSM механизм глубокой фильтрации упрощает задачу, стоящую перед компаниями по обеспечению защиты конфиденциальной информации, и помогает им соответствовать различным нормативным требованиям (HIPAA, SOX, Data Protection Act и др.).

Основные возможности

- Антивирусная защита в трафике HTTP, FTP, SMTP, POP3
- Защита от программ-шпионов
- Обнаружение и блокирование спама
- Антифишинг, защита от перехвата и подмены идентификационной информации
- Полная URL-фильтрация с использованием категорий и контролем доступа по времени
- Защита в режиме реального времени web-доступа, web-почты и передачи файлов через Web
- Интеграция с Damage Cleanup Server (DCS)
- Контентная фильтрация почтовых сообщений, позволяющая избежать несанкционированной отправки конфиденциальной информации
- Гибкие настройки фильтрации для реализации корпоративных политик безопасности
- Централизованное управление через web-консоль
- Автоматическое обновление в режиме 24 x 7
- Поддержка списков исключений URL
- Новая подсистема IntelliTap для эвристического анализа заархивированных или запакованных файлов с целью обнаружения в них вирусов
- Доступ к E-mail Reputation Services Portal

Дополнительная информация: http://www.cisco.com/en/US/products/ps6823/index.html

CISCO APPLICATION-ORIENTED NETWORKING

Cisco Application-Oriented Networking – новая концепция, обеспечивающая целостный набор интеллектуальных сетевых возможностей для эффективного и защищенного взаимодействия между приложениями, такими, как, например, SAP R/3, IBM WebSphere, Siebel, PeopleSoft, а также СУБД Sybase, Oracle и др., с помощью протоколов HTTP(S), SOAP, JMS/MQ, JMS/EMS, JDBC и т. д. AON позволяет управлять сообщениями приложений, повышать производительность сетевых приложений и помогает решить вопросы централизованного управления и назначения политик безопасности. Cisco AON доступен в виде модулей для Catalyst 6500 и Cisco 2600, 2800, 3700, 3800, а также в виде отдельного устройства Cisco 8340.

Основные возможности

- Всесторонняя проверка сообщений
- Ролевое управление (RBAC)
- Аутентификация сообщений на основе имени пользователя и пароля, цифрового сертификата и пр.
- Поддержка протоколов Kerberos и LDAP и интеграция с Microsoft AD, OpenLDAP, SunONE, Netegrity SiteMinder
- Поддержка механизмов авторизации SAML Authorization Assertion, WSS, группы в LDAP и т. д.
- Интеграция в инфраструктуру PKI
- Контроль XML/web-сервисов (XML Gateway, WS-Security, WSDL-Policy)
- Поддержка форматов XML и MIME
- Поддержка стандартов безопасности SAML, WS-Security, WS-I, W3C XML Encryption, XML Signatures, XKMS, WSDL и т. д.
- Централизованное управление ключами (поддержка Verisign Class 3 Certificate Service, PKCS#12, Java keystores)
- Обеспечение целостности и конфиденциальности сообщений
- Защита транспортного уровня на основе механизмов SSL v3 и TLS v1
- Отражение атак на уровне приложений (X-DoS, SQL Injection, XML Schema Poisoning, Coercive Parsing и т. д.)
- Аудит и анализ критичных событий с возможностью генерации отчетов
- Описание бизнес-логики с помошью AON Development Studio
- Создание своих обработчиков сообщений и поддержка других протоколов взаимодействия приложений

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

CISCO APPLICATION CONTROL ENGINE

Cisco Application Control Engine (ACE) – многофункциональный модуль для коммутаторов Cisco Catalyst 6500, консолидирующий в себе такие функции, как балансировка нагрузки, аппаратное ускорение SSL, оптимизация приложений и безопасность. Данный модуль позволяет эффективно защищать web-серверы и web-приложения, размещенные в центрах обработки данных.

