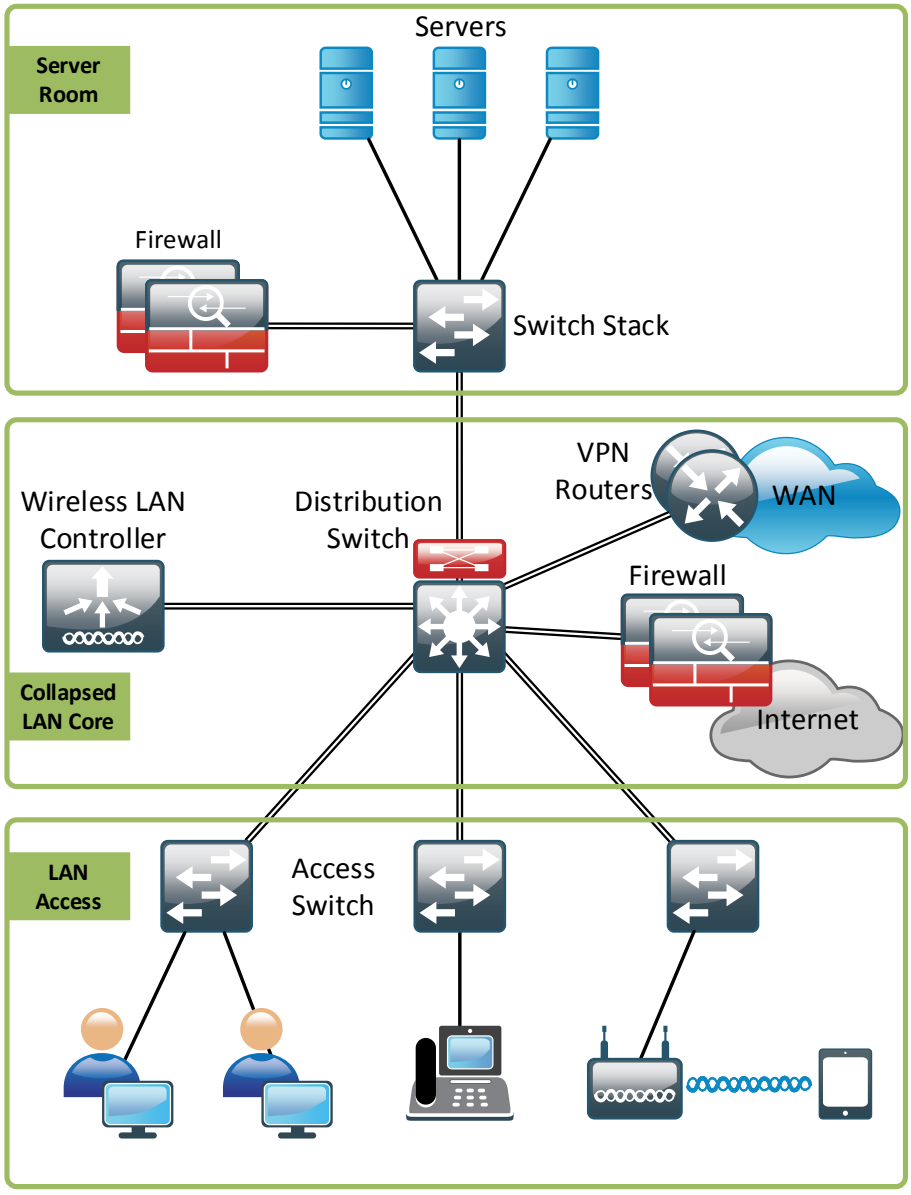
2014 Ver 1.0

John Cooper
NETSKILLS.RU
SKILL-ADMIN.BLOGSPOT.RU

Архитектура корпоративных сетей

Краткое руководство



NetSkills
online network school

ОГЛАВЛЕНИЕ

ЧИТАТЕЛЮ

Это небольшое руководство, которое каким-либо образом попало к вам в руки, создавалось долгие девять месяцев, длинными и дождливыми вечерами в попытке структурировать полученные знания и опыт. За это время книга дважды переписывалась и претерпела серьезные изменения в содержании для того, чтобы читатель получил максимум пользы от полученной информации. При этом автор старался сохранять доступный для понимания стиль изложения материала, рассчитанный на читателей разного уровня подготовки.

Единственная просьба к читателю это ценить труд и время автора - не нарушать авторское право и не публиковать данное руководство в открытый доступ в сети Интернет.

ВВЕДЕНИЕ

Данное руководство является результатом нескольких лет работы в области системной интеграции, а так же основано на анализе и переработке (с учетом российских реалий) архитектур Cisco SAFE и Cisco SBA Borderless Networks. Здесь будут рассмотрены Иерархическая модель и основные модули корпоративной сети, их расположение в сети, а так же основные методы защиты.

Будет описан процесс подключения удаленных филиалов к головному офису, подключение основных модулей корпоративной сети (серверный модуль, модуль Интернет (Internet Edge), модуль территориальных сетей WAN).

Рассмотрим возможные варианты оборудования для каждого из уровней иерархической модели и основных модулей. Определимся с методами реализации отказоустойчивости и повышения пропускной способности сети.

Руководство по дизайну корпоративных сетей предназначено для организаций с количеством пользователей до 10 000.

ДЛЯ КОГО ЭТО РУКОВОДСТВО

- Системные инженеры, которые нуждаются в стандартизации применяемых сетевых решений
- Преподаватели/тренера, которые ищут материалы для обучения сотрудников внутри организации

P.S. Документ в первую очередь предназначен для обучения сотрудников внутри организации и не является абсолютной истиной для всех.

ПРИМЕНЕНИЕ

Данный документ описывает основные аспекты проектирования крупных корпоративных сетей, однако может быть применен и для среднего и малого бизнеса. Естественно, что в рамках этого руководства невозможно рассмотреть все потребности всех организаций в части сетевой инфраструктуры. В настоящем документе представляется лишь некий “шаблон” которого стоит придерживаться при проектировании сетей, но он может быть изменен или модернизирован в соответствии с требованиями Заказчика.

Описанная ниже архитектура не гарантирует абсолютной безопасности вашей сети. Однако следуя этому руководству и используя рациональную политику безопасности, вы сможете существенно обезопасить сетевую инфраструктуру. Для построения более комплексной и надежной защиты необходимо разбираться в современных методах атак, вирусах и других вопросах безопасности, которые не будут рассматриваться в данном руководстве.

Все представленные решения основываются на оборудовании Cisco, однако я постараюсь описать некоторые альтернативы (дизайн для малого и среднего бизнеса) предназначенные для уменьшения стоимости сетевой архитектуры.

Так же предполагается, что читатель обладает необходимым уровнем знаний и способен отличить коммутатор от маршрутизатора.

1. ОСНОВЫ ДИЗАЙНА

Архитектура корпоративной сети включает в себя проводные и беспроводные соединения. В этом документе мы рассмотрим основные аспекты построения проводной сети.

Представленная архитектура не является каким-то открытием или новшеством в области сетевых технологий. Это просто комплекс, впитавший в себя все необходимое для обеспечения сетевой безопасности, а также устойчивости и масштабируемости.

Главные цели представленной архитектуры:

- Простота внедрения - развертывание решения в кратчайшие сроки.
- Гибкость и масштабируемость - модульная архитектура позволяет внедрять только те решения, которые необходимы в данный момент, с возможность последующего роста информационной инфраструктуры.
- Отказоустойчивость и безопасность - защита пользовательского трафика, отказоустойчивое исполнение гарантирующее стабильную работу сети даже во время атак.
- Простота управления - централизованное управление всей сетевой инфраструктурой.
- Готовность к новым технологиям - построенная архитектура позволяет легкое внедрение новых технологий и сервисов (например Cisco Collaboration).

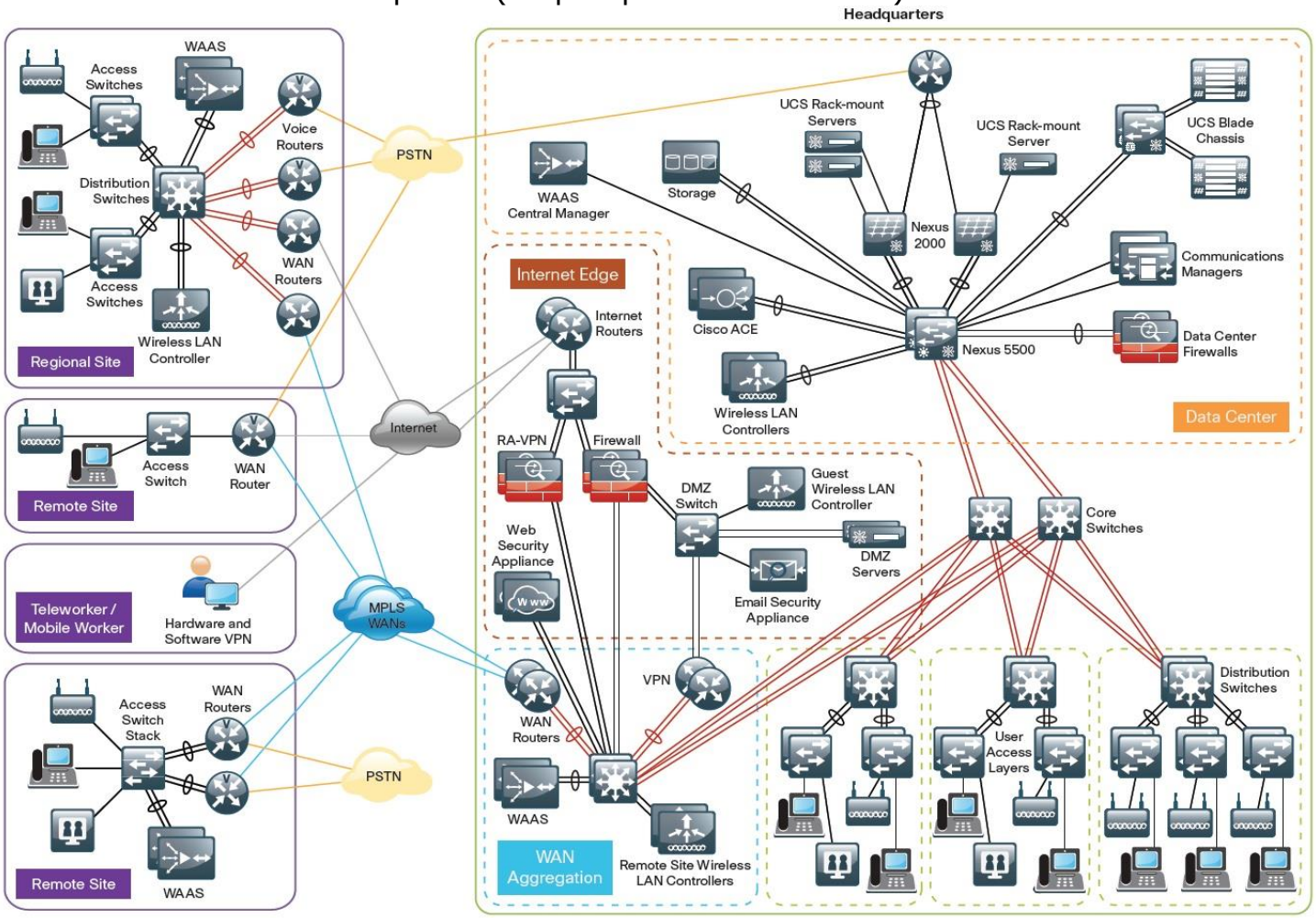


Рис.1.1. Архитектура корпоративной сети

1.1. ПРИНЦИП МОДУЛЬНОСТИ

Разбив архитектуру сети на модули можно сконцентрироваться на функционале каждого из них по отдельности, что существенно упрощает дизайн, внедрение и управление. Созданные модули, как детали конструктора из которых вы можете собрать сеть, соответствующую вашим требованиям. Эти же детали можно применять повторно (репликация), сильно сокращая время проектирования. Принцип репликации (повторения) элемента упрощает масштабируемость сети и ускоряет ее развертывание. На рис. 1.2 представлен процесс модернизации сети. Можно заметить, что масштабирование сводится к простому добавлению дополнительных модулей.

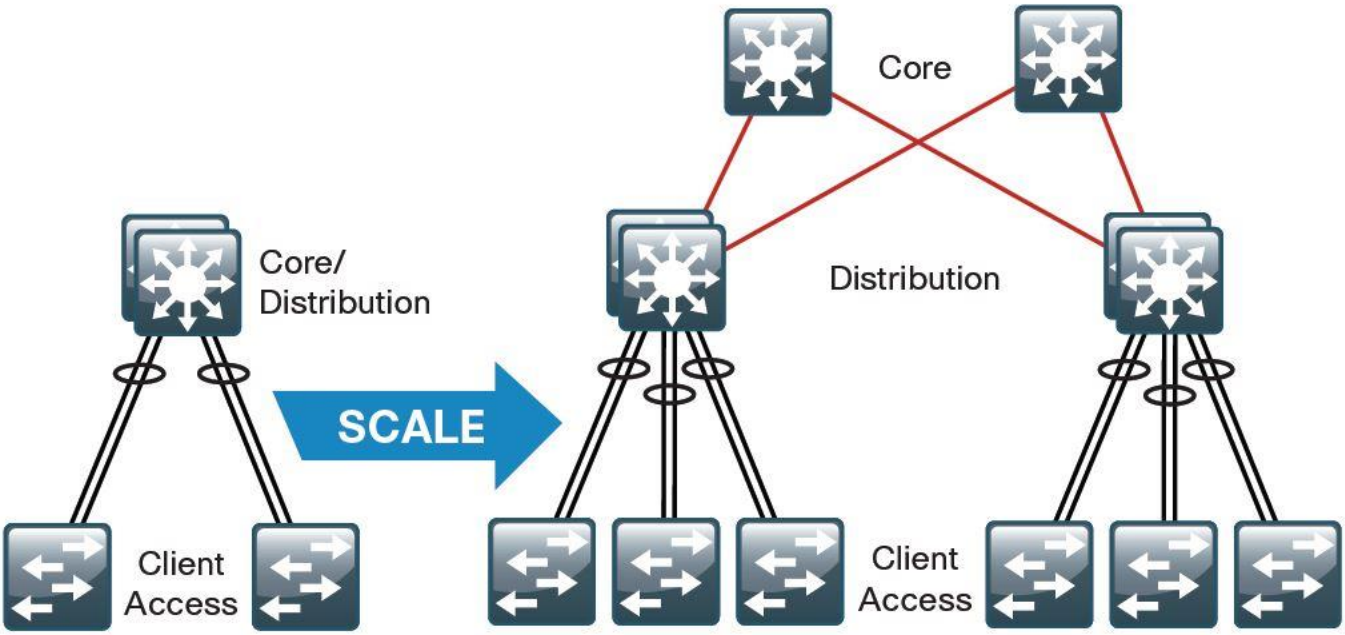


Рис. 1.2. Масштабируемость модульной сети

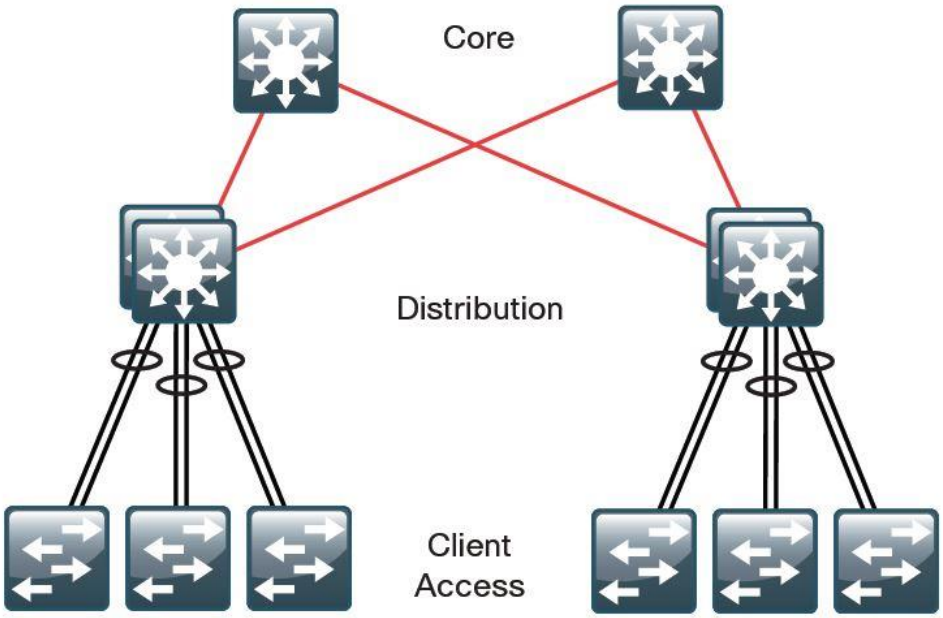


Рис. 1.3. Иерархическая модель сети

Разбиение большой сети на небольшие, простые для понимания, модули (уровни) способствует устойчивости сети за счет локализации возникающих проблем. Таким образом при возникновении какого-либо сбоя в сети необходимо определить на каком уровне возникла ошибка, затем приступать к ее решению, не затрагивая при этом другие модули сети.

2. ИЕРАРХИЧЕСКАЯ МОДЕЛЬ СЕТИ

Иерархическая модель представляет собой фундамент для сетевой инфраструктуры: подключение пользователей, принтеров, сканеров, WAN маршрутизаторов, устройств безопасности, серверов и т.д.

Иерархическая модель (Рис. 1.3) делит сеть на три основных уровня/модуля.

Уровни иерархической модели:

- Уровень доступа (Access Layer) - предоставляет пользователям или устройствам (принтер, сканер, ip-телефон) доступ к сети.
- Уровень распределения (Distribution Layer) - агрегирует/объединяет уровни доступа и предоставляет доступ к различным сервисам организации.
- Уровень ядра/базовый уровень (Core Layer) - агрегирует/объединяет уровни распределения в больших сетях.

Эти три уровня предоставляют различные функции и возможности. В зависимости от необходимости могут применяться один, два или все три уровня. Например для офиса с количеством пользователей менее 10 имеет смысл внедрять только уровень доступа. Для большой организации, занимающей несколько этажей или целое здание, будет разумным применение как уровня доступа, так и уровня распределения. Для огромных сетей, объединяющих несколько зданий необходимы все три уровня: уровень доступа, уровень распределения и уровень ядра.

2.1. УРОВЕНЬ ДОСТУПА (ACCESS LAYER)

Уровень доступа является точкой входа в сеть для пользователей и сетевых устройств (принтеры, сканеры, ip-телефоны и т.д.). Доступ как проводной, так и беспроводной. В более ранней литературе данный уровень называется “Модуль доступа”.

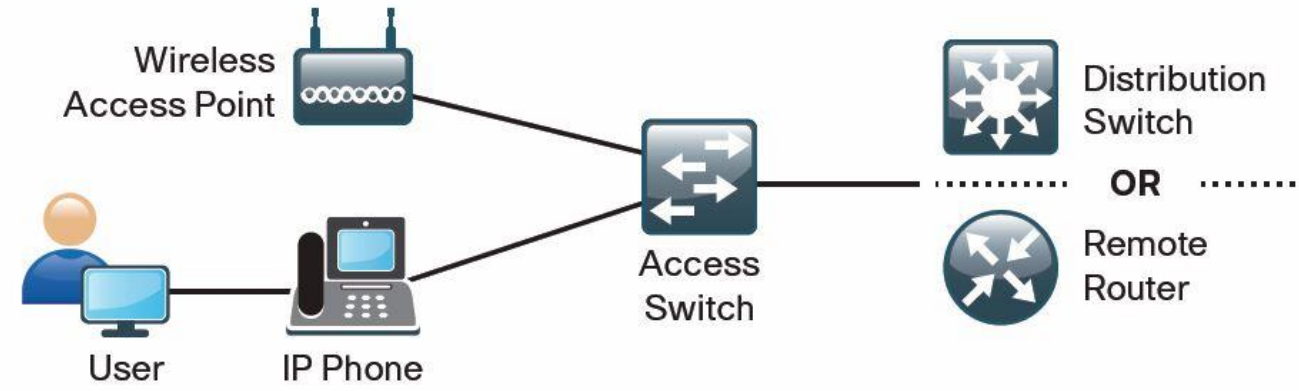


Рис. 2.1. Уровень доступа

2.1.1. УСТРОЙСТВА

Устройства уровня доступа это, как правило, коммутаторы второго уровня (L2) модели OSI, т.е. без функции маршрутизации. Коммутаторы осуществляют первичное сегментирование сети (технология VLAN). Однако в некоторых случаях могут применяться и устройства третьего

уровня (L3). Устройства уровня доступа должны предоставлять высокоскоростное проводное (Gigabit Ethernet) и беспроводное (802.11n) подключение к сети.

Оборудование которое может применяться в качестве уровня доступа:

Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot
Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E
Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports
Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports
Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports
Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports
Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports
Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports
Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports
Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports
Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports
Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports

2.1.2. УГРОЗЫ

Поскольку уровень доступа является входной точкой в сеть для клиентских устройств он в первую очередь должен обеспечивать защиту самих пользователей, корпоративных ресурсов и сеть от вредоносных атак со стороны подключаемых клиентов/устройств (в случае их заражения всевозможными вирусами) или хакеров, получивших доступ в локальную сеть.

Уровень доступа включает в себя следующие технологии защиты:

- DHCP-snooping - защищает пользователей от получения адреса от неизвестного DHCP-сервера, а так же не позволяет злоумышленнику захватить все ip-адреса.
- IP Source guard - защита от IP spoofing-а, т.е. от подмены IP-адреса источника.
- Port security - устанавливается ограничение на кол-во MAC адресов поступающих на порт коммутатора. Защищает от подмены MAC адреса и от атак, направленных на переполнение таблицы коммутации.
- Dynamic ARP inspection - защита от ARP spoofing-а, т.е. от перехвата трафика между компьютерами.

Более подробное рассмотрение технологий атак и защиты от них, выходит за рамки данного руководства.

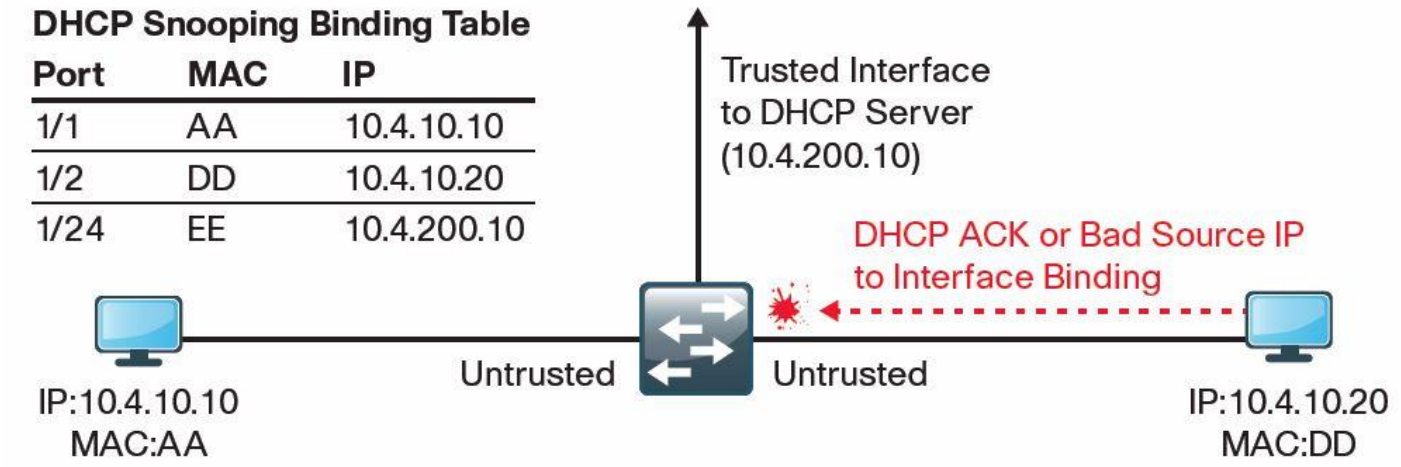


Рис. 2.2. DHCP-snooping и ARP Inspection

2.1.3. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

В случае если планируется подключение к сети таких устройств, как ip-телефоны, ip-видеокамеры или беспроводные точки доступа, будет разумным использовать коммутаторы с поддержкой технологии PoE (Power over Ethernet). Это существенно упростит и удешевит внедрение вышеуказанных устройств (исключается необходимость в дополнительном питании от электросети).

Наиболее экономичным решением являются коммутаторы Catalyst серии 2960. Решение на основе этих коммутаторов предоставляет самую низкую стоимость за порт (подключенного пользователя, сервера или какого-либо другого устройства), при этом обеспечивает весь необходимый функционал для уровня доступа (сегментирование сети, QoS, PoE, и т.д.). Использование коммутаторов уровня доступа позволяет существенно снизить затраты на подключение пользователей и серверов. В настоящий момент в линейке появилась новая, более производительная и современная модель Cisco Catalyst 2960-X, стоимость которой сопоставима со стоимостью предыдущей модели. При проектировании сетей будет уместным использование новых коммутаторов. Коммутаторы серии 3560, 3750, 4500 и 4507 применяются гораздо реже и только в том случае, когда покупка отдельного коммутатора для уровня доступа является нецелесообразной (малое количество пользователей). Данные коммутаторы больше подходят для уровня распределения.

В случае установки нескольких коммутаторов уровня доступа, расположенных в непосредственной близости (в одном серверном шкафу) рекомендуется использовать технологию стекирования (Рис. 2.3).

