Enterprise Security and Networks
Power Hour 2016

Cisco на страже кибербезопасности государственных органов: до, во время и после

Назим Латыпаев
Системный инженер, EMEAR

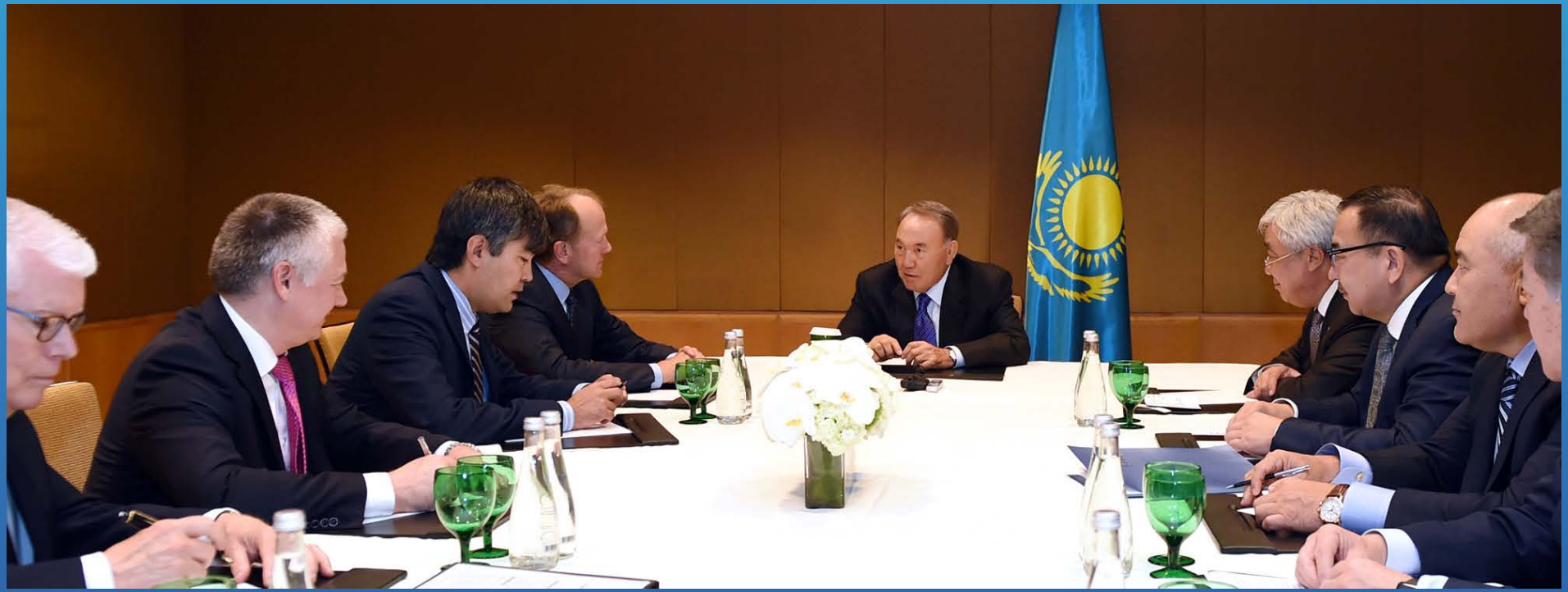
27/09/16

Cisco и ASTANA EXPO 2017

Источник:
https://emear.thecisconetwork.com/site/content/lang/en/id/4170

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Встреча Cisco и Президента РК



