10 YEARS JETSECURITY CONFERENCE 2019

ОБНОВЛЕНИЕ РЕШЕНИЙ ПО СЕТЕВОЙ БЕЗОПАСНОСТИ: SDSEC, CIS И СЕРТИФИКАЦИЯ ПО ТРЕБОВАНИЯМ ФСТЭК РОССИИ

Михаил Шпак
технический директор департамента корпоративных сетевых решений ООО «Техкомпания Хуавэй»
Shpak.Mikhail1@Huawei.com

HUAWEI

ДОВЕРИЕ. ПОЗИЦИЯ ВЕНДОРА

Важнейшим принципом взаимодействия Huawei с Заказчиками является Доверие:

- Подтвержденное качество
  ИКТ-продуктов и решений
- Прозрачность технологий
  создания продуктов на всех этапах жизненного цикла, демонстрация технологий, включая возможность анализа исходного кода ПО
- Достоверное документирование всех процессов
- Точное выполнение договоренностей
- Соблюдение деловой этики:
  честность, порядочность, открытость, конструктивный диалог, отсутствие попыток обмана
- Согласованный обмен конфиденциальной информацией
- Компетентные кадры
- Помощь и поддержка
  в достижении целей Заказчика даже в сложных ситуациях, близость к Заказчикам

Укрепление доверия – один из главных ориентиров компании Huawei в области цифровизации экономики и развития ИКТ

ПРАКТИКА

HUAWEI

Huawei является одной из самых активных из международных компаний-производителей:

- **по проведению независимого аудита**
  Аудит исходного кода ПО, в том числе встраиваемого в чипы
- **сертификации и экспертизы различных продуктов и решений Huawei**
  Привлекается ICSL и другие независимые лаборатории
- **по реагированию на инциденты ИБ в реальном масштабе времени**
  Команда PSIRT
- **по тестированию и моделированию атак**
- **по оперативному выявлению и устранению уязвимостей ПО**
  на всех этапах жизненного цикла

PSIRT

Huawei Product Security Incident Response Team (PSIRT) manages the receipt, investigation, internal coordination and disclosure of security vulnerability information related to Huawei offerings and it is the only window to disclose the vulnerability of Huawei products. Huawei hopes that security researchers, industry organizations, government agencies and vendors can proactively contact Huawei PSIRT to report potential Huawei product security vulnerabilities.

www.huawei.com/en/psirt

Всем этим Huawei на практике доказывает реальное состояние безопасности своих продуктов и решений для заказчиков и регуляторов

10 YEARS JETSECURITY CONFERENCE 2019

ENFORCER: БРАНДМАУЭР СЛЕДУЮЩЕГО ПОКОЛЕНИЯ (SMB) СЕРИИ USG6000

HUAWEI

- Включает три формы: рабочий стол, 1 U и 3 U.
- Пропускная способность идентификации приложений от 800 Мбит / с до 40 Гбит / с, максимальная IPS + 15 Гбит / с + антивирусная защита.
- Минимум 4 интерфейса GE, может быть расширен до 56 x GE + 8 SFP + 14 x 10GE

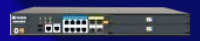
USG6680, 40 Gbps, 3 U, 4 x 10GE + 16GE + 8 SFP

USG6670, 35 Gbps, 3 U, 4 x 10GE + 16GE + 8 SFP

USG6660, 25 Gbps, 3 U, 2 x 10GE + 8GE + 8 SFP

USG6650, 20 Gbps, 3 U, 2 x 10GE + 8GE + 8 SFP

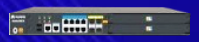
USG6630, 16 Gbps, 1 U, 8GE + 4 SFP



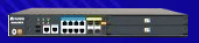
USG6620, 12 Gbps, 1 U, 8GE + 4 SFP

FSTEC Certification

USG6390, 8 Gbps, 1 U, 8GE + 4 SFP



USG6380, 6 Gbps, 1 U, 8GE + 4 SFP



USG6370, 4 Gbps,1 U, 8GE + 4 SFP

USG6360, 3 Gbps, 1 U, 4GE + 2 Combo

USG6350, 2 Gbps, 1 U, 4GE + 2 Combo

USG6330, 1 Gbps, 1 U, 4GE + 2 Combo

USG6320, 2 Gbps, Desktop, 8GE

Extension module

WSIC-2SFP+&8GE

WSIC-8GE

WSIC-4GE-BYPASS

WSIC-8SFP

SAS-600GB

10 YEARS JETSECURITY CONFERENCE 2019

ENFORCER: БРАНДМАУЭР СЛЕДУЮЩЕГО ПОКОЛЕНИЯ СЕРИИ USG9500 ДЛЯ ЦОД

HUAWEI

Model	USG9520 	USG9560 	USG9580 
Height	4 U (DC)/5 U (AC)	14 U	32 U
Number of expansion slots	3	8	16
FW throughput	120 Gbit/s	960 Gbit/s	1.92 Tbit/s
Number of new connections per second	1,600,000	12,800,000	25,600,000
Maximum number of concurrent connections	160,000,000	1,280,000,000	2,560,000,000
Interface types	GE, 10GE, 40GE, and 100GE		
Feature	FW: NAT, PAT, ASPF, Anti-DDoS, SLB, virtual FW VPN: IPSec/GRE/L2TP/SSL/IKEv2 NGFW: IPS, URL filtering, antivirus, DLP, ACTUAL awareness, Smart Policy Routing: RIP/OSPF/BGP/static routing/IGMP Reliability: hot standby (HRP), hot swap, link-group, IP-link, and dual-MPU		

