



Высокопроизводительная безопасность

Павел Родионов
Cisco CSE Security

18 мая 2016

Cisco
Forum

We're ready.
Are you?



Программа

- Ландшафт угроз
- ASA FirePower – первый межсетевой экран, ориентированный на угрозы
- Что умеет делать FirePower?
- Развитие NGFW
- Firepower 4100/9300. Новый подход к высокопроизводительной безопасности

Ландшафт угроз меняется с увеличивающейся скоростью



Source:
¹Cisco Annual Security Report 2014
²Cisco Midyear Security Report 2014
³Cisco Annual Security Report 2015
⁴Cisco Midyear Security Report 2015

Комплексная защита от угроз в течение всего жизненного цикла атаки

Жизненный цикл атаки

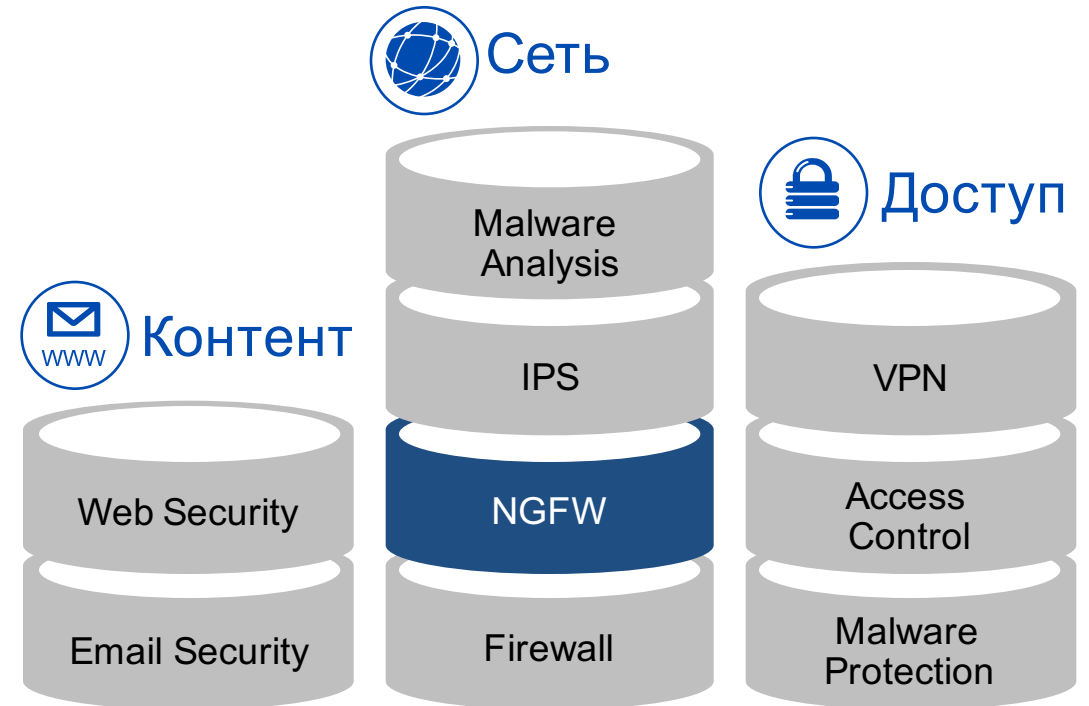


Обзор и автоматизация

Типичный NGFW узко ориентирован и сложно управляем



Фокус на приложениях, не угрозах



Приложения - это не все, что нужно

Они предотвращают атаки, но не эффективны во время и после ее реализации

Жизненный цикл атаки



Типичный NGFW

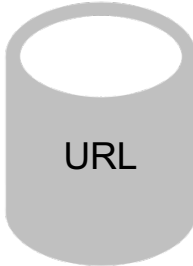


Разрешить приложения

Функции ИБ



IPS



URL



DDoS



Песочница



Реакция на инцидент

А это подтверждение



16 апреля 2015 года

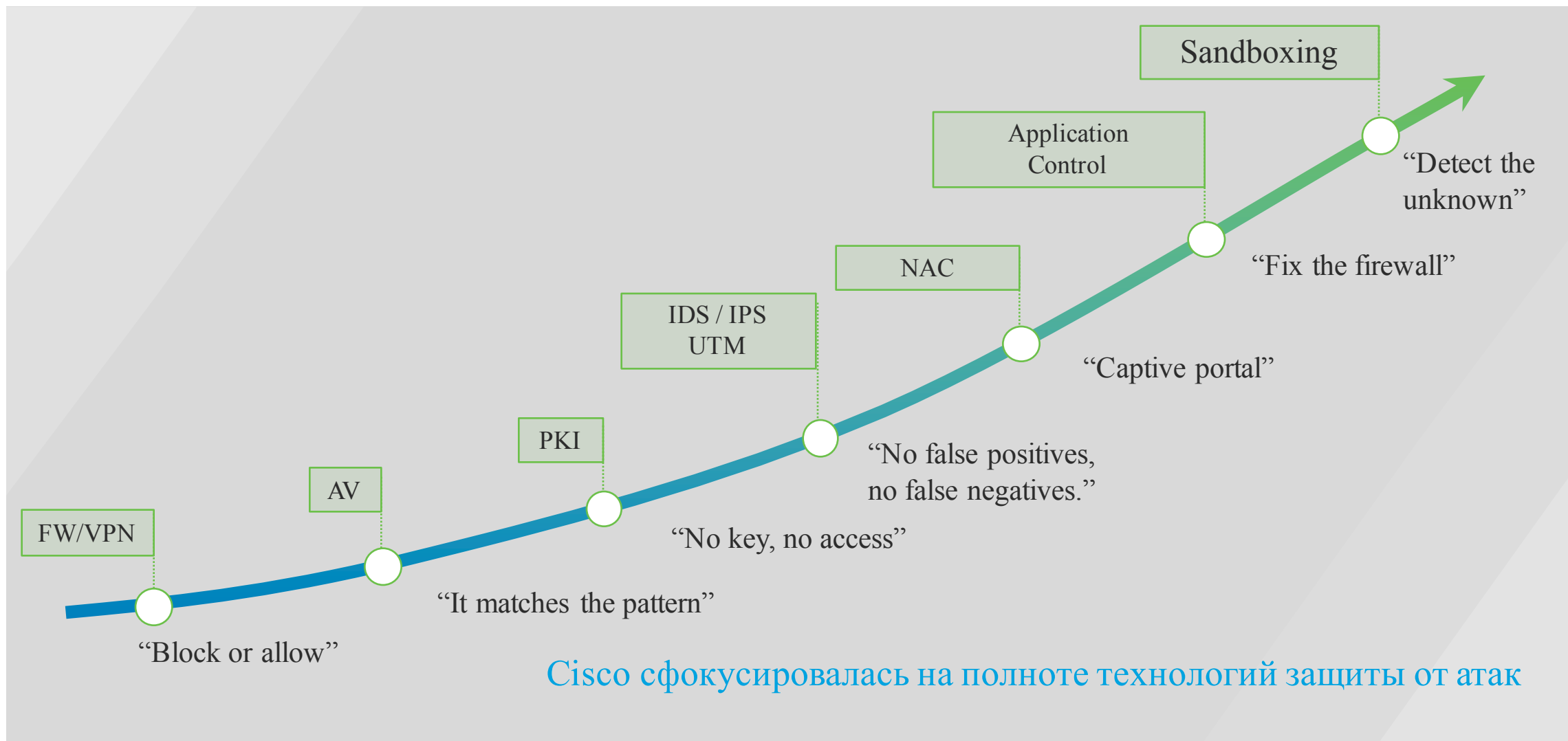
<http://www.zdnet.com/article/palo-alto-networks-mcafee-websense-gateway-systems-allow-malicious-traffic-to-slip-through-the-net/>

Дело **СОВСЕМ** не в названиях компаний, проблема в **МЕТОДОЛОГИИ**

Создание межсетевого экрана нового поколения



В безопасности не существует единой серебряной пули



Cisco: в центре внимания — безопасность!



Приобретение компании Sourcefire Security

- Ведущие в отрасли СОПВ нового поколения
- Мониторинг сетевой активности
- Advanced Malware Protection
- Разработки отдела по исследованию уязвимостей (VRT)
- Инновации в ПО с открытым исходным кодом (технология OpenAppID)

Коллективные исследования Cisco – подразделение Talos по исследованию и анализу угроз

- Подразделение Sourcefire по исследованию уязвимостей — VRT
- Подразделение Cisco по исследованию и информированию об угрозах — TRAC
- Подразделение Cisco по безопасности приложений — SecApps

AMP + FirePOWER
AMP > управляемая защита от угроз

2013

2014

2015...

Cognitive+ AMP



Приобретение компании Cognitive Security

- Передовая служба исследований
- Улучшенные технологии поведенческого анализа в режиме реального времени

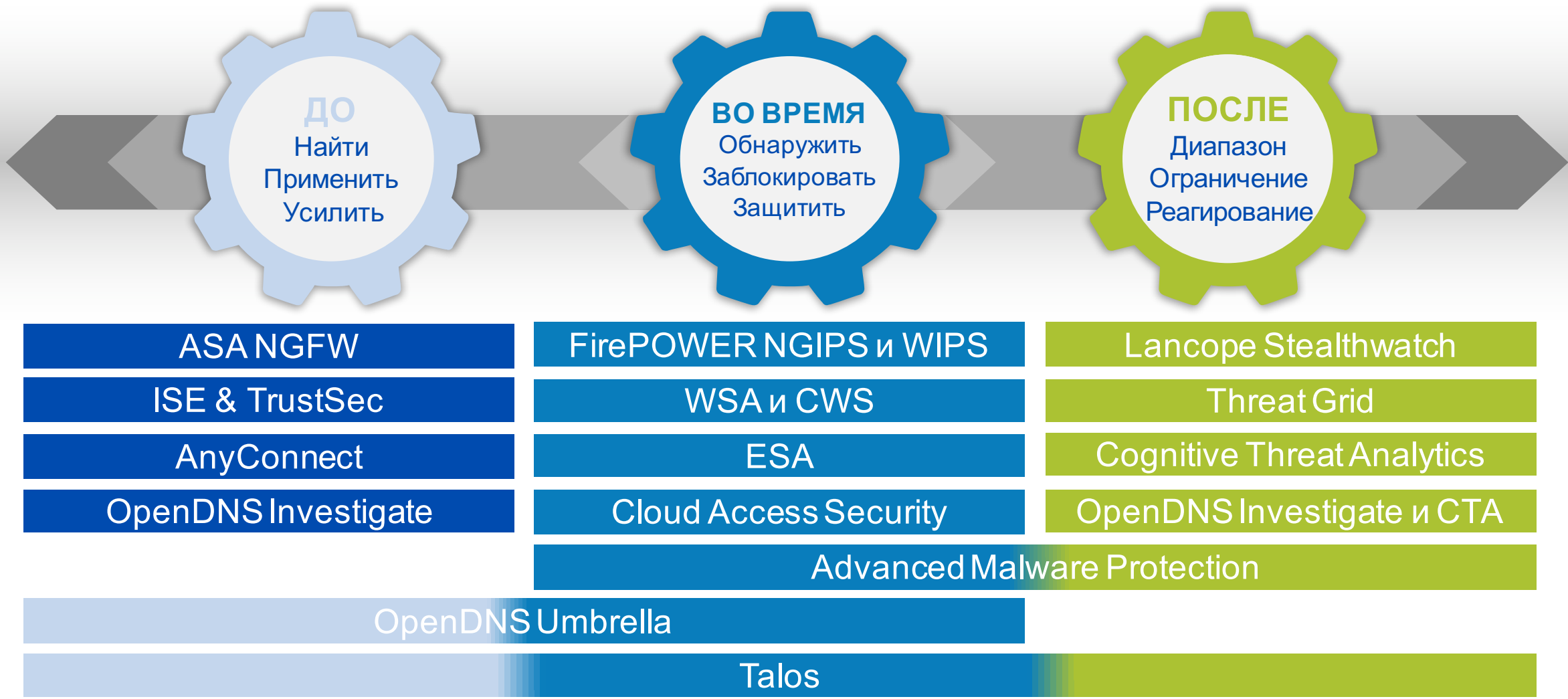
Коллективный анализ вредоносного кода
> Система коллективной информационной безопасности

Приобретение компании ThreatGRID

- Коллективный анализ вредоносного кода
- Анализ угроз



Cisco защищает на протяжении всего цикла атаки

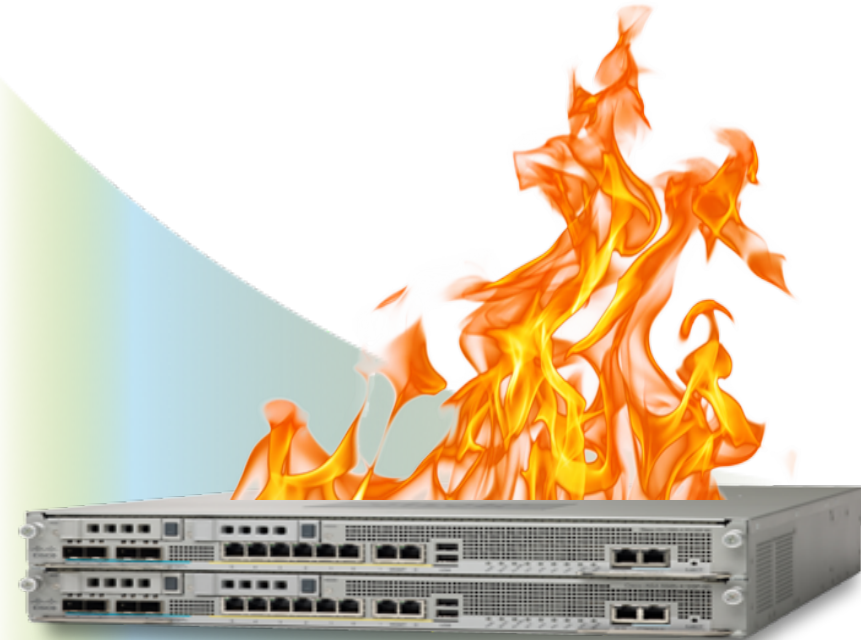


Начало: Cisco ASA с функцией FirePOWER

Первый в отрасли межсетевой экран нового поколения (NGFW), который смотрит шире и глубже

Анонсирован 16 сентября 2014 года

- ▶ Межсетевое экранирование Cisco® ASA в сочетании с системой предотвращения вторжений Sourcefire® нового поколения



МСЭ нового поколения, смотрящий шире и глубже других ASA FirePOWER

Особенности

- ▶ Межсетевое экранирование Cisco® ASA в сочетании с системой предотвращения вторжений Sourcefire® нового поколения
- ▶ Усиленная защита от вредоносного кода Advanced Malware Protection (AMP)
- ▶ Лучшие в своем классе технологии анализа ИБ (SI), мониторинга и контроля приложений (AVC) и фильтрации URL-адресов

Преимущества

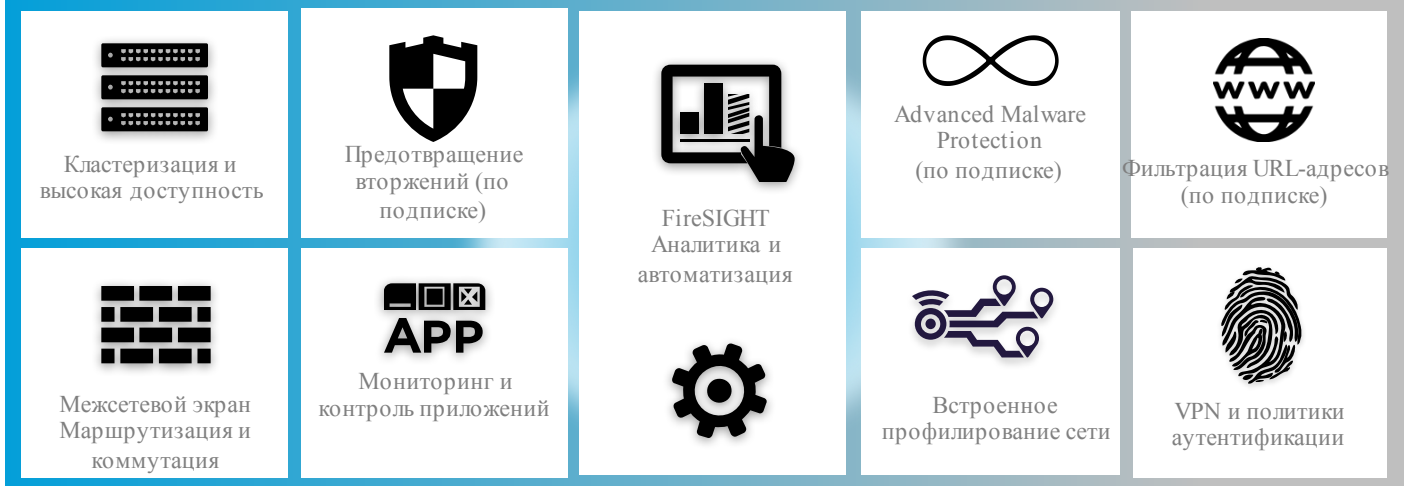
- ▶ Непревзойденная, многоуровневая защита от угроз
- ▶ Беспрецедентная прозрачность сетевой активности
- ▶ Комплексная защита от угроз на всем протяжении атаки
- ▶ Снижение стоимости и сложности систем



«С помощью многоуровневой защиты организации смогут расширить возможности для мониторинга, внедрить динамические механизмы безопасности и обеспечить усиленную защиту в течение всего жизненного цикла атаки»