Источник: http://kashagan.today/?p=8138

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Проблемы безопасности

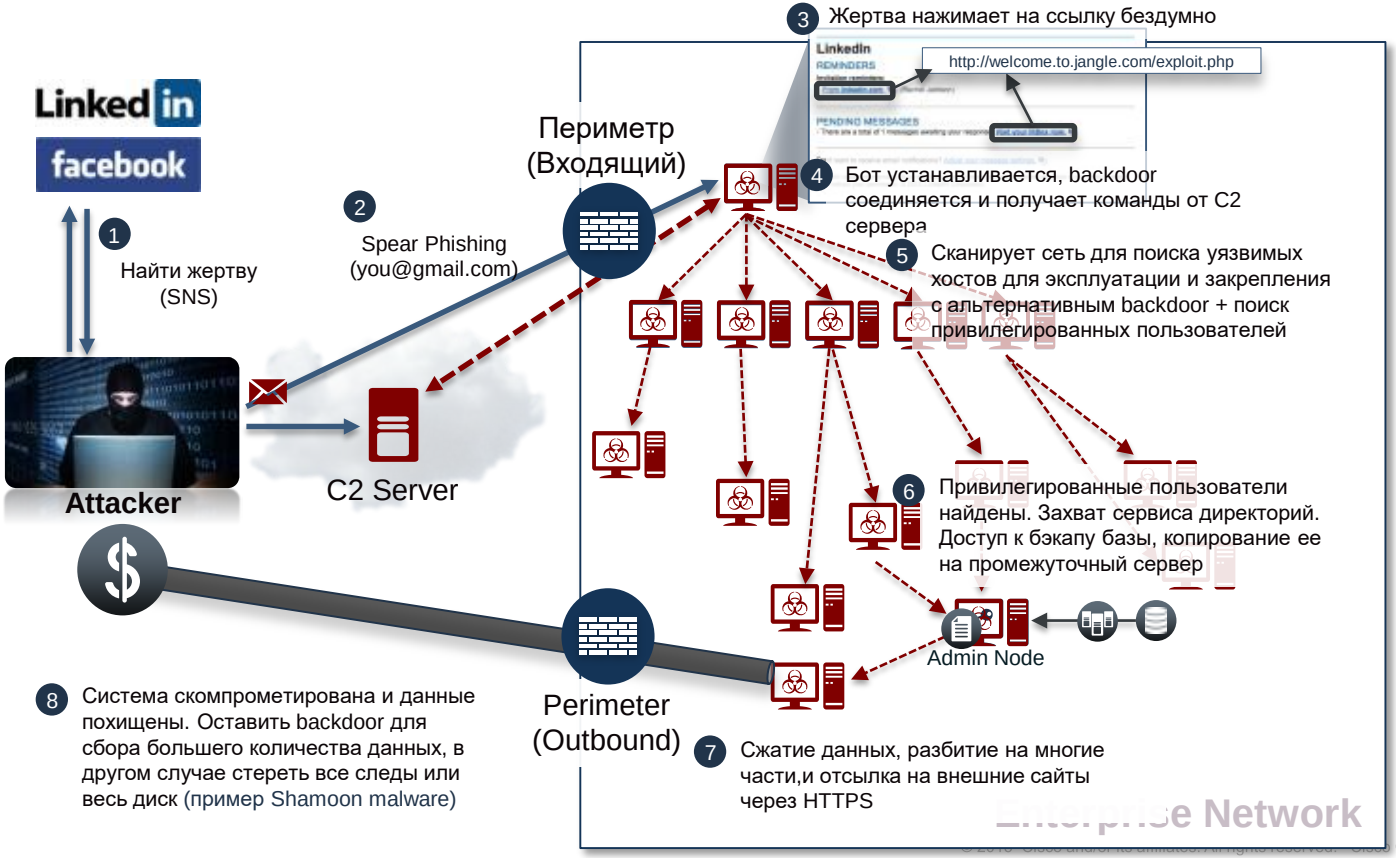
Растущий масштаб атак

Динамический ландшафт угроз

Сложность и фрагментация

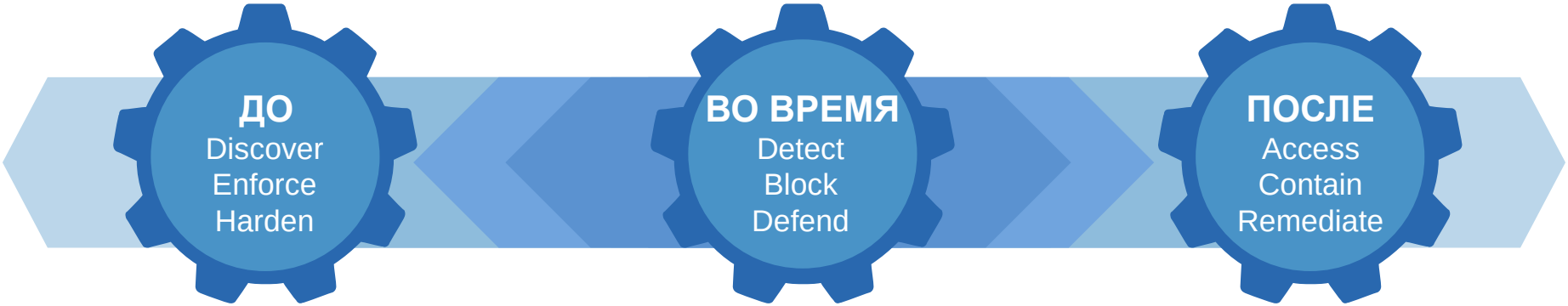
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Анатомия утечки данных



