Вопросы и ответы с вебинара «КриптоПро NGate. Решение прикладных задач с помощью уникального TLS-шлюза удаленного доступа и VPN» от 24.05.2019 г.

1. Есть-ли версия КриптоПро NGate для GNU Linux?

ПАК. Шлюз ставится в голый сервер. Установки на какие либо линуксы не предусмотрены из соображений безопасности, поддержки и прочего. Шлюз работает на очень обрезанной версии Linux Debian. с соблюдением необходимых мер безопасности. Именно поэтому это полное решение с встроенной операционкой.

2. Это программа или ПАК?

Это ПАК (есть несколько моделей с разной производительностью и сертификатами ФСБ по разным классам защиты) или готовый образ виртуальной машины. Клиентская часть для ЛИнукс есть.

3. Клиент под Android, надеюсь, тоже есть?

Есть и андроид и IOS и МАК ОС и прочее. Даже Sailfish работает с нами

4. А смысл использования обрезанного Linux?

Смысл использования обрезанного Linux в безопасности. Убраны все ненужные в работе сервисы и обеспечена так называемая "харденизация" дистрибутива.

5. Кластеризация горячего резерва поддерживается?

Да.

6. Где взять (приобрести) обрезанные дистрибутивы Linux? СПО дистрибутивы не допускаются?

Шлюз идет одним дистрибутивом который уже на этой обрезанной операционке. ничего приобретать не нужно.

7. VRRP умеем?.

VRRP в текущей конфигурации не нужен в принципе. Исходя из работы шлюза. Кластеризация делается по другим принципам. Когда введем в релиз IPSEC то появится своя кластеризация, скажем так похожая на VRRP.

8. Сейчас для создания PKI инфраструктуры производится много, по сути, стандартных действий, создание сертификатов, экспорт их с менеджера на гетвей и так далее. Планируется ли это автоматизировать данную процедуру? Указал на менеджере узел, куда все закинуть, указал параметры серта (имя,

компания, юнит), а всё остальное происходит автоматичеки, чтобы ускорить время установки и развёртывания? Или указал, что установка standalone и вперёд.

По поводу автоматизации работы с PKI - у нас будет интересное решение , мы явно всех удивим :) Но скорее всего в следующем году.

9. Реализована схема Master-Slave кластера? Кластер как-то защищается от split-brain?

split brain в текущей кластеризации не актуален.

10. А какие западные алгоритмы реализованы? RSA, ECDSA?

Все алгоритмы, которые входят в TLS 1.0, 1.1, 1.2, в том числе указанные в вопросе

11. Можно-ли Вашим решением заменить программный продукт Континент-АП (для доступа к СУФД УФК)?

В настоящее время наших шлюзов в СУФД УФК нет. Нам предстоит еще проработать этот вопрос и после того как наши шлюзы там появятся, они смогу заменить Континент-АП.

12. Подключения VPN, приходящие на внутренний интерфейс поддерживаются?

Да.

13. Планируется ли обеспечение возможности подключения мобильных устройств Andrid/iOS через TLS VPN с односторонней аутентификацей без ввода логина/пароля?

Под Апндроид и ИОС мы не выпускаем браузеров. Это больше вопрос к тому кто выпустит такой браузер если нужен ГОСТ. Под другими алгоритмами это и так возможно. Для клиента такое не планировали.

14. Траффик любого приложения на iOs будет туннелироваться по госту, либо только браузер? Речь о функционале самого приложения или о настройке клиента ngate?

Любого. Настройки маршрутизации для виртуального адреса который выдан на клиент. все настройки исключительно на шлюзе

15. У вас на сайте написано, что для кластера на все узлы кэшируются сессии. Это безопасно? Такое решение сертифицировано?

Да именно решение с такой кластеризацией сертифицировано. Все сессии кешируются безопасным образом и защищаются.

16. Будет-ли поддержка ГОСТ браузером Mozilla Firefox?

Firefox ГОСТ не поддерживает. Мы делаем и поддерживаем только версию хромиума (win , Linux) . Но к сожалению не сертифицировали ее. Сертифицированным является использование IE в том составе как описано в формуляре на библиотеки криптопро. Был браузер Спутник , плюс есть вероятность в дальнейшем сертификации других браузеров - но это к их владельцам

17. Обрезанный дистрибутив Linux на базе CentOS, Debian или?