Основные возможности

- Обеспечение высокой производительности и масштабируемости – 4, 8 и 16 Гбит/сек, 6,5 млн пакетов в секунду, до 4000 VLAN, до 4 млн одновременных соединений
- Поддержка до 4096 виртуальных и 16 000 реальных серверов
- Поддержка до 250 виртуальных контекстов с собственными настройками
- Инспекция пакетов HTTP (заголовки, URL, содержание пакетов и т. п.) с помощью технологии Deep Packet Inspection
- Аппаратная поддержка проверки таких протоколов, как HTTP, RTSP, DNS, FTP и ICMP
- Работа с ACL (до 256 000 записей)
- Поддержка статической и динамической NAT (до 1 000 000 соединений) и PAT
- Ролевое управление с помощью RBAC
- Аппаратное ускорение при работе с SSL
- Централизованное управление цифровыми сертификатами
- Поддержка SSL v2 и v3, TLS v1.0
- Проверка протокола TCP (состояние, заголовок, размер окна)
- Проверка протоколов UDP, DNS, POP, IMAP, Telnet, ICMP, TCP, Echo, SMTP, RADIUS, LDAP и др. на соответствие RFC
- Обеспечение высокой доступности и отказоустойчивости (между модулями в одном или нескольких коммутаторах, а также между виртуальными контекстами)

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

CISCO WEB APPLICATION FIREWALL

Cisco Web Application Firewall – это межсетевой экран прикладного уровня, ориентированный на защиту Web-сервисов, использующих в своей работе протоколы XML и SOAP. Помимо защитных функций, Web Application Firewall предоставляет и большое количество механизмов оптимизации и ускорения обработки XML и SOAP-трафика.

Данное решение будет незаменимым при обеспечении защиты Web-сервисов как при внедрении стратегии Web 2.0, так и для защищенного взаимодействия с бизнес-приложениями таких производителей, как Oracle, SAP, IBM, Siebel, Microsoft и т. д.

Основные возможности

- Отражение XML-атак, включая X-DoS, XML Schema Attack, XML-черви и т. п.
- Разграничение доступа к Web-сервисам
- Обеспечение целостности и конфиденциальности XML-сообщений
- Фильтрация XML-сообщений
- Поддержка WS-Security 1.0/1.1, SAML 1.0/2.0, XML Encryption, XML Digital Signature, XML Schema, XML DTD, SSL 2.x/3.0/TLS
- Поддержка криптографических алгоритмов AES, DES, 3DES, Blowfish, RSA, Диффи-Хелман, DSA, SHA-1, MD5, AS2 (RFC 3335)
- Поддержка форматов XML, SOAP 1.1+SWA, SOAP 1.2. MTOM, Flat-file
- Защита от перехвата ключей SSL (SSL key hijacking)
- Централизованное ролевое управление
- Производительность – 30000 XML-транзакций в секунду (в т. ч. – до 14000 SSL-транзакций в секунду)
- Поддержка до 40000 одновременных соединений
- Полное соответствие требованиям FIPS
- Интеграция с LDAP, Kerberos / Active Directory, CA / Netegrity, IBM Tivoli Access Manager, RSA SecurID
- SDK для подключения собственных механизмов аутентификации
- Экспорт журналов регистрации

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

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 сообщений размером 1 Кб.

Основные возможности

- Пропускная способность – до 4 Гбит/сек
- Число одновременно контролируемых абонентов – до 100 000
- Число одновременно обрабатываемых потоков – до 2 млн
- Поддержка свыше 600 протоколов, включая P2P (KaZaA, Gnutella, eDonkey и др.), почтовые (SMTP, POP3, IMAP4), мультимедийные (RTSP, SIP, Skype, H323, MGCP)
- Обеспечение высокой отказоустойчивости
- Поддержка MPLS, VLAN, 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
- Возможность задания сигнатур, включая многопакетные и двунаправленные, на основе простого графического интерфейса
- Идентификация и подавление зомби-атак
- Возможность сохранения собранных данных в любой SQL-совместимой БД

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

CISCO SUPERVISOR ENGINE 32 PISA

Supervisor Engine 32 Programmable Intelligent Services Accelerator (PISA) – это модуль для коммутаторов Catalyst 6500, основная задача которого – обеспечение всесторонней инспекции (deep packet inspection), понимания, безопасности и доступности корпоративных приложений. За счет аппаратного ускорения таких функций, как Network-based application recognition (NBAR) и Flexible Packet Matching (FPM), новое решение позволяет анализировать трафик на мультигигабитных скоростях и обеспечить при этом обнаружение в нем различных нарушений политики безопасности.