Модель безопасности ориентированная на угрозы

Жизненный цикл атаки



Сеть как сенсор

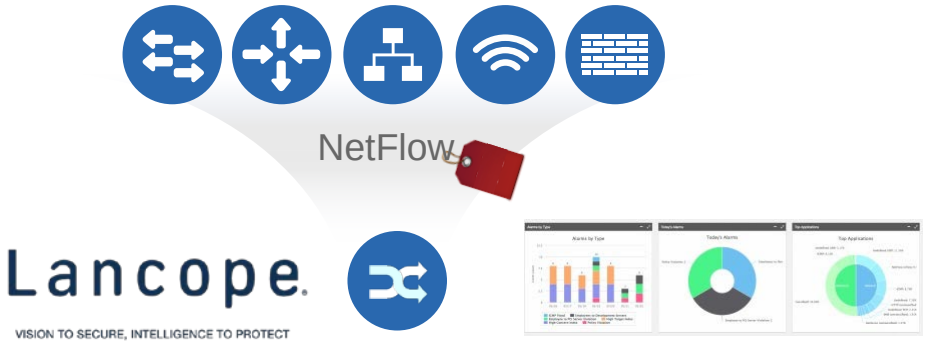
Сеть как средство контроля

Видимость с Cisco Identity Services Engine (ISE)

Обнаружить видимое и невидимое в сети

ЕДИНАЯ ПОЛИТИКА ДОСТУПА В ПРОВОДНОЙ, БЕСПРОВОДНОЙ И VPN СЕТИ

Сеть как сенсор: Lancope StealthWatch



Видимость в реальном времени на всех сетевых уровнях

- Интеллектуальный анализ во всей сети
- Обнаружение устройств
- Профилирование сети
- Мониторинг политики безопасности
- Обнаружение аномалий
- Средства реагирования на инциденты

Сеть как средство контроля
с использованием TrustSec

Традиционная политика безопасности

```
access-list 102 permit icmp 147.31.93.130 0.0.0.255 gt 968 154.44.194.206 255.255.255.255 eq 4533
access-list 102 deny tcp 154.57.128.91 0.0.0.255 lt 1290 106.233.205.111 0.0.31.255 gt 539
access-list 102 deny ip 9.148.176.48 0.0.1.255 eq 1310 64.61.88.73 0.0.1.255 lt 4570
access-list 102 deny ip 124.236.172.134 255.255.255.255 gt 859 56.81.14.184 255.55.255.255 gt 2754
access-list 102 deny icmp 227.161.68.159 0.0.31.255 lt 3228 78.113.205.236 255.55.255.255 lt 486
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
access-list 102 deny udp 32.124.217.1 255.255.255.255 lt 907 11.38.130.82 0.0.31.255 gt 428
access-list 102 permit ip 64.98.77.248 0.0.0.127 eq 639 122.201.132.164 0.0.31.255 gt 1511
access-list 102 deny tcp 247.54.117.116 0.0.0.127 gt 4437 136.68.158.104 0.0.1.255 gt 1945
access-list 102 permit icmp 136.196.101.101 0.0.0.255 lt 2361 90.186.112.213 0.0.31.255 eq 116
access-list 102 deny udp 242.4.189.142 0.0.1.255 eq 1112 19.94.101.166 0.0.0.127 eq 959
access-list 102 deny tcp 82.1.221.1 255.255.255.255 eq 2587 174.222.14.125 0.0.31.255 lt 4993
access-list 102 deny tcp 103.10.93.140 255.255.255.255 eq 970 71.103.141.91 0.0.0.127 lt 848
access-list 102 deny ip 32.15.78.227 0.0.0.127 eq 1493 72.92.200.157 0.0.0.255 gt 4878
access-list 102 permit icmp 100.211.144.227 0.0.1.255 lt 4962 94.127.214.49 0.255.255.255 eq 1216
access-list 102 deny icmp 88.91.79.30 0.0.0.255 gt 26 207.4.250.132 0.0.1.255 gt 1111
access-list 102 deny ip 167.17.174.35 0.0.1.255 eq 3914 140.119.154.142 255.255.255.255 eq 4175
access-list 102 permit tcp 37.85.170.24 0.0.0.127 lt 3146 77.26.232.98 0.0.0.127 gt 1462
access-list 102 permit tcp 155.237.22.232 0.0.0.127 gt 1843 239.16.35.19 0.0.1.255 lt 4384
access-list 102 permit icmp 136.237.66.158 255.255.255.255 eq 946 119.186.148.222 0.255.255.255 eq 878
access-list 102 permit ip 129.100.41.114 255.255.255.255 gt 3972 47.135.28.103 0.0.0.255 eq 467
```

Политика безопасности TrustSec

Source \ Destination	PCI Device	Employee	Guest	Suspicious	PCI Servers
PCI Device	✓	–	–	–	✓
Employee	–	✓	–	–	–
Guest	–	–	✓	–	–
Suspicious	–	–	–	–	–
PCI Servers	✓	–	–	–	✓

