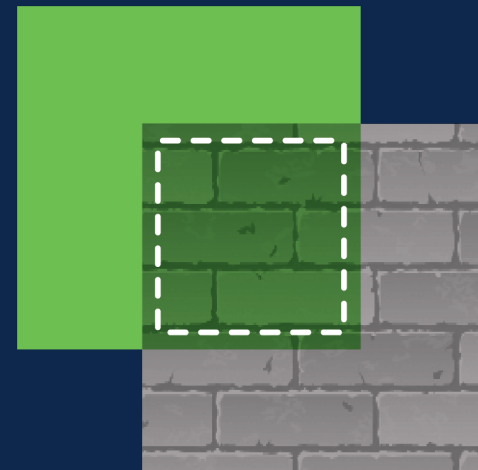


Cisco Secure Firewall

Новинки, информация и практика

Павел Родионов
Архитектор по кибербезопасности
GREM, CISSP, CCIE 11155



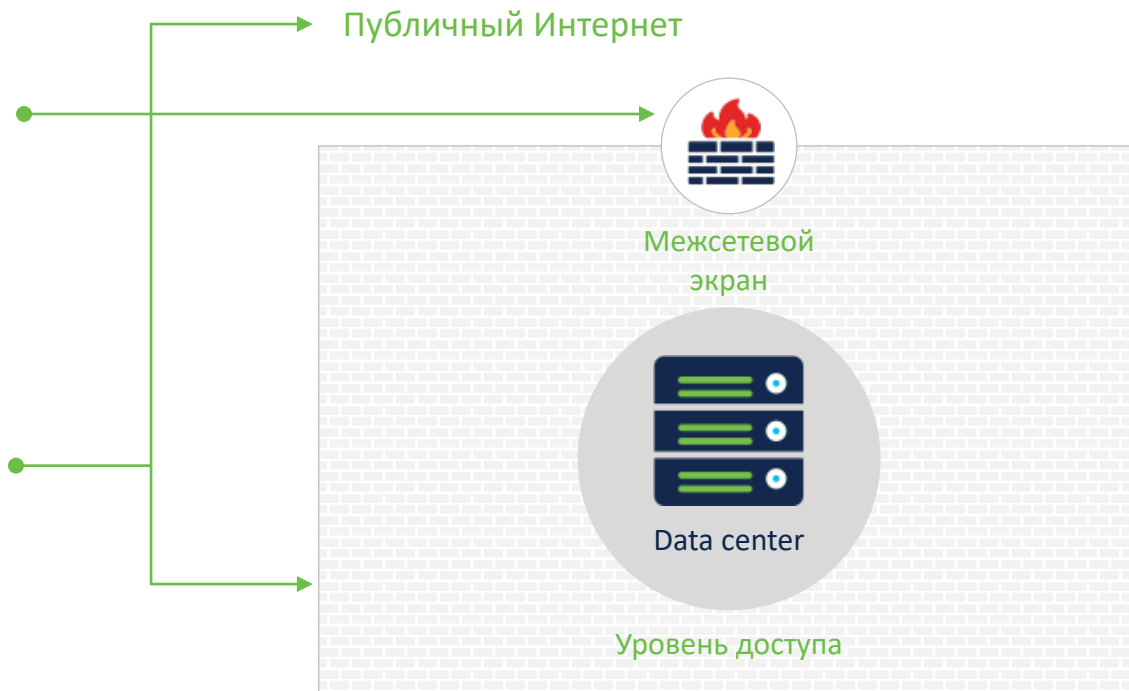
Программа

- 1 Обзор
- 2 Варианты платформ
- 3 Secure Firewall Threat Defense (FTD)
- 4 Единство политики и осведомленности
- 5 Управление с Firewall Management Center (FMC)
- 6 Сценарии использования

Традиционная сетевая безопасность

Одна точка контроля
всего трафика

Внутренний трафик был
доверенным, а внешний
таковым не являлся



Новая реальность

Модель всё включено показала себя не эффективной в текущих реалиях

Одна точка контроля не эффективна

Каждому окружению требуется свой микро-периметр

Изменение форм-фактора

Одна точка управления заменяется серией межсетевых экранов, как физических так и виртуальных

Разрастание политик

Соотношение политик между микро-периметрами – непростая задача



Сложность управления

NetSec и IT используют десятки точечных продуктов каждый со своей консолью управления

Эволюция ландшафта угроз

Продукты безопасности должны получать постоянную информацию об угрозах чтобы быть впереди злоумышленника

Проверенные сценарии использования МСЭ

В чем может помочь Cisco?



Граница Интернет



ЦОД



Филиалы



Облако/
Виртуализация



Продвинутый
IPS



Удаленный
VPN доступ

Почему Cisco Secure Firewall?



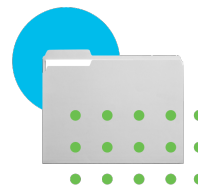
Средства безопасности мирового уровня

Защищайте сеть полным портфолио решений по межсетевому экранированию с поддержкой лучшего центра кибербезопасности



Целостная политика и осведомленность

Понятная политика безопасности и управление устройствами во всей сети с реализацией ключевых задач безопасности.



Интегрированное портфолио безопасности

Развивайте безопасность за пределы межсетевого экрана с защитой от вредоносных, маршрутизации по идентификации, многофакторной аутентификации и многим другим

Всестороннее портфолио Cisco по кибербезопасности



Средства безопасности мирового уровня



Secure Firewall Threat Defense



Secure Firewall ASA

TalOS Talos



Целостная политика и осведомленность



Secure Firewall Management Center



Secure Firewall Device Manager



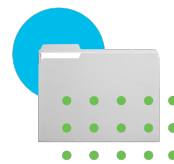
Cisco Defense Orchestrator



SecureX threat response



Secure Network Analytics



Интегрированное портфолио безопасности



Secure Access by Duo



Secure Endpoint



TrustSec



Cisco Identity Services Engine

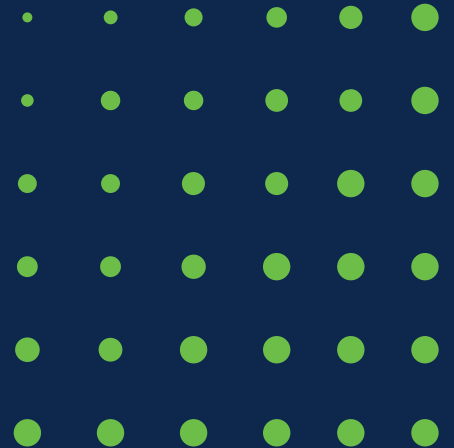


Rapid Threat Containment



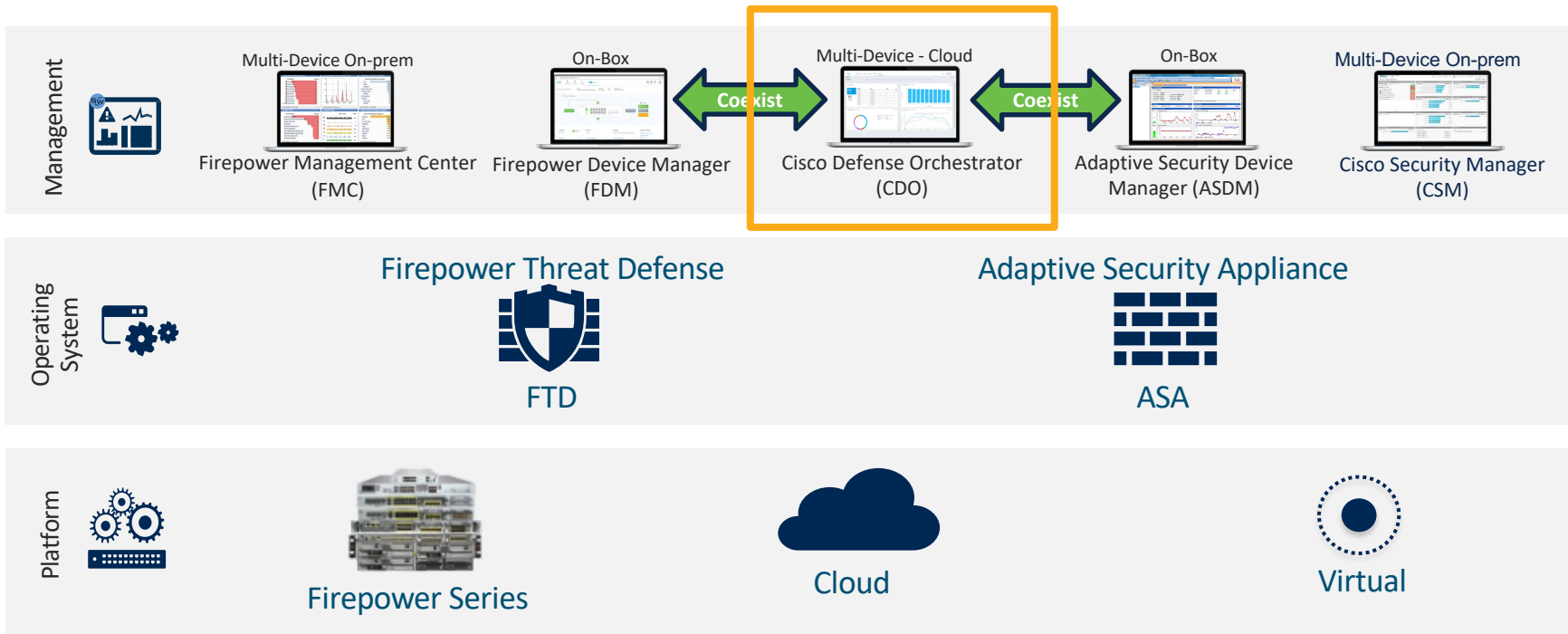
Application Centric Infrastructure

Платформы Secure Firewall



Cisco Next-Generation Firewall. Обзор портфолио

Платформы, операционные системы и опции управления



Выбор ПО и платформы



Образ ASA предоставляет возможности

Надежный, простой Stateful Firewall и VPN концентратор



Правила

- Stateful контроли
- 5-ти компонентные правила
- Два основных действия: разрешить и запретить



Возможности

- VPN: Remote Access, Clientless, EzVPN, IKEv1/L2TP/3rd party Remote Access, Site-Site Route Based и Policy Based VPN, DTLS 1.2
- Маршрутизация & Quality of Service
- Carrier Grade NAT
- DAP *
- SSO with SAML



Автоматизация

- Использование API's для интеграции с SIEM
- API's для создания правил на базе 5 компонентов



Безопасность

- Фильтрация пакетов и классическая безопасность от Layer 2 до Layer 4
- Нет расширенных контролей, как IPS, AMP, URL фильтрация, приложения (только ALG) и т.д..

Образ Firepower Threat Defense (FTD) предоставляет

Защита от угроз, контекст и видимость



Правила

- Правила основываются на комбинации 5 компонентов плюс Identity/Приложение/URL
- Действия правила trust, monitor, reset, allow и block
- Правила для расшифровки TLS и действий



Возможности

- Традиционные контроли как VPN, NAT, Routing и т.д.
- NGIPS с авто настройкой
- Anti-Malware защита с песочницей
- Ограничение полосы с параметрами Layer 7
- Приоритезация событий и авто реагирование.



Автоматизация

- Использование API's для автоматизации и оркестрации функций NGFW
- Интеграция с AMP EP, ISE, CTR, Tetration, SIEM и т.д.
- Использование API's для потребления информации и threat feeds
- Платформа для применения контролей

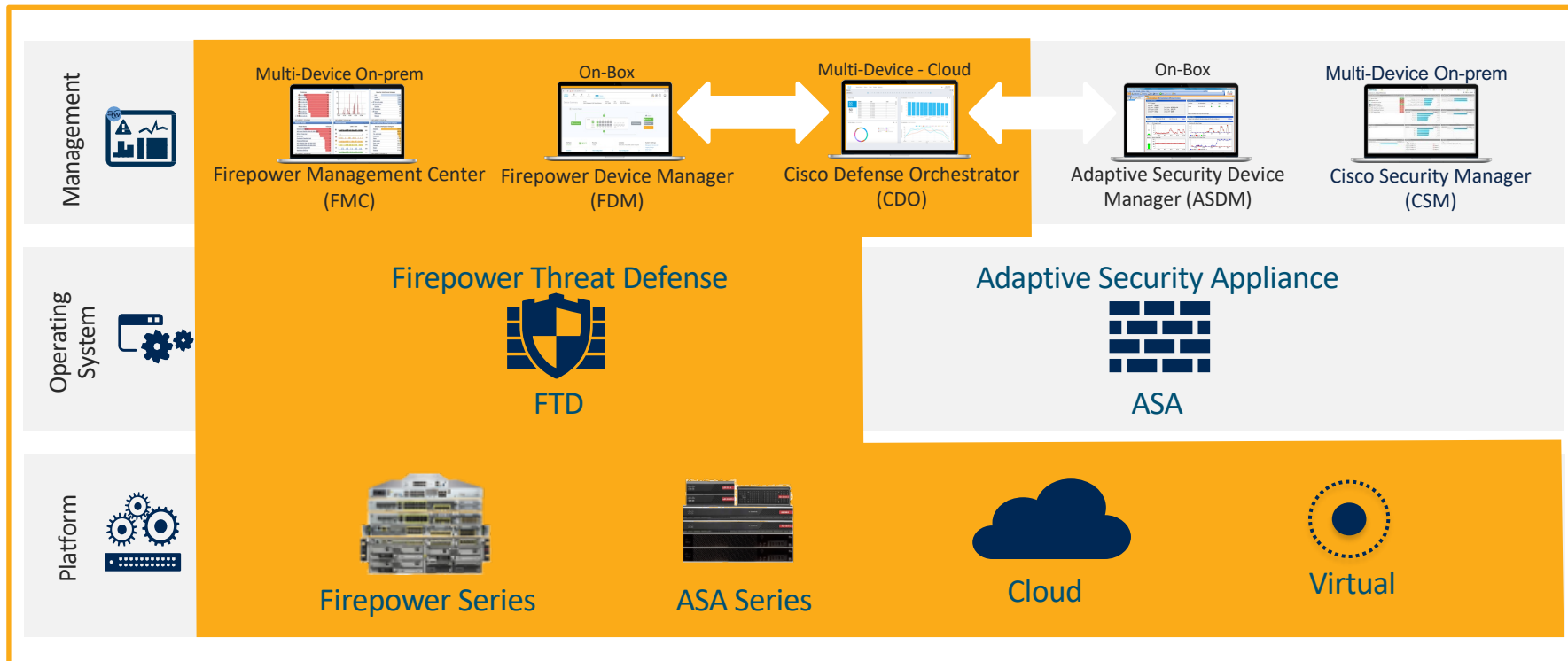


Безопасность

- Защита от Layer 2 до Layer 7
- Блокировка сетевых угроз
- Deep packet inspection
- Сканирование и блокировка вредоносных файлов.
- Интеграция с песочницей
- Dynamic Threat Intelligence

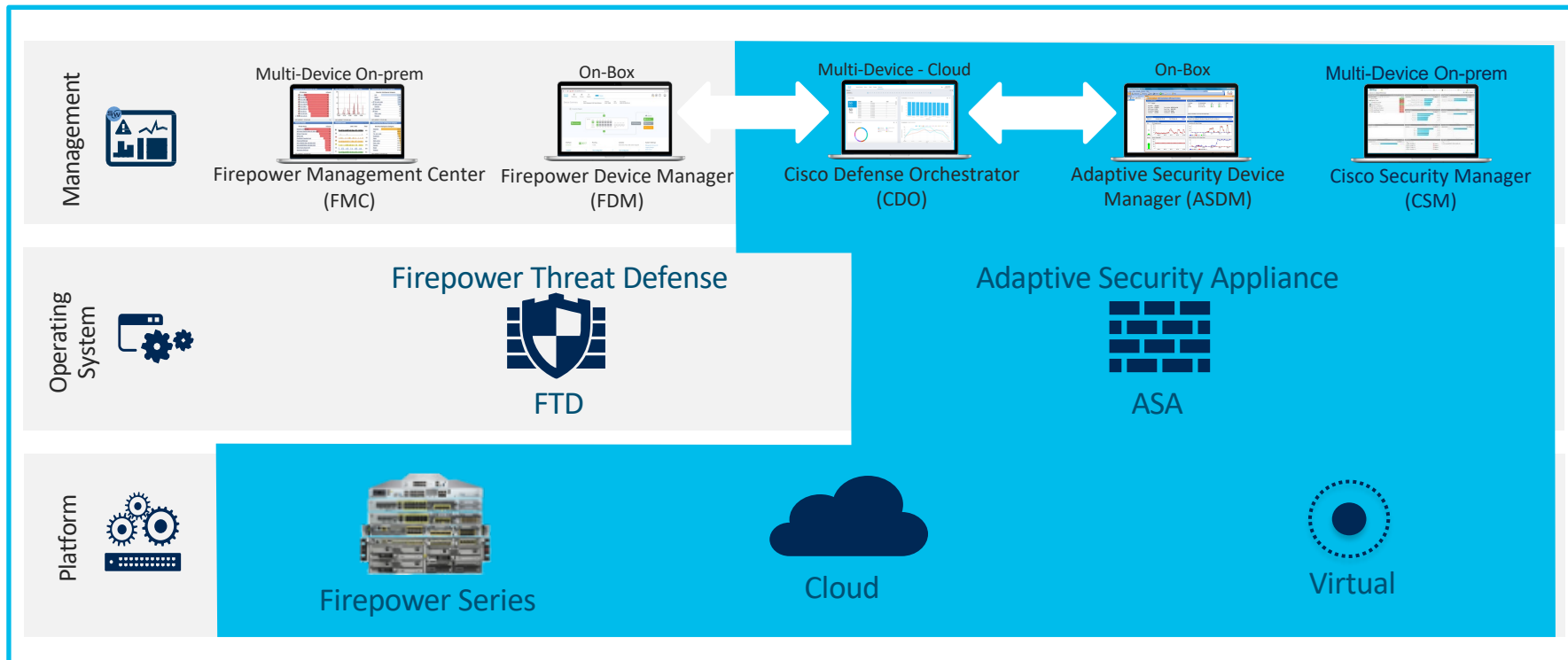
FTD : Опции платформы и управления

Platforms, Operating Systems and Management options



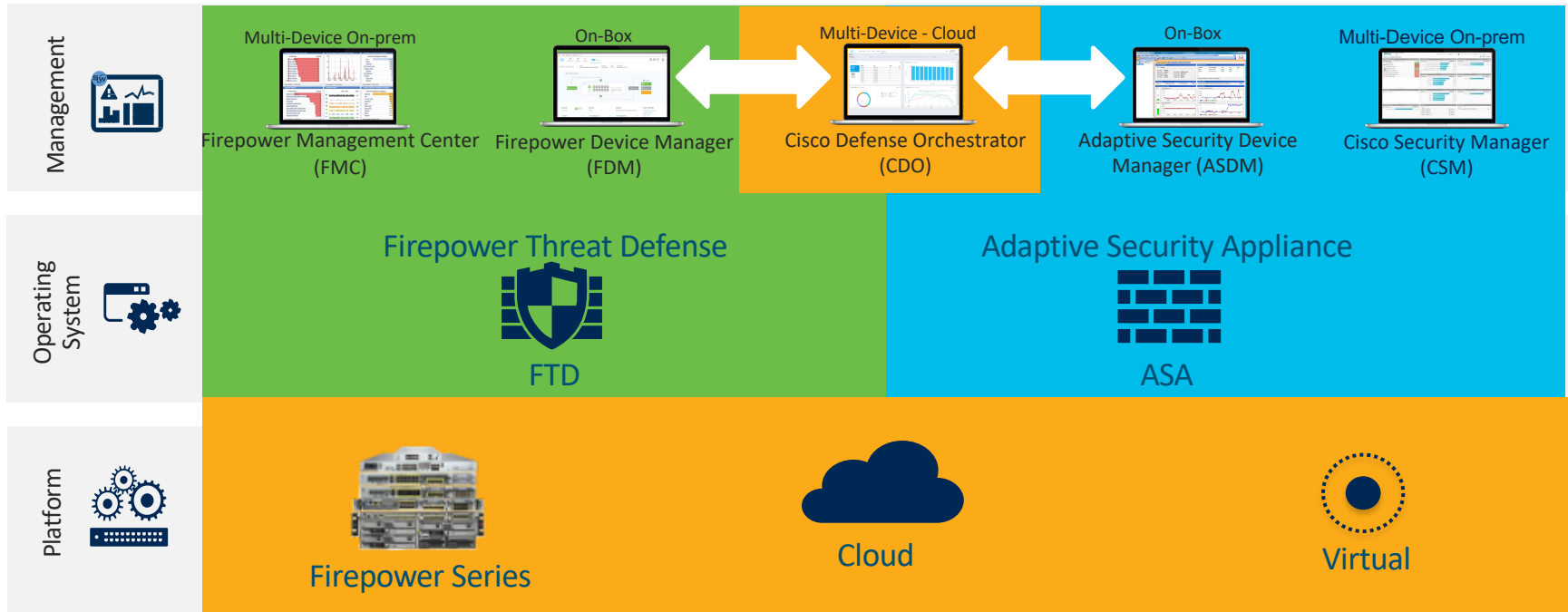
ASA: Опции платформы и управления

Platforms, Operating Systems and Management options



Собираем все вместе

Platforms, Operating Systems and Management options



Устройства и облачные платформы Firepower

Private Cloud*

Public Cloud*

FPR 4112/4115/25/45

FPR 4110/20/40/50

FPR 9300 Series

- SM-24 SM-40
- SM-36 SM-48
- SM-44 SM-56

FPR 1010

FPR 1120/40/50

FPR 2110/20/30/40



890 Mbps AVC or AVC+IPS 1.5-5 Gbps AVC or AVC+IPS 3-10 Gbps AVC or AVC IPS Stand-alone device: 16-53 Gbps AVC, 15-52 Gbps AVC+IPS 6 One Module: 55-70 Gbps AVC, 53-68 Gbps AVC+IPS

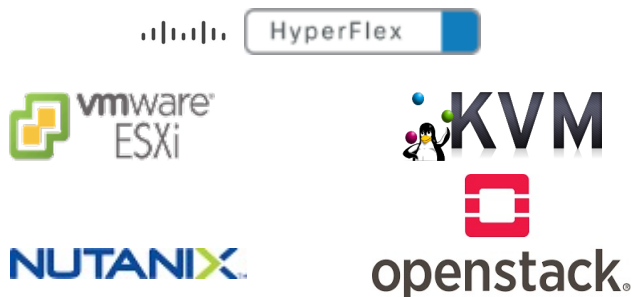
**Cloud performance depends on the allocation of underlying resources and average packet size*

SOHO/SMALL BUSINESS Branch Office Mid-Size Enterprise Large Enterprise Data Center Service Provider

Что нового? – Виртуальные платформы МСЭ

Частное облако

- FMCv и FTDv
 - Поддержка ESXi 7.0
 - Поддержка: Cisco Hyperflex, Nutanix Enterprise Cloud, OpenStack
- ASA Docker контейнеры (Cloud Native Firewall)



Публичное облако

- Azure Application Insights для метрик FTD
- FMCv/FTDv ASA в Google Cloud Platform и Oracle Cloud Infrastructure



Secure Firewall Cloud Native



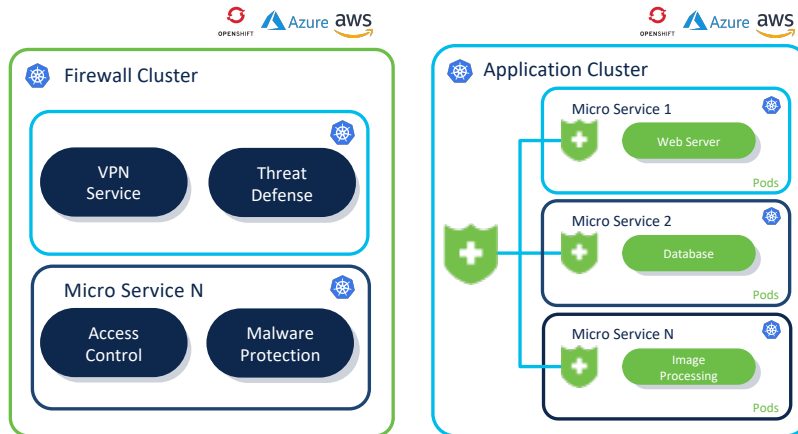
Простые в развертывании **сервисы межсетевого экрана** большого масштабирования и надежность облачной среды



Запускайте **средства безопасности** непосредственно с контейнерами приложений



Высоко **масштабируемый и гибкий межсетевой экран** для пограничного сценария – RA VPN, DC Backhaul, Mobility carriers, MSP/MSSP



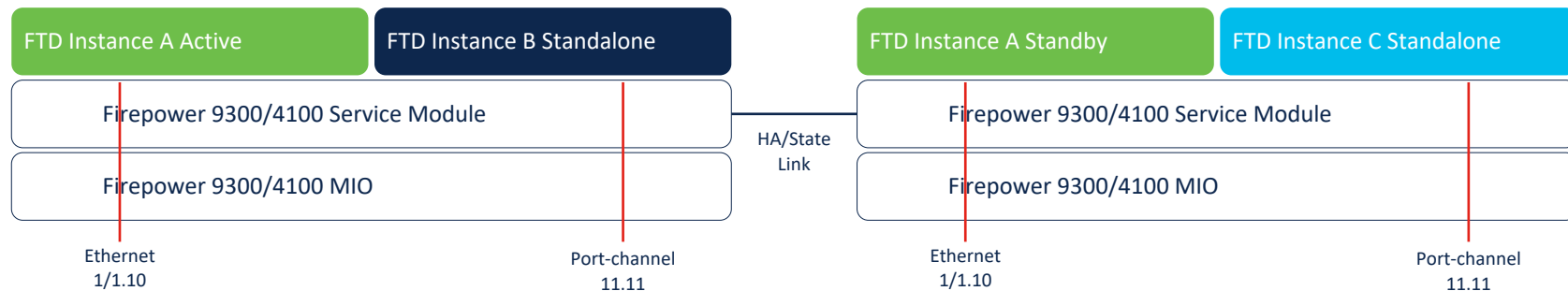
Удобный для разработчиков межсетевой экран для Kubernetes окружений

* FCS in May 2021 in AWS EKS, followed by Azure and Openshift this Fall

Multi-Instance. Уникальный режим виртуализации

- Развертывайте множество FTD логических устройств на одном модуле или устройстве
 - Контейнерная архитектура
 - Отказ одного instance не влияет на другие
- Позволяет осуществлять независимое управление, независимое обновление instance
- Поддержка HA между идентичными instance на разных физических устройствах
- Пример: 54 instance на шасси FPR9300 с 3 x SM-56 модулями
- Улучшенная аппаратная крипто-акселерация

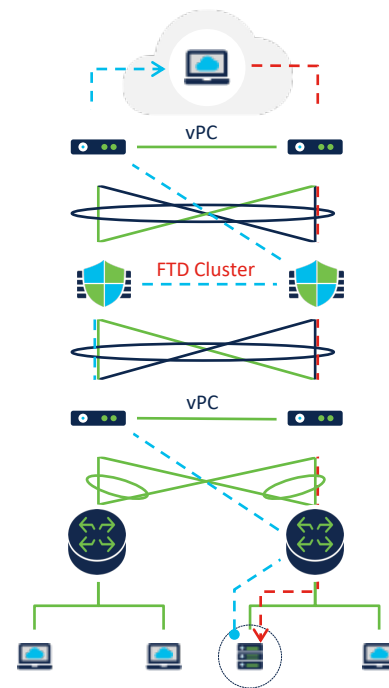
NEW



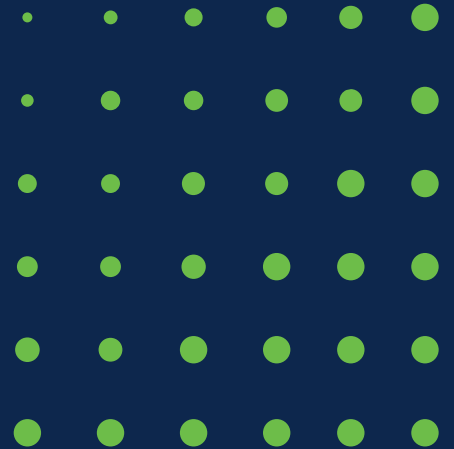
Кластеризация

Получайте лучший возврат инвестиций сохраняя отказоустойчивость

- Комбинируйте множество устройств для создания единого масштабируемого логического устройства
- Масштабирование по мере роста
 - Масштабируйте пропускную способность, новые и имеющиеся соединения
 - Может растягиваться на несколько ЦОД
- N+1 отказоустойчивость
- Прозрачно обрабатывает асимметричный трафик



Secure Firewall Threat Defense



Что такое Secure Firewall Threat Defense (FTD)?

