Образец содержит презентацию и доклад (речь на защиту)

Конфигурирование современной информационно-вычислительной сети объекта УИС

Презентация

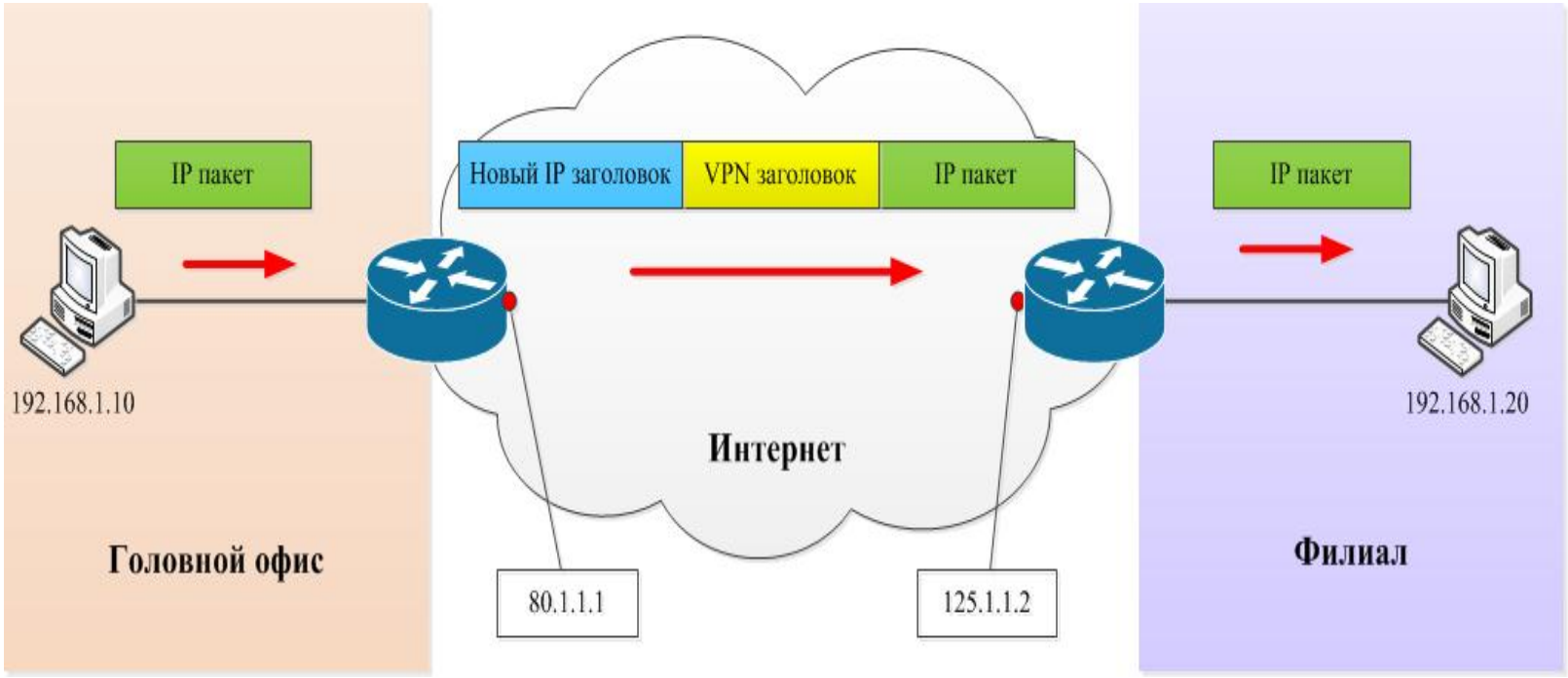
Цель

- Разработка и реализация локальной сети между сотрудниками, работающими удаленно от места постоянной дислокации учрежденияУИС при помощи общедоступных сетей

Задачи

- Провести теоретический обзор средств подключения удалённого доступа к локальным ресурсам вычислительной сети.
- Провести анализ подходов к конфигурированию современной информационно-вычислительной сети объекта УИС с реализацией безопасного удаленного доступа к ресурсам на предмет выявления оптимально применимого.
- Разработать конфигурацию современной информационно-вычислительной сети объекта УИС с реализацией безопасного удаленного доступа к ресурсам.
- Рассмотреть вопросы обеспечения безопасности жизнедеятельности при конфигурировании современной

VPN


IP пакет
Новый IP заголовок
VPN заголовок
IP пакет
IP пакет
192.168.1.10
Интернет
192.168.1.20
Головной офис
80.1.1.1
125.1.1.2
Филиал

Решаемые задачи

- Значительное упрощение процесса администрирования и поддержки пользователей;
- Организация защищенного доступа к критичной информации ФСИН с не доверенных узлов;
- Возможность применения на любых устройствах с выходом в Интернет без дополнительных сложных настроек.