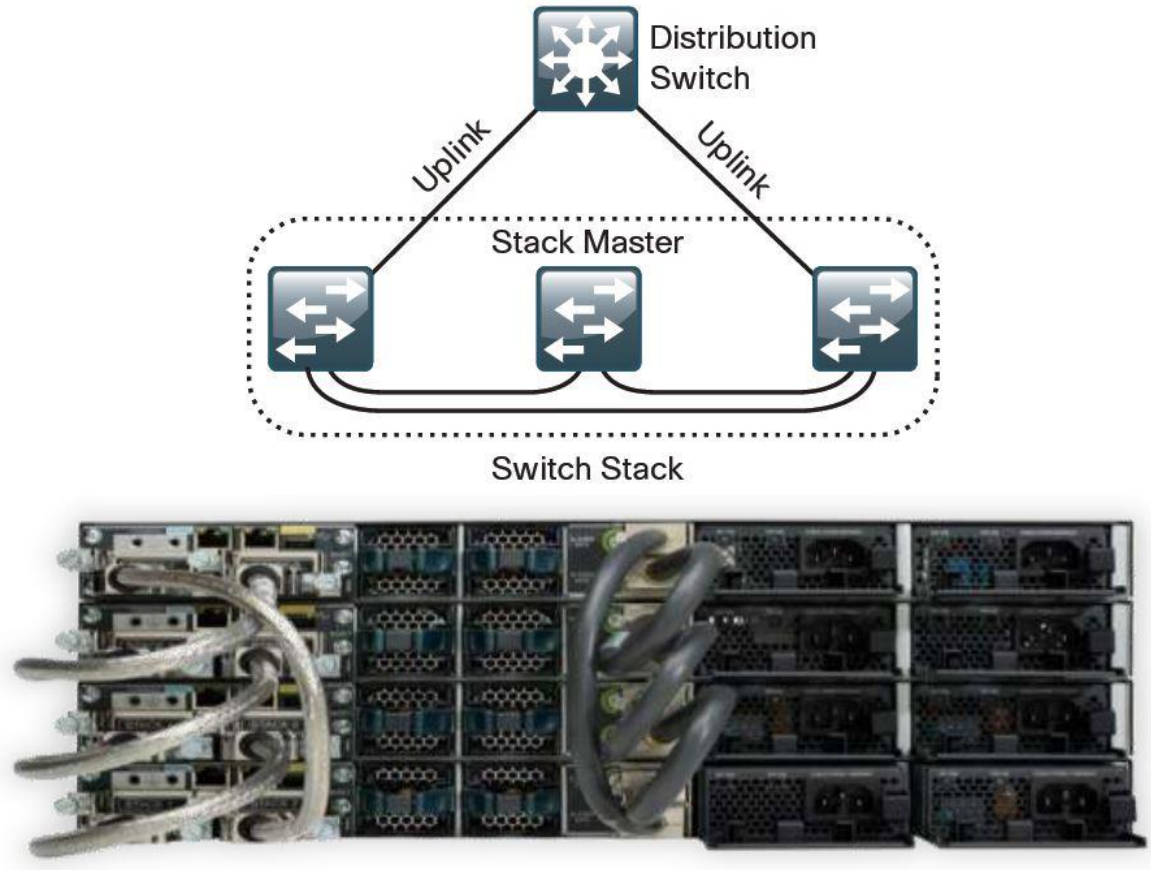


Рис. 2.3. Стек коммутаторов уровня доступа

Данная технология позволяет объединять оборудование в единое целое. Стек из трех 24-х портовых коммутаторов используется как одно устройство, имеющее 72 порта. Это существенно облегчает управление и конфигурирование, а так же реализует дополнительную отказоустойчивость. Однако следует отметить, что данное решение будет существенно дороже, т.к требует приобретения дополнительных модулей стекирования для коммутаторов серии 2960-S и 2960-X.

Каждый коммутатор уровня доступа должен подключаться к коммутаторам уровня распределения по агрегированному каналу (об этом чуть позже).

- Коммутаторы уровня доступа должны располагаться не более чем в 90 метрах от пользователей (коммутационный шкаф или серверная комната) для их подключения по витой паре.
- Если устройства уровня доступа находятся на расстоянии более чем 100 м от коммутаторов уровня распределения, то используется оптоволоконное соединение. Это стоит учитывать при проектировании и закладывать коммутаторы с поддержкой оптоволоконных подключений (технология SFP, SFP+).

2.1.4. АЛЬТЕРНАТИВЫ

Устройства уровня доступа являются самыми дешевыми в сетевой инфраструктуре, однако, их может быть большое кол-во, что ведет к большим затратам. Стоимость современного 24-х портового коммутатора компании Cisco (Catalyst 2960-X 24 GigE 4 x 1G SFP LAN Base) составляет около 2400$. При выборе других моделей стоит четко понимать какой функционал вам потребуется от устройств уровня доступа.

Коммутаторы второго уровня компаний D-link, Zyxel схожей конфигурации будут стоить дешевле в 2-3 раза. Такие коммутаторы подойдут для подключения серверов. Для подключения пользователей можно использовать более дешевые решения выше упомянутых компаний, но только в том случае, если требования к безопасности не слишком высоки. К примеру коммутаторы D-link и Zyxel очень распространены среди провайдеров интернет связи, ввиду своей дешевизны и достаточного для их задач функционала.

От себя хотелось бы добавить, что коммутаторы компании Cisco в крупном корпоративном сегменте стали практически стандартом.

2.2. УРОВЕНЬ РАСПРЕДЕЛЕНИЯ (DISTRIBUTION LAYER)

Уровень распределения обслуживает множество важных сервисов сети. Главной задачей уровня распределения является агрегация/объединение всех коммутаторов уровня доступа в единую сеть. Это позволяет существенно уменьшить количество соединений. Как правило, именно к коммутаторам распределения подключаются самые важные сервисы сети, другие модули сети: модуль сети Internet, модуль WAN сети, модуль дата-центра (Рис. 2.4).

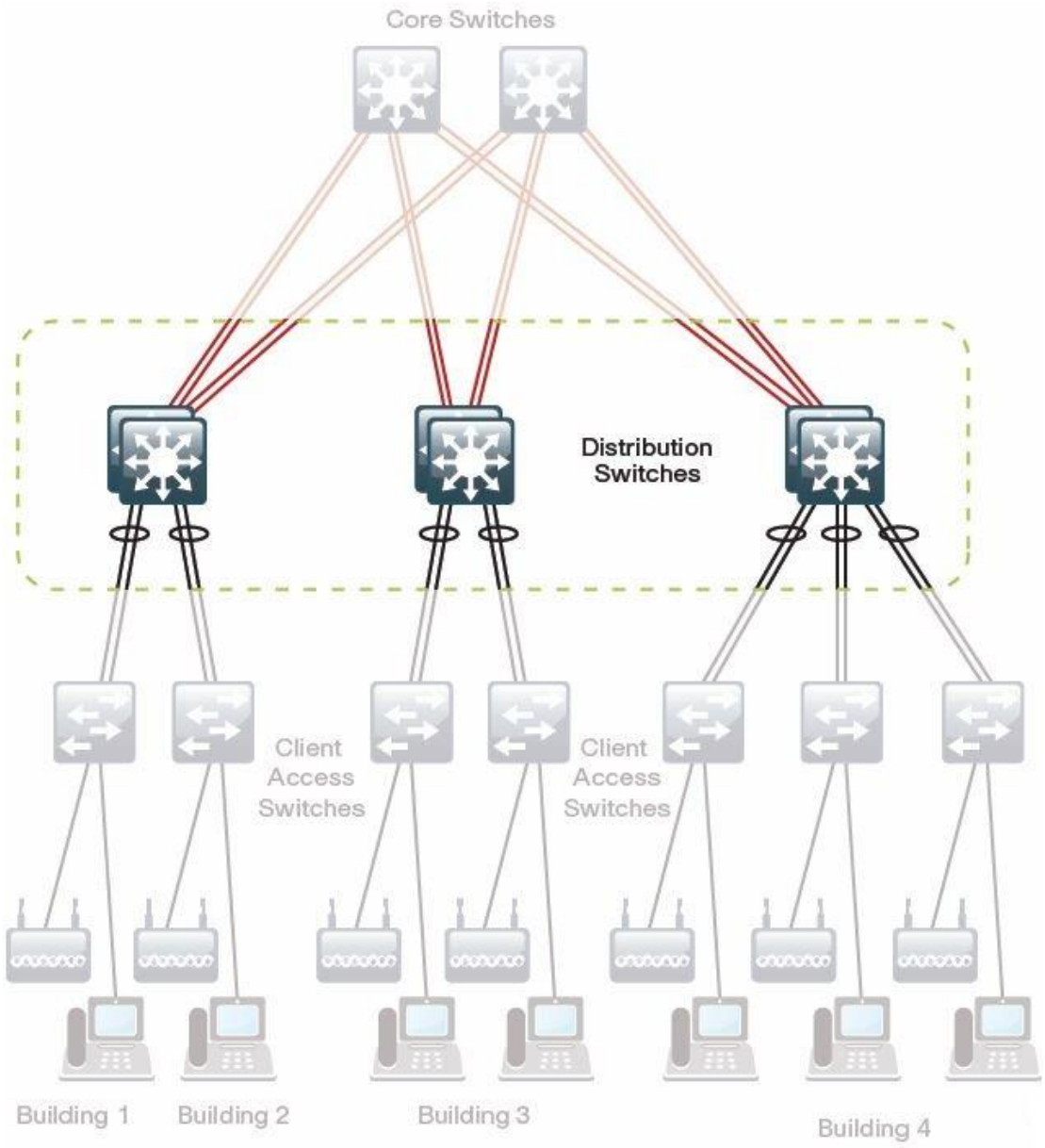


Рис. 2.4. Уровень распределения

2.2.1. УСТРОЙСТВА

Устройства уровня распределения это, как правило, коммутаторы третьего уровня (L3) модели OSI. Коммутаторы осуществляют маршрутизацию трафика между сегментами сети (между различными VLAN), а так же реализуют систему безопасности и сетевые политики (контроль доступа).

Оборудование которое может применяться в качестве уровня распределения:

Cisco Catalyst 6500 E-Series 6-Slot Chassis
Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4
Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4
Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4
Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4
Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module

Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot
Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps
Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module
Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module
Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports
Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module
Cisco Catalyst 3750-X Series Four GbE SFP ports network module

Так же можно использовать эти модели:
Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000
Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000

Однако, следует учитывать, что это Stand-Alone коммутаторы, т.е. не поддерживают технологию стекирования (в отличии от 3750-X), а значит высокопроизводительная и отказоустойчивая конфигурация не доступна при использовании коммутаторов этой модели.

2.2.2. УГРОЗЫ

Уровень распределения включает в себя следующие технологии защиты:

- Контроль доступа - атаки на корпоративные ресурсы ограничиваются политиками безопасности (списки доступа)
- Защита от IP spoofing-а

Как можно заметить, защита от угроз является второстепенной функцией уровня распределения. Основные функции описаны выше.

2.2.3. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

Уровень распределения является очень важным звеном в работе всей сетевой инфраструктуры и требует высокопроизводительного, отказоустойчивого исполнения.

Модель Cisco SBA LAN предполагает использование технологии стекирования и агрегированных соединений межу сетевыми устройствами, в то время как традиционная модель использует принцип избыточности (redundant).

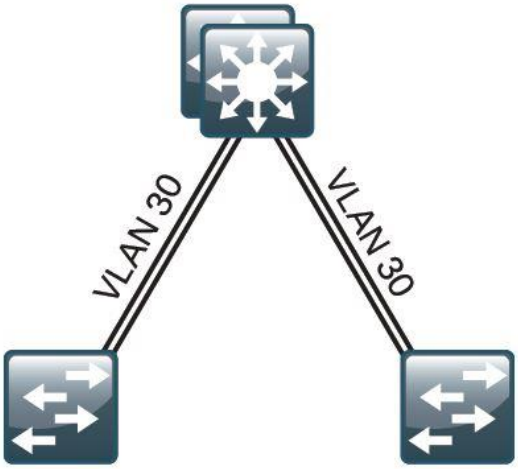


Рис. 2.5. Новая модель SBA LAN

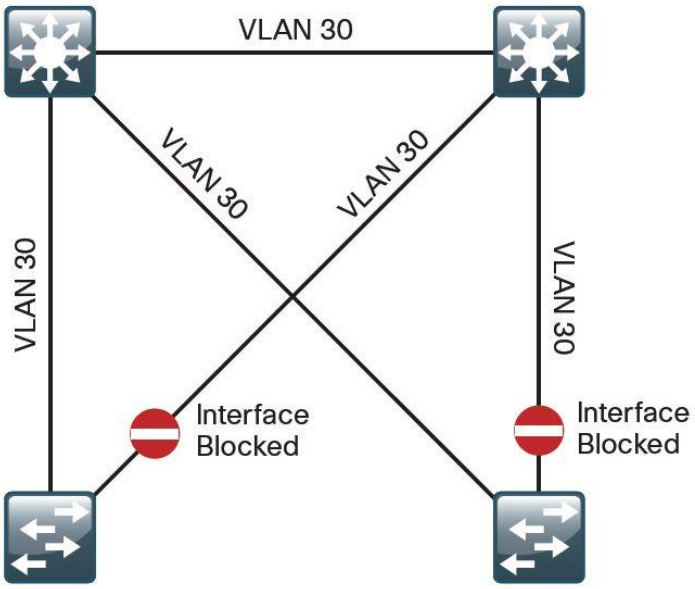


Рис. 2.6. Традиционная Избыточная модель

Новая модель SBA использует агрегированные каналы между устройствами уровня доступа и уровня распределения (с использование таких протоколов как EtherChannel) одновременно обеспечивая отказоустойчивость и более высокую производительность. Агрегированный канал является объединением 2-х, 3-х или более физических (проводных) соединений в одно логическое. При этом все соединения передают информацию, что существенно увеличивает пропускную способность канала (Рис. 2.5). В случае отказа одного из соединений, входящего в агрегированный канал, информация по прежнему передается по другим исправным соединениям без каких-либо перерывов в работе сети. Это выгодное отличие от традиционной Избыточной модели в которой блокируются дополнительные соединения (протокол STP, RSTP) для предотвращения петель (Рис. 2.6). Таким образом при использовании традиционной модели производительность не увеличивается, реализуется только отказоустойчивость.

Коммутаторы уровня распределения объединяются в стек (с использованием таких технологий как StackWise Plus). Агрегированный канал образуется при объединении портов разных коммутаторов стека (Рис. 2.7). Другими словами, логический интерфейс образуется объединением двух (или более) портов, при этом один порт принадлежит первому коммутатору стэка, а второй порт - второму. Оба порта участвуют в передаче трафика. Таким образом оказываются задействованными все устройства, обеспечивая высокую производительность и отказоустойчивость.

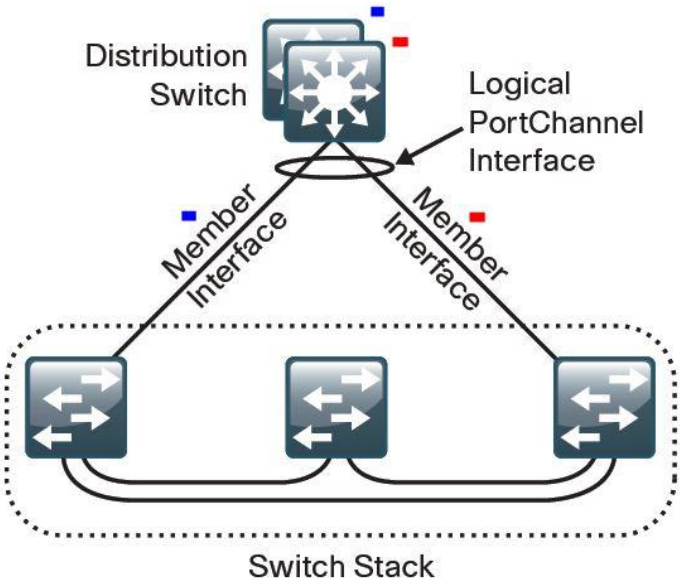


Рис. 2.7. Объединение портов стека коммутаторов в один PortChannel

В традиционной Избыточной (Redundant) модели сетевой трафик передает только одно устройство. Второе устройство становится активным только при падении первого, либо при отказе одного из активных соединений (сработает технология STP).

2.2.4. АЛЬТЕРНАТИВЫ

Для снижения затрат и общего числа устанавливаемых устройств можно объединить уровень распределения с уровнем ядра, если это позволяют размеры сети и требования к пропускной способности. Это довольно частая практика. Уровень распределения выступающий в качестве уровня ядра называется Collapsed core (Рис. 2.8).

В качестве альтернативного оборудования можно выбрать решения компании Juniper или HP. Данные компании является основными конкурентами компании Cisco в корпоративном сегменте. Коммутаторы Juniper и HP немного дешевле, однако если в сетевой инфраструктуре преобладают коммутаторы (а так же межсетевые экраны, IPS) компании Cisco, то не стоит "разводить зоопарк" из оборудования ради небольшой экономии. Гораздо проще управлять сетями, построенными на оборудовании одного вендора (особенно если это касается оборудования компании Cisco). Так же стоит учесть важность поддержки технологии стекирования.

Одним из самых дешевых решений являются коммутаторы компании D-Link. К примеру модель DGS-3120-24PC/B1ARI - L3 коммутатор, поддерживающий технологию стекирования.

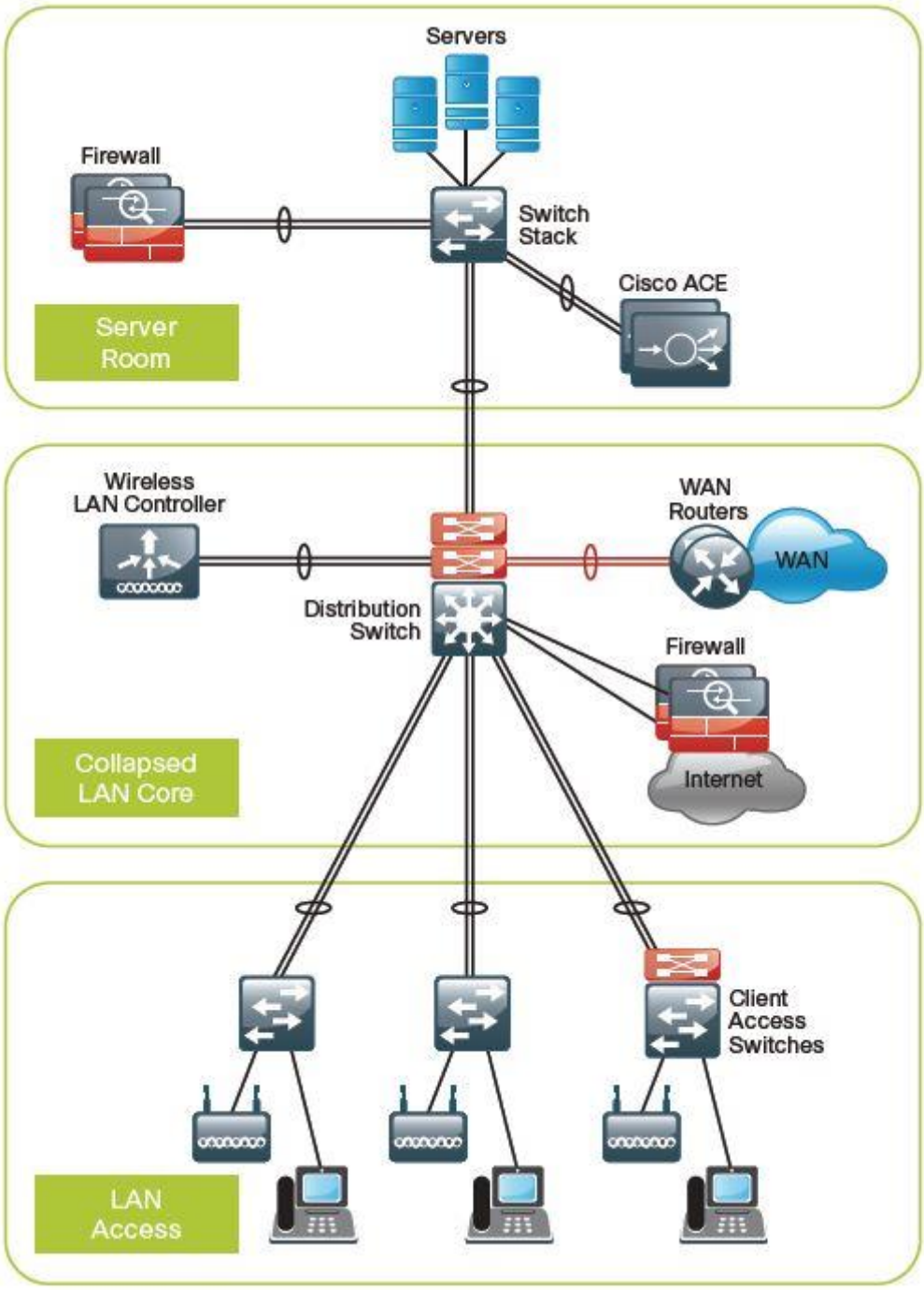


Рис. 2.8. Уровень распределения в качестве уровня ядра (Collapsed core)

2.3. УРОВЕНЬ ЯДРА (CORE LAYER)

Дизайн больших корпоративных сетей, охватывающих два и более зданий, обязывает использование Уровня Ядра. Главной задачей уровня ядра является агрегация/объединение всех коммутаторов уровня распределения в единую сеть. Это позволяет существенно уменьшить количество соединений. На Рис. 2.9 и 2.10 представлены дизайн сети, без и с уровнем ядра соответственно. Как видим, без использования уровня ядра количество соединений значительно больше.

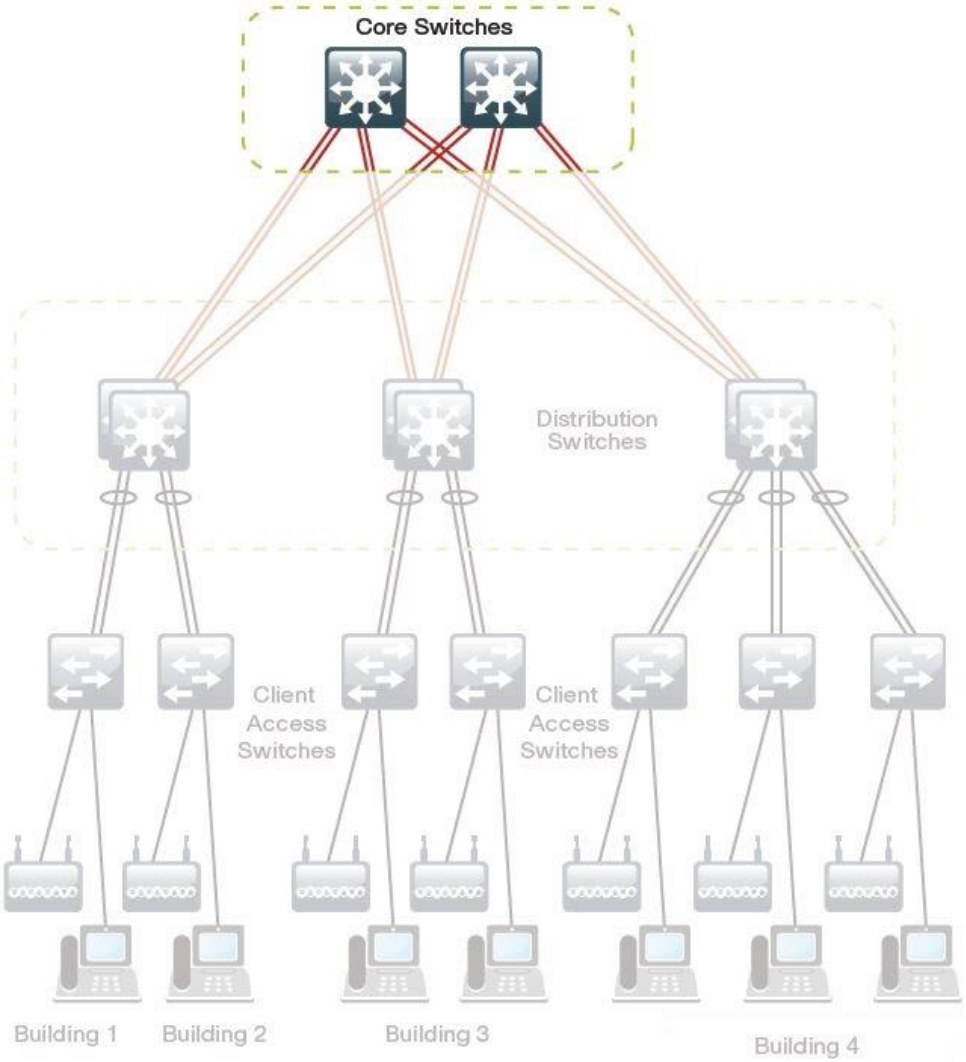


Рис. 2.9. Уровень Ядра (Core Layer)

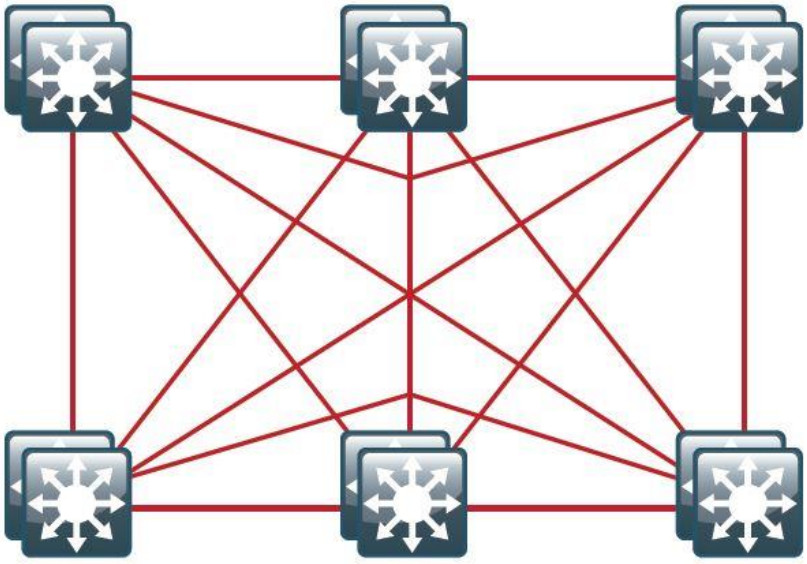


Рис. 2.10. Дизайн сети без уровня ядра

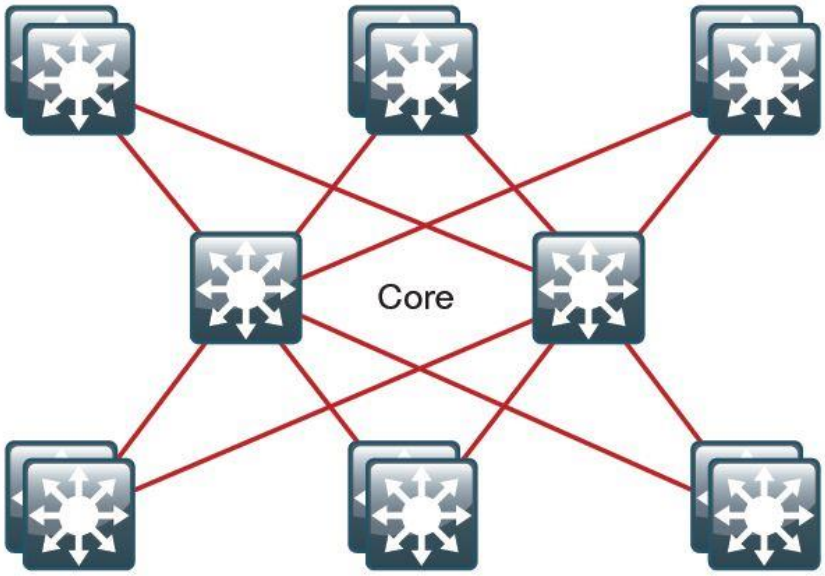


Рис. 2.11. Дизайн сети с уровнем ядра

2.3.1. УСТРОЙСТВА

Коммутаторы уровня ядра не должны выполнять каких-либо сложных действий. Их основная функция это маршрутизация трафика между модулями сети. Уровень ядра это, как правило, два коммутатора, подключение к которым осуществляется только на третьем уровне модели OSI, т.к. время сходимости на L3 уровне гораздо меньше чем на L2.

