

Программа и методика испытаний решений класса SD-WAN v 1.7

Оглавление

Используемые сокращения	3
Термины и определения	5
Введение	6
Цели	7
Объект тестирования	8
Перечень выполняемых проверок	11
Детальное описание тестов.....	16
Проверка архитектурных требований	16
Проверка функциональных требований	26

Используемые сокращения

Сокращение	Определение
AEAD	Authenticated Encryption with Associated Data
BGP	Border Gateway Protocol
CPE	Customer Premises Equipment
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DIA	Direct Internet Access
DSCP	Differentiated Services Code Point
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
KVM	Kernel-based Virtual Machine
L2/L3	Layer 2/Layer 3
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LTE	Long Term Evolution

MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
OFV	Open Virtualization Format
QEMU	Quick EMUlator
RAM	Random Access Memory
RFC	Request for Comments
RSTP	Rapid Spanning Tree Protocol
SD-WAN	Software-defined Wide Area Network
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
vCPE	Virtual Customer Premises Equipment
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtual Network Functions
VPN	Virtual Private Network
XML	eXtensible Markup Language
ZTP	Zero-touch Provisioning
OC	Операционная система

Термины и определения

Сокращение	Определение
Data Center Gateway	Шлюз центра обработки данных отвечает за обеспечение защищенного управления оборудованием CPE
Hub	Устройства CPE уровня Hub располагаются на центральных площадках и осуществляют транзит трафика между удаленными площадками. Работает через публичные IP адреса
Overlay	Автоматически построенные криптографические защищенные туннели управления и туннели передачи данных
SD-WAN Controller	Контроллер SD-WAN выполняет задачу управления оборудованием CPE и маршрутизацией в SD-WAN сети
Security Orchestrator	Оркестратор безопасности осуществляет управление виртуальными функциями безопасности на CPE (Security VNFs)
Spoke	Устройства CPE уровня Spoke находятся на удаленных площадках. Не требует наличия публичных IP адресов. Может находиться за любым типом NAT

Введение

В настоящем документе описана методика тестирования решений класса SD-WAN (Software-defined Wide Area Network), на основе которой производится тестирование решений данного класса.

Цели

Основная цель проведения работ — тестирование решений класса SD-WAN на соответствие требованиям технического задания заказчика для выбора максимально эффективного решения.

В ходе тестирования проверяются технические характеристики решений класса SD-WAN. Испытания проводятся на тестовом стенде Исполнителя. По результатам каждого теста фиксируется его выполнение или невыполнение, а также фиксируется значение измеряемой характеристики, где это применимо.

Задачи тестирования:

- разработка программы и методики испытаний;
- сборка, коммутация и настройка тестового стенда;
- выполнение тестирования систем, предлагаемых различными производителями;
- анализ полученных результатов и составление заключения.

Объект тестирования

Данная методика предназначена для тестирования решений класса SD-WAN на предмет соответствия требованиям технического задания заказчика.

Описание платформы

Тестирование выполняется на тестовом стенде Исполнителя с использованием его лабораторной инфраструктуры. Логическая и физическая схемы тестового стенда приведены на рисунках ниже.