Описание проекта

Простота использования.

Высокое качество соединения.

Высокая скорость соединения.

Безопасность работы.

Простота обслуживания.

Доступ к ресурсам в режиме реального времени.

ТопологияHub and Spoke (Client to Site).

Способ реализации – RemoteAccess.

Уровень модели OSI – Network.

Требования

Обеспечение доступа к общим сетевым ресурсам сотрудников, работающих удаленно от места постоянной дислокации учреждения,как к локальным ресурсам.

Защищённость канала путём шифрования[7].

ОтказоустойчивостьSLA/IKE Dead peerdetection/ State full IPSec.

Характеристики

Описание оборудования

Параметр	Значение
Тип устройства	Маршрутизатор
Возможность установки в стойку	Есть
Количество портов коммутатора	4 x Ethernet 10/100/1000 Мбит/сек
Web-интерфейс	Есть
Поддержка Telnet	Есть
Поддержка SNMP	Есть
WAN-порт	Есть
Межсетевой экран (Firewall)	Есть
NAT	Есть
SPI	Есть
DHCP-сервер	Есть
Поддержка Dynamic DNS	Есть
Статическая маршрутизация	Есть
Протоколы динамической маршрутизации	RIP v1, RIP v2
Поддержка VPN passthrough	Есть
Поддержка VPN-туннелей	Есть

Мониторинг

Zabbix

Grafana

Конец

- Спасибо за внимание

Слайд 1

Уважаемый председатель, уважаемые члены государственной аттестационной комиссии, Вашему вниманию предлагается дипломный проект на тему **«Конфигурирование современной информационно-вычислительной сети объекта УИС».**

Слайд 2

Актуальность темы выпускной квалификационной работы определяется тем, что в современном мире предъявляются все большие требования к мобильности в перемещении при организации совместной работы с данными, обработка которых осуществляется распределенным способом. Информационно-телекоммуникационные технологии интенсивно внедряемые в деятельность УИС реализованы в том числе на базе распределенных систем, а как известно вызовы, касающиеся обеспечения безопасности сведений, обрабатываемых автоматизировано являются приоритетными.

Наиболее эффективное решение по объединению удалённых рабочихмест в одну сеть при помощи каналов связи, проложенных через общедоступные сети связано с использованием технологиивиртуальных частных сетей (VirtualPrivateNetwork или VPN).

Исходя из этого, была сформированная цель работы «разработка и реализация локальной сети между сотрудниками, работающими удаленно от места постоянной дислокации учреждения УИС при помощи общедоступных сетей»

Слайд 3

Для достижения цели необходимо решить следующие задачи:

- Провести теоретический обзор средств подключения удалённого доступа к локальным ресурсам вычислительной сети.

- Провести анализ подходов к конфигурированию современной информационно-вычислительной сети объекта УИС с реализацией безопасного удаленного доступа к ресурсам на предмет выявления оптимально применимого.
- Разработать конфигурацию современной информационно-вычислительной сети объекта УИС с реализацией безопасного удаленного доступа к ресурсам.
- Рассмотреть вопросы обеспечения безопасности жизнедеятельности при конфигурировании современной информационно-вычислительной сети объекта УИС..

Слайд 4

В современных реалиях при постоянном прогрессе в области IT-сферы, в учреждениях УИС все больше уделяют внимание для модернизации существующих решений, а также для внедрения новых технологий.

На сегодняшний день на объектах УИС как правило для построения ИВС используется топология «звезда», либо ее разновидность. Реализованы как одноранговые, так и многоранговые сети, включающие в себя: сервера, сетевое оборудование, ИБП, АРМ, периферийные устройства. Внутри ИВС для облегчения работы сотрудникам и для ускорения электронного документа оборота, как правило разворачивают различные сервисы, такие как: ведомственная почта, файловое хранилище, сетевые информационные системы и т.д.

Современные технологии позволяют объединять удалённые сети и отдельные рабочие станции в одну корпоративную сеть при помощи общественных каналов связи по технологии VPN.