В качестве устройств уровня ядра применяются коммутаторы третьего уровня модели OSI (L3).

Оборудование которое может применяться в качестве уровня распределения:
Cisco Catalyst 6500 E-Series 6-Slot Chassis
Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4
Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4
Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4
Cisco Catalyst 6500 8-port 10GbE Fiber Module w/ DFC4

2.3.2. УГРОЗЫ

Что касается угроз, то обеспечение безопасности не входит в основные задачи уровня Ядра. Основная и главная функция уровня Ядра это маршрутизация трафика. Нагружать оборудование дополнительными задачами (списки доступа, port security, и т.д.) не рекомендуется, чтобы не снижать производительность сети.

2.3.3. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

Важно понимать, что объединение в единую сеть нескольких зданий возможно только с использованием контролируемой зоны. Под контролируемой зоной понимается собственный

канал передачи данных (оптический канал, медный и т.д.). Т.е. если между двух зданий соединение осуществляется по специальному выделенному каналу (который находится в контролируемой зоне) то в этом случае можно организовывать Уровень ядра. Если же два здание соединены по средствам Интернет канала, то в этом случае стоит применять специальный для этого модуль - либо модуль Интернет (Internet Edge) либо модуль сети WAN (WAN area), о которых мы поговорим позже.

К уровню ядра подключаются все модули сети (все коммутаторы уровня распределения). В общем виде схема подключения представлена на рисунке 2.12.

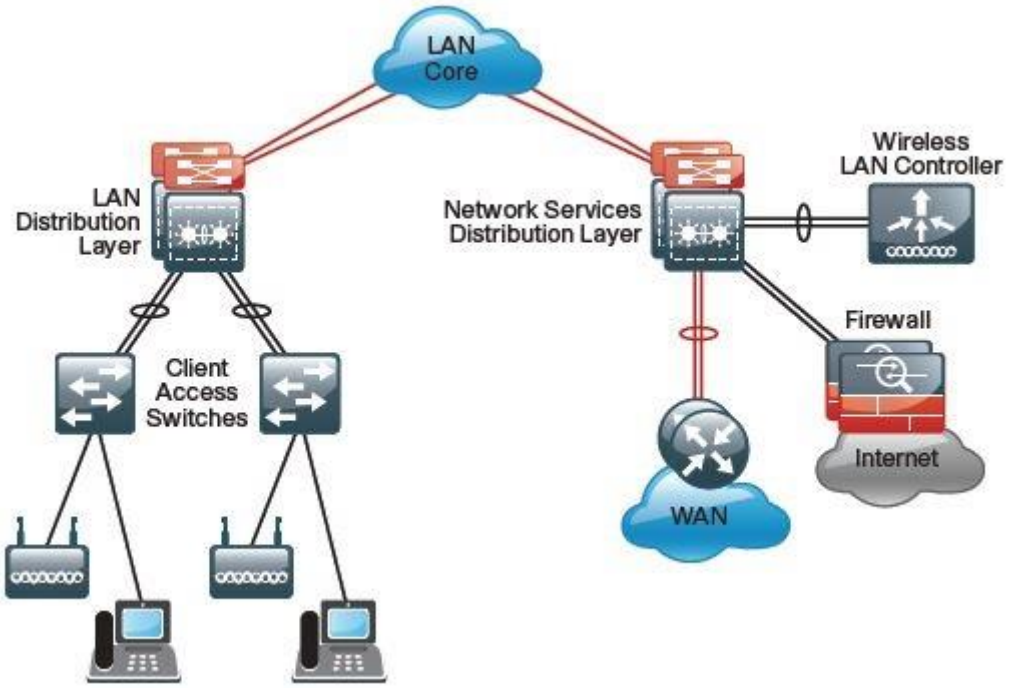


Рис. 2.12. Подключение модулей сети к уровню ядра

Коммутаторы уровня ядра должны обладать самой высокой пропускной способностью среди всех коммутаторов вашей сети (от 40 Гбит/с). Все коммутаторы уровня распределения и любые другие модули должны подключаться к обоим коммутаторам уровня яда, таким образом обеспечивая отказоустойчивость. Подключение осуществляется с использованием технологий EtherChannel, что позволяет балансировать поток трафика. На рисунке 2.13 представлен пример использования уровня Ядра.

2.3.4. АЛЬТЕРНАТИВЫ

Коммутаторы уровня Ядра являются самыми дорогими устройствами в иерархической модели сети (если рассматривать только коммутаторы и не брать в расчет устройства безопасности). Далеко не каждая организация может себе позволить данные устройства. Однако при необходимости использования уровня Ядра, в первую очередь нужно определиться с пропускной способностью, которая требуется от оборудования. Возможно, что для ваших целей подойдут устройства из более дешевого сегмента (например коммутаторы уровня распределения). Так же необходимо понимать, что одним из важнейших параметров уровня Ядра является отказоустойчивость, т.к. от устройства данного уровня зависит работа огромной

сети (в маленьких сетях уровень ядра обычно отсутствует или же интегрирован с уровнем распределения). Поэтому при выборе оборудования стоит обращать внимание на технологии организации отказоустойчивости, резервирования питания. Лидерами среди коммутаторов уровня ядра являются компании: Cisco, Juniper, HP, Brocade, Extreme Networks. Однако есть и более дешевые решения уровня ядра от компании D-Link.

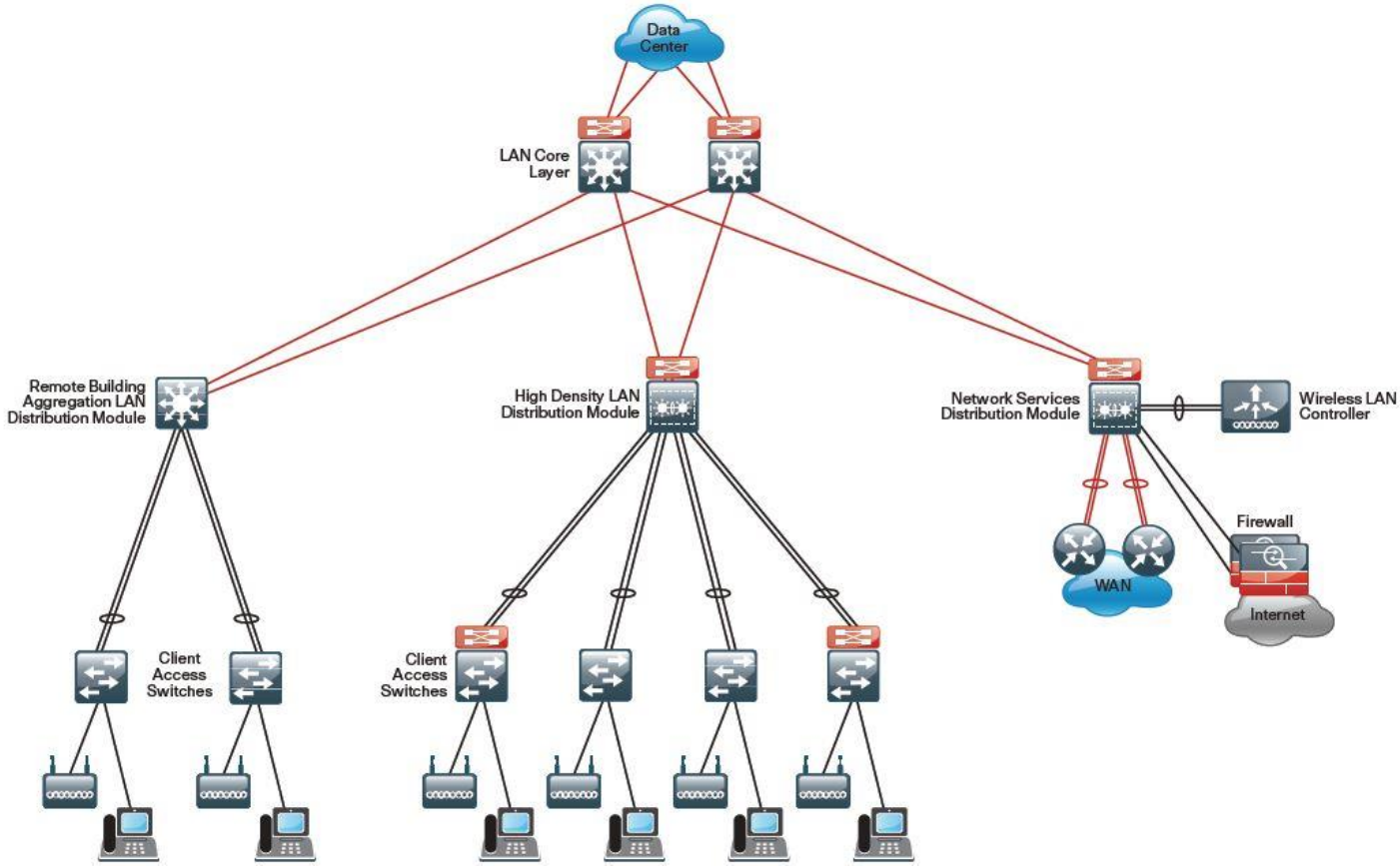


Рис. 2.13. Пример использования Уровня Ядра (LAN Core Layer)

3. МОДУЛИ КОРПОРАТИВНОЙ СЕТИ

Освоив иерархическую модель и построив “скелет” сети можно переходить к внедрению остальных корпоративных модулей. В этом и заключается одно из главных преимуществ модульной архитектуры - построение сети осуществляется небольшими, простыми для понимания, частями.

4. МОДУЛЬ СЕТИ ИНТЕРНЕТ

Трудно представить современную компанию без наличия доступа к сети Internet. Огромное количество бизнес процессов завязаны на использование интернет ресурсов (web-сайты, электронная почта и т.д.). Соответственно доступ в Internet должен быть стабильным и безопасным. Именно для этого используется Модуль сети Интернет (или, как еще его называют - Internet Edge).

Модуль сети Интернет в свою очередь разбивается на несколько функциональных блоков, обеспечивающих работу определенных сервисов. Таким образом организация может внедрять данные блоки исходя из бизнес потребностей.

Современный Модуль сети Интернет должен включать в себя следующие функциональные блоки:

- Межсетевой экран (МЭ) - осуществляет контроль доступа между различными сегментами сети (сегмент серверов, сегмент пользователей и т.д.), а также предоставляет другие сетевые сервисы, такие как NAT и организация DMZ.
- Система предотвращения вторжений (IPS) - проверяет (инспектирует) трафик на предмет подозрительной и аномальной активности.
- Удаленный доступ (Remote access или RA VPN) - предоставление безопасного удаленного доступа к локальным корпоративным ресурсам, не зависимо от местонахождения пользователя.
- Защита электронной почты - защита от спама и писем, содержащих вредоносный код.
- Веб-защита - контроль использования интернет ресурсов и обеспечение безопасности пользователя в сети Интернет.

Ключевое отличие модульной архитектуры - масштабируемость, эффективность и устойчивость. Каждый блок Модуля сети Интернет независим от остальных. Таким образом вы можете использовать только необходимые вашему бизнесу блоки, создавая свой собственный дизайн сети.

На рисунке 4.1 представлен пример реализации Модуля сети Интернет (Internet Edge).

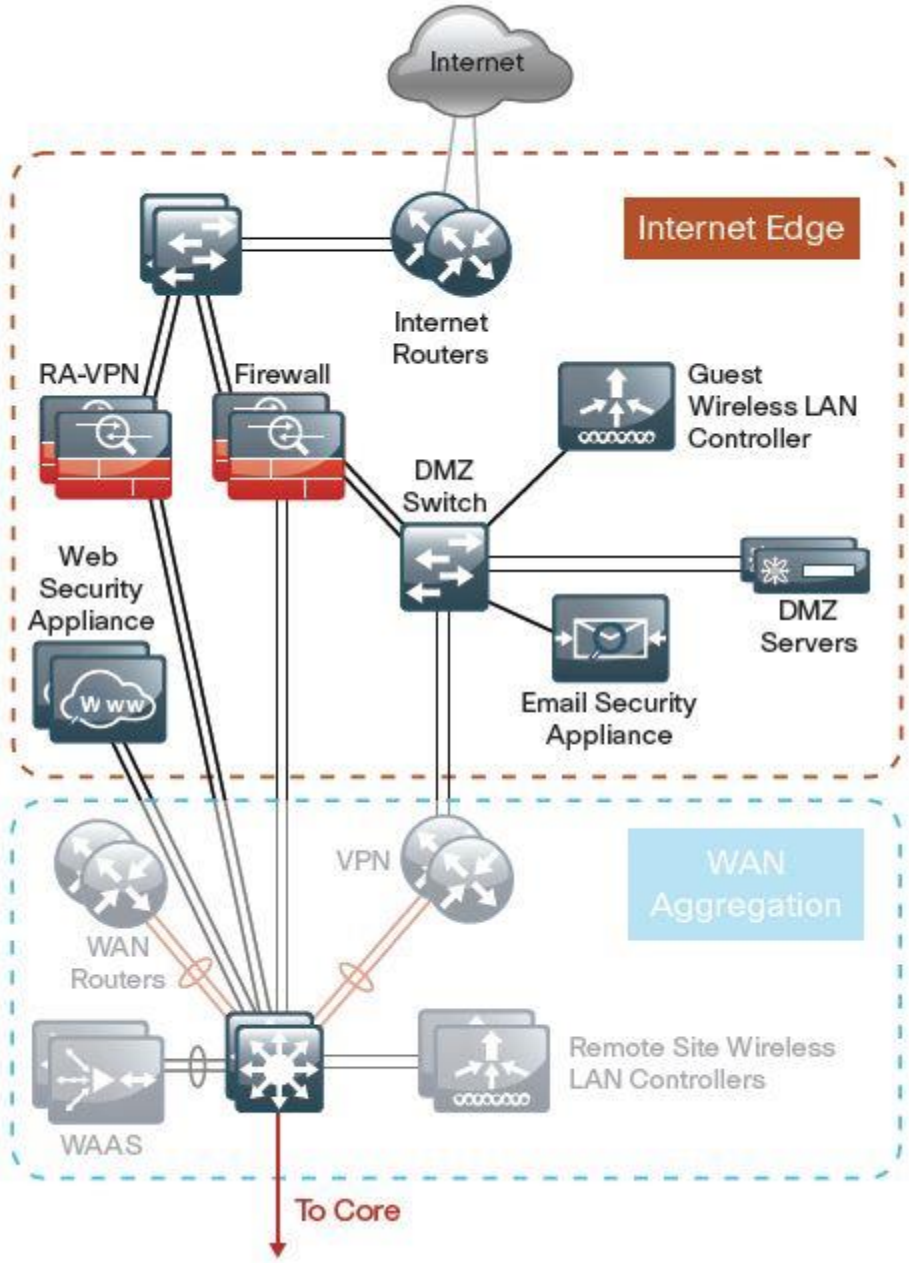


Рис. 4.1. Пример дизайна Модуля сети Интернет

4.1. ИНТЕРНЕТ ПОДКЛЮЧЕНИЕ

Три основных фактора, которые определяют требования к Интернет подключению для бизнеса:

- Значение сети Интернет для бизнеса
- Доход от бизнес процессов использующих интернет ресурсы
- Экономия от использования интернет сервисов
- Потери из-за простоя в случае разрыва интернет подключения
- Расходы на реализацию и поддержку системы обеспечивающей Интернет подключение

Три главных характеристики, которые используются при проектировании Интернет подключения:

1. Скорость подключения или “ширина” канала - Необходимая пропускная способность Интернет подключения.
2. Кол-во IP адресов - В зависимости от размера организации могут понадобиться дополнительные “белые” IP адреса для различных корпоративных web ресурсов, VPN подключений, почтовых серверов и т.д.
3. Отказоустойчивость - Наличие резервного Интернет канала.

В таблице 4.1 приводятся рекомендации компании Cisco по ширине канала относительно кол-ва пользователей организации.

Таблица 4.1. Рекомендации по ширине канала сети Интернет

Кол-во пользователей	Ширина канала
До 4500	20-50 Мбит/с
От 3000 до 7000	35-75 Мбит/с
От 6000 до 10000	70-130 Мбит/с

Что касается маршрутизации, то для большинства организаций (до 10 000 пользователей) достаточно статического маршрута по умолчанию для обеспечения доступа в сеть Интернет (использование динамических протоколов маршрутизации в данном случае нецелесообразно).

4.2. МЕЖСЕТЕВОЙ ЭКРАН

Модуль сети Интернет это точка, где локальная корпоративная сеть подключается к глобальной сети Интернет. Это, так называемый периметр сети, граница между публичной сетью и приватными ресурсами организации. Именно на этой границе должен находиться межсетевой экран. Сети, подключенные к Интернет, постоянно подвержены угрозам в виде вирусов, червей, троянских программ, направленных атак. Организации должны обеспечивать должный уровень защищенности персональных данных и информации о клиентах.

Межсетевой экран является одним из главных блоков в защите корпоративной сети. МЭ осуществляет контроль доступа между различными сегментами сети (сегмент Интернет, сегмент Пользователей, сегмент Бухгалтерии, сегмент Серверов и т.д.), а так же фильтрует нежелательный и вредоносный трафик. Межсетевой экран в большей степени предназначен для защиты от проникновения угроз в локальную сеть из вне. В большинстве организаций МЭ дополнительно реализует такие сервисы как NAT и удаленный доступ по VPN.

4.2.1. УСТРОЙСТВА

На момент написания книги серия межсетевых экранов Cisco ASA 5500 уже была объявлена как end of life, т.е. устройства уже не производятся, а 2018 год объявлен как последний год технической поддержки. Поэтому при выборе устройств стоит обратить внимание на новую линейку Cisco ASA 5500-X. Это более производительная и современная серия межсетевых экранов.

Рис. 4.2. Переход от Cisco ASA 5500 к Cisco ASA 5500-X

В таблице 4.2 приводится путь перехода на новую серию Cisco ASA 5500-X.

Таблица 4.2. Примерные эквиваленты межсетевых экранов

Устройство ASA 5500	Эквивалентное устройство ASA 5500-X
ASA 5510	ASA 5512-X
ASA 5510 Security Plus license	ASA 5515 или ASA 5512 Security Plus license
ASA 5520	ASA 5525-X
ASA 5540	ASA 5545-X
ASA 5550	ASA 5555-X

Оборудование которое может применяться в Модуле сети Интернет:

Cisco ASA 5545-X - security appliance (ASA5545-K9)
Cisco ASA 5525-X - security appliance (ASA5525-K9)
Cisco ASA 5515-X - security appliance (ASA5515-K9)
Cisco ASA 5512-X - security appliance (ASA5512-K9)
Cisco ASA5512-X Security Plus license (ASA5512-SEC-PL)

В отличии от серии 5500 в новой серии функционал IPS активируется с помощью лицензии, при этом не требуется установка дополнительного аппаратного модуля (в старой серии были необходимы модули AIP-SSM).

МЭ с уже активированной функцией IPS:

Cisco ASA 5545-X IPS Edition - security appliance (ASA5545-IPS-K9)
Cisco ASA 5525-X IPS Edition - security appliance (ASA5525-IPS-K9)
Cisco ASA 5515-X IPS Edition - security appliance (ASA5515-IPS-K9)
Cisco ASA 5512-X IPS Edition - security appliance (ASA5512-IPS-K9)
Cisco ASA5512-X Security Plus license (ASA5512-SEC-PL)

Стоит так же отметить, что в новой серии самая младшая модель это 5512X - стоечное устройство, устанавливаемое в серверный шкаф (1U). Замены настольной Cisco ASA 5505 (small business решение) на сегодняшний день нет.

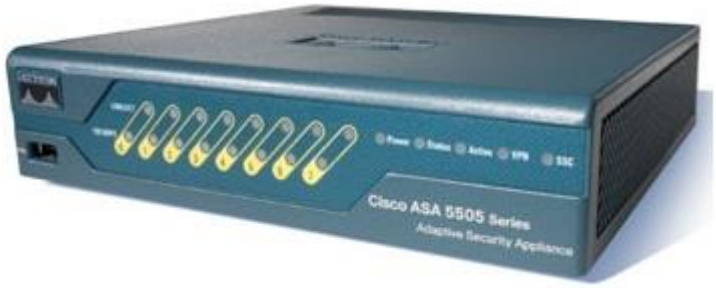


Рис. 4.3. Cisco ASA 5505

При проектировании Модуля сети Интернет выбор устройств основывается прежде всего на требуемой производительности. Мы должны учитывать следующие факторы:

- Ширину канала сети Интернет;
- Кол-во серверов находящихся в DMZ и требуемую для них пропускную способность сети для комфортной работы пользователей;
- Кол-во VPN подключений - удаленный доступ (RA VPN)

Ширину канала мы рассмотрели ранее в таблице 4.1. Рассматривая необходимую пропускную способность для DMZ серверов стоит учитывать:

- Трафик идущий из сети Интернет;
- Трафик идущий из локальной сети от пользователей, которым требуются сервисы предоставляемые DMZ серверами (Web сервер, ftp сервер, Email сервер и т.д.).

В таблице 4.3 представлена пропускная способность устройств для "реального трафика" (похожий на обычный пользовательский трафик организаций).

Таблица 4.3. Пропускная способность межсетевых экранов

Модель Cisco ASA	Пропускная способность реального трафика
Cisco ASA 5512-X	500 Мбит/с
Cisco ASA 5515-X	600 Мбит/с
Cisco ASA 5525-X	1 Гбит/с
Cisco ASA 5545-X	1.5 Гбит/с

4.2.2. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

Согласно документации Cisco SBA в дизайн Модуля сети Интернет должны входить следующие компоненты:

- Маршрутизатор;
- Outside коммутаторы в отказоустойчивом исполнении (отказоустойчивость реализуется с использованием технологии стекирования либо с помощью традиционной избыточной модели);
- Межсетевые экраны с функцией IPS в отказоустойчивом исполнении (отказоустойчивость реализуется с помощью active/active failover либо active/standby failover);

- DMZ коммутаторы в отказоустойчивом исполнении (отказоустойчивость реализуется с использованием технологии стекирования либо с помощью традиционной избыточной модели);
- Коммутаторы уровня распределения (Distribution) в отказоустойчивом исполнении (отказоустойчивость реализуется с использованием технологии стекирования либо с помощью традиционной избыточной модели).

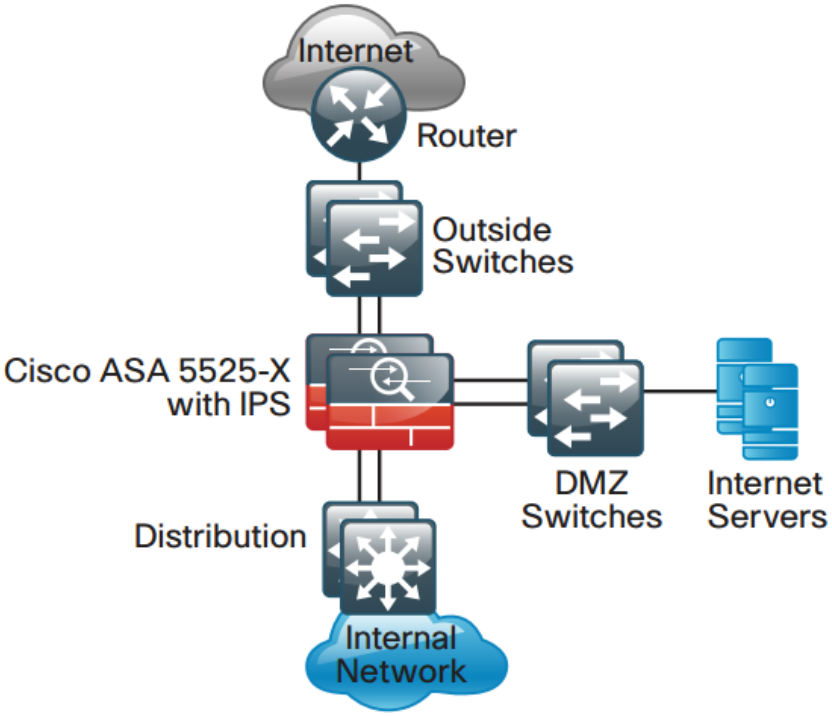


Рис. 4.4. Типовой дизайн модуля

В случае большого кол-ва VPN подключений (RA VPN) можно выделить отдельные МЭ для данной задачи. Так же возможно подключение двух Интернет провайдеров для дополнительной отказоустойчивости.