Непревзойденная комплексная и многоуровневая защита

Интеллектуальная экосистема коллективной информационной безопасности Cisco CSI

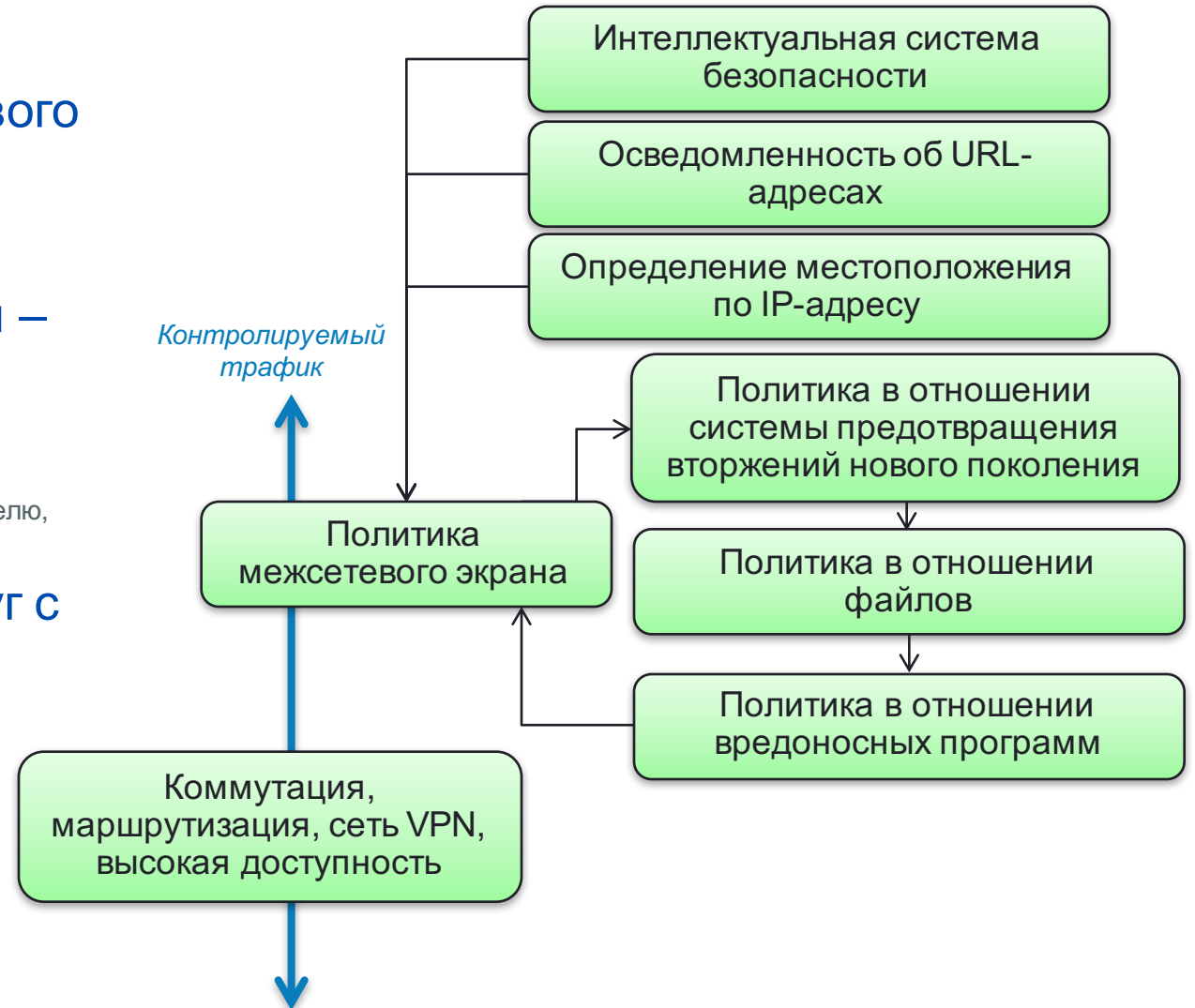


Cisco ASA

- ▶ Самый популярный межсетевой экран ASA корпоративного класса с функцией контроля состояния соединений
- ▶ Система гранулярного мониторинга и контроля приложений (Cisco® AVC)
- ▶ Ведущая в отрасли система предотвращения вторжений следующего поколения (NGIPS) с технологией FirePOWER
- ▶ Фильтрация URL-адресов на основе репутации и классификации
- ▶ Система Advanced Malware Protection с функциями ретроспективной защиты

Что умеет делать Firepower?

- Система предотвращения вторжений нового поколения – проверка содержимого
- Учет контекста
- Интеллектуальная система безопасности – управление черными списками
- Полный контроль доступа
 - По зоне сети, сети VLAN, IP, порту, протоколу, приложению, пользователю, URL-адресу
- И все эти компоненты интегрируются друг с другом
 - Используются политики системы предотвращения вторжений
 - Политики контроля файлов



Беспрецедентная прозрачность сетевой активности

Категории	Технологии FirePOWER	Прежние IPS	Прежние МСЭ
Угрозы	✓	✓	✓
Пользователи	✓	✗	✓
Веб-приложения	✓	✗	✓
Протоколы приложений	✓	✗	✓
Передача файлов	✓	✗	✓
Вредоносный код	✓	✗	✗
Серверы управления и контроля ботнета	✓	✗	✗
Клиентские приложения	✓	✗	✗
Сетевые серверы	✓	✗	✗
Операционные системы	✓	✗	✗
Маршрутизаторы и коммутаторы	✓	✗	✗
Мобильные устройства	✓	✗	✗
Принтеры	✓	✗	✗
VoIP-телефония	✓	✗	✗
Виртуальные машины	✓	✗	✗

Особенности функционала. NGFW



Политика NGFW

Overview Analysis **Policies** Devices Objects FireAMP Health System Help admin

Access Control Intrusion Files Network Discovery Application Detectors Users Correlation Actions

Inline Access Policy

LAB Access-policy for Inline installations

You have unsaved changes Save Cancel Save and Apply

Rules Targets (1) Security Intelligence HTTP Responses Advanced

Filter by Device Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLA...	U...	Applications	S...	De	URLs	Action				
Administrator Rules																
This category is empty																
Standard Rules																
1	Block-Bad URLs	any	any	any	any	any	any	any		any	any	Interact				
2	Block Bad Applications	any	any	any	any	any	any	OpenVPN	any	any	any	Block wi				
3	Block Facebook Games	any	any	any	any	any	any	Tags: Facebook g	any	any	any	Interact				
4	Block Skype File Transfer	any	any	any	any	any	any	Skype File Transf	any	any	any	Block				
5	Block High-Risk URLs (disabled)	any	any	any	any	any	any	any	any	any	any	Any (Reputation 1)	Interact			
6	Block High-Risk Applications (disabled)	any	any	any	any	any	any	Risks: High, Very	any	any	any	Interact				
7	Allow Other + Inspect	any	any	any	any	any	any	any	any	any	any	Allow				
Root Rules																
This category is empty																

1 Row Selected

Displaying 1 - 7 of 7 rules Page 1 of 1

Last login on Thursday, 2014-06-26 at 13:20:21 PM from 192.168.100.2

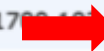
SOURCE inc

Распознавание приложений

- Анализ сетевого трафика позволяет распознавать широкий спектр различных приложений, которые затем можно использовать в правилах политики безопасности
- FirePOWER for ASA распознает и «локальные» приложения

<input type="checkbox"/> HTTP	<input type="checkbox"/> Chrome	32.0.1700.102	<input type="checkbox"/> Google		
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Google		
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Google APIs		
<input type="checkbox"/> HTTP	<input type="checkbox"/> Chrome	32.0.1700.102	<input type="checkbox"/> Google Analytics		
<input type="checkbox"/> HTTP	<input type="checkbox"/> Firefox	26.0	<input type="checkbox"/> Google Analytics		
<input type="checkbox"/> HTTP	<input type="checkbox"/> Firefox	26.0	<input type="checkbox"/> Google Safebrowsing		
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Google+		
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Mozilla		
<input type="checkbox"/> HTTP	<input type="checkbox"/> Firefox	26.0	<input type="checkbox"/> OCSP		
<input type="checkbox"/> HTTP	<input type="checkbox"/> Chrome	32.0.1700.102	<input type="checkbox"/> Rambler		
<input type="checkbox"/> HTTP	<input type="checkbox"/> Firefox	26.0	<input type="checkbox"/> Rambler		
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Rambler		
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Scorecard Research		
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> ShareThis		
<input type="checkbox"/> HTTP	<input type="checkbox"/> Chrome	32.0.1700.102	<input type="checkbox"/> Sourcefire.com		
<input type="checkbox"/> HTTP	<input type="checkbox"/> Chrome		<input type="checkbox"/> witter		
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> witter		
<input type="checkbox"/> HTTP	<input type="checkbox"/> Chrome	32.0.1700.102	<input type="checkbox"/> VKontakte		
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> WebEx		

encrypts communications, recent vulnerabilities, SSL protocol



Описание собственных приложений

- Приложения могут быть описаны шаблонами

ASCII

HEX

PCAP-файл

The screenshot displays the Cisco FireAMP console interface for configuring an Application Detector. The main page is titled "Please enter a name" and includes a "Save" button and a "Cancel" button. The configuration is organized into several sections:

- Detector Information:** Author: admin; Application Protocol: Select an application protocol; State: Inactive; Type: Application Protocol: FireSIGHT.
- Detection Criteria:** Protocol: TCP/UDP; Port(s): 80.
- Detection Patterns:** A table with columns "Pattern String T...", "Pattern String", and "Offset". The table is currently empty, with a message: "There are no patterns. Click 'Add' to add a pattern."
- Packet Captures:** A table with a column "Packet Capture Name". The table is currently empty, with a message: "There are no packet captures. Click 'Add' to add a packet capture."

An "Add Pattern" dialog box is open, showing the following fields:

- Type: Ascii
- Pattern String: Enter a pattern string (required)
- Offset: Enter a number to specify an offset (optional)

Фильтрация URL

Editing Rule - Web Block List

Name Web Block List Enabled **Action** Block **Move**

Zones **Networks** **VLAN Tags** **Users** **Applications** **Services** **URLs** **Policy** **Logging** **Comments**

Categories and URLs

- Any
- Abortion
- Abused Drugs
- Adult and Pornography
- Alcohol and Tobacco
- Auctions
- Bot Nets
- Business and Economy
- CDNs
- Computer and Internet Info
- Computer and Internet Security

Reputations

- Any
- 5 - Well known
- 4 - Benign sites
- 3 - Benign sites with security risks
- 2 - Suspicious sites
- 1 - High risk

Selected URLs

- Adult and Pornography (Any Reputation)
- Bot Nets (Any Reputation)
- Confirmed SPAM Sources (Any Reputation)
- Gambling (Any Reputation)
- Keyloggers and Monitoring (Any Reputation)
- Malware Sites (Any Reputation)
- Marijuana (Any Reputation)
- Nudity (Any Reputation)
- Open HTTP Proxies (Any Reputation)
- Parked Domains (Any Reputation)
- Pay to Surf (Any Reputation)

Различные категории URL

URLs категорированы по уровню рисков

Контроль по типам файлов и направлению передачи

The screenshot shows the 'Add File Rule' configuration window with three callout boxes pointing to dropdown menus:

- Callout 1:** A list of Application Protocols: Any, HTTP, SMTP, IMAP, POP3.
- Callout 2:** A list of Direction of Transfer: Any, Upload, Download.
- Callout 3:** A list of Actions: Detect, Detect, Malware Cloud Lookup, Block.

The main window contains the following sections:











- Application Protocol:** Any
- Direction of Transfer:** Any
- Action:** Malware Cloud Lookup
- File Type Categories:**

<input type="checkbox"/> Office Documents	7
<input type="checkbox"/> Archive	1
<input type="checkbox"/> Multimedia	1
<input checked="" type="checkbox"/> Executables	2
<input type="checkbox"/> PDF files	1
<input type="checkbox"/> Encoded	0
<input type="checkbox"/> Graphics	0
<input type="checkbox"/> System files	0
- File Types:**
 - Search name and description
 - All types in selected Categories
 - MSEXE
 - JARPACK
- Selected File Categories and Types:**
 - MSEXE
 - JARPACK








Buttons: Add, Save, Cancel

Геолокация и визуализация местонахождения атакующих

Top Events by Source Country

Country Name	Count
 United States	162
 Germany	36
 China	18
 Japan	13
 France	11
 Russia	4
 North Korea	2
 Pakistan	1
 Iraq	1
 Iran	1

Last updated 1 minutes ago

Initiator IP	Initiator Location	Responder IP
 76.100.209.66	 USA	 10.4.32.112
 10.4.10.131		 10.4.32.112
 10.4.10.131		 10.4.32.112
 10.4.33.95		 10.5.32.206
 89.188.101.82	 ISR	 10.5.32.206
 200.189.215.85	 BRA	 10.4.33.44
 10.4.31.237		 10.5.32.206
 10.4.11.216		 10.5.39.206

- Визуализация карт, стран и городов для событий и узлов

Детали по геолокации

- IP –адреса должны быть маршрутизируемыми
- Два типа геолокационных данных
 - Страна – включено по умолчанию
 - Full – Может быть загружено после установки:
 - Почтовый индекс, координаты, TZ, ASN, ISP, организация, доменное имя и т.д.
 - Ссылки на карты (Google, Bing и другие)
- Страна сохраняется в запись о событии
 - Для источника & получателя

Geolocation for **94.236.27.33**

Country	United Kingdom  (Europe)
Region	Lnd
City	London
Postal Code	wc2n 5
Latitude/Longitude	51.5073, -0.12601
Maps	   
Timezone	GMT:+0

▼ Additional Information

ASN	15395 (Uk Rackspace)
ISP	Cogent Communications
Home/Business	Business
Domain Name	hayward.co.uk
Connection Type	Broadband

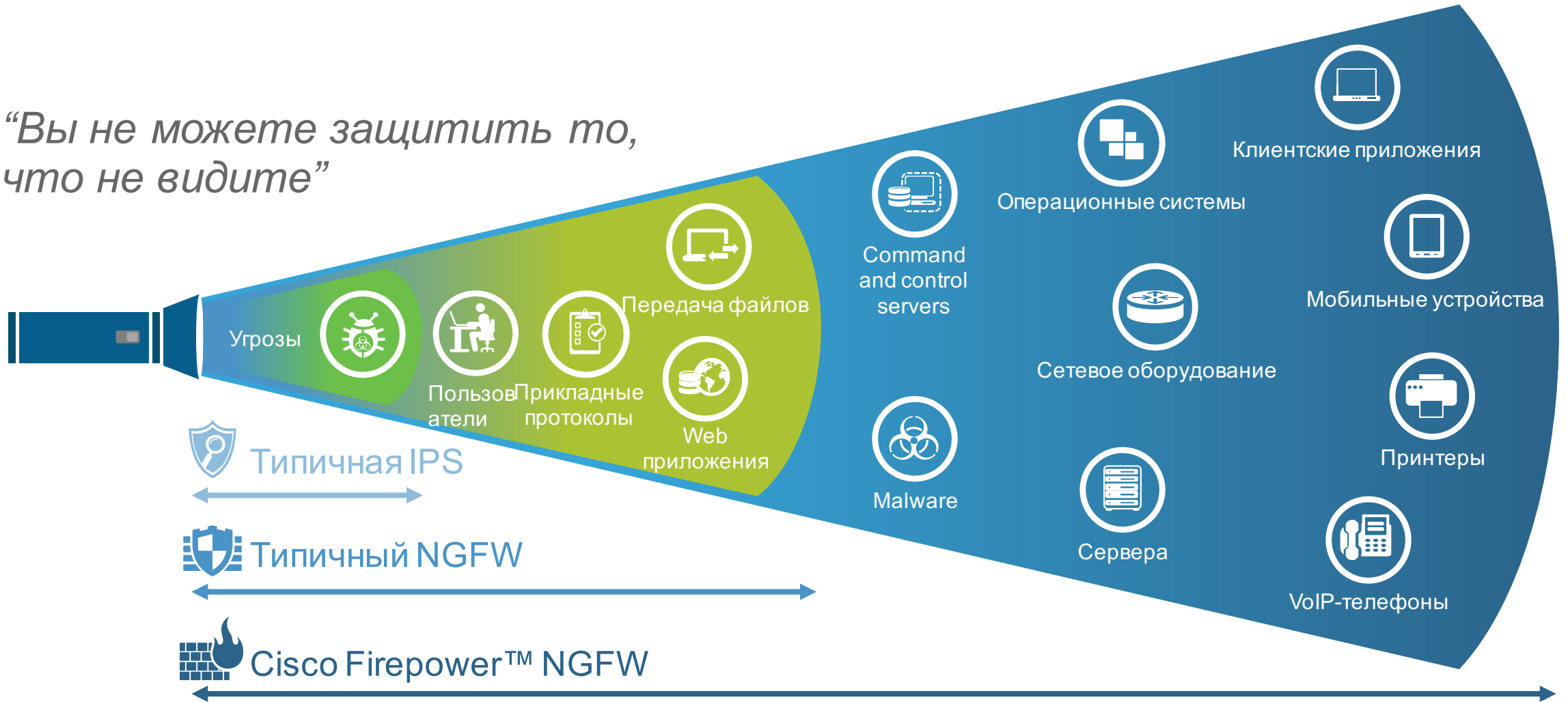
Особенности функционала. NGIPS



Смотреть глубже и шире



“Вы не можете защитить то, что не видите”



Анализ происходящего на узлах

The screenshot shows a network security dashboard with several key sections:

- Host Profile:** Details for host 'mango (1)' including NetBIOS Name, Device (Hops), MAC Addresses (TTL), Host Type, Last Seen, Events, Intrusion Events, Current User (LDAP), and Operating System (Microsoft Windows 2000).
- Connection Events:** A table view of connection events with columns for Port, Application Protocol, and Vendor and Version.
- User Identity:** Profile for user 'cgillian' with fields for Username, Authentication Protocol (LDAP), First Name (Charles), Last Name (Gillian), Email (charles.gillian@sourcefire.com), Department (SF (ron)), and Phone (867-5309).
- Host History:** A table showing connections to various hosts (10.4.10.117, 10.5.32.75, 10.4.10.116, 10.4.32.60) on 2011-10-19 and 2011-10-20.
- Client Applications:** A list of client applications such as Internet Explorer, Chrome, and Google, with their versions.

Callouts provide context for the data:

- Кто на хосте** (Who is on the host) - points to the Current User field.
- Идентифицированная операционная система и ее версия** (Identified operating system and its version) - points to the Operating System field.
- Серверные приложения и их версия** (Server applications and their version) - points to the Application Protocol and Vendor and Version columns.
- Клиентские приложения** (Client applications) - points to the Client column.
- Версия клиентского приложения** (Client application version) - points to the Version column.
- Приложение** (Application) - points to the Application Protocol column.
- Какие еще системы / IP-адреса использует пользователь? Когда?** (Which other systems / IP addresses does the user use? When?) - points to the Host History table.