- Автоматизация контроля
- Упрощенное управление доступом
- Улучшенная эффективности системы ИБ

Программно-задаваемая **сегментация**

Сетевая фабрика

Flexible and Scalable Policy Enforcement

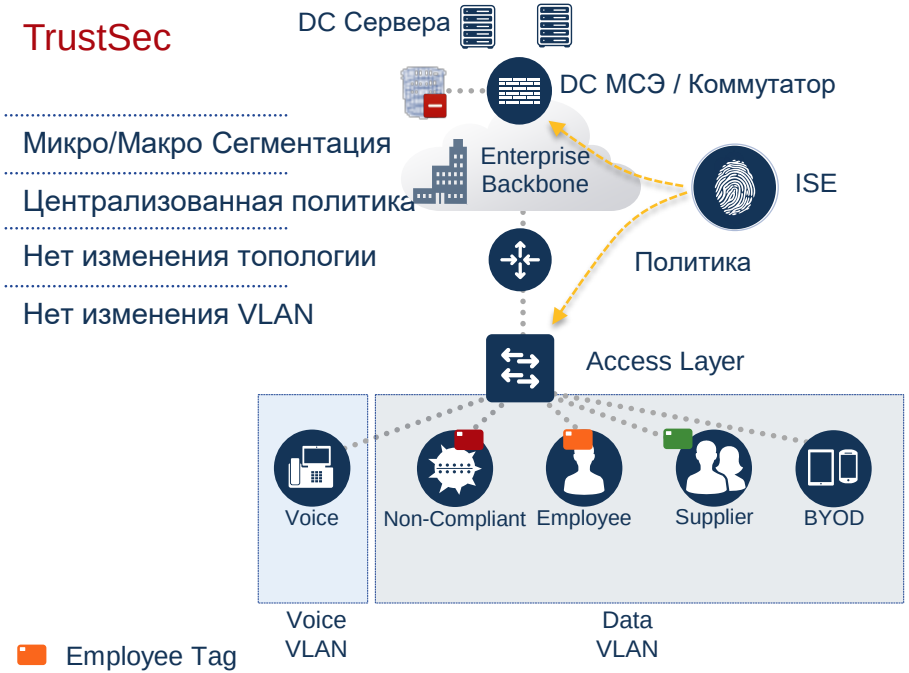
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Как TrustSec упрощает сегментацию сети

Традиционная сегментация

Политика безопасности основанная на Топологии
Высокая стоимость и сложность управления

TrustSec



Использование имеющейся топологии и автоматизация политики безопасности с уменьшением OpEx

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TrustSec Functions and Platform Support

Классификация

Catalyst 2960-S/-C/-Plus/-X/-XR/-CX
Catalyst 3560-E/-C/-X/-CX
Catalyst 3750-E/-X
Catalyst 3850/3650
WLC 5760
Catalyst 4500E (Sup6E/7E)
Catalyst 4500E (Sup8)
Catalyst 4500X
Catalyst 6500E (Sup720/2T), 6800
Wireless LAN Controller
2500/5500/WiSM2, 8500
Nexus 7000
Nexus 6000
Nexus 5600
Nexus 5500
Nexus 1000v (Port Profile)
ISR G2 Router, CGR2000
ASR 1000, CSR
IE2000/3000, CGS2000
ASA5500 (VPN RAS)

Распространение

SXP		ISE 2.0
SXP		Catalyst 2960-S/-C/-Plus/-X/-XR/-CX
SXP		Catalyst 3560-E/-C/-X/-CX, 3750-E
SXP	SGT	Catalyst 3560-X, 3750-X
SXP	SGT	Catalyst 3850/3650
SXP		Catalyst 4500E (Sup6E)
SXP	SGT	Catalyst 4500E (7E, 8), 4500X
SXP		Catalyst 6500E (Sup720)
SXP	SGT	Catalyst 6500E (2T), 6800
SXP		WLC 2500, 5500, WiSM2, 8500
SXP	SGT	WLC 5760
SXP	SGT	Nexus 1000v
SXP	SGT	Nexus 6000/5600
SXP	SGT	Nexus 5500/22xx FEX
SXP	SGT	Nexus 7000/22xx FEX
SXP	SGT	GETVPN. DMVPN, IPsec — ISRG2, CGS2000
SXP	SGT	GETVPN. DMVPN, IPsec — ASR1000
SXP	SGT	ASA5500 Firewall, ASASM

- Inline SGT on all ISRG2 except 800 series:

Контроль

Catalyst 3560-X
Catalyst 3750-X
Catalyst 3850/3650
WLC 5760
Catalyst 4500-X
Catalyst 4500E (7E)
Catalyst 4500E (8E)
Catalyst 6500E (2T)
Catalyst 6800
Nexus 7000
Nexus 6000
Nexus 5600
Nexus 5500
Nexus 1000v
ISR G2 Router, CGR2000
ASR 1000 Router
CSR-1000v Router
ASA 5500 Firewall
ASAv Firewall

www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

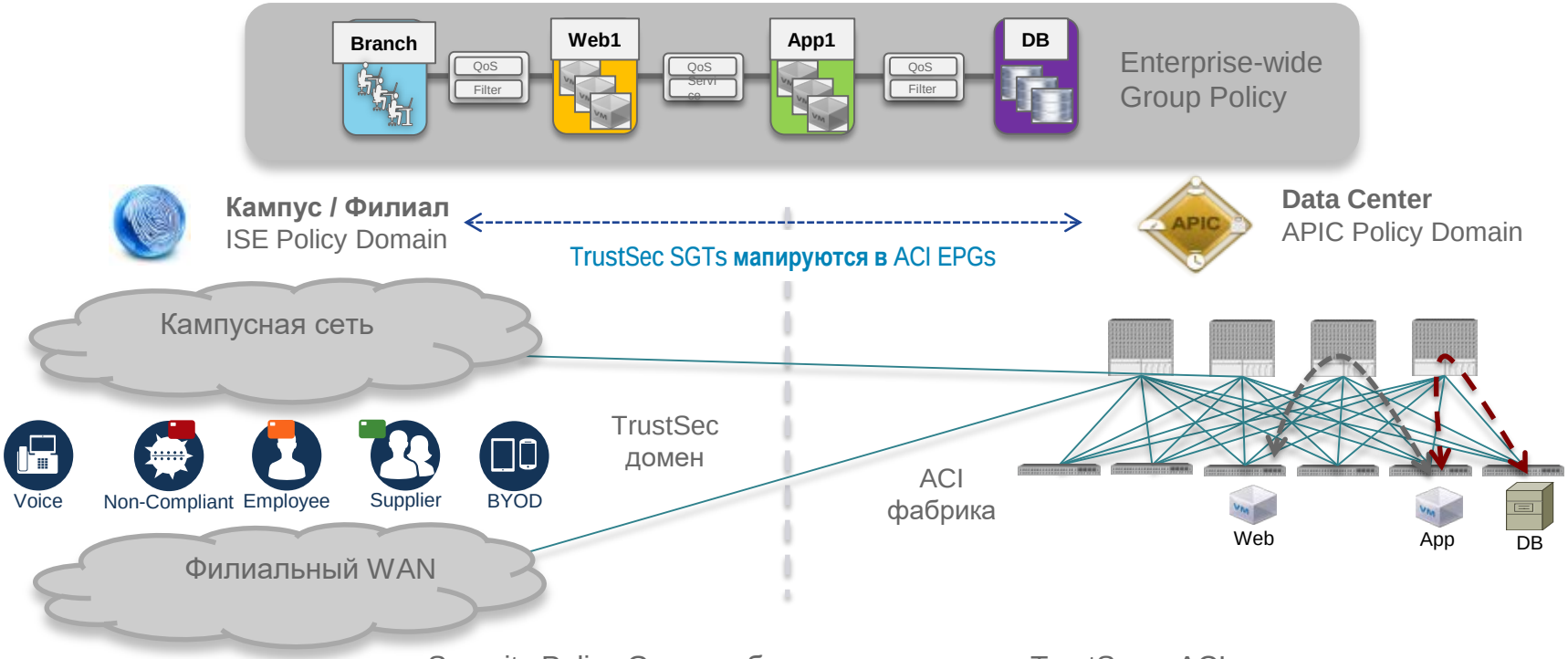
TrustSec-ACI Интеграция

Public Statement of Direction June 15

- Cisco намеревается интегрировать TrustSec и ACI группы политик чтобы дать возможность заказчикам решать вопросы вторжений, сегментации, требований соответствия соответствия с использованием контекста из TrustSec-сети совместно с ACI политикой ЦОД
- Позволяет заказчикам применять целостную политику безопасности во всей сети – использовать пользовательские роли и типы устройств вместе с контекстом приложений
- Совмещенный подход к политике основанной на группах TrustSec и ACI сильно упрощает дизайн для реализации безопасной, управляемой и соответствующей требованиям сети