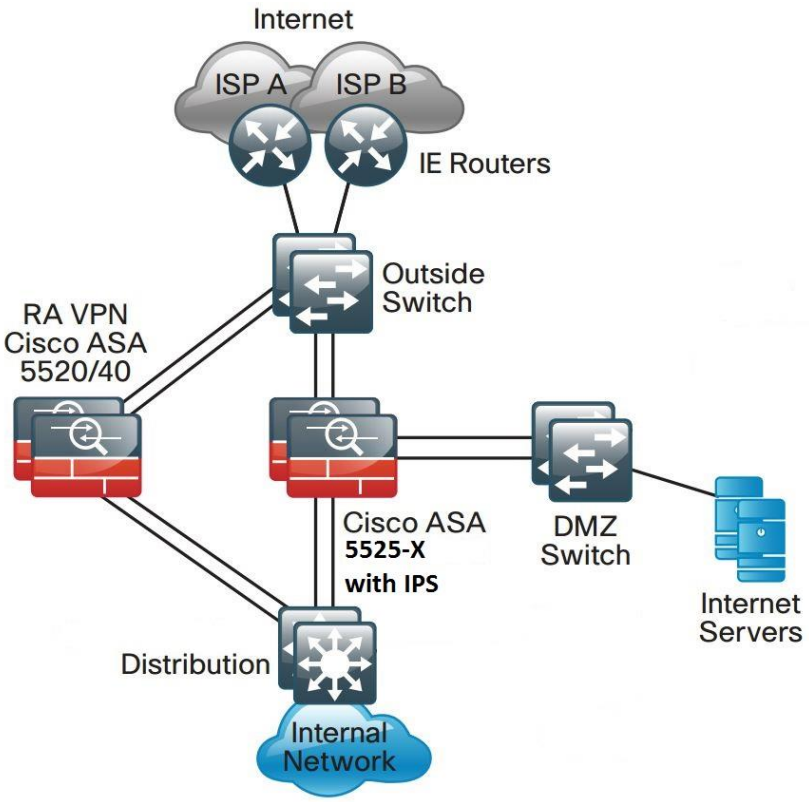


Рис. 4.5. Типовой дизайн модуля

Все соединения между устройствами выполнены в отказоустойчивом исполнении с использованием технологии EtherChannel.

Однако представленные схемы является весьма дорогостоящими в реализации. Как правило малые и средние компании не могут себе позволить подобные решения и стремятся уменьшить расходы путем сокращения кол-ва устройств за счет пренебрежения отказоустойчивостью и объединения нескольких функций в одном устройстве.

Более экономичный вариант может выглядеть следующим образом:

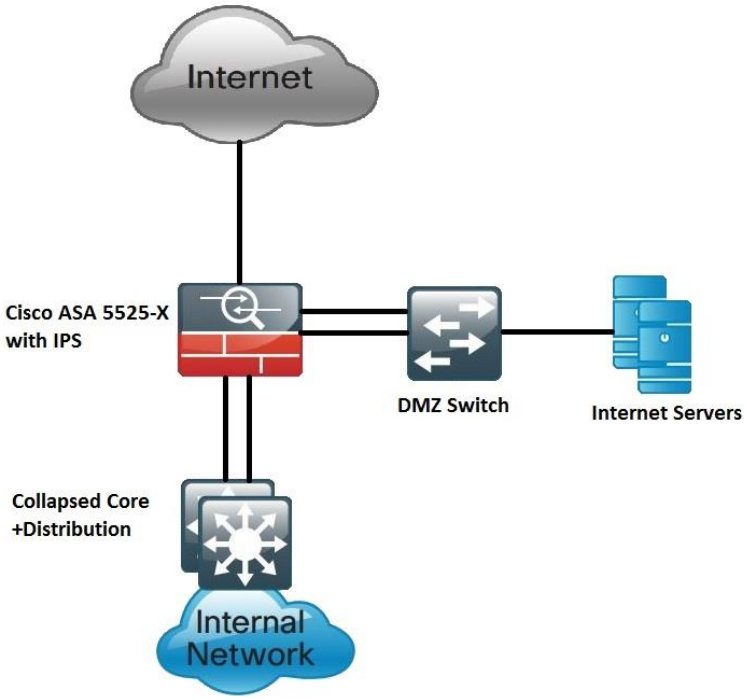


Рис. 4.6. Типовой дизайн модуля

В случае использования одного Интернет провайдера и одного межсетевого экрана можно отказаться от outside коммутатора. Так же для экономии можно использовать один DMZ коммутатор. Отказавшись от выделенных коммутаторов уровня распределения можно существенно сократить расходы. При этом используются существующие коммутаторы уровня распределения выступающие в качестве уровня ядра (collapsed core).

Подключения между МЭ и коммутаторами выполнены в отказоустойчивом исполнении с использованием технологии EtherChannel.

Отказоустойчивость МЭ достигается с помощью использования технологии failover, либо технологии кластеризации, которая присутствует в Cisco ASA серии 5500-X и отсутствует в предыдущей серии.

4.2.3. АЛЬТЕРНАТИВЫ

На сегодняшний день на рынке существует огромное кол-во вендоров, производящих межсетевые экраны. Как платные, так и в виде свободного программного обеспечения (open source).

Первое на что стоит обратить внимание, это тип организации в которой планируется установить МЭ. Согласно приказу ФСТЭК России от 11 февраля 2013 года №17 "устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней (далее – защита информации) при обработке указанной информации в государственных информационных системах.

Настоящие Требования могут применяться для защиты общедоступной информации, содержащейся в государственных информационных системах, для достижения целей, указанных в пунктах 1 и 3 части 1 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».”

Таким образом для некоторых организаций основным требованием к МЭ может стать сертификат ФСТЭК на соответствие оборудования одному из 5 классов. В этом случае искать альтернативу оборудованию Cisco можно только среди сертифицированных межсетевых экранов.

Если же к организации нет подобных требований то список возможных альтернатив значительно увеличивается. На рисунке 4.7 представлен “магический квадрант Гартнера” для межсетевых экранов используемых в различных корпорациях. Данный график отражает мировых лидеров в области сетевой безопасности.

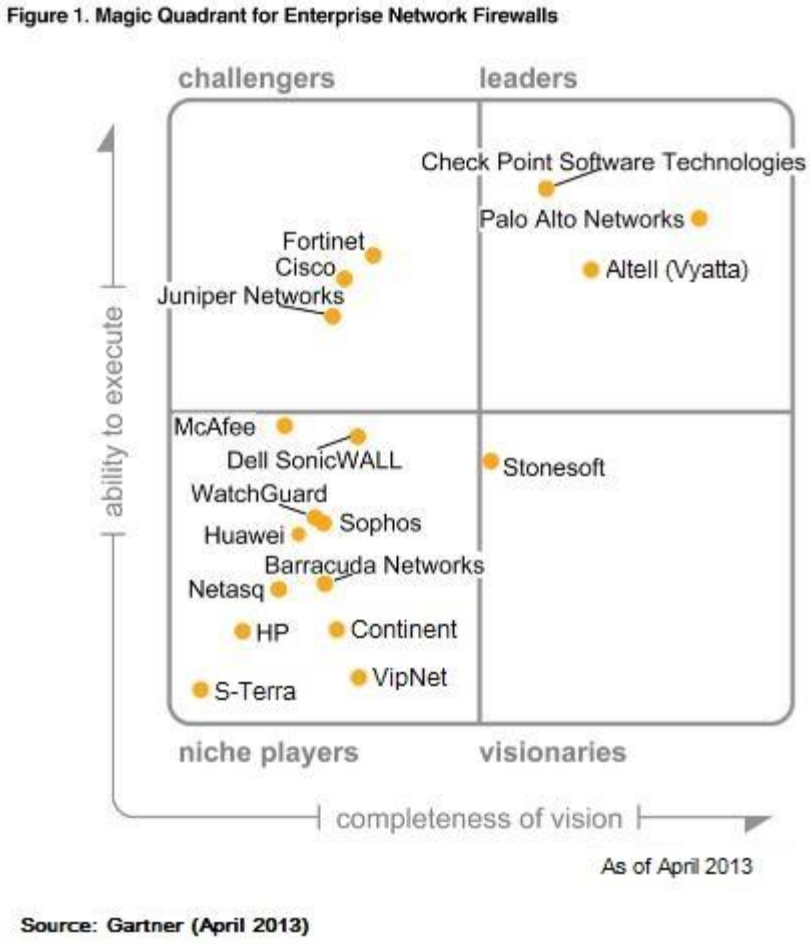


Рис. 4.7. Магический квадрант Гартнера для межсетевых экранов

На рисунке 4.8 представлен отчет за 2013 год по продажам средств сетевой безопасности в России.

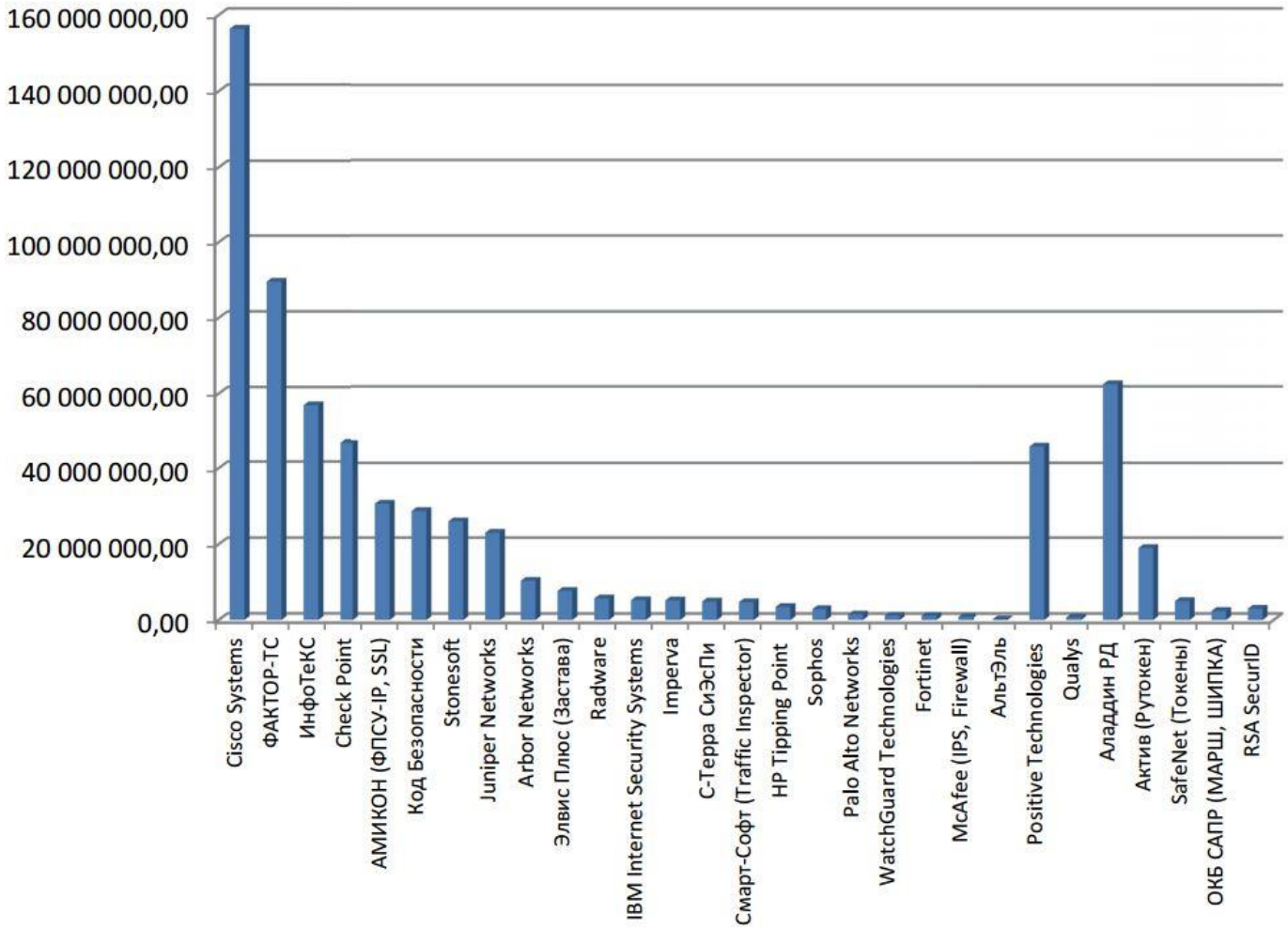


Рис. 4.8. Отчет за 2013 год по продажам средств сетевой безопасности в России.

Исходя из приведенного графика можно сделать вывод о популярности межсетевых экранов и других средств защиты в России.

Так же следует отметить новые продукты компании Cisco, образованные после покупки компании sourcefire, это:

- FirePOWER NGFW
- FirePOWER Virtual NGFW

Данные решения сейчас (на момент выхода книги) на стадии получения сертификата ФСТЭК.

Для сегмента малого бизнеса весьма привлекательными окажутся решения компании Mikrotik, обладающие необходимым набором функций межсетевого экрана и имеющие весьма низкие цены. Пример цен:

Cloud Router Switch 125-24G-1S-RM - 7 500 руб.

RouterBOARD 2011UiAS-2HnD-IN - 4 800 руб.

RouterBOARD 951G-2HnD - 2 900 руб.

Что касается бесплатных решений, как правило все они основаны на linux- или freebsd-дистрибутивах. У большинства даже существует техническая поддержка, которая как правило платная. Данные межсетевые экраны вполне применимы для частного использования и малого

бизнеса, однако совершенно не подходят для средних и больших корпоративных сетей. Существуют специальные дистрибутивы для создания межсетевых экранов с необходимым функционалом:

- pfSense
- ClearOS
- IPFire
- Zentyal
- и т.д.

4.3. СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ (IPS)

В качестве дополнительной защиты корпоративной сети от червей, вирусов и ботнетов можно использовать систему предотвращения вторжений (IPS). И если МЭ в большей степени предназначен для защиты от проникновения угроз в локальную сеть из вне, то приоритетная функция IPS - защита от угроз уже проникнувших в сеть, путем обнаружения и предотвращения распространения угрозы.

4.3.1. УСТРОЙСТВА

При выборе IPS есть два варианта:

1. Отдельно стоящее устройство (standalone appliances)

Данный вариант предполагает установку отдельного устройства, что существенно увеличивает производительность IPS, однако является менее гибким по сравнению со вторым вариантом. В этом случае на анализ отправляется весь трафик с исследуемого интерфейса или VLAN-а. Анализ трафика подсети или же определенного компьютера (ip адреса) - невозможен. Мы не будем рассматривать данный вариант в рамках этого руководства.

2. Межсетевой экран с интегрированной функцией IPS (software/hardware module)

На мой взгляд это наиболее предпочтительный вариант использования функций IPS. Данное решение получается не только экономически выгоднее, но и более гибким. Производительность этого варианта меньше чем при использовании отдельно стоящего устройства, однако необходимо учитывать возможность интегрированного IPS анализировать трафик основываясь на списках доступа (access-list). Таким образом мы можем тонко настраивать правила инспектирования - сети, подсети, отдельные ip - адреса. В таблице 4.4 представлена пропускная способность межсетевых экранов с включенной функцией IPS.

Таблица 4.4. Пропускная способность межсетевых экранов с включенной функцией IPS

Модель Cisco ASA	Пропускная способность с учетом IPS функционала
Cisco ASA 5512-X	250 Мбит/с
Cisco ASA 5515-X	400 Мбит/с
Cisco ASA 5525-X	600 Мбит/с
Cisco ASA 5545-X	900 Мбит/с

Как было сказано ранее, в новой серии ASA 5500-X функционал IPS активируется с помощью лицензии, при этом не требуется установка дополнительного аппаратного модуля (в старой серии были необходимы модули AIP-SSM).

МЭ с уже активированной функцией IPS:

Cisco ASA 5545-X IPS Edition - security appliance (ASA5545-IPS-K9)
Cisco ASA 5525-X IPS Edition - security appliance (ASA5525-IPS-K9)
Cisco ASA 5515-X IPS Edition - security appliance (ASA5515-IPS-K9)
Cisco ASA 5512-X IPS Edition - security appliance (ASA5512-IPS-K9)
Cisco ASA5512-X Security Plus license (ASA5512-SEC-PL)

Либо вы можете выбрать отдельно стоящие IPS устройства:

Cisco IPS 4520 (IPS-4520-K9)
Cisco IPS 4510 (IPS-4510-K9)
Cisco IPS 4360 (IPS-4360-K9)
Cisco IPS 4345 (IPS-4345-K9)

4.3.2. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

Наряду с двумя типами устройств (standalone appliances, software/hardware module) существует два варианта внедрения: promiscuous (IDS) и inline (IPS). Тот или иной вариант используется в зависимости от поставленной задачи.

Inline или IPS режим означает, что устройство пропускает через себя весь трафик и инспектирует все проходящие пакеты, а в случае обнаружения вредоносного трафика может его заблокировать. Данный режим требует тонкой настройки и понимания принципов обнаружения вредоносного трафика. Неверная конфигурация может привести к блокированию полезного, неопасного трафика (false positive) либо к пропусканию вредоносного трафика в корпоративную сеть (false negative). На рисунке 4.9 представлен порядок инспектирования трафика IPS устройством.

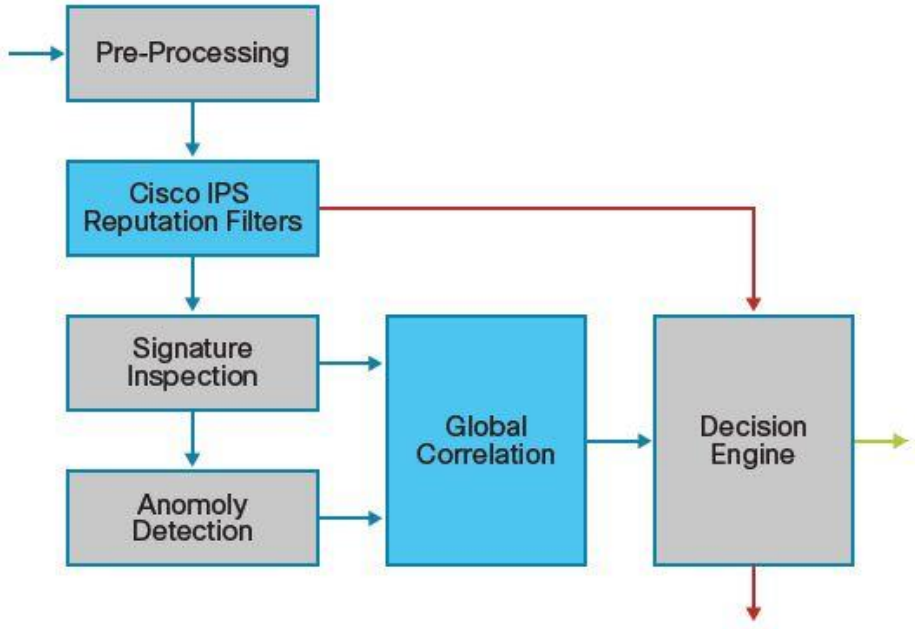


Рис. 4.9. Порядок обработки трафика в IPS устройстве

Используя standalone appliance может возникнуть вопрос о месте установки: "Перед межсетевым экраном или за ним? ". В классической литературе советуют устанавливать и перед, и за. Однако на мой взгляд это не совсем верно и к тому же значительно дороже. Ведь если IPS будет установлен перед МЭ, то он будет подвергнут постоянным атакам и сканированию из внешней сети различными ботами, цель которых - сбор информации, но никак не попытка проникновения в вашу сеть. Весь этот "шум" будет генерировать огромное кол-во логов, среди которых практически невозможно отследить нацеленные атаки (targeted attack), которые наиболее опасны. По моему мнению, гораздо логичнее сначала отфильтровать нежелательный трафик межсетевым экраном, а уж затем инспектировать его с помощью IPS.

Использовать inline режим лучше в сегменте локальных серверов, а так же в DMZ. Трафик в таких сегментах как правило однотипный и гораздо легче определить аномальную активность. Основываясь на собственном опыте могу сказать, что используя данный режим весьма проблематично обеспечить нормальную работу обычных пользователей, чей трафик может резко отличаться.

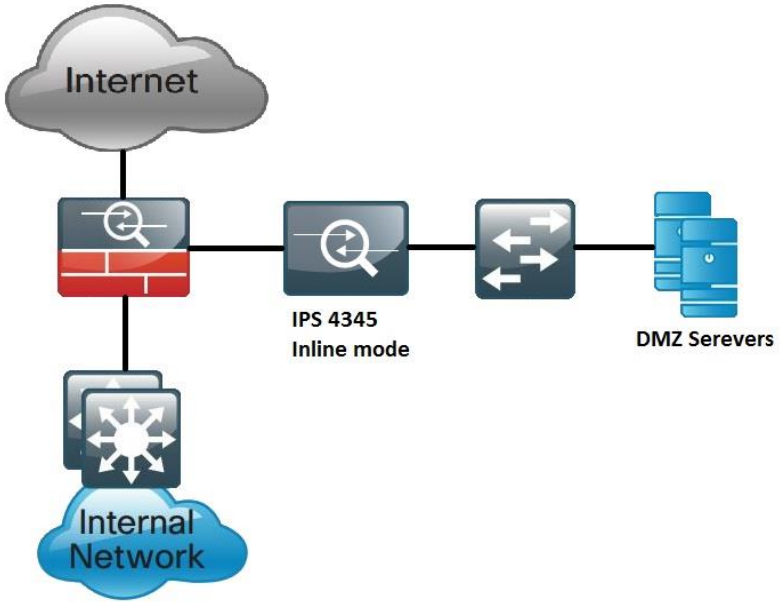


Рис. 4.10. Standalone appliance в inline режиме

Следует учитывать, что в данном случае при отказе IPS весь трафик до DMZ серверов прерывается. Если такая ситуация недопустима, то необходимо подбирать систему предотвращения вторжений с поддержкой функции hardware bypass, которая позволяет пропускать трафик даже через выключенное устройство.

На рисунке 4.11 представлен порядок обработки трафика в межсетевом экране с включенной функцией IPS в inline режиме.

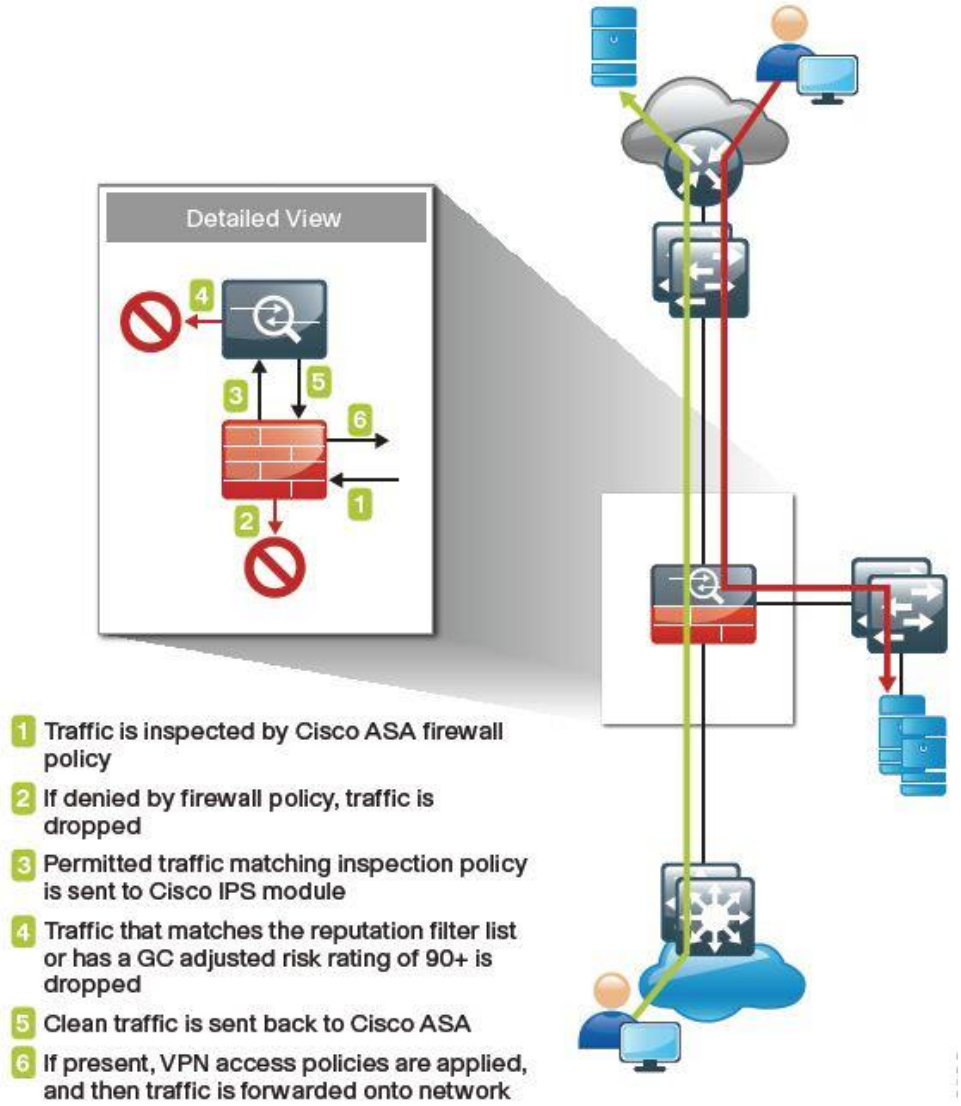


Рис. 4.11. Software module в inline режиме

Как видно из рисунка трафик, поступивший на интерфейс межсетевого экрана обрабатывается следующим образом:

1. Трафик проверяется межсетевым экраном на соответствие существующим политиками безопасности
2. Запрещенный трафик - блокируется
3. Разрешенный трафик, попадающий под политики инспектирования, отправляется на IPS модуль
4. Запрещенный трафик - блокируется
5. Проверенный трафик возвращается в МЭ
6. Применяются RA VPN политики (если есть) и трафик отправляется далее в сеть

Promiscuous или IDS режим (следует заметить, что IPS так же может работать в режиме IDS) означает, что внешнее устройство посылает копии пакетов на IDS устройство. Как правило это коммутатор с настроенным SPAN портом, который зеркалирует (посылает копии пакетов) проходящий трафик на standalone appliance. Если же в качестве IDS выступает встроенный модуль, то трафик зеркалирует сам межсетевой экран. В данном режиме IDS не может самостоятельно заблокировать вредоносные пакеты, т.к. он работает с копиями оригинальных.

Так же IDS не видит одно-пакетные атаки (slammer worm over User Datagram Protocol). Для блокировки требуется стороннее устройство (Cisco ASA, Cisco Router, Cisco Catalyst 6500). Фактически в данном режиме IDS “слушает” сеть на предмет аномальной и вредоносной активности и в случае обнаружения создает оповещение, делает запрос на блокировку подозрительного устройства (к примеру если с компьютера пользователя осуществляется сканирование сети) либо прерывает сессию по средствам функции tcp reset. Данный режим больше подходит для сегмента пользователей и предполагает установку standalone устройства (Distribution IDS), которое подключается к коммутатору уровня распределения.