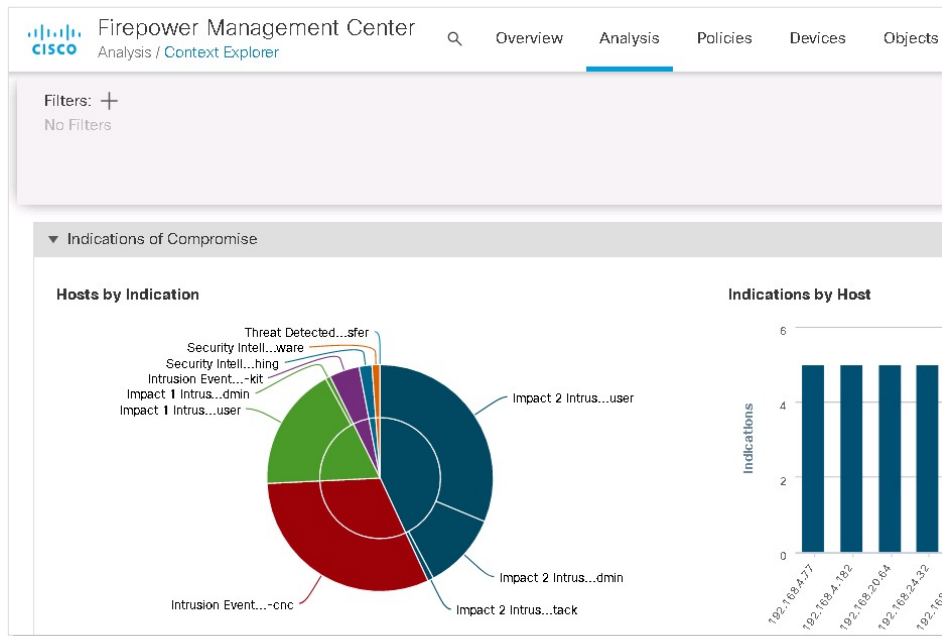
Позволяет высочайшей эффективностью блокировать вредоносные потоки и защитить сеть от угроз

- **Ключевые преимущества**

- Разграничение управления Tenant
- Рост по необходимости
- Анализ воздействия
- Приоритетное управление

- **Функции**

- Межсетевой экран
- Защита от угроз
- Интегрированная дешифровка TLS
- VPN
- Cisco Threat Intelligence Director
- Защита от вредоносного кода в ретроспективе



Firewall Threat Defense 7.0

Важные изменения в extra long-term релизе – переход на 7.0 2021

Scalable Eventing and Logging

Просмотр событий в реальном времени, масштабируемое хранение событий и логирование на площадке с использованием SAL

Динамические объекты для быстрых изменений

Политика на основе атрибутов добавляет динамические сетевые объекты в политику AC

Проще в использовании

Унифицированные метрики состояния (через SNMP), Дэшборд состояния для FMC, Управление изменениями (откат, просмотр изменений, улучшенный аудит, поиск и фильтрация)

Улучшение обнаружения угроз

Улучшено обнаружение угроз с важным архитектурным изменением: появление Snort 3 с FMC

Публичные облака и виртуализация

Поддержка динамических объектов для нативных облачных политик и создание быстрых Instance (с Secure Threat Services)

Преимущества бизнеса

Отладка и отслеживание текущих, исторических событий в едином UI

Изменение динамических объектов в политиках быстро без необходимости deploy

Сильно улучшенный пользовательский опыт, снижение операционной сложности и расходов

Заказчик получает лучшее обнаружение с меньшей затратой ресурсов

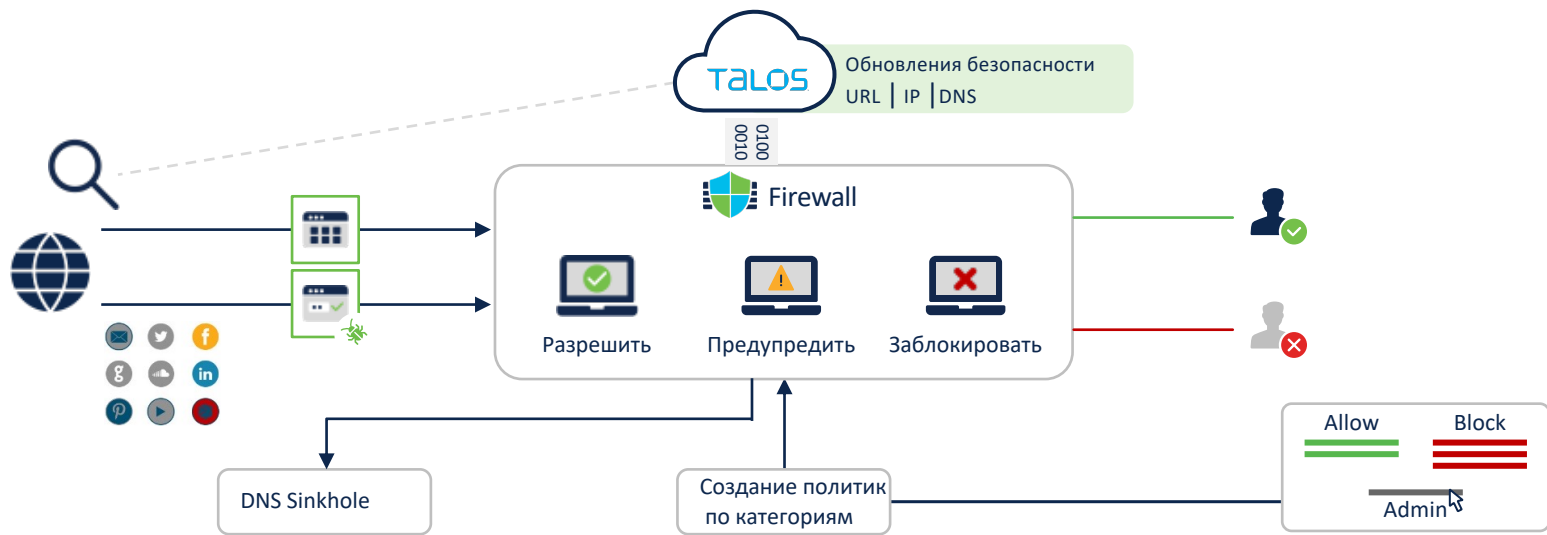
Поддержка гибридных облаков для любого развертывания заказчика

Много других улучшений в ...

- Remote access и site-to-site VPN
- Интеграция Secure-X
- FMC API для оркестрации и миграции
- APIC FMC App Multi domain
- Работа PAT в кластере
- Поддержка множества доменов для идентификации пользователя

Политика МСЭ усиленная Talos и OpenAppID

Контролируйте трафик на основании IP, URL, FQDN, или приложения



Security Intelligence:
Заблокировать свежие вредоносы
IPs, URLs и FQDN

AVC с OpenAppID:
Идентификация и контроль
более 4,000+ приложений

AVC с OpenAppID:
Легко создавайте детекторы
своих приложений

URL Категории:
Классификация более **280M+** URL
используя **80+** категорий






Secure IPS

Снижайте шум/объем событий и выставляйте приоритет задач управления

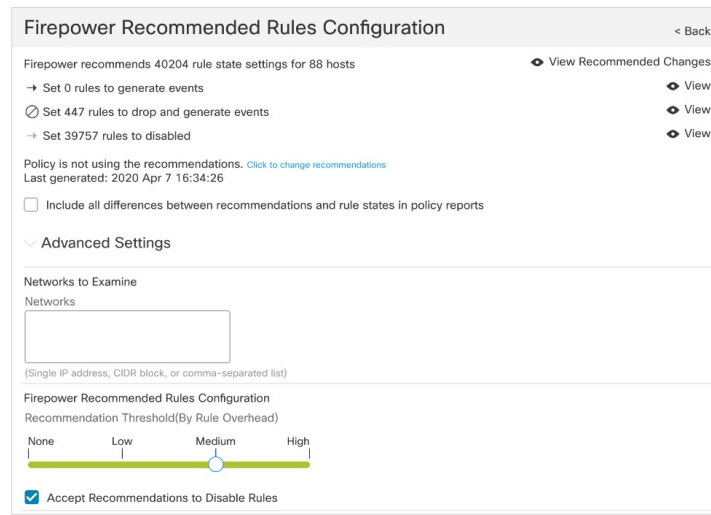
Обеспечивается Snort 3 – Лучшим IPS с открытым кодом

Межсетевой экран добавляет контекст в функции IPS

Воздействие событий IPS может быть вычислено

Impact flag	Administrator action	Why
1 	Действуйте немедленно, уязвимо	Событие соответствует имеющейся уязвимости хоста
2 	Расследуйте, Потенциально уязвимо	Атакующий порт открыт или используется нет уязвимости
3 	К сведению, не доступно	Порт или протокол не используются
4 	К сведению, цель не известна	Сеть наблюдается, но хост не известен
0 	К сведению, неизвестная сеть	Сеть не под наблюдением

Рекомендации МСЭ могут настраивать IPS.



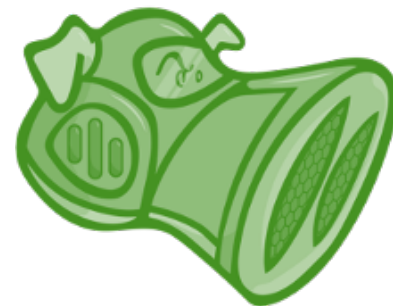
The screenshot shows the 'Firepower Recommended Rules Configuration' interface. It includes a title bar with a '< Back' button. The main content area displays: 'Firepower recommends 40204 rule state settings for 88 hosts' with a 'View Recommended Changes' link. Below this are three action items: 'Set 0 rules to generate events', 'Set 447 rules to drop and generate events', and 'Set 39757 rules to disabled', each with a 'View' link. A note states 'Policy is not using the recommendations' with a 'Click to change recommendations' link and a timestamp 'Last generated: 2020 Apr 7 16:34:26'. There is an unchecked checkbox for 'Include all differences between recommendations and rule states in policy reports'. An 'Advanced Settings' section is partially visible, showing 'Networks to Examine' with an empty input field and a note '(Single IP address, CIDR block, or comma-separated list)'. At the bottom, there is a 'Firepower Recommended Rules Configuration' section with a 'Recommendation Threshold(By Rule Overhead)' slider ranging from 'None' to 'High', currently set to 'Medium'. A checked checkbox 'Accept Recommendations to Disable Rules' is also present.

Snort 2 vs. Snort 3

	Snort 2	Snort 3
Многоядерная архитектура		✓
Может запускать множество процессов Snort	✓	✓
Независимая от порта инспекция протоколов		✓
IPS Акселерация / поддержка Hyperscan		✓
Модульность – Проще обновлять для TALOS		✓
Масштабируемое выделение памяти		✓
Правила TALOS нового поколения – прим., Regex/Rule Опции/Sticky Buffers		✓
Новые и улучшенные and HTTP инспекторы – пример., поддержка HTTP/2		✓
Более легкое обновление контента от TALOS		✓

Обзор релиза 7.0 Snort 3

- Устройства обновленные на релиз 7.0 продолжают использовать Snort 2, вновь развернутые используют Snort 3
- Можно менять версию используемого Snort в закладке FMC Device Management
- Простая миграция политик и из Snort 2 в Snort 3
- Синхронизация политики обнаружения вторжений
- Группы правил IPS включают собственные группы
 - Можно менять уровень Severity для групп правил
- Suppression/Threshold функция теперь доступна в объектах правил
- Новый синтаксис правил в Snort 3



Корреляция Профилей Хоста и IPS

Проводите анализ воздействия и включайте рекомендованные правила

Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2020-04-07 13:51:41	2020-04-07 13:51:41
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2020-04-07 13:51:40	2020-04-07 13:51:40
Impact 1 Attack	Impact 1 Intrusion Event - attempted-admin	The host was attacked and is likely vulnerable	2020-04-07 13:51:40	2020-04-07 13:51:40



Impact flag	Administrator action	Why
1	Act immediately, Vulnerable	Event Corresponds to vulnerability mapped to host
2	Investigate, Potentially Vulnerable	Relevant port open or protocol in use but no vuln mapped
3	Good to know, Currently Not available	Relevant port not open or protocol not in use
4	Good to know, Unknown Target	Monitored network but unknown host
0	Good to know, Unknown Network	Unmonitored network

Firepower Recommended Rules Configuration

Firepower recommends 40204 rule state settings for 88 hosts

- Set 0 rules to generate events
- Set 447 rules to drop and generate events
- Set 39787 rules to disabled

Policy is not using the recommendations. [click to change recommendations](#)

Last generated: 2020 Apr 7 18:34:26

Include all differences between recommendations and rule states in policy reports

Advanced Settings

Networks to Examine

Networks

(Single IP address, CIDR block, or comma-separated list)

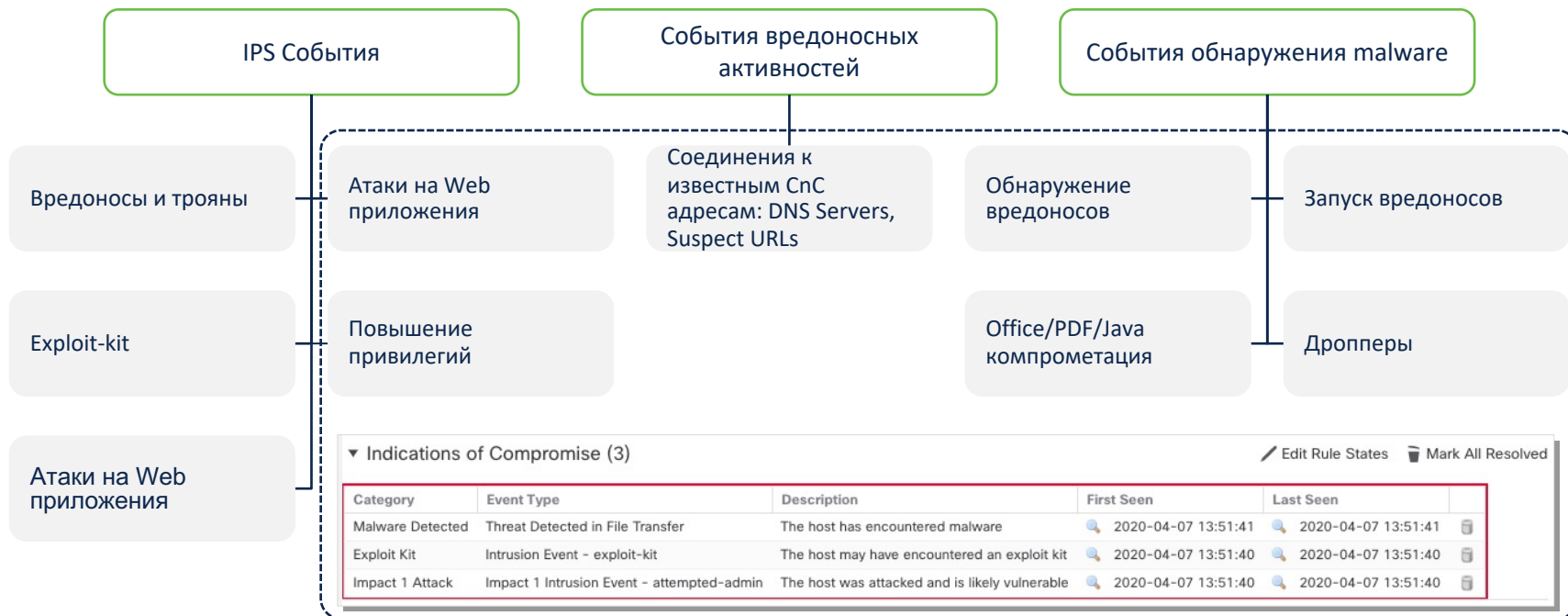
Firepower Recommended Rules Configuration

Recommendation Threshold(By Rule Overhead)

None Low Medium High

Accept Recommendations to Disable Rules

События индикаторов компрометации (IoC)

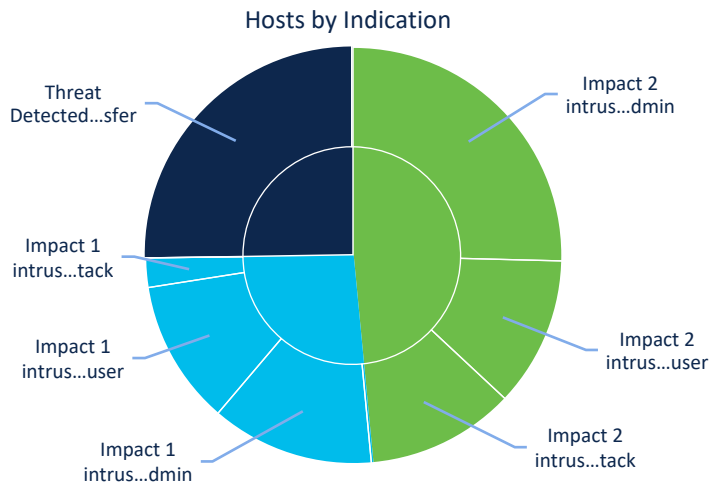


IoC содействуют исправлению состояния

Ускоряют понимание и исправление для снижения степени воздействия

- Идентифицирует компрометированный и потенциально компрометированные системы
- Применение автоматизированных действий с Cisco Rapid Threat Containment

Indications of Compromise



Host Profile

IP Addresses 10.1.112.42

NetBIOS Name

Device (Hops) FTD (2)

MAC Addresses (TTL) 00:01:24:56:9B:CF (Acer Incorporated) (128)
00:04:00:81:81:D0 (LEXMARK INTERNATIONAL, INC.) (254)
00:04:F2:E7:3E:52 (Polycom) (64)
...(show all)

Host Type Host

Last Seen 2020-04-07 16:15:47

Current User kennedy.larson (dcloud.cisco.com\klarson, LDAP)

View [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)

Scan Host Generate White List Profile

▼ Indications of Compromise (3) [Edit Rule States](#) [Mark All Resolved](#)

Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2020-04-07 13:51:41	2020-04-07 13:51:41
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2020-04-07 13:51:40	2020-04-07 13:51:40
Impact 1 Attack	Impact 1 Intrusion Event - attempted-admin	The host was attacked and is likely vulnerable	2020-04-07 13:51:40	2020-04-07 13:51:40

▼ Operating System [Edit Operating System](#)

Vendor	Product	Version	Source
Microsoft	Windows	Vista, 7, Server 2008	Firepower

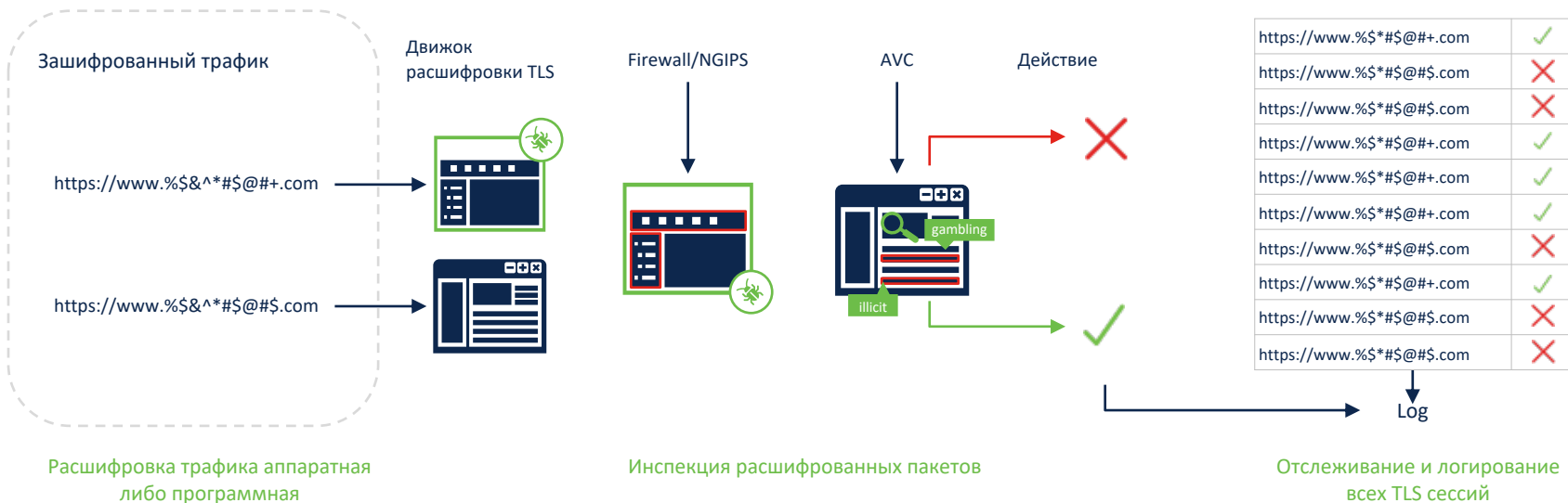
Applications (14)

Application Protocol	Client	Version	Web Application
BitTorrent	BitTorrent		
HTTP	Chrome	44.0.2403.107	CNET Download
HTTP	Internet Explorer	9.0	Casale

Интегрированная расшифровка TLS

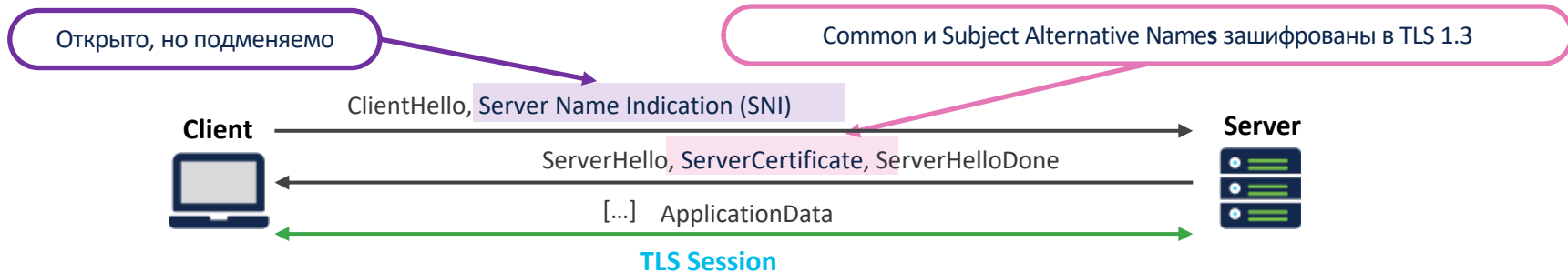
Находим зашифрованные угрозы снижая влияние на производительность

- Аппаратная акселерация TLS предоставляет высокую производительность инспекции TLS-трафика
- Централизованное применение политик для сертификатов TLS
 - Примеры: Блокирование само-подписанных сессий, отдельных версий TLS, отдельных крипто-наборов