Данное решение позволяет эффективно решить проблемы контроля трафика в новом подходе, который подразумевает постепенный отход от «клиент-серверной» модели в сторону активного использования P2P-приложений, унифицированных коммуникаций, беспроводных соединений и т. д.

Основные возможности

- Идентификация и контроль свыше 90 протоколов и приложений (P2P, мультимедиа, почтовые и Интернет-протоколы и т. д.)
- Анализ утилизации канала связи в реальном времени (по интерфейсам, по протоколам) с подробной статистикой
- «Super ACL», обеспечивающие более тонкую и гибко настраиваемую фильтрацию
- Обнаружение атак «отказ в обслуживании», некорректно сформированных пакетов, вирусов и червей
- Инсталляция новых фильтров на коммутаторе без перезагрузки
- Различные варианты реагирования – блокирование, приоритезация, ограничение полосы пропускания и т. д.
- Производительность FPM/NBAR – свыше 2 Гбит/сек
- Совместимость с MRTG, Concord (CA), Micromuse (IBM), InfoVista
- Описание новых протоколов и приложений с помощью специального языка
- Управление и мониторинг с помощью Cisco Security Manager и Cisco MARS

Дополнительная информация: http://www.cisco.com/en/US/products/ps7209/index.html

CISCO SECURITY MANAGER

Cisco Security Manager (CSM) – система централизованного управления всеми средствами защиты компании Cisco, пришедшая на смену CiscoWorks VMS. Отличительными особенностями CSM являются поддержка большего числа и типов устройств защиты, различные формы представления информации, механизмы обнаружения несоответствий в политике безопасности, автоматизация рутинных задач и т. д.

Основные возможности

- Графический интерфейс управления
- Различные формы представления информации – в виде топологии сети, в виде географической карты, в виде таблицы правил
- Обнаружение конфликтов в правилах политики безопасности
- Обнаружение правил, не влияющих на защищенность сети
- Группирование объектов
- «Клонирование» настроек для ускорения внедрения средств защиты
- Поддержка иерархии и наследования политик безопасности
- Откат к предыдущей конфигурации
- Импорт настроек из различных источников
- Инвентаризация политик для уже внедренных средств защиты
- Автоматическая настройка VPN-туннелей для различных топологий (Site-to-Site, Hub & Spoke, Partial Mesh, Full Mesh и т. д.)
- Управление механизмами отказоустойчивости, балансировки нагрузки и контроля качества обслуживания для управляемых средств защиты
- Ролевое управление административным доступом с помощью Cisco Secure ACS
- Автоматическое обновление средств защиты
- Управление ACL и VLAN на Catalyst 6500 и Cisco 7600
- Интеграция с Cisco MARS для корреляции сетевых событий и заданных правил на МСЭ, что помогает более быстро принимать решения и повышает работоспособность сети
- Управление и конфигурирование политик безопасности на МСЭ Cisco, включая устройства Cisco ASA 5500, Cisco PIX, модули на Cisco Catalyst 6500
- Обеспечение высокой доступности
- Контроль административных действий на защитных устройствах
- Управление SSL VPN
- Расширенная интеграция с Cisco MARS
- Уведомление об истекших правилах
- Поддержка расписания для внедрения систем защиты

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

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 режиме реального времени. Автоматическое блокирование обнаруженных атак достигается с помощью механизма AutoMitigate™, который позволяет реконфигурировать различные средства защиты и сетевое оборудование.

Основные возможности

- Обработка до 10 000 событий в секунду или свыше 300 000 событий Netflow в секунду
- Возможность создания собственных правил корреляции
- Уведомление об обнаруженных проблемах по e-mail, SNMP, через syslog и на пейджер
- 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
- Поддержка IOS 802.1x, NAC (фаза 2)
- Мониторинг механизмов защиты коммутаторов (Dynamic ARP Inspection, IP Source Guard и т. д.)
- Интеграция с Cisco Security Manager (CSM Policy Lookup)
- Интеграция с системами управления инцидентами с помощью XML Incident Notification
- Слежение за состоянием контролируемых устройств
- Аутентификация на RADIUS-сервере
- Мониторинг работоспособности компонентов Cisco MARS
- Syslog forwarding
- Динамическое распознавание новых сигнатур атак на Cisco IPS и загрузка их в Cisco MARS

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

CISCO IP SOLUTION CENTER

Cisco IP Solution Center (ISC) – платформа централизованного управления сетевой инфраструктурой крупных компаний и сервис-провайдеров. В том числе 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

CISCO DDOS MULTIDEVICE MANAGER

Cisco DDoS MultiDevice Manager – это бесплатное программное обеспечение, позволяющее обеспечить всесторонний и консолидированный взгляд на инфраструктуру отражения атак «отказ в обслуживании», состоящую из множества устройств или сервисных модулей Cisco Guard и Cisco Traffic Anomaly Detector.