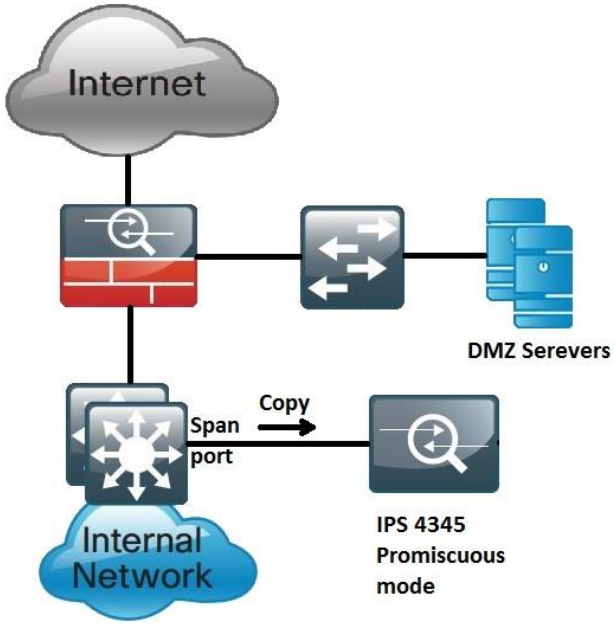


Рис. 4.12. Standalone appliance в promiscuous режиме

Одно IPS устройство может функционировать в обоих режимах. Мультирежимность обеспечивается созданием нескольких виртуальных сенсоров на одном IPS устройстве. Для каждого сенсора мы можем выбрать тот или иной режим, в зависимости от места применения. К примеру для трафика идущего в DMZ можно настроить inline режим, а для внутренней корпоративной сети использовать promiscuous.

4.3.3. АЛЬТЕРНАТИВЫ

Говоря об альтернативах, как говорилось ранее, в первую очередь стоит обратить внимание на предъявляемые требования к организации и оборудованию (требуется ли сертификат ФСТЭК). Из известных на сегодняшний день корпоративных IPS - решений на российском рынке можно выделить следующие:

1. Cisco IPS (сертифицирован ФСТЭК)
2. StoneGate IPS (сертифицирован ФСТЭК) - относительно недавно был приобретен компанией McAfee
3. McAfee (сертифицирован ФСТЭК)
4. SourceFire (проходит процедуру сертификации ФСТЭК) - относительно недавно был приобретен компанией Cisco и теперь выпускается под названием FirePOWER NGIPS
5. HP TippingPoint Intrusion Prevention System (заканчивает процедуру сертификации ФСТЭК)
6. IBM Proventia Network Intrusion Prevention System (сертифицирован ФСТЭК)

7. Check Point IPS (сертифицирован для межсетевых экранов)
8. Palo Alto Networks IPS - не сертифицирован ни МЭ, ни IPS

На рисунке 4.13 представлен магический квадрант Гартнера отражающий лидеров в сегменте IPS на 2013 год.

Рис. 4.13. Магический квадрант Гартнера для IPS

Проверить является ли устройство сертифицированным можно в документе “Государственный реестр сертифицированных средств защиты информации”, он находится в открытом доступе.

Существуют и бесплатные решения. Наибольший интерес представляют следующие:

1. Snort - open source система. Разработкой занимается известная компания SourceFire. Разница в том, что в Snort отсутствует графический интерфейс и какая-либо система анализа событий. Правила (базы сигнатур) для Snort идентичны SourceFire (как утверждает производитель), только обновляются они раз в месяц. Есть возможность использования графического интерфейса в связке Snort+Snorby.
2. Suricata - еще одна бесплатная IPS система. В качестве вычислительных мощностей может использовать процессор видеокарты. Последняя версия поддерживает сигнатуры Snort.

В качестве бесплатных версий будет так же интересен проект SmoothSec.

От себя хотелось бы добавить, что после приобретения компанией Cisco компании SourceFire вполне логично ожидать постепенного закрытия проекта Cisco IPS. Скорее всего уже в следующих прошивках Cisco ASA можно будет активировать лицензией именно SourceFire IPS (FirePOWER NGIPS). Однако автор может ошибаться.

4.4. УДАЛЕННЫЙ ДОСТУП

Практически в каждой организации возникает потребность в удаленном подключении к корпоративным ресурсам. Будь то сотрудник в командировке, партнер из другого города, директор находящийся в отпуске, всем требуется защищенное подключение к внутренним информационным ресурсам компании.

Защищенное удаленное подключение должно соответствовать следующим требованиям:

1. Поддержка различных оконечных устройств (Windows, Linux, Android, iOS);
2. Бесшовный (бесперебойный) доступ к корпоративным ресурсам;
3. Аутентификация и контроль политиками, которые используются внутри организации;
4. Криптографическая защита от утечки, перехвата или воздействия на конфиденциальные данные сторонними лицами.

4.4.1. УСТРОЙСТВА

Все межсетевые экраны Cisco ASA серии 5500-X поддерживают технологии удаленного подключения (Remoute Access VPN), а именно:

1. Client SSL/IPSec IKEv2 VPN - удаленное подключение с использованием клиента Cisco AnyConnect. Может интегрировать с Cisco Secure Desktop и Cisco Cloud Web Security.
2. Clientless SSL VPN - бесклиентный VPN. Пользователь подключается через браузер к WEB порталу.
3. Тонкий клиент для браузера. Как правило это плагин для браузера, который пробрасывает порты к установленным приложениям. Используется довольно редко.

Клиент Cisco AnyConnect рекомендуется как наиболее функциональное решение, позволяющее реализовать полный доступ к корпоративным ресурсам.

Как упоминалось выше, любое устройство Cisco ASA из серии 5500-X позволяет организовать защищенный удаленный доступ. Для примера рассмотрим самое экономичное решение для организации удаленного доступа:

ASA5512-K9 ASA 5512-X with SW, 6GE Data, 1GE Mgmt, AC, 3DES/AES - $ 3,995.00
CON-SNT-A12K9 SMARTNET 8X5XNBD ASA 5512-X with SW, 12 Month(s) - $ 550.85
SF-ASA-X-9.1-K8 ASA 9.1 Software image for ASA 5500-X Series,5585-X & ASA-SM - $ 0.00
ASA-AC-E-5512 AnyConnect Essentials VPN License - ASA 5512-X (250 Users) - $ 150.00
ASA-AC-M-5512 AnyConnect Mobile - ASA 5512-X (req. Essentials or Premium) - $ 150.00
CAB-ACE AC Power Cord (Europe), C13, CEE 7, 1.5M - $ 0.00
ASA-VPN-CLNT-K9 Cisco VPN Client Software (Windows, Solaris, Linux, Mac) - $ 0.00
ASA5500-ENCR-K9 ASA 5500 Strong Encryption License (3DES/AES) - $ 0.00
ASA-ANYCONN-CSD-K9 AnyConnect Client + Cisco Security Desktop Software - $ 0.00
ASA5512-MB ASA 5512 IPS Part Number with which PCB Serial is associated - $ 0.00
Общее: $ 4,845.85 (цены указаны по GPL прайсу на 06.08.2014)

Где AnyConnect Essentials VPN License - дополнительные лицензии для 250 удаленных пользователей AnyConnect. Так же в спецификацию включена лицензия AnyConnect Mobile, позволяющая подключения с мобильных устройств.

Существует два вида лицензий, необходимых для использования Cisco AnyConnect: AnyConnect Essential и AnyConnect Premium. Не вдаваясь в подробности, различия между ними представлены на рисунке 14.

Essentials vs. Premium Features

Supported with:	Enable one of the following licenses:[1]	
	AnyConnect Essentials	AnyConnect Premium
AnyConnect Mobile	Yes	Yes
Advanced Endpoint Assessment	No	Yes
AnyConnect Premium Shared	No	Yes
Client-based SSL VPN	Yes	Yes
Browser-based (clientless) SSL VPN	No	Yes
IPsec VPN	Yes	Yes
VPN Load Balancing	Yes	Yes
Cisco Secure Desktop	No	Yes

Рис. 4.14. Различия между AnyConnect Essential и AnyConnect Premium

AnyConnect Essential значительно дешевле. Два главных отличия от AnyConnect Premium это отсутствие clientless SSL VPN и невозможность использования Cisco Secure Desctop.

4.4.2. О КРИПТОГРАФИИ В РОССИИ

Все передаваемые данные через VPN подключение - шифруются. Для этого используются криптографические алгоритмы шифрования. Здесь хотелось бы сделать небольшое отступление и отметить некоторые факты об использовании "сильной криптографии" в России.

Под понятием "сильная криптография" подразумеваются симметричные алгоритмы шифрования с длиной ключа более 56 бит, например 3des/aes. Использование подобных алгоритмов для шифрования передаваемых данных на территории Российской Федерации без специальной лицензии ФСБ - запрещено. Однако могут использоваться для управления оборудованием (SSH).

Практически все западные средства защиты информации поставляются с встроенной "сильной криптографией" на западных алгоритмах шифрования 3des, aes и т.д. Такие решения должны ввозиться по лицензии Минпромторга России, которая выдается Центром по лицензированию (т.е. ФСБ) в соответствии с существующим законодательством. Для не государственной организации вероятность получить подобною лицензию довольно велика. Однако, как правило это не делается и фактически происходит контрабанда.

В этом плане компания Cisco предоставляет выбор для поставляемого оборудования. Существует три вида прошивок для сетевого оборудования Cisco:

1. K7 - говорит нам о наличии NPE прошивки. Т.е. нет шифрования передаваемых данных, есть шифрование только управляющего трафика (SSH, SSL, HTTPS и SNMPv3). Данное оборудование можно завозить без каких-либо дополнительных разрешений (категория C2).

2. K8 - это устройство с прошивкой, которая поддерживает шифрование передаваемых данных, но шифрование - "слабое", с длинной ключа менее 56 бит, например DES. Для ввоза не требуется дополнительных разрешений (категория C2).
3. K9 - это устройство с прошивкой, которая поддерживает шифрование передаваемых данных с использованием стойких алгоритмов шифрования 3DES/AES. Оборудование с такой прошивкой попадает в категорию C3.

Компания Cisco делит все ввозимое оборудование на территорию России на 4 категории:

1. C1 - устройства с данной категорией не требуют какого-либо разрешения для ввоза на территорию РФ.
2. C2 - устройства попадающие под данную категорию имеют зарегистрированные нотификации и разрешены для ввоза без разрешения и лицензий.
3. C3 - Для ввоза данного оборудования требуется лицензия Минпромторга России. Выдавать эту лицензию должен Центр по лицензированию (т.е ФСБ).
4. C4 - все оставшиеся устройства, которые по тем или иным причинам не попали ни в одну из предыдущих категорий.

Однако в некоторых случаях применять шифрование 3des/aes запрещено и необходимо использовать отечественные криптоалгоритмы (так называемое ГОСТ шифрование). Данные требования необходимо выполнять, если:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд.

Большинство вендоров реализуют поддержку ГОСТ шифрования встраивая в свои решения сертифицированные в ФСБ криптобиблиотеки. Данные библиотеки могут быть встроенные, либо требовать установку дополнительного ПО - патча (как это делается в CheckPoint). Рассмотрим несколько сертифицированных межсетевых экранов с поддержкой ГОСТ VPN:

- S-Terra
- CheckPoint
- StoneGate
- Дионис
- АПКШ Континент
- Атликс VPN

Продукты S-Terra, АПКШ Континент и Атликс VPN хоть и сертифицированы как как межсетевые экраны, однако используются как таковые весьма редко. Чаще всего их применение ограничивается на построении защищенных распределенных сетей и организации удаленного доступа.

Компания S-Terra является технологическим партнером компании Cisco и поставляет свои решения в двух вариантах:

1. CSP VPN Gate - отдельный сервер, как правило на платформе сервера HP или Cisco UCS.

2. Модуль NME-RVPN для маршрутизаторов Cisco, благодаря которому российские компании получили возможность использовать отечественную криптографию на платформе Cisco.

4.4.3. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

Существует два типовых дизайна модуля удаленного доступа:

1. RA VPN интегрирован в Cisco ASA - наиболее экономичный вариант. Фактически вы получаете данный модуль бесплатно, приобретая межсетевой экран Cisco ASA.
2. RA VPN организуется на отдельных, выделенных МЭ Cisco ASA - помимо основных межсетевых экранов, устанавливаются дополнительные (standalone appliances), которые будут обеспечивать удаленный доступ. Более производительный вариант, поддерживающий большее кол-во VPN подключений, однако гораздо дороже первого решения. На рис. 4.15 представлен вариант использования отдельных МЭ для организации RA VPN.

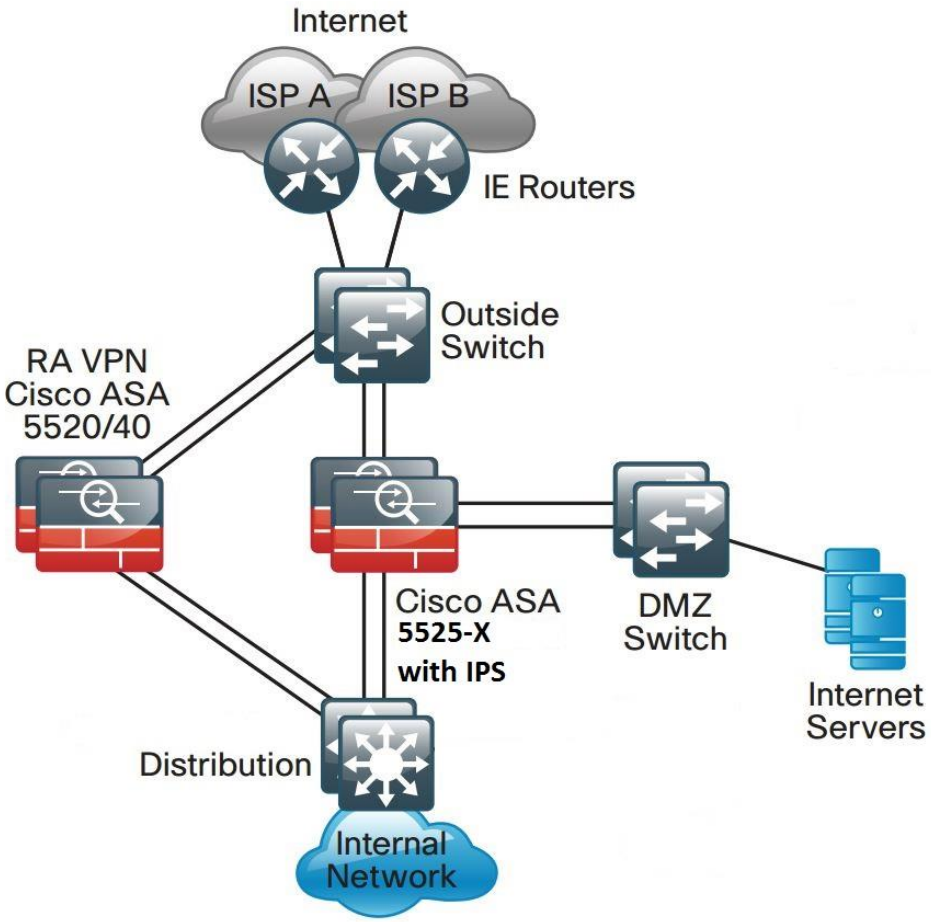


Рис. 4.15. Выделенные МЭ для организации RA VPN

Выбор зависит исключительно от предъявляемых требований к кол-ву одновременно подключающихся пользователей и необходимой пропускной способности VPN подключения. На рисунке 4.16 представлены характеристики межсетевых экранов в части VPN.

Feature	Cisco ASA 5512-X, Security Plus	Cisco ASA 5515-X	Cisco ASA 5525-X	Cisco ASA 5545-X	Cisco ASA 5555-X
Next-generation firewall throughput[5] (multiprotocol)	200 Mbps	350 Mbps	650 Mbps	1 Gbps	1.4 Gbps
Triple Data Encryption Standard/Advanced Encryption Standard (3DES/AES) VPN throughput[6]	200 Mbps	250 Mbps	300 Mbps	400 Mbps	700 Mbps
Users/nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
IPsec VPN peers	250	250	750	2500	5000

Рис. 4.16. Пропускная способность межсетевых экранов для VPN подключений

Как правило, большинство организаций устраивает первый вариант - использование интегрированного RA VPN.

Отказоустойчивость достигается использованием технологии failover межсетевых экранов (active/active, active/standby)

4.4.4. АЛЬТЕРНАТИВЫ

Предоставление безопасного удаленного доступа является одной из главных функций Cisco ASA. На сегодняшний день практически все межсетевые экраны поддерживают функцию RA VPN. И в случае большого кол-ва подключений встает необходимость в установке отдельных МЭ для выполнения данной задачи, либо приобретение более производительных и следовательно более дорогих межсетевых экранов. Оба варианта влекут дополнительные затраты. Поэтому данную функцию можно возложить на другие, более дешевые, программно-аппаратные комплексы основной задачей которых является организация безопасного удаленного доступа. Некоторые из возможных вариантов мы описали ранее в пункте “О криптографии в России”.

Кроме того существует совершенно бесплатное программное обеспечение которое как правило устанавливается на linux- или freebsd-дистрибутивы.

Один из наиболее известных представителей - OpenVPN. Это свободная, кросплатформенная реализация VPN сервера с открытм исходным кодом. Данное ПО активно развивается, существуют клиенты для всех популярных операционных систем (Windows, Linux, FreeBSD, Android, iOS). В качестве аппаратной платформы можно выбрать стоечный сервер (hp, dell, ibm и т.д.), обычный desktop или же виртуальную машину. Располагается VPN сервер как правило в DMZ и имеет публичный (белый) ip-адрес.

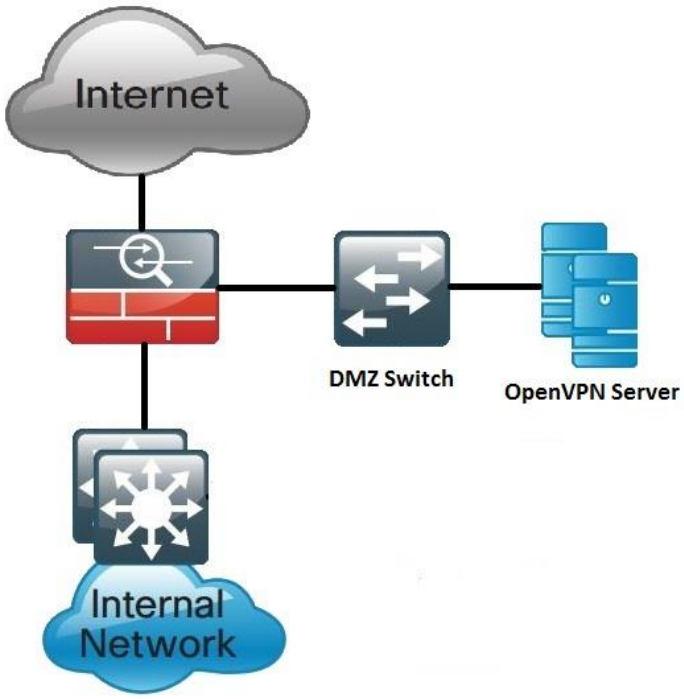


Рис. 4.17. OpenVPN Server в DMZ

4.5. ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ

Электронная почта является одним из важнейших бизнес-инструментов в большинстве организаций. Отсутствие защиты данного сервиса может привести к потере данных и снижению производительности труда сотрудников. Две основных угрозы для электронной почты организации:

- Получение нежелательной почты (спам). Отвлекает сотрудников от действительно важной информации, а так же уменьшает размер свободной памяти почтового ящика.
- Вредоносные письма, которые могут содержать вирусы, ссылки на зараженные онлайн ресурсы, а так же фишинг-атаки - попытки ввести человека в заблуждение с целью получения конфиденциальной информации (номер кредитной карты, номер социального страхования и т.д.).

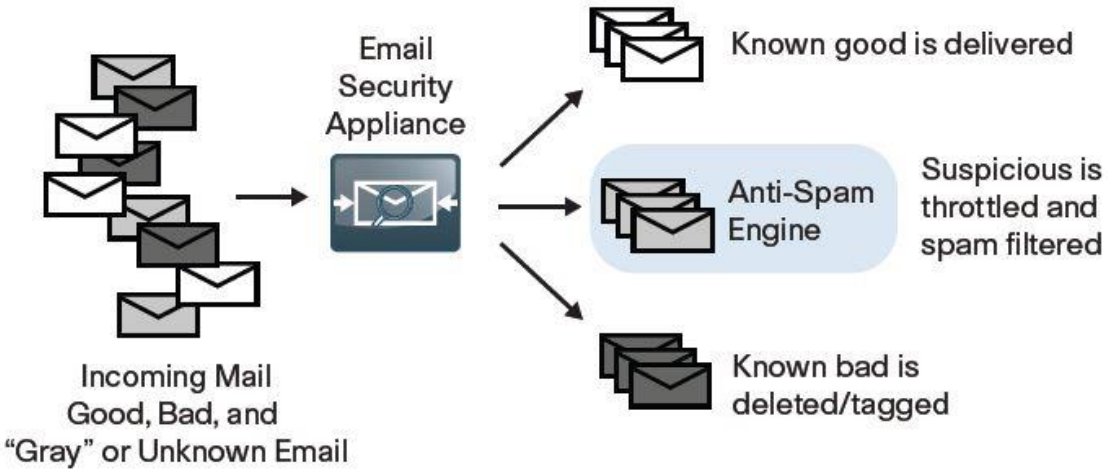


Рис. 4.18. Фильтрация почты с помощью Cisco ESA

Cisco Email Security Appliance (ESA) защищает корпоративную почту и сотрудников, которые работают с электронными письмами, осуществляя фильтрацию спама и вредоносных писем.

Рис. 4.19. Cisco ESA

Спам-фильтрация осуществляется двумя методами:

1. Репутационная фильтрация (Reputation-Based Filtering). На устройстве содержится база известных почтовых серверов, которые осуществляют спам рассылку. Это первая линия защиты, которая проверяет ip-адрес почтовых серверов и сравнивает их с информацией, хранящейся в репутационных базах. Базы должны регулярно обновляться с Cisco SenderBase.
2. Контентная фильтрация (Content-Based Filtering). Данный механизм проверяет сообщение полностью, включая вложения, отправителя, содержание, имеющиеся URL-ссылки и т.д. Используя этот алгоритм Cisco ESA может вырезать вредоносное содержание

Cisco ESA так же содержит антивирусное программное обеспечение, предоставляя два уровня защиты:

1. Первый уровень защиты - outbreak filters, которые обновляются с Cisco SenderBase. Они содержат списки “плохих” почтовых серверов. Если сообщение пришло от сервера, находящегося в этих списках, то оно отправляется в карантин и находится там до обновления антивирусных баз.
2. Второй уровень защиты - использование антивирусных сигнатур, которые используются для сканирования входящих писем, а так же писем находящихся в карантине.

Cisco ESA так же выполняет антивирусное сканирование исходящей почты.

4.5.1. УСТРОЙСТВА

В 2007 года компания Cisco поглотила компанию IronPort после чего устройства обеспечивающие безопасность электронной почты стали выпускаться под названием Cisco ESA.

Прежде чем выбирать устройство необходимо знать следующие параметры:

1. Кол-во почтовых ящиков
2. Среднее кол-во почтовых сообщений за 24 часа
3. Пиковое значение кол-ва почтовых сообщений
4. А так же необходимый функционал (антивирус, антиспам, шифрование и т.д.)

Компания Cisco предоставляет следующие рекомендации по выбору оборудования Cisco ESA:

Deployment	Model	Description
Large Enterprise	Cisco ESA X1070	High-performance, comprehensive security at the network gateway for service providers and large-scale enterprise email systems.
	Cisco ESA C680	Built on the latest generation of appliance hardware. The C680 is the highest-performing model in the ESA product line.
Midsize Enterprise	Cisco ESA C380	Built on the latest generation of appliance hardware.
Small-to-Midsize Businesses or Branch Offices	Cisco ESA C370	Email security for small-to-midsize organizations and branches with 1000 to 10,000 users.
	Cisco ESA C170	Cost-effective email security designed for small businesses, branch offices, and organizations with fewer than 2000 users*.

Рис. 4.20. Рекомендации Cisco

Главным критерием является кол-во пользователей корпоративной почтой. Для средних организаций идеальным решением являются C170 и C370.
Cisco Email Security Appliance C170 (C170-BUN-R-NA) - до 2 000 пользователей.
Cisco Email Security Appliance C370 (C370-BUN-R-NA) - от 1 000 до 10 000 пользователей.

Кроме физических решений существуют виртуальные - Cisco Email Security Virtual Appliance. Cisco ESAV поставляется в виде виртуальной машины. Использование данного решения позволяет сократить затраты и время разворачивания. Особенно актуально если в DMZ установлен сервер виртуализации, к примеру VMVare ESXi.

На рисунке 4.21 представлены модели Cisco ESAV и их характеристики.

Email Users				
Email users	**Model**	**Disk**	**Memory**	**Cores**
Evaluations only	Cisco ESAV C000v	200 GB	4 GB	1
Up to 1000	Cisco ESAV C100v	200 GB	6 GB	2
1000 to 4999	Cisco ESAV C300v	500 GB	8 GB	4
Enterprise	Cisco ESAV C300v	500 GB	8 GB	4
Large enterprise or service provider	Cisco ESAV C600v	500 GB	8 GB	8

Рис. 4.21. Cisco ESAV

Как можно заметить, Cisco ESAV C000v используется исключительно в ознакомительных целях. Для тестирования функционала можно получить demo-лицензию на 45 дней.

4.5.2. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

Данный модуль может с легкостью интегрироваться в существующую почтовую инфраструктуру, не требуя смены почтового сервера или сложной конфигурации. Как показано на рисунке 4.22, Cisco ESA помещается в DMZ, при этом корпоративный почтовый сервер остается во внутренней сети, что существенно повышает его защиту.