Быстрое определение приложений и URL с TLS 1.3

AVC, URL, и действия по расшифровке заголовков TLS до версии 1.3



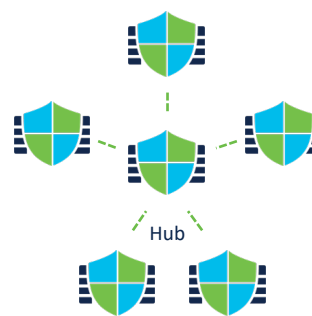
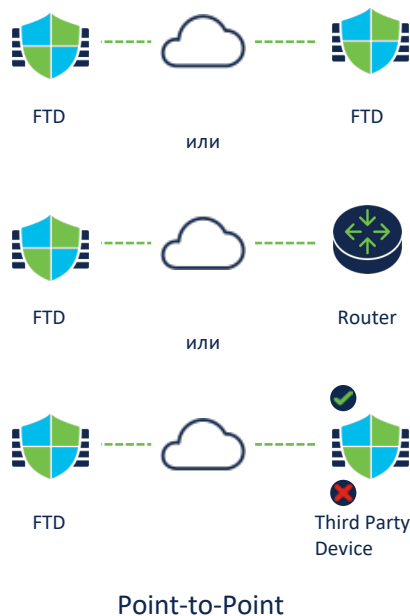
TLS Server Identity Discovery без расшифровки начиная с **FTD 6.7**



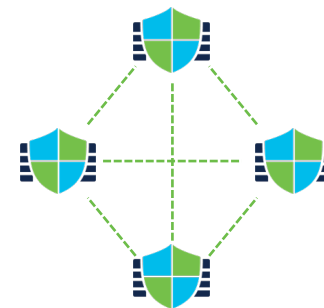
Site-to-Site VPN

Легко и безопасно соединять удаленные сайты

- IKEv1/IKEv2 policy-based VPN
- Простые конфигурации VPN с многими участниками в топологиях:
 - Point-to-point
 - Hub and Spoke
 - Full Mesh
- Гибкие опции аутентификации – общий ключ (автоматически) и сертификаты



Hub and Spoke

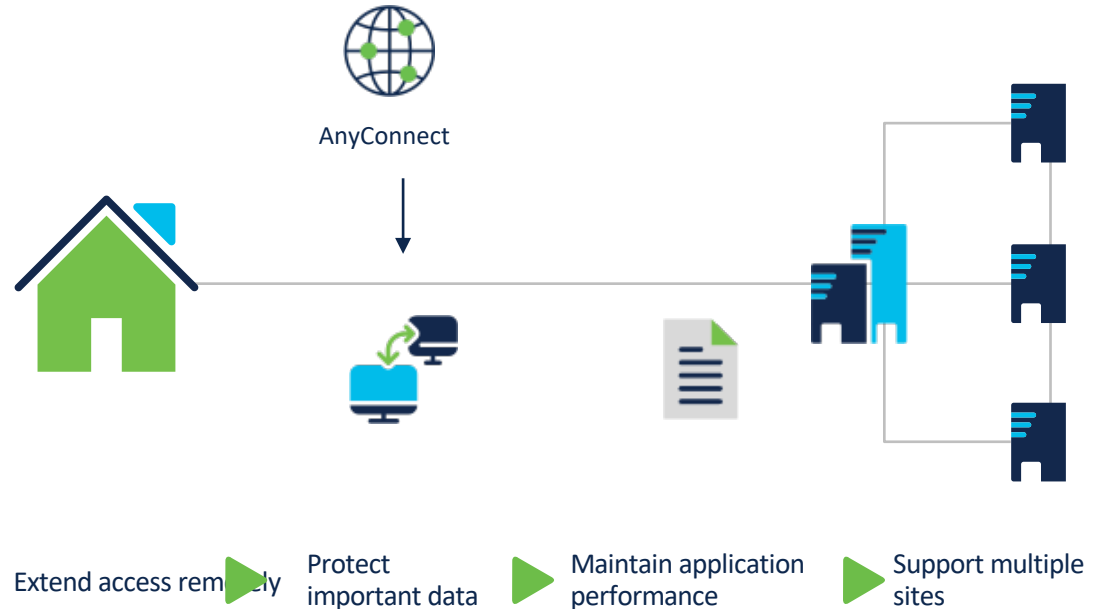


Full Mesh

Remote Access VPN

Provide ubiquitous secure access from remote and roaming users

- Posture assessment
- Uses TLS, DTLS or IKEv2
- Easy wizard-based configuration
- Identity based security policies
- Enhanced security with 2 FA/MFA provided by Secure Access (Duo)
- Passwordless Authentication



Cisco Threat Intelligence Director (CTID)

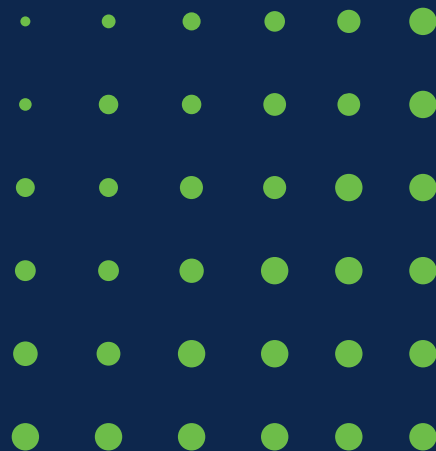
Поддержка открытых интеграций

- Расширяет преимущества информации от Talos Security Intelligence сторонними источниками
- Анализируйте и действуйте с простыми и сложными индикаторами угроз



Платформы управления

Целостная политика и осведомленность

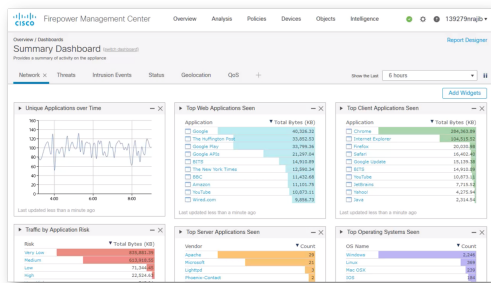


Управления для любого пользователя

Гибкость облачного или локального развертывания

Интеграции безопасности

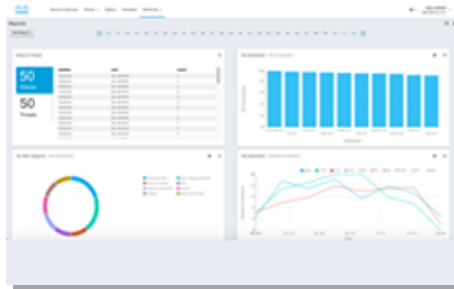
Firewall Management Center



Локальное централизованное управление с прицелом на безопасность

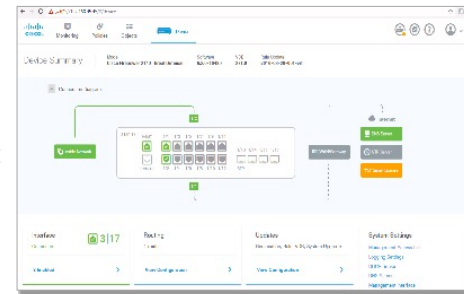
Общие API

Cisco Defense Orchestrator



Облачное централизованное управление, с прицелом на сетевые функции

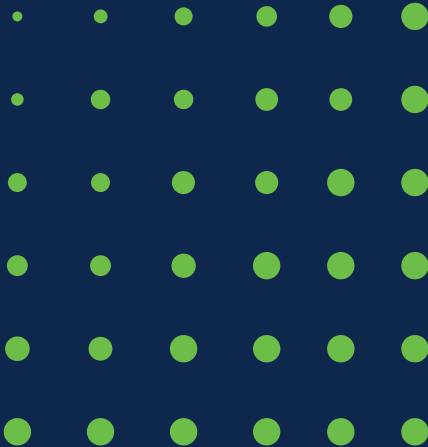
Cisco Firewall Device Manager (FDM)



Локальное управление с прицелом на сетевые функции

Coexist

Secure Firewall Management Center (FMC)



Что такое Firewall Management Center (FMC)?

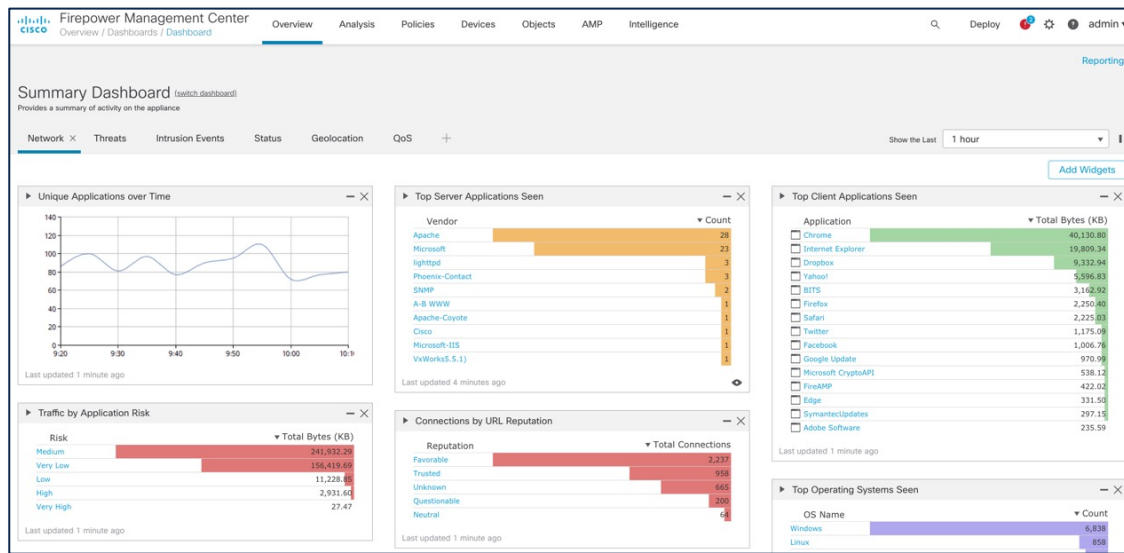
Локальная централизованная система управления для распределенных инсталляций

- **Ключевые преимущества**

- Управление многими сайтами
- Контроль доступа и политик
- Расследование инцидентов
- Приоритет реагирования
- Физическое или виртуальное устр-во

- **Функции**

- Мульти-доменное управление
- Ролевой доступ
- Высокая доступность
- APIs и pxGrid интеграция
- Политики и управление устройством
- Хосты
- Информация об угрозах



Что нового? – FMC

Новости релиза FTD 7.0

- Snort 3
- Динамические объекты
- Унифицированный просмотр событий
- Кросс-доменное доверие AD
- DNS репутационная фильтрация
- SecureX интеграция
- ACI интеграция – FMC Endpoint Update App
- Улучшения в инсталляции и обновлении
 - Проще, быстрее, меньше
 - Улучшенная отчетность по статусу и ошибкам
 - Простота наблюдения за процессом обновления
 - Больше устройств обновлять одновременно
- Улучшения в работе
 - Поиск по политикам и объектам
- Управление изменениями
 - Предв. просмотр конфигурации и история
 - Отдельное развертывание VPN функций
 - Откат настроек

Обнаружение сети

Предоставляет нужные данные в нужное время в нужном виде

- Обнаруживает приложения, пользователей и хосты благодаря пассивному анализу трафика
- Собирает контекст и помогает понять степень воздействия атаки
- Настраивает набор сигнатур IPS на основании полученных данных
- Дополняет профили хостов данными, полученными от сторонних сканеров уязвимостей

The screenshot displays the Cisco Secure NetworkMiner interface, divided into two main sections: Servers and Host Profile.

Servers (3)

Protocol	Port	Application Protocol	Vendor and Version
tcp	139	pending	
udp	0	IGMP	
tcp	80	HTTP	

Applications (1)

Application Protocol	Client	Version	Web Application
NetBIOS-dgm	NetBIOS-dgm		

User History

Users	2020-01-12 11:31:21	2020-01-13 11:31:21
maik pennington (D\CLOUD-SOC\ypenn, LDAP)		
vicente vanbuskirk (D\CLOUD-SOC\pvamb, LDAP)		
maureen cepeda (D\CLOUD-SOC\iscepe, LDAP)		
diane tibbott (D\CLOUD-SOC\dtibbott, LDAP)		
chassidy francisco (D\CLOUD-SOC\mfran, LDAP)		
garth harrington (D\CLOUD-SOC\aharr, LDAP)		
eula gruber (D\CLOUD-SOC\lgrub, LDAP)		
joy shanklin (D\CLOUD-SOC\jshank, LDAP)		
cherilyn spicer (D\CLOUD-SOC\lspic, LDAP)		
misty pagano (D\CLOUD-SOC\lpago, LDAP)		
elmira shih (D\CLOUD-SOC\lshih, LDAP)		
julian ibarra (D\CLOUD-SOC\oibarr, LDAP)		
laurine gibb (D\CLOUD-SOC\lgibb, LDAP)		
jaclyn parris (D\CLOUD-SOC\lparris, LDAP)		
takako collado (D\CLOUD-SOC\lcoll, LDAP)		
collin carlson (D\CLOUD-SOC\lucarl, LDAP)		
lavenia cohn (D\CLOUD-SOC\lcohn, LDAP)		
rochell gaspar (D\CLOUD-SOC\rgasp, LDAP)		

Host Profile

Domain: Global \ Cisco_Backend \ Cisco_SOC
IP Addresses: 10.0.10.151
NetBIOS Name: NGIPV.dcloud.cisco.com (1)
Device (Hops): NGIPV.dcloud.cisco.com (128)
MAC Addresses (TTL): 00:0C:29:03:DF:AD (VMware, Inc.) (128), 00:0C:29:61:F5:5F (VMware, Inc.) (128), 00:10:45:CE:A7:2B (Nortel Networks) (128)

Host Type: Host
Last Seen: 2020-01-13 10:31:46
Current User: sean crowley (D\CLOUD-SOC\vcrow, LDAP)

Indications of Compromise (1)

Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2020-01-13 07:39:38	2020-01-13 07:39:38

Operating System

Vendor	Product	Version	Source
Microsoft	Windows	8.1	Firepower

Управление политикой

Снижение сложности управления политикой

- Централизованное локальное управление политиками на различных платформах межсетевых экранов
- Интегрирует множество функций безопасности в единой политике доступа
- Снижает необходимость ручной настройки путем наследования и использования шаблонов.

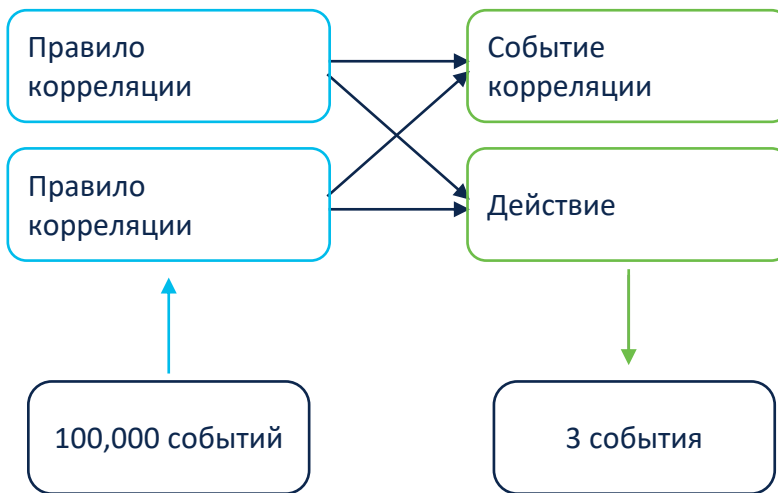
Name	Source Zone	Dest Zone	Source Network	Dest Network	VLAN Tag	Users	Applic.	Source Ports	Dest Ports	URIs	Source SCL	Dest SCL	Action
1 Spurk Access	OutZone	InZone	198.16.13	Spurknet	Any	Any	Any	Any	Any	LOP (172)	Any	Any	Trust
2 Block SSH for HR	Any	Any	Any	Any	Any	Any	dCloudRes	OpenSSH SSH	Any	Any	Any	Any	Block will
3 Block Extranet11	InZone	OutZone	Any	Extranet12	Any	Any	Any	Any	Any	Any	Any	Any	Block will
4 Block ICMP Over	GRE	Any	Any	Any	Any	Any	Any	ICMP	ICMP for p	Any	Any	Any	Block will
5 Block Unwcopts	Any	Any	Any	Any	Any	Any	Any	Any	Any	Pornograp Adult (Any Gaming) Letters & Hate Spee	Any	Any	Block will
6 Block Extra to Int	OutZone	InZone	Extranet	Infrastruc	Any	Any	Any	Any	Any	Any	Any	Any	Block will

ФМС: Автоматизация реагирования на угрозы

Снизить шум и точно среагировать

- Корреляция событий безопасности
- Вызов автоматического реагирования
 - Email
 - Syslog
 - SNMP
 - Remediation module
- Интеграция с системой контроля доступа и сторонними продуктами

Политика корреляции

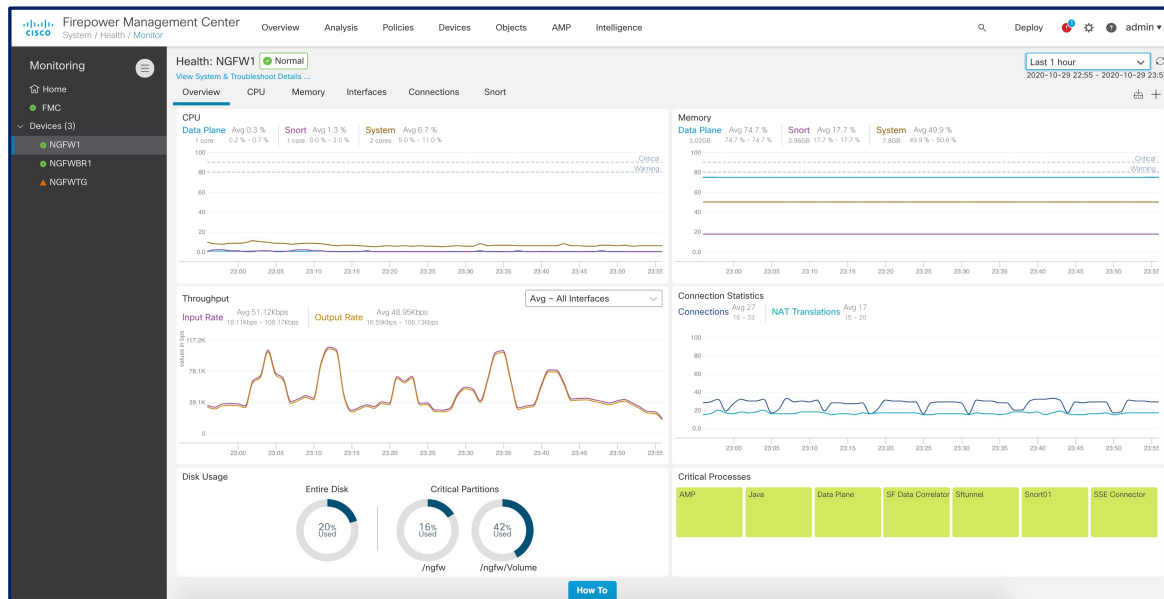


Мониторинг состояния устройств

Унифицированная статистика из подсистем и критических процессов

Функции

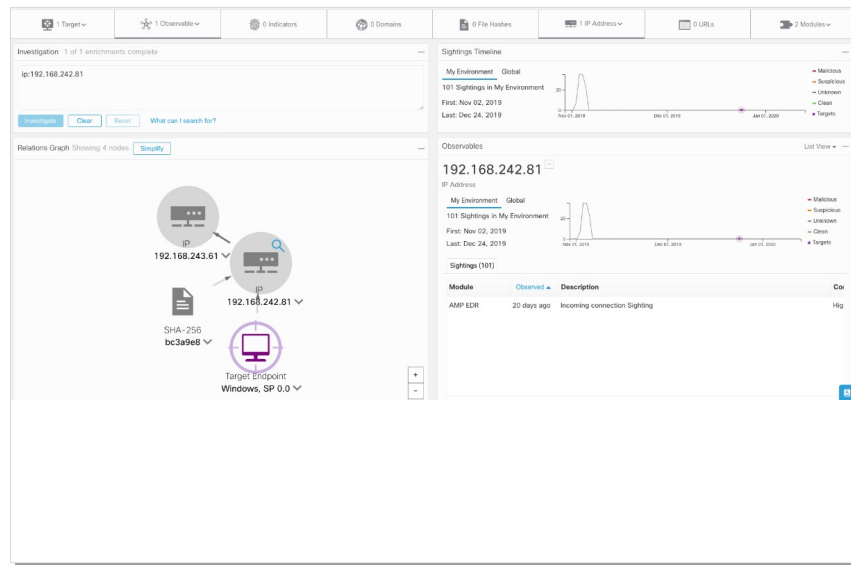
- Графики с трендами, наложение данных и собственные графики
- Улучшенный живой мониторинг включая статус отказоустойчивости и кластера
- Унифицированный Data plane и метрики Snort (прим. CPU, Memory)
- Отчетность по Snort, Настройкам, Соединениям и статистике Процессов
- Доступно через API



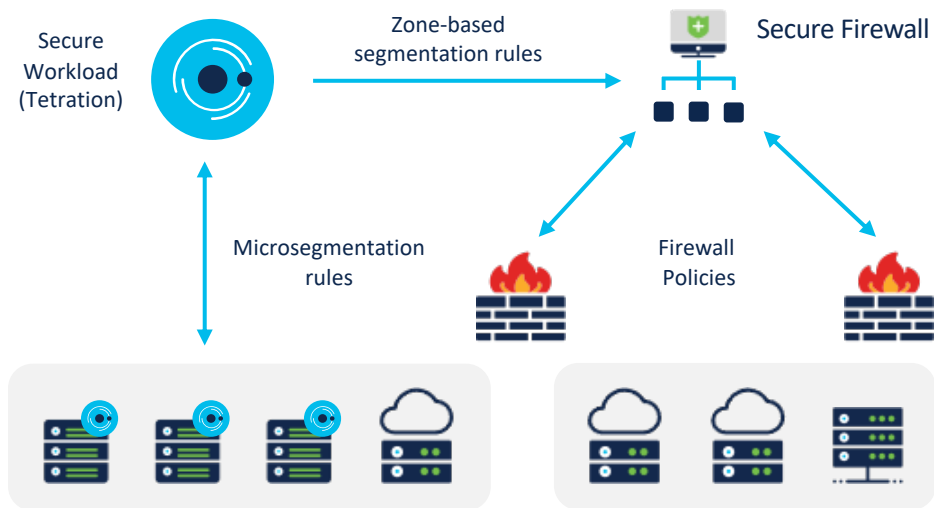
FMC Интеграции

Осведомленность и аналитика выходящие за рамки анализа сети

- Тесная интеграция FMC с Secure Endpoint
- Основанные на стандартах вектора угроз (STIX/TAXII)
 - Cisco Threat Intelligence Director (CTID)
- Снизить время на реагирование с широкими возможностями обнаружения и корреляции
 - SecureX Threat Response (CTR)
- Использовать другие продукты Cisco и сторонние продукты для расширения возможностей
 - FMC внешние запросы
- Использовать SIEMы с Унифицированными событиями



Динамическая политика в Multi-Cloud окружении



Прозрачная интеграция

Единая политика сегментации в Secure Firewall и Secure Workload



Динамические политики

Политика обновляется автоматически основываясь на связях приложения



Расширение в Cloud провайдеров

Этой осенью, расширение рекомендуемого функционала в AWS и Azure группы безоп-ти

“ Ждем с нетерпением! Интеграция в multcloud позволит лучше выстраивать выстраивать безопасность в распределенной среде. ”

-- Global payments and fleet management enterprise

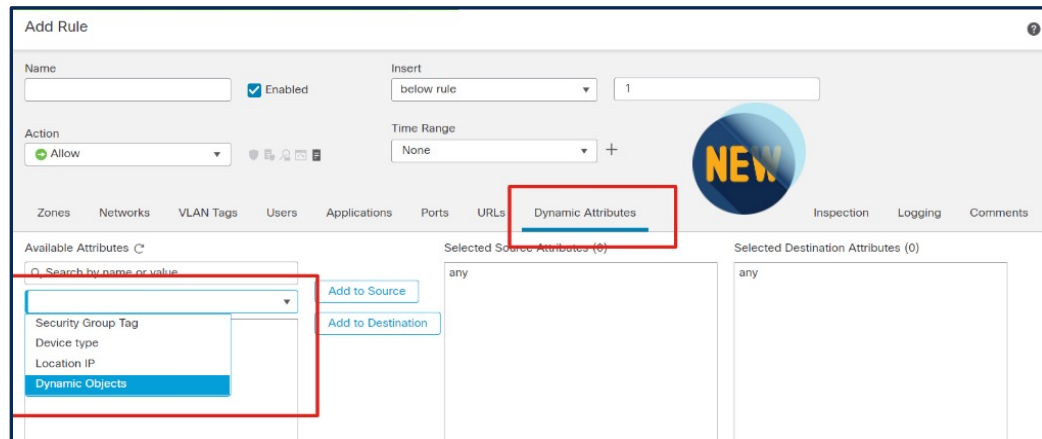
Cisco Secure Dynamic Attribute Connector



Потребность: В динамическом и multicloud мире, администраторы не успевают следить за постоянно меняющимися объектами IP для приложений по мере их запуска и отключения или изменения.

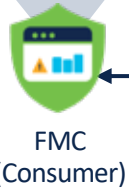
Решение: Cisco предоставляет программируемый метод создания, удаления и управления динамическими объектами. Работает для VMware, AWS, и Azure тегов в том числе.