FSTEC Certification

10 YEARS JETSECURITY CONFERENCE 2019

СЕРТИФИКАЦИЯ ФСТЭК HUAWEI USG СЕРИИ NGFW

Vendor	Huawei	Cisco	Fortinet	CheckPoint
Class	**Class 4 (New)**	Class 6(New)	Class 4(New)	Class 4 (New)
Certificate Number	4083	1264/1/4	3720	3634
Invalided Date	**04.02.2019-02.02.2024**	05.07.2016-05.07.2019	16.03.2017-16.03.2020	03.10.2016-03.10.2019
Version	V500	NA	FortiOS 5.4.1	R77.10
Model	**USG6320 USG6330 USG6350 USG6360 USG6370 USG6380 USG6390 USG6620 USG6630 USG6650 USG6660 USG6670 USG6680 USG9560 USG9580**	Only ASA-5520	NA	NA

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4083

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 4 февраля 2019 г.

Выдан: 4 февраля 2019 г.
Действителен до: 4 февраля 2024 г.

Настоящий сертификат удостоверяет, что **межсетевой экран Huawei USG6000 (модели: USG6320 (Eudemon200E-N1D), USG6330 (Eudemon200E-N1), USG6350 (Eudemon200E-N2), USG6360, USG6370 (Eudemon200E-N3), USG6380, USG6390 (Eudemon200E-N5), USG6620 (Eudemon1000E-N3), USG6630 (Eudemon200E-N5), USG6650, USG6660 (Eudemon1000E-N6), USG6670 (Eudemon1000E-N3), USG6680 (Eudemon1000E-N3), USG9560 (Eudemon8000E-X8), USG9580 (Eudemon8000E-X16)) версии V500,** разработанный компанией Huawei и производимый ООО «САТЕЛ», является межсетевым экраном, соответствует требованиям по безопасности информации, установленным в документах «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016) при выполнении указаний по эксплуатации, приведенных в формуляре САБУ.702215.006 ФО.

Сертификат выдан на основании технического заключения от 19.12.2018, оформленного по результатам сертификационных испытаний испытательной лабораторией АО «НПО «Эшелон» (аттестат аккредитации от 18.04.2017 № СЗИ RU.0001.01БИ00.Б018), и экспертного заключения от 24.12.2018, оформленного органом по сертификации АО «Лаборатория ППШ» (аттестат аккредитации от 09.03.2017 № СЗИ RU.0001.01БИ00.А006).

Заявитель: ООО «САТЕЛ»
Адрес: 129223, г. Москва, проспект Мира, д. 119, стр. 619, каб. 5Б
Телефон: (495) 785-8877

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Note: Class 4 is highest certification foreign vendors can get in Russia

Source：fstec.ru

O SD-Sec

НОВОЕ РЕШЕНИЕ HUAWEI SD-SEC

Анализатор: мозг

Используйте интеллектуальную систему анализа безопасности больших данных и изолированную программную среду в качестве основных компонентов, чтобы обеспечить такие возможности, как обнаружение неизвестных угроз, осведомленность о ситуации и отслеживание источников угроз, и связываться с правоохранительными органами для интеллектуального ответа.