Debian, это указанно в Формуляре

18. Балансировщик входит в ваше решение?

Нет, не входит. Можно использовать любой внешний, в том числе бесплатный HAProxy

19. Какой аппаратный балансировщик порекомендуете?

Citrix, например.

20. В кластере могут быть ПАКи разного "размера"? например:

1. **Сначала купили ПАК на 1000 клиентов**
2. **Потом докупили ПАК на 500 клиентов**
3. **Через год докупили еще один на N клиентов**

Да, могут

21. Может ли NGate заменить Континент

Зависит от решаемых задач. Если говорить про шлюз континент TLS - то да

22. Какие основные преимущества по сравнению с Континент TLS VPN Сервер 2.0?

Эту версию мы пока не видели

23. Есть ли деплоймент чтобы цус был со шлюзом вместе на одной железке?

Да, есть.

24. Без КП CSP двухстороняя аутентификация через NGate возможна (по типу Континент TLS Клиент с встроенным КБ CSP)?

CSP нужен, в теории подойдет любой, но нужно тестировать.

25. На какой аппаратной платформе NGate поддерживается до 10 Гбит/с?

NGATE-2000 и выше

26. А какие балансировщики рекомендуете? Просто не понимаю фразы на сайте "данные о сессии синхронизируются между устройствами балансировщиком". Почему синхронизация балансировщиком производится?

Наверно не точно выразились. Синхронизация своя. ни от каких внешних систем не зависит. А балансировщик внешний - для балансировки между нодами кластера сессий. Балансировщик может быть любой.

27. Клиент лицензируется наверняка?

Клиент бесплатен

28. TLS туннель будет работать только с клиентом NGate? Уточню: TLS туннель будет работать только с клиентом NGate?
Или можно использовать любой криптопровайдер?

Туннель реализуется с двух сторон иначе не будет работать. Соответственно да, только с клиентом NGate

29. Но схема лицензирования возможна, когда головная организация платит за клиентские лицензии на NGate, а для самих клиентов будет бесплатно?

У нас нет клиентских лицензий Нгейт. Есть клиентские лицензии на CSP, которые требуются приобретать при аутентификации клиентов по сертификатам.

30. Клиент проверяет АРМ на соответствие политикам безопасности, например присутствие антивируса?

Пока нет, это у нас в роадмапе.

31. Получается для синхронизации сессий синхронизируются и все ключи? А если компроментация, то все узлы получается выходят из обслуживания?

Сессионные ключи не синхронизируются

32. Какие процессоры используются в шлюзах?

Intel

33. Можно ли ограничить доступ в интернет после установки соединения клиентом с сервером нгейта?

Да, можно

34. Да, возможно сейчас система пропатчена от текущих уязвимостей. А что дальше?

У нас не производится выполнение произвольного кода.

35. Как будет обновляться kernel в Вашем дистрибутиве Linux?

Вместе с дистрибутивом

36. А дистрибутив/обновления Вы будете постоянно сертифицировать?

Да, будем

37. Не планируете на клиентской стороне поддержать сторонние CSP?

Для бразуера - можно использовать любой криптопровайдер.

38. Сертифицированным является использование IE в том составе как описано в формуляре на библиотеки криптопро. А использование Chromium Gost не является сертифицированным?

Хромиум-ГОСТ не сертифицирован.

39. Как долго будет поддерживаться Хромиум-ГОСТ?

Судя по всему - ещё очень долго.

40. При подключении по VPN, есть возможность разрешить/запретить сообщение между клиентами?

Да, есть.

41. Имеется-ли возможность расшарить криптошлюз для пользователей локальной сети?

Если сотрудникам доступ нужен извне к своим ресурсам, то это реализуемо и было продемонстрировано в рамках вебинара. А на самом шлюзе можно нарезать целую кучу поддоменов, в которых будут свои правила аутентификации и свои ресурсы и для внутренних пользователей это можно сделать.

42. Можно-ли зарезервировать систему управления?

Да, в новой версии, которая сейчас будет выходить, да

43. Приведу конкретный сценарий. Есть мобильное приложение, которое имеет свои механизмы аутентификации, но защита канала до мобильного устройства должна защищаться сертифицированной криптографией. Сертификата у пользователя нет, мы можем поставить NGate Клиент на устройство пользователя, но он, чтобы подключиться, сначала должен получить

логи/пароль для подключения к Ngate шлюзу, а потом еще логин/пароль для подключения к мобильному приложению

Да, так возможно.