Преимущества: Категорически снизить загрузку администраторов по отслеживанию актуальности политик, предоставляет обновления политики по запросу без промедления и необходимости развертывания политики

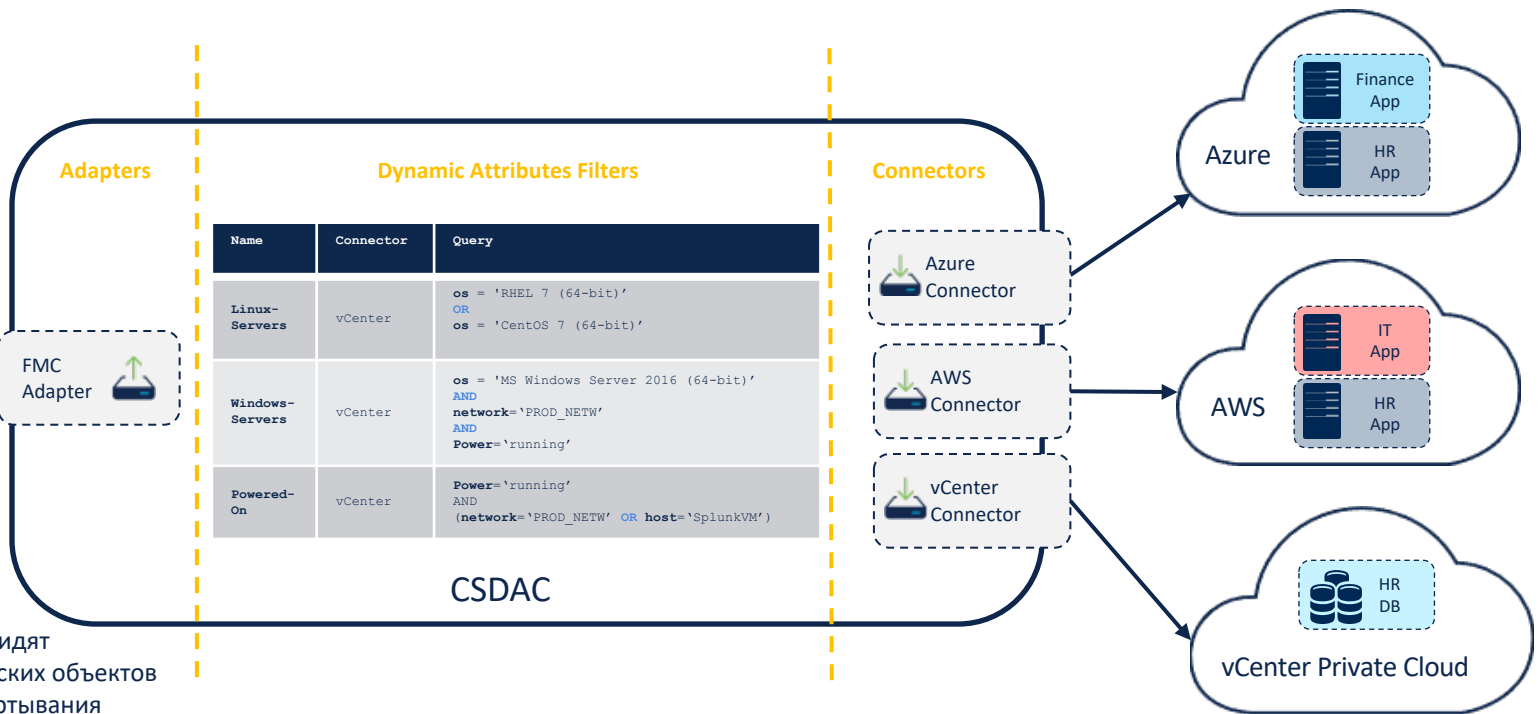


Cisco Secure Dynamic Attributes Connector (CSDAC)

Dynamic Object	Mappings
Linux-Servers	172.16.0.1 172.16.0.3
Windows-Servers	10.0.1.11 10.0.1.14 10.0.1.20
Powered-On	10.0.1.14



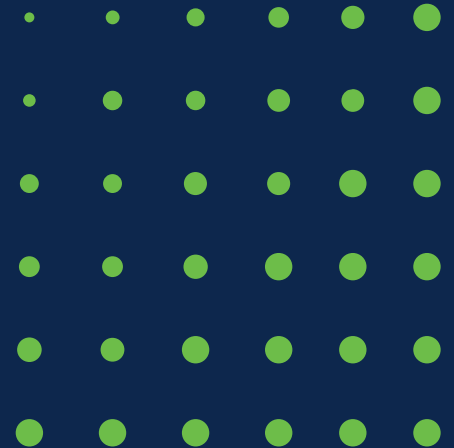
{REST}



Преимущества:

- Сенсоры мгновенно видят изменения динамических объектов
- Изменения без развертывания политики

Secure Firewall Device Manager (FDM)



Что такое Secure Firewall Device Manager (FDM)

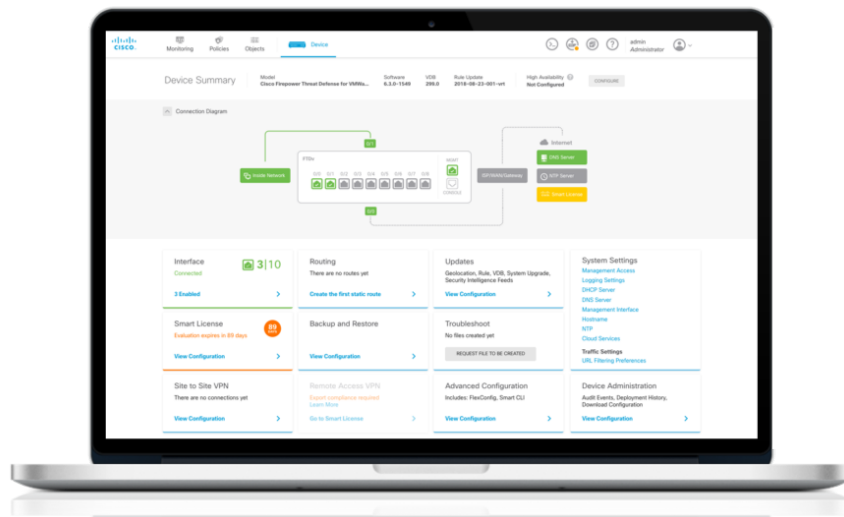
Управление одним устройством и API платформа

- Важные преимущества

- Простая настройка
- Контроль доступа и политик
- Автоматизация настройки
- Продвинутое управление

- Функции

- Ролевой доступ
- Высокая доступность
- NAT и маршрутизация
- IPS и борьба с Malware
- Мониторинг состояния
- Поддержка VPN



Что нового? – FDM

Новое в релизе FTD 7.0

- DNS фильтрация репутации
- ECMP
- DHCP Relay Service
- IPv6 DHCP Autoconfig
- IPS улучшения
 - Snort 3 собственные правила
 - Правила доступа по времени (только API)
 - Множественные виртуальные маршрутизаторы



Простое управление межсетевым экраном

Простота настройки, управления, мониторинга

Управляет Firepower Threat Defense на низко и средне производительных платформах



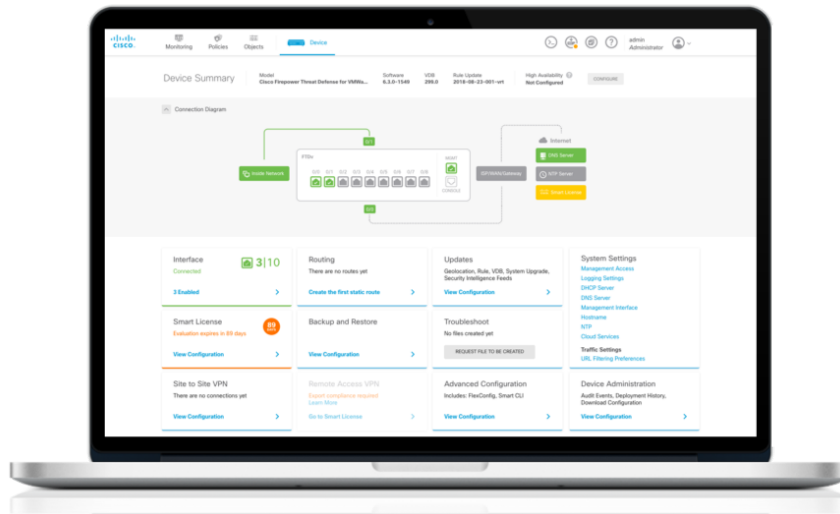
Простые мастера конфигурации



Пред-настроенные политики безопасности для простого управления

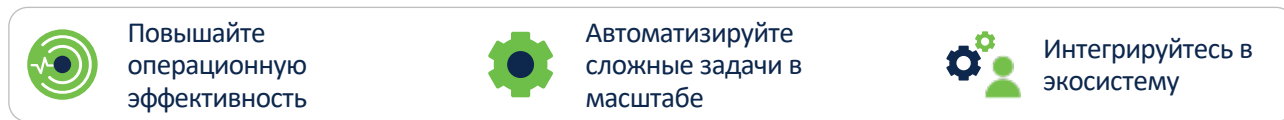


Построен на API FTD устройств



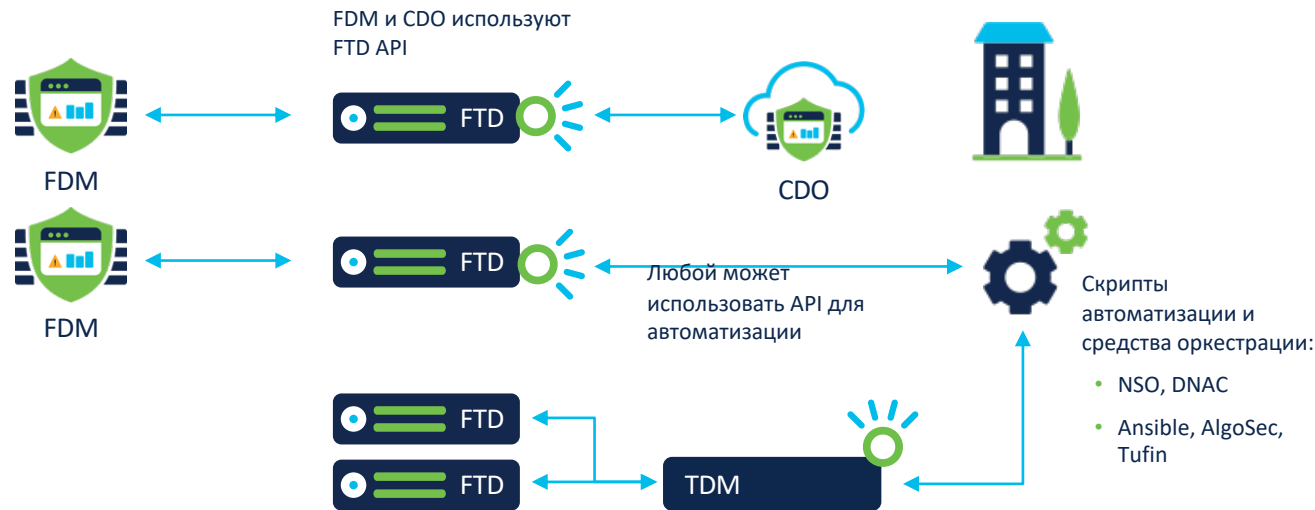
Подход API-First

Открытая архитектура управления и отчетности

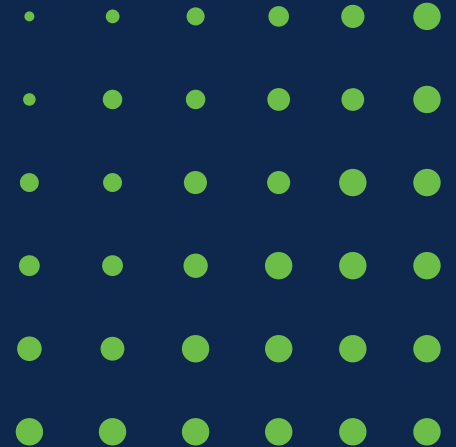


Ключевые функции

- Day 0 Развертывание
- Day 1-2 Управление настройкой
- Обслуживание, отладка, мониторинг



Cisco Defense Orchestrator



Что такое Cisco Defense Orchestrator

Целостно управляйте политикой различных продуктов безопасности

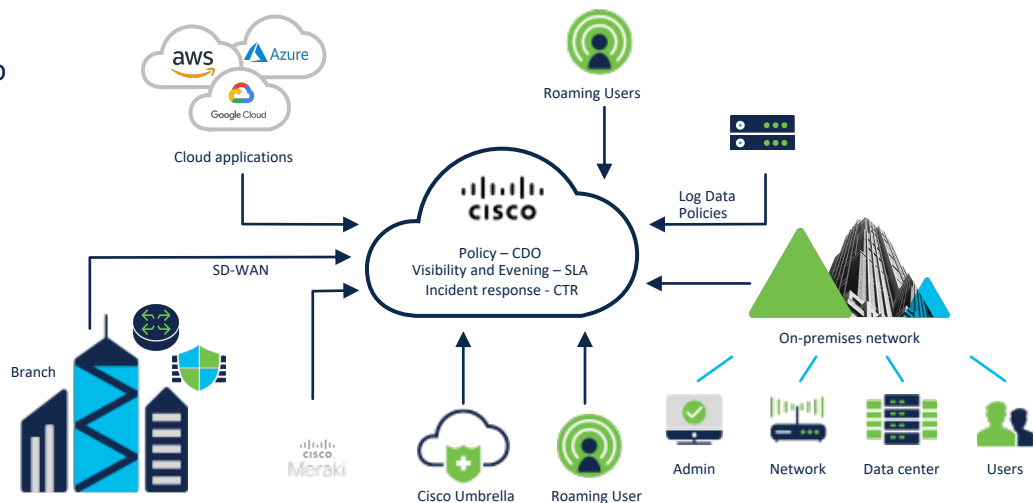
CDO это облачное приложение, которое абстрагирует сложность для экономии времени и поддерживает организацию защищенной от актуальных угроз.

Ключевые преимущества

- Оптимизация управления безопасностью
- Снижение времени, затрачиваемого на управление политикой до 90%
- Получить лучше безопасность со сниженной сложностью
- Приоритетное реагирование

Функции

- Целостное применение политик
- Быстрое развертывание устройств
- Управление настройками

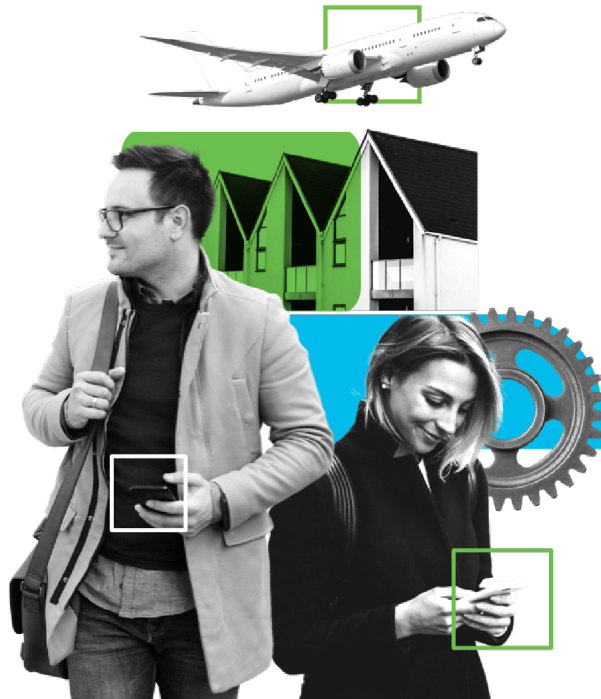


Что нового? – CDO

Май 2021

- Сервис уведомлений
- Поддержка интерфейса EtherChannel в FTD
- Поддержка Multi-tenant
- Low Touch Provisioning
- Secure Group Tags (SGT)
- Объекты AD Objects

CDO постоянно обновляется, [здесь](#) свежая информация



Cisco Defense Orchestrator

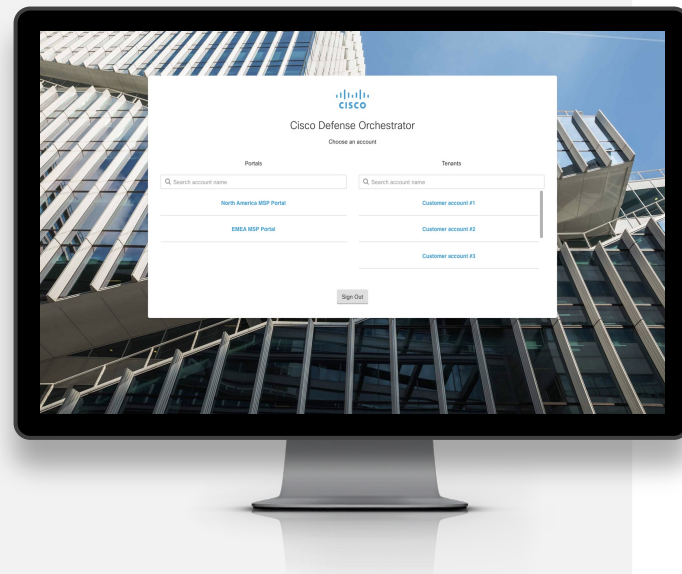
MSP портал

- Используйте CDO MSP портал для управления неограниченным количеством пользовательских аккаунтов
- Простое отображение и поиск устройств во всех Tenant'ах заказчиков
- Распределение заказчиков по MSP порталам для ограничения административных функций



Benefits

- Низкие начальные расходы – Платите по мере роста
- Быстрый запуск и внедрение
- Централизованная осведомленность с MSP порталом
- Поддержка Multi-Tenant архитектуры
- Аудит и оптимизация
- Автоматизация с API



Преимущество Облачного / SaaS решения

Высокая доступность, полнофункциональное облачное решение

Глобально

- Управляйте устройствами через API с TLS v1.2
- Настройки зашифрованы как при хранении так и при передаче.
- CDO локации размещения:
 - AWS – US West
 - AWS – US East
 - AWS – EU Central
 - AWS – APJC
- Безопасное управление с ролевой моделью и SAML 2-хфакторной аутентификацией
- Позволяет multi-tenant управление – полное разделение клиентов

- Масштабирование / Гибкость
- Без обслуживания
- Быстрое внедрение функций
- Низкие входные затраты
- Быстрое реагирование на изменение требований

99.999%

SLA доступности



Развертывание
<1 дня



Модель подписки с
моделью Pay as you
Grow

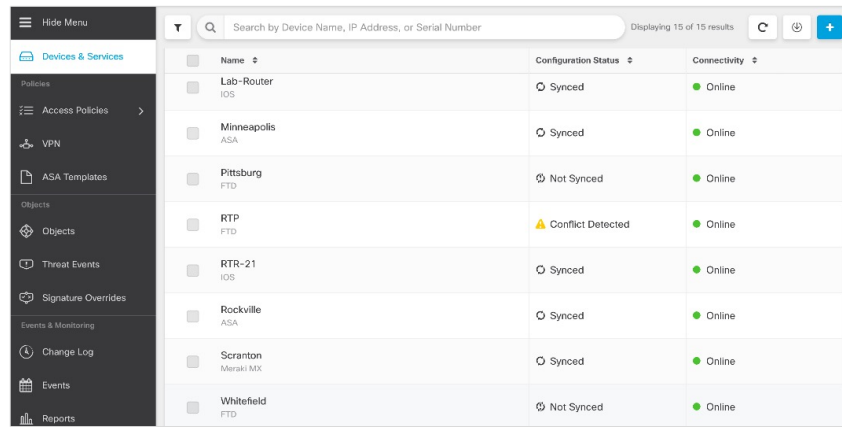


Низкие расходы на
содержание

Масштабируемое управление политиками

Простая гибкая платформа управления для смешанных окружений

- Управление политиками в крупном масштабе
 - Шаблоны и макросы позволяют быстро создавать конфигурации для тысяч устройств
 - Простая миграция ASA в FTD
 - Интеграция различных функций безопасности в единую политику доступа



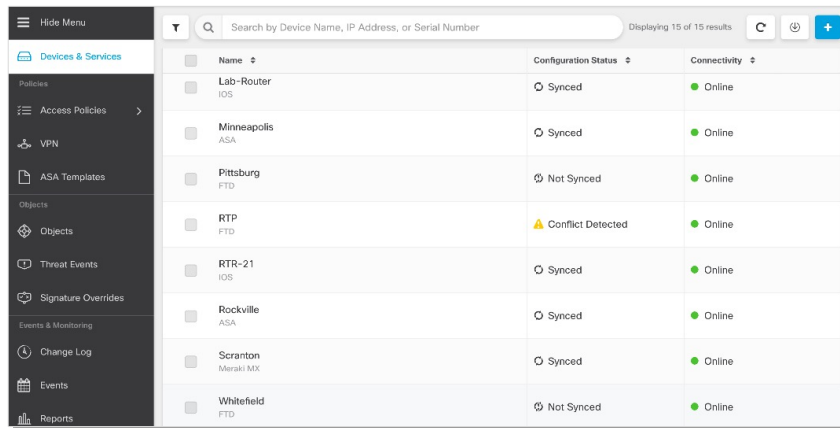
The screenshot displays the Cisco Secure Policy Center interface. On the left is a dark sidebar menu with categories like 'Policies', 'VPN', 'Objects', 'Threat Events', 'Signature Overrides', 'Events & Monitoring', and 'Reports'. The main area shows a table of devices with columns for Name, Configuration Status, and Connectivity. A search bar at the top right indicates 'Displaying 15 of 15 results'.

Name	Configuration Status	Connectivity
Lab-Router IOS	Synced	Online
Minneapolis ASA	Synced	Online
Pittsburg FTD	Not Synced	Online
RTP FTD	Conflict Detected	Online
RTR-21 IOS	Synced	Online
Rockville ASA	Synced	Online
Scranton Meraki MX	Synced	Online
Whitefield FTD	Not Synced	Online

Простое и эффективное управление объектами

Простое графическое сравнение объектов

- Обнаружение конфликта объектов с простым исправлением ненужных объектов
 - Дубликаты
 - Не используемые
 - Не полные
- Анализ объектов снижает объем конфигураций



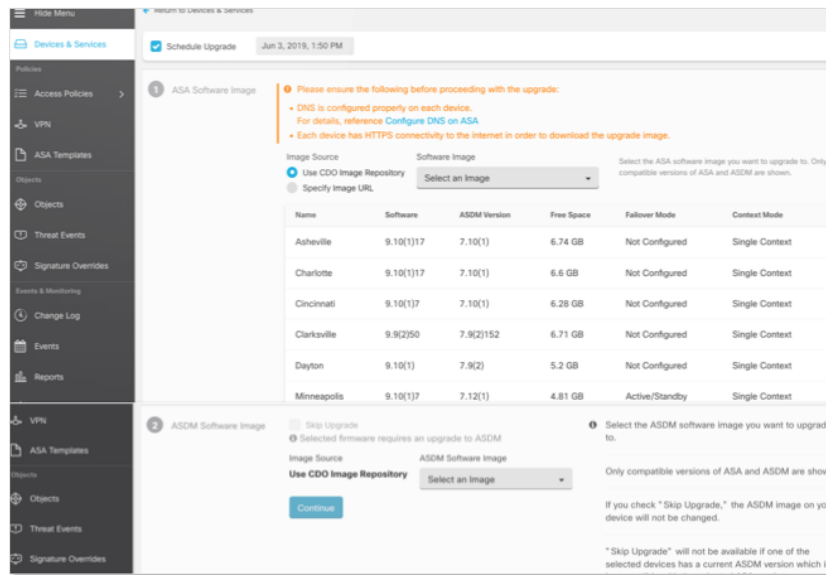
The screenshot displays the Cisco Secure configuration management interface. On the left is a dark sidebar menu with categories like Policies, VPN, ASA Templates, Objects, Threat Events, Signature Overrides, Events & Monitoring, Change Log, Events, and Reports. The main area shows a search bar and a table of 15 devices. The table has columns for Name, Configuration Status, and Connectivity. One device, RTP (FTD), is highlighted with a yellow warning icon and the text 'Conflict Detected'.

Name	Configuration Status	Connectivity
Lab-Router IOS	Synced	Online
Minneapolis ASA	Synced	Online
Pittsburg FTD	Not Synced	Online
RTP FTD	Conflict Detected	Online
RTR-21 IOS	Synced	Online
Rockville ASA	Synced	Online
Scranton Meraki MX	Synced	Online
Whitefield FTD	Not Synced	Online

CDO: Проще управлять устройствами

Полный жизненный цикл управления МСЭ

- Быстрая регистрация устройств
- Простое массовое обновление
 - Снижение времени на планирование и выполнение обновления
- Глобальное отслеживание изменения настроек с аудит логом
- Быстрое резервное копирование настроек и их восстановление снижает простои



Поддерживаемые платформы Defense Orchestrator

Платформы

Минимальный софт

ASA 5500-X



ASA 8.4 FTD 6.4

Firepower 1000



ASA 9.13 FTD 6.4

Firepower 2100



ASA 8.4 FTD 6.4

Firepower 4100



ASA 8.4 FTD 6.5

Firepower 9300



ASA 8.4 FTD 6.5

Virtual – Private Cloud

KVM, VMWare

ASA 8.4 FTD 6.4

Virtual – Public Cloud

AWS, Azure

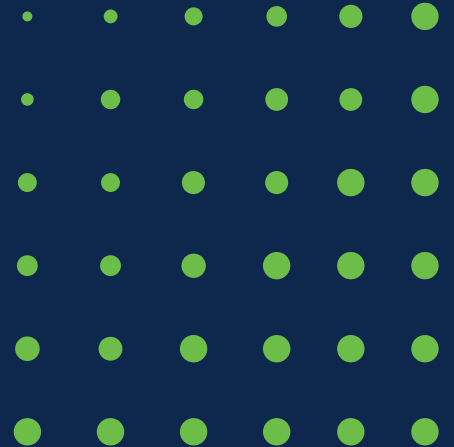
ASA 8.4 FTD 6.5 (Azure)

Meraki MX



Последняя версия ПО

Cisco Security Analytics and Logging



Архитектура аналитики и логирования



SAL (SaaS) Облачные функции



Облачное хранение 90 дней (по умолчанию) до 3 лет, с просмотром и выгрузкой из CDO



Поддержка **всех** Cisco FTD и ASA устройств. Опция **напрямую в облако** доступа в FMC 7.0+ управляемых устройствах



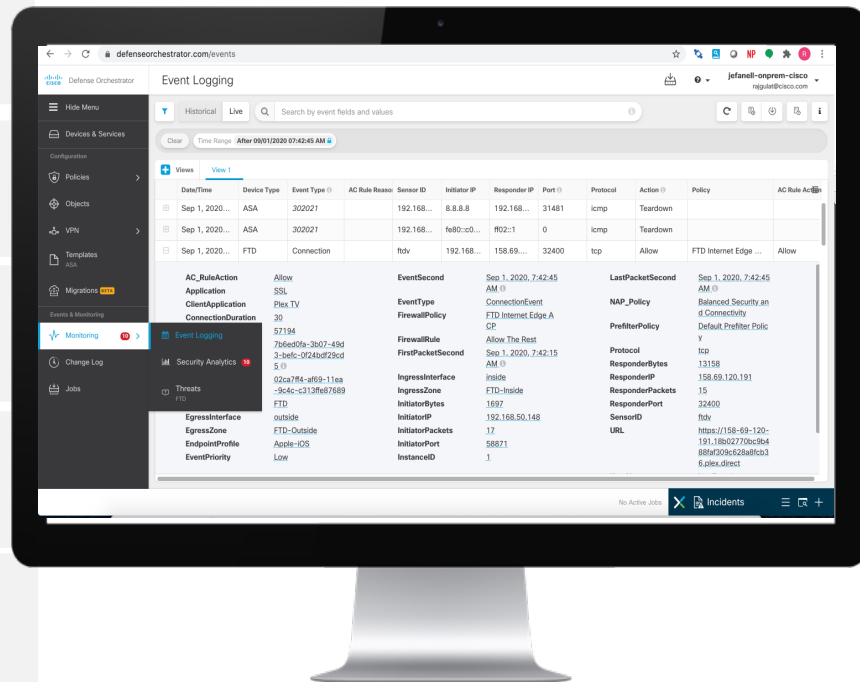
Анализ логов МСЭ для обнаружения продвинутых угроз с использованием Secure Cloud Analytics (SCA)



Корреляция логов МСЭ с внутренней сетью и логами из облака в SCA

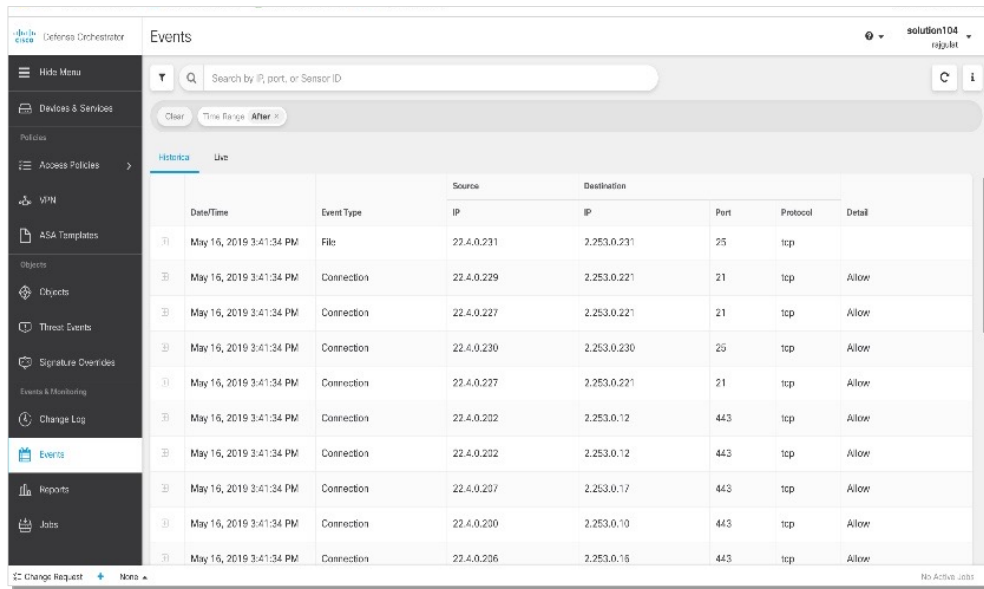


Существующие заказчики CTR-SecureX могут легко использовать SAL логирование объединив его со своим SecureX tenant



CDO: Cisco Security Analytics and Logging

Снизить сложность и объем событий лога



The screenshot shows the Cisco CDO Events page. The interface includes a search bar, a time range filter set to 'After', and a table of events. The table has columns for Date/Time, Event Type, Source IP, Destination IP, Port, Protocol, and Detail. The events listed are all 'Connection' events from May 16, 2019, at 3:41:34 PM, involving various source and destination IP addresses and ports.

Date/Time	Event Type	Source IP	Destination IP	Port	Protocol	Detail
May 16, 2019 3:41:34 PM	File	22.4.0.231	2.253.0.231	25	tcp	
May 16, 2019 3:41:34 PM	Connection	22.4.0.229	2.253.0.221	21	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.227	2.253.0.221	21	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.230	2.253.0.230	25	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.227	2.253.0.221	21	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.202	2.253.0.12	443	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.202	2.253.0.12	443	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.207	2.253.0.17	443	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.200	2.253.0.10	443	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.206	2.253.0.16	443	tcp	Allow



Храните безопасно в облаке сетевые и МСЭ логи, доступные для поиска из CDO



Идентифицировать и обогащать высокоприоритетные уведомления



Более продвинутое реагирование и снижение времени расследования



Использовать функции обнаружения угроз с лучшей в классе аналитикой безопасности

Функции SAL On-Premise



FTD (включая логи data-plane) и логи ASA logging в масштабируемом локальном хранилище логов



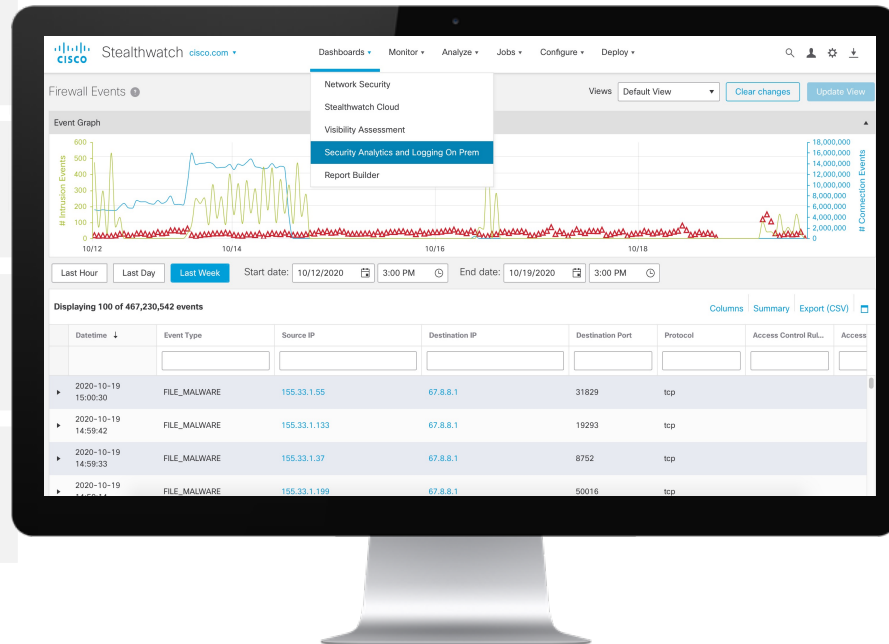
Мастер настройки логирования в FMC 7.0+ упрощает настройку облачного и локального логирования



В версии FMC 7.0+ масштабирование для логирования и аналитики улучшено в 300X magnitude с использованием удаленного query SAL/ SNA 7.3.2+



Контекстная навигация в просмотре событий внутри Secure Network Analytics (SNA) для лучшего контекста



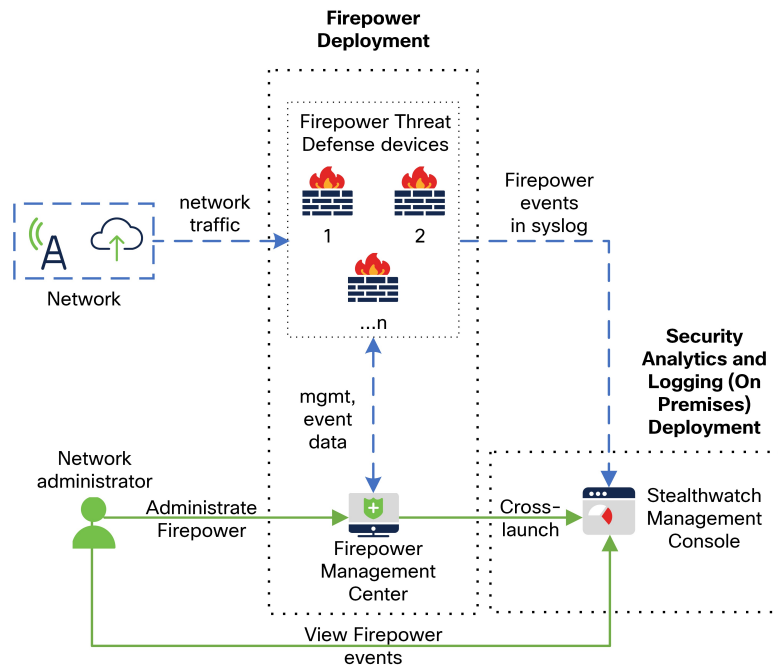
FMC интеграция с Cisco Security Analytics and Logging (On-Prem)

Кнопка для простой настройки

- В FMC настраиваются ссылки кросс-запуска для консоли аналитики Secure Analytics
- Настраиваются учетные данные для запроса данных из удаленного хранилища

Лучше масштабирование времени и емкости хранения

- Внешнее хранилище с использованием Cisco Security Analytics and Logging On-Prem
- Автоматический выбор источника событий для отображения или ручное указание



Лицензирование Security Analytics and Logging

3 уровня лицензии (вложенные)



Logging and Troubleshooting*

Масштабирование логирования событий FTD и ASA как в облаке так и локально, с API интеграцией через Manager; CDO для облака, и FMC для локального хранения



Logging Analytics and Detection

Анализ логов МСЭ используя поведенческий анализ угроз в Secure Cloud Analytics (SaaS)

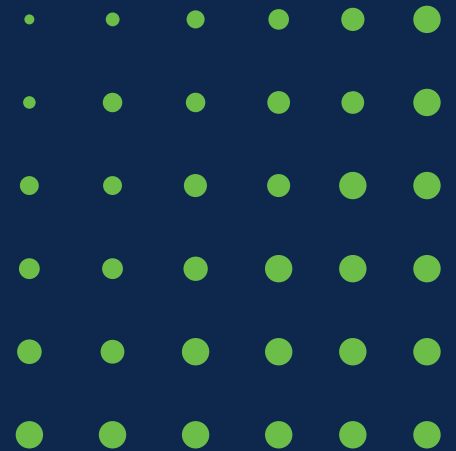


Total Network Analytics and Detection

Консолидированный анализ, происходящий по наборам данных МСЭ, внутренних и логов публичного облака для более полного анализа угроз

*Security Analytics and Logging (On Premises) На текущий момент доступен только с лицензией Logging and Troubleshooting, включающей удаленные запросы от FMC

ASA



Adaptive Security Appliance (ASA)

Надежный и эффективный межсетевой экран, инспектирующий с отслеживанием статуса соединения мощным VPN функционалом

ASA 5500X серия или Firepower серия с программным обеспечением ASA

- Основные преимущества
 - Базовая инспекция (L2-L4)
 - Инспекция протоколов Layer 7
 - Простые правила по 5-ти параметрам (5-tuple)
 - Multi-Context
 - Балансировка нагрузки VPN
- Функции
 - Remote Access и Clientless VPN
 - EzVPN, IKEv2/L2TP, DTSL1.2
 - Site to Site VPN
 - SSO with SAML, DAP
 - Маршрутизация, CG NAT, QOS



Программное обеспечение ASA предоставляет

Надежный и эффективный межсетевой экран, инспектирующий с отслеживанием статуса соединения мощным VPN функционалом



Правила

- Контроль с отслеживанием статуса
- Правила только на основе 5-ти условий
- Два варианта реагирования – Разрешить или заблокировать



Функции

- VPN: Remote Access, Clientless, EzVPN, IKEv2/L2TP/3rd party Remote Access, Site-Site Route Based и Policy Based VPN, DTLS 1.2
- Маршрутизация и качество обслуживания
- Carrier Grade NAT
- DAP
- SSO with SAML



Автоматизация

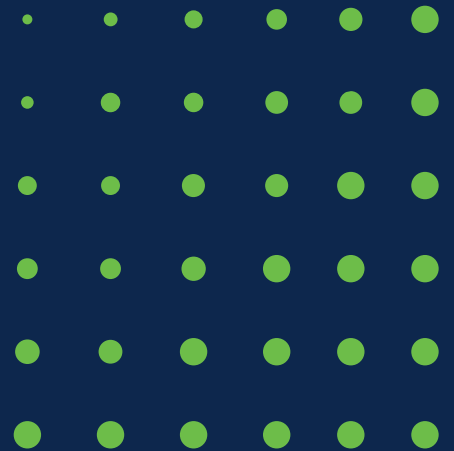
- Использование API для интеграции с SIEM
- Использование API для создание фильтров по 5-ти параметрам



Безопасность

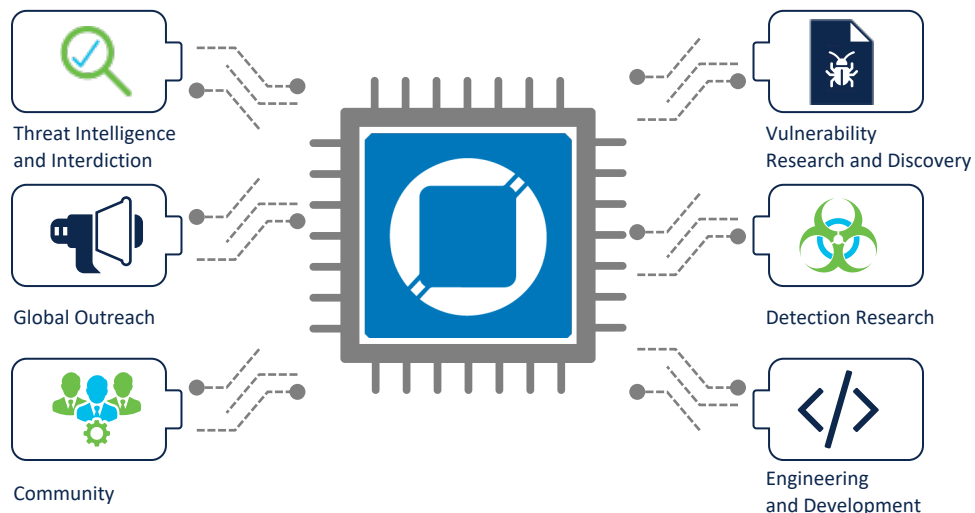
- Фильтрация пакетов и классические методы фильтрации от Layer 2 до Layer 4
- Отсутствуют продвинутые сервисы безопасности, такие как IPS, Endpoint, URL Filtering, Application control и другие.

Talos



Что такое Talos?

Talos это большая интеллектуальная группа в Cisco. Мы здесь чтобы сражаться на светлой стороне – мы работаем чтобы защищать от угроз наших заказчиков и пользователей в целом.



От непонятого к известному

Продуктовая телеметрия



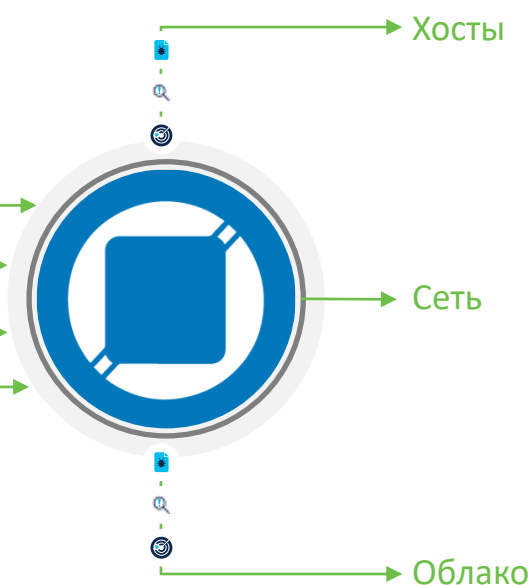
Обмен данными



Обнаружение уязвимостей



Ловушки для угроз



- Endpoint Detection and Response
- Mobile Security
- Multi-factor authentication

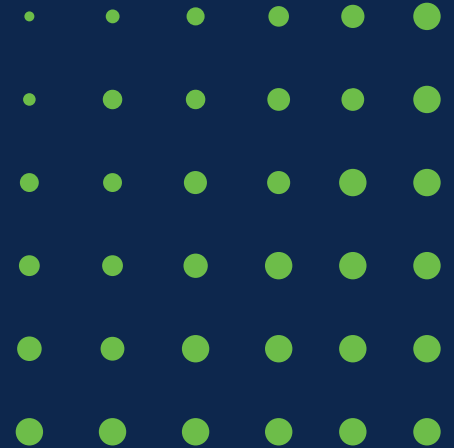


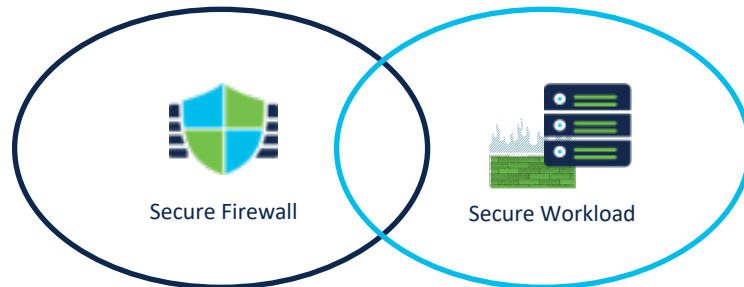
- Firewall
- Intrusion Prevention
- Web Security
- SD Segmentation
- Behavioral Analytics



- Security Internet Gateway
- DNS Security
- Secure Email

Secure Firewall & Secure Workload





Кто?

Архитекторы
безопасности

DevSecOps

NetOps

Аудит

Почему?

Безопасность будущего

Динамические политики

Поддерживать актуальность

Согласованность между firewall и
workload

Ценность

Синхронизированная безопасность

Видимость и автоматизация

Динамические объекты = быстро и
просто

Простой вид гарантирует наличия
контролей на своем месте



Управление политиками является существенным камнем преткновения при добавлении сегментации

Cisco Secure Workload (ранее Tetration) предлагает возможности по интегрированному обнаружению и созданию политик в как часть жизненного цикла управления политик



Локальный



SaaS



Увидеть всю сетевую
активность приложений



Автоматически обнаружить
группу и идентификацию
приложения



Валидировать и симулировать
политику до применения

Secure Workload (Tetration)



Сквозная защита cisco убирает пробелы

Безопасность North-South с
Cisco Secure Firewall
(ранее NGFW)



Безопасность East-West с
Cisco Secure Firewall



Безопасность Workload с
Cisco Secure Workload
(ранее Tetration)



Широкая видимость

- Secure Firewall на границе УОД
- Видимость в internet, бранч, кампус
- Политики на базе атрибутов



Грубый контроль

- Сегментация в ЦОД
- Управление workload без агентов
- Обычные или мультиоблака
- Физический/виртуальный форм фактор



Точный контроль

- Обеспечение детального контроля между приложениями
- Поддержка быстрой автоматизации

Ближе к приложению

Интеграция Secure Firewall/Secure Workload

Secure Workload интегрируется с Secure Firewall для передачи информации о Workload.

Политики Secure Workload могут обновлять правила Access Control на firewall.

Устройства Firewall как:

- Граница Internet
- Пользователь - приложение
- Публичные облака

Используется для расширения и улучшения защиты, которая предлагается агентами Secure Workload.

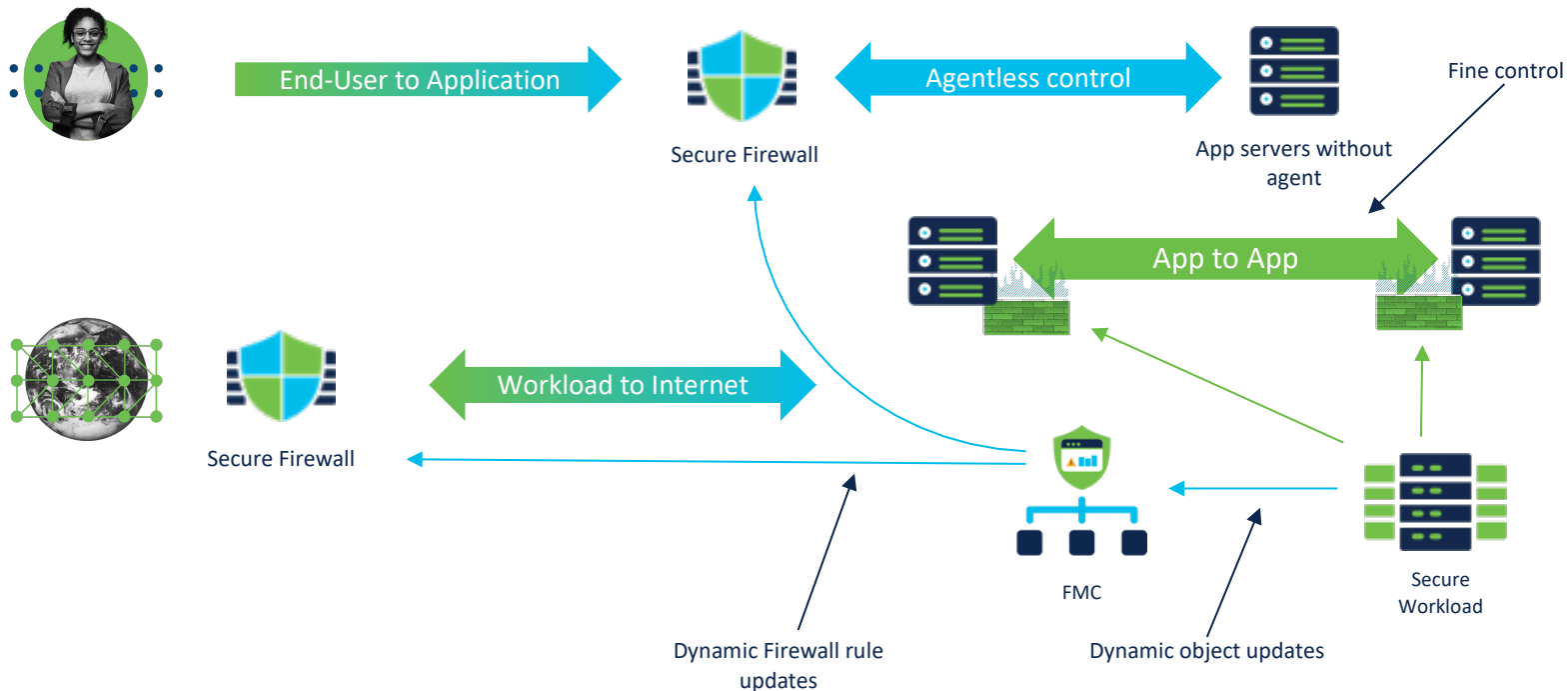
Ключевые функции

- Динамическое обновление правил Firewall
- Дополнительный уровень защиты, который основан на существующих политиках Secure Workload
- Advanced access control options (intrusion and file policy, URL filtering, etc.)
- Device firewall rule updates without policy deployment

Key Capabilities

- Automated firewall rule updates based on workload changes
- Workload protection anywhere you deploy Secure Firewall even if Secure Workload agent is not available
- Fine grained control without firewall bottleneck
- Enhance static firewall rules with dynamic workload intelligence
- Secure Workload policy simulation
- Keep pace with constantly changing DevOps application environment

Secure Workload Integration



Secure Workload Integration



End-User to Application

Secure Firewall



Agentless control



App Сервера без агентов

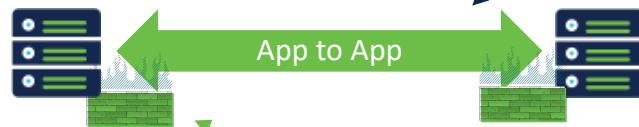
Fine control

Подключениями пользователей приложений, проходящих через межсетевую экран Cisco Secure, можно управлять для рабочих нагрузок приложений независимо от того, развернут ли агент Secure Workload в экземпляре приложения.



Secure Firewall

Workload to Internet



App to App



FMC



Secure Workload

Secure Firewall также обеспечивает расширенные функции безопасности, такие как глубокая проверка пакетов и анализ файлов вредоносных программ.

Динамическое обновление правил

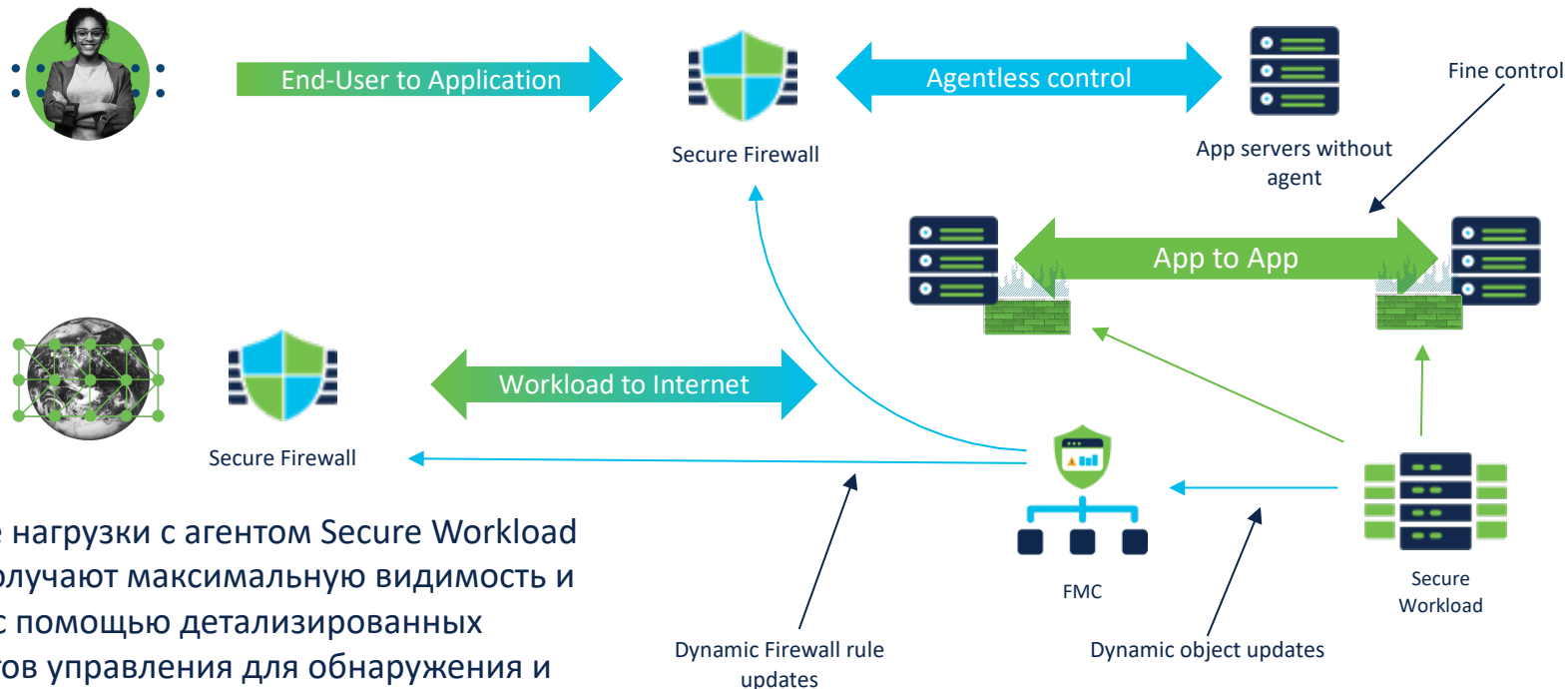
Динамическое обновления объектов

Интеграция Secure Workload



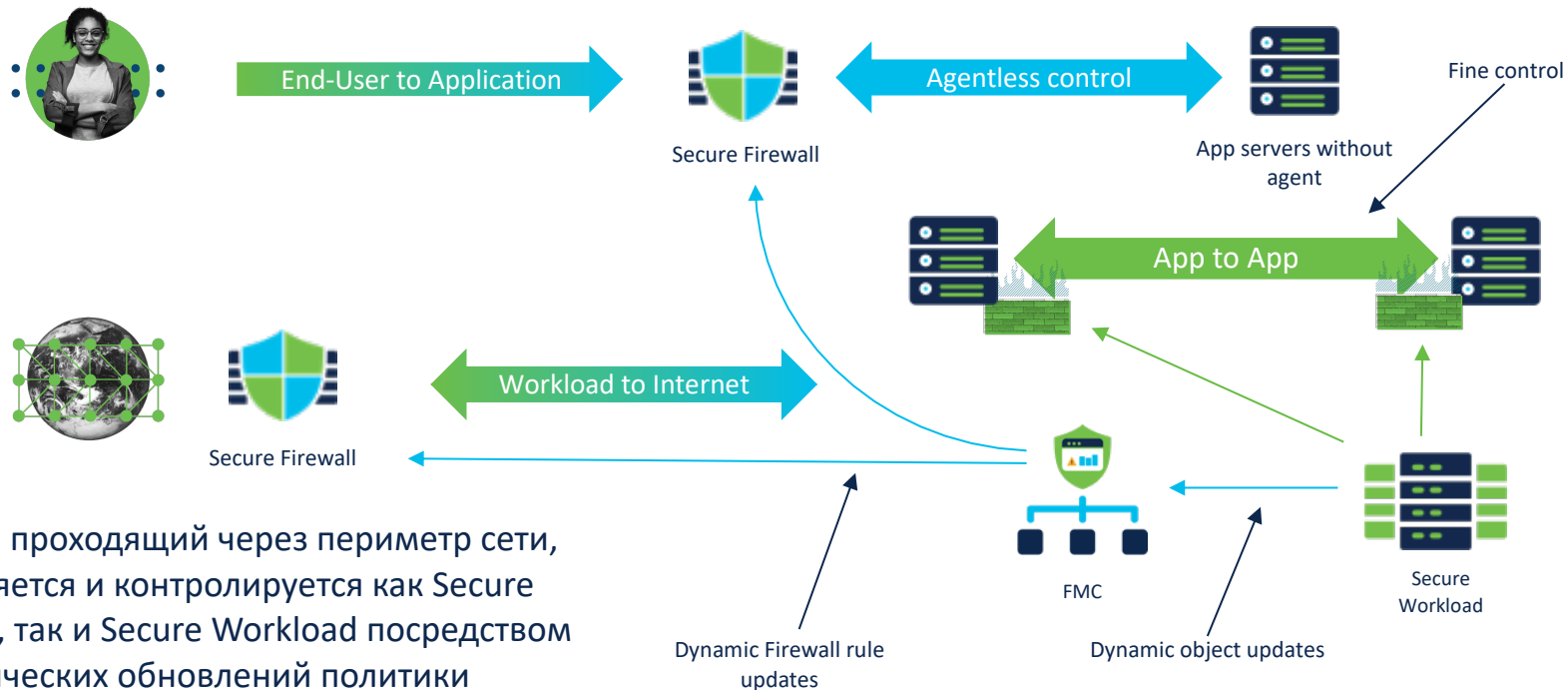
В тех случаях, когда агент Secure Workload не может быть установлен, Secure Firewall может обеспечить защиту и контроль взаимодействия рабочих нагрузок.

Интеграция Secure Workload



Рабочие нагрузки с агентом Secure Workload Agent получают максимальную видимость и защиту с помощью детализированных элементов управления для обнаружения и предотвращения вредоносной активности.

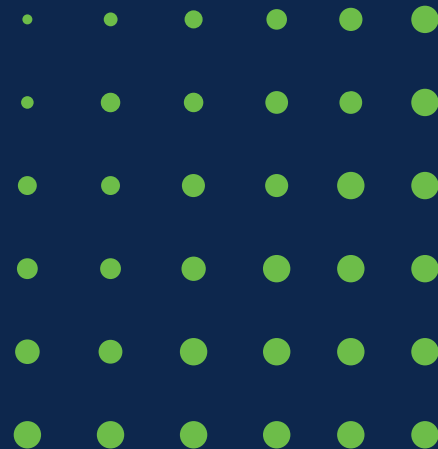
Интеграция Secure Workload



Трафик, проходящий через периметр сети, проверяется и контролируется как Secure Firewall, так и Secure Workload посредством динамических обновлений политики брандмауэра.

SecureX

Платформа безопасности



Что такое SecureX threat response?

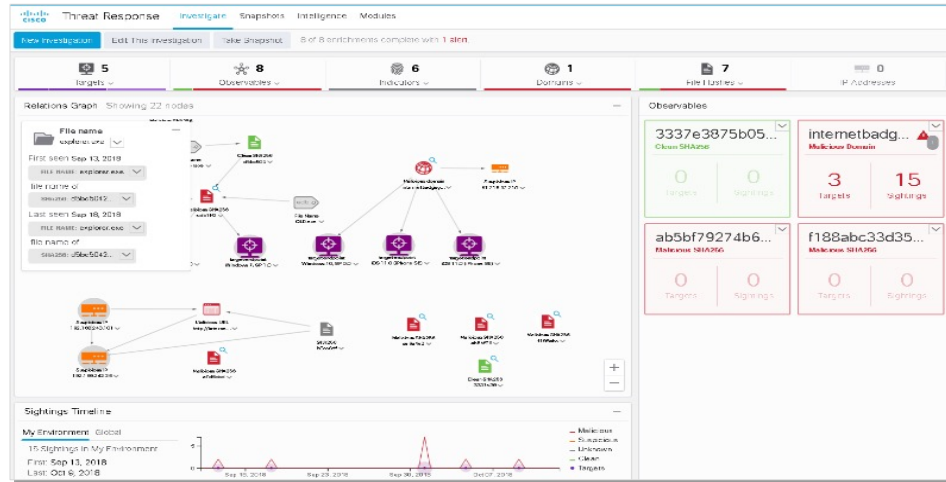
Автоматизирует интеграцию между сетями, узлами и облачными средами

• Ключевые преимущества

- Встроенная интеграция
- Ускорение кибер-расследований
- Включено в лицензии на продукты безопасности Cisco
- Уменьшите нагрузку на другие продукты безопасности

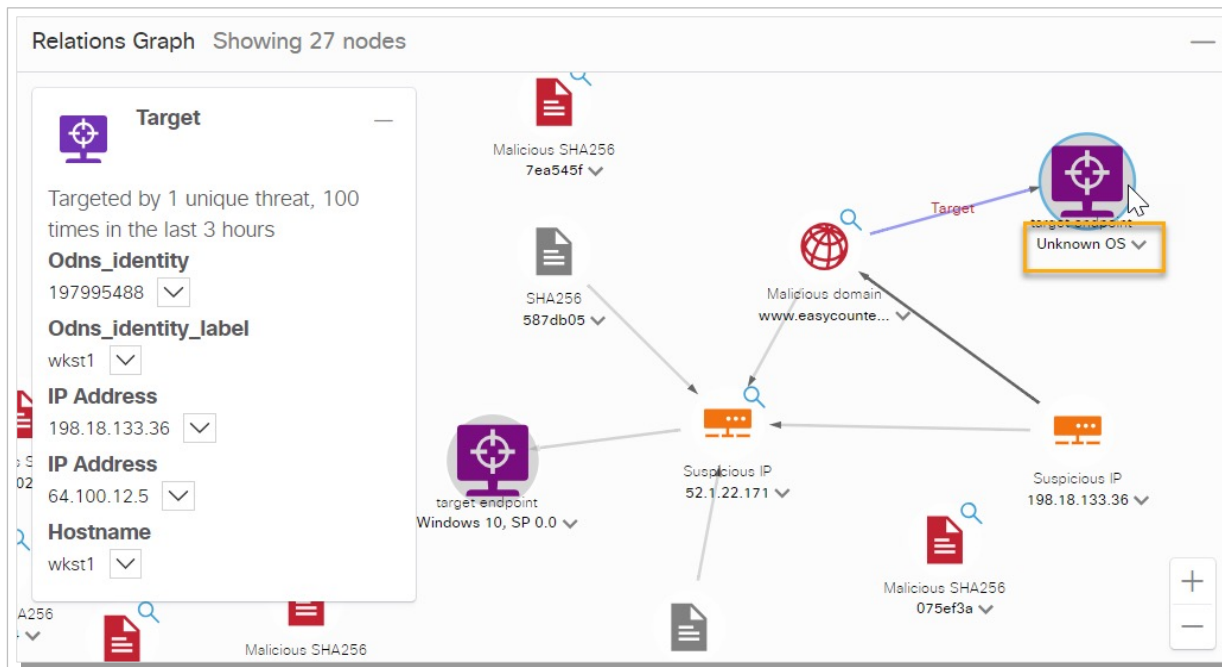
• Функции

- Агрегированная аналитика угроз
- Автоматическое обогащение
- Отслеживание инцидентов
- Бесшовная детализация
- Прямое восстановление



Расследуйте любой объект: Endpoint

Снижение сложности и времени, необходимого для поиска угроз



Используйте бесшовный рабочий процесс

FTD предоставляет события безопасности для реагирования на угрозы SecureX

The screenshot shows the Firepower Management Center (FMC) interface. The main content area displays a table titled "Events By Priority and Classification". The table has columns for Message, Priority, Classification, and Count. The events listed include various malware and trojan detections, such as "EXPLOIT-KIT Rig Exploit Kit URL outbound communication" and "MALWARE-CNC Win.Trojan.Cryptowall variant outbound connection".

Message	Priority	Classification	Count
EXPLOIT-KIT Rig Exploit Kit URL outbound communication [1:42898:3]	high	Attempted User Privilege Gain	1
MALWARE-CNC Win.Trojan.Cryptowall variant outbound connection [1:34318:4]	high	A Network Trojan was Detected	3
MALWARE-CNC Win.Trojan.Ukafin variant outbound connection attempt [1:42894:4]	high	A Network Trojan was Detected	1
MALWARE-CNC DNS assynikovs_bit_top_dns_query [1:42841:8]	high	A Network Trojan was Detected	1
MALWARE-CNC Win.Trojan.Kpot variant outbound connection [1:56125:1]	high	A Network Trojan was Detected	1
MALWARE-CNC Win.Trojan.Lov0D variant certificate exchange attempt [1:49552:1]	high	A Network Trojan was Detected	1
MALWARE-CNC Win.Trojan.TesaaCrypt server reply [1:38917:1]	low	Misc Activity	1

The screenshot shows the SecureX Threat Response interface. It displays investigation details for "Win.Trojan.Mkey-673586-0" with a "SIGNINGS TIME" graph and a "Relations Graph" showing 27 nodes. The interface includes various filters and search options.

- В облаке хранятся ограниченные данные
- FMC может отправлять события IPS в SecureX threat response
- Любой IP, домен, файловый хеш или IoC в FMC может быть запрошен в SecureX threat response, снижая сложность и время поиска угроз
- Непрерывный анализ с ретроспективой облегчает исправление и расширяет возможности расследований

Расширение FMC SecureX Ribbon

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects' (selected), 'AMP', and 'Intelligence'. The 'Objects' section is active, showing a 'Network' object management page. The page title is 'Network' and it includes an 'Add Network' dropdown and a search filter. A checkbox for 'Show Unused Objects' is present. A descriptive text states: 'A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.' Below this is a table with columns: Name, Value, Type, and Override. The table contains two entries: 'any' with value '0.0.0.0/0 ::/0' and type 'Group', and 'any-ipv4' with value '0.0.0.0/0' and type 'Network'. The bottom ribbon features a 'SecureX Ribbon' with icons for Casebook, Incidents, Orbital, and Settings. The 'Applications' section lists: SecureX (Launch), PM-NAM-AMP (Launch), Security Services Exchange (Launch), TG via SecureX-NAM Org (Launch), Threat Grid (Launch), and Threat Response (Launch). The 'My Account' section shows the user 'Kishore Chakraborty' with email 'kischakr+platform@cisco.com', role 'admin', and status 'IROH Testing', logged in with a Cisco Security Account.

Name	Value	Type	Override
any	0.0.0.0/0 ::/0	Group	
any-ipv4	0.0.0.0/0	Network	

SecureX threat response и интеграция CDO

Переход к threat response из CDO с помощью event viewer

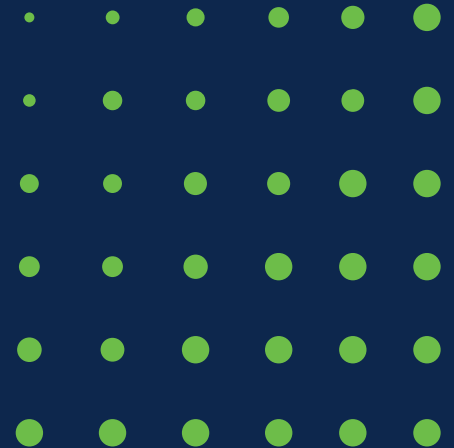
The screenshot displays the Cisco SecureX interface. On the left is a navigation sidebar with options like 'Hide Menu', 'Devices & Services', 'Policies', 'VPN', 'ASA Templates', 'Objects', 'Threat Events', 'Signature Overrides', 'Events & Monitoring', 'Change Log', 'Events', and 'Jobs'. The main area is titled 'Events' and shows a search bar and filters for 'Event Types' (Malware is selected) and 'Time Range' (After 05/05/2019 04:24:31 PM). A table of events is visible, with one event selected. An 'Investigate' window is open on the right, showing '8 new observables were found' and a list of observables including URLs and IP addresses. Below the observables, a table of metadata is shown.

Key	Value
deviceId	9944117f-64a9-4fab-8436-030ecc6aedb3
tenantId	cd082044-338f-451b-bd50-1a8a3d6d726b
timestamp	* 2019-05-05T21:00:09.000Z
traceld	8583d217-f5d0-4cc2-905f-b86596980ba

Дополнительная информация по SecureX

- Вебинар XDR. Как мы это себе представляем
 - Запись вебинара https://youtu.be/E_Sq4VdFKcg

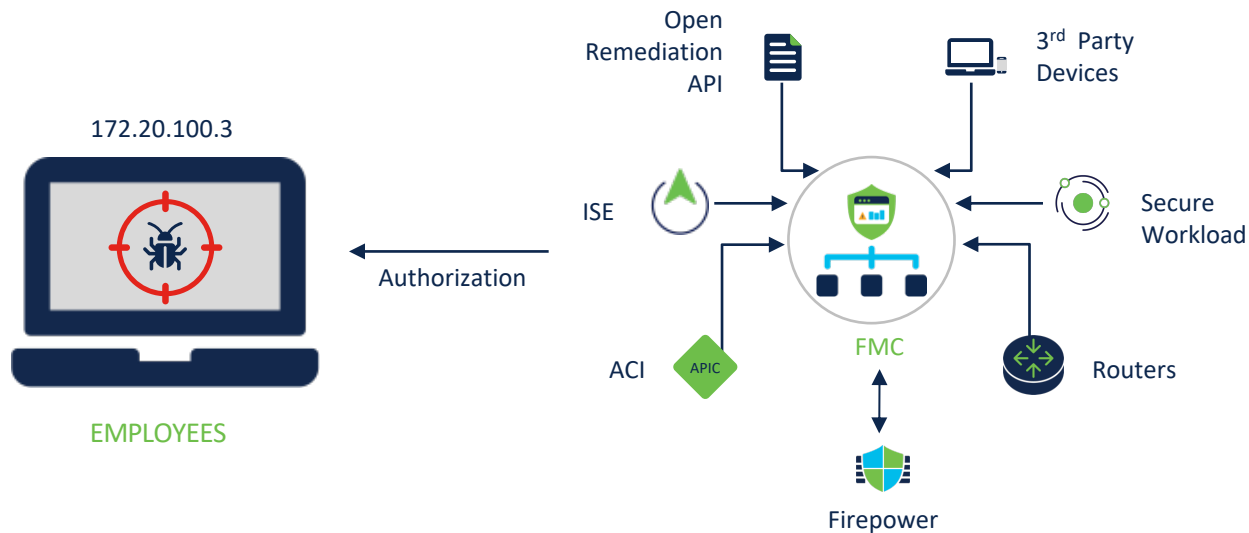
Additional Features



Cisco Rapid Threat Containment

Proven approach to reduce time and impact of threat

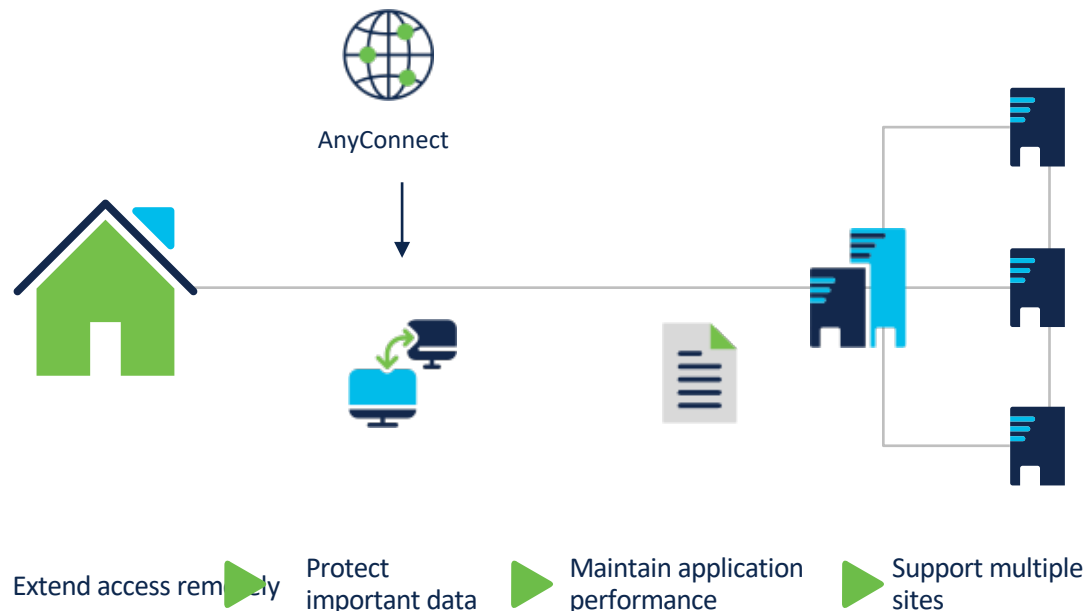
- Automatic network threat containment using the network as an enforcer
- Threat-centric network access determines network access based on IoCs
- Richer visibility from bidirectional data sharing with the network access



Remote Access VPN with Secure Access by Duo

Provide ubiquitous secure access from remote and roaming users

- Posture assessment
- Uses TLS, DTLS or IKEv2
- Easy wizard-based configuration
- Integration with LDAP and RADIUS
- Identity based security policies
- Enhanced security with 2 FA/MFA provided by Secure Access (Duo)



Protect Your Network Using AMP

Understand the motion and behavior of files through network and endpoint visibility.

Breadth and Control points



Email



Endpoints



Web



Network



IPS



Devices

Threat Visibility



Retrospective
Detection



Behavioral
IoCs



File
Trajectory



Threat
Hunting

Telemetry Stream



File and Network I/O



Process Information

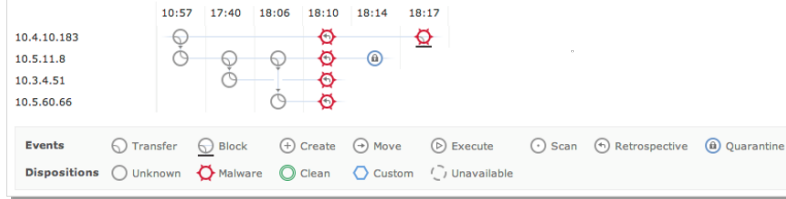


File Fingerprint and
Metadata



Talos and Malware Analytics
Intelligence

Trajectory



Application-Centric Infrastructure

Transparent policy-based security for both physical and virtual environments

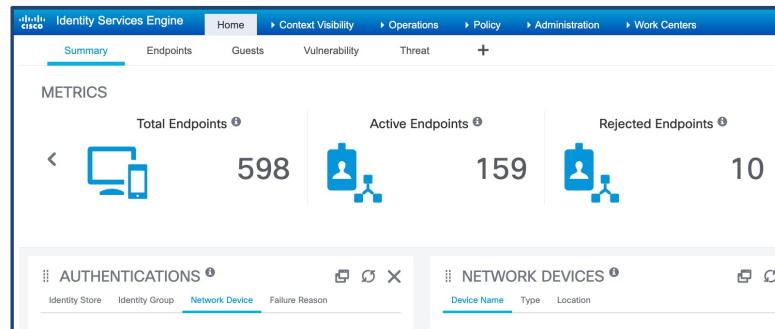
- Link security to software defined networking
- Create identity-based policy with Application Policy Infrastructure Controller (APIC)
- Segment physical and virtual endpoints based on group policies with detailed and flexible segmentation
- Release 7.0 – FMC Endpoint Update app 1.2 adds multi-site / multi-domain support

The screenshot shows the 'Configure Interface, PC, And VPC' configuration page in the Cisco FMC. The interface is divided into several sections:

- CONFIGURED SWITCH INTERFACES:** A table with columns for SWITCH PROFILE, INTERFACES, IF TYPE, and ENCAP. Below it is a 'VPC SWITCH PAIRS' section with columns for VPC DOMAIN ID, SWITCH 1, and SWITCH 2.
- Select Switches To Configure Interfaces:** Radio buttons for 'Quick' (selected) and 'Advanced'.
- Switches:** A dropdown menu showing '101'.
- Switch Profile Name:** A text field containing 'Switch101_Profile'.
- Interface Type:** Radio buttons for 'Individual' (selected), 'PC', and 'VPC'.
- Interfaces:** A text field with a red error icon and the message 'e.g. 1/17-18. Select interfaces by typing, e.g. 1/17-18.'.
- Interface Selector Name:** A text field with a red error icon and the message 'e.g. 1/17-18. Select interfaces by typing, e.g. 1/17-18.'.
- Link Level Policy:** A dropdown menu with 'select or type to pre-provision'.
- MCP Policy:** A dropdown menu with 'select or type to pre-provision'.
- STP Interface Policy:** A dropdown menu with 'select or type to pre-provision'.
- Storm Control Policy:** A dropdown menu with 'select or type to pre-provision'.
- Attached Device Type:** A dropdown menu with 'ESX Hosts'.
- Domain Name:** A text field with a red error icon and the message 'e.g. 15.20-30,200-300. Please use comma to separate VLANs.'.
- VLAN Range:** A text field with a red error icon and the message 'e.g. 15.20-30,200-300. Please use comma to separate VLANs.'.
- Interface Policy Group:** Radio buttons for 'Create One' (selected) and 'Choose One'.
- CDP Policy:** A dropdown menu with 'select or type to pre-provision'.
- LLDP Policy:** A dropdown menu with 'select or type to pre-provision'.
- Monitoring Policy:** A dropdown menu with 'select or type to pre-provision'.
- L2 Interface Policy:** A dropdown menu with 'select or type to pre-provision'.
- vCenter Login Name:** A text field.
- Password:** A text field.
- vCenter/vShield:** A section with a '+' icon and a table with columns for Name, IP, Type, and Stats Collection.
- Security Domains:** A dropdown menu.
- Confirm Password:** A text field.
- vSwitch Policy:** Checkboxes for 'MAC Pinning', 'CDP', and 'LLDP'.
- Buttons:** 'SAVE' and 'CANCEL' buttons at the bottom right.

Control Traffic Based on User Awareness

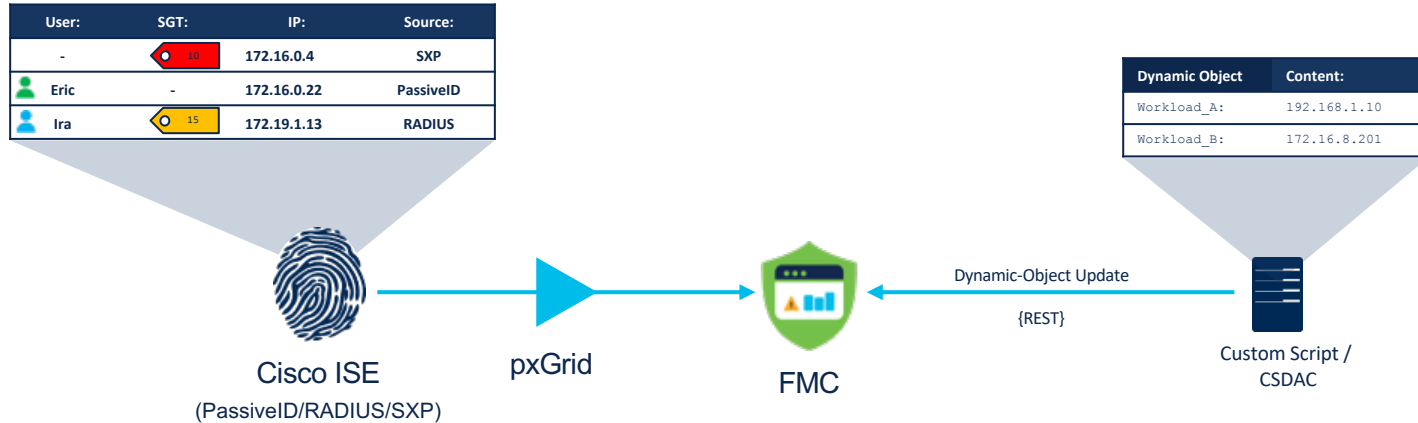
- Use Active Directory users and groups in policy configuration
- Use Cisco Identity Services Engine to provide identity
 - TrustSec Security Group Tag (SGT)
 - Device type (endpoint profiles) and location
 - Identity Mapping Propagation & device level filtering
- Examples
 - Block HR users from using personal iPads
 - Create rules for quarantined iPhones



The screenshot shows the Cisco Firepower Management Center (FMC) interface for editing a 'Branch Access Control Policy'. The table below lists the policy rules.

#	Name	Source SGT	Dest SGT	Action
>	Mandatory - Branch Access Control Policy (-)			
✓	Default - Branch Access Control Policy (1-2)			
1	block quarantined hosts	Quarantined_Systems	ANY	Block with reset

Identity Mapping Propagation



Simplify Security Management with TrustSec

Leverage the network and investment

- Scalable and agile segmentation technology in over 40 different Cisco product families
- Enables dynamic, role-based policy enforcement anywhere on your network
- Extend TrustSec policies over Firepower Threat Defense with SRC & DST SGT matching



Simplified Access Management

Manage policies using plain language and maintain compliance by regulating access based on business role



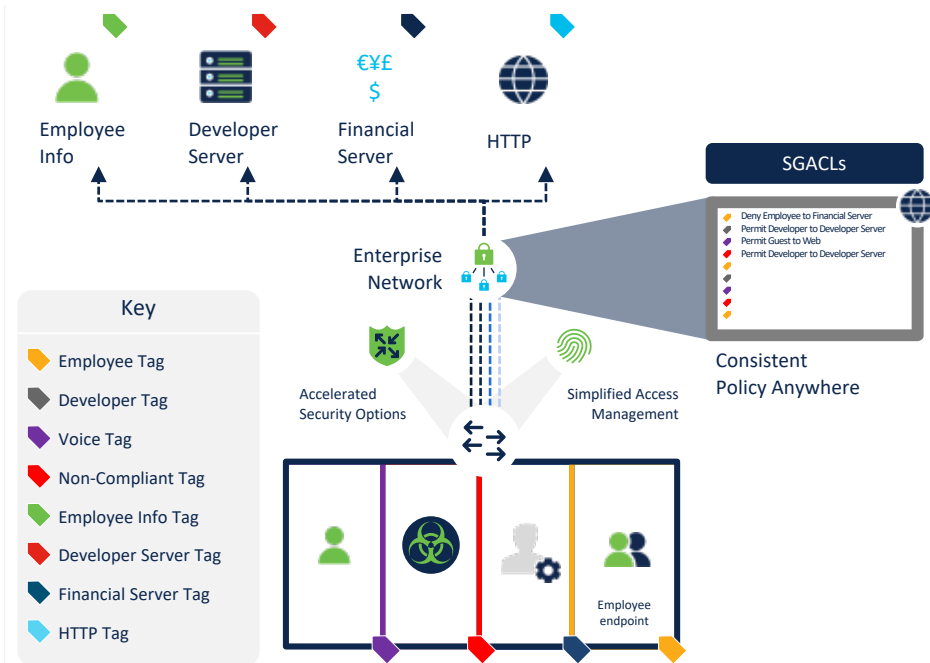
Rapid Security Administration

Speed-up adds, moves, and changes, simplifying firewall administration to speed up server onboarding



Consistent Policy Anywhere

Control all network segments centrally, regardless of whether devices are wired, wireless or on VPN



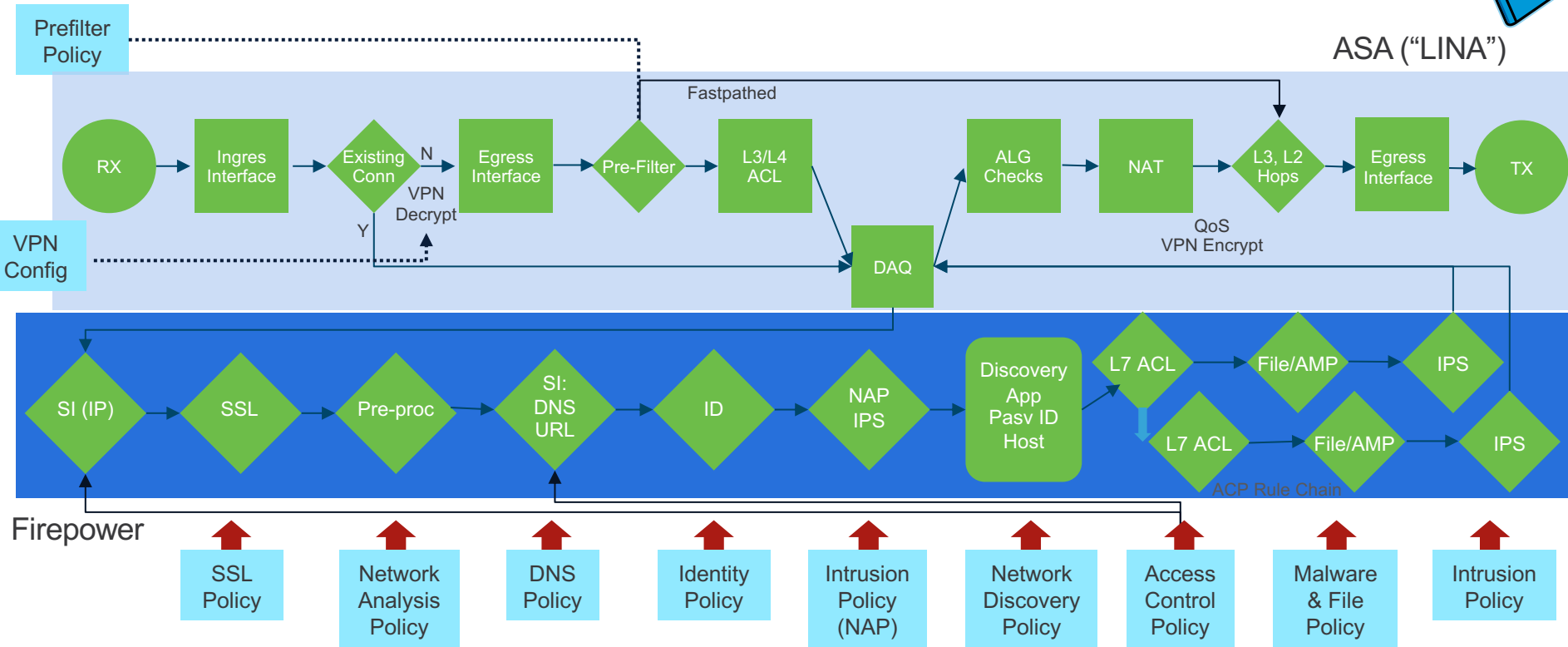


Отдельные заметки по работе с политиками

Пакеты и политики: как знать, где что происходит



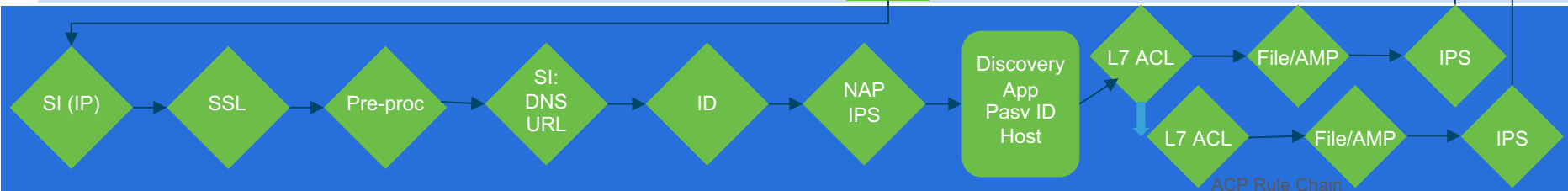
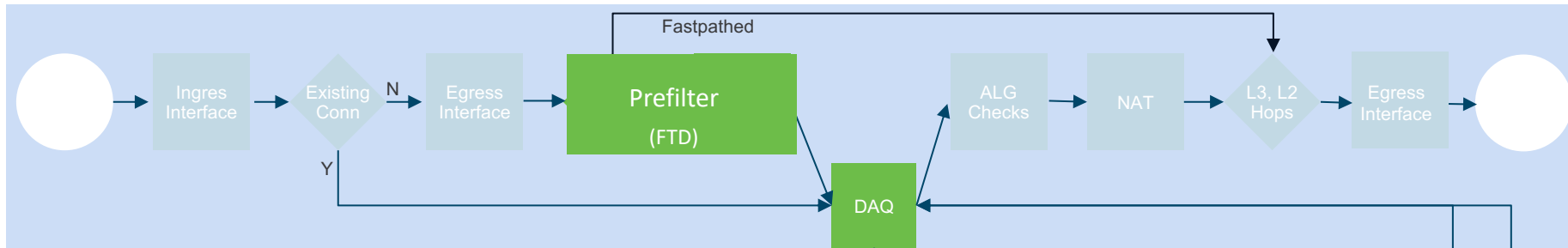
ASA ("LINA")



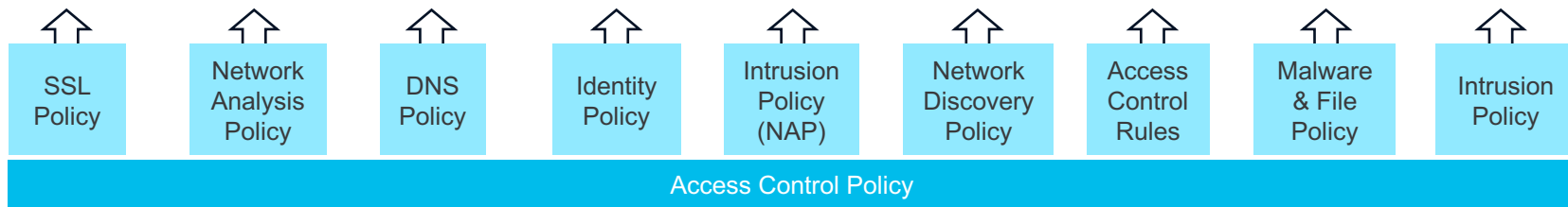
Пакеты и политики: как знать, где что происходит



ASA ("LINA")



Firepower



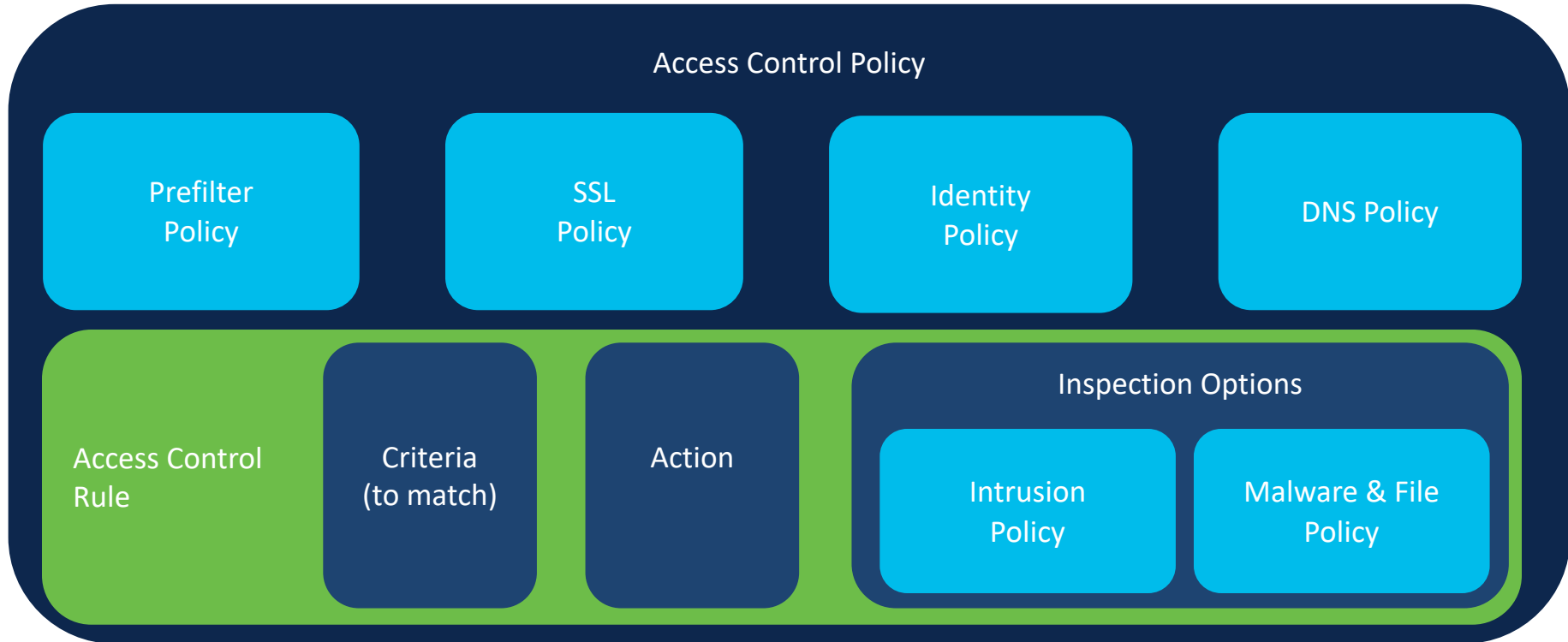
Политики Firepower

Как часто они модифицируются?

Часто	Периодически	Редко
Access Control Policy	Malware and File Policy	Network Discovery Policy
Intrusion Policy	DNS Policy	Network Analysis Policy
	SSL Policy	Correlation Policy
	Identity Policy	Health Policy
	Prefilter Policy	

Access Control Policy

Ключ, который все объединяет



Типы политик NGFW в FTD

Тип политики	Функция
Access Control	Определение, инспекция и журналирование трафика
Intrusion	Инспекция трафика на предмет нарушений (
Malware & File	Детектирование, инспекция и блокировка malware
SSL	Инспекция зашифрованного трафика
DNS	Контроль списков allow/block для доменов
Identity	Сбор идентификации пользователей
Prefilter	Высокоскоростное управление трафиком на L1 – L4 уровнях

URL политика: настраивается в рамках Access Control Rule

Prefilter Policy

Add Prefilter Rule

❶ Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.

Name: Database Backups Enabled

Action: **Analyze** (selected)

Insert: above rule 3

Time Range: [] +

VLAN Tags: [] Ports: []

Available Interface Objects: Search by name

- External
- Inline_Inside
- Inline_Outside
- Inside
- inside_ig
- Inside_zone** (selected)
- Internal
- Outside

Source Interface Objects (1): Inside_zone

Destination Interface Objects: any

FTD-Only Feature

Это первый набор правил, на основании которых инспектируется трафик

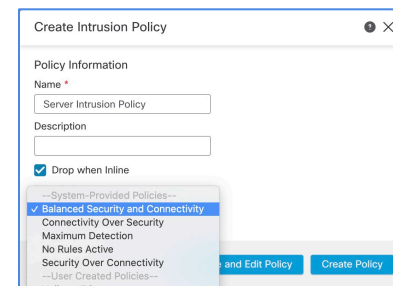
Fastpath это ускоренная обработка трафика. Analyze отправка трафика на доп. инспекцию.

Intrusion Policy

Intrusion Policy определяет, какие правила Snort rules используются для инспекции.

The image displays two overlapping screenshots from the Cisco Firepower Management Center. The background screenshot shows the 'Policy Information' configuration page for a policy named 'Server Intrusion Policy'. The page includes fields for Name, Description, and a checked 'Drop when Inline' option. It also shows the 'Base Policy' dropdown set to 'Balanced Security and Connectivity' and a status message indicating the base policy is up to date. A sidebar on the left lists navigation options like 'Policy Information', 'Rules', and 'Advanced Settings'. The foreground screenshot shows the 'Create Intrusion Policy' dialog box, which has a dropdown menu open for selecting a base policy. The selected option is 'Balanced Security and Connectivity'. Other options include 'Connectivity Over Security', 'Maximum Detection', 'No Rules Active', and 'Security Over Connectivity'. Buttons for 'and Edit Policy' and 'Create' are visible at the bottom of the dialog.

Базовые политики



Policy	CVSS Score	Vulnerability Age
Connectivity over Security	10	Текущий год плюс два предыдущих (2021, 2020, 2019)
Balanced Security and Connectivity	9+	Текущий год плюс два предыдущих Категории: Malware-CNC, Blacklist, SQL Injection, Exploit Kit
Security over Connectivity	8+	Текущий год + три предыдущих (2021, 2020, 2019, и 2018) Категории: Malware-CNC, Blacklist, SQL Injection, Exploit Kit, App-Detect
Maximum Detection	7.5+	2005 и позже Категории: Malware-CNC, Exploit Kit

Network Discovery Policy

- Определяет, что изучает Firepower.
- Используется для управления **Firepower Recommended Rules** в Intrusion Policy.

The screenshot shows the Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies' (selected), 'Devices', 'Objects', 'AMP', and 'Intelligence'. The right side of the navigation bar shows 'Deploy' with a green checkmark, a settings gear, a help icon, and the user 'admin'. Below the navigation bar, there are tabs for 'Networks', 'Users', and 'Advanced'. The 'Networks' tab is active. On the right side of the main content area, there are links for 'Custom Operating Systems' and 'Custom Topology', and a status message: 'Snort3 is not supported' with a green link 'Up to date on all targeted devices.' Below this, there is a '+ Add Rule' button. The main content area displays a table with the following data:

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action	
IPv4-Private-All-RFC1918	any	none	none	➔ Discover: Hosts, Users, Applications	✎ 🗑
IPv6-Link-Local IPv6_INSIDE_Network	any	none	none	➔ Discover: Hosts, Users, Applications	✎ 🗑
198.51.100.0/24	any	none	none	➔ Discover: Hosts, Users, Applications	✎ 🗑
2006:DB8:40C:EC01::/64	any	none	none	➔ Discover: Hosts, Users, Applications	✎ 🗑
203.0.113.0/24	any	none	none	➔ Discover: Hosts, Users, Applications	✎ 🗑

Intrusion Policy и Network Discovery Policy

Firepower Recommended Rules автоматически настраивают правила Snort для приложений, серверов и узлов в вашей сети.

The screenshot displays the Firepower Management Center interface. The top navigation bar includes the Cisco logo, the title "Firepower Management Center", and several menu items: Overview, Analysis, Policies (which is currently selected), Devices, Objects, AMP, and Intelligence. On the right side of the top bar, there are icons for Deploy, a settings gear, and a user profile labeled "admin".

The left sidebar contains a navigation menu with the following items: "Policy Information" (with a sub-item "Rules"), "Firepower Recommendations" (highlighted in blue), "Advanced Settings", and "Policy Layers".

The main content area is titled "Firepower Recommended Rules Configuration" and includes a "< Back" link. Below the title, there is a message: "No recommendations have been generated." Below this message is a checkbox labeled "Include all differences between recommendations and rule states in policy reports", which is currently unchecked.

Under the "Advanced Settings" section, there is a "Networks to Examine" section with a "Networks" label and an empty text input field. Below the input field is a note: "(Single IP address, CIDR block, or comma-separated list)".

Below the "Networks to Examine" section is the "Firepower Recommended Rules Configuration" section, which includes a "Recommendation Threshold (By Rule Overhead)" slider. The slider has four markers: "None", "Low", "Medium", and "High". The "Medium" marker is currently selected, indicated by a blue circle on a green bar.

Below the slider is a checkbox labeled "Accept Recommendations to Disable Rules", which is checked.

At the bottom right of the configuration area, there are two buttons: "Generate Recommendations" and "Generate and Use Recommendations".

At the bottom center of the page, there is a blue "How To" button.

Impact Flags

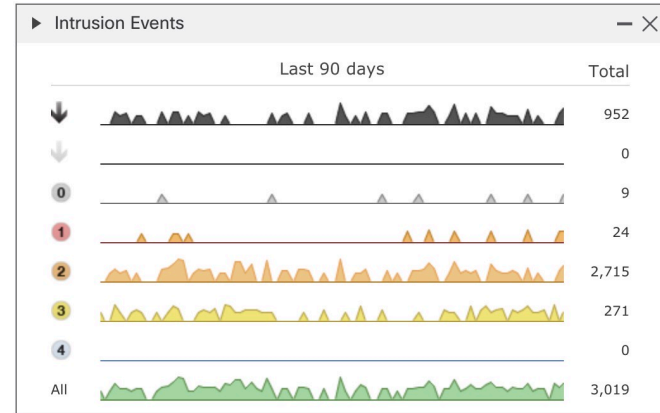
Мы настраивали Network Discovery Policy...

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' tab is active. Below the navigation bar, there are links for 'Custom Operating Systems' and 'Custom Topology', and a status message 'Short3 is not supported Up to date on all targeted devices.' The main content area shows a table of Network Discovery Policies.

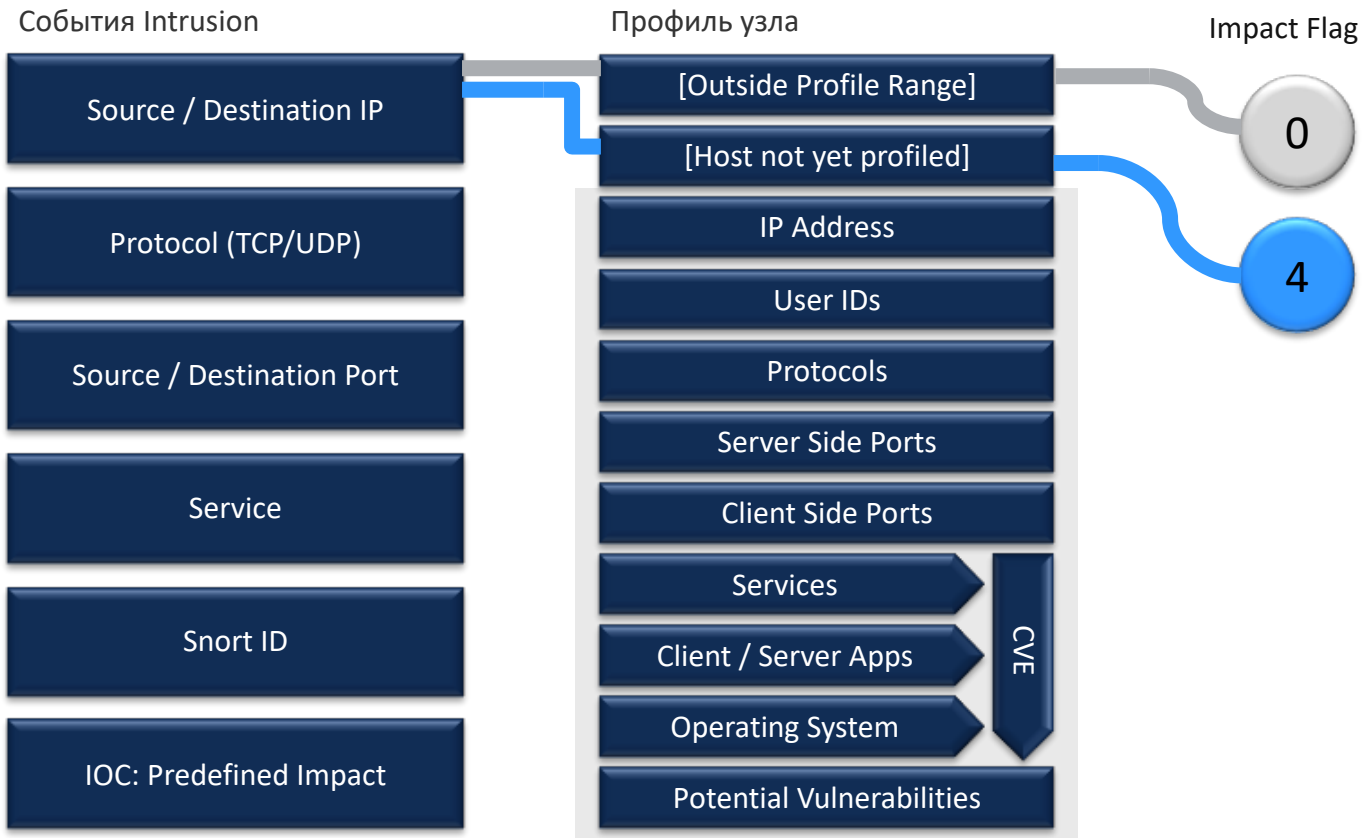
Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
IPv4-Private-All-RFC1918	any	none	none	Discover: Hosts, Users, Applications
IPv6-Link-Local IPv6_INSIDE_Network	any	none	none	Discover: Hosts, Users, Applications

Это включает Impact Flags для анализа.

Что это значит?



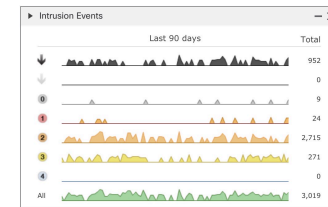
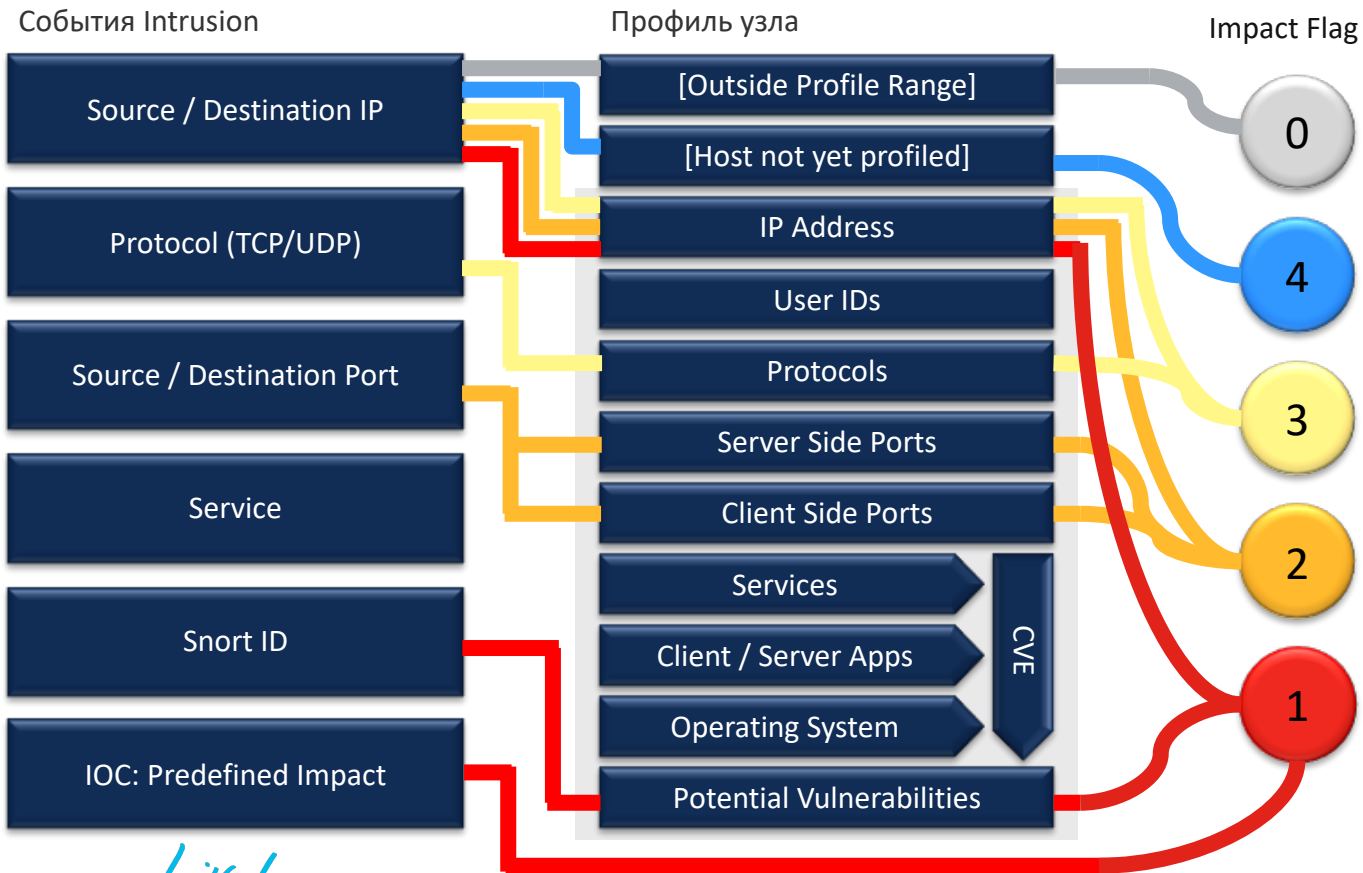
Понимание Impact Flags



Событие вне профилированных сетей

Ранее невидимый узел в профилированной сети

Понимание Impact Flags



- События вне профилированной сети
- Ранее невидимый узел в рамках профилированной сети
- Релевантный порт не открыт или не используется протокол
- Порт/протокол совпадает, но нет уязвимости
- Узел уязвим и показан в IOC

Snort правила



Firepower использует Snort правила для Intrusion Prevention.

Cisco обеспечивает регулярные обновления правил. Большинство клиентов обновляется автоматически.

Сторонние правила могут добавляться самостоятельно через Rule Editor (Objects -> Intrusion Rules -> Create Rule), или импортироваться.

The screenshot shows the Cisco FMC web interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects' (selected), 'AMP', 'Intelligence', 'Deploy', and 'admin'. The main content area is titled 'Intrusion Rules' and features a search bar and three buttons: 'Delete Local Rules', 'Import Rules', and 'Create Rule'. On the left, there is a 'Group Rules By' dropdown menu set to 'Category'. The main area displays a list of rule categories with their respective counts:

- Category (52383)
 - app-detect (165)
 - browser-chrome (57)
 - browser-firefox (289)
 - browser-ie (2602)
 - browser-other (92)
 - browser-plugins (2535)
 - browser-webkit (104)
 - content-replace (23)
 - decoder (153)

Access Control Policy

Для инспекции трафик должен попасть в Access Control Policy

The screenshot displays the Cisco Firepower Management Center interface for configuring an IPS Policy. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The current page is titled 'IPS Policy' and shows a 'You have unsaved changes' warning. Below the title, there are buttons for 'Show Warnings', 'Analyze Hit Counts', 'Save', and 'Cancel'. The page is divided into several tabs: 'Rules', 'Security Intelligence', 'HTTP Responses', 'Logging', and 'Advanced'. The 'Rules' tab is active, showing a table of rules. The table has columns for Name, Source Zones, Dest Zones, Source Networks, Dest Networks, VLAN Tags, Users, Applicati..., Source Ports, Dest Ports, URLs, Source SGT, Dest SGT, Action, and various icons. The table is currently empty, with a message 'There are no rules in this section. Add Rule or Add Category' displayed under the 'Mandatory - IPS Policy (-)' and 'Default - IPS Policy (-)' sections. At the bottom, there is a 'Default Action' dropdown menu set to 'Intrusion Prevention: Server Intru'.

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin

IPS Policy You have unsaved changes Show Warnings Analyze Hit Counts Save Cancel

Inheritance Settings | Policy Assignments (0)

Prefilter Policy: FTD Test PreFilter SSL Policy: None Identity Policy: None

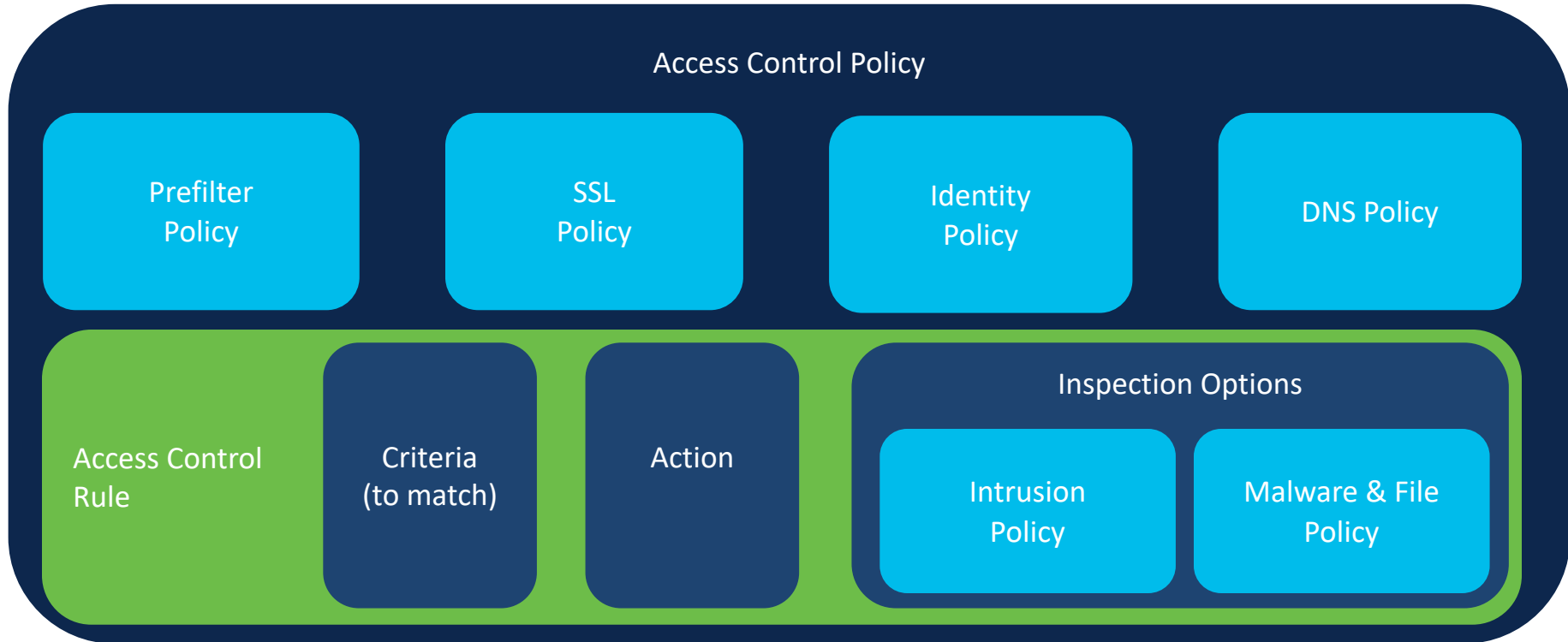
Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rules

	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action					
▼	Mandatory - IPS Policy (-)																		
There are no rules in this section. Add Rule or Add Category																			
▼	Default - IPS Policy (-)																		
There are no rules in this section. Add Rule or Add Category																			
Default Action															Intrusion Prevention: Server Intru				

Access Control Policy

Ключ, который все объединяет





Оптимизация правил Access Control

Управление политиками -- категории

- Все политики доступа содержат две категории - Mandatory и Default
- Для организации правил могут создаваться пользовательские категории
- После создания категории вы не можете ее переместить. Вы можете ее удалить, переименовать, перемещать в нее правила, удалять правила и т.д...

The screenshot displays a configuration table for network security policies. The table has columns for various attributes: #, Name, Source Zone, Destination Zone, Source Network, Destination Network, VLAN, Users, Applications, Sources, Destinations, URLs, IS... Att..., and A... (Action). Below the table, there are several policy categories listed with expand/collapse arrows and edit/delete icons. Two categories are highlighted with red boxes: 'Mandatory - Europe Data Center Policy (-)' and 'Default - Europe Data Center Policy (-)' (top), and 'Blanket Rules (-)', 'SAP Rules (-)', and 'Active Directory Rules (-)' (bottom). Green callout boxes with arrows point to these categories, containing the text 'Существует по умолчанию, не удаляется' and 'Пользовательские категории'. At the bottom, a 'Default Action' dropdown is set to 'Access Control: Block All Traffic'.

#	Name	So... Zo...	Dest Zo...	So... Ne...	Dest Ne...	VL...	Us...	Ap...	So...	De...	URLs	IS... Att...	A...	
▶	Mandatory - Europe Data Center Policy (-)													
▼	Default - Europe Data Center Policy (-)													
▶	Blanket Rules (-)													
▶	SAP Rules (-)													
▶	Active Directory Rules (-)													

Default Action: Access Control: Block All Traffic

Создание ваших Access Control Policy

Prefilter Policy (без AVC/IPS/AMP)

Layer 1-4 блокировка
и/или

Layer 1-4 работает с потоками, которые не нуждаются в инспекции (резервные копии, TCP/UDP Stream (Мультимедиа), зашифрованный трафик)

Access Control Policy

Layer 1-4 блок правила
и/или

Layer 1-4 правила для короткоживущих потоков (DNS)

Layer 5 блок правила (блокировка серверов с самоподписанными сертификатами)
и/или

Layer 7 URL блок правила (Блок URL категории Adult)

Layer 7 блок приложений (блок Office 365)

Определенные правила разрешающие L7 (разрешить HTTP с AMP политикой)


Generic layer 7 allow rules (e.g. allow all traffic with generic IPS policy)

- Prefilter правила самые быстрые
 - Любые правила L1-L4 и те, которые не требуют дополнительной инспекции
- Порядок правил в Access Control Policy не строго определен
 - Все еще правило первого срабатывания
 - Задача – обеспечить быструю блокировку с меньшим количеством переданных пакетов
 - Используйте Rule Conflict

Best Practices Docs

Cisco Firepower Threat Defense Policy Management Common Practices

NGFW Basic Policy Creation for Firepower



Basic Policy Creation for Firepower

First Published: May 25, 2018
Last Updated: January 30, 2019





Table of Contents

Document Scope:	
Traffic Flow Overview:	
Security Intelligence:	
Access Control Policy:	
Building an access control policy:.....	4
Adding Rules to Access Control Policy:.....	4

NGFW Policy Order of Operations



NGFW Policy Order of Operations

First Published: May 22, 2018
Last Updated: May 22, 2018

Table of Contents

Policy Order of Operations.....	2
Introduction: Purpose.....	2
Policy Firewall: Funnel Approach (Threat tornado)	2
Common Misconceptions:	3
Firewall Funnel Model:	3
Order of Operations Best Practices.....	4
Path of the packet and policy checkpoints:	6
Best practices for policy ordering:	7
Policy Inheritance:	7

Policy Management Table of Contents:

1. Access Policies

- Rationalizing
- Connection Logging
- Defining Flows
- Blocking Bad Traffic
- Determining What Needs Encryption

2. IPS Policies

- Testing Policies
- Leveraging Firepower Recommendations
- Deploying Strict Controls
- Leverage X-Forwarding
- Fine-Tuning Rules

3. Malware Policies

4. SSL Policies

5. Identity Policies

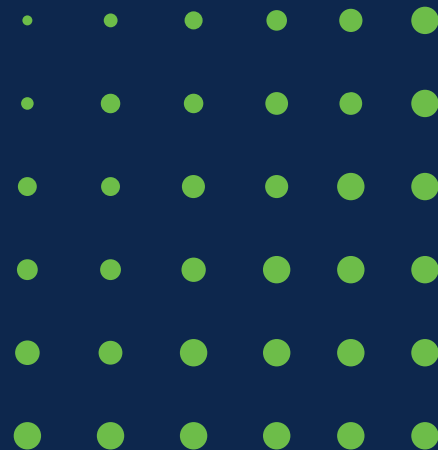
6. Network Analysis Policies

https://explore.cisco.com/ngfw_ftd_common-practices/ngfw-ftd-policy-mgmt

https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/Self-Help/Basic_Policy_Creation_on_Cisco_Firepower_Devices.pdf

https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/Self-Help/NGFW_Policy_Order_of_Operations.pdf

Новые и рекомендуемые релизы ПО



Рекомендуемый образ FTD

Downloads Home / Security / Firewalls / Firewall Management / Firepower Management Center Virtual Appliance / Firepower Management Center Software- 6.6.5

[Expand All](#) [Collapse All](#)
Suggested Release
6.6.5
Latest Release
6.6.5.1
6.4.0.13
7.1.0
7.0.1
All Release
7.1
7.0
6.7
6.6

Firepower Management Center Virtual Appliance

Release 6.6.5
[My Notifications](#)

Related Links and Documentation
[Release Notes for 6.6.5](#)
[Documentation Roadmap](#)

File Information	Release Date	Size	
Firepower Management Center upgrade Cisco_Firepower_Mgmt_Center_Upgrade-6.6.5-81.sh.REL.tar Advisories	03-Aug-2021	2023.15 MB	↓ 🛒 📄
FMCv300: VMware install pack Cisco_Firepower_Mgmt_Center_Virtual_VMware-6.6.5-81.tar.gz Advisories	03-Aug-2021	2271.81 MB	↓ 🛒 📄
FMCv: KVM install pack Cisco_Firepower_Mgmt_Center_Virtual_KVM-6.6.5-81.tar.gz Advisories	03-Aug-2021	2214.19 MB	↓ 🛒 📄
FMCv: VMware install pack Cisco_Firepower_Mgmt_Center_Virtual_VMware-6.6.5-81.tar.gz Advisories	03-Aug-2021	2221.27 MB	↓ 🛒 📄

Рекомендуемый образ на 08 декабря 2021 года

Firewall Threat Defense 7.0

Важные изменения в extra long-term релизе – переход на 7.0 2021

Scalable Eventing and Logging

Просмотр событий в реальном времени, масштабируемое хранение событий и логирование на площадке с использованием SAL

Динамические объекты для быстрых изменений

Политика на основе атрибутов добавляет динамические сетевые объекты в политику AC

Проще в использовании

Унифицированные метрики состояния (через SNMP), Дэшборд состояния для FMC, Управление изменениями (откат, просмотр изменений, улучшенный аудит, поиск и фильтрация)

Улучшение обнаружения угроз

Улучшено обнаружение угроз с важным архитектурным изменением: появление Snort 3 с FMC

Публичные облака и виртуализация

Поддержка динамических объектов для нативных облачных политик и создание быстрых Instance (с Secure Threat Services)

Преимущества бизнеса

Отладка и отслеживание текущих, исторических событий в едином UI

Изменение динамических объектов в политиках быстро без необходимости deploy

Сильно улучшенный пользовательский опыт, снижение операционной сложности и расходов

Заказчик получает лучшее обнаружение с меньшей затратой ресурсов

Поддержка гибридных облаков для любого развертывания заказчика

Много других улучшений в ...

- Remote access и site-to-site VPN
- Интеграция Secure-X
- FMC API для оркестрации и миграции
- APIC FMC App Multi domain
- Работа PAT в кластере
- Поддержка множества доменов для идентификации пользователя

Что нового? – FTD



NEW

FTD Релиз 7.0



- Snort 3
- Улучшения производительности
- Common Criteria
- Улучшения в Low touch provisioning
- Улучшения в процедурах обновления и инсталляции
- FMC
 - VPN – DAP, SAML, локальные пользователи, множественные сертификаты
 - Удобство пользования – откат конфигураций, унифицированный просмотр событий
 - Динамические объекты
 - Фильтры устройств по ассоциациям идентификации
- Cisco Secure Dynamic Attributes Connector (CSDAC)

Программные функции

- Фильтрация трафика по репутации DNS
- Резервный VTI для маршрутизируемого site-to-site VPN
- Улучшения в мониторинге состояния

Основные улучшения в релизе 7.0



Защита от угроз

- Snort 3 – Настройка в FMC
- Новые парсеры протоколов
- HTTP/2 Инспекция
- Улучшения производительности
- Lightweight Security Package (LSP)



Управление VPN




- FMC управление – DAP, SAML, локальная аутентификация, множественные сертификаты
- Поддержка Diffie-Hellman group 31
- IPsec настройки lifetime для site-to-site VPN
- резервный virtual tunnel interface (VTI) для маршрутизируемого site-to-site VPN + увеличение количества VTI до 1024



Улучшения в идентификации

- Динамические объекты + CSDAC
- Кросс-доменное доверие для AD доменов
- Фильтры соответствий идентификации
- Политики на основании атрибутов

Основные изменения релиза 7.1

 <p>Snort 3</p>	<ul style="list-style-type: none">• Elephant flow visibility• Encrypted Visibility Engine• Intrusion Rule Recommendations• Additional rule actions
 <p>VPN Management</p>	<ul style="list-style-type: none">• Unique local tunnel ID for IKEv2• Anyconnect native browser support• RA VPN multiple trust points in SAML IDP• Copy RA VPN access config on FMC• Site to site VPN enhancements
 <p>Public Cloud</p>	<ul style="list-style-type: none">• Additional instance type support in AWS, Azure• FMCv HA and FMCv300 in AWS and OCI• Geneve AWS proxy support• Automated FTDv horizontal scaling in OCI• AWS CloudWatch health monitoring integration

Encrypted Visibility Engine

- Экспериментальная функция в 7.1
- Использует машинное обучение для определения приложения, которое генерирует пакет Client Hello
- Идентифицирует известные процессы/браузеры
- Идентификация malware на основании отпечатков Secure Malware Analytics



Policy Based Routing настройка - пример

- Несколько PBR на основании разных интерфейсов.

Policy Based Routing

Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly

Configure Interface Priority Add

Ingress Interfaces	Match Criteria	Egress Interfaces	Actions
inside1 inside2	If traffic matches the Access List DIA_Cloud_Applications_ACL	Send and load balance it through #0 outside_ISP_1 #0 outside_ISP_2 If above link fails, Send through #1 outside_ISP_3	
	If traffic matches the Access List YoutubeTraffic	Send through #0 outside_ISP_1 If above link fails, Send through #0 outside_ISP_2	
lab_intf	If traffic matches the Access List LabTestNetwork	Send through 41.77.36.26	

Список входящих интерфейсов

Правила с приложениями

Список сбалансированных исходящих интерфейсов

Список интерфейсов по порядку.

Упрощенное развертывание для региональных офисов

Secure Elastic Connectivity

- Настройка Route-based VPN VTI туннелей между филиалами на HQ.
- IPv6 VTI
- BGPv6 over VTI (7.1)

Увеличение полосы пропускания (7.1)

- ECMP поддержка для балансировки между ISPs
- ECMP поддержка для VTI

Упрощенное управление

- Low Touch Provisioning
- Data Interface Management
- Auto Config Rollback (7.1)
- FDM Driven Onboarding (7.1)

Высокая доступность с
около нулевым
временем
восстановления

- Настройка Dual ISP configuration
- Active-Standby Backup VTI туннели с мониторингом SLA

Прямой доступ в Internet и для гостевого трафика (7.1)

- Детектор SAAS приложений (Первый пакет AVC)
- Policy Based Routing с приложением в качестве критерия

Обзор функционала



How it Works

- FTD API (и FDM) могут использоваться для настройки FMC
 - Использует доступ к интерфейсу данных
 - Использует доступ к интерфейсу управления
- Какой менеджер: FDM и FTD REST API
- Ограничения
 - Не поддерживаются FTD в HA режиме
 - Не поддерживаются FTD с Universal PLR
 - FTD с FlexConfig не поддерживается поскольку FMC не синхронизирует конфигурацию
 - FTD может управляться только одним менеджером, FMC или FDM

Device > System Settings > Management Center

Firepower Device Manager

Monitoring Policies Objects Device: fdm124

Model Cisco Firepower Threat Defense for VMwa... Software 7.1.0-1653 VDB 338.0 Intrusion Rule Update 20210414-1949 Cloud Services Not Registered | Register High Availability Not Configured

Inside Network

ISPWAN/Gateway

Internet

DNS Server

NTP Server

Smart License

Interfaces

Connected

Enabled 3 of 9

View All Interfaces

Routing

There are no static routes yet

View Configuration

Updates

Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds

View Configuration

System Settings

Management Access

Logging Settings

Cloud Services

HTTP Proxy

Web Analytics

Reboot/Shutdown

Management Center

URL Filtering Preferences

See more

Smart License

Evaluation expires in 90 days

Tier: FTDv30 - Tiered (8 core / 16 GB)

View Configuration

Backup and Restore

View Configuration

Troubleshoot

No files created yet

REQUEST FILE TO BE CREATED

See more

Site-to-Site VPN

There are no connections yet

View Configuration

Remote Access VPN

Requires RA VPN license

No connections | 1 Group Policy

Configure

Advanced Configuration

Includes: FlexConfig, Smart CLI

View Configuration

Device Administration

Audit Events, Deployment History, Download Configuration

View Configuration

Management Center может запускаться:

- После Easy Setup Wizard
- Или пропустить Easy Setup Wizard
- Или на FTD которое уже управляется FDM

System Settings

Management Access

Logging Settings

DHCP Server / Relay

Cloud Services

HTTP Proxy

DNS Service

DNS Server

Web Analytics

Reboot/Shutdown

Management Center

URL Filtering Preferences

See more

Готовы начать?



Обновите свой Firewall сегодня!

Подпишитесь на бесплатный trial:

[Тестирование и Health Check](#)

[Firepower](#)

[Тестирование Cisco Defense](#)

[Orchestrator](#)

Спасибо