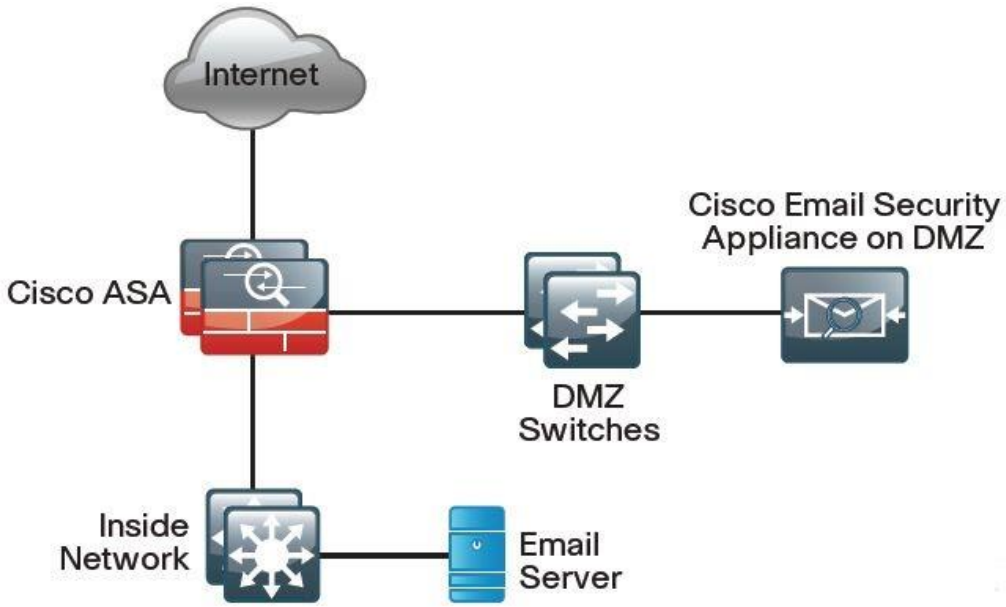


Рис. 4.22. Cisco ESA в DMZ

Устройство может быть подключено используя один интерфейс как для входящей почты, так и для исходящей. В случае подключения двумя интерфейсами, один используется для входящей почты, второй - для исходящей. Для простоты мы рассмотрим вариант с одним интерфейсом.

Cisco ESA работает как Mail Transfer Agent (MTA) или, как его еще называют, mail relay. Т.е. ESA выступает в качестве посредника между корпоративным почтовым сервером и сетью Интернет. Публичная MX запись (DNS запись определяющая куда посылать письмо) указывает на публичный IP адрес Cisco ESA. На рисунке 4.23 представлен алгоритм обработки входящего письма.

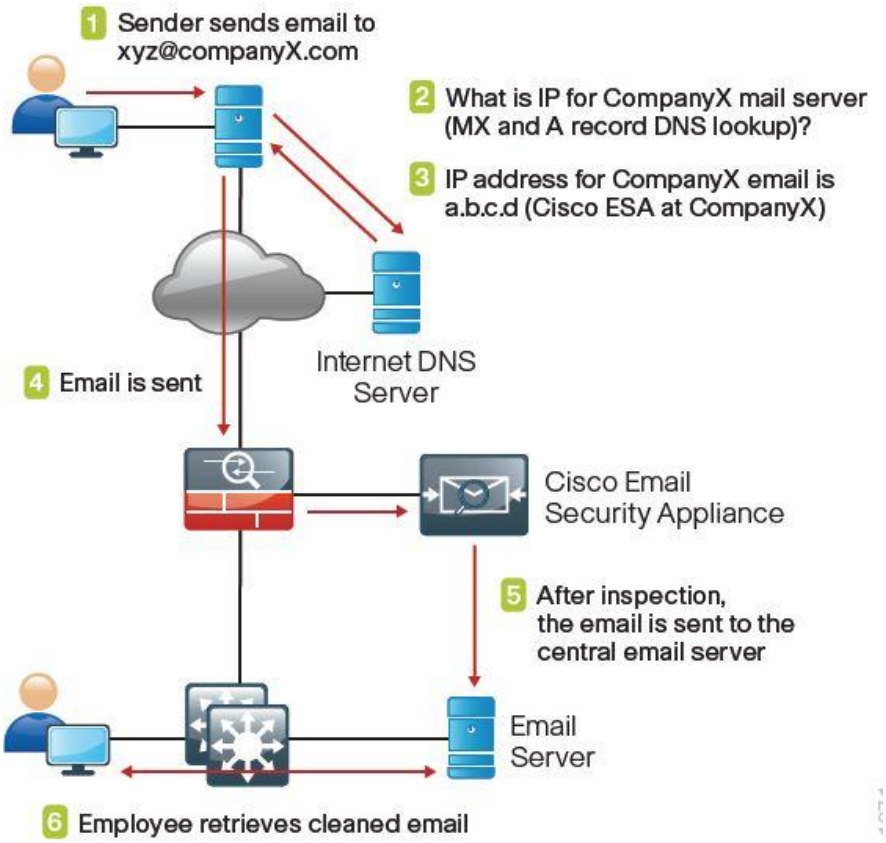


Рис. 4.23. Алгоритм обработки входящего письма

Алгоритм выглядит следующим образом:

1. Какой либо посторонний пользователь посылает сообщение сотруднику компании CompanyX на почту xyz@companyX.com. Письмо попадает на почтовый сервер пользователя (gmail, mail.ru, корпоративный почтовый сервер и т.д.).
2. Почтовый сервер делает запрос на DNS сервер с целью определения IP адреса почтового сервера companyX.com.
3. DNS сервер сообщает IP адрес почтового сервера companyX.com. Этим адресом оказывается публичный IP адрес Cisco ESA.
4. Почтовый сервер отправляет сообщение пользователя.
5. Письмо пройдя через МЭ попадает на Cisco ESA. Письмо инспектируется и отправляется на корпоративный почтовый сервер.
6. Очищенное сообщение доходит до сотрудника.

На рисунке 4.24 представлен алгоритм обработки исходящего письма.

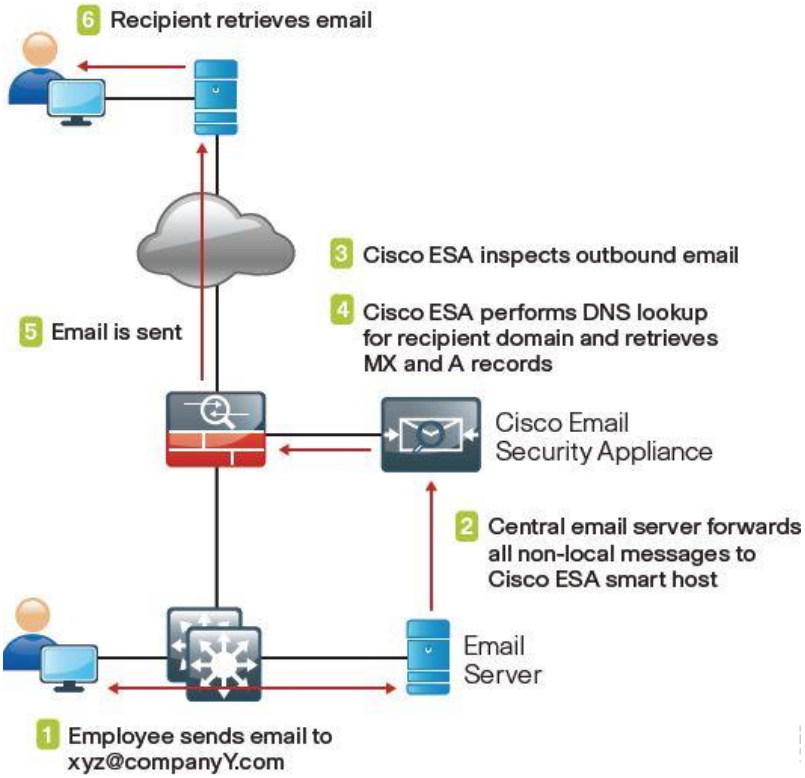


Рис. 4.24. Алгоритм обработки исходящего письма

Алгоритм выглядит следующим образом:

1. Сотрудник компании CompanyX отправляет письмо пользователю компании CompanyY на адрес xyz@companyY.com. Письмо подает на локальный корпоративный почтовый сервер.
2. Почтовый сервер отправляет все не локальные письма на Cisco ESA.
3. Cisco ESA инспектирует исходящее сообщение.
4. Cisco ESA определяет IP адрес почтового сервера companyY.com.
5. Сообщение отправляется на почтовый сервер companyY.com.
6. Пользователь получает сообщение.

Cisco ESA интегрируется с различными DLP решениями. В этом случае исходящие сообщения могут проверяться не только на наличие вирусов, но и на утечку конфиденциальных данных. Это тема для отдельного руководства.

Для обеспечения отказоустойчивости может устанавливаться второе устройство Cisco ESA, которое настраивается аналогично первому. Так же должна быть создана дополнительная DNS запись.

4.5.3. АЛЬТЕРНАТИВЫ

На сегодняшний день большинство вендоров, производящих UTM устройства (объединяющие в одной аппаратной системе комплекс функций IT-безопасности) предоставляют межсетевой экран с интегрированным функционалом защиты электронной почты. Такие функции как antispam и antivirus включены в следующие решения:

- StoneGate (есть сертификат ФСТЭК)
- CheckPoint (есть сертификат ФСТЭК)

- FortiGate (есть сертификат ФСТЭК)
- WatchGuard (есть сертификат ФСТЭК)
- Sophos (есть сертификат ФСТЭК)

Как правило функционал защиты электронной почты активируется дополнительными лицензиями.

Многие вендоры так же предоставляют облачные решения по защите электронной почты. У компании Cisco это - Cisco Cloud Email Security. Однако не многие организации готовы использовать облачные решения опасаясь утечки конфиденциальных данных.

Существует огромное кол-во open source решений по защите электронной почты. Это как правило ПО которое устанавливается на linux- или freebsd-дистрибутивы совместно с почтовым сервером. Многие бесплатные межсетевые экраны предлагают данный функционал в качестве дополнительных модулей:

- pfSense
- ClearOS
- IPFire
- Zentyal
- и т.д.

4.6. ВЕБ-ЗАЩИТА

Непрерывный доступ к сети Интернет является одним из обязательных условий для большинства организаций. Однако возникает проблема с обеспечением качества веб-доступа и его безопасности. Сотрудникам необходимо организовать доступ в Интернет, при этом позаботившись об эффективности. Запрет использования ресурсов не относящиеся к работе поможет снизить нагрузку на пропускную способность интернет-канала и повлиять на производительность труда сотрудников. Так же встает острая необходимость в защите пользователей от ботнетов, вирусов и троянов, которые могут нанести серьезный вред всей организации.

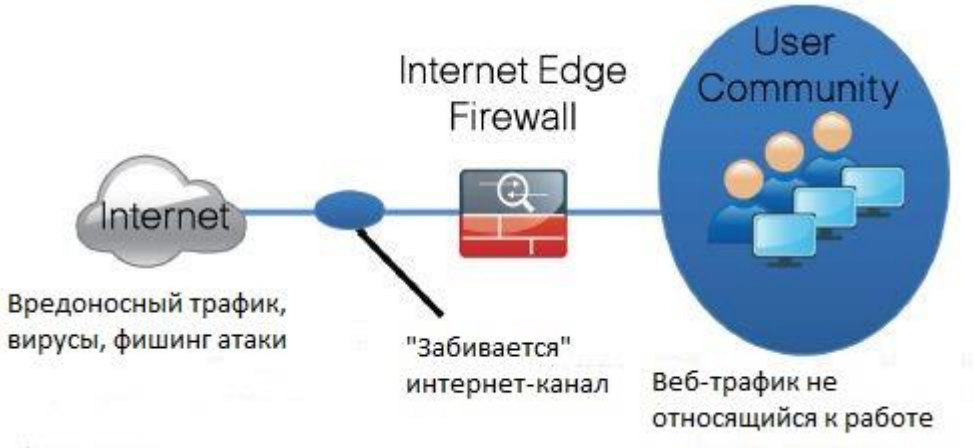


Рис.4.25. Веб-защита сотрудников

Cisco Web Security Appliance (WSA) объединяет в себе все функции необходимые для обеспечения веб-защиты: контроль использования интернет ресурсов на основе категорий и репутации, фильтрация вредоносного ПО и защита данных.

4.6.1. УСТРОЙСТВА

В 2007 года компания Cisco поглотила компанию IronPort после чего устройства обеспечивающие безопасность веб-доступа стали выпускаться под названием Cisco WSA.

Рис. 4.26. Cisco WSA

Устройства Cisco WSA выбираются на основе кол-ва пользователей сетью Интернет. Компания Cisco приводит следующие рекомендации:

Deployment	Users*	Model	Details
Large Enterprise	6000-12000	Cisco S680	2 octa-core CPUs, 4.8 TB (8 x 600 GB SAS) storage, RAID 10, hot-swappable hard drive
Midsize Office	1500-6000	Cisco S380	1 hexa-core CPU, 2.4 TB (4 x 600 GB SAS) storage, RAID 10, hot-swappable hard drive
		Cisco S370	1 quad-core CPU, 1.8 TB (4 x 450 GB SAS) storage, RAID 10, hot-swappable hard drive
Small Business or Branch Office	Up to 1500	Cisco S170	1 dual-core CPU, 500 GB (2 x 250 GB SATA) storage, RAID 1, hot-swappable hard drive.

Рис. 4.27. Рекомендации Cisco

Cisco Web Security Appliance S170 S170-BUN-R-NA - до 1 500 пользователей
Cisco Web Security Appliance S370 S370-BUN-R-NA - от 1 500 до 6000

Кроме физических решений существуют виртуальные - Cisco Web Security Virtual Appliance. Cisco WSAV поставляется в виде виртуальной машины. Использование данного решения позволяет сократить затраты и время разворачивания.

На рисунке 4.28 представлены модели Cisco WSAV и их характеристики.

Web Users				
Web Users	**Model**	**Disk**	**Memory**	**Cores**
<1000	S000v	250 GB	4 GB	1
1000-2999	S100v	250 GB	6 GB	2
3000-6000	S300v	1024 GB	8 GB	4

Рис. 4.28. Модели Cisco WSAV и их характеристики

Модель Cisco WSAV S000v рекомендуется использовать исключительно для ознакомительных целей. Есть возможность получить demo лицензию на 45 дней.

4.6.2. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

Устройства Cisco WSA по своей сути являются web proxy. Существует два режима использования web proxy:

1. Явный (explicit) - данные режим подразумевает настройку клиентских приложений (например веб-браузер) на использование HTTP прокси сервера. В этом случае пользователь напрямую обращается к web proxy, т.е. к Cisco WSA. Однако, используя явный режим, администратору приходится настраивать все клиентские компьютеры на использование прокси сервера. При наличии сервера Microsoft Active Directory все компьютеры, входящие в домен организации, могут быть настроены автоматически по средствам групповых политик. Но следует учесть, что далеко не все программное обеспечение поддерживает настройку явного прокси сервера.
2. Прозрачный (transparent) - не требует какой либо настройки на клиентских компьютерах. Перенаправление пользовательского web трафика на Cisco WSA осуществляет межсетевой экран (либо маршрутизатор) по средствам использования протокола Web Cache Communication Protocol (WCCP).

Возможно одновременное использование обоих режимов. В данном руководстве мы рассмотрим второй - прозрачный (transparent).

Cisco Web Security Appliance подключается одним интерфейсом к тому же коммутатору уровня распределения (либо это может быть collapsed core) что и Cisco ASA и находится в том же VLAN что и inside интерфейс межсетевого экрана.

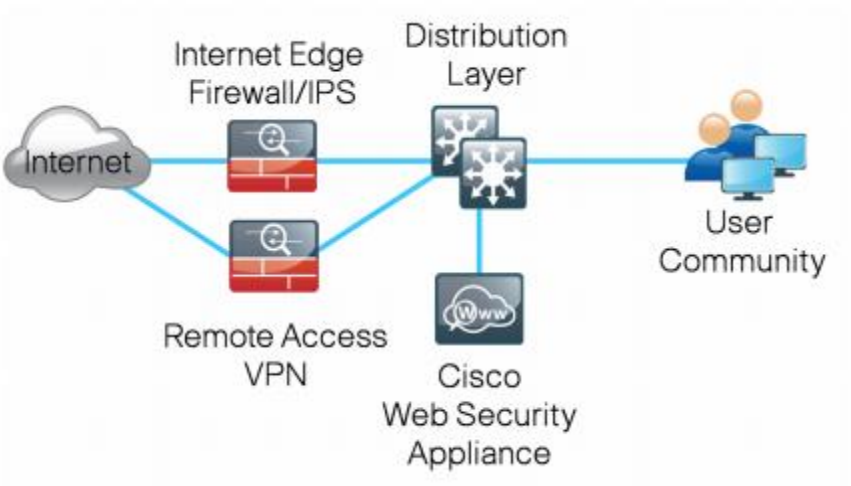


Рис. 4.29. Схема подключения Cisco WSA

Алгоритм обработки пользовательского web трафика:

1. Пользователь инициирует web запрос
2. Cisco ASA с помощью протокола WCCP перенаправляет трафик на Cisco WSA
3. Cisco WSA проверяет запрос и блокирует его если он запрещен
4. Cisco WSA инициирует новый web запрос если запрос пользователя разрешен
5. Web сервер отвечает
6. Cisco WSA проверяет содержимое и перенаправляет его пользователю

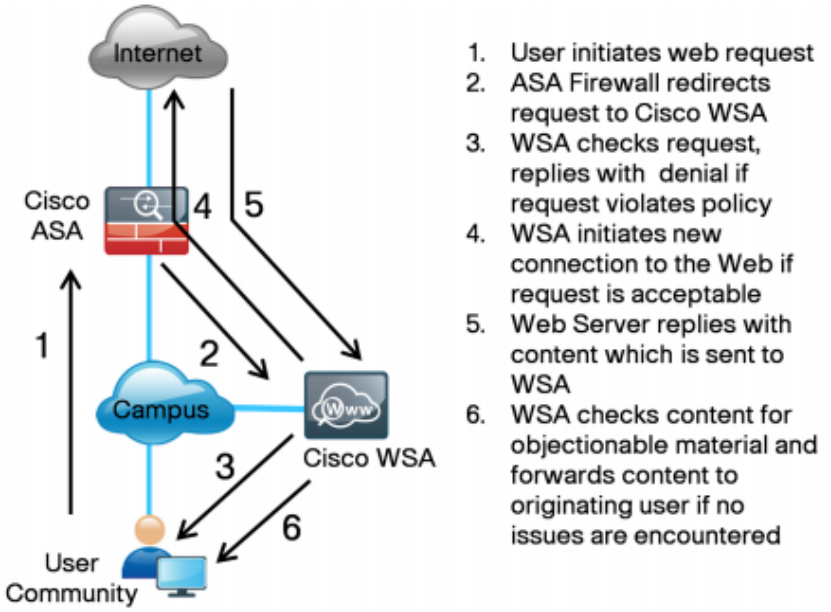


Рис. 4.30. Алгоритм обработки пользовательского web трафика

С помощью Cisco ASA и Cisco WSA возможно осуществлять проксирование web-запросов удаленных пользователей. К примеру удаленный пользователь подключившийся к открытой сети wi-fi в гостинице устанавливает VPN соединение до Cisco ASA используя клиент AnyConnect. Профиль VPN подключений на Cisco ASA конфигурируется таким образом, что весь трафик от удаленного пользователя перенаправляется через установленное защищенное соединение и затем инспектируется Cisco WSA, как если бы пользователь был в локальной сети. Таким образом можно обезопасить удаленного сотрудника даже при использовании им открытых wi-fi сетей.

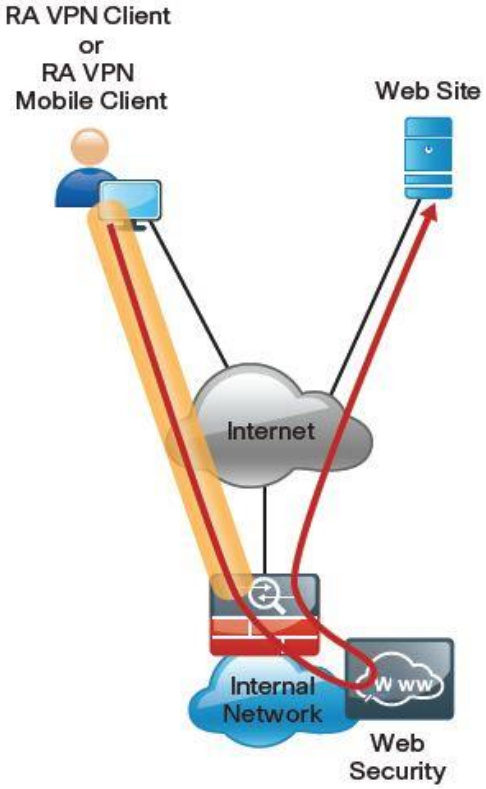


Рис. 4.31. Защита удаленного пользователя

4.6.3. АЛЬТЕРНАТИВЫ

Устройства обеспечивающие веб-защиту часто называют средством контентной фильтрации. Решения контентной фильтрации обеспечивают безопасность интернет-соединений защищая организацию от вирусов, шпионских программ, фишинг-атак и много другого. Как правило такие устройства представляются в нескольких вариантах: программно-аппаратные комплексы, программное обеспечение, облачные сервисы, гибридные решения.

На данный момент основными игроками на рынке контентной фильтрации являются:

- BlueCoat
- Websense
- SafeNet
- McAfee

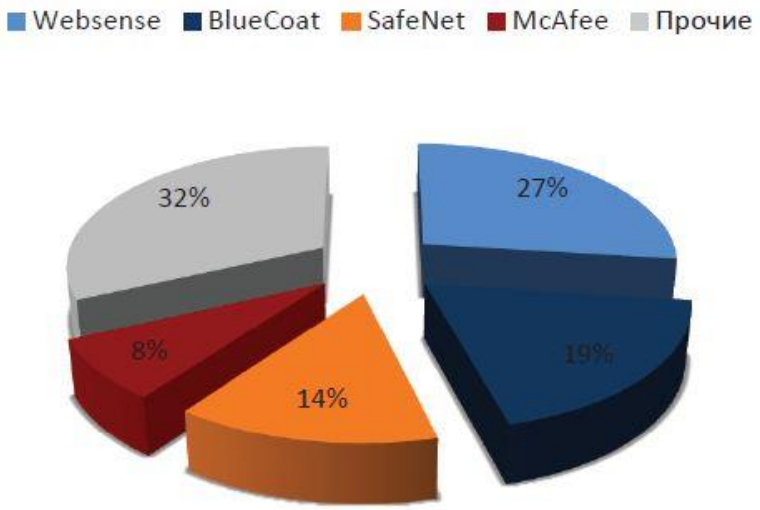


Рис. 4.32. Доли рынка контентной фильтрации на 2013 год

За ними следуют нишевые игроки:

- Cisco
- Symantec
- TrendMicro
- Microsoft
- PaloAlto
- Sophos
- Fortinet
- BarracudNetworks
- Zscaler
- PineApp

В виду такой большой конкуренции производители стараются снабдить свои устройства уникальным функционалом, отличающих от других решений на рынке. Контентный фильтр это уже не просто база категорий ресурсов сети Интернет, это потоковый антивирус, проксирование приложений, контроль утечек информации (DLP), контроль полосы пропускания, верификация сертификатов, удаление активного контента.

Как и в случае с устройствами защиты электронной почты, многие вендоры включают функционал контентной фильтрации в свои UTM решения. О плюсах и минусах подобного подхода мы поговорим немного позже.

Многие производители так же предоставляют облачные решения по веб-защите. У компании Cisco это - Cisco Cloud Web Security. Однако не многие организации готовы использовать облачные решения опасаясь утечки конфиденциальных данных.

Что касается бесплатных решений, то одним из самых известных и используемых прокси серверов является Squid. Данное ПО обладает большинством необходимых функций, что позволяет использовать его даже в больших организациях. Squid устанавливается на linux- или freebsd-дистрибутив, может использоваться в связке с бесплатным антивирусом ClamAV. Многие бесплатные межсетевые экраны предлагают данный функционал в качестве дополнительного модуля:

- pfSense
- ClearOS
- IPFire
- Zentyal
- и т.д.

4.7. UTM – РЕШЕНИЯ

Абсолютное большинство организаций активно используют информационные технологии. Разве можно представить современную компанию у которой нет корпоративной почты, веб-сайта, файлового хранилища, выделенных физических и виртуальных серверов и т.д. Перед специалистами по информационной безопасности встает серьезная проблема обеспечения защиты корпоративной сети. Вот неполный перечень средств защиты ИТ инфраструктуры:

1. Межсетевой экран (FW);
2. Система предотвращения вторжений (IPS);
3. Защищенный удаленный доступ (VPN);
4. Веб-фильтрация (proxy сервер);
5. Защита электронной почты (antispam, antivirus);
6. И т.д.

Каждое средство, указанное выше, требует наличие квалифицированного специалиста, способного осуществить внедрение, настройку и дальнейшее обслуживание. Это в свою очередь ведет к необходимости найма дополнительного персонала обладающего соответствующими навыками либо дорогостоящее обучение имеющихся специалистов, особенно если все описанные средства являются решениями различных вендоров.

Кроме того, на устройствах может происходить дублирование функционала, что в итоге отражается в виде неоправданных затрат. Возможное некорректное взаимодействие смежных средств защиты и отсутствие единой панели управления существенно сказывается на удобстве использования всей ИТ инфраструктуры.

Учитывая выше описанные факторы стало весьма логичным появление устройств нового поколения - UTM (Unified Threat Management System). UTM устройства представляют собой целый комплекс средств защиты сетевых ресурсов. Функции межсетевого экрана, IPS, VPN, веб-фильтрации, защиты от спама и многое другое реализованы в одном устройстве с единым интерфейсом управления.

Сейчас перед специалистами по информационной безопасности встает вопрос: “Что выбрать? Придерживаться традиционного подхода и использовать узкоспециализированные автономные средства защиты или же выбрать UTM (все в одном) решение?” Попытаемся рассмотреть основные плюсы и минусы UTM устройств, а так же область их применения.

Согласно мнению исследовательской компании Gartner, минимальный функционал современного UTM устройства должен выглядеть следующим образом:

- Межсетевое экранирование;
- Предотвращение сетевых вторжений;
- Организация защищенного удаленного доступа (VPN);
- Веб-фильтрация - проверка на наличие вредоносного трафика, URL - фильтрация, контроль приложений.

Некоторые производители UTM устройств реализуют дополнительные возможности:

- Контроль утечек информации через электронную почту (DLP);
- Антиспам - фильтрация нежелательной почты;
- Антивирус и защита от шпионского ПО. Как правило осуществляется проверка на вирусы и черви в протоколах HTTP, FTP, SMTP, POP3.