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

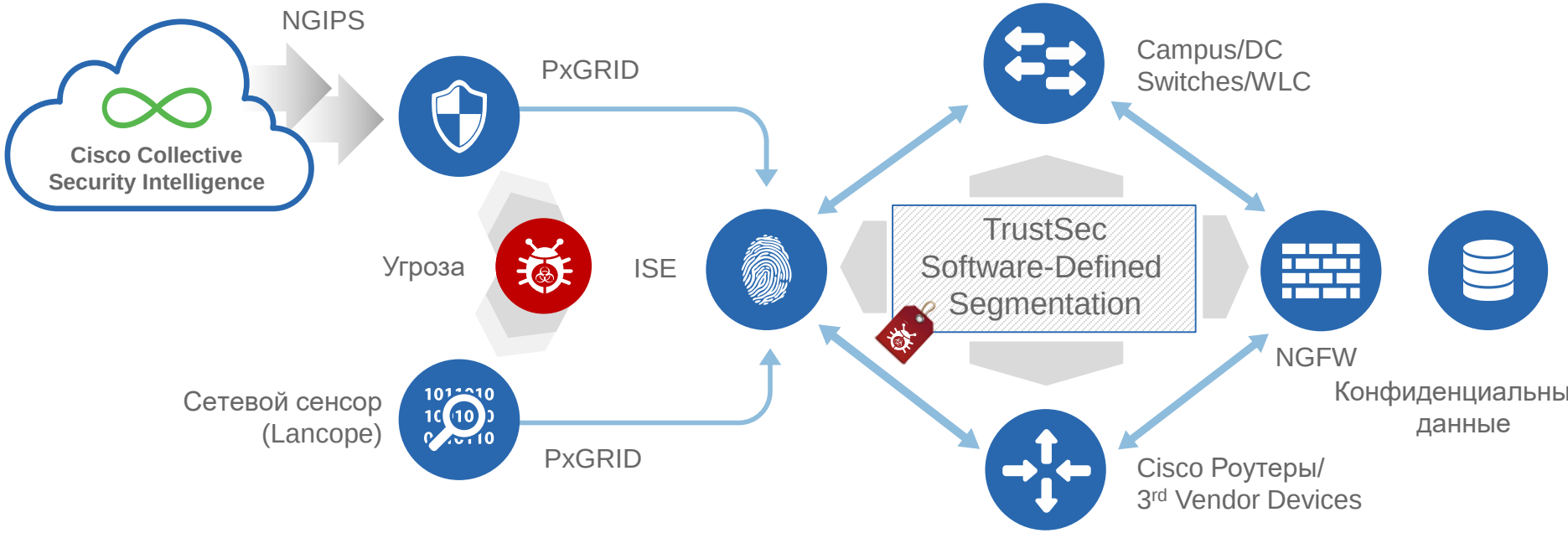
TrustSec-ACI Интеграция: Запуск политики основанной на Группах в сети



- Security Policy Groups обмениваются между TrustSec и ACI доменами
- Позволяет кампусным группам безопасности использоваться в ACI политиках
- Позволяет Endpoint группам использоваться в кампусных политиках

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Создавая архитектуру безопасной сети
Объединяя Сеть как сенсор / Сеть как средство контроля



Сетевые сенсоры	Обмен контекстом и политикой	Сетевые точки контроля

Cisco End to End Архитектура безопасности.
Защита от угроз: При уменьшении затрат на изменения

1. Сложность контроля политик на МСЭ используя традиционные методы - Много усилий для написания и поддержания в актуальном состоянии правил основанных на IP адресах и подсетях. *Каждый раз когда что-либо меняется требуется править/добавлять правила.*

2. TrustSec предоставляет автоматическую классификацию пользователей и их данных. Членство в группе распространяется вместе с данными. *Правила МСЭ могут быть написаны основываясь на группах на более высоком уровне абстракции. Когда пользователь перемещается, ISE и сеть автоматически классифицирует его заново – без необходимости изменения правил МСЭ.*

3. С помощью TrustSec и ISE матрица политик строится на ISE и распространяется на поддерживаемые точки контроля в сети на роутерах и коммутаторах *Таким образом сегментирую кампус или контролируя ЦОД для трафика Восток-Запад*

4. Предоставляет автоматическую классификацию пользователей и устройств при доступе в кампус и автоматическую классификацию ресурсов ЦОД. *Если что-либо перемещается, сеть автоматически классифицирует это при переподсоединении. Редко изменяемые правила в МСЭ и сетевых устройствах. Должным образом сегментированная сеть с упрощением правил МСЭ и автоматизацией.*

5. Но также необходимо активно наблюдать за вредоносной активностью в сети. С лидером рынка SourceFire IPS и мониторингом потоков трафика с обнаружением аномалий с помощью StealthWatch. *SW получает Netflow от каждого Cisco коммутатора и Роутера в корпоративной сети. StealthWatch и ISE интегрированы через API /PxGrid так что SW получает идентификацию от ISE и ISE может узнать об обнаруженных аномалиях и предпринять соответствующее действие автоматически.*

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Угроза:

За последние несколько лет я использовал эти “Организации” для иллюстрации “Угрозы”

Теперь я больше склонен согласиться с JC:

Корпоративная безопасность все еще вызывает растущее беспокойство. Угрозы становятся более Изощренными – результаты более разрушительными, Проблема безопасности НИКУДА НЕ УХОДИТ!