Инвентаризация и профилирование узлов

- Профиль хоста включает всю необходимую для анализа информацию
 - IP-, NetBIOS-, MAC-адреса
 - Операционная система
 - Используемые приложения
 - Зарегистрированные пользователи
 - И т.д.
- Идентификация и профилирование мобильных устройств

The screenshot displays the FireAMP interface with the 'Hosts' tab selected. The main area shows a 'Host Profile' for IP address 192.168.99.16. The profile includes details such as NetBIOS Name (sfsensor.ashes.cc), Device (Hops), MAC Addresses (TTL), Host Type (Host), Last Seen (2014-02-04 00:02:40), and Current User. Below this, there are sections for 'Operating System', 'Servers (1)', and 'Applications (29)'. The 'Operating System' section shows a table with columns for Vendor, Product, Version, and Source. The 'Servers (1)' section shows a table with columns for Protocol, Port, and Application Protocol. The 'Applications (29)' section shows a table with columns for Application Protocol and Client. A pop-up window is visible in the bottom right corner, showing a 'Host Profile' for IP address 10.5.55.4. This profile includes details such as Hostname (portal.sup.sourcefire.com), NetBIOS Name, Device (Hops), MAC Addresses (TTL), Host Type (Host), Last Seen (2012-07-06 18:40:12), and Current User (Yi Lu (yilu, LDAP)). Below this, there are sections for 'Operating System', 'Servers (2)', and 'User History'. The 'Operating System' section shows a table with columns for Vendor, Product, Version, and Source. The 'Servers (2)' section shows a table with columns for Protocol, Port, Application Protocol, and Vendor and Version. The 'User History' section shows a table with columns for Users and a date range (2012-07-05 18:49:06 to 2012-07-06 18:49:06).

Vendor	Product	Version	Source
Apple	Mac OSX	10.5, 10.6, Server 10.5, Server 10.6	FireSIGHT

Protocol	Port	Application Protocol
tcp	3689	<input type="checkbox"/> HTTP

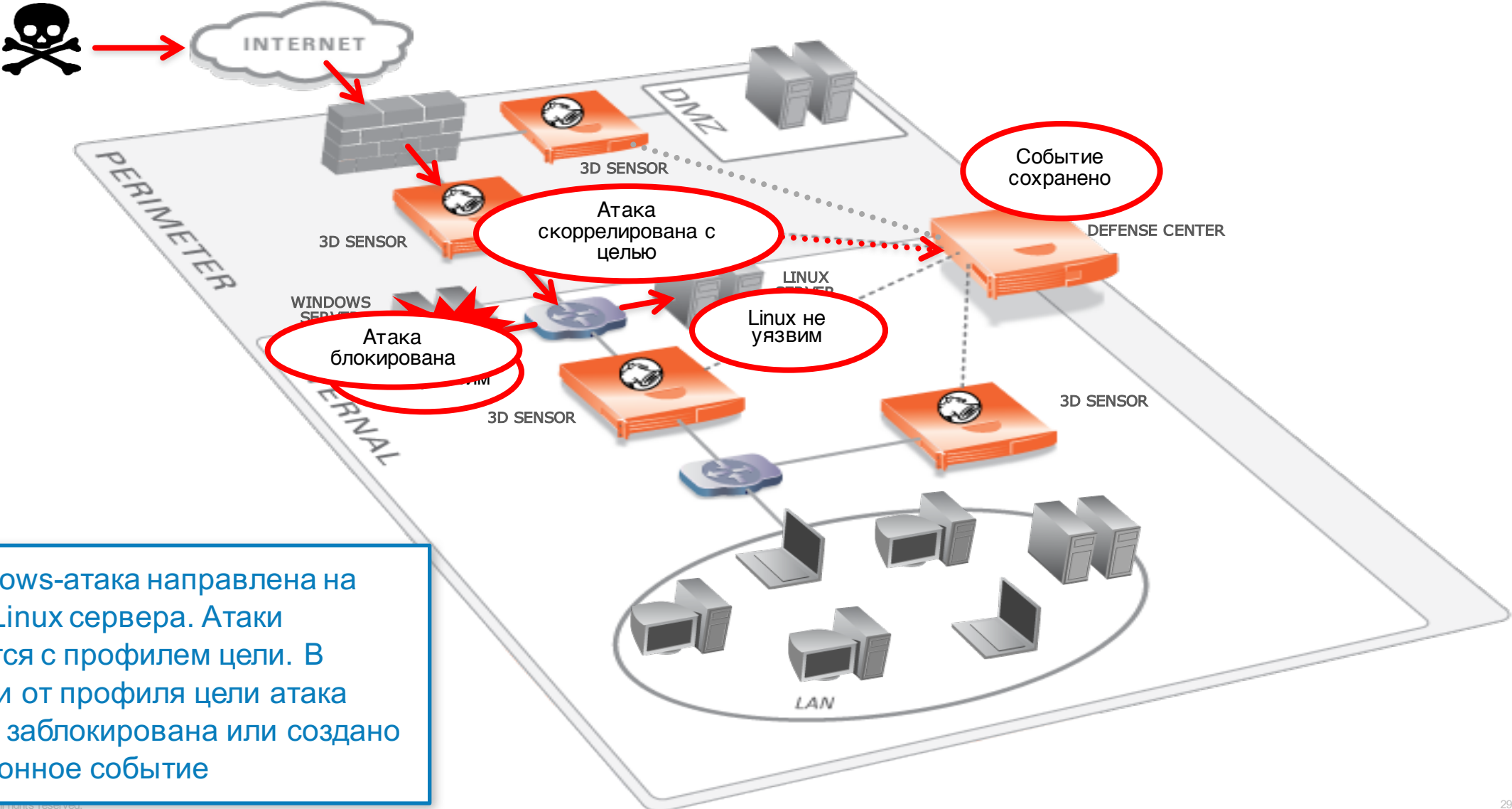
Application Protocol	Client
<input type="checkbox"/> AOL Instant Messenger	<input type="checkbox"/> AOL Instant Mess
<input type="checkbox"/> SSH	<input type="checkbox"/> OpenSSH
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client

Vendor	Product	Version	Source
Google	Android	4.0.3	FireSIGHT

Protocol	Port	Application Protocol	Vendor and Version
tcp	443	<input type="checkbox"/> HTTPS	
tcp	22	<input type="checkbox"/> SSH	OpenSSH 5.3

Users	2012-07-05 18:49:06	2012-07-06 18:49:06
Yi Lu (yilu, LDAP)		

Корреляция событий безопасности



Новая Windows-атака направлена на Windows и Linux сервера. Атаки сравниваются с профилем цели. В зависимости от профиля цели атака может быть заблокирована или создано информационное событие

Автоматизированная, комплексная защита от угроз

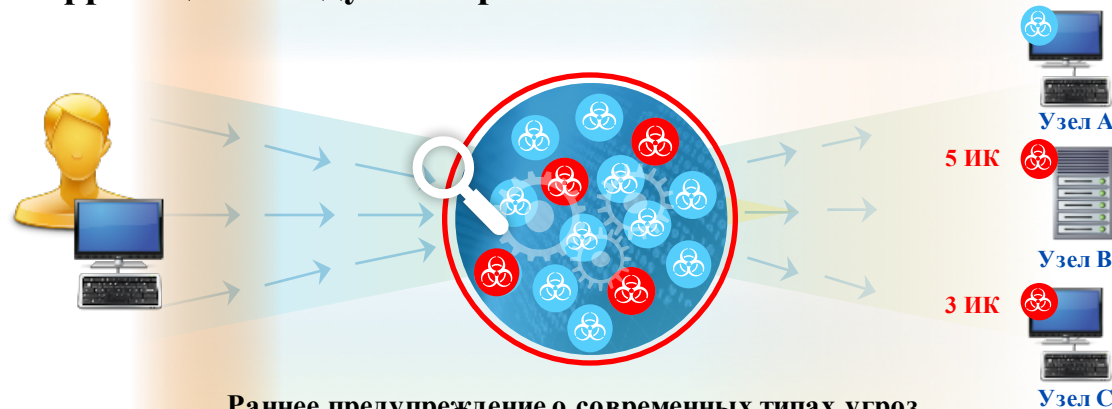
Непревзойденная защита в течение всего жизненного цикла атаки

Корреляция между контекстом и угрозами



Оценка вредоносного воздействия

Корреляция между векторами атаки



Раннее предупреждение о современных типах угроз

Динамические механизмы безопасности



Адаптация политик к рискам

Ретроспективная защита



Сокращение времени между обнаружением и нейтрализацией

Система корреляции событий

- Правила корреляции могут включать любые условия и их комбинации на базе идентифицированных в сети данных

Приложения

Уязвимости

Протоколы

Пользователи

Операционные системы

Производитель ОС

Адреса

Место в иерархии компании

Статус узла и т.п.

The screenshot shows a rule configuration page for 'Critical phone Attacks'. The rule description is 'Attacks on Executives Android-based phones' and the rule group is 'Executive Attacks'. The rule is configured with the following conditions:

- Event Type:** an intrusion event occurs
- Conditions:**
 - Impact Flag is 1 - red (Vulnerable)
 - Inline Result is not dropped

The rule is also qualified by host and user profiles:

- Host Profile Qualification:** Only generate an event if the host(s) involved have the following properties:
 - Destination Host Operating System has the following properties:
 - OS Vendor is Google
 - OS Name is Android
 - OS Version is any
 - Destination Host Jailbroken is Yes
- User Identity Qualification:** Only generate an event if the user(s) involved have the following properties:
 - Identity on Destination Department is Executives

Дополнительная система корреляции событий

- Различные типы события для системы корреляции

Атаки / вторжение

Активность пользователя

Установлено соединение

Изменение профиля трафика

Вредоносный код

Изменение инвентаризационных данных (например, появление нового узла в сети или ОС на узле)

Изменение профиля узла

Появление новой уязвимости

Overview Analysis **Policies** Devices Objects FireAMP Health System Help admin

Access Control Intrusion Files Network Discovery Application Detectors Users **Correlation** Actions

Alerts Remediations Groups

Policy Management **Rule Management** White List Traffic Profiles

Rule Information

Rule Name

Rule Description

Rule Group

Select the type of event for this rule

If and it meets the following conditions:

Rule

Snoot generates an event, snooze for hours

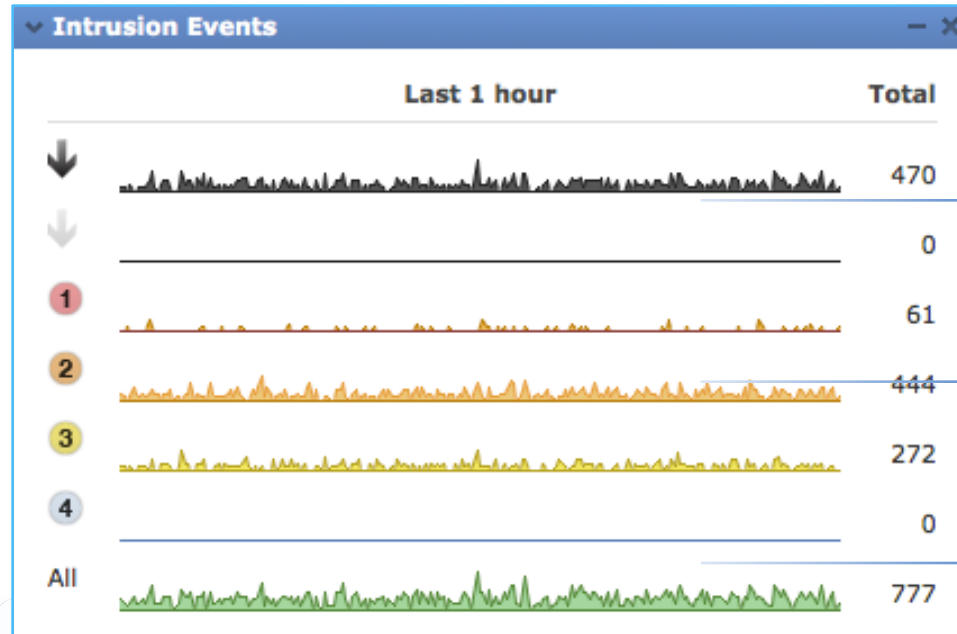
Inactive Periods There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

Автоматизация создания и настройки политик

The screenshot displays a web-based interface for managing intrusion events and policies. On the left, a window titled "Intrusion Events" shows a "Last 1 hour" view with a series of line graphs. The graphs are color-coded and numbered 1 through 4, with an "All" option at the bottom. Graph 1 is red, 2 is orange, 3 is yellow, and 4 is green. The "All" graph is also green. On the right, a "Policy Information" panel is open, showing details for a policy named "Default Production Demo Lab IPS Policy". The description is "Sourcefire Provided. For best results, do not modify." and "Drop when Inline" is checked. The "Base Policy" is set to "Security Over Connectivity", which is up to date. The policy defines 0 variables and has 9038 enabled rules: 558 generate events and 8480 drop and generate events. FireSIGHT recommends 7154 rule state settings for 7430 hosts: 214 to generate events, 3550 to drop and generate events, and 3390 to be disabled. The policy is not using these recommendations. The last generated time is 2013 Oct 10 10:15:33. At the bottom right of the panel are "Commit Changes" and "Discard Changes" buttons.

Анализ сети, протоколов, приложений, сервисов, устройств, ОС, уязвимостей и др. позволяет автоматизировать создание политик и правил МСЭ и IPS

Оценка вредоносного воздействия



Каждому событию вторжения присваивается уровень воздействия атаки на объект

УРОВЕНЬ ВОЗДЕЙСТВИЯ	ДЕЙСТВИЯ АДМИНИСТРАТОРА	ПРИЧИНЫ
 1	Немедленно принять меры, опасность	Событие соответствует уязвимости, существующей на данном узле
 2	Провести расследование, потенциальная опасность	Открыт соответствующий порт или используется соответствующий протокол, но уязвимости отсутствуют
 3	Принять к сведению, опасности пока нет	Соответствующий порт закрыт, протокол не используется
 4	Принять к сведению, неизвестный объект	Неизвестный узел в наблюдаемой сети
 0	Принять к сведению, неизвестная сеть	Сеть, за которой не ведется наблюдение

Использование информации об уязвимостях

Users (no user history available)

Attributes ▾ 

Host Criticality None

Host Protocols ▾

Protocol	Layer
icmp	Transport
tcp	Transport
udp	Transport
IP	Network

Vulnerabilities (362) ▾ 

Name
Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability
Adobe Flash Player and AIR 'intf_count' Integer Overflow Vulnerability
Adobe Flash Player and AIR (CVE-2009-1866) Stack Buffer Overflow Vulnerability

Vulnerability Detail

Sourcefire Vulnerability ID	94754
Snort ID	15728, 15729, 15727, 19268, 19269, 19270, 19271, 19272, 19273, 19274, 19275, 19276, 19277, 19278, 19279, 19280
BugTraq ID	35759, 44503
WebPage	title,OoApp Guestbook XSS vuln. author,rakstija r0t3d3v1l url,http://pridels0.blogspot.com/2005/12/ooapp-guestbook-xss-vuln.html
CVE ID	2009-1862
Title	Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability
Impact Qualification	<input type="button" value="Enabled"/>
Date Published	2009-07-21
Vulnerability Impact	8
Remote	TRUE
Available Exploits	
Description	Multiple Adobe products are prone to a remote code-execution vulnerability.
Technical Description	Adobe Acrobat and Reader are applications for handling PDF files. Adobe Flash Player is a multimedia application. The applications are available for multiple platforms. Acrobat, Reader, and Flash Player are prone to a remote code-execution vulnerability that arises in the Adobe ActionScript Virtual Machine and affects the 'flash9f.dll' and 'authplay.dll' modules. Specifically, an arbitrary value for an object scope can be placed on the stack as a memory address and then later referenced by a call to 'MethodEnv::findproperty'. This call will reference heap memory containing arbitrary code specified by the attacker and will allow code execution in the context of the user running the affected application. The attacker can exploit this issue by supplying a malicious Flash ('.swf') file or by embedding a malicious Flash application in a PDF file. Failed attempts will likely result in denial-of-service conditions. The issue affects the following: Reader and Acrobat 9.1.2 Flash Player 9 and 10 Updates are available. Please see the references for details.
Solution	

Additional Information ▶

Fixes ▾

Upgrade Flash-player-10.0.32.18-1.i586.rpm	Download
Patch MacOSXUpd10.6.1.dmg	Download
Patch MacOSXServerUpd10.6.1.dmg	Download
Patch SecUpd2009-005.dmg	Download
Patch SecUpdSrvr2009-005.dmg	Download
Patch SecUpd2009-005Intel.dmg Intel	Download
Patch SecUpd2009-005PPC.dmg PPC	Download

Признаки (индикаторы) компрометации



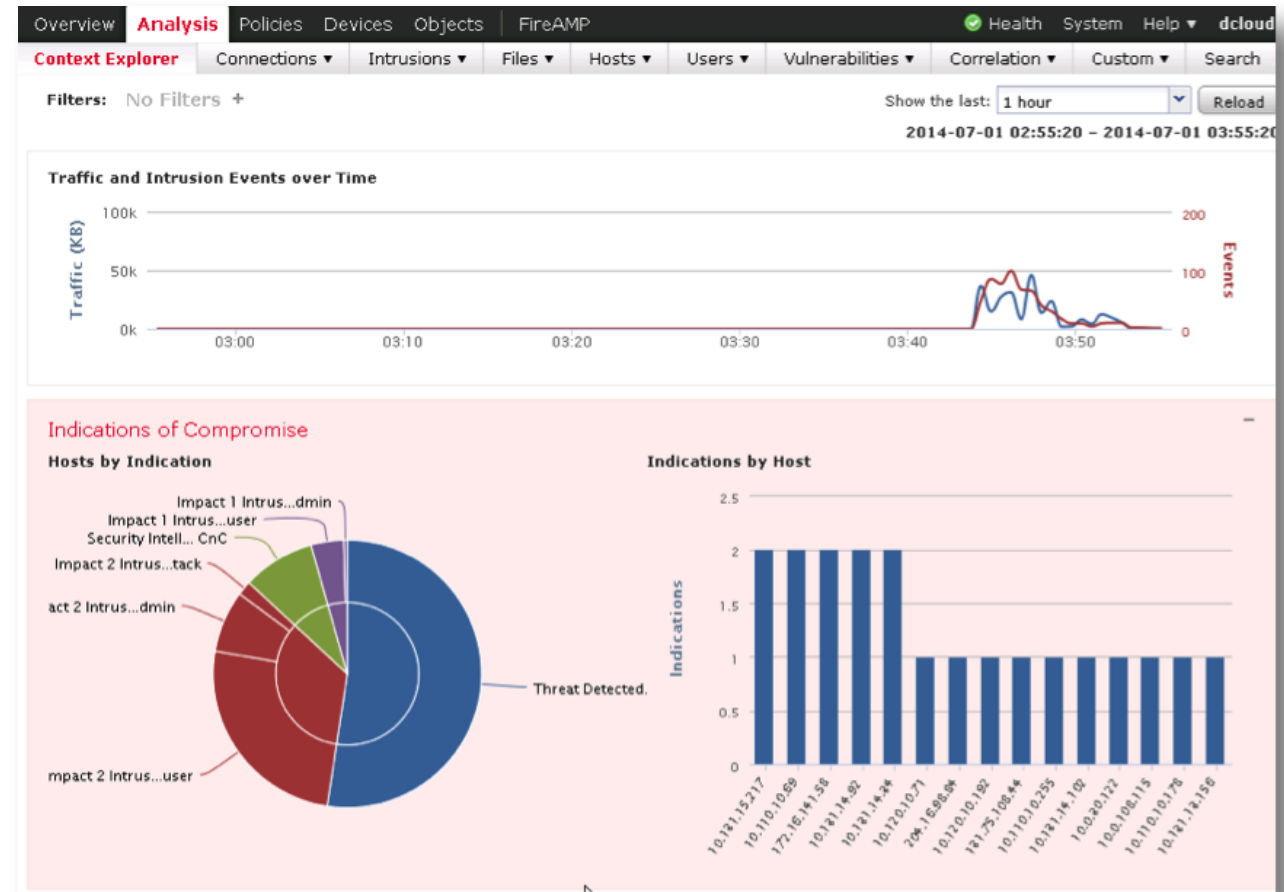
Indications of Compromise (3)