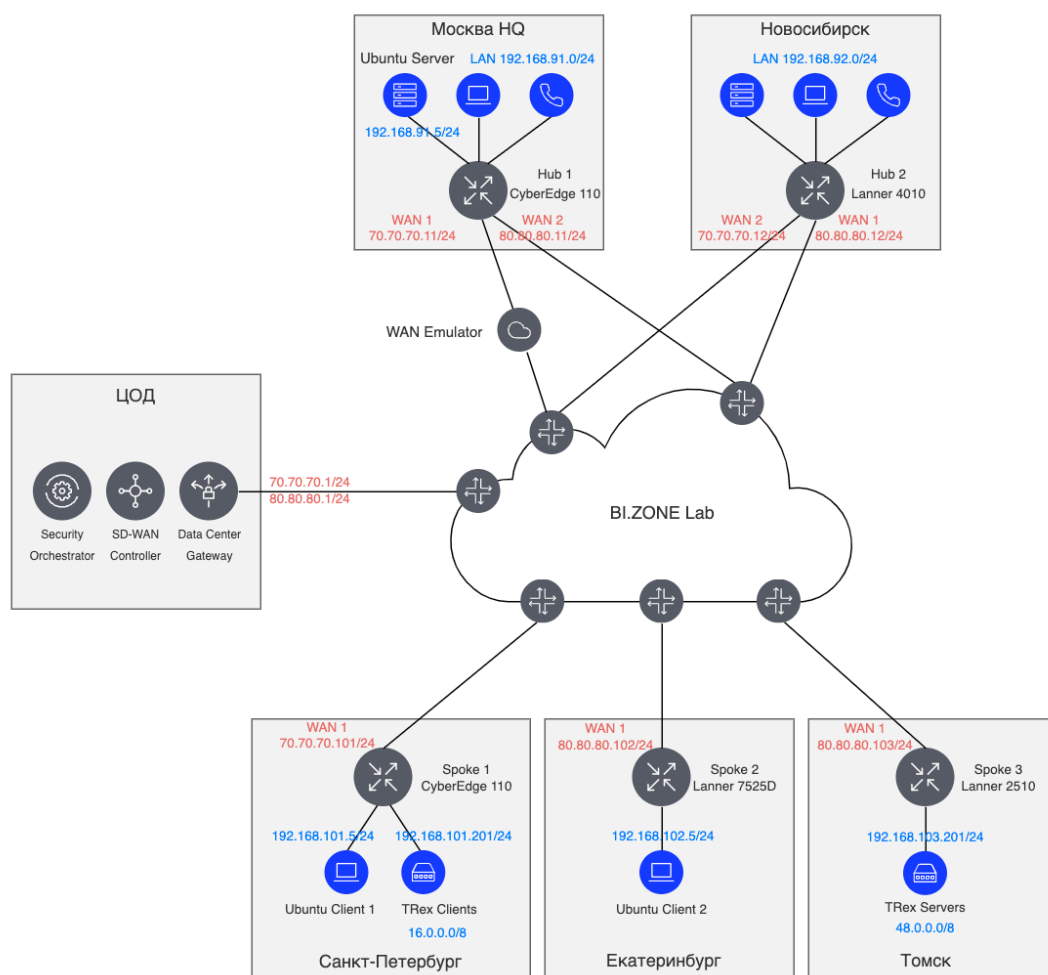


Рис. 1. Логическая схема тестового стенда

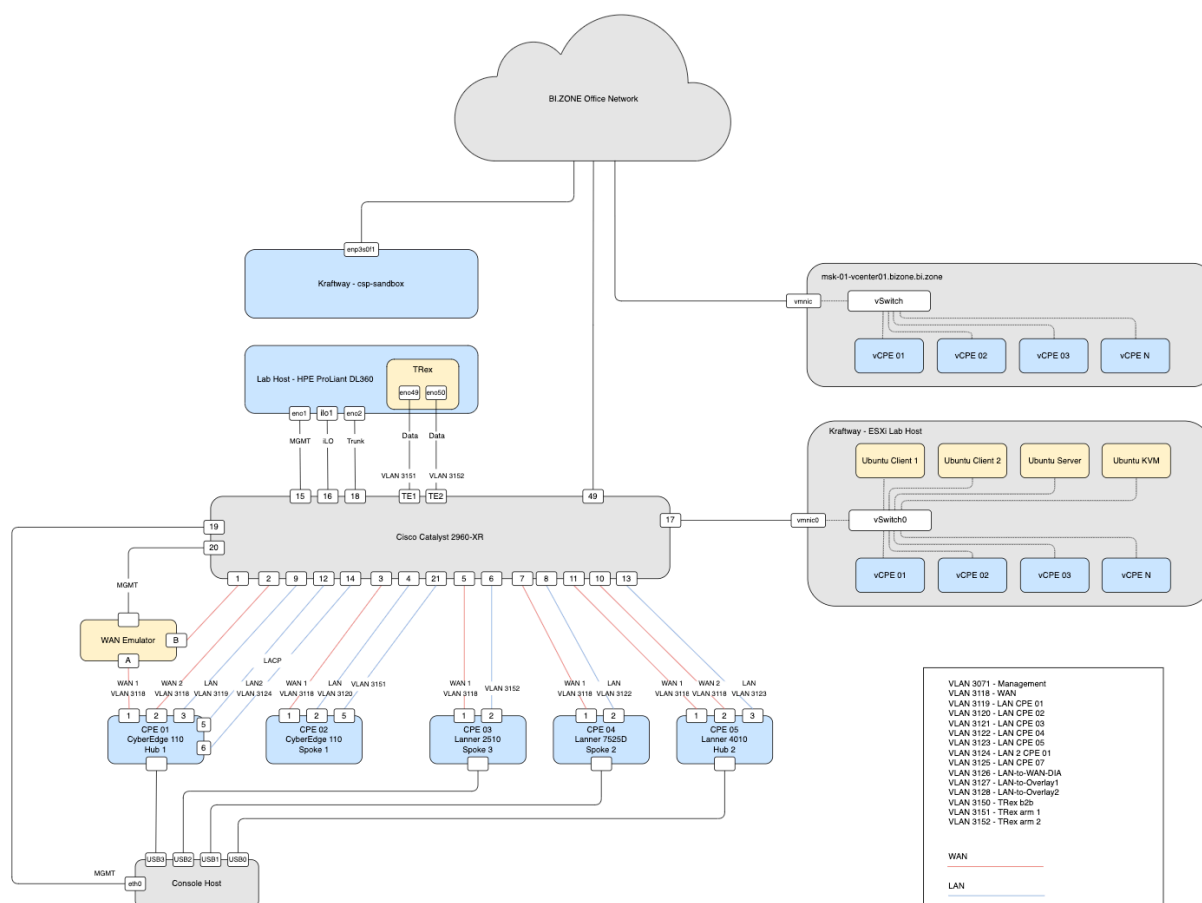


Рис. 2. Физическая схема тестового стенда

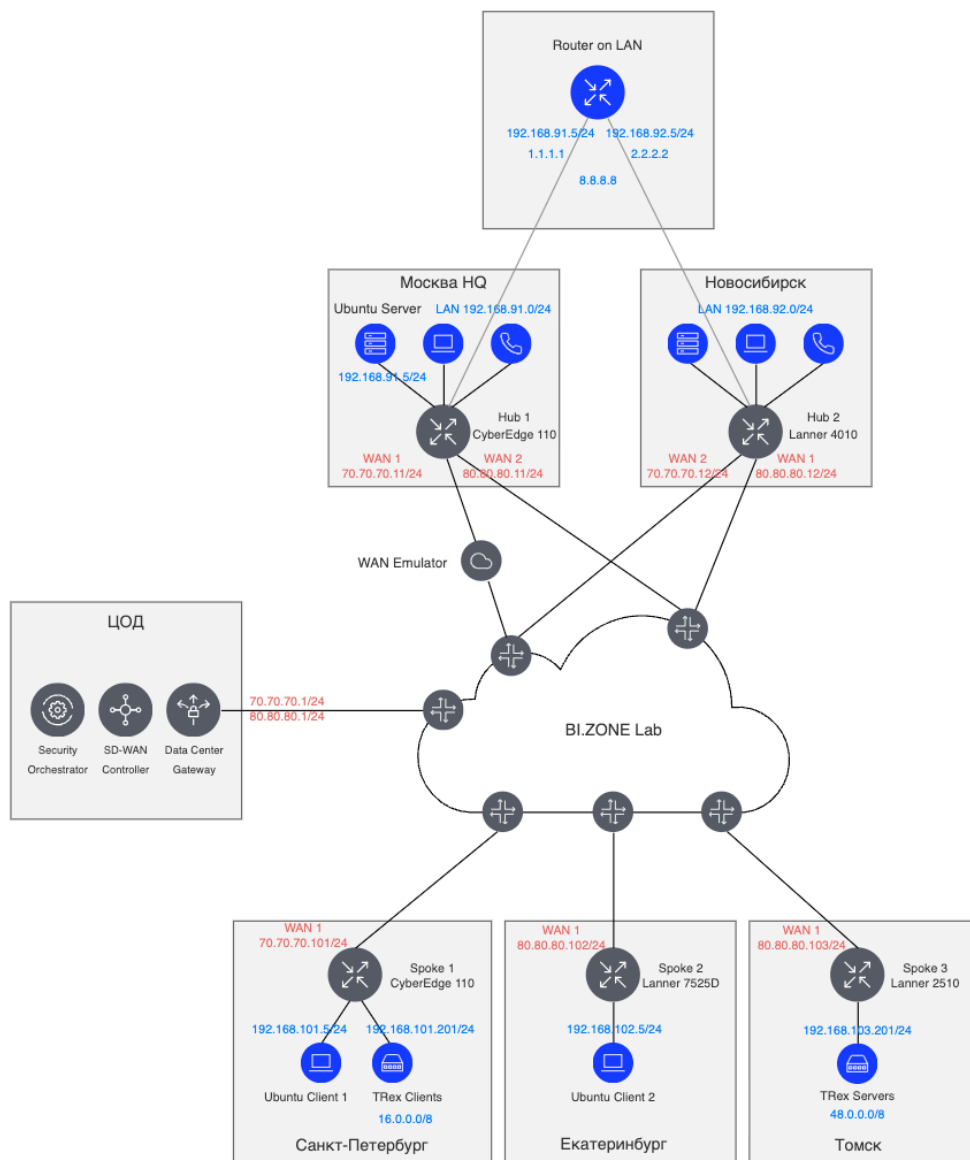


Рис. 3. Схема тестирования отказоустойчивости с помощью протокола BGP

Перечень выполняемых проверок

В ходе тестирования выполняются проверки, разделенные в соответствии со следующими категориями требований:

Архитектурные требования

1. Добавление пользователей системы с возможностью использования двухфакторной аутентификации (сертификат X.509 и логин/пароль). Управление сертификатами пользователей с возможностью их отзыва. Возможность привязки пользователей к сети определенного заказчика.
2. Создание аппаратной CPE в централизованной системе управления и активация с помощью ZTP с получением полной конфигурации и маршрутной информации.
3. Создание в централизованной системе управления CPE в формате виртуальной машины (VM) VMware и QEMU, активация с помощью ZTP с получением полной конфигурации и маршрутной информации.
4. Активация CPE, находящейся за NAT.
5. Создание в централизованной системе управления независимых и изолированных друг от друга сетей (проектов) с возможностью разграничения доступа к данным сетям (проектам).
6. Автоматическое создание криптографически защищенных туннелей управления через каждый локальный WAN интерфейс после создания и активации CPE.
7. Автоматическое создание криптографически защищенных туннелей передачи данных через каждый локальный WAN интерфейс после создания и активации CPE.
8. Поддержка пересечения подсетей на WAN интерфейсах CPE.
9. Автоматическая передача маршрутной информации на CPE через контроллер по защищенным каналам управления.
10. Возможность удаленного подключения пользователей с помощью защищенного соединения через WAN интерфейсы CPE уровня Hub. Поддержка подключения удаленных пользователей на базе устройств с различными ОС (Windows, Linux, macOS, iOS, Android).