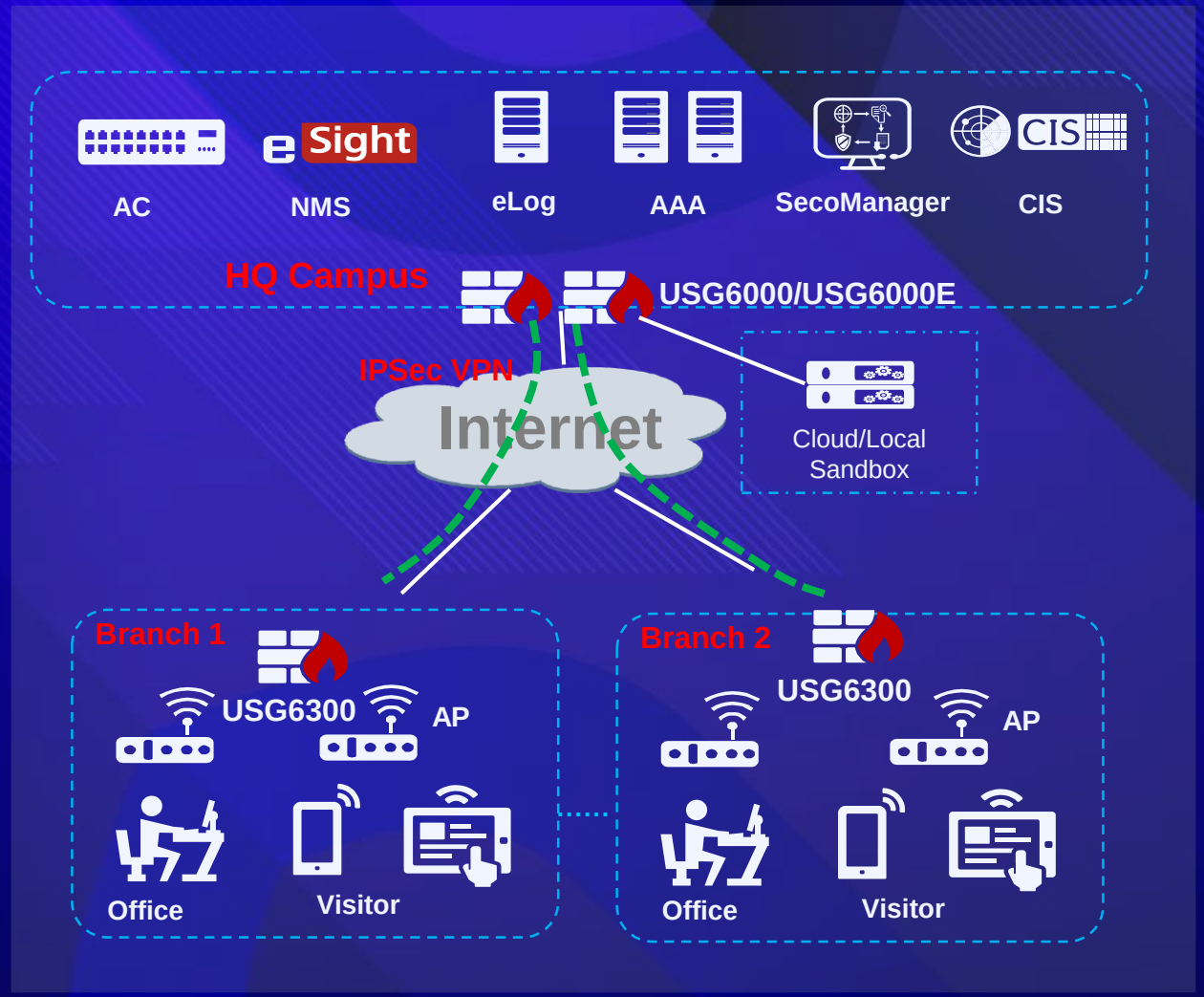
Контроллер: Центральная нервная система

Планируйте и управляйте всеми сетевыми сетями и сетевыми элементами безопасности унифицированным образом, включая коммутаторы, маршрутизаторы, точки доступа и брандмауэры.

Enforcer: конечности

Блокирование путей заражения угроз и предотвращение внутреннего горизонтального распространения на основе взаимодействия с контроллером, а также отвлечения трафика, анализа и определения местоположения с помощью платформы анализа безопасности больших данных.