Слайд 5

Для подключения к сети ФСИН сотруднику необходим только Интернет-обозреватель, в котором необходимо указать адрес SSL VPN сервера ФСИН. После этого появляется сообщение с требованием аутентифицироваться и применяютсяполитики безопасности:

- Проверка на вредоносный код;
- Применение средств защиты и контроля (в том числе, удаление всех полученных файлов из сети ФСИН, после завершения сеанса) [1].
- После успешного прохождения процедур безопасности в Интернет-обозревателе становятся доступны ссылки для доступа к ресурсам ФСИН:
- к файловым серверам с возможностью передачи файлов на сервер [6];
- к Web-приложениям ФСИН (например, внутренний портал, OutlookWebAccess и т.п.);
- Терминальный доступ (MS, Citrix);
- Инструменты для администраторов (например, ssh консоль).
- Список доступных ссылок редактируется в зависимости от введенных пользователем данных в процессе аутентификации

Слайд 6

Объектом разработки является существующая локальная вычислительная сеть подразделения и сотрудника, работающего удаленно от места постоянной дислокации учреждения,организации:

- В настоящий момент в центральном подразделении организации существует внутренняя локальная сеть.
- В настоящий момент сотрудник имеет доступ к глобальной информационной сети.
- Во всех подразделениях может быть доставлено и установлено сетевое оборудование Cisco.

- Во всех подразделениях имеется доступ в сеть интернет.
- Организация доступа сотрудников, работающих удаленно от места постоянной дислокации учреждения,к ресурсам центрального подразделения отсутствует.

К проекту объекта ИВС предъявляются следующие требования, изложенные ниже.

Основное требование обеспечение качественной и безопасной связи:

- Простота использования.
- Высокое качество соединения.
- Высокая скорость соединения.
- Безопасность работы.
- Простота обслуживания.
- Доступ к ресурсам в режиме реального времени.
- ТопологияHub and Spoke (Client to Site).
- Способ реализации - RemoteAccess.
- Уровень модели OSI – Network.

Разрабатываемый продукт должен обладать следующими функциональными характеристиками:

- Обеспечение доступа к общим сетевым ресурсам сотрудников, работающих удаленно от места постоянной дислокации учреждения,как к локальным ресурсам.
- Защищённость канала путём шифрования.
- ОтказоустойчивостьSLA/IKE Dead peerdetection/ State full IPSec.

С учетом выполняемой роли в программной системе, к различным группам персонала предъявляются разные требования, без выполнения которых невозможно обеспечить надлежащее функционирование программной системы.

Слайд 7

В качестве сетевого оборудования был предоставлен маршрутизатор Cisco RV320 DualGigabit WAN VPN Router.

Слайд 8

Для своевременного и быстрого реагирования на все сбои оборудования, будем использовать систему мониторинга на базе Zabbix + Grafana.

Grafana является одним из самых известных инструментов с открытым исходным кодом для мониторинга и получения информации о нескольких источниках данных. Он хорошо известен своими красивыми панелями инструментов, где их можно легко настроить. Он может предоставлять удивительные графики и управлять оповещениями, чтобы помочь пользователю принять правильные меры.

Zabbix - это решение распределенного мониторинга корпоративного класса с открытыми исходными кодами.

Zabbix - это программное обеспечение для мониторинга многочисленных параметров сети, жизнеспособности и целостности серверов. Zabbix использует гибкий механизм оповещений, что позволяет пользователям конфигурировать уведомления основанные на e-mail практически для любого события. Это позволяет быстро реагировать на проблемы с серверами. Zabbix предлагает отличные функции отчетности и визуализации данных основанные на данных истории. Это делает Zabbix идеальным для планирования мощности.

Слайд 9

В результате данной работы была разработана и реализована виртуальная частная сеть между сотрудниками, работающими удаленно от места постоянной дислокации учрежденияи центральным учреждением

организации при помощи создания туннеля через сети общественного пользования (VPN). Для достижения цели были решены следующие задачи:

- Исследована информационно-техническая инфраструктура сети организации.
- Исследована теоретическая информация об организации виртуальных частных сетей.
- Исследованы правила настройки виртуальных частных сетей.
- Сделан выбор в пользу определённых технологий.
- Спроектирована виртуальная частная сеть между сотрудниками, работающими удаленно от места постоянной дислокации учреждения центральным учреждением с применением имеющегося программного и аппаратного обеспечения.

Таким образом, все задачи были выполнены, а цель работы достигнута.

Благодарю за внимание. Доклад окончен. Теперь я готов ответить на ваши вопросы.