Edit Rule States Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2013-09-17 16:52:11	2013-09-20 03:55:45
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2013-09-17 20:09:23	2013-09-19 17:32:49

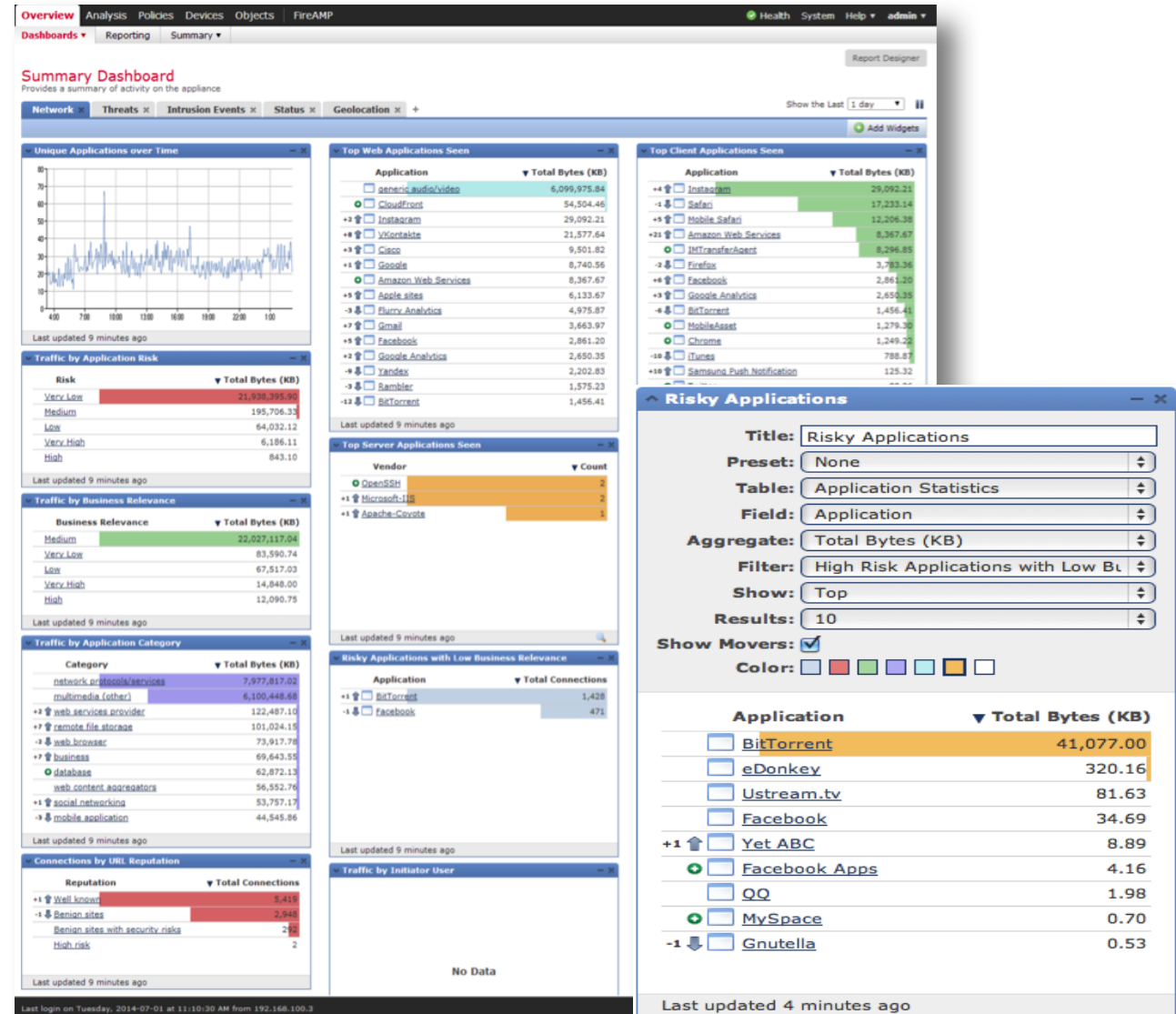
Мониторинг общей информации о сети

- Корреляция событий безопасности, трафика и вредоносного кода
- Активность конкретных пользователей и их приложений
- Используемые ОС и активность сетевого обмена
- Оценка событий по уровню воздействия и приоритета
- Статистика по вредоносному коду и зараженным файлам
- Геолокационные данные
- Категории сайтов и посещаемые URL



Мониторинг сетевых событий

- Использование сервисов
- Использование приложений
- Использование операционных систем
- Распределение соединений
- Активность пользователей
- Уязвимые узлы и приложения
- И т.д.



Мониторинг событий безопасности

- Основные нарушители
- Основные атаки
- Заблокированные атаки
- Основные цели
- Приоритет событий
- Уровень воздействия



Детализация событий безопасности

- Подробная информация о событии безопасности
- Возможность изменения правил реагирования
- Возможность тюнинга правила / сигнатуры
- Сетевой дамп

The screenshot displays the Cisco FireAMP interface, specifically the 'Events' section. The main heading is 'Events By Priority and Classification'. The event details are as follows:

Event	EXPLOIT Microsoft IIS ASP handling buffer overflow attempt (3:15974)
Timestamp	2014-07-01 06:02:05
Classification	Web Application Attack
Priority	high
Ingress Security Zone	Zone A
Device	198.18.133.11
Ingress Interface	eth1
Source IP	10.131.10.108
Source Port / ICMP Type	52914 / tcp
Destination IP	10.131.12.163
Destination Port / ICMP Code	80 (http) / tcp
Intrusion Policy	Cisco Security BG - Production Demo IPS Policy
Access Control Policy	Cisco Security BG - Production Demo AC Policy
Rule	alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"EXPLOIT Microsoft IIS ASP handling buffer overflow attempt"; sid:15974; gid:3; rev:3; classtype:web-application-attack; reference:bugtraq,27676; reference:cve,2008-0075; reference:url,technet.microsoft.com/en-us/security/bulletin/ms08-006; metadata:engine shared, soid 3 15974, service http, policy balanced-ips drop, policy security-ips drop;)
Summary	This event is generated when an attempt is made to exploit a known vulnerability in Internet Information Server.

Actions

- Rule Actions
 - [Edit](#)
 - [View Documentation](#)
 - [Rule Comment](#)
 - [Disable in current policy \(Cisco Security BG - Production Demo IPS Policy \)](#)
 - [Set this rule to drop the triggering packet and generate an event in current inline intrusion policy \(Cisco Security BG - Production Demo IPS Policy \)](#)
 - [Set this rule to generate events in all locally created policies](#)
 - [Disable this rule in all locally created policies](#)
 - [Set this rule to drop the triggering packet and generate an event in all locally created inline intrusion policies](#)
- Set Thresholding Options
 - ▶ in the current policy (Cisco Security BG - Production Demo IPS Policy)
 - ▶ in all locally created policies
- Set Suppression Options
 - ▶ in the current policy (Cisco Security BG - Production Demo IPS Policy)
 - ▶ in all locally created policies

Packet Information

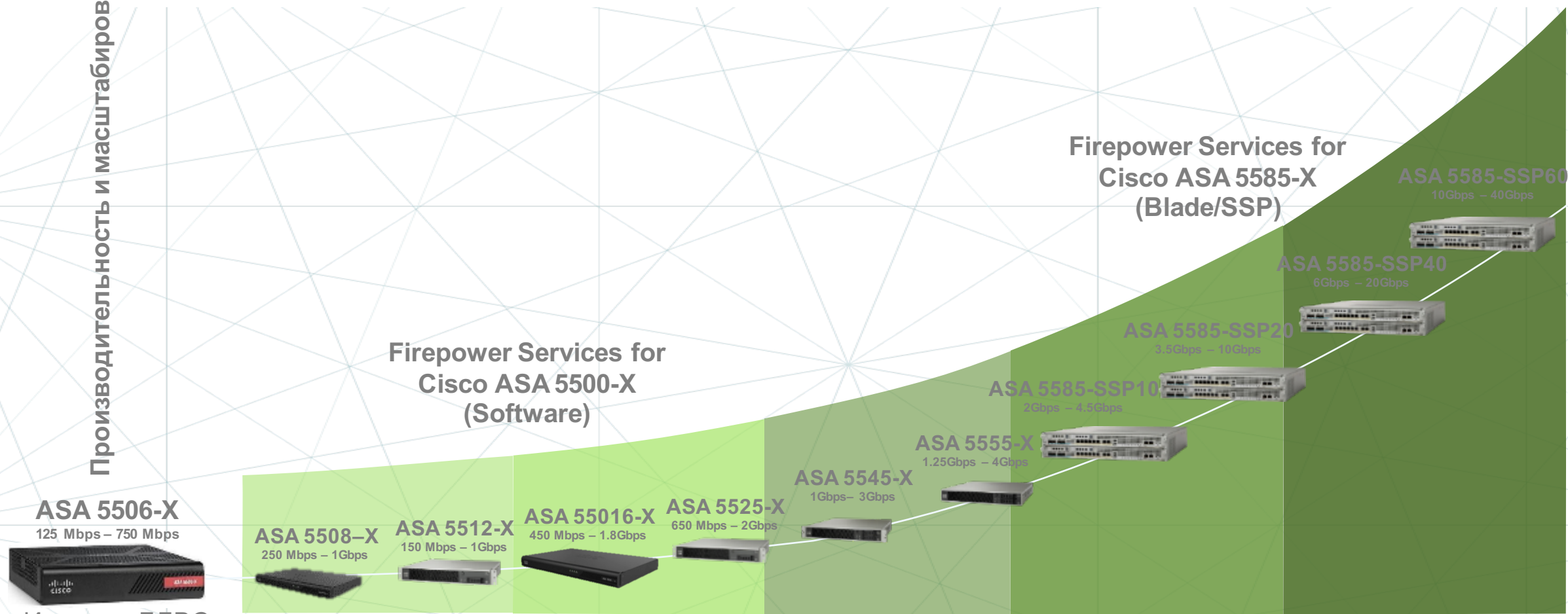
FRAME 1 (Expand All)

Платформы



ASA Продуктовое портфолио

Производительность и масштабирование

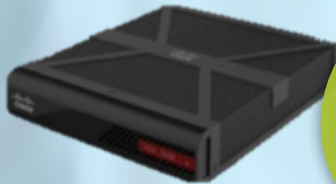


Имеются БЛВС и
Индустриальная
версии

Старые модели ASA	ASA 5505	ASA 5510	ASA 5520	ASA 5540	ASA 5550	ASA 5580
-------------------	----------	----------	----------	----------	----------	----------

Новые модели Cisco ASA with FirePOWER Services

5506-X



Идеальна
для
замены
Cisco®
ASA 5505

Desktop Model

100% NGFW -
поставляется с AVC

5506W-X



Integrated
Wireless AP

Wi-Fi может управляться
локально или через
Cisco WLC

5508-X
5516-X



Выше
производительность

1RU; новая платформа —
лучшее сочетание цены
и производительности

5506H-X



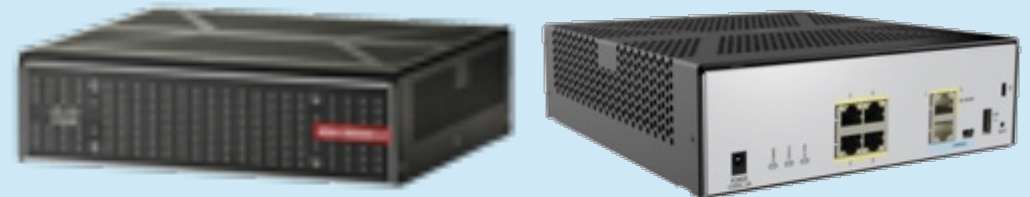
Для АСУ ТП

NGFW для критичных
инфраструктур и
объектов

Cisco ASA 5506H-X в защищенном исполнении

*** Конфигурация Cisco® ASA 5506-H идентична Desktop ASA 5506-X, исключая следующие параметры:

Параметр	Значение
Порты	4 x портов данных
Управление	1 порт, 10/100/1000BASE-T, 100BASE-FX, 1000BASE-X, SFP
Напряжение	5V (***) 5506 is 12V)
Диапазон температур	От -20 до 60°C (рабочий) От -40 до 85°C (обычный)
Монтаж	Wall-Mount, Horizontal Desk, Rack-Mount и DIN rail-mount



9 x 9.2 x 2.5 in.

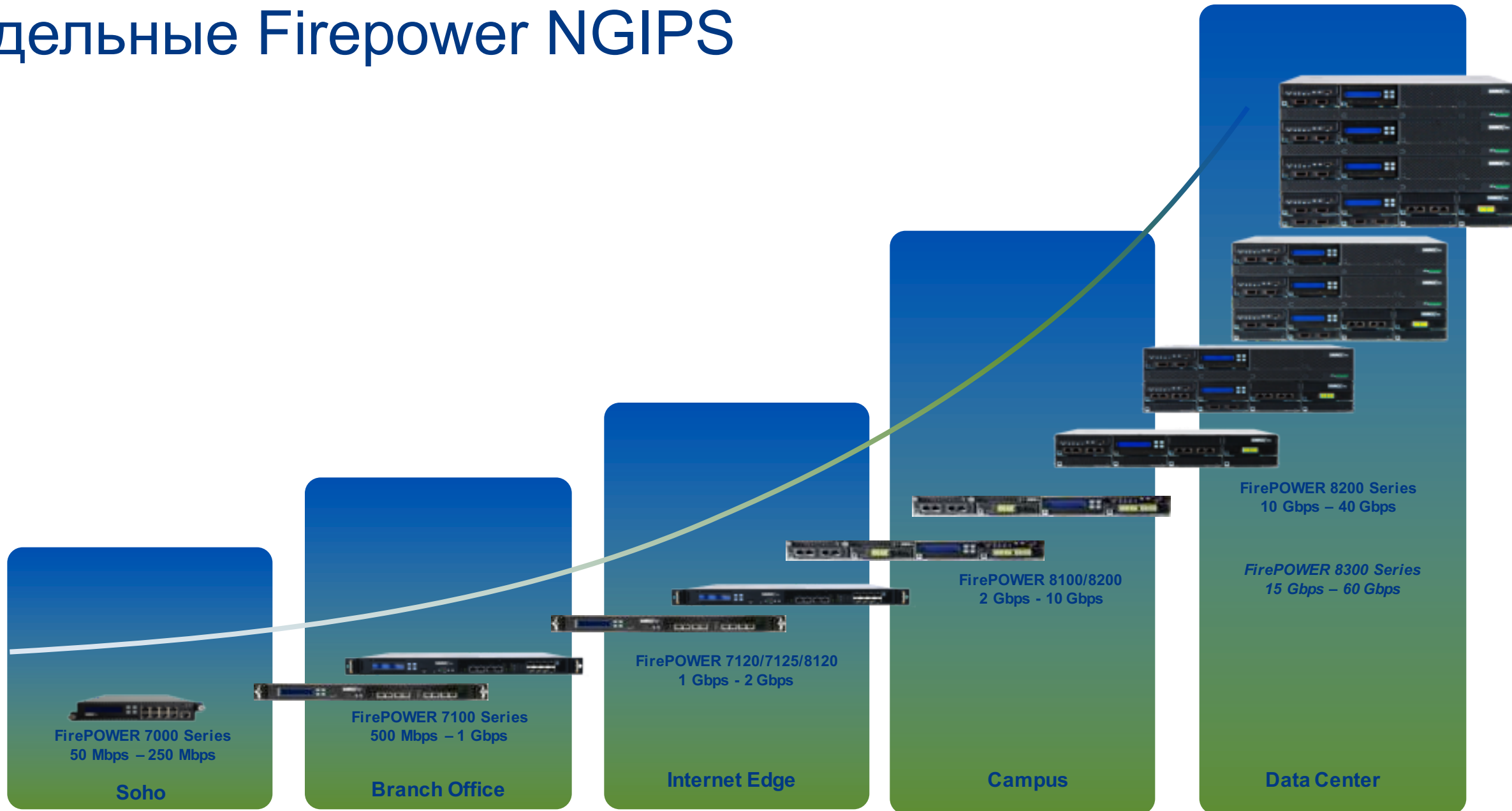
Промышленный МСЭ/IDS Cisco ISA 3000



- Производительность: 2 Gbps
- Кол-во IPSec/SSL VPN: 25
- IPv4 MAC Security ACE: 1000
- Кол-во интерфейсов: 4x1GE или 2xGE, 2xFiber (SFP)
 - Медный: 4x10/100/1000BaseT
 - Оптический: 2x1GbE (SFP), 2x10/100/1000BaseT
- 4 ядра Intel Rangely, SSD 64 GB
- 8 GB DRAM, 16 GB Flash
- Питание DC
- Исполнение: -40C до 60C без обдува; -40C до 70C с 40LFM; -34C до 74C с 200LFM

