**Intecso Edge 2.0. Руководство пользователя**

**1. Общие сведения о системе Intecso Edge 2.0**

Edge — это программно-определяемая сетевая платформа, обеспечивающая следующие возможности:

* **Маршрутизация:** Поддержка статической и динамической маршрутизации (OSPF, BGP, RIP).
* **Межсетевой экран (Firewall):** На основе iptables/nftables для управления трафиком, фильтрации пакетов и организации безопасного периметра.
* **NAT:** Преобразование адресов и портов для интеграции с внешними сетями.
* **VPN:** Поддержка множества протоколов (IPsec, OpenVPN, WireGuard) для безопасного подключения удаленных филиалов и мобильных пользователей.
* **QoS и Policy-based routing:** Тонкая настройка приоритетов трафика.
* **Журналирование и мониторинг:** Возможность контроля состояния сети, анализ логов, экспорт данных на внешние системы.
* **Шифрование по ГОСТ:** Поддержка российских криптографических стандартов, что особенно актуально для организаций, обязанных использовать ГОСТ-алгоритмы шифрования.

Edge ориентирован на CLI-конфигурацию в стиле JunOS/Cisco IOS. Конфигурация системы хранится в текстовом виде и может быть версионирована, что упрощает аудит изменений. Команды настройки вводятся в режиме конфигурации (configure), изменения применяются командой commit, а сохранение — save. По умолчанию аутентификация осуществляется учетными записями локальных пользователей.

**2. Первоначальный доступ к системе**

Предполагается, что вы уже вошли в систему под пользователем с правами администратора (обычно edge). При первом запуске стоит изменить пароль по умолчанию, если вы этого еще не сделали:

bash

configure

set system login user edge authentication plaintext-password 'НовыйПароль'

commit

save

Таким образом, вы обеспечите базовую защиту устройства. Далее рекомендуется настроить доступ по SSH для удаленного администрирования (если требуется):

bash

configure

set service ssh port 22

set service ssh listen-address 192.168.1.1

commit

save

Вы можете настроить аутентификацию по SSH-ключам для более безопасного доступа без пароля:

bash

configure

set system login user edge authentication public-keys mykey key "ssh-rsa AAAAB3NzaC1y..."

set system login user edge authentication public-keys mykey type ssh-rsa

commit

save

**3. Настройка сетевых интерфейсов и базовой маршрутизации**

Перед началом развертывания сложной инфраструктуры важно правильно настроить интерфейсы. Предположим, у вас есть два интерфейса: eth0 для WAN и eth1 для LAN.

Назначим статический адрес на LAN-интерфейс:

bash

configure

set interfaces ethernet eth1 address 192.168.10.1/24

commit

save

Если необходимо, настроим WAN-интерфейс под DHCP:

bash

configure

set interfaces ethernet eth0 address dhcp

commit

save

При необходимости статической маршрутизации (например, если нужно указать статический маршрут к другой подсети):

bash

configure

set protocols static route 10.10.10.0/24 next-hop 192.168.10.254

commit

save

Для доступа в интернет часто требуется маршрут по умолчанию (если ваш провайдер назначает вам шлюз динамически через DHCP, маршрут по умолчанию будет настроен автоматически). Если же требуется вручную задать маршрут по умолчанию:

bash

configure

set protocols static route 0.0.0.0/0 next-hop 203.0.113.1

commit

save

**4. Управление брандмауэром (Firewall) и NAT**

Firewall в Edge позволяет создавать набор правил для входящего, исходящего и проходящего трафика. Правила объединяются в имена (имена firewall-сетов), которые привязываются к интерфейсам.

Пример: разрешим входящий SSH только с определенного адреса 203.0.113.10, остальной трафик отбрасываем:

bash

configure

set firewall name WAN\_LOCAL default-action drop

set firewall name WAN\_LOCAL rule 10 action accept

set firewall name WAN\_LOCAL rule 10 protocol tcp

set firewall name WAN\_LOCAL rule 10 destination port 22

set firewall name WAN\_LOCAL rule 10 source address 203.0.113.10

set interfaces ethernet eth0 firewall local name WAN\_LOCAL

commit

save

Таким образом, мы защищаем Edge от несанкционированного доступа по SSH.