Таким образом системы "всё в одном" обеспечивают все необходимые функции защиты сетевых ресурсов одновременно сокращая стоимость внедрения и эксплуатации, а так же существенно уменьшая время развертывания. Столь обширный набор функций обеспечивает возможность использования одного единственного устройства для защиты сети, что в свою очередь позволяет унифицировать используемое оборудование и применять его в качестве типового решения. Упрощаются процессы настройки, мониторинга, обновления и поиска проблем. Обучение специалистов по информационной безопасности обходится дешевле, чем при использовании традиционного мультивендорного решения с отдельным устройством для каждой функции защиты.

Еще одним неоспоримым плюсом многофункциональных систем является модульность. Большинство UTM решений в базовой оснащенности имеют только функцию межсетевого экрана, остальные же функции (IPS, SSL VPN, Antispam, Antivirus URL-фильтрация и т.д.) включаются с помощью дополнительных лицензий. Это позволяет создавать решения именно с той функциональность, которая требуется в данный момент. Требования к системе защиты информации могут формироваться исходя из потребностей бизнеса, а так же финансовых возможностей потребителя. При этом любая из дополнительных функций может быть активирована уже после внедрения не требуя каких-либо изменений в топологии сети.

Ниже приведены основные вендоры, предоставляющие UTM решения на Российском рынке:

- Fortinet (есть сертификат ФСТЭК);
- Check Point (есть сертификат ФСЭК);
- WatchGuard (есть сертификат ФСТЭК);
- Sophos (есть сертификат ФСТЭК);
- Cisco (есть сертификат ФСТЭК);
- Ideco ICS (есть сертификат ФСТЭК)
- StoneGate (есть сертификат ФСТЭК)

Текущая ситуация на рынке UTM устройств сравнима с "гонкой вооружений". Компании-производители стремятся обеспечить как можно большую функциональность своих решений зачастую жертвуя производительностью и качеством. Как правило все вендоры устройств защиты информации специализируются в одной либо двух областях. Именно поэтому в последнее время участилась практика поглощения крупными компаниями более мелких игроков на рынке информационной безопасности. Для реализации дополнительных функций производители используют сторонние решения интегрируя их в свои продукты. И далеко не всегда эта интеграция проходит успешно. Это похоже на попытку собрать хороший автомобиль из запчастей от нескольких машин. Таким образом, при выборе UTM устройства стоит отдать предпочтение решению основанному на единой платформе, которая обеспечивает все заявленные функции.

Не следует забывать о производительности. При активации всех средств защиты (FW, IPS, VPN, Proxy, Antispam и т.д.) производительность любого UTM решения уменьшается в десятки раз. В этом плане традиционная модель с использованием автономных устройств является более привлекательной, к примеру, загруженный IPS никаким образом не повлияет на производительность межсетевого экрана.

Учитывая описанные плюсы и минусы UTM решений может возникнуть вопрос относительно области применения. Традиционно считается, что устройства данного класса подходят для малых и средних организаций, а так же для филиалов крупных компаний. Однако в последнее время заметна тенденция использования многофункциональных устройств и в сегменте крупных компаний, головных офисов, гос. учреждений. Связано это в первую очередь с желанием унифицировать применяемые решения, а так же значительно упростить сетевую топологию, ведь при использовании многофункциональных систем отпадает необходимость в сложной физической коммутации между устройствами защиты, вся обработка трафика происходит в одной “коробке”.

Резюмируя все выше сказанное можно с уверенностью сказать, что рынок UTM устройств в России весьма популярен и эта популярность будет только расти. Есть все основания полагать, что многофункциональные системы со временем полностью вытеснят традиционные мультивендорные решения, ведь их появление является своего рода эволюцией в мире информационной безопасности.

5. МОДУЛЬ ТЕРРИТОРИАЛЬНЫХ СЕТЕЙ WAN (WAN EDGE)

Прежде всего необходимо понять, что такое WAN. Если перевести дословно Wide Area Network - глобальная сеть. Говоря простым языком, WAN это объединение нескольких локальных сетей, географически разнесенных. Одним из примеров WAN сети является Internet, объединяющий множество мелких сетей.

Большинство современных организаций имеют удаленные офисы, которые могут находиться в других городах, странах и материках. При этом большинство информационных ресурсов, необходимых для повседневных бизнес процессов, располагаются в головном офисе. Удаленные площадки должны так же иметь к ним доступ, т.к. установка отдельных серверов в каждом офисе не целесообразна ни экономически, ни логически. Таким образом возникает необходимость в организации канала передачи данных между удаленным и головным офисом. Естественно, что данное подключение должно быть защищенным, т.к. передаваемая информация может являться конфиденциальной.

Существует несколько основных технологий организации WAN сетей:

1. MPLS WAN
2. Layer 2 WAN
3. Internet with VPN WAN
4. Internet 3G/4G with VPN WAN

Мы не будем подробно рассматривать все технологии, т.к. каждая из них заслуживает отдельного руководства. Кратко рассмотрим способ Internet with VPN WAN в виду его простоты и быстроты развертывания.

5.1. УСТРОЙСТВА

Выбор устройств для построения VPN сети зависит от конкретных требований организации, а так же исходя из имеющегося бюджета.

Далее приводится несколько примеров и альтернатив.

5.2. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

На сегодняшний день, практически любая организация имеет Интернет подключение. Глядя на тенденции развития этой сети, можно заметить, что предоставляемая пропускная способность увеличивается с каждым годом и, в свете непрерывной конкуренции провайдеров Интернет, стабильно дешевеет. Подключение удаленного филиала так же не представляет особых трудностей. Кроме того Интернет гораздо дешевле выделенного канала между двумя офисами, которые могут находиться на разных континентах. На данный момент MPLS является одной из самых распространенных технологий для построения WAN сетей, однако стоимость канала с пропускной способностью 3 Мбит/с сопоставима со стоимостью 50-100 Мбит/с сети Интернет. Экономия очевидна.

Логично предположить, что сотрудникам удаленного офиса так же необходимо пользоваться интернет ресурсами. Отсюда возникают аналогичные угрозы, которые мы рассмотрели в рамках модуля Internet Edge, и появляется необходимость в соответствующих средствах защиты (Межсетевой экран, Система предотвращения вторжений, Удаленный доступ, Защита электронной почты, Веб-защита). Однако установка всех этих средств защиты в

удаленном офисе обернется большими и не оправданными затратами. Решением данной проблемы является использование средств защиты головного офиса. Рассмотрим пример, представленный на рис. 5.1.

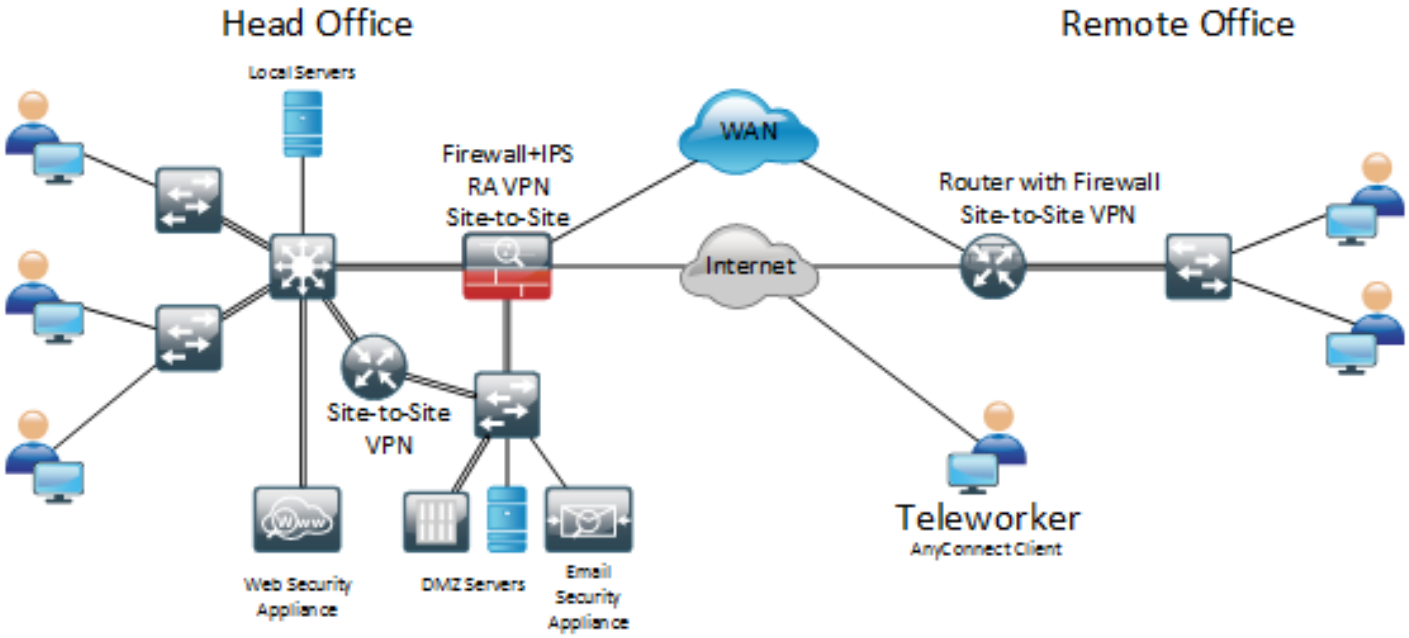


Рис. 5.1. Пример подключения удаленного офиса

Головной офис (Head Office) имеет все необходимые средства защиты в модуле Internet Edge (о его компонентах и дизайне мы говорили ранее):

1. Cisco ASA 5512-X IPS Edition - Межсетевой экран с функцией IPS.
2. Cisco Email Security Appliance C170 (C170-BUN-R-NA) - Защита электронной почты.
3. Cisco Web Security Appliance S170 S170-BUN-R-NA - Веб защита.

Удаленный офис подключается к сети Интернет. В качестве маршрутизатора устанавливается Cisco CISCO2911-SEC/K9 2911 Security Bundle with sec License Pak с функцией межсетевого экрана. Интернет в удаленном офисе выступает в качестве транспортной сети и используется для организации Site-to-Site VPN подключения до центрального узла.

В головном офисе для построения Site-to-Site VPN может использоваться как основной межсетевой экран, так и дополнительно установленный VPN маршрутизатор (рис. 5.1), который помещается в DMZ сегмент. Используя для этих целей межсетевой экран снижаются затраты. В случае использования выделенного VPN маршутизатора повышается производительность и масштабируемость. В качестве маршрутизатора может использоваться любое устройство поддерживающее Site-to-Site IPSec VPN (CISCO2911, CISCO2921, CISCO2951 и т.д.).

Следует понимать разницу между Site-to-Site VPN и Remote Access VPN.

Remote Access VPN предназначен для временного защищенного доступа удаленного пользователя к корпоративным ресурсам, при этом у пользователя должно быть установлено специально программное обеспечение - vpn клиент (Cisco AnyConnect). Соединение может инициировать только сам пользователь.

Site-to-Site VPN предназначен для организации постоянного двустороннего канала между двумя объектами (Рис. 5.2.). При этом пользователи не нуждаются в установке дополнительного ПО.

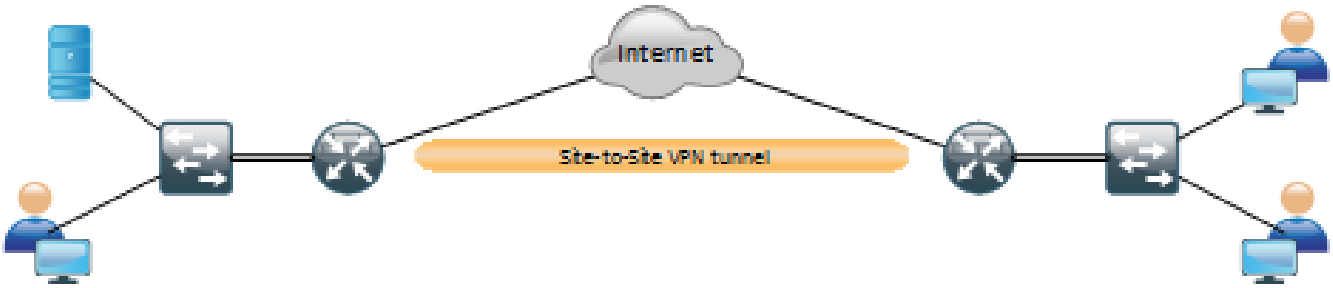


Рис. 5.2. Site-to-Site VPN туннель

Сеть Интернет в удаленном офисе используется только для организации VPN канала и весь трафик пользователей к интернет ресурсам проходит через существующий модуль Internet Edge, расположенный в головном офисе. В результате пользователи удаленного офиса получают все необходимые средства защиты (Межсетевой экран, Система предотвращения вторжений, Удаленный доступ, Защита электронной почты, Веб-защита)

Таким образом используя технологию Internet with VPN WAN мы сокращаем расходы на построение территориальной сети за счет меньшей стоимости канала Интернет и использования уже существующих средств защиты.

5.3. АЛЬТЕРНАТИВЫ

Т.к. WAN сети образуются с использованием глобальной сети Интернет, то совершенно логично, что передаваемые данные необходимо шифровать. Ранее в параграфе “О криптографии в России” мы ознакомились с некоторыми особенностями использования шифрования в нашей стране. Следовательно некоторые организации не могут использовать решения компании Cisco для построения WAN сетей и обязаны применять отдельные (даже при наличии МЭ с функцией VPN) средства использующие отечественные алгоритмы шифрования (ГОСТ VPN) - криптошлюзы. А это все государственные и муниципальные структуры; организации работающие с информацией, принадлежащей государству; организации работающие с информацией ограниченного доступа (охраняемая государством).

Большинство средств защиты использующие ГОСТ VPN мы рассмотрели ранее:

- S-Terra
- CheckPoint (требуется установка ГОСТ-патча)
- StoneGate
- Дионис
- АПКШ Континент
- Атликс VPN

Более подробно в параграфе “О криптографии в России”.

Для сегмента малого бизнеса (и там, где не требуется ГОСТ шифрование) весьма привлекательными окажутся решения компании Mikrotik, обладающие необходимым набором функций для построения WAN сетей и имеющие весьма низкие цены. Пример цен:

Cloud Router Switch 125-24G-1S-RM - 7 500 руб.

RouterBOARD 2011UiAS-2HnD-IN - 4 800 руб.

RouterBOARD 951G-2HnD - 2 900 руб.

Кроме того данные устройства позволяют организовать VPN канал с решениями компании Cisco и идеально подойдут для удаленных филиалов.

Что касается бесплатных средств, то здесь как всегда существует большое кол-во opensource решений. Один из наиболее известных представителей - OpenVPN. Это свободная, кросплатформенная реализация VPN сервера с открытм исходным кодом. Данное ПО активно развивается. В качестве аппаратной платформы можно выбрать стоечный сервер (hp, dell, ibm и т.д.), обычный desktop или же виртуальную машину. Располагается VPN сервер как правило в DMZ и имеет публичный (белый) ip-адрес.

6. СЕРВЕРНЫЙ МОДУЛЬ

Серверный модуль - это последний модуль который будет рассмотрен в рамках данного руководства. Тема построения датацентра заслуживает отдельного подробного руководства, автор же постарается описать основные принципы построения сетевой инфраструктуры для подключения корпоративных серверов малых и средних организаций (до 1 000 человек).

На данный момент существует три подхода при построения серверной инфраструктуры:

1. Использование физических серверов. Практически для каждого сервиса используется отдельный "железный" сервер. Иногда некоторые сервисы объединяют в рамках одного сервера (AD+DNS+NTP+DHCP и т.д.).
2. Использование виртуальных серверов. Создаются виртуальные машины на сервере виртуализации. В качестве платформы виртуализации может выступать один высокопроизводительный сервер, либо несколько, которые объединяются в один ресурс вычислительной мощности.
3. Гибридный подход. Используются как виртуальные так и физические сервера.

На тему преимуществ виртуализации перед традиционным подходом написано не мало статей и книг. Экономия электроэнергии, снижение затрат на поддержку существующей инфраструктуры, повышение коэффициента использования вычислительных ресурсов, масштабируемость, скорость развертывания, упрощение администрирования - лишь немногие преимущества виртуальных серверов. Согласно текущим тенденциям рынка виртуальные решения полностью вытеснят физические сервера в ближайшие несколько лет.

6.1. УСТРОЙСТВА

Для серверного модуля построенного на основе физических серверов будет требоваться оборудование отличное от оборудования необходимого при использовании виртуальной инфраструктуры.

6.1.1. СЕРВЕРНЫЙ МОДУЛЬ НА ОСНОВЕ ФИЗИЧЕСКИХ СЕРВЕРОВ

Обязательным компонентом модуля серверов является коммутатор второго (L2) или третьего (L3) уровня модели OSI. В этот коммутатор подключаются сетевые интерфейсы серверов. Могут применяться коммутаторы уровня доступа.

Коммутаторы которые могут применяться в серверном модуле:

Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot
Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E
Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45)
Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45)
Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000
Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000
Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000
Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000
Cisco Catalyst 2960-X Series 24 Ethernet 10/100/1000
Cisco Catalyst 2960-X Series 48 Ethernet 10/100/1000
Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000

Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000

Использование коммутаторов с поддержкой PoE в сегменте серверов - нецелесообразно, т.к. в данном сегменте отсутствуют устройства требующие питание по Ethernet-кабелю.

Наиболее оптимальным решением является коммутатор серии Cisco Catalyst 2960-X. Он обладает необходимым набором функций, все порты поддерживают гигабитные соединения. Среди гигабитных коммутаторов 2960-X является самым дешевым. В случае большого кол-ва серверов лучше использовать стэкируемые коммутаторы, что упростит конфигурацию и администрирование. К примеру Cisco 3750-X.

В качестве средств защиты в сегменте серверов (в случае использования физических серверов) используются межсетевой экран и система предотвращения вторжений.

МЭ которые могут применяться в модуле серверов:

Cisco ASA 5545-X - security appliance (ASA5545-K9)
Cisco ASA 5525-X - security appliance (ASA5525-K9)
Cisco ASA 5515-X - security appliance (ASA5515-K9)
Cisco ASA 5512-X - security appliance (ASA5512-K9)
Cisco ASA5512-X Security Plus license (ASA5512-SEC-PL)

МЭ с уже активированной функцией IPS:

Cisco ASA 5545-X IPS Edition - security appliance (ASA5545-IPS-K9)
Cisco ASA 5525-X IPS Edition - security appliance (ASA5525-IPS-K9)
Cisco ASA 5515-X IPS Edition - security appliance (ASA5515-IPS-K9)
Cisco ASA 5512-X IPS Edition - security appliance (ASA5512-IPS-K9)
Cisco ASA5512-X Security Plus license (ASA5512-SEC-PL)

Отдельно стоящие IPS устройства (Standalone Appliances):

Cisco IPS 4520 (IPS-4520-K9)
Cisco IPS 4510 (IPS-4510-K9)
Cisco IPS 4360 (IPS-4360-K9)
Cisco IPS 4345 (IPS-4345-K9)

Выбор конкретной модели зависит от требуемой пропускной способности. Пропускная способность устройств представлена в 4.2.1, 4.3.1.

6.1.2. СЕРВЕРНЫЙ МОДУЛЬ НА ОСНОВЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

При использовании виртуальной инфраструктуры так же необходим коммутатор к которому будут подключаться высокопроизводительные сервера виртуализации. Наиболее оптимальным решением в данном случае является коммутатор Cisco Catalyst 2960-X.

В качестве гипервизора используется VMWare ESXi - программный комплекс обеспечивающий возможность одновременной, параллельной работы нескольких операционных систем на одном физическом сервере.

Новые технологии требуют новых механизмов защиты. Традиционные средства уже не удовлетворяют требованиям безопасности виртуальной инфраструктуры. Новые необходимые устройства:

Cisco Nexus 1000V - виртуальный коммутатор
Cisco VSG - виртуальный шлюз безопасности
Cisco ASA 1000V - виртуальный межсетевой экран

Данные средства поставляются в виде образов виртуальных машин.

Практически любой сетевой сегмент начинается с коммутации. Серверный модуль не является исключением. При использовании физических серверов их сетевые интерфейсы подключаются к коммутаторам, порты которых определяются в соответствующий VLAN. В случае виртуальной инфраструктуры к физическому коммутатору подключаются только сетевые интерфейсы серверов виртуализации. Созданные внутри виртуальные машины имеют виртуальные сетевые интерфейсы, которые так же необходимо коммутировать. Для этих целей используются так называемые виртуальные коммутаторы. В состав гипервизора VMWare ESXi входят две версии виртуальных коммутаторов:

- vSphere Standart Switch
- vSphere Distributed Switch (Распределенный коммутатор)

Различия между этими версиями представлены на рисунке 6.1.

Features	Standard Switch	Distributed Switch
Management	Standard switch needs to managed at each individual host level	Provides centralized management and monitoring of the network configuration of all the ESXi hosts that are associated with the dvswitch.
Licensing	Standard Switch is available for all Licensing Edition	Distributed switch is only available for enterprise edition of licensing
Creation & configuration	Standard switch can be created and configured at ESX/ESXi host level	Distributed switch can be created and configured at the vCenter server level
Layer 2 Switch	Yes, can forward Layer 2 frames	Yes, can forward Layer 2 frames
VLAN segmentation	Yes	Yes
802.1Q tagging	Can use and understand 802.1q VLAN tagging	Can use and understand 802.1q VLAN tagging
NIC teaming	Yes, can utilize multiple uplink to form NIC teaming	Yes, can utilize multiple uplink to form NIC teaming
Outbound Traffic Shaping	Can be achieved using standard switch	Can be achieved using distributed switch
Inbound Traffic Shaping	Not available as part of standard switches	Only possible at distributed switch
VM port blocking	Not available as part of standard switches	Only possible at distributed switch
Private VLAN	Not available	PVLAN can be created as part of dvswitch. 3 types of PVLAN(Promiscuous, Community and Isolated)
Load based Teaming	Not available	Can be achieved using distributed switch
Network vMotion	Not available	Can be achieved using distributed switch
Per Port policy setting	Policy can be applied at switch and port group	Policy can be applied at switch, port group and even per port level
NetFlow	Not available	Yes
Port Mirroring	Not available	Yes

Рис. 6.1. Виртуальные коммутаторы VMWare

Самое главное отличие - Distibuted Switch позволяет создать единый виртуальный коммутатор для нескольких виртуальных серверов, что существенно упрощает топологию и администрирование виртуальной сети (Рис. 6.2). Standart Switch работает только в рамках одно физического сервера.

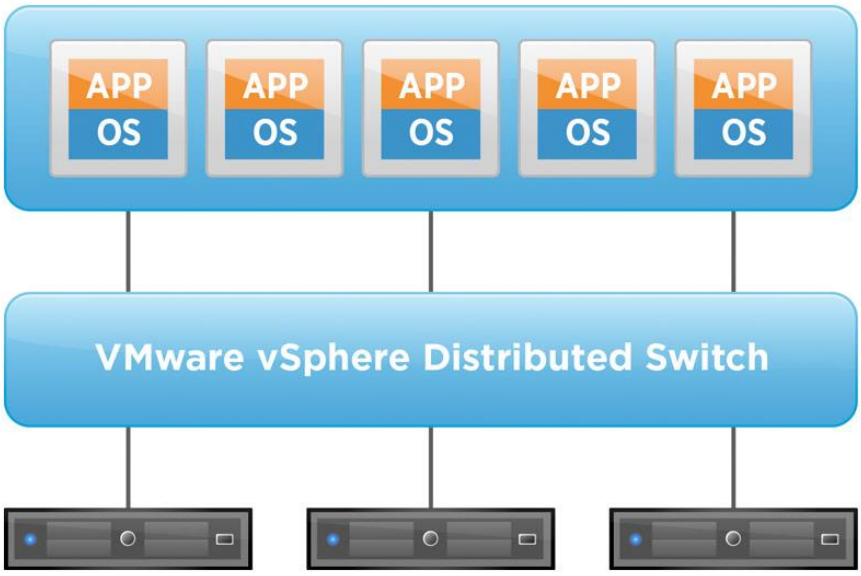


Рис. 6.2. Распределенный коммутатор

Компания Cisco разработала замену встроенному коммутатору VMWare - Cisco Nexus 1000v. Коммутатор Cisco Nexus 1000v доступен в двух версиях:

Cisco Nexus 1000V Pricing

Tiered Licensing – Essential & Advanced Editions

	Essential ($0)	Advanced ($695/cpu)
VLANs, ACL, QoS	✓	✓
vPath	✓	✓
LACP	✓	✓
Multicast	✓	✓
Netflow, SPAN, ERSPAN	✓	✓
Management (SNMP etc.)	✓	✓
SCVMM Integration	✓	✓
DHCP Snooping		✓
IP Source Guard		✓
Dynamic ARP Inspection		✓
Virtual Security Gateway**		✓

Рис. 6.3. Сравнение функций бесплатной и платной версии Cisco Nexus 1000v

Из рисунка видно, что вместе с платной версией коммутатора становится доступен виртуальный шлюз безопасности Cisco VSG. Лицензирование производится исходя из кол-ва процессоров на сервере виртуализации.

Лицензирование Cisco ASA 1000v производится аналогично Cisco Nexus 1000v - по кол-ву процессоров.

6.2. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

Как было сказано ранее, в зависимости от выбранного подхода построения серверного модуля будет различаться набор необходимого сетевого оборудования, а следовательно и сам дизайн серверного модуля.

6.2.1. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ С ИСПОЛЬЗОВАНИЕ ФИЗИЧЕСКИЙ СЕРВЕРОВ

Дизайн серверного модуля во многом схож с дизайном модуля Интернет. Как в большинстве модулей, построение начинается с коммутации. Для этих целей используется коммутатор второго или третьего уровня модели OSI. Выбор конкретной модели в большей степени зависит от необходимой пропускной способности, т.к. сервера организации испытывают наибольшую сетевую нагрузку. Коммутатор обеспечивает первичную сегментацию сети, а так же базовые функции защиты по средствам использования port-securtity и private vlan.

Для защиты модуля серверов так же используются межсетевой экран и система предотвращения вторжений. На рисунке 6.4 изображен типовой дизайн серверного сегмента.