Отдельные Firepower NGIPS

Производительность и масштабирование



FirePower 8200 & 8300 Series



8250 / 8350
10 Gbps / 15 Gbps



8260 / 8360
20 Gbps / 30 Gbps



8270 / 8370
30 Gbps / 45 Gbps

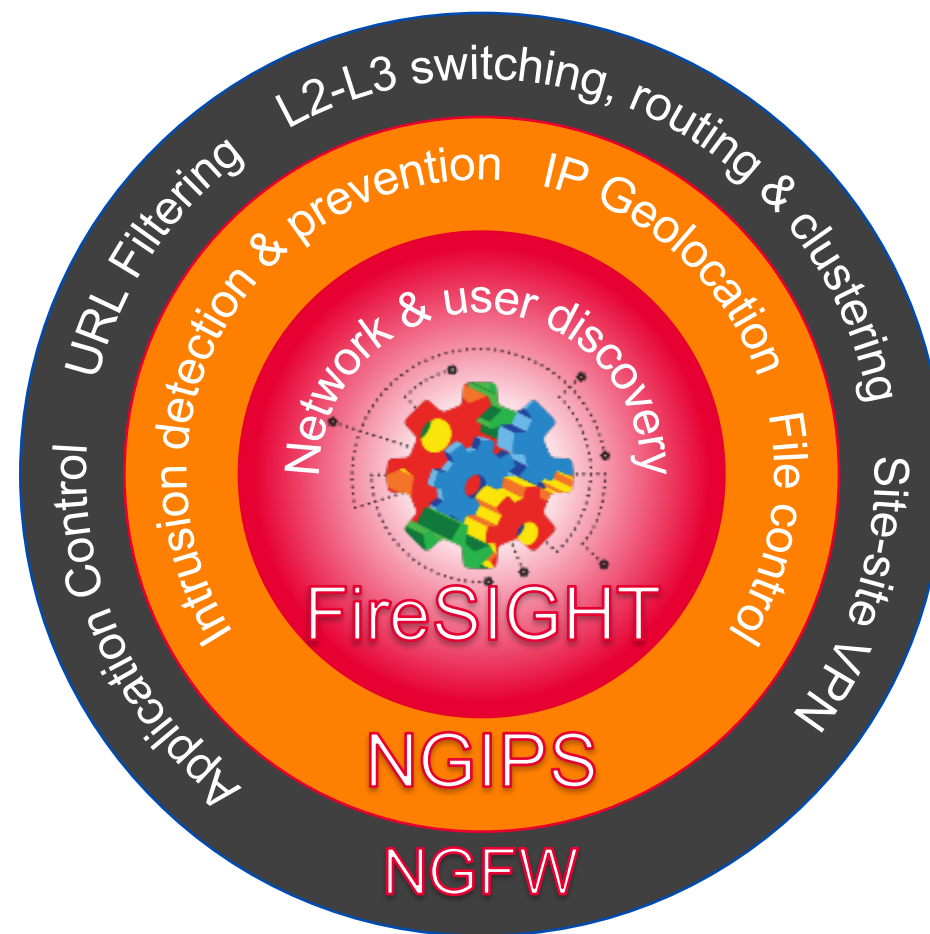


8290 / 8390
40Gbps / 60 Gbps

- Обычно используется в ЦОД
- Стекируемая конфигурация
- Возможность расти с увеличением потребностей
- Каждая серия стекируется только с такой же моделью

FirePower Management Centre (FireSight)

- Контекст и пользователи коррелируются MC
- Контроль доступа осуществляется встроенным NGIPS
- Приложения и их контроль доступа, свичинг и роутинг осуществляется NGFW



Cisco FirePower Management Center Models



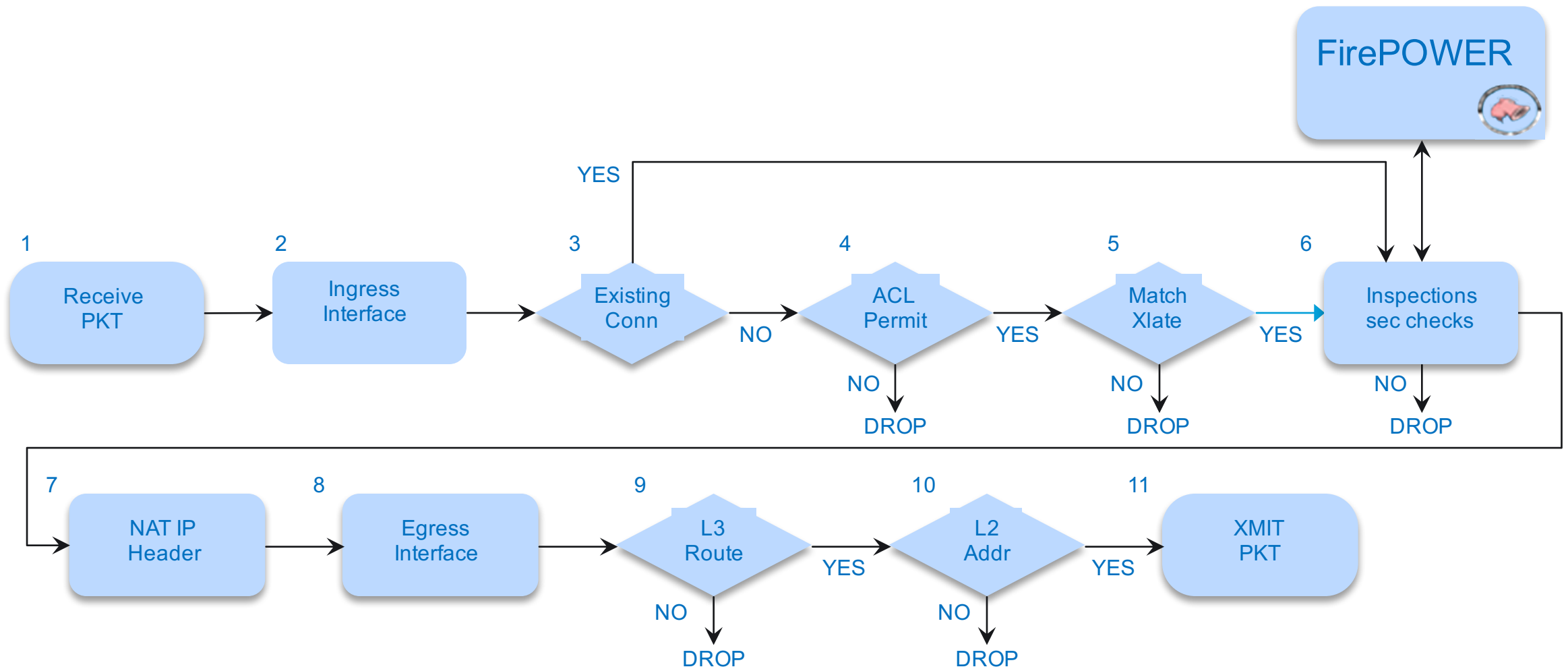
Feature	FireSIGHT FS750	FireSIGHT FS1500	FireSIGHT FS2000	FireSIGHT FS3500	FireSIGHT FS4000	FireSIGHT FS-VMW-SW
Maximum number of sensors managed	10	35	70	150	300	25 10 2
Maximum number of IPS events	20 million	30 million	60 million	150 million	300 million	10 million
Event storage	100 GB	125 GB	1.8TB	400 GB	4.8 TB	250 GB
Maximum network map (hosts/users)	2,000/2,000	50,000/50,000	150,000/150,000	300,000/300,000	600,000/600,000	50,000/50,000
Maximum flow rate (flows per second)	2,000 fps	6,000 fps	12,000 fps	10,000 fps	20,000 fps	Varies [*]
Network Interfaces	2 x 1Gbps	2 x 1Gbps	2 x 1Gbps 2 x 10Gbps (Optional SFP's available via CCW)	2 x 1Gbps	2 x 1Gbps 2 x 10Gbps (Optional SFP's available via CCW)	1 x 1Gbps
High availability	Lights-out management (LOM)	RAID 1, LOM, high-availability pairing	RAID 5, LOM, high-availability pairing	RAID 5, LOM, high-availability pairing	RAID 5, LOM, high-availability pairing	No

For ASA FP or Virtual FP only

Развитие NGFW

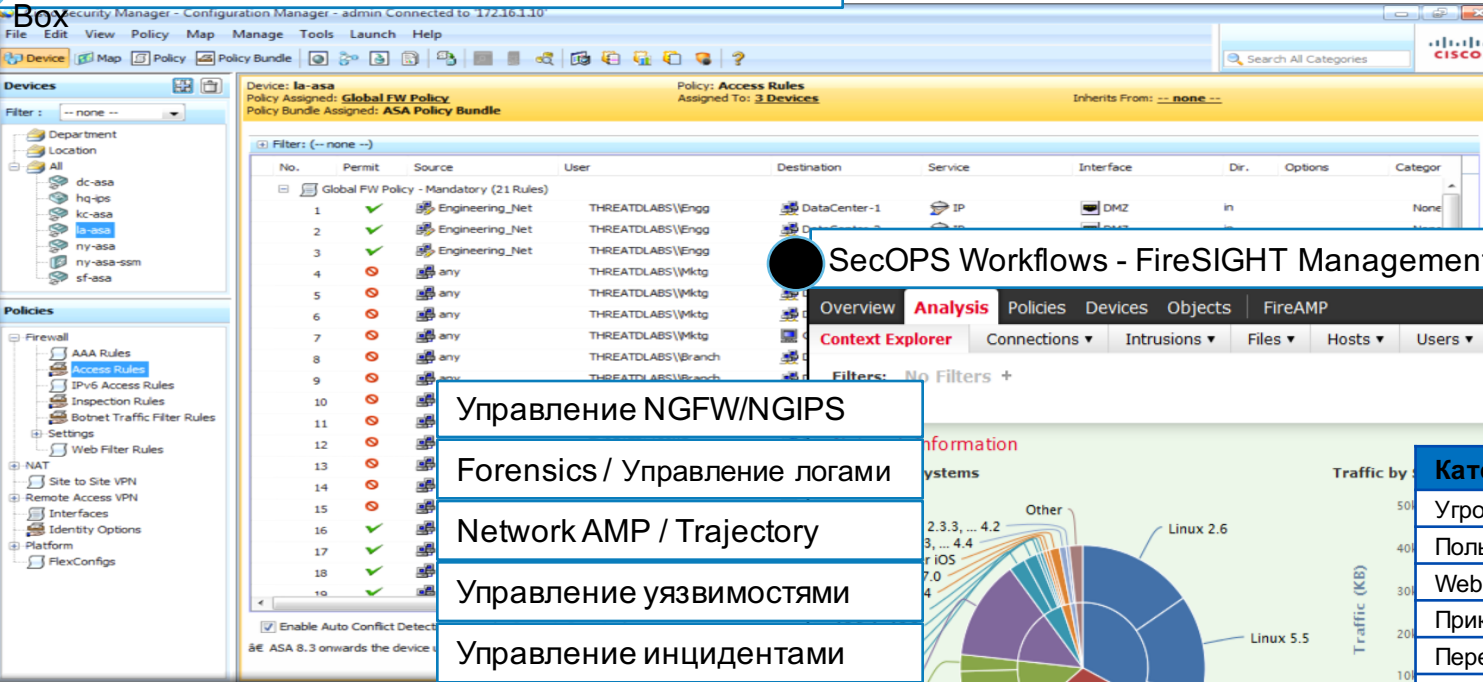


ASA FirePower. Алгоритм обработки пакетов



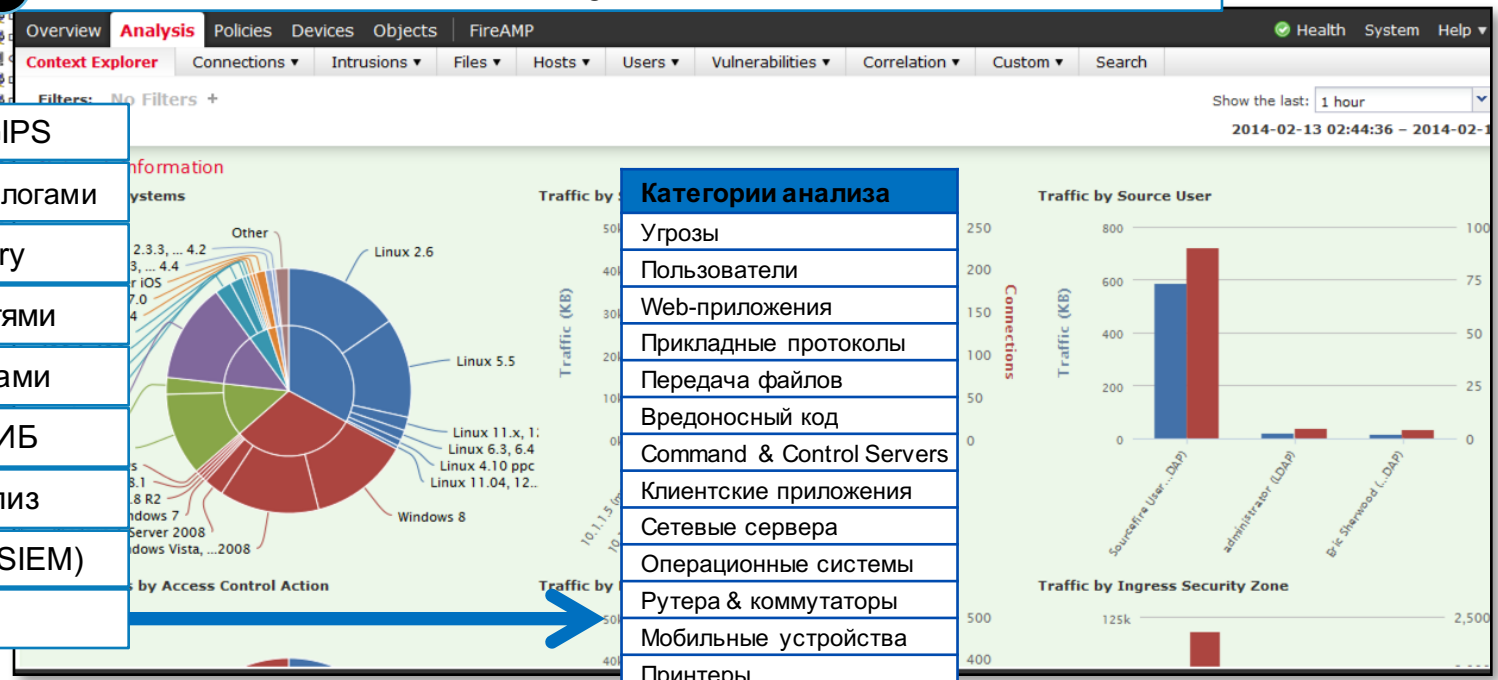
Управление ASA FirePower требует наличия двух систем!

NetOPS Workflows - CSM 4.6/7 или ASDM-ASA-On-



FireAMP Connector
(Managed by FMC)

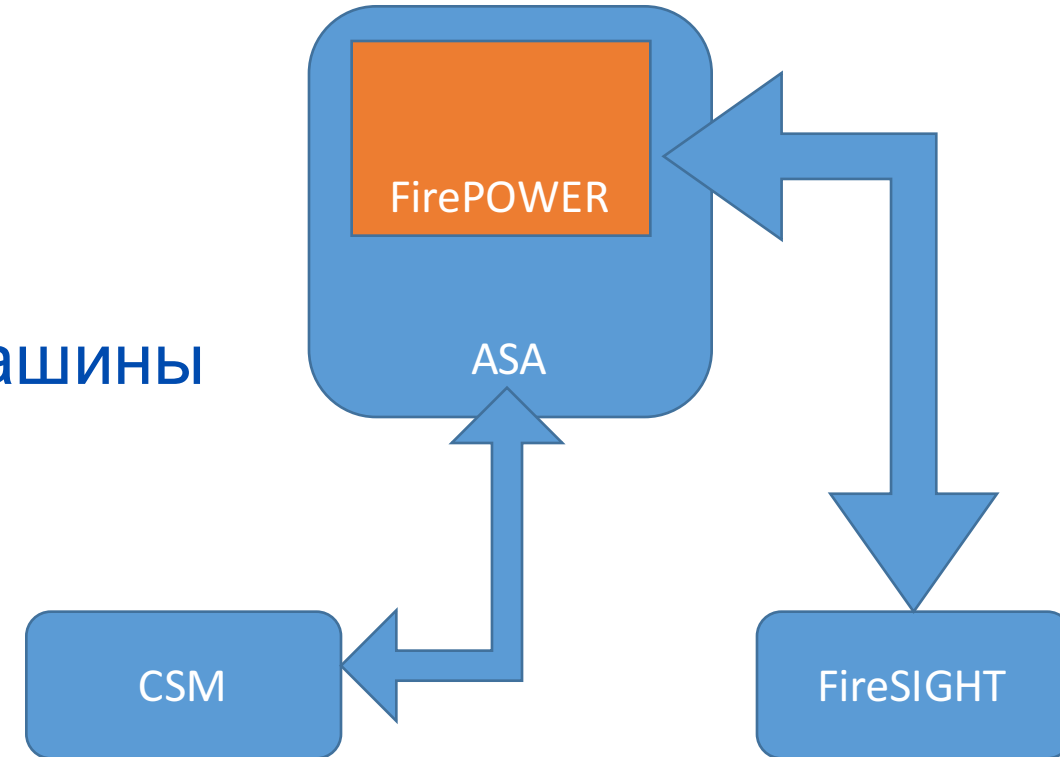
SecOPS Workflows - FireSIGHT Management Center



- Управление NGFW/NGIPS
- Forensics / Управление логами
- Network AMP / Trajectory
- Управление уязвимостями
- Управление инцидентами
- Адаптивная политика ИБ
- Ретроспективный анализ
- Корреляция событий (SIEM)
- Распознавание

Недостатки платформы

- Для ASA FirePower
- Разворачиваются два образа
- Работают две OS
- Пакеты проходят через виртуальные машины
- Дублируется функционал
- 2 интерфейса управления

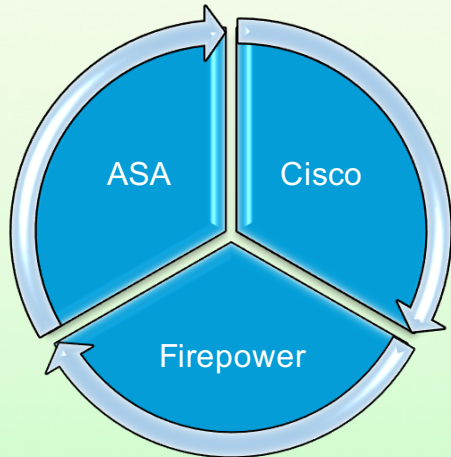


Развитие нашей стратегии безопасности

Унифицированное ПО

Routing, NAT,
Identity, Firewall,
Clustering / HA

Service
Chaining &
Orchestration



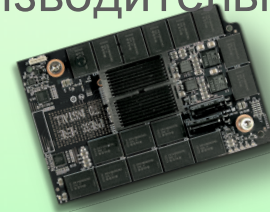
Threat prevention, advanced
malware, and application
visibility and control

Унифицированные устройства

Использование
архитектуры Cisco



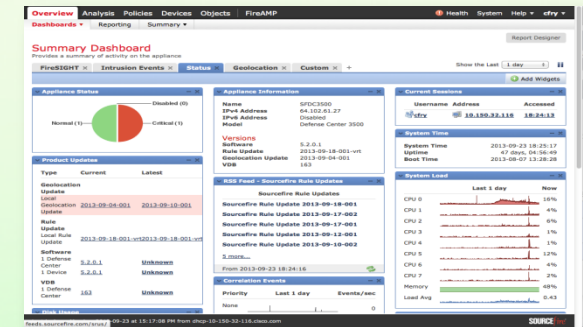
Ускорение для
максимальной
производительности