Для NAT (например, если нам нужно скрыть частную сеть за одним публичным IP):

bash

configure

set nat source rule 100 outbound-interface eth0

set nat source rule 100 source address 192.168.10.0/24

set nat source rule 100 translation address masquerade

commit

save

Это позволит всем хостам в сети 192.168.10.0/24 выходить в Интернет под IP-адресом, назначенным интерфейсу eth0.

**5. ГОСТ-шифрование и VPN**

Одной из ключевых особенностей Intecso Edge 2.0 является поддержка шифрования по российским стандартам ГОСТ. Это может быть востребовано в организациях, где регулятивные или внутренние нормативы требуют использовать ГОСТ-алгоритмы шифрования (например, ГОСТ Р 34.12-2015 для блочного шифрования, ГОСТ Р 34.10-2012 для электронно-цифровой подписи и т.д.).

**5.1 Поддержка ГОСТ в криптосистеме Intecso Edge 2.0**

Edge изначально использует стандартные пакеты strongSwan или OpenVPN для VPN, WireGuard для легковесных соединений, а также SSL/TLS для веб-сервисов. Расширенная сборка с поддержкой ГОСТ позволяет выбирать ГОСТ-алгоритмы шифрования и аутентификации в конфигурации IPsec и, в перспективе, других VPN-протоколов.

**5.2 Настройка IPsec с ГОСТ**

Рассмотрим пример настройки IPsec-туннеля между двумя площадками (Site-to-Site VPN), где требуется шифрование трафика по ГОСТ. Предположим, у нас есть два узла: Edge-A (публичный IP: 203.0.113.5) и Edge-B (публичный IP: 198.51.100.10), и мы хотим соединить сети 192.168.10.0/24 на стороне A и 172.16.20.0/24 на стороне B.

**Шаги:**

1. **Генерация ГОСТ-сертификатов и ключей:**

Предполагается, что вы уже сгенерировали сертификаты и ключи по ГОСТ, используя криптобиблиотеки, поддерживающие ГОСТ (например, OpenSSL с плагинами ГОСТ). Ключи и сертификаты нужно разместить в /config/auth/ на каждой стороне.

1. **Настройка IPsec-фаз:**

Для ГОСТ, в зависимости от поддерживаемых алгоритмов, можно указать не стандартные AES/SHA, а ГОСТ-алгоритмы, например gost-mac, gost-28147-89 и т.д.

На стороне Edge-A:

bash

configure

# Определяем фазы IKE (фаза 1)

set vpn ipsec ike-group GOST-IKE proposal 1 encryption gost-28147-89

set vpn ipsec ike-group GOST-IKE proposal 1 hash gost-28147-89-mac

set vpn ipsec ike-group GOST-IKE lifetime 3600

set vpn ipsec ike-group GOST-IKE key-exchange ikev2

# Определяем фазы ESP (фаза 2)

set vpn ipsec esp-group GOST-ESP proposal 1 encryption gost-28147-89

set vpn ipsec esp-group GOST-ESP proposal 1 hash gost-28147-89-mac

set vpn ipsec esp-group GOST-ESP lifetime 3600

# Конфигурация peer

set vpn ipsec site-to-site peer 198.51.100.10 authentication mode rsa

set vpn ipsec site-to-site peer 198.51.100.10 authentication remote-id "edge-b.example.com"

set vpn ipsec site-to-site peer 198.51.100.10 local-address 203.0.113.5

set vpn ipsec site-to-site peer 198.51.100.10 ike-group GOST-IKE

set vpn ipsec site-to-site peer 198.51.100.10 esp-group GOST-ESP

set vpn ipsec site-to-site peer 198.51.100.10 authentication id "edge-a.example.com"

set vpn ipsec site-to-site peer 198.51.100.10 authentication certificate /config/auth/edge-a\_cert.pem

set vpn ipsec site-to-site peer 198.51.100.10 authentication private-key /config/auth/edge-a\_key.pem

# Указываем сети

set vpn ipsec site-to-site peer 198.51.100.10 tunnel 1 local prefix 192.168.10.0/24

set vpn ipsec site-to-site peer 198.51.100.10 tunnel 1 remote prefix 172.16.20.0/24

commit

save

exit

Аналогичные настройки производятся на стороне Edge-B, где в качестве peer будет указан адрес Edge-A. Важно, чтобы используемые алгоритмы шифрования и аутентификации совпадали.