Основные возможности

- Консолидированные отчеты как по зонам, так и по устройствам Cisco Guard и Cisco Traffic Anomaly Detector
- Анализ в режиме реального времени и анализ «постфактум» на основе собранной статистики
- Активация функций обнаружения аномалий, отражения атак и процесса обучения на одной или всех зонах
- Агрегирование всех фильтров в единый список
- Агрегирование всех событий со всех устройств в один журнал регистрации
- Распределение эталонной конфигурации и политик на все устройства отражения атак (синхронизация)
- Возможность синхронизации в ручном и автоматическом режиме
- Обнаружение конфликтов и несоответствий между эталонной и текущей конфигурациями
- Функционирование на RedHat Enterprise Linux
- Интуитивно понятный Web-интерфейс управления
- Защищенное управление по SSL
- Полная поддержка TACACS AAA
- Управление Customer Portal для ограничения доступа к тем или иным зонам и устройствам
- Возможность модификации конфигурации зоны в активном режиме работы
- Возможность удаления политик для зоны и списка удаленных сенсоров из процесса синхронизации
- Расширенные возможности управления пороговыми значениями

Дополнительная информация: http://www.cisco.com/en/US/products/ps7020/index.html

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 режиме реального времени статистики о событиях безопасности, сетевой активности и т. п.
- Защищенное управление с помощью SSL или SSH

Дополнительная информация:

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 ADAPTIVE SECURITY DEVICE MANAGER

Cisco Adaptive Security Device Manager (ASDM) предоставляет широко распространенные функции управления и мониторинга устройств Cisco через наглядный и простой в использовании web-интерфейс. В сочетании с устройствами Cisco ASA 5500 и Cisco PIX программное обеспечение Cisco ASDM позволяет ускорить процесс развертывания устройств защиты с помощью интеллектуальной подсистемы настройки оборудования. Cisco ASDM имеет эффективные инструментальные средства администрирования и гибкие функции мониторинга, которые дополняют интегрированные возможности самих устройств.

Основные возможности

- Визуальный мониторинг устройств в реальном масштабе времени
- Архитектура на базе web позволяет свободно сосуществовать с другими приложениями на основе браузера
- Полная поддержка возможностей программного обеспечения Cisco ASA и Cisco PIX, включая функции настройки и управления IPSec и SSL VPN, IPS (модуль AIP-SSM) и антивирусом (модуль Anti-X)
- Расширенные возможности конфигурирования сервисов проверки приложений и протоколов (HTTP, FTP, ESMTP, DNS, ICMP, SQL*Net, NFS и др.)
- Контроль PIM, OSPF, 802.1q и QoS
- Ролевое управление (16 уровней авторизации пользователей)
- Защищенное управление по SSL
- Возможность аутентификации на основе локальной базы данных или RADIUS/TACACS-сервера
- Поддержка в одном устройстве Cisco ASA 5500 или Cisco PIX множества виртуальных контекстов безопасности с собственными настройками
- Создание объектов защиты для их использования в различных политиках безопасности
- Фильтрация Syslog на основе множества критериев с подсветкой выбранных событий безопасности
- Запатентованная подсистема Packet Tracer для отслеживания проблем с устройством
- Корреляция правил МСЭ с событиями безопасности Syslog
- Мониторинг производительности

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

CISCOWORKS NETWORK COMPLIANCE MANAGER

CiscoWorks Network Compliance Manager (NCM) – web-приложение из семейства продуктов CiscoWorks, позволяющее отслеживать конфигурацию и изменения ПО в многовендорной сетевой инфраструктуре на соответствие требованиям различных государственных, международных и корпоративных стандартов не только в области безопасности, но и в области ИТ. Помимо проверки, NCM позволяет также сформулировать рекомендации по их корректировке. Внедрение NCM помогает идентифицировать изменения в настройке сетевого оборудования, лучше понимать тенденции в сетевой инфраструктуре, что позволяет оперативно устранять бреши в защите сети и повышает стабильность ее работы.