44. VPN соединение держится на одном узле или может переходить с одной ноды на другую, без разрыва?

Это зависит от некоторых факторов. В каких-то случаях да, в каких-то случаях придется сделать переаутентификацию, но данные все сохраняются.

45. "Траффик любого приложения на iOs" - можно любой трафик заворачивать в туннель , если это настроено

Да, можно любое приложение заворачивать в зависимости от настроек. Мы выдаем подключающемуся устройству виртуальный ip-адрес, для этого ip-адреса настроится политика – это и маршрутизация и к каким сетям он может достучаться. Далее, если это приложение туда коннектиться, он сможет законнектиться.

46. А как регулятор относится к ГОСТовым браузерам, yandex-browser, chromium-gost, etc?

Этот вопрос лучше уточнить у регулятора

47. Какие гипервизоры поддерживаются?

Официально – VMWare и Xen. Технически может работать и на других, но не рекомендуется.

48. Аппаратный клиент планируется?

Если имеется ввиду тонкий клиент, то у нас есть опыт работы с аппаратными тонкими клиентами DELL и еще одним производителем.

49. Какие основные преимущества по сравнению с Континент TLS VPN Сервер 2.0?

Мы еще не видел эту версию Континента. По запросу готовы предоставить сравнение с предыдущей версией – из основных преимуществ – выше скорость раза в 4, больше методов аутентификации и режимов работы, универсальность (поддержка и ГОСТ и не ГОСТ алгоритмов), большее количество сертификатов ФСБ (на NGate есть сертификаты по КС1, КС2, КС3) и VPN – клиент у Континента был раньше только под Windows, у NGate – полный охват ОС, в том числе мобильных.

50. Работа vpn-клиента в качестве сервиса, со стартом системы (Windows), до входа пользователя будет реализовано?

Такая работа сейчас ведется. Ближе к концу года будет реализовано

51. В каких случаях необходимо приобретение аппаратной платформы под ЦУС?

Это зависит от класса защиты. Если нужен КС3, то необходимо.

52. Можно ли использовать виртуальный цус и аппаратные ПАК в кластере для КС1?

Да, можно

53. Поддерживается ли кластеризация ЦУС? Если ЦУС вышел из строя, как управлять комплексом?

Сейчас у нас холодное резервирование. Чуть попозже будет резервирование аля hot-standby.

54. для соединения нод в кластер, разрешается использовать внутренние сертификаты?

У нас там своя система выдачи служебных сертификатов для связи между компонентами NGate и ничего снаружи вставить нельзя. Решение сертифицировано именно так.

55. Встроенный в ЦУС СА сейчас выпускать "боевые" сертификаты вроде не может. Только служебные. Планируется ли реализовать выпуск сертификатов для "работы" для клиентов и сервера встроенным СА?

Мы рассчитываем на инфраструктуру заказчиков. И в большинстве случаев свои центры сертификации уже есть. Пока планов по реализации выпуска сертификатов для клиентов и сервера встроенным СА нет, но если на рынке будут реальные потребности в этом, то мы рассмотрим этот вариант.

56. Реализовано разделение ролей операторов?

Предварительно осенью 2019 года такое разделение появится.

57. TLS туннель будет работать только с клиентом NGate?

Да, все туннельные реализации как правило проприетарные, у нас в том числе.

58. Организация управления ключами клиентов для обеспечения их жизненного цикла (ключей) в случае их территориально-отдаленного расположения

Мы не вмешиваемся в управление ключами клиентов, т.е. если вы раздали когда-то клиентам ключи КриптоПро CSP, то вы их же можете использовать и для связи по TLS.

59. а может клиент терминироваться на произвольном сервере где установлен крипто-про с серверной лицензией?

Нет. Потому что туннель организуется именно на шлюзе и на клиенте.

60. для клиента NGate получается необходим CSP, можно использовать криптопровайдер не криптоПро в связке с клиентом??

Какой-то криптопровайдер, который реализует криптографические функции – да, нужен. Это вопрос тестирования.

61. Мы рассматриваем сейчас решения от разных компаний и ищем кластерное решение, поэтому столько вопросов. Какая задержка между синхронизациями сессий между узлами кластера? Что будет при пиковой нагрузке с большим количеством коротких(по размеру) запросов, будет ли успевать кластер синхронизировать все сессии между узлами кластера?

Несколько миллисекунд.

62. При работе клиента NGate удалённые соединения к АРМ блокируются?

В NGate предусмотренные определенные блокировки. Но пока в NGate не реализован персональный файервол. Поэтому, например, если у ПК две сетевые карты, то вторая сетевая карта никак не будет блокироваться, естественно. Это в роадмапе у нас есть, это будет несколько позже.

63. Планируется ли "дооснастить" ОС NGate межсетевым экраном для безопасности "устройства" и разграничения/запрета обмена сквозь него данными между сегментами сетей?

Каким-то базовым межсетевым экраном да, таким как Outpost – нет. Проще купить какой-нибудь антивирус Касперского со встроенным файерволом.

64. Клиент NGate будет работать с криптопровайдером не КриптоПро?

В теории да, но нужно тестировать

65. а чем отличие от Cisco anyconnect? кроме как Гостового шифрования

Функционал NGate близок к Cisco Anyconnect. На текущий момент функционал Cisco несколько шире, но в некоторых вопросах в части обслуживания и подключения шифрованной связи NGate проще. Кроме этого, в отличие от Cisco и 90% других производителей в основе нашего решения не используем OpenSSL (а используем собственный криптопровайдер Криптопро CSP) и к уязвимостям (например, Heartblead), найденным в OpenSSL никакого отношения не имеем.

66. Что если завтра будут санкции от intel?

Через некоторое время для NGate будет обеспечена поддержка отечественных процессоров Байкал и Эльбрус.

67. А как же уязвимости zombieload mds spectre meltdown?

Мы следим за тем как эти и другие уязвимости можно пропатчить, необходимые патчи выпускаем, делаем компиляцию с нужными параметрами.

68. Как будут обновляться шлюзы, при обнаружении spectre like уязвимостей?

Мы необходимые билды выпускаем достаточно часто и стараемся оповещать о них наших заказчиков. А дальше каждый заказчик решает сам применима к нему эта ситуация или нет. Тут конечно встает вопрос с сертификацией, этот вопрос запущен у нас на постоянной основе.

69. А виртуализация средствами OpenStack/Hyper-V?

У нас большие планы на поддержку OpenStack

70. Вопрос по трудозатратам на поддержку и эксплуатацию: какое количество администраторов, на ваш взгляд, потребуется для реализации, например, на ~10 тыс пользователей?

С точки зрения управления шлюзами мы не видим большую разницу между управлением шлюзами на 10 000 или на 1 000 пользователей. Управление происходит на уровне правил и групп пользователей. С точки зрения управления пользователями – у нас клиент максимально автоматизирован и сильно трудозатраты от количества клиентов не должны.

71. Как вы видите автоматизацию CA? Ведь у большинства сертифицированных CA в правилах пользования явно написано, что нужно, чтобы пользователь лично пришел, подтвердил свою личность, администратор ему сгенерировал сертификат и отдал в руки вместе с распечаткой.

Пока это коммерческий секрет.

72. С патчами от уязвимостей CPU падает производительность

Да, мы с этим боремся, мы оптимизируем некоторые наши модули, чтобы они работали гораздо быстрее и у нас есть очень хорошие результаты

73. Будет ли интеграция с "облачными технологиями" хранения ключей ЭП пользователей (HSM, CSP 5.0, КриптоПро DSS)?

Да, эта работа активно ведется и уже используется в некоторых схемах, в том числе в рамках решений ЕБС (NGate + HSM). Кроме этого уже сейчас можно использовать NGate для организации защищенного канала от пользователей DSS к серверной части DSS.

74. Можно ли кластер развернуть на ВМках и юзать в продуктиве? Или ПАК обязателен?

Да, можно. Только нужно не забывать про ограничение класса защиты (КС1) для виртуалок.

75. Haproxy же можно как балансировщик юзать? есть рекомендации настроек или тонкостей для haproxy например?

Да, можно

76. "Падает производительность", "мы это решаем успешно". Т.е. вы круче, чем Intel и Линус?

Есть определенные технологии, которые можно применить для увеличения производительности, которые мы постепенно внедряем, постепенно оптимизируем код, оптимизируем решения, что-то переводим с одного языка на другой и т.д. Поэтому будет расти производительность решения и сможет компенсировать потерю производительности от патчей – может быть не полностью, может быть полностью, мы работаем над этим.