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

С чем мы боремся: угрозы

Примеры

Зомби

DDoS

Пользователи, выдающие себя за других

Перенаправлени

Разрушение

Трояны

Черви

Шпионское ПО

Команда и управление

Атаки нулевого дня

Проникновение

Добавление услуг

Просачивание наружу

Шпионские программы

Вирусы

Утечки

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

С помощью чего мы боремся: возможности


Управление доступом с использованием TrustSec


Анализ/корреляция


Обнаружение аномалий


Анти-вредоносное ПО


Анти-спам


Мониторинг и контроль приложений (AVC)


Безопасность клиента


Cisco Cloud Web Security


Предотвращение утечки данных


База данных


Защита от DDoS-атак


Шифрование электронной почты


Защита электронной почты


Коммутация фабрики


Межсетевой экран


Межсетевой экран


Анализ потока


Идентификация Авторизация


Идентификация Авторизация


Обнаружение вторжений


Предотвращение вторжений


Коммутация L2


Виртуальная коммутация L2


Сеть L2/L3


Сеть L2/L3


Коммутация L3


Балансировщик нагрузки


Регистрация в журнале/ отчетность


Песочница для вредоносного ПО

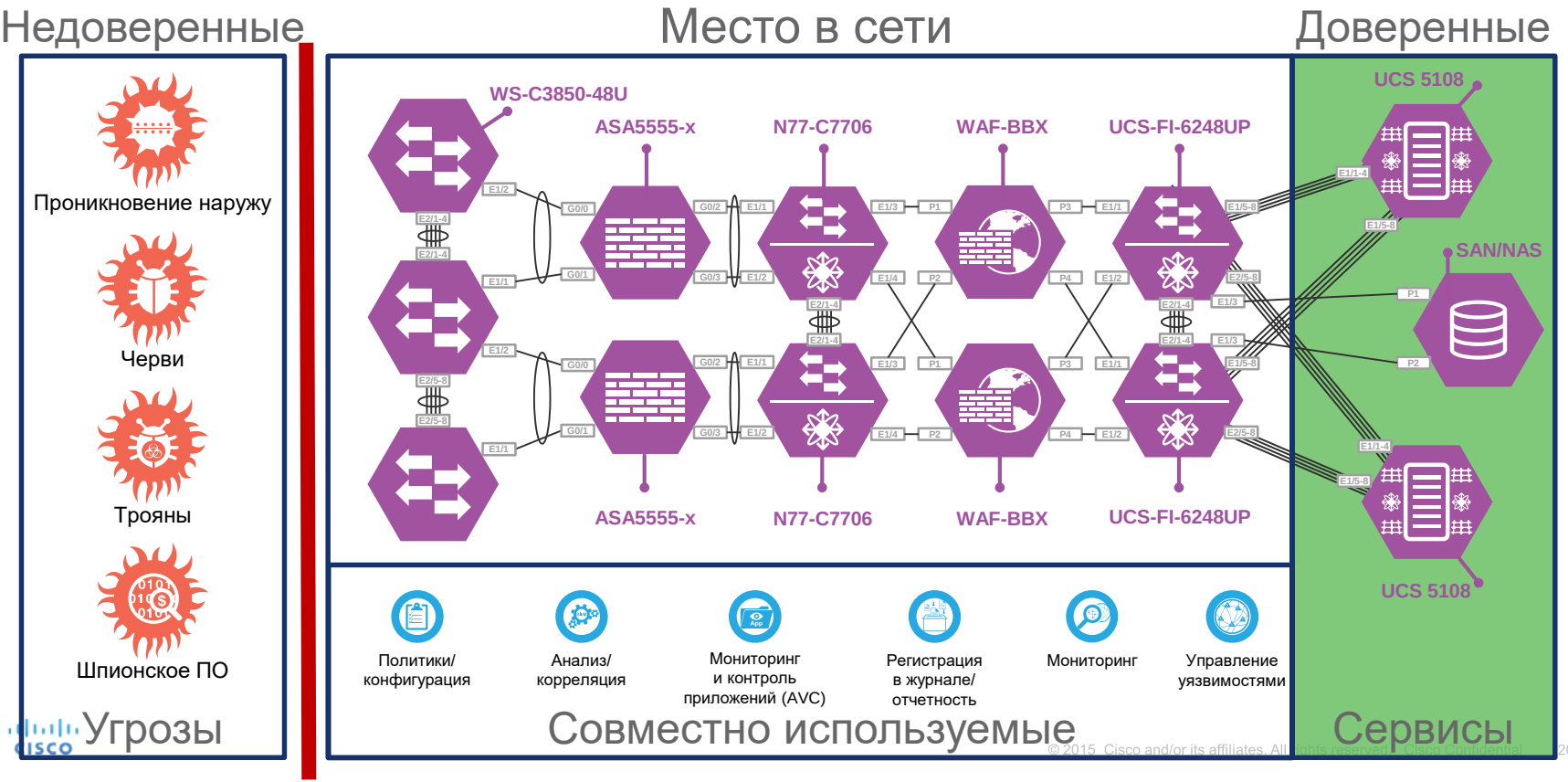

Управление мобильными устройствами


Мониторинг


Политики/ конфигурация

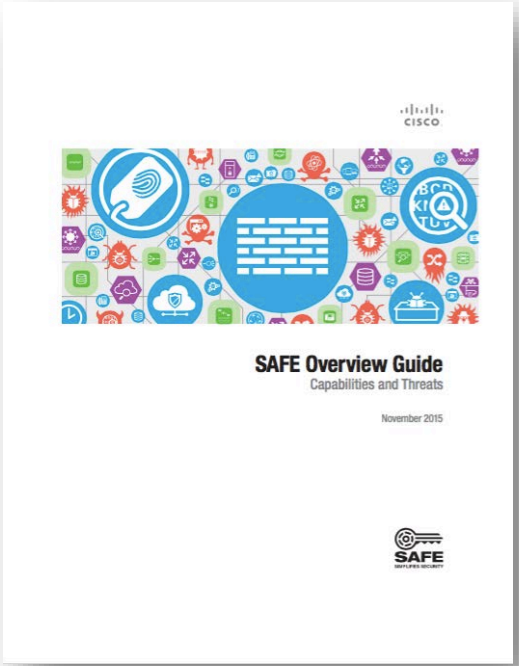
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

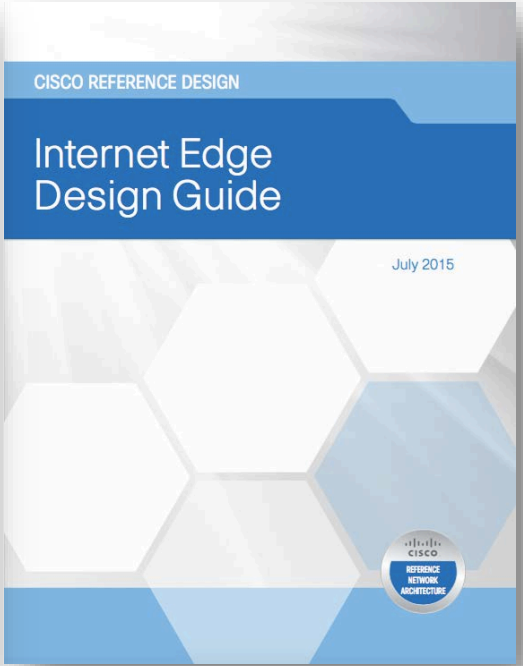
Стратегия дизайна

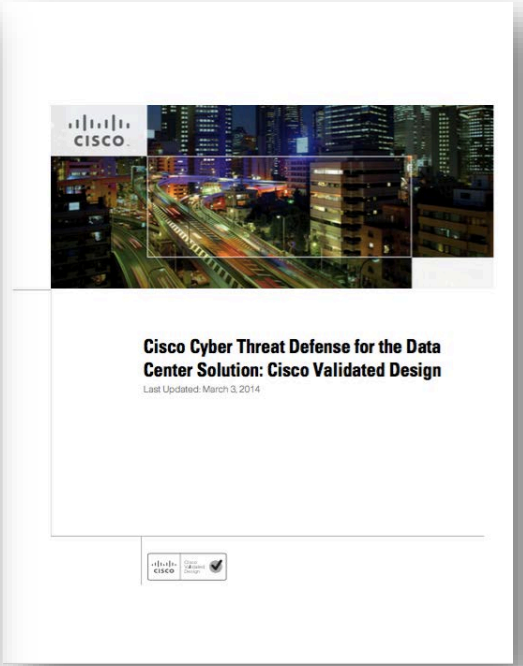


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

На сайте Cisco документы уже есть!







© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO