Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Keenetic в офисе 10-50 РМ: наш стандарт настройки

Сегменты 802.1Q, Multi-WAN с Ping Check, IKEv2 и WireGuard, SNMP и syslog

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Офис на 10-50 РМ обычно живёт на одном плоском /24 и одном канале: принтеры, камеры, гостевой Wi-Fi и серверы 1С в общем broadcast-домене, VPN на самоподписанном сертификате, резерва нет. Обрыв провайдера или заражённый ноутбук в гостевой сети останавливает кассу и обмен с банком. Мы приводим периметр к схеме: сегменты, приоритеты каналов с автопроверкой, VPN и логи наружу.

Почему это важно бизнесу

- Простой канала = остановка 1С, эквайринга и ЭДО: час без интернета стоит дороже второго провайдера за год
- Плоская сеть: заражение гостевого ноутбука сразу достаёт до файлового сервера и бэкапов
- Пароль от Wi-Fi на стикере не отзывается при увольнении — доступ остаётся у бывшего сотрудника
- Без syslog и SNMP инцидент нечем разбирать: причину обрыва определить постфактум невозможно
- Роутер без резерва и без выгрузки show running-config восстанавливается часами, а не за 15 минут

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

5.0

KeeneticOS, на который приводим парк: отдельное приложение WireGuard VPN Server и Application…

релиз KeeneticOS 5.0, ветка Main

5 с

интервал Ping Check для Ethernet-канала: по умолчанию 10 с, для Ethernet документация даёт 5 с…

раздел документации Ping Check fine-tuning

3

порог Ping Check (число неуспешных проверок) для Ethernet вместо дефолтных 5 — быстрее уходим…

раздел документации Ping Check fine-tuning

5

сегментов офиса: Office, Servers, IoT, Guest, VoIP — каждый отдельным bridge с тегом 802.1Q и…

наш стандарт конфигурации

3.1

версия KeeneticOS, где появились WPA3-PSK, OWE и WPA/WPA2/WPA3-Enterprise; корпоративный SSID…

раздел документации WPA3, OWE and WPA Enterprise

90%

доля замеренной полосы, которую вносим в IntelliQoS вручную: при автоопределении шейпер не дер…

наш стандарт конфигурации

РЕАЛИЗАЦИЯ 1 ИЗ 3

Сегментация 802.1Q и два SSID на RADIUS

Что настраиваем

Периметровый Keenetic Giga/Ultra/Peak и управляемый коммутатор доступа; все проводные и Wi-Fi клиенты офиса

Как мы это делаем

1. Заводим сегменты Office/Servers/IoT/Guest/VoIP: каждый — отдельный bridge с тегом VLAN на GigabitEthernet0/VlanN, со своим ip address, ip dhcp pool и security-level…
2. Гостевой сегмент оставляем на security-level protected и включаем isolate-private, чтобы клиенты не видели ни друг друга, ни LAN
3. Корпоративный SSID переводим на WPA2/WPA3-Enterprise: ставим компонент WPA Enterprise, указываем RADIUS-сервер (NPS на контроллере домена) и общий секрет
4. Гостевой SSID держим на WPA2/WPA3-PSK с ежеквартальной сменой ключа и привязкой к сегменту Guest
5. Межсегментные правила пишем явно: из Office к Servers только 445/1433/1541/1560-1591 и RDP, из IoT и Guest — только наружу

РЕЗУЛЬТАТ

Заражение или потеря гостевого ноутбука больше не даёт доступа к 1С и файловому серверу. Печать и камеры перестают шуметь broadcast'ом в офисном сегменте, а увольнение сотрудника закрывается отключением учётки в домене, а не сменой Wi-Fi-пароля для всех.

КЛЮЧЕВОЙ НЮАНС

Сегменты Wi-Fi мультиплексируются тем же 802.1Q, что и проводные: если аплинк к коммутатору не сделан транком с нужными VLAN, гостевой SSID молча окажется в офисной сети.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Multi-WAN: приоритеты каналов, Ping Check и 4G-резерв

Что настраиваем

WAN-интерфейсы основного и резервного провайдера плюс USB-модем LTE на том же Keenetic

Как мы это делаем

1. Основной канал — статика или PPPoE от провайдера, резервный поднимаем на втором Ethernet-порту, переназначенном в WAN
2. Третьим уровнем добавляем USB-модем LTE; порядок использования задаём приоритетом подключений в политике
3. На каждый WAN вешаем свой Ping Check: цели задаём IP-адресами (не именами), режим ICMP echo или TCP/TLS-порт, интервал 5 с, порог 3 отказа
4. Критичные сегменты (кассы, VoIP) привязываем отдельной политикой подключений, чтобы они уходили в резерв первыми
5. Проверяем сценарий вживую: выдёргиваем патч-корд основного WAN и замеряем реальное время переключения и возврата

РЕЗУЛЬТАТ

Отработка резерва происходит по трём триггерам: пропадание линка, провал Ping Check и ручное отключение интерфейса. Возврат на основной канал автоматический, пользователи видят короткий разрыв TCP-сессий вместо часа простоя.

КЛЮЧЕВОЙ НЮАНС

Ping Check нужен именно на основном канале: без него роутер видит линк «живым» при аварии внутри сети провайдера и в резерв не уходит. Хост проверки не должен жить у того же провайдера, а режим TCP/TLS снимает…

РЕАЛИЗАЦИЯ 3 ИЗ 3

Удалённый доступ и наблюдаемость: IKEv2, WireGuard, SNMP, syslog

Что настраиваем

Компоненты VPN-серверов, SNMP server и системный журнал периметрового роутера; коллектор логов в сегменте Servers

Как мы это делаем

1. Ставим компонент «IKEv1/IKEv2 IPsec VPN-серверы» и поднимаем IKEv2 для сотрудников — клиент встроен в Windows и macOS
2. Сертификат для IKEv2 выпускаем на доменное имя KeenDNS, а не на IP: иначе клиенты Windows ругаются на несовпадение subject
3. Для инженеров держим отдельный WireGuard VPN Server (штатное приложение с KeeneticOS 5.0) с доступом только в сегмент Servers
4. Ставим компонент SNMP server и запускаем его командой service snmp, системный журнал уводим на коллектор командой system log server (порт 514/UDP)
5. Ежемесячно снимаем show running-config в git-репозиторий конфигураций и сверяем diff перед обновлением прошивки

РЕЗУЛЬТАТ

Удалёнка работает без сторонних клиентов и без проброса RDP наружу, доступ выдаётся и отзывается на роутере или в домене. Логи и SNMP-метрики позволяют разобрать обрыв канала постфактум и увидеть деградацию до жалоб пользователей.

КЛЮЧЕВОЙ НЮАНС

Каждому VPN-серверу задаём, какой сегмент ему доступен: по умолчанию удалённый сотрудник видит больше, чем нужно, — доступ в Servers должен быть исключением, а не нормой.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Резерв без Ping Check**
  Линк до модема провайдера жив, а интернета нет — переключения не будет. Включаем Ping Check на каждом основном WAN и задаём два независимых хоста.

- ✕ **Хост проверки у того же провайдера**
  DNS или шлюз основного оператора отвечают при аварии его же магистрали. Целями берём IP-адреса в разных автономных системах, а не доменные имена.

- ✕ **Гостевой SSID без isolate-private**
  Клиенты видят друг друга и остатки LAN. Гостевой сегмент держим на security-level protected с включённой изоляцией клиентов.

- ✕ **VLAN на роутере, но access-порт на свитче**
  Сегменты Wi-Fi ходят тем же 802.1Q. Аплинк роутер-коммутатор всегда транк с явным списком разрешённых VLAN.

- ✕ **IKEv2 на самоподписанном сертификате**
  Windows и macOS отказываются подключаться. Выпускаем сертификат на имя KeenDNS и следим за автопродлением до истечения.

- ✕ **IntelliQoS с автоопределением скорости**
  Шейпер не удержит очередь VoIP, если реальная полоса ниже. Замеряем скорость и вносим значения вручную, оставляя запас ~10%.

- ✕ **Один админский пароль на весь парк**
  Компрометация одного офиса открывает все. Уникальный пароль на устройство в парольном хранилище, веб-доступ из интернета закрыт.

- ✕ **Прошивка обновляется «когда сломается»**
  Копятся уязвимости и баги Multi-WAN. Обновляем плановым окном на ветке Main, предварительно сняв show running-config.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Модель под нагрузку: Giga на 10-40 PM, Ultra на 30-70 PM, Peak — при SFP-аплинке и б...
- Отдельный гостевой сегмент с isolate-private и WPA2/WPA3-PSK
- Уникальный пароль администратора, веб-интерфейс наружу закрыт, доступ через KeenDNS
- Резервный канал (второй провайдер или USB-модем LTE) и Ping Check на основном WAN

НОРМАЛЬНО

- 5 сегментов 802.1Q: Office, Servers, IoT, Guest, VoIP с явными межсегментными правил...
- IKEv2/IPsec для сотрудников на сертификате доменного имени KeenDNS
- Ping Check на каждом WAN: цели IP-адресами, ICMP или TCP/TLS, интервал 5 с, порог 3...
- Компонент SNMP server (service snmp) и system log server на коллектор в сегменте Ser...

ХОРОШО

- Корпоративный SSID на WPA2/WPA3-Enterprise с RADIUS (NPS) и доменными учётками
- WireGuard VPN Server для инженеров с доступом только в сегмент Servers
- IntelliQoS с ручной полосой (90% от замера) и приоритетом VoIP, отдельная политика д...
- Конфигурации в git, плановое окно обновления прошивки и учения по отказу канала

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Есть ли второй независимый канал и настроен ли Ping Check на основном WAN с внешним хостом?
- [ ] Проверяли ли отказ вживую — выдёргивали основной WAN и замеряли время переключения и обратного возврата?
- [ ] Разделена ли сеть на сегменты 802.1Q и запрещён ли доступ из Guest и IoT в сегмент Servers?
- [ ] Включена ли изоляция клиентов (isolate-private) на гостевом Wi-Fi и меняется ли его ключ по графику?
- [ ] Корпоративный SSID работает на WPA2/WPA3-Enterprise с RADIUS или всё ещё на общем PSK?
- [ ] Удалённый доступ идёт через IKEv2/WireGuard, а не через проброшенный наружу RDP?
- [ ] Действителен ли сертификат VPN и настроено ли его автопродление на имя KeenDNS?
- [ ] Запущен ли SNMP-сервер (service snmp) и уходит ли системный журнал на внешний syslog-коллектор?
- [ ] Хранится ли актуальный show running-config вне роутера и знаете ли вы дату последней прошивки?
- [ ] Известен ли уникальный пароль администратора и закрыт ли веб-интерфейс из интернета?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Проектируем и внедряем сегментацию 802.1Q офиса под ключ: роутер, транки, DHCP, межсегментные правила
- Настраиваем Multi-WAN с резервом на втором провайдере и LTE, Ping Check и проверкой отказа вживую
- Поднимаем IKEv2 и WireGuard для удалёнки, корпоративный Wi-Fi на RADIUS с доменными учётками
- Подключаем роутер к мониторингу: SNMP, syslog, алерты по падению канала и деградации Wi-Fi
- Ведём парк: резервные копии конфигураций, плановые обновления KeeneticOS, замена по гарантии

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Using multiple ISPs (Multi-WAN) и приоритеты подключений (help.keenetic.com — 2026)

02 Internet availability checking (Ping Check) и Ping Check fine-tuning (help.keenetic.com — 2026)

03 Описание компонентов KeeneticOS: SNMP server, WireGuard VPN Server (support.keenetic.com — 5.0)

04 IKEv2/IPsec VPN server и IPsec site-to-site (help.keenetic.com — 2026)

05 WPA3, OWE and WPA Enterprise wireless security (help.keenetic.com — 3.1+)

06 Setting up the SNMP server и Saving system event logs to a Syslog server (support.keenetic.com — 2026)

07 Релиз KeeneticOS 5.0: WireGuard VPN Server, Application Filters, DNS-Based… (keenetic.com — 5.0)

08 Шаблон ITfresh: базовая конфигурация офисного Keenetic (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.