11. Обработка пользовательского трафика должна осуществляться на CPE без его отправки в централизованную систему управления.
12. Решение должно обеспечивать отказоустойчивую работу по передаче пользовательского трафика на распределенной части сети при выходе из строя центрального контроллера и системы управления.
13. Централизованное анонсирование маршрута по умолчанию 0.0.0.0/0 с помощью протокола BGP. При наличии маршрута по умолчанию выход в интернет осуществляется через сетевой сервер уровня Hub, при его отсутствии, сетевые серверы уровня Spoke осуществляют выход в интернет самостоятельно.
14. Резервирование устройств уровня Hub. При отключении CPE уровня Hub, сетевые серверы уровня Spoke осуществляют автоматическую диагностику и переключение транзитных туннелей передачи данных через другой доступный Hub.
15. Резервирование доступа к LAN сетям на площадке с использованием протокола BGP. При отключении одной из CPE уровня Hub или Spoke, имеющей на LAN интерфейсах активные BGP соседства, контроллер должен удалить из таблицы маршрутизации все маршруты, полученные по BGP от данной CPE, и выслать всем доступным CPE обновленную таблицу маршрутизации от другой CPE на площадке, имеющей активные BGP соседства.
16. При отключении CPE уровня Spoke, не имеющей на LAN интерфейсах BGP соседств, контроллер должен удалить из таблицы маршрутизации все маршруты, полученные от данной CPE, и выслать всем доступным CPE обновленную таблицу маршрутизации.
17. Сброс конфигурации CPE.

Функциональные требования

18. Возможность агрегации интерфейсов Ethernet на LAN портах сетевого сервера с использованием стандартного протокола LACP для обеспечения отказоустойчивости физических каналов.
19. Поддержка VLAN тегирования на WAN и LAN интерфейсах сетевого сервера в режимах Access/Trunk.
20. Поддержка протокола RSTP на LAN интерфейсах сетевого сервера.
21. Поддержка работы LAN портов сетевого сервера в режиме L3 с возможностью настройки IP адреса на интерфейсе.

22. Возможность работы в режиме DHCP Client на WAN интерфейсах сетевого сервера.
23. Возможность работы в режиме DHCP Server на LAN интерфейсах сетевого сервера.
24. Создание статических маршрутов с возможностью их автоматического анонсирования на всю сеть.
25. Контроль пересечений адресных пространств при создании L3 интерфейса на LAN портах сетевого сервера.
26. Поддержка протокола BGP с возможностью установления сессии с другими сетевыми устройствами и получения маршрутов от них.
27. Анонсирование маршрутов, полученных по протоколу BGP, на всю сеть, в том числе на другие CPE, не имеющих активных BGP сессий.
28. Автоматическое переключение на резервный канал при отказе основного канала связи.
29. Автоматический мониторинг качества каналов связи с возможностью переключения на резервные каналы при достижении определенных порогов деградации качества. Данные пороги должны быть регулируемы.
30. Поддержка классификации трафика по его типу с возможностью установления порогов по потерям в канале связи для переключения трафика определенного класса на резервные каналы связи. Поддержка не менее 7 пользовательских классов с собственными порогом.
31. Мониторинг и отображение в едином интерфейсе управления параметров производительности CPE, а также качества её каналов связи, включая:
 - загрузка CPU (исторический график)
 - загрузка RAM (исторический график)
 - загрузка WAN интерфейсов
 - загрузка LAN интерфейсов
 - количество VPN трафика (исторический график)
 - количество DIA-трафика (исторический график)
 - количество трафика управления Control Plane (исторический график)

- характеристика качества каждого WAN канала (исторический график)
32. Поддержка отправки на CPE атомарных (единичных) изменений конфигурации с возможностью проверки статуса их выполнения.
 33. Наличие виртуальной сетевой функции защиты VNF Firewall на CPE с возможностью локальной обработки всего трафика в соответствии с настроенными политиками безопасности.
 34. Поддержка создания политик безопасности на основе:
 - групп интерфейсов, объединенных в зоны
 - сетевых сервисов (протоколов)
 - адресных групп
 35. Поддержка версионирования конфигурации межсетевого экрана с возможностью применения одной из предыдущих версий конфигурации (commit and rollback).
 36. Возможность импорта в VNF Firewall и использования списков доверенных и недоверенных IP адресов (black and white lists).
 37. При настройке политик безопасности межсетевого экрана использование в качестве применяемого действия NAT-трансляцию с возможностью указания трансляции в пул адресов, а также в Input interface IP address.
 38. Мониторинг и отображение текущего статуса всех виртуальных сетевых функций защиты в едином интерфейсе управления.
 39. Создание и редактирование шаблонов устройств CPE с возможностью настройки необходимого количества системных ресурсов (CPU, Disk, RAM), количества медных и оптических интерфейсов, а также настройки различных типов WAN интерфейсов.
 40. Аудит всех действий администраторов и пользователей в централизованной системе управления.
 41. Возможность внесения изменений и настройки конфигурации на недоступной или отключенной в данный момент CPE. После включения и активации CPE, на контроллере есть возможность проверки статуса выполнения внесенных изменений конфигурации.
 42. Поддержка современных стандартов и алгоритмов шифрования трафика с возможностью шифрования по ГОСТ.

-
43. Сетевой сервер должен иметь в наличии не менее шести интерфейсов 10/100/1000 Mbps Ethernet.
 44. Сетевой сервер должен поддерживать работу стандарта Wi-Fi 802.11 n на LAN интерфейсах.
 45. Сетевой сервер должен поддерживать работу стандарта LTE на WAN интерфейсах.

Детальное описание тестов

Проверка архитектурных требований

- 1. Добавление пользователей системы с возможностью использования двухфакторной аутентификации (сертификат X.509 и логин/пароль).
Управление сертификатами пользователей с возможностью их отзыва.
Возможность привязки пользователей к сети определенного заказчика.**

Описание

Участник испытаний создает учетную запись пользователя в системе управления, назначает ему пароль и прикрепляет его к одному из существующих в системе заказчиков. Далее участник скачивает пользовательский сертификат X.509 и производит вход в систему под данной учетной записью. Проверяется, что созданному пользователю доступны только проекты заказчика, к которому он прикреплен.

Далее в системе управления создается другой пользователь с собственным сертификатом. Проверяется, что с сертификатом первого пользователя невозможно авторизоваться в системе управления используя логин и пароль второго пользователя.

Далее сертификат первого пользователя отзывается и выполняется попытка повторной авторизации в системе под первым пользователем.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность создание пользователей с поддержкой двухфакторной аутентификации (X.509 сертификат + логин/пароль). Комбинация логин/пароль каждого пользователя может использоваться только совместно с сертификатом данного пользователя. Пользователю, прикрепленному к сети определенного заказчика доступны только проекты данного заказчика. Авторизации в системе после отзыва сертификата оказалась unsuccessful.