Основные возможности

- Автоматическое обнаружение сетевых устройств (auto-discovery)
- Построение карты сети для упрощения поиска и устранения неисправностей
- Импорт информации о сети из CiscoWorks DCR
- Простота в отслеживании изменений в конфигурации устройств
- Генерация различных отчетов, включая необходимые для проверки соответствия нормативным требованиям (SoX, VISA CISP/PCI, HIPAA, GLBA, FISMA, ITIL, CobiT, COSO и др.)
- Интеграция с приложениями CiscoWorks (CiscoWorks LMS, Device Center, CiscoView)
- Поддержка ролевого управления
- Централизованное управление ACL
- Высокая масштабируемость (контроль сетей из десятков тысяч узлов)
- Обеспечение отказоустойчивости
- Аудит различных типов оборудования – межсетевые экраны, маршрутизаторы, коммутаторы, VPN, точки беспроводного доступа и т. п.
- Анализ оборудования 35 различных производителей – Cisco, 3Com, Check Point, Crossbeam, Enterasys, Extreme, HP, Juniper, Nortel, ZyXEL и т. д.
- Идентификация критических рисков и возможных уязвимостей с последующей расстановкой приоритетов
- Интеграция с Remedy AR
- Обеспечение отказоустойчивости
- Инсталляция и проверка контрольных сумм на имиджах ОС на сетевых устройствах
- Расширение функциональности подсистемы управления политиками, которые не только позволяют облегчить управление политиками, но и позволяют к каждому правильно подключать скрипт (remediation script), срабатывающий при несоответствии данному правилу.

Дополнительная информация: http://www.cisco.com/en/US/products/ps6923/index.html

CISCO CONFIGURATION ASSURANCE SOLUTION

Cisco Configuration Assurance Solution (CAS) – программное средство, позволяющее повысить защищенность и работоспособность сети на основе проверки соответствия текущих настроек сетевого оборудования и требований существующих политик или международных стандартов безопасности. Cisco CAS диагностирует ошибки в настройке оборудования, неэффективности в работе, проблемные места в защите, помогая оценить защищенность сети на соответствие требованиям HIPAA, ISO 17799, ITIL/BS15000 и др.

Основные возможности

- Обнаружение ошибок в настройке сетевого оборудования и средств защиты
- Проверка корректности используемых сетевых политик безопасности (например, на Cisco Pix, Cisco ISR или Cisco Catalyst)
- Аудит решений третьих фирм (Check Point, Juniper, Nokia, Nortel и т. д.)
- Создание отчетов по соответствию нормативным документам, таким как Sarbanes-Oxley, HIPAA, FISMA и др.
- Поддержка более 400 правил для стандартных протоколов и технологий (IP, RIP, OSPF, IGRP, EIGRP, BGP, ACL, HSRP, SNMP, AAA, RADIUS, Kerberus, TACACS+, VLAN, VPN, QoS и др.)
- Доступ к сетевому оборудованию через SSH или SNMP
- Поддержка ключевых процессов архитектуры управления ИТ, включая ITIL/BS15000 и ISO 17799
- Импорт данных для последующего анализа и аудита от Cisco NetFlow FlowCollector, CiscoWorks RME, Campus Manager, Cisco Network Connectivity Center, Cisco Info Center
- Рассылка уведомлений в случае критических ошибок на e-mail или пейджер
- Возможность персонализированной настройки правил проверки, частоты и времени проведения аудита, создаваемых отчетов
- Создание собственных политик безопасности для последующих проверок

Дополнительная информация: http://www.cisco.com/en/US/products/ps6364/index.html

ENTERPRISE POLICY MANAGER

Enterprise Policy Manager (EPM) – программное решение, предназначенное для управления доступом пользователей к различным приложениям и другим элементам корпоративной ИТ-инфраструктуры. EPM состоит из трех основных компонентов:

– Cisco Policy Administration Point (PAP) – подсистема управления политиками безопасности,

– Cisco Policy Decision Point (PDP) – подсистема принятия решения о предоставлении доступа на основе принятых политик доступа

– Cisco Policy Enforcement Point (PEP) – подсистема реализации политик доступа, принятых PDP.