SD-SEC РЕШЕНИЕ ДЛЯ КАМПУСА



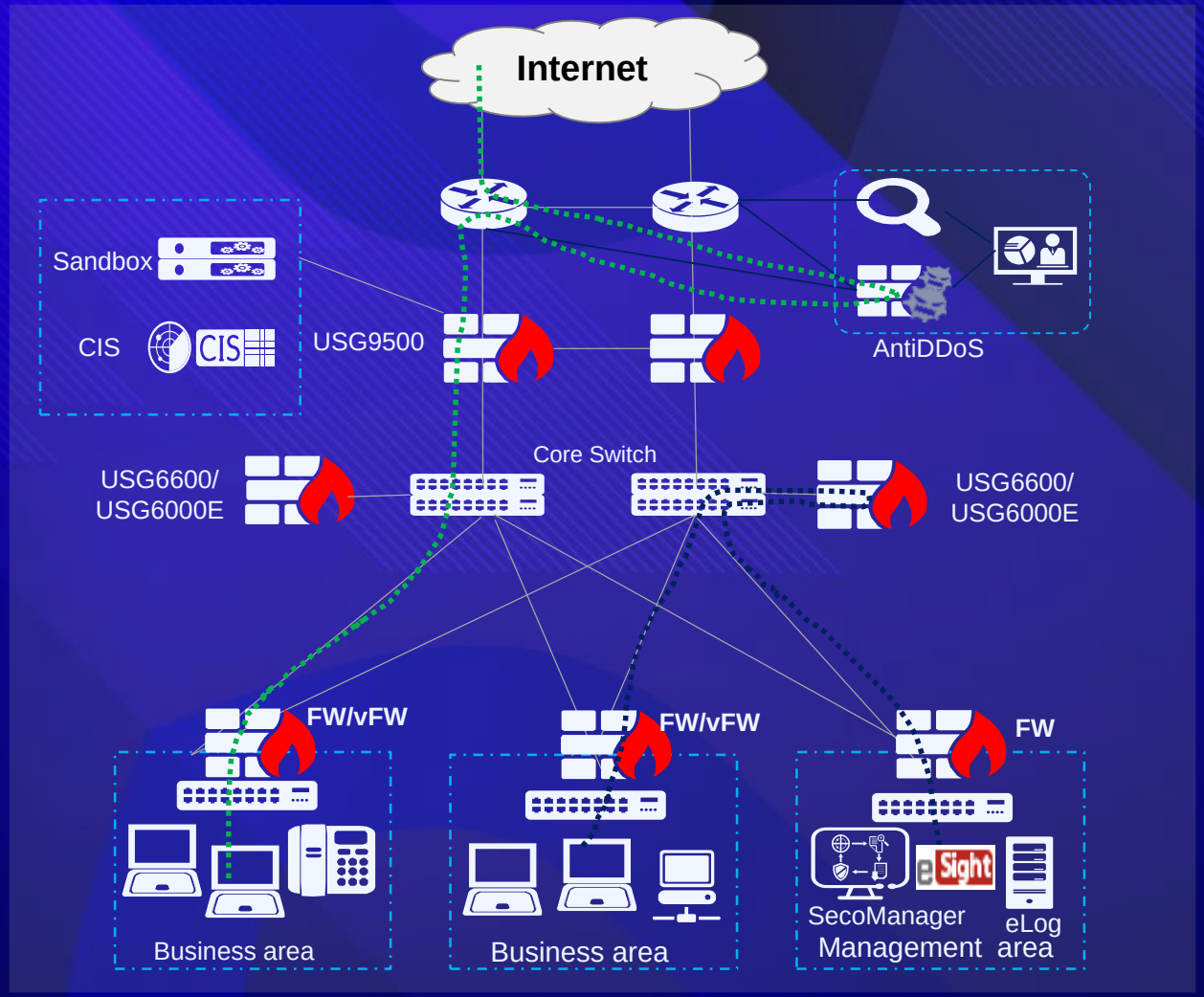
Проблемы безопасности

- Прямая ссылка приносит больше риска безопасности
- Плохой опыт работы в ключевой службе
- Как реализовать маркетинговую деятельность
- Большой масштаб приносит проблемы управления

Solution

- Высокая экономичность и всесторонняя защита
- Детальное управление трафиком для улучшения взаимодействия с пользователем. Интеллектуальный выбор канала ISP и выбор оптимального маршрута для IPSec
- Упрощенная гостевая аутентификация и push-ссылка на приложение и реклама
- Нулевой опыт развертывания с использованием карт памяти USB и простого и централизованного управления
- Управление облаком и Plug-and-Play, быстрое развертывание

РЕШЕНИЕ SD-SEC ДЛЯ ЦОД



Проблемы безопасности

- DDoS-атаки
- Различные цены провайдера приводят к несбалансированному трафику между несколькими ссылками.
- Требование независимого управления безопасностью для нескольких арендаторов
- Низкая производительность ключевых узлов вызывает перегрузку
- Высокие требования к надежности устройства

Solution

- Разверните AntiDDoS на границе, чтобы убрать DDoS-атаки
- Выбор и категоризация Smart Link из нескольких измерений (таких как приложение, маршрутизация, пользователь, время и ссылка) сокращают ненужное потребление полосы пропускания.
- Настройка ресурсов, таких как функции безопасности, пропускная способность и сеансы, для нескольких арендаторов
- Производительность до 1,92 Тбит / с: самый быстрый в мире межсетевой экран для центров обработки данных, протестированный NSS Labs
- Высокая доступность 99,999%: использование программного и аппаратного обеспечения избыточности - Cluster.

КОМПОНЕНТЫ РЕШЕНИЯ HUAWEI SD-SEC

HUAWEI

Сервис безопас-ности

Security Library

- Botnet Signature Library
- Spam Library
- Application Library
- URL Library
- Virus Library
- Vulnerability Library

Security Service

- Emergency Response
- Security Management
- On-line Upgrade
- Manager Security Service
- Credibility Assessment
- Security Consulting

Управление безопасностью

- eLog — Security Event Management System
- CIS — Cybersecurity Intelligence System
- Agile CONTROLLER — Unified control system
- SecoManager

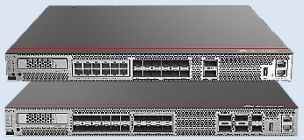
ЦОД и облачная безопасность

- T-Grade NGFW — USG9500

- AntiDDoS — AntiDDoS8000

- Virtual security — USG6000V

- New AntiDDoS — AntiDDoS1800



Сетевая безопас-ность Кампуса

- NGFW — USG6000

- USG6000E

- Sandbox — FireHunter6000

- Облачная песочница базируется в России

- AntiDDoS — AntiDDoS1600/8000

10 YEARS JETSECURITY CONFERENCE 2019

ENFORCER: СЕРИЯ USG6000E, НОВЫЙ NGFW

HUAWEI

1920Gbps

Security card： 20 → 40Gbps

USG9500

160Gbps

NEW

USG6700E

2*100GE or 4*40GE

USG6680E

4*40GE

40Gbps

USG6680
USG6670
USG6660

USG6650E、6630E

2*40GE

20Gbps

USG6650

USG6630
USG6620

USG6610E/66220E
(2019.7)

2*40GE

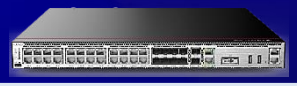
8Gbps

USG6390
USG6380
USG6370

USG6360
USG6350
USG6330

USG6320,Desktop

USG6500E Series



2*10GE

Desktop (4*POE) ： 2*GE(SFP)