1. **Проверка состояния VPN:**  
   Используйте команду show vpn ipsec sa, чтобы убедиться, что тоннель установлен, а шифрование и аутентификация по ГОСТ функционируют корректно.

**5.3 Использование ГОСТ в OpenVPN**

Если вы хотите использовать ГОСТ-шифрование в OpenVPN (при условии, что ваша сборка Intecso Edge 2.0 поддерживает соответствующие патчи и параметры), укажите ГОСТ-цифросистему в конфигурации OpenVPN. Пример (для справки, может отличаться в зависимости от версии):

bash

configure

set interfaces openvpn vtun0 mode server

set interfaces openvpn vtun0 tls encryption gost-tls

# Указываем сертификаты ГОСТ

set interfaces openvpn vtun0 tls ca-cert-file /config/auth/gost\_ca.pem

set interfaces openvpn vtun0 tls cert-file /config/auth/gost\_server\_cert.pem

set interfaces openvpn vtun0 tls key-file /config/auth/gost\_server\_key.pem

commit

save

exit

Теперь трафик по каналу OpenVPN будет шифроваться ГОСТ-алгоритмами, если клиент также их поддерживает.

**6. Расширенные возможности маршрутизации**

**6.1 Динамические протоколы**

Edge поддерживает OSPF, BGP и другие протоколы маршрутизации. Например, настройка OSPF:

bash

configure

set protocols ospf area 0 network 192.168.10.0/24

set protocols ospf parameters router-id 192.168.10.1

commit

save

BGP-настройки схожи: указываем автономную систему, соседа, сети:

bash

configure

set protocols bgp 65001 neighbor 203.0.113.6 remote-as 65002

set protocols bgp 65001 network 192.168.10.0/24

commit

save

**6.2 Policy-based routing**

Если требуется маршрутизировать отдельный трафик через другой шлюз в зависимости от источника или протокола:

bash

configure

set policy route-map CUSTOM permit 10 match ip address prefix-list SPECIAL\_NET

set policy route-map CUSTOM permit 10 set next-hop 203.0.113.50

set policy prefix-list SPECIAL\_NET rule 10 action permit

set policy prefix-list SPECIAL\_NET rule 10 prefix 192.168.99.0/24

commit

save

Далее применяем эту политику к интерфейсу или демону маршрутизации.

**7. Управление учетными записями, аутентификацией и безопасностью доступа**

Edge позволяет создавать нескольких пользователей, задавать им пароли или ключи:

bash

configure

set system login user admin authentication plaintext-password 'AdminPass'

set system login user admin level admin

commit

save

Для интеграции с внешними системами аутентификации (например, RADIUS или TACACS+) можно настроить соответствующие параметры:

bash

configure

set system login radius-server 203.0.113.100 key "secret"

set system login radius-server 203.0.113.100 source-address 192.168.10.1

set system login radius-server 203.0.113.100 authentication-port 1812

commit

save

**8. Мониторинг, журналирование и диагностика**

**8.1 Логи системы**

Логи в Intecso Edge 2.0 по умолчанию пишутся в /var/log/. Для управления объемом логов и уровнями логирования используются системные настройки. Можно перенаправить логи на удаленный syslog-сервер:

bash

configure

set system syslog host 192.168.10.200 facility all level info

commit

save

**8.2 Диагностика**

Используйте команды:

* show interfaces для просмотра состояния интерфейсов.
* show ip route для отображения таблицы маршрутизации.
* ping, traceroute для диагностики сетевых проблем.
* show vpn ipsec sa для проверки состояния IPsec.
* show vpn l2tp или show vpn openvpn для проверки состояния VPN.

**8.3 SNMP и мониторинг**

Если необходимо мониторить устройство через SNMP:

bash

configure

set service snmp community "public" authorization ro

set service snmp community "public" network 192.168.10.0/24

commit

save

Это позволит вашему мониторинговому серверу (например, Zabbix, Nagios) собирать показатели о состоянии системы.

**9. Обновление системы и резервное копирование**

Edge поддерживает обновление через образы и пакеты. Рекомендуется перед обновлением сохранять текущую конфигурацию:

bash

show configuration commands | tee /config/config\_backup.txt

Позднее вы можете восстановить конфигурацию, выполнив команды из этого файла. Рекомендуется регулярно делать резервные копии и хранить их в безопасном месте.

При обновлении убедитесь, что версия Intecso Edge 2.0 поддерживает ваш криптопровайдер для ГОСТ и сохранит совместимость с существующими VPN-туннелями. Обновление может потребовать перезагрузки.

**10. Организация кластеризации и отказоустойчивости (HA)**

Для повышения надежности Intecso Edge 2.0 поддерживает протоколы VRRP (Virtual Router Redundancy Protocol). Это позволяет организовать отказоустойчивую пару маршрутизаторов Edge:

bash

configure

set high-availability vrrp group G1 interface eth1

set high-availability vrrp group G1 address 192.168.10.254/24

set high-availability vrrp group G1 vrid 10

set high-availability vrrp group G1 priority 100

commit

save

При сбое одного узла, второй возьмет на себя его роль.

**11. Дополнительные возможности и советы по эксплуатации**

* **Версионирование конфигурации:**  
  Конфигурация Intecso Edge 2.0 — это текстовый файл. Вы можете хранить его в системе контроля версий (Git) для отслеживания изменений. Это упростит возврат к предыдущим настройкам.
* **Автоматизация и Ansible:**  
  Intecso Edge 2.0 можно автоматизировать с помощью Ansible или других инструментов DevOps. Скрипты Ansible, взаимодействующие с Edge, позволяют массово применять конфигурации, делать бэкапы, обновления.
* **API и управление:**  
  Новые версии Intecso Edge 2.0 могут иметь API для интеграции с внешними системами управления, оркестраторами. Это особенно полезно в крупных сетевых инфраструктурах.
* **Оптимизация производительности:**  
  При высоких нагрузках стоит обратить внимание на железо. Используйте сетевые карты с аппаратным ускорением, отключайте неиспользуемые службы, настраивайте очереди (RPS/RFS), рассмотрите настройку QoS.
* **Шифрование на уровне L2/L3:**  
  Кроме ГОСТ для IPsec, вы можете использовать GRE-over-IPsec и другие комбинации туннелей. При этом ГОСТ может использоваться для реализации IPsec поверх GRE, обеспечивая совместимость с существующей инфраструктурой.
* **Высокая доступность Crypto:**  
  Если ваш сценарий требует непрерывного VPN, рассмотрите кластеризацию с несколькими узлами Intecso Edge 2.0. Это повысит надежность VPN с ГОСТ-шифрованием.

**12. Безопасность и соответствие требованиям**

Использование ГОСТ-шифрования накладывает на вас определенные организационные и технические требования. Обязательно убедитесь, что вы используете сертифицированные криптосредства, соответствующие стандартам, и что выбранные ГОСТ-алгоритмы корректно согласованы с партнерами по VPN. Перед разворачиванием в продуктивной среде может потребоваться консультация с аудиторами или специалистами по информационной безопасности.

Обновляйте систему своевременно, проверяйте настройки firewall, используйте минимально необходимые права доступа для пользователей. Защитите консоль устройства физическим образом (в случае аппаратного решения).

**13. Поддержка, документация и сообщество**

* **О нас:** https://www.intecso.pro/#about\_us
* **Наши контакты:** https://www.intecso.pro/#contacts
* **Продукция:** https://www.intecso.pro/#PRS