До мульти-100Гбит портов

Унифицированное управление

FireSIGHT UI с
объединенным
управлением



Firepower Threat Defense

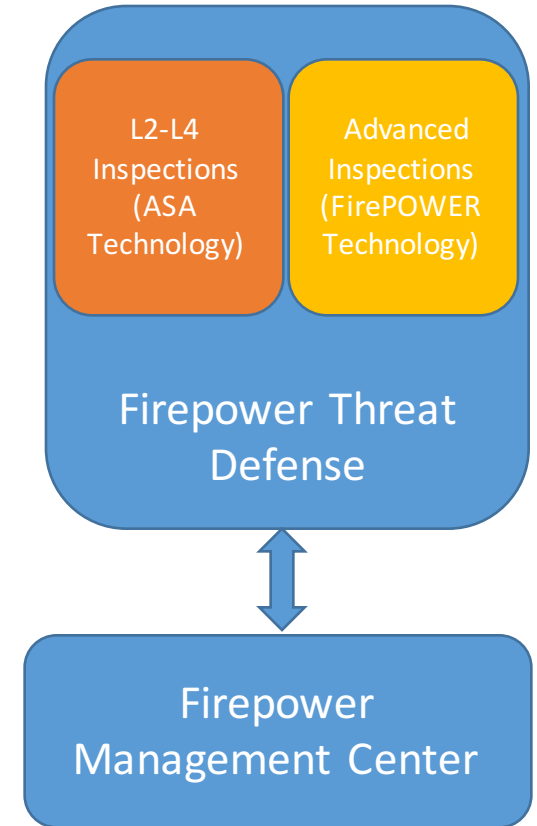
Новое предложение NGFW

Объединяет все лучшее от ASA и от FirePower

однопроходная инспекция

Не дублируется функционал*

Один интерфейс управления



НОВЫЕ ВОЗМОЖНОСТИ в Firepower Threat Defense 6.0

Threat Innovation

DNS Inspection and Sinkholing
URL-based Security Intelligence
SSL Decryption
OpenAppID
Captive Portal and Active Auth
File Property Analysis and Local
Malware Checks
ISE Identity/Device/SGT in Policy

Enterprise Management

Domains with Role-Based Access
Policy Inheritance

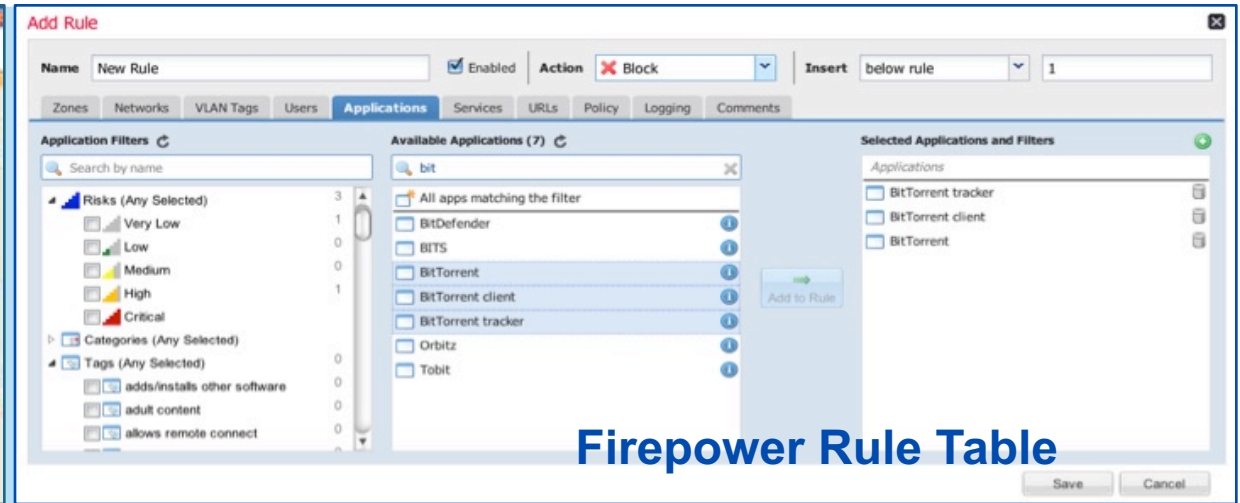
Firepower Threat Defense Image

Unified ASA and Firepower Rules
and Objects
ASA Dynamic and Static NAT
ASA Routing Support: OSPF (not
OSPFv3), BGP4, RIP, Static (not
Multicast)
Syn Cookies, Anti-Spoofing
ASA ALGs (fixed configuration)
VMware and AWS Support
Smart Licensing Support

Общее для всех платформ FirePower

Только в FIREPOWER
THREAT DEFENSE

Таблица правил с одной политикой (Firepower Threat Defense)



One Rule Table

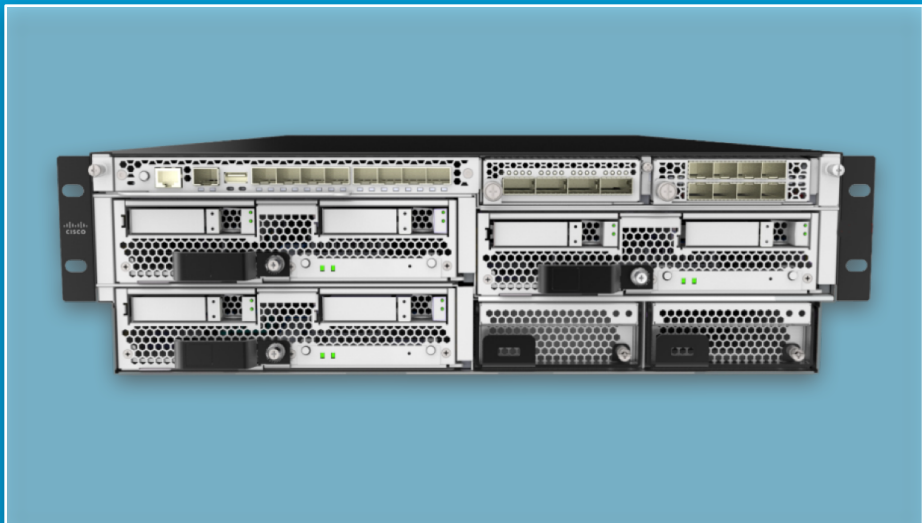
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action				
Mandatory - acl (1-5)																
1	test-rule	any	any	1.1.1.1 2.2.2.2	1.1.1.1 2.2.2.2	any	any	any	any	HTTPS	any	Block			0	
2	r2	any	any	IPv4-Private-1	any	any	any	any	any	any	any	Block			0	

Unified Policy and Objects

Сравнение функционала

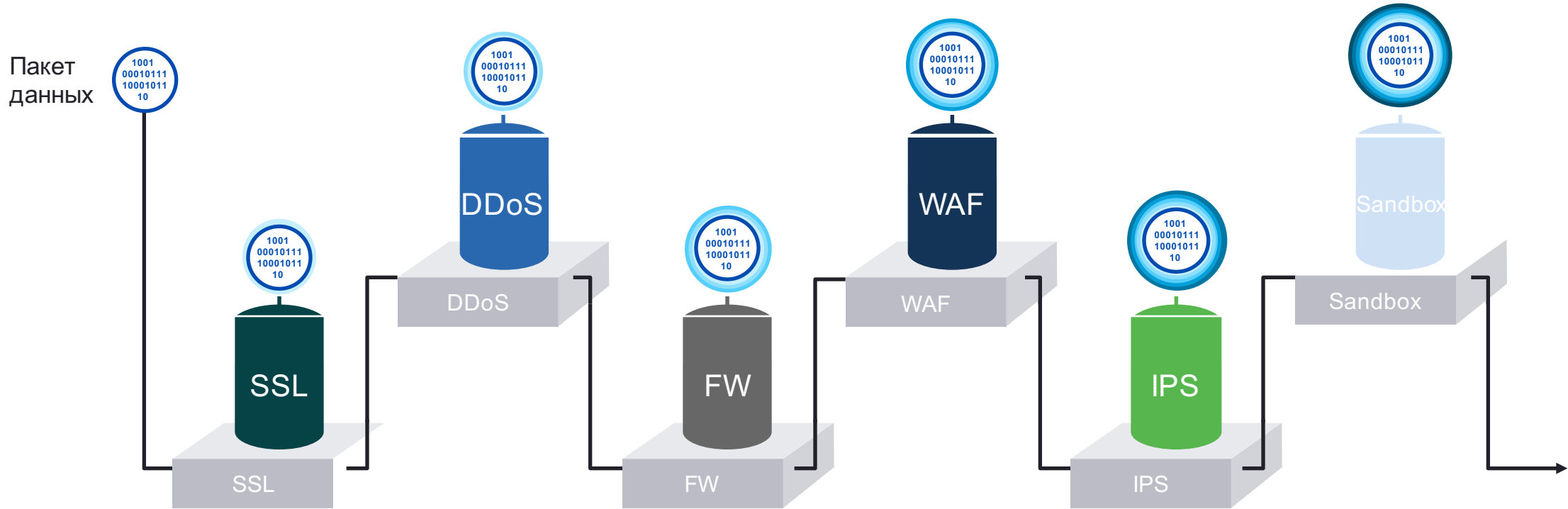
ASA with FirePOWER Services	Firepower Threat Defense
<p>ALL ASA functionality, including:</p> <ul style="list-style-type: none"> • Access Rules / Objects • Active/Passive HA & Clustering • Transparent & Routed Deployment • NAT (Dynamic & Static) • Unicast & Multicast Routing • Syn Cookies / Anti-Spoofing • Configurable ALGs • Site-to-Site & RAVPN • Multi-contexts 	<p>Phase 1 of ASA functionality (at GA):</p> <ul style="list-style-type: none"> • ASA + Firepower Rules / Objects • Active/Passive HA • Transparent & Routed Deployment • NAT (Dynamic & Static) • Unicast Routing (OSPF, BGP, RIP, Static) • Syn Cookies / Anti-Spoofing • ALGs (fixed configuration)
<p>ALL Firepower Functionality:</p> <ul style="list-style-type: none"> • User / Host / App Visibility and Control • Security Intelligence: DNS/URL/IP • Malware file lookup / dynamic analysis / IOC • URL Category and Reputation Filtering • NGIPS 	<p>ALL Firepower Functionality:</p> <ul style="list-style-type: none"> • User / Host / App Visibility and Control • Security Intelligence: DNS/URL/IP • Malware file lookup / dynamic analysis / IOC • URL Category and Reputation Filtering • NGIPS
<p>Management:</p> <ul style="list-style-type: none"> • Firepower Management Center for Firepower Services • Central Manager GUI & Full Config CLI • CSM / ADSM / CLI for ASA functions 	<p>Management:</p> <ul style="list-style-type: none"> • Firepower Management Center - Unified Manager for all functionality

Примечание: список не полный, функциональность быстро расширяется



Высокопроизводительная безопасность

Устаревшая модель безопасности



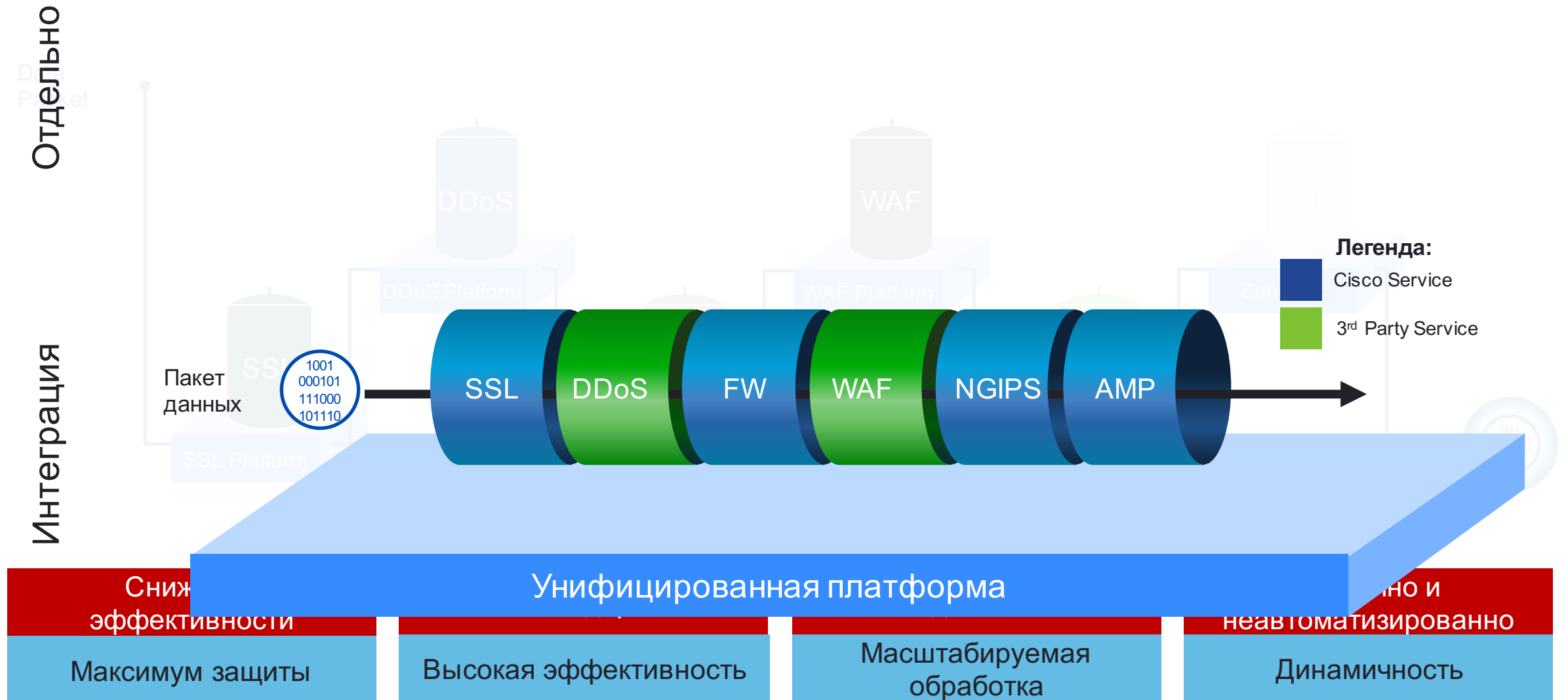
Снижение
эффективности

Рост задержек

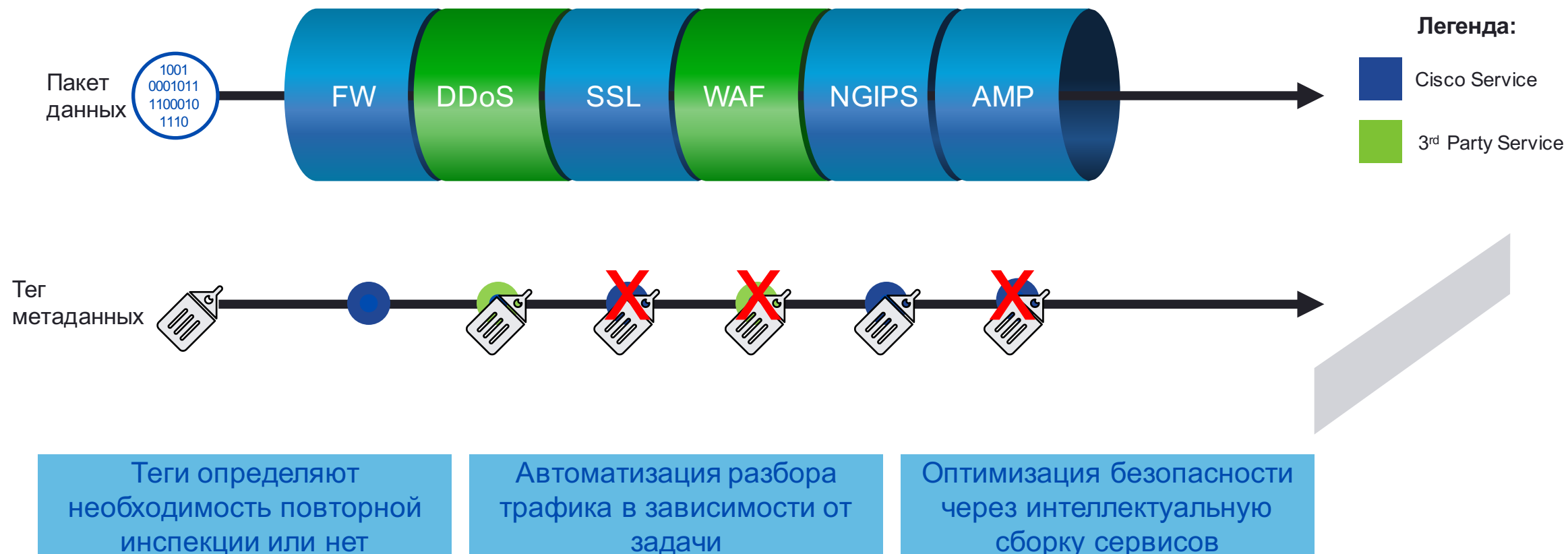
Замедление сети

Статично и
неавтоматизированно

Cisco трансформирует интеграцию сервисов ИБ



Что впереди: интеллектуальная обработка



Платформа Firepower 9300

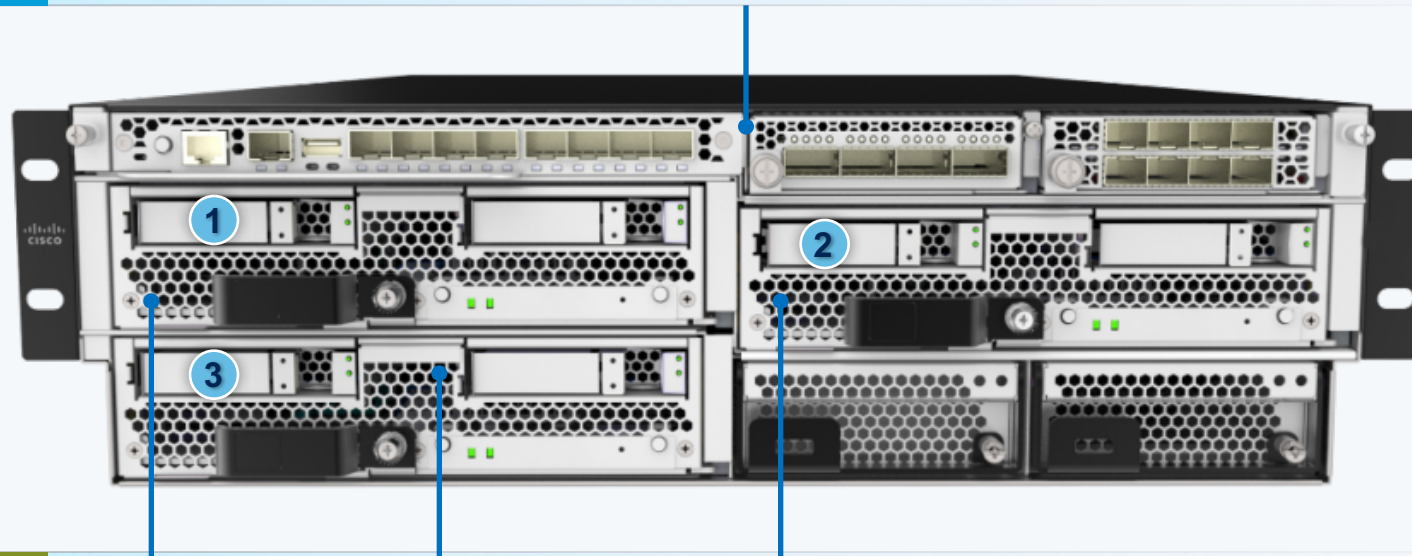
- Модульная платформа операторского класса с интерфейсами 10, 40, и 100 Гбит/с.
- Объединение сервисов безопасности компании Cisco и других компаний
- Эластичная масштабируемость за счет кластеризации
- Ускоренная обработка для доверенных приложений
- Функции ПО Cisco ASA для операторов СВЯЗИ
 - Эффективная защита на сетевом и транспортном уровне
 - Трансляция адресов операторского класса (Carrier-grade NAT)
 - Анализ протоколов GTPv1 и GTPv2 начиная с ASA 9.5(1)
 - Анализ SCTP и Diameter в планах