Higher performance , Lower price , 4*POE

2019 new product

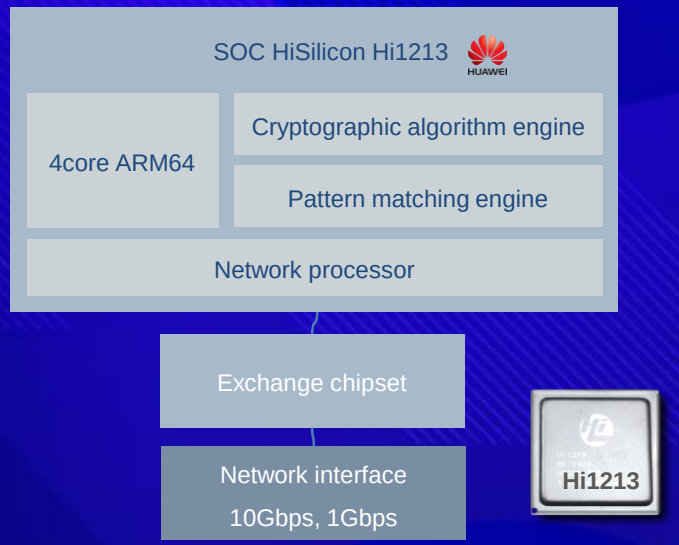
10 YEARS JETSECURITY CONFERENCE 2019

USG6000E: НОВАЯ АРХИТЕКТУРА ДЛЯ ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ

HUAWEI

1~8Gbps Model

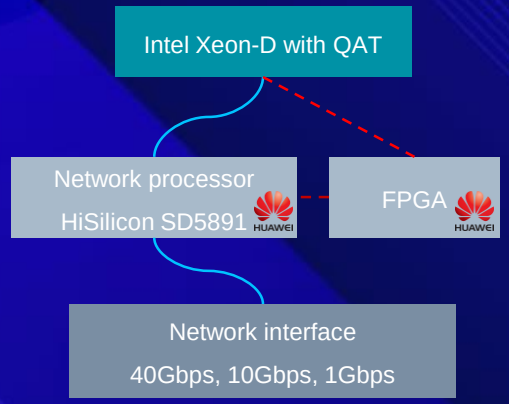
USG6510E/6530E/6515E/6550E/6560E/6580E



10~40Gbps Model

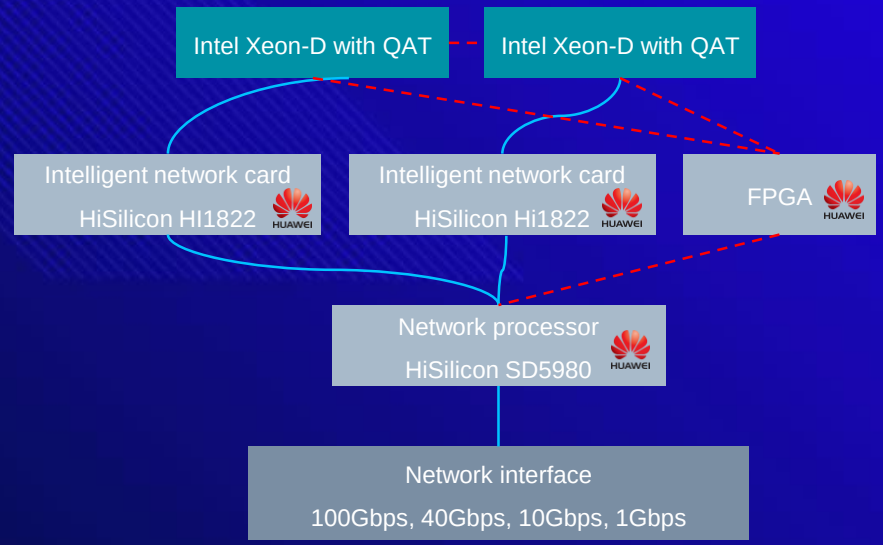
USG6610E/6620E/6630E/6650E

R19C00 GA 2019-7



80~160Gbps Model

USG6680E/6712E/6716E



1 HiSilicon Hi1213

- Система на чипе (SOC), низкое энергопотребление, небольшой размер
- ARM64 ядро, сопоставление с образцом, криптография, NP

2 HiSilicon SD5891/SD5980

- Сетевой процессор (NP), переадресация трафика через брандмауэр, уменьшение DDOS

3 Intel Xeon

- Служба осведомленности (Контроль приложений), IPS, Антивирус, фильтрация URL, DLP

4 HiSilicon Hi1822

- Интеллектуальная сетевая карта, чтобы уменьшить потребление ресурсов процессора
- Расширьте возможности связи с большой пропускной способностью
- Управление полосой пропускания, уровень 2/3/4 разгрузки сетевого протокола

5 FPGA (Field - Programmable Gate Array)

- Расширение масштабов доступа к сессии NP и производительность
- Достижение высокой производительности шаблона регулярного выражения для улучшения пропускной способности фильтрации SA / IPS / URL / DLP