- 2. Создание аппаратной CPE в централизованной системе управления и активация с помощью ZTP с получением полной конфигурации и маршрутной информации.**

Описание

Участник испытаний в централизованной системе управления создает новую CPE из шаблона согласно используемой модели CPE и задает в настройке необходимые настройки WAN и LAN интерфейсов. После чего генерируется ссылка активации данной площадки. Участник подключается к CPE через LAN интерфейс, дожидается получения адреса от CPE по DHCP, после чего переходит по данной ссылке активации. Проверяется успешная активация CPE в контроллере, а также наличие и статус туннелей передачи данных и маршрутов до всех IP адресов, существующих в данной сети. Все настройки, связанные с туннелями передачи данных и распространением маршрутной информации должны быть сгенерированы для всех CPE автоматически и не требовать действий администратора. Тест повторяется для нескольких CPE, в результате теста в системе должны быть заведены не менее 1 устройства типа Hub и не менее 2 устройств типа Spoke.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность создания и активация аппаратной CPE в централизованной системе управления с помощью ZTP. Активированные CPE имеют полную конфигурацию и маршрутную информацию, туннели передачи данных построены и находятся в работоспособном состоянии.

3. Создание в централизованной системе управления CPE в формате виртуальной машины (VM) VMware и QEMU, активация с помощью ZTP с получением полной конфигурации и маршрутной информации.

Описание

Участник испытаний производит установку CPE в формате VM в соответствующей виртуальной инфраструктуре. Используются гипервизор VMware ESXi версии 6.5 или выше и гипервизор QEMU/KVM. Далее в контроллере создается виртуальная площадка с необходимыми параметрами и генерируется ссылка активации данной площадки.

Участник подключается к системе управления VMware vSphere и выбирает опцию Deploy OFV Template, указывает необходимые параметры развертывания и в заключительном окне вводит ссылку активации данной CPE. Проверяется успешная активация CPE в контроллере.

Участник осуществляет запуск виртуальной машины в QEMU/KVM с помощью XML файла, содержащего необходимые параметры развертывания VM. После чего ссылка активации CPE передается с хоста (гипервизора) на LAN интерфейс vCPE. Проверяется успешная активация CPE в контроллере.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность создания и активации в централизованной системе управления виртуальных CPE в формате виртуальной машины VMware и QEMU.

4. Активация CPE, находящейся за NAT.

Описание

Произвольная CPE размещается на стенде за маршрутизатор или межсетевой экран, выполняющей Source NAT трансляцию в сторону сети «Интернет» стенда. Таким образом эмулируется типовая ситуация, когда любое соединение может быть организовано только со стороны CPE. Участник испытаний в централизованной системе управления создает новую CPE типа Spoke из шаблона согласно используемой модели CPE и задает необходимые настройки WAN и LAN интерфейсов. После чего генерируется ссылка активации данной площадки. Участник подключается к CPE через LAN интерфейс, дожидается получения адреса от CPE по DHCP, после чего переходит по данной ссылке активации. Проверяется успешная активация CPE в контроллере, а также наличие и статус туннелей передачи данных и маршрутов до всех IP адресов, существующих в данной сети. Все настройки, связанные с туннелями передачи данных и распространением маршрутной информации должны быть сгенерированы для всех CPE автоматически и не требовать действий администратора.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность активации CPE, находящейся за NAT (CGNAT) в централизованной системе управления с помощью ZTP. Активированные CPE имеют полную конфигурацию и маршрутную информацию, туннели передачи данных построены и находятся в работоспособном состоянии.

5. Создание в централизованной системе управления независимых и изолированных друг от друга сетей (проектов) с возможностью разграничения доступа к данным сетям (проектам).

Описание

Участник испытаний в графическом интерфейсе централизованной системы управления создает два проекта и активирует в каждом из этих проектов по две CPE. После создания и активации всех CPE в контроллере участник демонстрирует, что CPE, включенные в первый проект недоступны во втором проекте и наоборот. CPE, находящиеся в одном проекте построили туннели передачи данных между собой. CPE, находящиеся в разных проектах не строят туннели передачи данных между собой.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность создания независимых друг от друга участков. CPE, находящиеся в разных проектах изолированы друг от друга и не строят туннели передачи данных между собой.

6. Автоматическое создание криптографически защищенных туннелей управления через каждый локальный WAN интерфейс после создания и активации CPE.

Описание

Участник испытаний в централизованной системе управления создает виртуальную площадку с двумя WAN интерфейсами и указывает на них IP адреса. После чего генерируется ссылка активации данной площадки. Участник подключается к CPE через LAN интерфейс и переходит по данной ссылке активации. Проверяется успешная активация CPE в контроллере. Демонстрируется, что CPE автоматически построила криптографически защищенные туннели управления с каждого локального WAN интерфейса к централизованной системе управления.

С помощью утилиты tcpdump или Wireshark проверяется отсутствие незашифрованных данных в канале управления.

Аппаратным или программным путем отключается основной канал связи CPE. Проверяется, что управление CPE возможно через резервный канал связи (при наличии IP связности через резервный канал связи с системой управления). CPE должна переключать управление на резервный канал без использования динамических протоколов маршрутизации на WAN интерфейсах.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность автоматического создания криптографически защищенных туннелей

управления через каждый локальный WAN интерфейс после создания и активации CPE. CPE должна автоматически выбирать работоспособный туннель управления без необходимости настройки динамических протоколов на WAN.

7. Автоматическое создание криптографически защищенных туннелей передачи данных через каждый локальный WAN интерфейс после создания и активации CPE.

Описание

Участник испытаний в централизованной системе управления создает виртуальную площадку с двумя WAN интерфейсами и указывает на них IP адреса. После чего генерируется ссылка активации данной площадки. Участник подключается к CPE через LAN интерфейс и переходит по данной ссылке активации. Проверяется успешная активация CPE в контроллере. Демонстрируется, что CPE автоматически построила криптографически защищенные туннели передачи данных с каждого локального WAN интерфейса на каждый активный WAN интерфейс всех существующих в данной сети CPE уровня Hub.

С помощью утилиты tcpdump или Wireshark проверяется отсутствие незашифрованных данных в канале передачи данных.

Аппаратным или программным путем отключается основной канал связи CPE. Проверяется, что передача данных возможна через резервный канал связи (при наличии IP связности через резервный канал связи с хотя бы одним Hub). CPE должна переключать трафик на резервный канал без использования динамических протоколов маршрутизации на WAN интерфейсах.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность автоматического создания криптографически защищенных туннелей передачи данных через каждый локальный WAN интерфейс после создания и активации CPE. CPE должна автоматически выбирать работоспособный туннель передачи данных без необходимости настройки динамических протоколов на WAN.

8. Поддержка пересечения подсетей на WAN интерфейсах CPE.

Описание

На WAN интерфейсах CPE настраивается адресация из одной подсети, например, 192.168.5.2/24. На стороне каналаобразующего оборудования данных WAN

настраивается шлюз из той же подсети и Source NAT трансляция в сторону сети «Интернет» стенда. Таким образом эмулируется типовая ситуация, когда на стороне оператора связи установлен модем с типовыми настройками по умолчанию. Проверяется успешная работа CPE через оба канала связи, а также наличие и статус туннелей передачи данных и маршрутов до всех IP адресов, существующих в данной сети.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность работы CPE через каналы связи, имеющие пересекающуюся адресацию на последней миле.

9. Автоматическая передача маршрутной информации на CPE через контроллер по защищенным каналам управления.

Описание

Участник испытаний в централизованной системе управления открывает настройки ранее созданной CPE и проверяет наличие маршрутной информации на данной CPE. После чего на другой CPE, находящейся в данной сети, производится добавление статического маршрута. Демонстрируется, что первая CPE через защищенные каналы управления получила новый маршрут от второй CPE автоматически.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность автоматической передачи маршрутной информации на CPE через контроллер по защищенным каналам управления.

10. Возможность удаленного подключения пользователей с помощью защищенного соединения через WAN интерфейсы CPE уровня Hub. Поддержка подключения удаленных пользователей на базе устройств с различными ОС (Windows, Linux, macOS, iOS, Android).

Описание

Участник испытаний производит настройку подключения VPN клиента к CPE уровня Hub на произвольных ОС из списка: Windows, Linux, macOS, iOS, Android.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность удаленного подключения пользователей с помощью защищенного соединения через WAN интерфейсы CPE уровня Hub. Продемонстрирована поддержка подключения устройств с различными ОС (Windows, Linux, macOS, iOS, Android).

11. Обработка пользовательского трафика должна осуществляться на CPE без его отправки в централизованную систему управления.

Описание

Участник испытаний производит предварительную настройку системы для работы сети, состоящей из двух CPE уровня Spoke, с транзитом через Hub. К каждому из Spoke в LAN интерфейс подключены порты генератора трафика. На генераторе трафика ставится задача по отправке легитимного HTTP-трафика объемом 100 Мбит/с через сеть SD-WAN. В разделе мониторинга каналов связи централизованной системы управления сравнивается количество трафика, проходящего по каналам передачи данных и по каналам управления. Показания системы мониторинга проверяются с помощью утилиты tcpdump или через счетчики на интерфейсах оборудования стенда.

Результат

Тест считается успешно пройденным, если участник подтвердил, что обработка пользовательского трафика осуществляется на CPE без его отправки в централизованную систему управления. Каналы передачи данных загружены на ~100 Мбит/с, при этом каналы управления имеют значительно меньшую загрузку.

12. Решение должно обеспечивать отказоустойчивую работу по передаче пользовательского трафика на распределенной части сети при выходе из строя центрального контроллера и системы управления.

Описание

Участник испытаний производит предварительную настройку системы для работы сети, состоящей из двух CPE уровня Spoke, с транзитом через Hub. К каждому из Spoke в LAN интерфейс подключены по одному хосту, находящиеся в разных подсетях, но имеющие связность друг с другом через сеть SD-WAN. С первого хоста отправляются HTTP GET запросы на второй хост, в ответ на которые

приходят ответы с кодом 200 ОК. Далее участник производит отключение центрального контроллера и системы управления путем выключения сервера или виртуальной машины, либо путем разрыва логической связности между контроллером и распределенной частью сети. В течение 5 минут после отключения контроллера проверяется отсутствие потерь легитимного трафика между хостами.

Результат

Тест считается успешно пройденным, если участник продемонстрировал отказоустойчивую работу по передаче пользовательского трафика на распределенной части сети при выходе из строя центрального контроллера и системы управления. Потери в легитимном трафике между хостами в течение 5 минут после отключения контроллера не зафиксированы.

13. Централизованное анонсирование маршрута по умолчанию 0.0.0.0/0 с помощью протокола BGP. При наличии маршрута по умолчанию выход в интернет осуществляется через сетевой сервер уровня Hub, при его отсутствии, сетевые серверы уровня Spoke осуществляют выход в интернет самостоятельно.

Описание

Участник испытаний производит настройку связности между CPE уровня Hub и CPE уровня Spoke. На Hub дополнительно производится настройка централизованного анонсирования маршрута по умолчанию 0.0.0.0/0 с помощью протокола BGP. На CPE уровня Spoke проверяется наличие в таблице маршрутизации маршрута по умолчанию, полученного с Hub. Далее производится отключение CPE уровня HUB. На Spoke проверяется отсутствие маршрута по умолчанию, полученного ранее с Hub, а также проверяется возможность локального выхода в интернет.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность централизованного выхода в Интернет, через Hub а также возможность локального выхода в интернет с CPE уровня Spoke при отключении CPE уровня Hub.

14. Резервирование устройств уровня Hub. При отключении CPE уровня Hub, сетевые серверы уровня Spoke осуществляют автоматическую

диагностику и переключение транзитных туннелей передачи данных через другой доступный Hub.*Описание*

Участник испытаний производит настройку сети, состоящей из двух CPE уровня Spoke, подключенным к двум CPE уровня Hub. На Spoke проверяется наличие туннелей передачи данных через Hub 1 и Hub 2, при этом маршруты через Hub 1 являются более приоритетными. Далее производится отключение Hub 1, после чего на Spoke проверяется отсутствие туннелей передачи данных через Hub 1, при этом для передачи трафика используются туннели через Hub 2.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность резервирования устройств уровня Hub. CPE уровня Spoke осуществили автоматическую диагностику и переключение транзитных туннелей передачи данных через Hub 2 после отключения Hub 1.

15. Резервирование доступа к LAN сетям на площадке с использованием протокла BGP. При отключении одной из CPE уровня Hub или Spoke, имеющей на LAN интерфейсах активные BGP соседства, контроллер должен удалить из таблицы маршрутизации все маршруты, полученные по BGP от данной CPE, и выслать всем доступным CPE обновленную таблицу маршрутизации от другой CPE на площадке, имеющей активные BGP соседства.

Описание

Участник испытаний производит настройку сети, состоящей из двух CPE уровня Spoke, подключенных к двум CPE уровня Hub. На LAN интерфейсах Hub 1 и Hub 2 настроены активные BGP сессии с клиентским маршрутизатором на площадке, через которые в сеть анонсируются маршруты. На Spoke 1 проверяется наличие маршрутов, полученных от Hub 1. Далее производится отключение Hub 1 и на Spoke 1 проверяется обновленная таблица маршрутизации, где маршрутов, полученных от Hub 1 больше нет, при этом в таблице маршрутизации есть маршрут, полученный от Hub 2 по протоколу BGP.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность резервирования доступа к LAN сетям на площадке с использованием

протокола BGP. Маршруты, полученные по BGP от Hub 1 после отключения данной CPE, отсутствуют в обновленной таблице маршрутизации на Spoke 1, при этом в таблице маршрутизации есть маршрут, полученный от Hub 2 по протоколу BGP.

16. При отключении CPE уровня Spoke, не имеющей на LAN интерфейсах BGP соседств, контроллер должен удалить из таблицы маршрутизации все маршруты, полученные от данной CPE, и выслать всем доступным CPE обновленную таблицу маршрутизации.

Описание

Участник испытаний производит настройку сети, состоящей из двух CPE уровня Spoke, подключенных к одной CPE уровня Hub. На Spoke 1 производится добавление статического маршрута, который автоматически анонсируется по сети. На Spoke 2 проверяется наличие данного маршрута. Далее участник производит следующие настройки:

1. На Spoke 1 отключается связность между CPE и контроллером путем создания запрещающего данный обмен ACL или иным путем. При этом таблица маршрутизации на Spoke 2 содержит маршруты, полученные от Spoke 1, трафик между Spoke успешно передается.
2. Производится выключение Spoke 1, при этом на всей сети отзываются маршруты, полученные с данной CPE. На Spoke 2 в обновленной таблице маршрутизации отсутствуют маршруты от Spoke 1.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность резервирования устройств уровня Spoke. Все маршруты, полученные от Spoke 1 отзываются после выключения данной CPE. При этом перебои связи между CPE и контроллером не влияют на анонсирование данных маршрутов.

17. Сброс конфигурации CPE.

Описание

Участник испытаний производит сброс конфигурации CPE к заводской с использованием аппаратной кнопки на CPE, а также через веб-интерфейс управления. После чего в веб-интерфейсе данная CPE удаляется и создается новая CPE. Далее генерируется ссылки активации новой CPE и применяется на ранее сброшенное к заводской конфигурации устройство.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность сброса конфигурации CPE программным и аппаратным путем с последующей переактивацией данной CPE.

Проверка функциональных требований

18. Возможность агрегации интерфейсов Ethernet на LAN портах сетевого сервера с использованием стандартного протокола LACP для обеспечения отказоустойчивости физических каналов.

Описание

Участник испытаний производит настройку агрегации интерфейсов на LAN портах сетевого сервера с использованием протокола LACP. В качестве ответной стороны используется произвольный коммутатор, поддерживающий стандартный протокол LACP. После настройки на CPE и коммутаторе проверяется статус агрегированного канала.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность агрегации интерфейсов Ethernet на LAN портах сетевого сервера с использованием стандартного протокола LACP. На обоих устройствах статус агрегированного канала Active (Enabled).

19. Поддержка VLAN тегирования на WAN и LAN интерфейсах сетевого сервера в режимах Access/Trunk.

Описание

Участник испытаний в централизованной системе управления производит настройку VLAN тегирования на WAN и LAN интерфейсах сетевого сервера в режимах Access/Trunk, при этом в одном VLAN должно находиться не менее двух физических портов.

Результат

Тест считается успешно пройденным, если участник продемонстрировал поддержку VLAN тегирования на WAN и LAN интерфейсах сетевого сервера в режимах Access/Trunk.

20. Поддержка протокола RSTP на LAN интерфейсах сетевого сервера.

Описание

Участник испытаний производит настройку протокола RSTP на LAN интерфейсе сетевого сервера. В качестве ответной стороны используется произвольный коммутатор, поддерживающий стандартный протокол RSTP. После настройки на обоих устройствах проверяется статус RSTP.

Результат

Тест считается успешно пройденным, если участник продемонстрировал поддержку протокола RSTP на LAN интерфейсах сетевого сервера. На обоих устройствах статус RSTP на настраиваемых портах в режиме Active (Enabled).

21. Поддержка работы LAN портов сетевого сервера в режиме L3 с возможностью настройки IP адреса на интерфейсе.

Описание

Участник испытаний в централизованной системе управления производит настройку LAN порта в режиме L3 и назначает на соответствующем интерфейсе IP адрес.

Результат

Тест считается успешно пройденным, если участник продемонстрировал поддержку работы LAN портов сетевого сервера в режиме L3 с возможностью настройки IP адреса на интерфейсе.

22. Возможность работы в режиме DHCP Client на WAN интерфейсах сетевого сервера.

Описание

Участник испытаний в централизованной системе управления производит настройку режима работы DHCP Client на WAN интерфейсе сетевого сервера, после чего данный интерфейс подключается в сеть, где настроен DHCP Server. Проверяется автоматическое назначение IP адреса на WAN интерфейсе с помощью протокола DHCP.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность работы в режиме DHCP Client на WAN интерфейсе сетевого сервера. WAN интерфейс автоматически получил IP адрес по протоколу DHCP.

23. Возможность работы в режиме DHCP Server на LAN интерфейсах сетевого сервера.

Описание

Участник испытаний в централизованной системе управления производит настройку режима работы DHCP Server на LAN интерфейсе сетевого сервера, после чего данный интерфейс подключается в сеть, где находится хост, сетевой интерфейс которого настроен в режиме DHCP Client. Проверяется автоматическое назначение IP адреса на сетевом интерфейсе хоста с помощью протокола DHCP, при этом полученный IP адрес соответствует настроенному пулу адресов на LAN интерфейсе CPE.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность работы в режиме DHCP Server на LAN интерфейсе сетевого сервера. Целевой хост получил IP адрес по протоколу DHCP из настроенного на LAN интерфейсе пула адресов.

24. Создание статических маршрутов с возможностью их автоматического анонсирования на всю сеть.

Описание

Участник испытаний производит настройку сети, состоящей из двух CPE уровня Spoke, подключенных к одной CPE уровня Hub. На Spoke 1 проверяется наличие маршрутной информации, после чего на Spoke 2 производится добавление статического маршрута без его анонсирования. Таблица маршрутизации на Spoke 1 должна остаться прежней. Далее на Spoke 2 производится добавление ещё одного статического маршрута с анонсированием по сети. Проверяется обновленная таблица маршрутизации на Spoke 1, второй статический маршрут должен быть получен от Spoke 2 автоматически.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность создания статических маршрутов с возможностью их автоматического

анонсирования на всю сеть. Второй статический маршрут получен на Spoke 1 автоматически.

25. Контроль пересечений адресных пространств при создании L3 интерфейса на LAN портах сетевого сервера.

Описание

Участник испытаний в централизованной системе управления производит настройку одного из LAN портов в режиме L3 и назначает на соответствующем интерфейсе IP адрес. После чего на другом LAN порту назначается IP адрес из той же подсети, который был назначен на предыдущем порту. Система должна сообщить о пересечении адресов и не позволить создать второй L3 интерфейс в одном и том же адресном пространстве.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность контроля пересечений адресных пространств при создании L3 интерфейсов на LAN портах сетевого сервера. Второй L3 интерфейс в одном и том же адресном пространстве создать не удалось.

26. Поддержка протокола BGP с возможностью установления сессии с другими сетевыми устройствами и получения маршрутов от них.

Описание

Участник испытаний в централизованной системе управления открывает настройки ранее созданной CPE и проверяет наличие маршрутной информации на данной CPE. После чего на стороне LAN настраивается BGP соседство с другим сетевым устройством и проверяется обновленная таблица маршрутизации, которая должна содержать маршруты, полученные по протоколу BGP.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность установления сессии по протоколу BGP с другими сетевыми устройствами и возможность получения маршрутов от них.

27. Анонсирование маршрутов, полученных по протоколу BGP, на всю сеть, в том числе на другие CPE, не имеющих активных BGP сессий.

Описание

Участник испытаний производит настройку сети, состоящей из двух CPE уровня Spoke, подключенных к одной CPE уровня Hub. На Spoke 2 проверяется текущая таблица маршрутизации и проверяется отсутствие активных BGP сессий. После чего на LAN интерфейсе Hub настраивается BGP соседство с другим сетевым устройством, при этом настраивается редистрибуция маршрутов, полученных по протоколу BGP, в сторону других CPE, на которых BGP процесс выключен. Далее на CPE уровня Spoke проверяется обновленная таблица маршрутизации, которая должна содержать новые маршруты, полученные от Hub.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность анонсирования маршрутов, полученных по протоколу BGP, на всю сеть, в том числе на другие CPE, которые не имеют активных BGP сессий.

28. Автоматическое переключение на резервный канал при отказе основного канала связи.

Описание

Участник испытаний производит настройку сети, состоящей из не менее одной CPE уровня Hub, имеющей два WAN канала и не менее одной CPE уровня Spoke. На Hub проверяется наличие туннелей передачи данных через данные каналы, при этом маршруты через WAN 1 назначаются более приоритетными.

Участник устанавливает интервал проверки работоспособности канала связи в значение 100 мс. На промежуточном коммутаторе выполняется логическая блокировка трафика на канале Hub WAN 1 (например, переводом порта в другой VLAN или с помощью WAN эмулятора). После чего на Hub проверяется, что канал связи был автоматически переключен на резервный и для передачи данных используются туннели, построенные через WAN 2. Время переключения на резервный канал должно составлять не более 1 секунды.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность автоматического переключения на резервные каналы при отказе основного канала. Канал передачи данных был автоматически переключен с WAN 1 на WAN 2 при отказе WAN 1 за время, не превышающее 1 секунду.

29. Автоматический мониторинг качества каналов связи с возможностью переключения на резервные каналы при достижении определенных порогов деградации качества. Данные пороги должны быть регулируемыми.

Описание

Участник испытаний производит настройку сети, состоящей из не менее одной CPE уровня Hub, имеющей два WAN канала и не менее одной CPE уровня Spoke. На Hub проверяется наличие туннелей передачи данных через данные каналы, при этом маршруты через WAN 1 назначаются более приоритетными.

1. Участник устанавливает пороговое значение на максимальное количество потерь в канале в размере 1%. На WAN эмуляторе, установленном на канале WAN 1, настраивается значение потерь в канале связи в размере 2% от объема передаваемого трафика. После чего на Hub проверяется, что при достижении установленного порога, канал связи был автоматически переключен на резервный и для передачи данных используются туннели, построенные через канал WAN 2.
2. Участник устанавливает пороговое значение на максимальную величину задержки передачи пакетов в канале в размере 100 мс. На WAN эмуляторе, установленном на канале WAN 1, настраивается величина задержки в канале связи в размере 110 мс. После чего на Hub проверяется, что при достижении установленного порога, канал связи был автоматически переключен на резервный и для передачи данных используются туннели, построенные через канал WAN 2.
3. Участник устанавливает пороговое значение на максимальную величину джиттера в канале в размере 30 мс. На WAN эмуляторе, установленном на канале WAN 1, настраивается значение джиттера в канале связи в размере 40 мс. После чего на Hub проверяется, что при достижении установленного порога, канал связи был автоматически переключен на резервный и для передачи данных используются туннели, построенные через канал WAN 2.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность автоматического мониторинга качества каналов связи с возможностью переключения на резервные каналы при достижении определенного порога потерь трафика в канале связи, задержек передачи пакетов и джиттера. Канал передачи данных был автоматически переключен с WAN 1 на WAN 2 при достижении установленных порогов.

30. Поддержка классификации трафика по его типу с возможностью установления порогов по потерям в канале связи для переключения трафика определенного класса на резервные каналы связи. Поддержка не менее 7 пользовательских классов с собственными пороговыми значениями.

Описание

Участник испытаний производит настройку сети, состоящей из не менее одной CPE уровня Spoke, имеющей два WAN канала и не менее одной CPE уровня Hub. На Spoke проверяется наличие туннелей передачи данных через данные каналы, при этом маршруты через WAN 1 назначаются более приоритетными.

На Spoke производится настройка, осуществляющая классификацию трафика по его типу и для класса Voice (определяемого как DSCP EF) устанавливается порог в 100 мс задержки в канале связи. Также проверяется возможность настройки не менее 7 пользовательских классов с собственными пороговыми значениями и возможность классификации трафика с помощью следующих параметров:

- DSCP
- Src/dst IP
- L4 protocol + TCP/UDP ports

С клиентского хоста, подключенного к Spoke 1, запускается трафик через Hub 1 до клиентского хоста, подключенного к Spoke 2. Трафик должен иметь значение DSCP равное 46. На WAN эмуляторе, установленном в канале WAN 1, выставляется значение задержки в канале связи в размере 200 мс. После чего на Spoke 1 проверяется, что при достижении установленного порога, канал связи был автоматически переключен на резервный и для передачи данных класса Voice используются туннели, проходящие через WAN 2. Данное правило должно применяться только к трафику, попадающему под класс Voice.

Результат

Тест считается успешно пройденным, если участник продемонстрировал поддержку классификации трафика по его типу с возможностью установления порогов по потерям в канале связи для переключения трафика определенного класса на резервные каналы связи. Продемонстрирована поддержка не менее 7 пользовательских классов с настройкой собственных пороговых значений. Канал передачи данных был автоматически переключен с WAN 1 на WAN 2 при достижении установленного порога.

31. Мониторинг и отображение в едином интерфейсе управления параметров производительности CPE, а также качества её каналов связи, включая:

- **загрузка CPU (исторический график)**
- **загрузка RAM (исторический график)**
- **текущая загрузка WAN интерфейсов**
- **текущая загрузка LAN интерфейсов**
- **количество VPN трафика (исторический график)**
- **количество DIA трафика (исторический график)**
- **количество трафика управления Control Plane (исторический график)**
- **характеристика качества каждого WAN канала (исторический график)**

Описание

Участник испытаний в графическом интерфейсе централизованной системы управления заходит в раздел мониторинга параметров производительности CPE и качества её каналов связи и демонстрирует отображение указанных в требовании параметров.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность мониторинга и отображения в едином интерфейсе управления параметров производительности CPE, а также качества её каналов связи по всем указанным в требовании параметрам.

32. Поддержка отправки на CPE атомарных (единичных) изменений конфигурации с возможностью проверки статуса их выполнения.

Описание

Участник испытаний в централизованной системе управления открывает настройки ранее созданной CPE и производит изменение в конфигурации, например изменение IP адреса на LAN интерфейсе. После чего в централизованной системе управления проверяется статус выполнения данного изменения конфигурации. При

этом на CPE была отправлена только команда на изменение данного IP адреса (и связанных настроек), а не запрос на полное обновление конфигурации устройства.

Результат

Тест считается успешно пройденным, если участник продемонстрировал поддержку отправки на CPE атомарных (единичных) изменений конфигурации с возможностью проверки статуса их выполнения в централизованной системе управления.

33. Наличие виртуальной сетевой функции защиты VNF Firewall на CPE с возможностью локальной обработки всего трафика в соответствии с настроенными политиками безопасности.

Описание

Участник испытаний в централизованной системе управления создает виртуальную площадку из шаблона и задает в настройке необходимые параметры. После чего генерируется ссылка активации данной площадки. Участник подключается к CPE через LAN интерфейс и переходит по данной ссылке. Проверяется успешная активация CPE в контроллере, а также наличие автоматически развернутого VNF Firewall на данной CPE. VNF Firewall находится в активном состоянии и имеет ряд предустановленных правил, которые по умолчанию разрешают только минимально необходимые взаимодействия. Для проверки работоспособности политик безопасности, включенных по умолчанию, запускаются Ping (ICMP) и Traceroute (UDP) запросы между различными сегментами.

Результат

Тест считается успешно пройденным, если участник продемонстрировал наличие виртуальной сетевой функции защиты VNF Firewall на CPE с возможностью локальной обработки всего трафика в соответствии с настроенными политиками безопасности. Политики безопасности по умолчанию активированы автоматически и производят фильтрацию трафика.

34. Поддержка создания политик безопасности на основе:

- **групп интерфейсов, объединенных в зоны**
- **сетевых сервисов (протоколов)**
- **адресных групп**

Описание

Участник испытаний в централизованной системе управления открывает настройки ранее созданной CPE и переходит в раздел создания политик безопасности. Производится создание трех новых политик безопасности на основе: 1) групп интерфейсов, объединенных в зоны, 2) сетевых сервисов (протоколов), 3) на основе адресных групп.

Результат

Тест считается успешно пройденным, если участник продемонстрировал поддержку создания политик безопасности указанными способами. Новые политики безопасности созданы и находятся в активном состоянии.

35. Поддержка версионирования конфигурации межсетевого экрана с возможностью применения одной из предыдущих версий конфигурации (commit and rollback).

Описание

Участник испытаний в централизованной системе управления открывает настройки ранее созданной CPE и переходит в раздел создания политик безопасности. Производится создание новой политики безопасности, которая применяется в системе (Apply), но не подтверждается (Commit) в установленное на это время. При этом уже примененные, но неподтвержденные за установленное время изменения конфигурации межсетевого экрана отменяются (Rollback). Проверяется наличие в централизованной системе управления истории всех изменений и возможности отката к произвольному историческому состоянию.

Результат

Тест считается успешно пройденным, если участник продемонстрировал поддержку версионирования конфигурации межсетевого экрана с возможностью применения одной из предыдущих версий конфигурации (commit and rollback). Созданная политика применилась, но так как за установленное время она не была подтверждена, данная политика была отменена.

36. Возможность импорта в VNF Firewall и использования списков доверенных и недоверенных IP адресов (black and white lists).

Описание

Участник испытаний в централизованной системе управления открывает настройки ранее созданной CPE и переходит в раздел настройки политик безопасности. Создается и импортируется в систему список недоверенных IP адресов.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность импорта в VNF Firewall и использования списков доверенных и недоверенных IP адресов (black and white lists). Созданный black list создан и успешно импортирован. Трафик к/от адресов из загруженного списка блокируется.

37. При настройке политик безопасности межсетевого экрана использование в качестве применяемого действия NAT трансляцию с возможностью указания трансляции в пул адресов, а также в Input interface IP address.

Описание

Участник испытаний в централизованной системе управления открывает настройки ранее созданной CPE и переходит в раздел создания политик безопасности. Создается два правила, в первом в качестве действия для трафика, попадающего под данное правило, назначается NAT трансляция в задаваемый пул адресов, а во втором правиле назначается NAT трансляция в Input interface IP address.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность при настройке политик безопасности межсетевого экрана использования в качестве применяемого действия NAT трансляцию с возможностью указания трансляции в пул адресов, а также в Input interface IP address. Оба правила успешно созданы и находятся в активированном состоянии.

38. Мониторинг и отображение текущего статуса всех виртуальных сетевых функций защиты в едином интерфейсе управления.

Описание

Участник испытаний в централизованной системе управления открывает раздел мониторинга и отображения текущего статуса виртуальных сетевых функций защиты и демонстрирует наличие следующей информации по каждому из VNF: тип и версия VNF, статус синхронизации конфигурации, дата последней синхронизации конфигурации.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность мониторинга текущего статуса всех виртуальных сетевых функций защиты в едином интерфейсе управления, а также возможность отображения всей дополнительной информации о каждом VNF.

39. Создание и редактирование шаблонов устройств CPE с возможностью настройки необходимого количества системных ресурсов (CPU, Disk, RAM), количества медных и оптических интерфейсов, а также настройки различных типов WAN интерфейсов.

Описание

Участник испытаний в централизованной системе управления заходит в раздел создания шаблонов устройств CPE и открывает ранее созданный шаблон аппаратной CPE для его редактирования. Производится изменение шаблона, например, меняется количество WAN портов с 1 на 2 порта, после чего измененный шаблон успешно сохраняется. Далее участник создает новый шаблон виртуальной CPE с указанием названия "QEMU" и добавляет 3 LAN порта для данной vCPE.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность создания и редактирования шаблонов устройств CPE с возможностью настройки необходимого количества системных ресурсов (CPU, Disk, RAM), количества медных и оптических интерфейсов, а также настройки различных типов WAN интерфейсов. Шаблон аппаратной CPE был успешно отредактирован, шаблон виртуальной CPE успешно создан.

40. Аудит всех действий администраторов и пользователей в централизованной системе управления.

Описание

Участник испытаний в централизованной системе управления демонстрирует возможность аудита всех действий администраторов и пользователей системы, для чего с помощью учетной записи администратора системы производится изменение конфигурации CPE — изменение IP адреса одного из LAN интерфейсов, создание нового пользователя системы, изменение политики безопасности.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность аудита всех действий администраторов и пользователей в централизованной системе управления. Все внесенные изменения в конфигурацию устройства отображены в журнале аудита. Должна отсутствовать возможность очистки журналов аудита администраторами.

41. Возможность внесения изменений и настройки конфигурации на недоступной или отключенной в данный момент CPE. После включения и активации CPE, на контроллере есть возможность проверки статуса выполнения внесенных изменений конфигурации.

Описание

Участник испытаний в централизованной системе управления выключает одну из ранее созданных CPE. Участник убеждается, что CPE отключена и недоступна в системе, после чего производит изменение в конфигурации данной CPE, например изменение IP адреса на LAN интерфейсе. После изменения конфигурации CPE включается и в централизованной системе управления проверяется текущий статус CPE, который должен сообщать, что устройство вновь активно, а также проверяется статус выполнения внесенных ранее изменений конфигурации.

Результат

Тест считается успешно пройденным, если участник продемонстрировал возможность внесения изменений и настройки конфигурации на недоступной или отключенной в данный момент CPE. После включения и активации CPE, отображается статус внесенных ранее изменений конфигурации.

42. Поддержка современных стандартов и алгоритмов шифрования трафика с возможностью шифрования по ГОСТ.

Описание

Участник испытаний в централизованной системе управления создает два новых проекта:

1. Без использования отечественных алгоритмов шифрования.
2. С использованием шифрования по ГОСТ.

Для проверки автоматического создания криптографически защищенных туннелей управления и туннелей передачи данных в каждый проект добавляется и активируется по две CPE.

На каждой CPE должны поддерживаться следующие алгоритмы:

Алгоритмы симметричного шифрования:

- ChaCha20 с поддержкой RFC7539 AEAD (или аналог с поддержкой AEAD и стойкостью не хуже указанного)
- ГОСТ Р 34.12–2015 (Кузнечик)

Аутентификация:

- Poly1305 с поддержкой RFC7539 AEAD (или аналог с поддержкой AEAD и стойкостью не хуже указанного)
- Р 1323565.1.026–2019 (режим MGM с поддержкой AEAD)

Хеширование:

- BLAKE2s (RFC7693) (или аналог)
- ГОСТ Р 34.11-2012

К произвольным CPE в LAN интерфейсы подключаются клиентские хосты и запускается пользовательский трафик через сеть SD-WAN. С помощью утилиты tcpdump или Wireshark проверяется отсутствие незашифрованных данных в канале передачи данных.

Результат

Тест считается успешно пройденным, если участник продемонстрировал поддержку всех указанных алгоритмов шифрования. В канале передачи данных отсутствует незашифрованный трафик данных.

43. Сетевой сервер должен иметь в наличии не менее шести интерфейсов 10/100/1000 Mbps Ethernet.

Описание

Участник испытаний демонстрирует наличие на сетевом сервере не менее шести интерфейсов 10/100/1000 Mbps Ethernet.

Результат

Тест считается успешно пройденным, если участник продемонстрировал наличие на сетевом сервере не менее шести интерфейсов 10/100/1000 Mbps Ethernet.

44. Сетевой сервер должен поддерживать работу стандарта Wi-Fi 802.11 n на LAN интерфейсах.

Описание

Участник испытаний в централизованной системе управления производит настройку стандарта Wi-Fi 802.11 n на LAN интерфейсе, после чего для проверки производится подключение хоста к CPE с помощью Wi-Fi. После установления беспроводного соединения и получения IP адреса на хосте выполняется проверка версии стандарта Wi-Fi.

Результат

Тест считается успешно пройденным, если участник продемонстрировал поддержку работы стандарта Wi-Fi 802.11 n на LAN интерфейсах сетевого сервера.

45. Сетевой сервер должен поддерживать работу стандарта LTE на WAN интерфейсах.

Описание

Тест производится при наличии SIM карт и доступа к стенду из сети мобильного оператора.

Участник испытаний в централизованной системе управления производит настройку LTE на WAN интерфейсе, после чего для проверки производится подключение CPE к сети мобильного оператора с помощью LTE.

Результат

Тест считается успешно пройденным, если участник продемонстрировал поддержку работы стандарта LTE на WAN интерфейсах сетевого сервера.