Обзор платформы Cisco Firepower 9300

Модуль управления

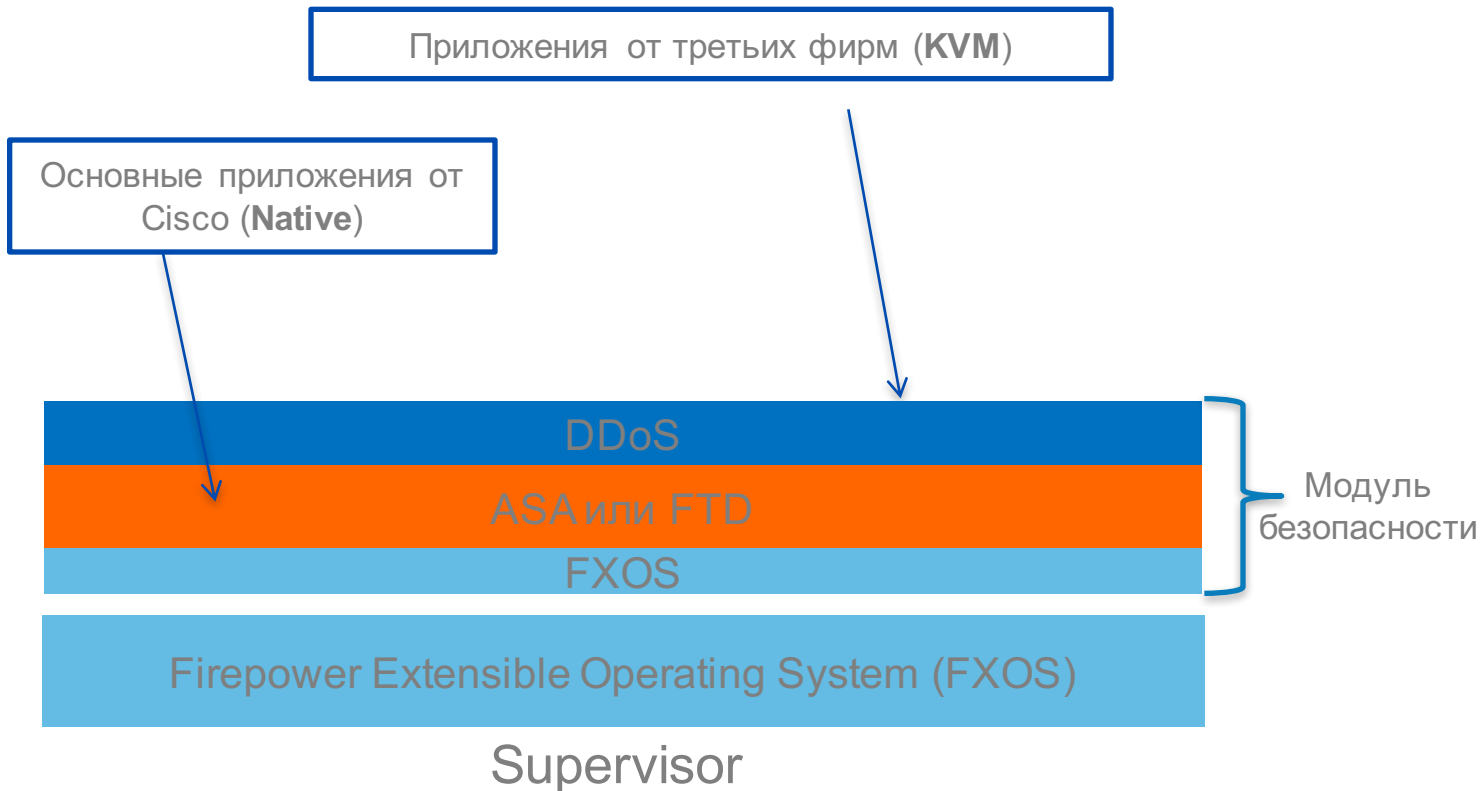
- Внедрение и управление приложениями
- Сетевые интерфейсы и распределение трафика
- Кластеризация для сервисов Cisco® ASA и прочих



Модули безопасности

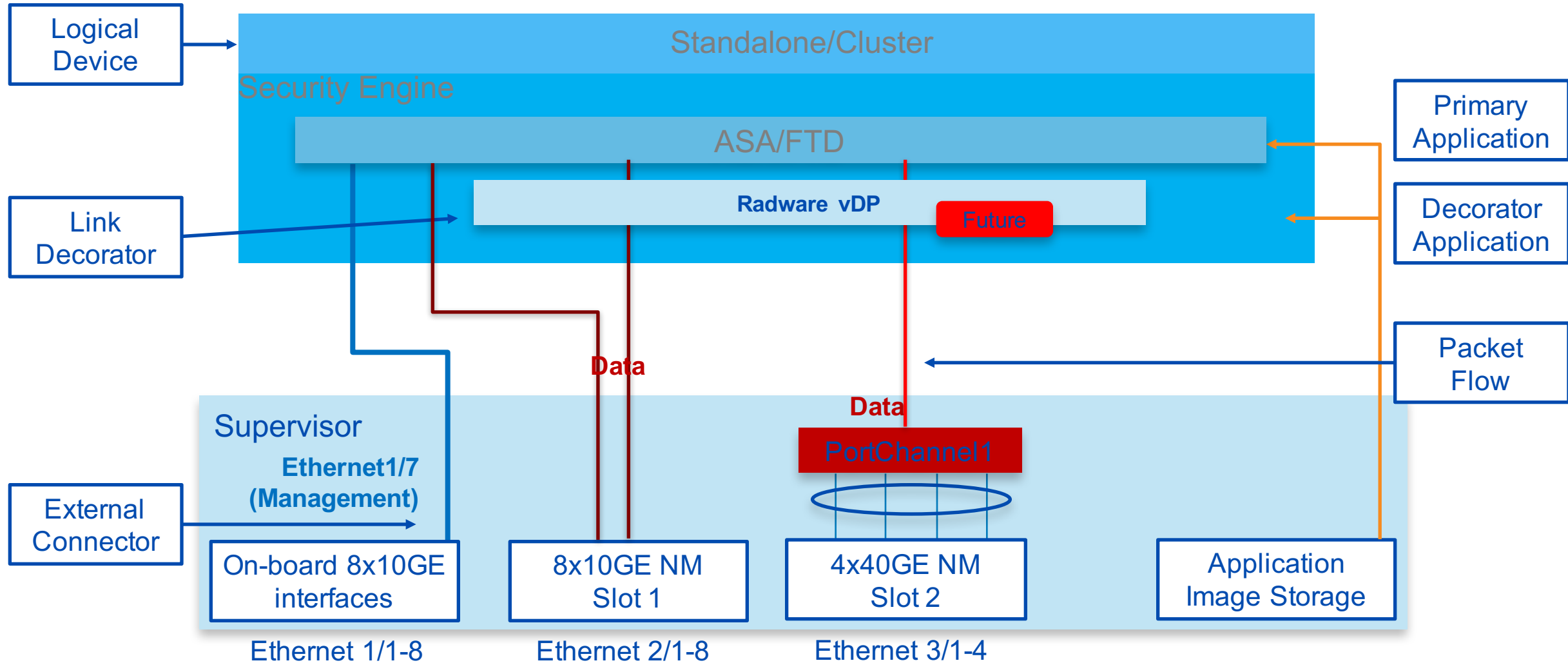
- Встроенный классификатор пакетов и потоков, а также ускоритель шифрования
- Приложения компании Cisco (МСЭ, СОВ, и т.п.) и 3-их компаний (защита от DDoS, балансировка)
- Работает отдельно или в кластере (до 240 Гбпс на шасси и более 1 Тбпс на кластер)

Программная архитектура



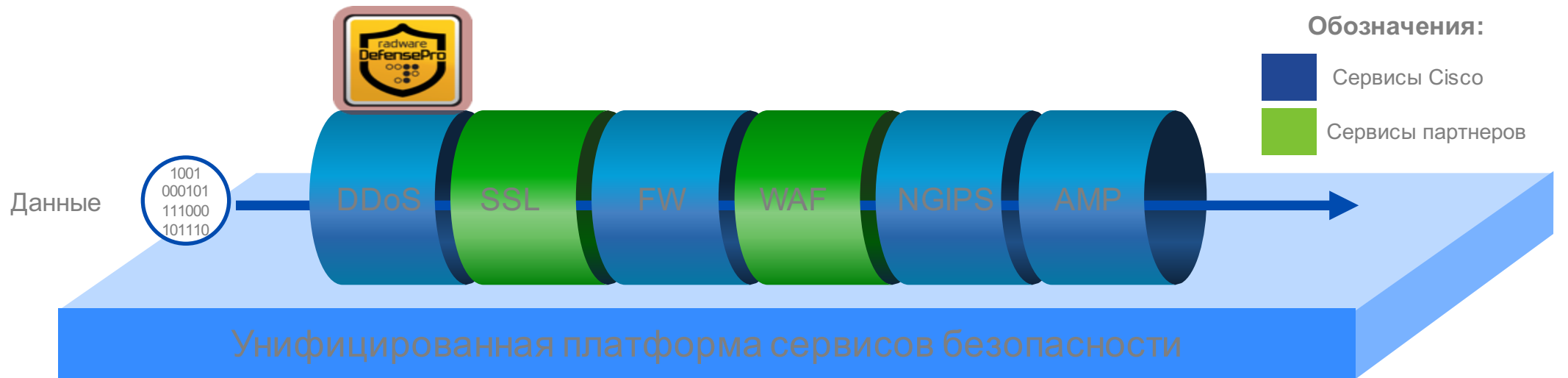
- FXOS обеспечивает интерфейс для управления устройством и его контроля для приложений безопасности на модулях безопасности
- Все образы подписаны и проверяются через Secure Boot
- Образы приложений безопасности в формате Cisco Secure Package (CSP)
 - Разные версии одних приложений могут быть сохранены на Supervisor. Они могут быть размещены на модулях безопасности по требованию
 - Содержит основные системы (например, ASA, FTD) и другие образы (например, ASDM, REST и др.)

Архитектура безопасности для новых платформ FirePower



Firepower 9300 изменяет модель интеграции сервисов

- Radware vDP – первое из приложений 3-х компаний, ставшее элементом новой архитектуры
- Защита от DDoS работает на входных интерфейсах Firepower 9300



Максимальная защита

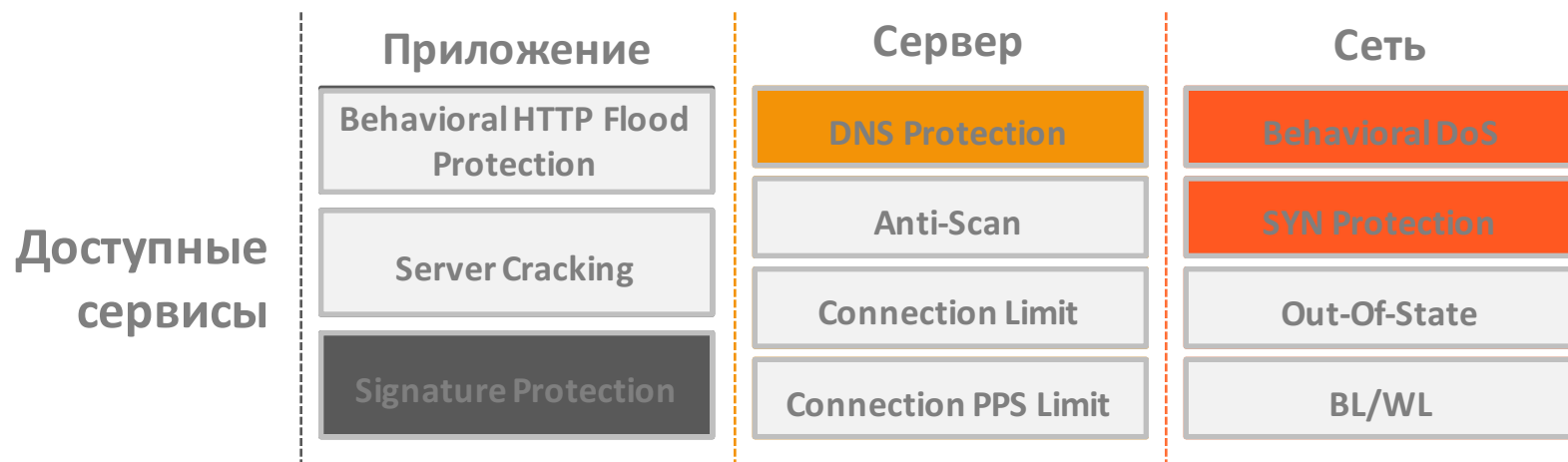
Высокая
эффективность

Масштабируемость

Гибкость

Обзор Radware vDefensePro

- Фокус на поведенческих DDoS-атаках, а не основанных на объеме



- До 10Gbps на модуль на 6 выделенных ядрах x86 CPU
- Внутришассийная кластеризация vDP позволяет обеспечить до 30Gbps на 3-х модулях

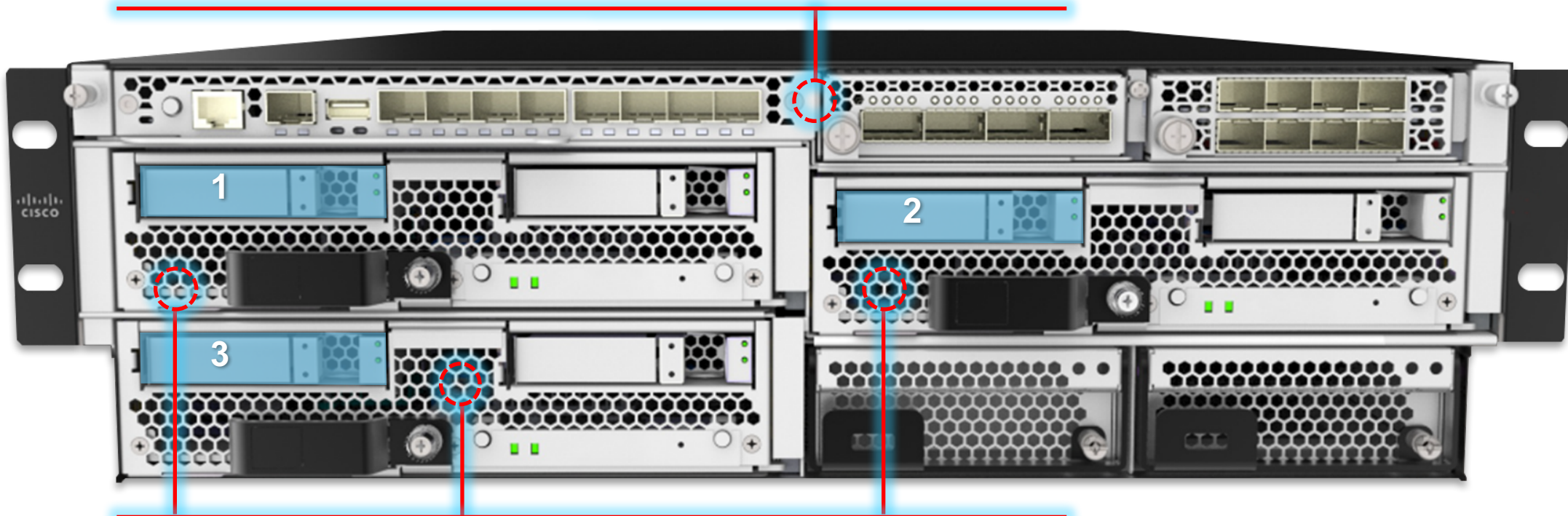
Обзор Firepower 9300

Supervisor

Внедрение и оркестрация защитных приложений

Управление сетевыми модулями (10GE/40GE) и движением трафика

Базовая кластеризация для ASA или Cisco NGFW



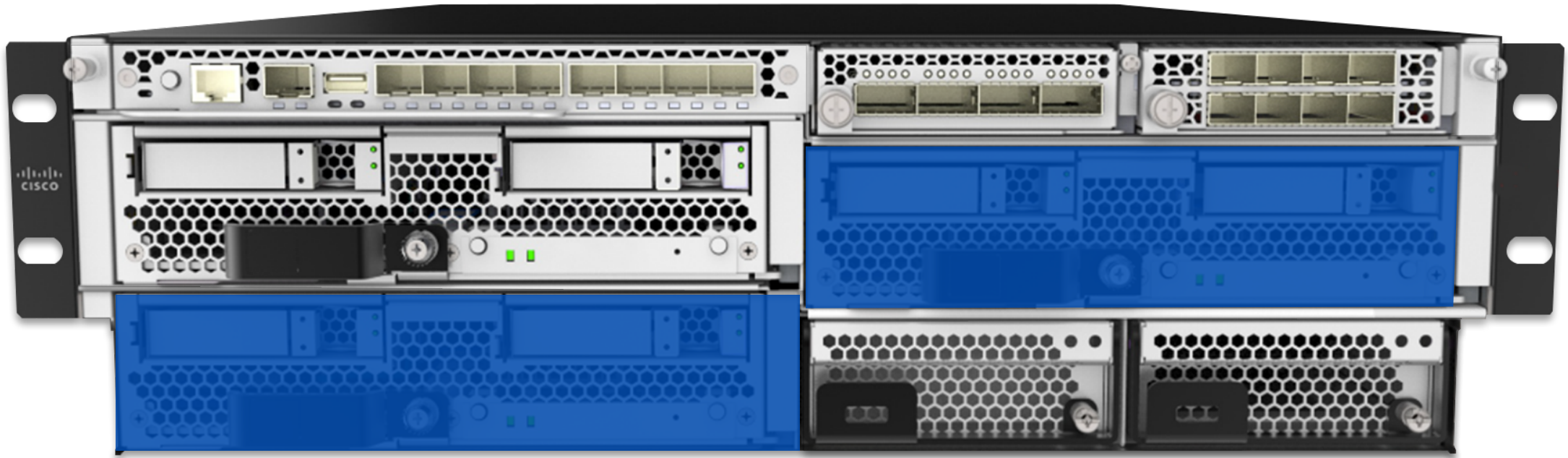
Модули безопасности

Встроенный классификатор пакетов/потоков (Smart NIC) и криптоакселератор

CPU с 24 или 36 физическими ядрами (48 или 72 с hyperthreading)