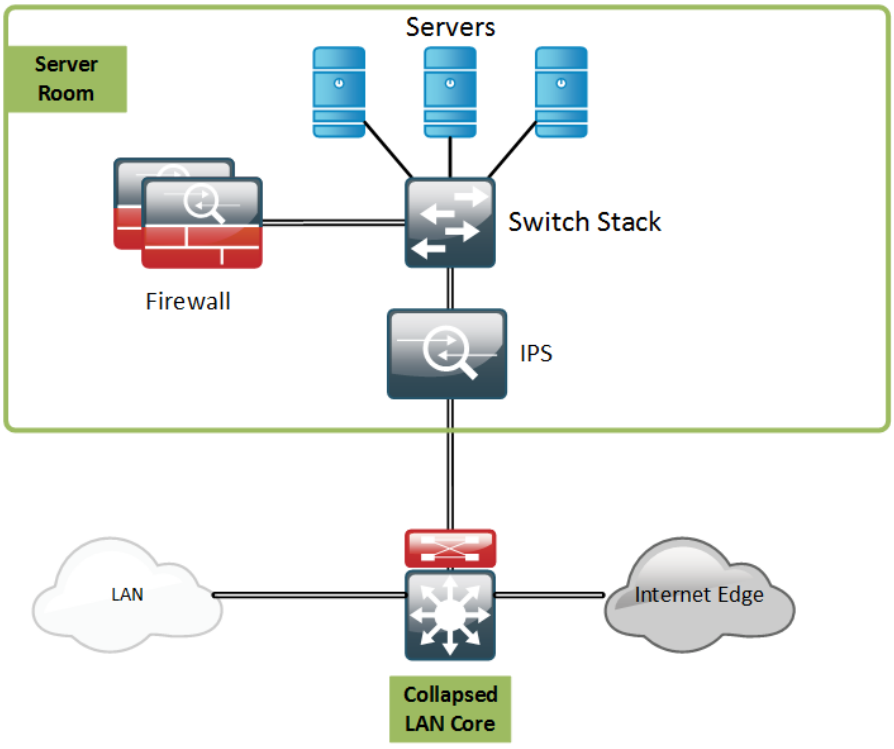


Рис. 6.4. Типовой дизайн серверного модуля

Межсетевой экран может устанавливаться в отказоустойчивом исполнении и подключается к одному или нескольким коммутаторам серверов. МЭ обеспечивает маршрутизацию и разграничение доступа между различными сегментами серверного модуля.

IPS устанавливается в inline режиме. Т.к. в данном режиме весь трафик проходит через устройство, желательно чтобы IPS обладал функцией hardware bypass, это позволит циркулировать трафику даже при выключенном IPS.

6.2.2. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

В случае использования виртуальный инфраструктуры традиционный подход защиты уже не является эффективным. На одном физическом сервере находится несколько виртуальных машин и все их сетевое взаимодействие осуществляется в рамках единой платформы не выходя за пределы сетевого интерфейса сервера виртуализации. Таким образом существует три выхода из данной ситуации:

1. Пренебречь защитой внутри виртуальной инфраструктуры и ограничиться разграничением доступа до всего сегмента серверов. Самый худший вариант, т.к. в данном случае если злоумышленник получает доступ хотя бы к одной виртуальной машине, то под угрозой оказывается вся виртуальная инфраструктура. Эта проблема особенно актуальна если на сервере виртуализации существуют машины, логически помещенные в DMZ зону, что является довольно частой практикой.
2. Сегментировать всю виртуальную инфраструктуру, помещая каждую виртуальную машину в выделенный сегмент. Для контроля межсетевого взаимодействия используется традиционный межсетевой экран (как было описано в пункте 6.2.1). Однако в случае большого кол-ва виртуальных машин сильно усложняется топология сети и резко повышается требование к производительности МЭ, что существенно сказывается на затратах.
3. Использовать специализированные средства защиты для виртуальной инфраструктуры: Cisco Nexus 1000v, Cisco VSG, Cisco ASA 1000v. Именно этот вариант рассматривается ниже.

Благодаря применяемой технологии vPath (применяемая в виртуальных продуктах Cisco) появилась возможность определять порядок обработки трафика, не изменяя при этом топологию виртуальной сети. На рисунке 6.5 представлен пример использования технологии vPath в виртуальной среде.

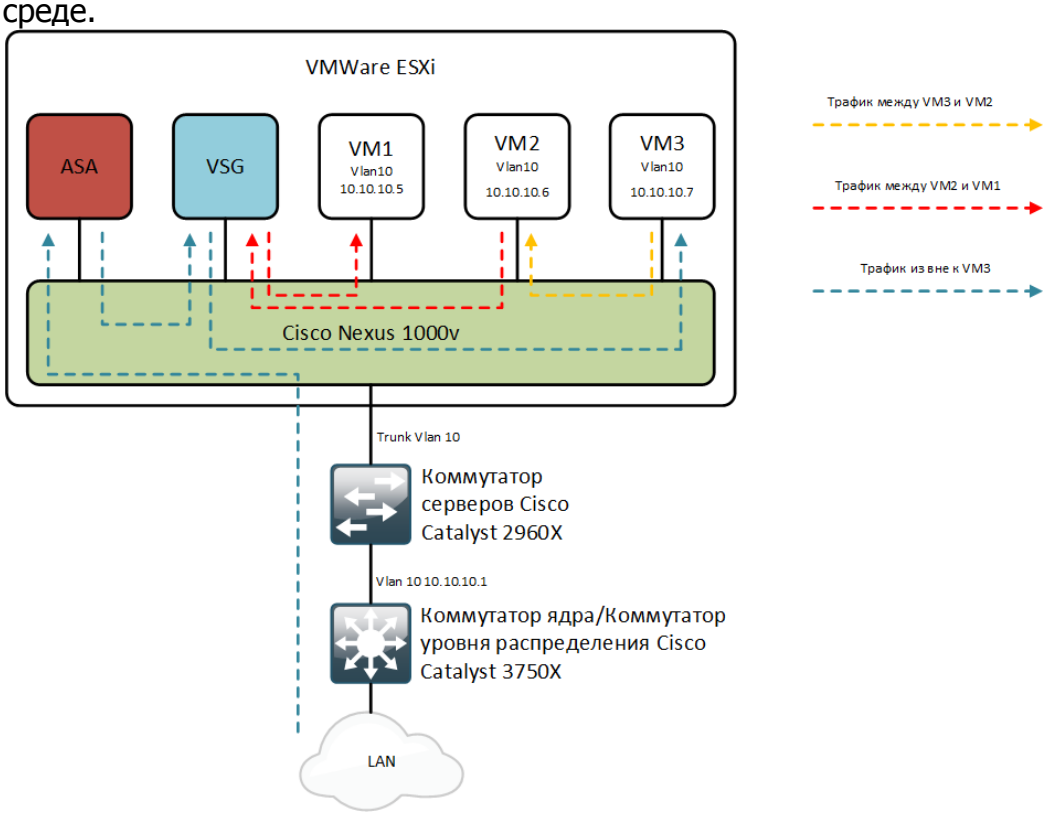


Рис. 6.5. Использование технологии vPath

Как видно из рисунка, все три виртуальные машины расположены в одном сегменте и имеют ip-адреса из одной сети. Маршрутизируется данный сегмент на коммутаторе ядра или коммутаторе уровня распределения. При данной топологии традиционные средства не позволяют разграничивать доступ между виртуальными машинами. Для определения порядка обработки трафика используется технология vPath, которая осуществляет инкапсуляцию проходящих пакетов и перенаправляет трафик виртуальных машин в соответствии с существующими политиками безопасности.

К примеру трафик между VM3 и VM2 разрешен без каких либо ограничений. Пакеты между VM2 и VM1 должны сначала попасть на VSG и пройти пакетную фильтрацию. Трафик из "вне" вынужден пройти межсетевой экран Cisco ASA 1000v, VSG и лишь затем попадет на VM3. Соответствующие политики доступа формируются централизованно с помощью Cisco Virtual Network Management Center (сейчас данный продукт известен как Cisco Prime Network Services Controller). Следует отметить, что Cisco Prime Network Services Controller предоставляется бесплатно для управления Nexus 1000v, VSG и ASA 1000v.

Используя технологию vPath мы получаем возможность маршрутизировать трафик в виртуальной инфраструктуре на новом уровне.

Использование виртуального межсетевого экрана Cisco ASA 1000v позволяет оперативно организовать защиту виртуальных машин не изменяя существующую топологию сети и не требует больших финансовых вложений.

6.3. АЛЬТЕРНАТИВЫ

В случае использования физических серверов справедливы все ранее приведенные альтернативы для МЭ (параграф 4.2.3) и для IPS (параграф 4.3.3).

Говоря об виртуальной инфраструктуре, то на момент написания данного руководства какой-либо альтернативы технологии vPath - нет. Подавляющее большинство вендоров уже выпустили либо стремятся выпустить виртуальные версии своих средств защиты (МЭ, IPS и т.д.). Данные решения во многом удобнее, дешевле, выше скорость развертывания, однако они не решают главной проблемы - безопасное взаимодействие виртуальных машин внутри гипервизора. Использование подобных решений предполагает сегментирование сети и серьезное изменение топологии. Дизайн при этом аналогичен дизайну с использованием физических серверов, только физический коммутатор и МЭ заменяют виртуальные решения.

Бесплатным аналогом распределенного виртуального коммутатора является Open vSwitch - позволяет объединять виртуальные машины с разных серверов виртуализации в рамках одного коммутатора.

У следующих вендоров имеются виртуальные решения межсетевых экранов:

- Cisco (ASAv)
- StoneGate FW
- CheckPoint
- Fortinet
- Ideco ICS
- и т.д.

Что касается бесплатных решений то практически любой opensource дистрибутив может быть установлен в виртуальной инфраструктуре:

- pfSence
- ClearOS

- IPFire
- Zentyal
- и т.д.

Бесплатные системы предотвращения вторжений Snort и Suricata могут быть установлены в качестве виртуальной машины.

Так же стоит обратить внимание на решение компании Mikrotik - RouterOS. Данная операционная система может быть установлена в виртуальной инфраструктуре и выполнять роль межсетевого экрана, прозрачного прокси сервера, vpn-концентратора и многое другое. Для использования RouterOS требуется приобретение лицензии. Стоимость лицензии, раскрывающей максимальный функционал, составляет порядка 5500 рублей.

Существуют альтернативы среди используемых гипервизоров. Компания VMWare имеет несколько конкурентов, однако по прежнему сохраняет лидерство на рынке виртуализации. На рис. 6.6. представлен магических квадрант Гартнера для инфраструктуры виртуализации x86 серверов.

Рис. 6.6. Магический квадрант для инфраструктуры виртуализации x86-серверов

Как видно из рисунка, VMWare с продуктом ESXi является лидером среди гипервизоров. ESXi доступен в бесплатной версии с незначительными ограничениями и идеально подходит для малого и среднего бизнеса. Платные версии обладают большим функционалом и внедряются в крупных организациях.

Вторую позицию занимает компания Microsoft с продуктом Hyper-V. Фактически при покупке Windows Server вы получаете бесплатно гипервизор Hyper-V. В случае если вы приобретаете Windows Server Datacenter, то вы получаете возможность использования неограниченного кол-ва виртуальных машин с Windows Serever.

Далее следует компания Oracle, которая обладает бесплатным десктопным решением VirtualBox, которое идеально подходит для тестирования и макетирования различных операционных систем.

Citrix XenServer является бесплатной корпоративной платформой виртуализации с платной технической поддержкой.

Так же стоит обратить внимание на бесплатное решения Proxmox, обладающее всеми необходимыми функциями, которые работают “из коробки”.

7. ПРИМЕР

Для закрепления прочитанного материала автор предлагает вашему вниманию два небольших примера построения корпоративной сети для средней организации. Первый пример будет содержать только продукты компании Cisco, второй – более дешевые аналоги.

На рис. 7.1 представлена типовая схема сети для средних организаций (от 100 до 1000 пользователей).

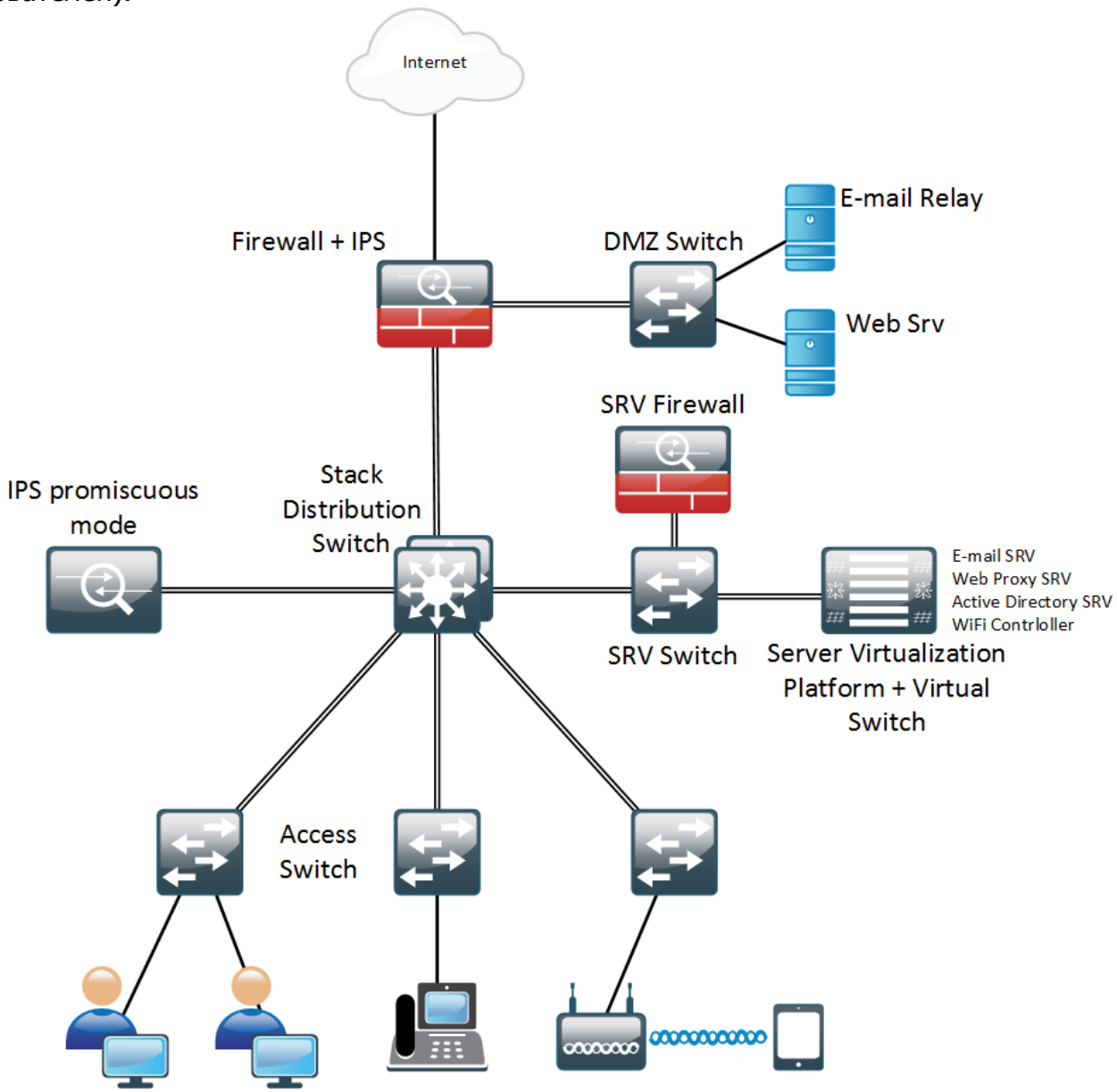


Рис. 7.1. Типовая схема сети для средних организаций

7.1. РЕШЕНИЕ НА ОСНОВЕ ОБОРУДОВАНИЯ CISCO

В качестве коммутаторов доступа используются самые дешевые коммутаторы. Главное требование – наличие двух гигабитных портов (uplink). Для примера приобретаются два коммутатора по 48 портов: WS-C2960-48TT-S.

Так же могут понадобиться коммутаторы уровня доступа с поддержкой технологии PoE для питания устройств по кабелю Ethernet (ip-телефоны, ip-видеокамеры, wifi точки доступа). Используем один коммутатор WS-C2960-24PC-S.

В качестве коммутаторов распределения и ядра (collapsed core) используются самые дешевые L3 коммутаторы поддерживающие технологию стекирования: WS-C3750X-24T-S.

Коммутатор в модуле серверов (SRV Switch) и коммутатор в модуле Internet (DMZ Switch) должны обладать гигабитными портами, т.к. к ним подключаются сервера. Выбираем два коммутатора WS-C2960X-24TS-L.

В качестве МЭ в модуле Интернет выбираем межсетевой экран с встроенной функцией IPS: ASA5512-IPS-K8. МЭ будет так же выступать в качестве VPN концентратора и использоваться для организации RA VPN и Site-to-Site VPN. Лицензия на активацию шифрования 3DES/AES – бесплатна. Так же приобретаются лицензии для удаленных пользователей.

Для защиты корпоративной почты используется E-mail Relay, а именно: Iron Port ESA-C170-K9.

Для обеспечения веб безопасности так же используется продукт Iron Port, но в виде виртуальной машины, т.к. внутренняя серверная инфраструктура основана на сервере виртуализации. Приобретается только лицензия WSA-WSE-LIC= на 100 человек (к примеру).

В локальной сети устанавливается IPS в promiscuous режиме, т.е. как IDS. Используется модель IPS-4345-K9.

Т.к. серверная инфраструктура представляет из себя сервер виртуализации, предполагается использование виртуальных средств защиты:

Cisco Nexus 1000v - L-N1K-VLCPU-04= (включает в себя VSG)

Cisco ASA 1000v - L-ASA1000V-04-PR=

Лицензии приобретаются с учетом наличия четырех процессоров на сервере виртуализации.

Итоговая спецификация представлена в таблице 7.1

Таблица 7.1. Спецификация оборудования Cisco

Product	Description	Quan-tity	List Price ($)	Selling Price($)
WS-C2960-48TT-S	Catalyst 2960 48 10/100 + 2 1000BT LAN Lite Image	2	1425	2850
CON-SCIN-2964TTS	SC IPS 8X5XNBD 48 10/100 ports + 2	2	225,4	450,8
CAB-ACE	AC Power Cord (Europe) C13 CEE 7 1.5M	2	0	0
PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE	2	0	0
WS-C2960-24PC-S	Catalyst 2960 24 10/100 PoE + 2 T/SFP LAN Lite Image	1	2050	2050
CON-SCIN-C24PCS	SC IPS 8X5XNBD Catalyst 2960 24 10/100 PoE + 2 T/SFP	1	325,45	325,45
CAB-ACE	AC Power Cord (Europe) C13 CEE 7 1.5M	1	0	0
PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE	1	0	0
WS-C3750X-24T-S	Catalyst 3750X 24 Port Data IP Base	2	6500	13000
CON-SCN-3750X2TS	SC CORE 8X5XNBD Catalyst 3750X 24 Port Data IP Base	2	448,5	897
CAB-3KX-AC-EU	AC Power Cord for Catalyst 3K-X (Europe)	2	0	0
S375XVK9T-12255SE	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	2	0	0
CAB-STACK-50CM	Cisco StackWise 50CM Stacking Cable	2	0	0
CAB-SPWR-30CM	Catalyst 3750X and 3850 Stack Power Cable 30 CM	2	0	0
C3KX-PWR-350WAC	Catalyst 3K-X 350W AC Power Supply	2	0	0
PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE	2	0	0
WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE 4 x 1G SFP LAN Base	2	2395	4790
CON-SCAN-WSC296XT	SC ADV 8X5XNBD Catalyst 2960-X 24 GigE 4 x 1G SFP LAN	2	165,6	331,2
CAB-ACE	AC Power Cord (Europe) C13 CEE 7 1.5M	2	0	0

Product	Description	Quan-tity	List Price ($)	Selling Price($)
ASA5512-IPS-K8	ASA 5512-X with IPS SW 6GE Data 1GE Mgmt AC DES	1	6495	6495
CON-SCIN-A12IPS8	SC IPS 8X5XNBD ASA 5512-X with IPS SW 6GE Data 1GE	1	861,35	861,35
SF-ASA-X-9.1-K8	ASA 9.1 Software image for ASA 5500-X Series5585-X & ASA-SM	1	0	0
SF-ASAIPS64-7.1-K9	ASA 5500-X IPS Software 7.1 for IPS SSP	1	0	0
ASA-AC-E-5512	AnyConnect Essentials VPN License - ASA 5512-X (250 Users)	1	150	150
ASA5512-IPS-SSP	ASA 5512-X IPS SSP License	1	0	0
ASA-AC-M-5512	AnyConnect Mobile - ASA 5512-X (req. Essentials or Premium)	1	150	150
CAB-ACE	AC Power Cord (Europe) C13 CEE 7 1.5M	1	0	0
ASA5500-ENCR-K8	ASA 5500 Base Encryption Level (DES)	1	0	0
ASA5512-MB	ASA 5512 IPS Part Number with which PCB Serial is associated	1	0	0
ESA-C170-K9	ESA C170 Email Security Appliance with Software	1	3950	3950
CON-SNT-C170-K9	SMARTNET 8X5XNBD ESA C170 Email Security Appliance with SW	1	272,55	272,55
CAB-ACE	AC Power Cord (Europe) C13 CEE 7 1.5M	1	0	0
SF-ESA-7.5.2-K9	ESA Async OS v7.5.2	1	0	0
CCS-HD-250GB-	Content Sec 250 GB HD for ESA C170 SMA M170 WSA S170	2	0	0
IPS-4345-K9	IPS 4345 with SW 8 GE data + 1 GE mgmt AC Power	1	39995	39995
CON-SCIN-IPS4345	SC IPS 8X5XNBD IPS 4345 with SW 8	1	11958,85	11958,85
SF-IPS-4300-7.1-K9	IPS 4345 and 4360 Software Version 7.1	1	0	0
CAB-ACE	AC Power Cord (Europe) C13 CEE 7 1.5M	1	0	0
WSA-WSE-LIC=	Web Essentials SW Bundle (WREP+WUC) Licenses	100	0	0
WSA-WSE-3Y-S1	Web Essentials SW Bundle (WREP+WUC) 3YR 100-199 Users	100	72,59	7259
L-N1K-VLCPU-04=	Nexus 1000V Adv Ed eDelivery Multi-Hypervisor License Qty4	1	2775	2775
CON-SCU1-VLCPU4	SC CORE SUP SAU Nexus 1000V eDelivery	1	0	0
L-N1K-VLCPU-01	Nexus 1000V Adv Ed eDelivery Multi-Hypervisor License Qty1	4	0	0
CON-SCU1-L-VLCPU	SC CORE SUP SAU Nexus 1000V eDelivery	4	174	696
L-VSG-VL-CPU-01	VSG eDelivery CPU License Qty 1	4	0	0
L-VSG-VL-CPU-04	VSG eDelivery CPU License Qty 4	1	0	0
L-ASA1000V-04-PR=	4 ASA1000V / VNMC incremental promo licenses (eDelivery)	1	7945	7945
CON-SAU-A1V4PR	SW APP SUPP + UPGR 4 ASA 1000V / VNMC i	1	1589	1589
L-ASA1000V-CPU-01	ASA 1000V K9 license for securing 1 CPU socket (eDelivery)	4	0	0
L-VNMC2X-ASA1K-01	VNMC 2.X ASA1000V management one CPU eDelivery	4	0	0
		Итого:	**$108,791.20**	

Все оборудование приобретается с контрактом технической поддержки SmartNet.

Стоит учитывать, что в данном примере не заложена отказоустойчивость (кроме коммутаторов уровня распределения), что существенно снижает стоимость общей спецификации. Как видно из примера, самым дорогостоящим компонентом является IPS – порядка 40 000 $.

7.2. РЕШЕНИЕ НА АЛЬТЕРНАТИВНОМ ОБОРУДОВАНИИ

Предыдущий пример содержит примерную стоимость типовой сети средней организации построенной на оборудовании Cisco. Далеко не каждая организация может себе позволить подобные затраты. Рассмотрим возможное альтернативное решение.

Коммутаторы уровня доступа - D-link DES-3200-52.

Коммутаторы уровня доступа с поддержкой технологии PoE - DES-1210-28P.

Стэкируемые коммутаторы уровня распределения/ядра - DGS-3324SR.

Коммутаторы с гигабитными портами SRV Switch и DMZ Switch - D-link DES-1228

В качестве межсетевого экрана возможно использовать бесплатное opensource решение с интегрированной функцией IPS на основе Snort. К примеру pfSense. Он же используется для построения VPN подключений.

В качестве E-mail Relay – бесплатное решение Postfix с бесплатным потоковым антивирусом Clam AV.

В роли прокси сервера выступает бесплатное ПО Squid.

В качестве IDS используется выделенный физический сервер установленной связкой Snort+Snorby.

Для обеспечения коммутации в виртуальной инфраструктуре используется бесплатный распределенный виртуальный коммутатор – Open vSwitch.

Для защиты виртуальной инфраструктуры может так же использоваться МЭ pfSense, установленный на виртуальной машине.

В таблице 7.2 представленная примерная спецификация

Таблица 7.2. Примерная спецификация сетевой инфраструктуры

Product	Description	Quan-tity	List Price (руб)	Selling Price (руб)
D-Link DES-3200-52	48 портовый коммутатор D-Link	2	18 000	36 000
DES-1210-28P	Коммутатор D-Link с поддержкой технологии PoE	1	13 000	13 000
DGS-3324SR	Стэкируемые коммутаторы D-Link L3	2	46 000	92 0000
D-link DES-1228	Гигабитные коммутаторы для серверов	2	7 500	15 000
		Итого:	**156 000 руб (4 500 $)**	

В представленной спецификации отсутствует серверное оборудование, необходимое для установки бесплатных opensource решений (МЭ, IPS), однако, даже не учитывая эти затраты, экономия – очевидна.

ЗАКЛЮЧЕНИЕ

Как было написано в самом начале, данное руководство не является абсолютной истиной и носит лишь рекомендательный характер. Все описанные решения основаны на личном опыте автора, с учетом лучших практик от компании Cisco (Cisco SAFE, Cisco SBA).

В следующих версиях данного руководства планируется осветить такие темы как:

- SIEM – системы;
- Мониторинг информационно-вычислительной сети;
- Централизованное управление сетевой инфраструктурой;
- Построение сети в виртуальной инфраструктуре;
- Актуализация ранее освещенных решений.

Автор искренне надеется, что данное руководство помогло читателям в структурировании полученных и уже известных знаний в области сетевых технологий.

По всем вопросам обращайтесь на электронный адрес **cooper051@yandex.ru**.