Основные возможности

- Всестороннее создание и управление политиками безопасности для каждого приложения
- Поддержка Microsoft SharePoint/.NET, IBM Lotus Domino/ WebSphere, Jabber XCP, Documentum, BEA WebLogic, JBoss, IBM Lotus Sametime, IBM DB2, MS SQL, Oracle и т. п.
- Иерархическое управление политиками на базе правил или ролей, включая наследование, делегирование и т. п.
- Интеграция с LDAP или Active Directory
- Различные варианты отображения «пользователь → группа», «пользователь → роль», «группа → роль»
- Расширенные механизмы поиска групп, ролей и пользователей
- Расширенная поддержка различных атрибутов пользователей, групп и ролей
- Подсистема моделирования «Что если»
- Тесная интеграция с существующей инфраструктурой идентификации и аутентификации
- Поддержка протоколов XACML, SAML и SOAP
- Расширенный аудит доступа
- Генерация отчетов
- Наличие SDK для интеграции с различными приложениями

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

CISCO SECURITY INTELLISHIELD ALERT MANAGER SERVICE

Cisco Security IntelliShield Alert Manager Service – web-сервис, позволяющий освободить технических специалистов от постоянного поиска и отслеживания уязвимостей в продуктах, используемых в корпоративной сети компании. Основное отличие Cisco Security IntelliShield Alert Manager Service от множества других сервисов – уведомление только о тех уязвимостях, которые присущи именно Вашему программному обеспечению.

IntelliShield Alert Manager состоит из 4-х компонентов – защищенного web-портала, скрытой от пользователя инфраструктуры сбора и анализа информации об угрозах, базы данных уязвимостей и системы документооборота, обеспечивающей отслеживание, связывание, уведомление об уязвимости и контроль методов устранения.

Основные возможности

- Постоянно пополняемая всесторонняя база данных уязвимостей – информация о 16 000 уязвимостей с мая 2000 г.
- Информация предоставляется по 18 500 версий 5500 продуктов 1700 известных разработчиков
- Совместимость с CVE
- Автоматическая генерация отчетов
- Включение в уведомления и отчеты ссылок на обновления
- Возможность интеграции уведомлений от IntelliShieldAlert Manager в собственные приложения при помощи XML
- Настраиваемые интеллектуальные фильтры (Smart Filters) – поиск и выборка по любым параметрам (производитель, продукт, версия, ключевые слова, критичность, дата и т. д.)
- Встроенная система ранжирования рисков
- Различные варианты рассылки уведомлений об уязвимостях (e-mail, пейджер, SMS)
- Различные пороговые значения для генерации уведомлений с целью минимизации получаемой информации
- Связь уязвимостей и угроз IntelliShield с сигнатурами Cisco IPS

Получить тестовый 6-месячный бесплатный доступ можно по адресу: http://www.cisco.com/go/intellishield/trial/

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

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 различными типами 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 различных производителей токенов, одноразовых паролей и смарт-карт
- Высокая масштабируемость (свыше 300 000 пользователей, десятки тысяч устройств)
- Возможность проверки дополнительных условий перед разрешением доступа в сеть
- Интеграция с Network Admission Control (NAC), включая фазу 2
- Интеграция с PKI и поддержка списка отозванных сертификатов (CRL)
- Регистрация всех попыток доступа пользователей, включая неуспешные
- Генерация отчетов
- Возможность поставки в виде специального устройства с защищенной ОС
- Классификация и управление запросами на доступ к ресурсам с помощью профилей сетевого доступа
- Расширенные функции управления паролями, учетными записями и генерацией отчетов для соответствия новым законодательным требованиям (например, SOX)
- Поддержка syslog
- Поддержка VMWare ESX Server 3 и Windows 2003 Server
- Возможность временного повышения администраторами привилегий отдельных пользователей

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, таких, как мобильный (например, CDMA2000 или GPRS), беспроводные корпоративные сети и публичные точки доступа (хотспоты), широкополосный или коммутируемый доступ, SSG, 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 к базе данных или биллинговой системе, а также накладывающих определенные ограничения, включая блокирование доступа и т. п.

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 сведений 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

CISCO MONITOR MANAGER И DIRECTOR

Cisco Monitor Manager и Monitor Director – это системы управления, которые дают возможность проактивно контролировать решения Cisco, установленные на удаленных площадках или в небольших компаниях, распознавать и прогнозировать различные нештатные ситуации, до того как они смогут произойти, и сигнализировать об этом ответственному персоналу. К таким нештатным ситуациям могут быть отнесены – повышенная утилизация процессора или оперативной памяти устройства, скорое завершение лицензии, EoS/EoL устройства, устаревшая версия операционной системы, выход устройства из строя, статус интерфейсов и т. д.

Cisco Monitor Manager отвечает за сбор информации с контролируемых устройств, а Cisco Monitor Director предназначен для централизованной обработки и хранения информации, полученной с множества Cisco Monitor Manager. Cisco Monitor Director может быть использован в качестве системы мониторинга и управления у провайдеров услуг безопасности (Managed Security Service Provider).

Основные возможности

- Инвентаризация сети и построение физической топологии
- Защищенный доступ к удаленным устройствам
- Мониторинг производительности
- Мониторинг интерфейсов
- Подсчет трафика
- Уведомления в реальном времени по e-mail или через пейджер с возможностью настройки адреса уведомления в зависимости от времени суток
- Система фильтрации уведомлений по различным критериям
- Генерация текстовых или графических отчетов
- Архив конфигураций
- Встроенные инструменты поиска неисправностей
- Интеграция с системой управления инцидентами
- Распределенная архитектура
- Центральный портал для доступа к информации о контролируемых устройствах
- Поддержка Cisco ISR, Cisco ASA 5505/5510, Cisco Pix 501, 506, 506E, 515 и 515E и т.д.

Дополнительная информация: http://www.cisco.com/en/US/products/ps7244/index.htmlи
http://www.cisco.com/en/US/products/ps7246/index.html

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

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

- **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.** Осуществляются подготовка и планирование действий на случай 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.** 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.** Разрабатывается 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 соответствии 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 (24 x 7) авторизованный доступ к сайту www.cisco.com.
- Постоянный (24 x 7) 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.
- Упреждающую замену запчастей. Возможны три варианта в зависимости от срочности:
  - ✓ SMARTnet 8 x 5 x NBD – гарантированная доставка запчастей на следующий рабочий день, если запрос делается до 15.00 по местному времени.
  - ✓ SMARTnet 8 x 5 x 4 – 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 24 x 7 x 4 – 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 третьей 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 второй или первой 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 поддержке – обслуживание 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. Данный 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

АВТОРИЗОВАННОЕ ОБУЧЕНИЕ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Компания Cisco Systems предлагает множество авторизованных программ обучения по информационной безопасности. В очной форме интенсивные курсы по безопасности проводятся на базе сертифицированных учебных центров. Для партнеров Cisco Systems открыт доступ к курсам в дистанционной форме на Partner E-Learning Connection (www.cisco.com/go/pec).

Авторизованное обучение проводят инструктора со статусом CCSI (Certified Cisco Systems Instructor), имеющие большой практический опыт разработки и обслуживания сетей в России и за рубежом. Каждый слушатель курсов получает соответствующий комплект учебных пособий и соответствующий международный сертификат Cisco Systems.

Курсы позволяют подготовиться к сдаче экзаменов на получение различных уровней сертификации по безопасности Cisco Specialist или Cisco Certified Security Professional (CCSP). Статус Cisco Specialist может быть получен по одному из следующих направлений:

- Cisco Advances Security Field Specialist;
- Cisco Firewall Specialist;
- Cisco IPS Specialist;
- Cisco Security Sales Specialist;
- Cisco Security Solutions and Design Specialist;
- Cisco VPN Specialist.

Существует также ряд дополнительных курсов, рекомендованных инженерам, готовящимся к сдаче экзамена на высший статус эксперта Cisco Certified Internetwork Expert (CCIE) Security.

Завершение обучения по программам CCNA и Cisco Specialist позволяет получить статус INFOSEC Professional (стандарт образования 4011), поддерживаемый Агентством национальной безопасности США (NSA) и Комитетом США по национальным системам безопасности (CNSS).

Полная информация о тренинге и сертификации по информационной безопасности Cisco Systems:

http://www.cisco.com/go/securitytraining

Информация об учебных партнерах на территории России и СНГ:

http://www.cisco.com/global/RU/training/training_contact.shtml

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ

Существует множество российских и международных стандартов и требований по информационной безопасности – PCI DSS, 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, требования по защите персональных данных, ключевых систем информационной инфраструктуры и др. 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 систему управления Cisco Security Manager на соответствие техническим условиям, руководящим документам и заданиям по безопасности.

Уникальным достижением компании Cisco в России послужило получение сертификата ФСТЭК на Cisco ASA 5500 на отсутствие недекларированных возможностей, а также сертификация производства более 20 наименований продуктов Cisco, включая маршрутизаторы, коммутаторы, многофункциональные средства защиты Cisco ASA 5500 и т.д.

Общее число выданных Федеральной службой по техническому и экспортному контролю (ФСТЭК) компании Cisco Systems сертификатов превысило 380, что существенно больше числа 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):

- Foundation Express (подраздел Security),
- Advanced Security,
- Master Security.

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

CISCO SYSTEMS CAPITAL®

Подразделение Cisco Systems – Cisco Capital – предлагает простые и гибкие схемы финансирования вопросов приобретения, аренды и лизинга устройств безопасности и сетевого оборудования Cisco для организаций любого размера и формы собственности. Благодаря этому предприятия могут реализовывать проекты, повышающие защищенность важнейших бизнес-приложений, даже в условиях нехватки финансовых ресурсов.

Предоставляемые преимущества

- *Возможность быстрого внедрения.* Минимальные начальные инвестиции и распределение платежей на период лизинга позволяют без существенных капитальных затрат приобрести технологию, необходимую уже сегодня.
- *Экономия капитала.* За счет распределения расходов на новые технологии по времени высвобождается ликвидный капитал для инвестиций в другие направления деятельности компании.
- *Максимум простоты и гибкости.* Cisco Capital предлагает широкий спектр условий и схем лизинга, включая отсрочку первоначального лизингового платежа сроком до шести месяцев, а также возможность модернизации решений по безопасности в течение всего срока лизинга.
- *Комплексная финансовая поддержка.* Обеспечивается финансирование как затрат на приобретение решений по безопасности, так и расходов на оплату сервисной поддержки, которые также включаются в лизинговые платежи.
- *Упрощение процессов бюджетирования.* Лизинг позволяет предприятиям использовать бюджеты текущих расходов для приобретения тех решений по безопасности, которые максимально соответствуют потребностям предприятия.
- *Налоговые преимущества.* Лизинговые платежи относятся на себестоимость, снижая налогооблагаемую базу на прибыль. Ускоренная амортизация при использовании лизинга существенно сокращает отчисления по налогу на имущество.

Для связи с Cisco Systems Capital: http://www.cisco.com/global/RU/contacts/feedback.shtml

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

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 к одному из наших партнеров с целью проведения аудита безопасности (дополнительную информацию об этом смотрите на стр. 72).

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 (495) 961-1410
  - ✓ В Санкт-Петербурге: +7 (812) 346-7733
  - ✓ В Алматы: +7 (3272) 58-4658
  - ✓ В Киеве: +7 (38044) 490-3600
  - ✓ В Баку: +7 (99450) 250-9994
  - ✓ В Ташкенте: +7 (99871) 140-4460
  - ✓ В Новосибирке: +7 (383) 230-2670

- По электронной почте: security-request@cisco.com (сообщения можно отсылать на русском языке)

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

Составитель: Алексей Лукацкий

Cisco
Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауерс»,
Космодамианская наб., 52, стр. 1, 4-й этаж.
Телефон: +7 (495) 961 1410
Факс: +7 (495) 961 1469
www.cisco.ru
www.cisco.com

Cisco
Россия, 191186, Санкт-Петербург,
бизнес-центр «Регус»,
Невский пр-т, 25, 2-й этаж, офисы 9, 30.
Телефон: +7 (812) 336 6531
Факс: +7 (812) 346 7800
www.cisco.ru
www.cisco.com

Cisco
Россия, 630099, Новосибирск,
бизнес-центр «Росевроплаза»,
Димитрова пр-т, 2, 5-й этаж.
Телефон: +7 (383) 230 2670
Факс: +7 (383) 230 1795
www.cisco.ru
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**