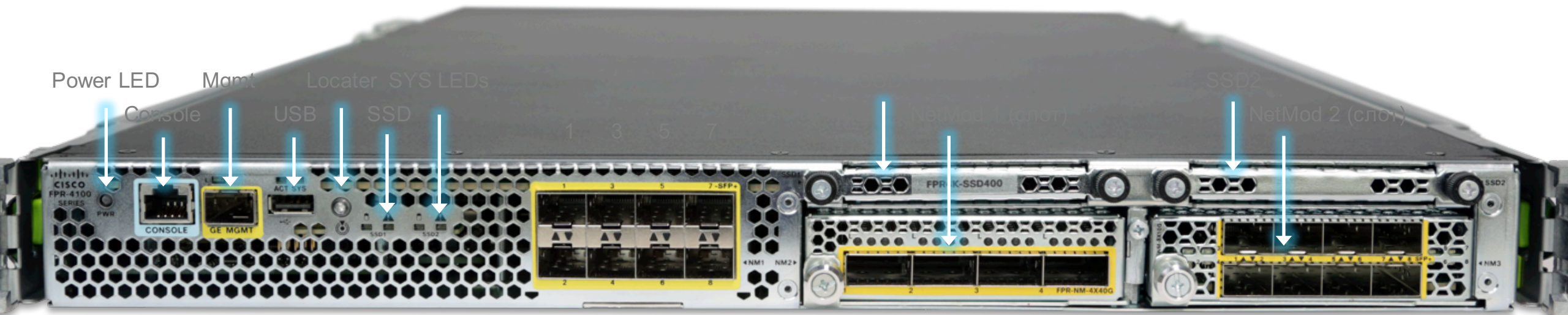
Стандартный или шасси (до 240Gbps) и на все кластер (1Tbps+)







И мы приходим к Firepower 4100 Series



2 4 6 8
Фиксированная конфигурация
8x SFP+ (10G) фиксированных портов
Security Engine

Модульная система
2x слота для сетевых модулей (NetMod)
2x слота для 2.5" SSD

Устройства Firepower 4100 Series

Разработан с использованием Security Services Platform (SSP)

Инфраструктурная платформа для сервисов безопасности

Интегрирует сервисы безопасности Cisco и сервисы ИБ третьих фирм

Архитектура разработана для быстрого добавления новых сервисов по требованиям рынка

Разработан для:

Периметра Интернет

Периметра кампуса

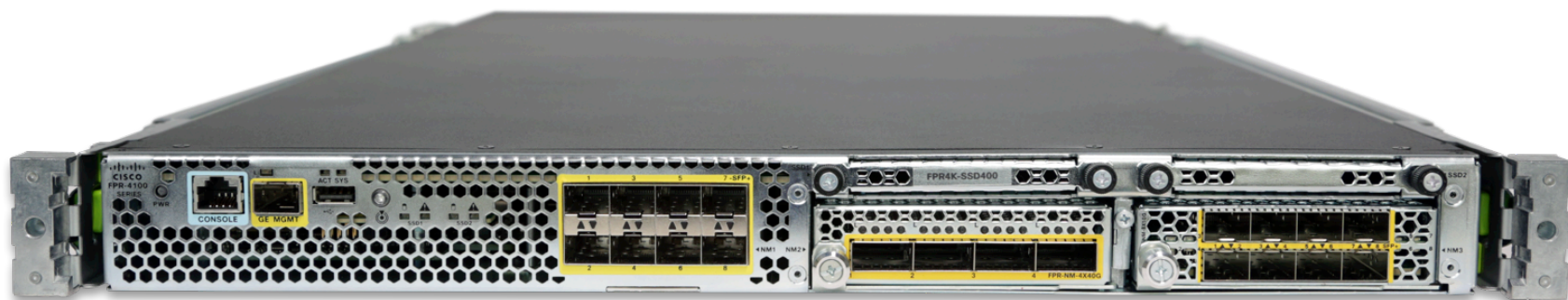
Периметра ЦОД

Аппаратная платформа
для:

Firepower NGFW

Cisco AMP

ASA



Firepower 4120/40/50 – аппаратные компоненты

Модуль Supervisor :

Консоль и порты управления
8 10G фиксированных Ethernet портов
2 x Network Modules (до 40 GE)

Модуль безопасности:

Два CPU, каждый подключен к Smart NIC и карте Crypto accelerator

Два SSD - 1 основной + 1 дополнительный (для сервиса AMP)

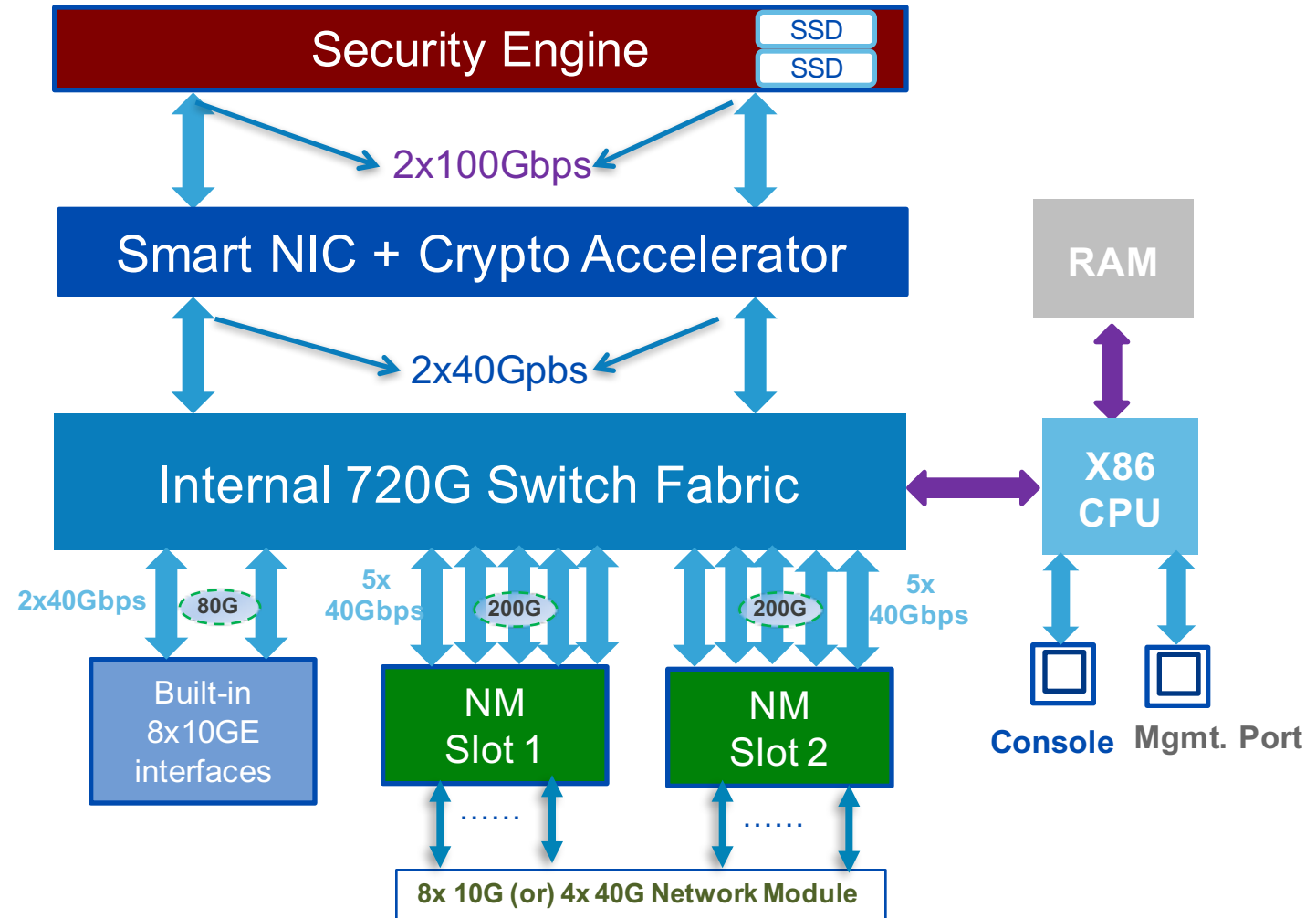
Размер SSD

200GB для 4120

400GB для 4140

Backplane

80GB Backplane



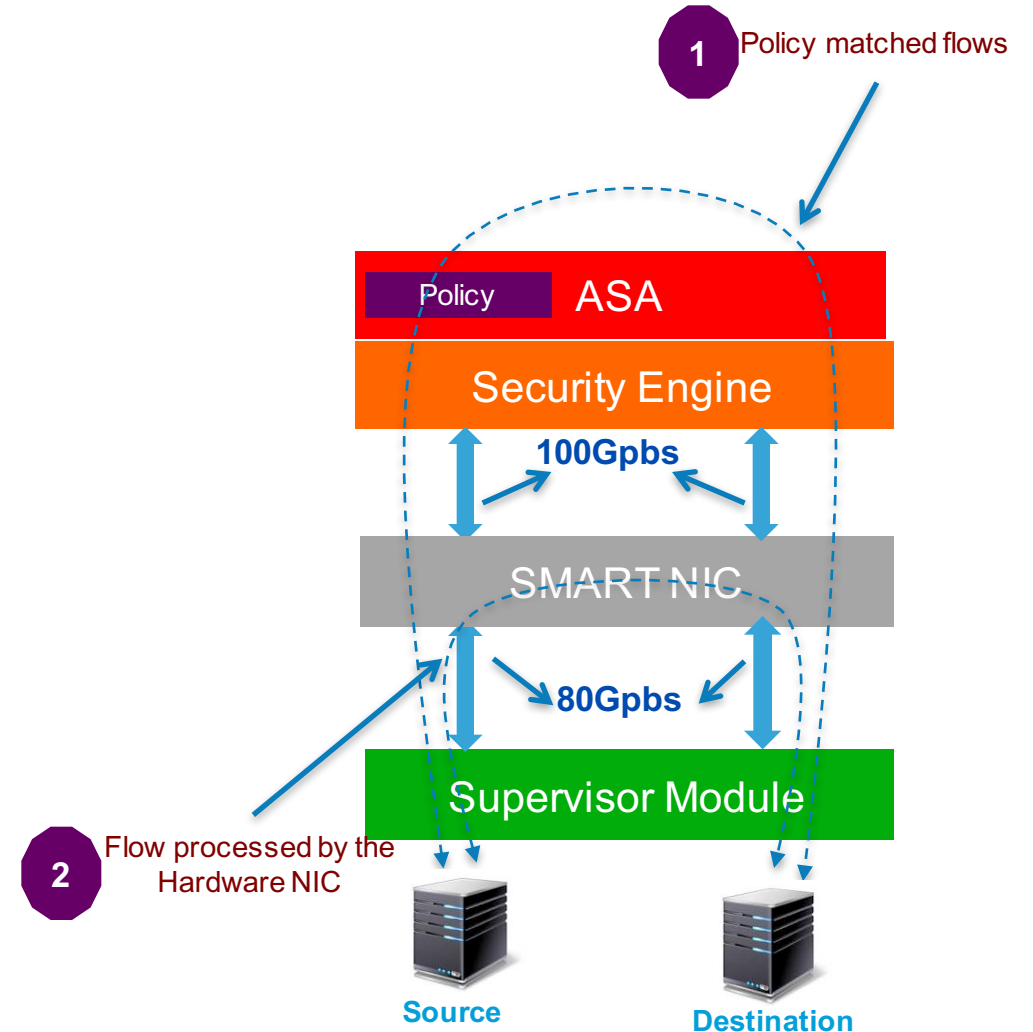
Операции разгрузки потоков

Обработка доверенных потоков на сверх высоких скоростях с помощью SMART NIC

- Аппаратная обработка без нагрузки x86
- 30-40 Гбит/с на один TCP/UDP поток , <5мкс задержка.

Использование:

- Потокое медиа
- Высокопроизводительные вычисления
- Intra/Inter DC резервное копирование или синхронизация БД
- GRE туннелирование



От Cisco ASA к Cisco Firepower

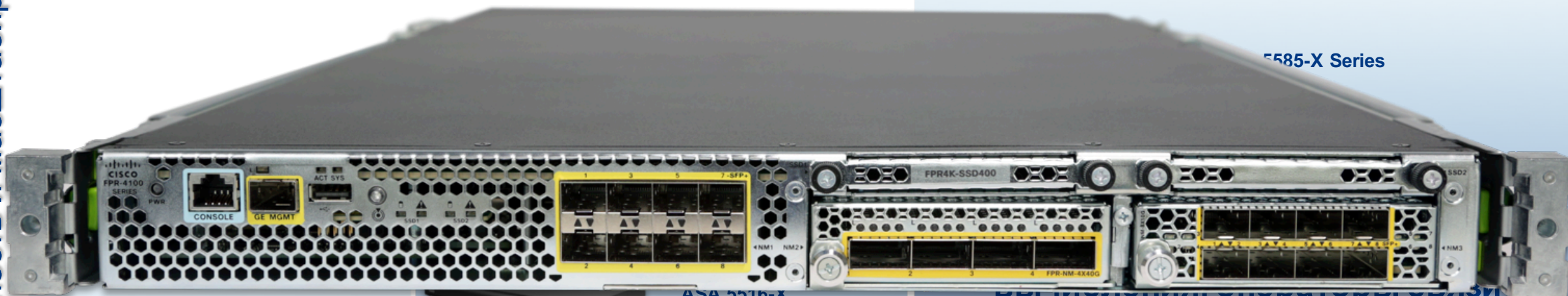
Производительность и масштабируемость



FP 9300

FP 4100 Series

5585-X Series



ASA 5516-X



ASA 5508-X



ASA 5506W
ASA 5506-X
ASA 5506H

**SMB &
филиалы**

**Предприятия &
корпорации**

FTD производительность

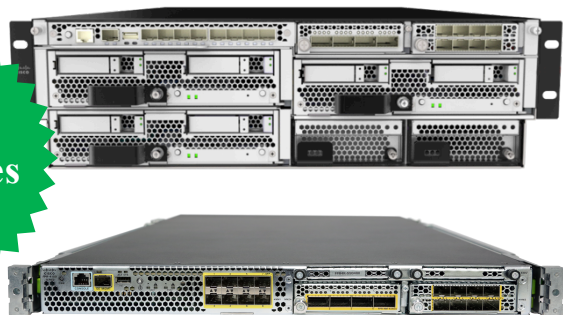
	4110	4120	4140	SM-24	SM-36	SM-36x3
Max Throughput: Application Control (AVC)	12G	20G	25G	25G	35G	100G
Max Throughput: Application Control (AVC) and IPS	10G	15G	20G	20G	30G	90G
Sizing Throughput: AVC (450B)	4G	8G	10G	9G	12.5G	30G
Sizing Throughput: AVC+IPS (450B)	3G	5G	6G	6G	8G	20G
Maximum concurrent sessions w/AVC	4.5M	11M	14M	28M	29M	57M

ASA производительность

	4110	4120	4140	SM-24	SM-36	SM-36x3
Stateful inspection firewall throughput (maximum)	20G	40G	60G	75G	80G	225G
Stateful inspection firewall throughput (multiprotocol)	10G	20G	30G	50G	60G	100G
Concurrent firewall connections	10M	15M	25M	55M	60M	70M
New connections per second	150K	250K	350K	0.6M	0.9M	2M
Security contexts	250	250	250	250	250	250
Virtual Interfaces	1024	1024	1024	1024	1024	1024
IPSec 3DES/AES VPN Throughput	8G	10G	14G	15G	18G	18G

Платформы Cisco NGFW

New Appliances



Firepower 4100 Series
and Firepower 9300



Firepower Services
on ASA 5500-X



Firepower Services
on ASA 5585-X

Все управляются с помощью FirePower Management Center

*5585-X management avail 2H '16 (pre-commit date)

5 отличительных особенностей FirePOWER/AMP

1. Знаем КТО и ЧТО в сети
- Интеграция в Cisco ISE



2. Продвинутое система защиты от вирусов



3. Карта сети
- Видим приложения, уязвимости....



4. Автонастройка
- Проще внедрять и поддерживать



5. Open AppID
- Добавьте свое кастомное приложение



FirePOWER

МСЭ нового поколения, смотрящий шире и глубже

Непревзойденная прозрачность

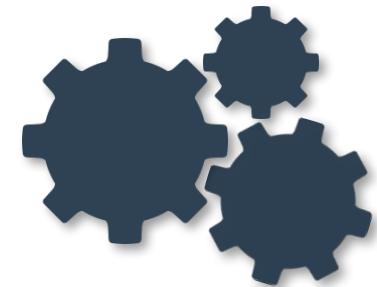
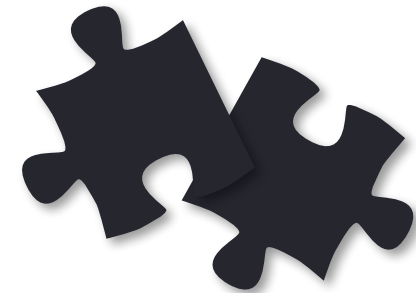
- ▶ Полная осведомленность о сетевом контексте для устранения уязвимостей

Комплексная защита от угроз

- ▶ Лучшая в своем классе многоуровневая защита в одном устройстве

Автоматизация

- ▶ Простота управления, динамическое реагирование и восстановление





Вопросы?

Thank you.