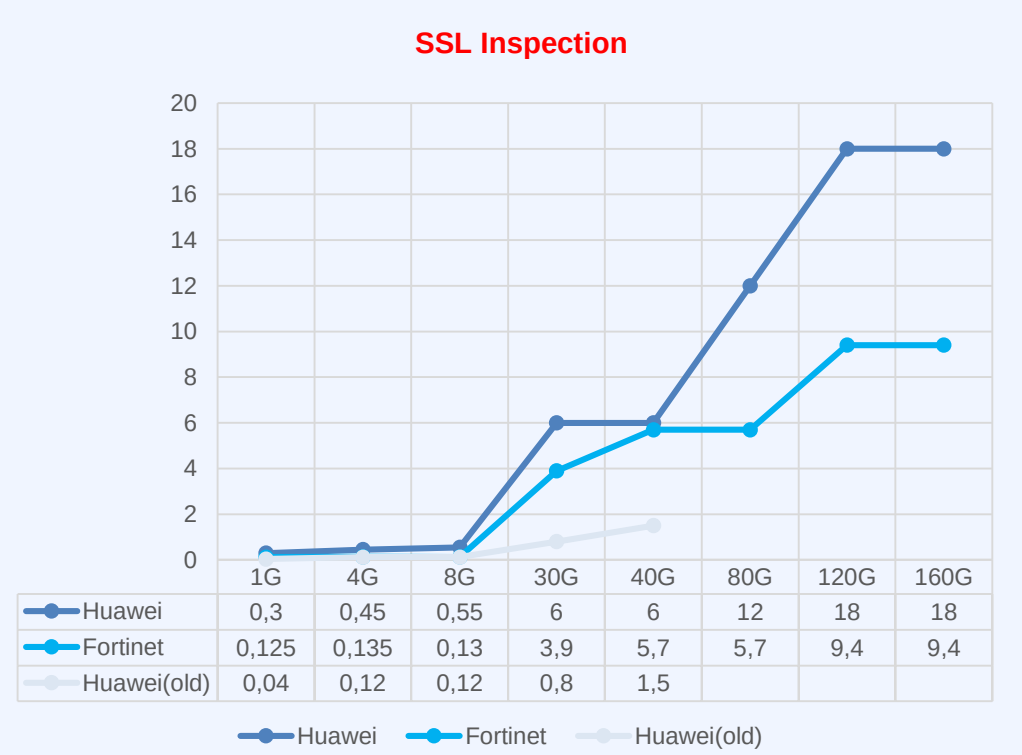
6 Ascend 310 (R19C10)

- Дополнительная плата для ускоренного обучения, архитектура Da Vinci с AI Engine (AIE), возможность обнаружения угроз, интеллектуальный анализ политики

10 YEARS JETSECURITY CONFERENCE 2019

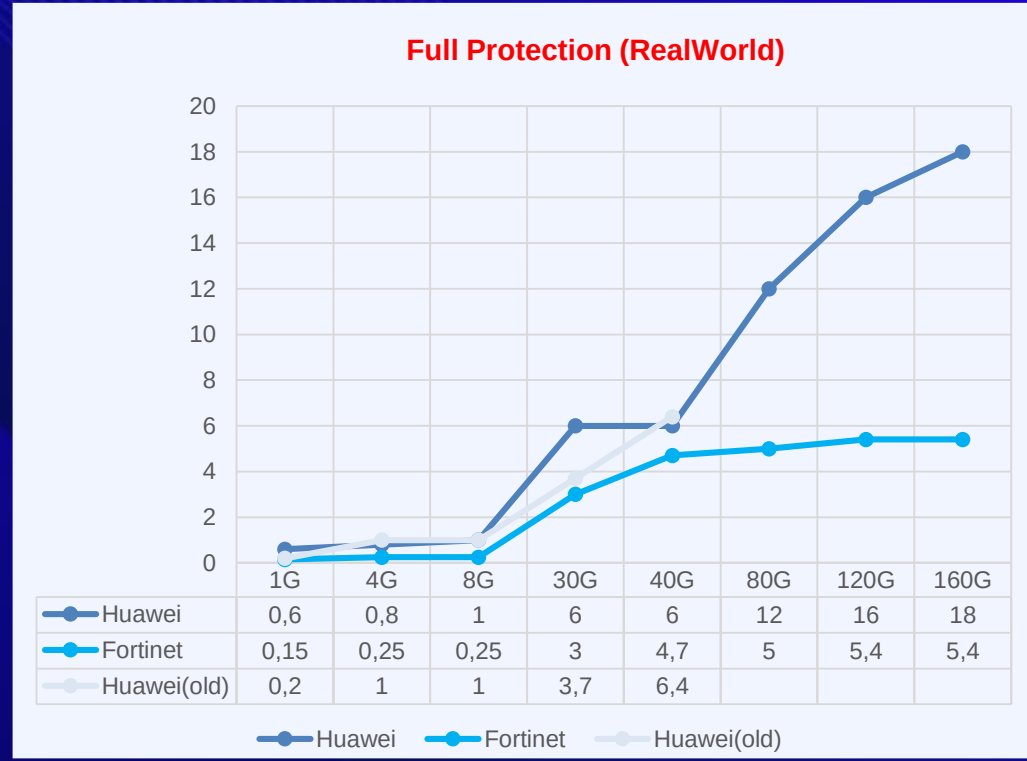
USG6000E: УЛУЧШЕННАЯ ПРОПУСКНАЯ СПОСОБНОСТЬ ПРОВЕРКИ SSL И ЗАЩИТЫ ПРИЛОЖЕНИЙ

HUAWEI



	1G	4G	8G	30G	40G	80G	120G	160G
Huawei	0,3	0,45	0,55	6	6	12	18	18
Fortinet	0,125	0,135	0,13	3,9	5,7	5,7	9,4	9,4
Huawei(old)	0,04	0,12	0,12	0,8	1,5			

- По сравнению с USG6000 пропускная способность проверки SSL в USG6000E значительно улучшена, что превышает Fortigate.
- 1) оптимизация потока обработки кода
- 2) Оптимизация стека протоколов Ssl, заменив openssl1.1
- 3) C sec engine и QAT engine (технология Quick Assist, для ускорения SSL)



	1G	4G	8G	30G	40G	80G	120G	160G
Huawei	0,6	0,8	1	6	6	12	16	18
Fortinet	0,15	0,25	0,25	3	4,7	5	5,4	5,4
Huawei(old)	0,2	1	1	3,7	6,4			

- Полная пропускная способность защиты Huawei (RealWorld) измеряется с помощью брандмауэра, SA, IPS и антивируса, модели трафика Enterprise Mix.
- Пропускная способность защиты от угроз (Ent. Mix) измеряется при включенном брандмауэре, IPS, управлении приложениями и защите от вредоносных программ, трафике Enterprise Mix.
- После того, как Fortigate активирует защиту приложений, производительность сильно падает.

10 YEARS JETSECURITY CONFERENCE 2019

USG6000E: УЛУЧШЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

HUAWEI

Контроль доступа

- 6000+ APP Awareness
- 6 dimension control
- LDAP, AD, Radius, …

TOP2

- New 300 Ent. APP
- TOP100 Ent. APP
- 70+ VPN App

VPN

- IPSec, L2tp, SSL, GRE,…
- DSVPN
- SSL VPN

- SSL VPN client: Win/Mac/iOS/Android

Веб-фильтрация

- База120M URL
- 130+ Category

- 130M URL, Query hit rate 20%->80%
- Malicious URL 25K->450K
- Safe search, google account control

Anti-Malware

- 5M вирусных сэмплов, ежедневное обновление
- Обнаружение доменного имени DGA
- Корреляция с песочницей

- Анализ зашифрованный связи (EC) зонд,
- Облачная песочница (Германия, Россия, Китай)

Маршрутизация и NAT

- IPv4: static routing, RIP, OSPF, BGP, and IS-IS
- IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6
- NAT

IPS

- 5500+Signatures
- 98+% effectiveness
- 4000+ CVE

TOP2

- 12000+ Signatures
- 8000+ CVE
- Malicious Domain 1000+->5000+

Anti-DDoS

- TCP, UDP Flood
- DNS, Http, https ,SIP Flood

- Botnet IP Intelligence
- Policy hits analysis
- Adaptive policy optimization

DLP & Email

- 30+ сборка файлов и фильтрация контента
- 120+ фильтрация типов файлов
- Спам, получатель, отправитель, заголовок, ключевое слово, вложение, фильтрация

- SSL encrypted mail filtering

10 YEARS JETSECURITY CONFERENCE 2019

КОНТРОЛЛЕР: SECOMANAGER

HUAWEI

Единый менеджмент

- Централизованное управление политикой безопасности
- Специфичная для арендатора услуга O&M
- Визуализированное устройство и состояние развертывания политики

Автоматическая сервисная оркестрация

- Отображение взаимного доступа к приложениям и управление политиками на основе приложений
- Управление политикой на основе бизнес-разделов клиента
- Автоматическое развертывание службы безопасности

Интеллектуальная настройка

- Проверка соответствия перед развертыванием
- Моделирование развертывания политик, которые должны быть развернуты, и оценка воздействия на сервисы
- Анализ избыточных политик

Совместная работа всей сети

- Совместная ассоциация сети и безопасности, а также обработка угроз с замкнутым контуром на минимальном уровне

АНАЛИЗАТОР: ПЕСОЧНИЦА ДЛЯ ПРОВЕРКИ НЕИЗВЕСТНЫХ ФАЙЛОВ

HUAWEI

Принцип работы песочницы

Песочница Huawei FireHunter6000
100 000 файлов / день
Точность обнаружения 99,5%

Углубленное обнаружение вредоносных файлов в APT-атаках

Обнаружение проникновения и управление настройками фаз APT-атак.

Принципы песочницы

- Объедините динамический и статический контроль и используйте машинное обучение для обнаружения угроз.
- Запускайте подозрительные файлы в виртуальной среде, которая автоматически справляется с такими средствами уклонения, как фрагментация, сегментация и оболочка.

Типы файлов, которые могут быть обнаружены

- Исполняемые файлы Windows: EXE и DLL
- Веб-страницы, такие как JavaScript, Flash и JavaApplet
- Офисные документы, такие как Office, PDF и WPS
- Различные файлы изображений, такие как JPEG, PNP и JPG
- Сжатые файлы и файлы оболочки

10 YEARS JETSECURITY CONFERENCE 2019

КЕЙС: ИНТЕЛЛЕКТУАЛЬНОЕ ОБНАРУЖЕНИЕ И РЕАГИРОВАНИЕ НА РИСК ФИНАНСОВОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ РЕШЕНИЯ SD-SEC

HUAWEI

Challenge

Коммерческие банки Китая увеличили риски ИБ

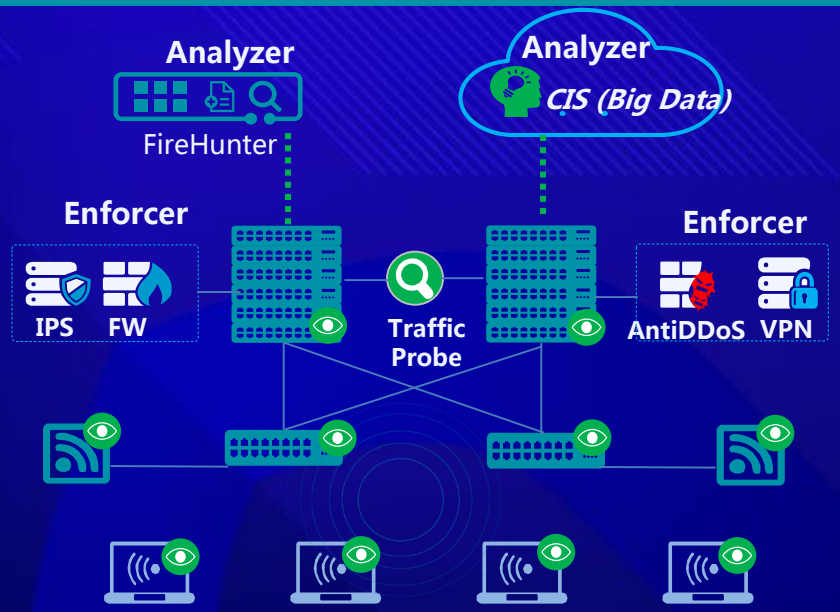
- ✓ **Кража ключевой информации: имя пользователя, пароль, данные банковской карты с подозрением на утечку**
- ✓ **Ветка легко доступна: ветвь обнаружила, что доменные имена DGA и связь C & C**
- ✓ **Почтовый вирус: за 2 недели было обнаружено 19 вредоносных писем**

Неизвестная вредоносная программа использует уязвимость 0day, и ее трудно идентифицировать

Как только вредоносное ПО проникло во внутреннюю сеть, оно быстро распространится

Между обнаружением угрозы и экстренным реагированием существует фатальная задержка

Solution Components



Analyzer
CIS Big data Security analysis platform

Штаб-квартира, филиальные сетевые зонды, осведомленность о состоянии безопасности всей сети

Analyzer
FireHunter Sandbox

Почтовый сервер, интернет-шлюз
Идентификация вредоносного файла

Enforcer
USG NGFW

Восстановление вредоносных файлов
Угроза совместной блокировки

Customer Value

2 months after the system deployed, the effect is obvious

- **8** — 8 впервые в мире обнаружено передовое вредоносное ПО
- **9** — 9 серверов под контролем внутренних или зарубежных хакеров
- **34** — 34 Вируса, которые не обнаружило существующее антивирусное ПО

Клиент решил распространить решение на весь банк.

10 YEARS JETSECURITY CONFERENCE 2019

РАЗВИТИЕ ЭКСПЕРТНОГО СООБЩЕСТВА В МИРЕ

HUAWEI

700,000+ профессионалов в ИКТ отрасли к 2023

Студенты & Public

Альянс талантов

ИКТ Академии и учебные партнеры

Сертификация/повышение навыков и компетенций

ИКТ Таланты

Отбор специалистов

ИКТ Соревнования
Ярмарка вакансий

Возможности трудоустройства/Круглый стол для работодателей

Потребность в ИКТ профессионалах

Требования к профессионалам

Сертификация Huawei

Глобально в ближайшие 10 лет ожидание дефицита порядка 7 млн. ИКТ профессионалов

Сертификация Huawei

83 сертификационных экзаменов и **18** тех. направлений

Более **130,000** сертифицированных профессионалов

ИКТ Академии

600+

Авторизованные учебные партнеры

100+

Обучение студентов

45,000+/в год

4-е Глобальные ИКТ соревнования

60+ стран, **1600+** ВУЗов и колледжей, **100,000+** студентов участников

10 YEARS JETSECURITY CONFERENCE 2019

Методы и средства обучения

Лекции, практические занятия	Онлайн медиа курсы/Web-based training	Вебинары/Live Virtual Classroom LVC	Телеприсутствие	Удаленный доступ к оборудованию
• Авторизованные учебные центры Huawei	• База данных эл. курсов (600 + курсов), более • 2 млн. курсов в год • Online тесты	• Лекции через платформу удаленного обучения Live Virtual Classroom (LVC)	• Лекции посредством видеоконференцсвязи	• E-Lab • Equipment Simulators (e.g. eNSP, Dorado)

10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Михаил Шпак
технический директор департамента корпоративных сетевых решений ООО «Техкомпания Хуавэй»
Shpak.Mikhail1@Huawei.com

HUAWEI