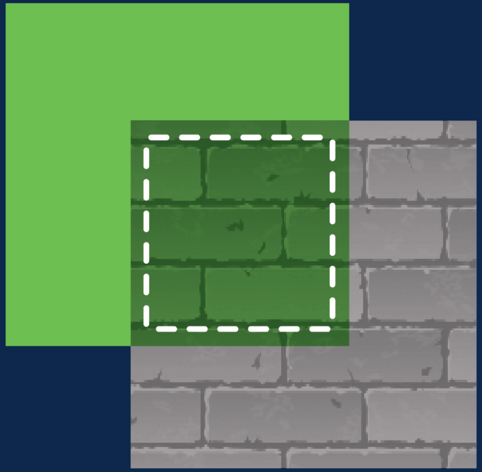
CISCO SECURE

The bridge to possible

Cisco Secure Firewall

Новинки, информация и практика



Павел Родионов
Архитектор по кибербезопасности
GREM, CISSP, CCIE 11155

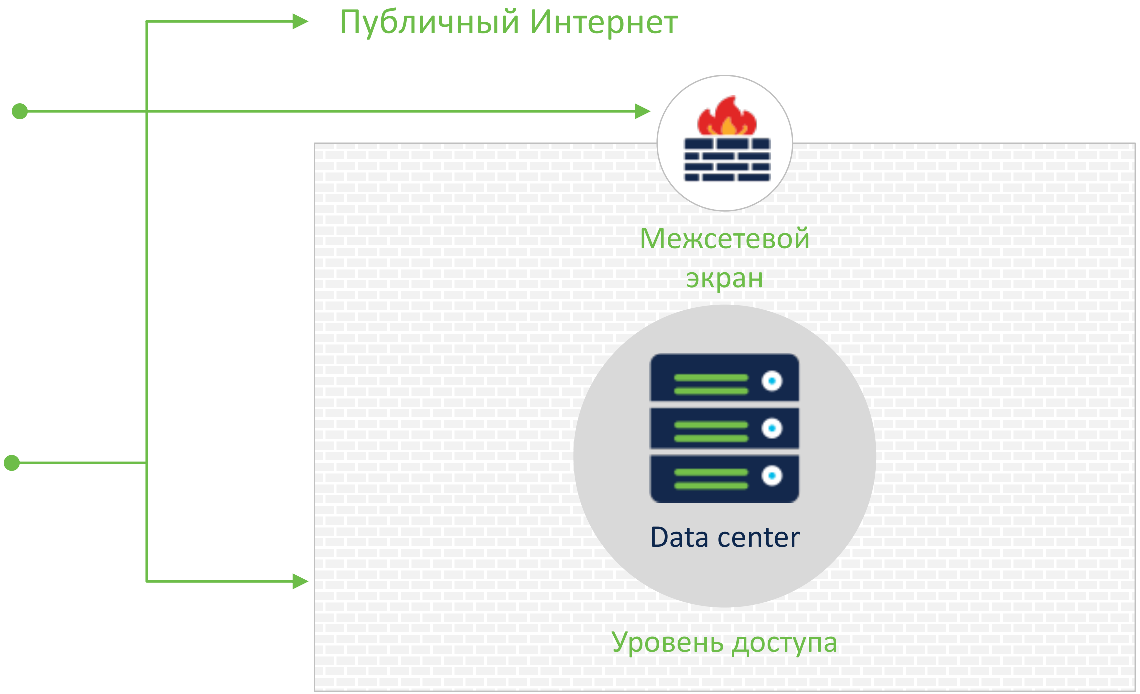
Программа

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

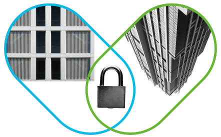
Филиалы

Облако/ Виртуализация

Продвинутый IPS

Удаленный VPN доступ

Почему Cisco Secure Firewall?

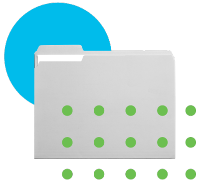


Средства безопасности мирового уровня

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

Целостная политика и осведомленность

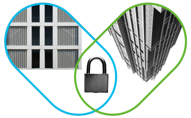
Понятная политика безопасности и управление устройствами во всей сети с реализацией ключевых задач безопасности.



Интегрированное портфолио безопасности

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

Всестороннее портфолио Cisco по кибербезопасности

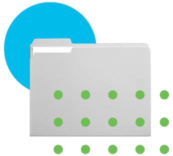


Средства безопасности мирового уровня

- Secure Firewall Threat Defense
- Secure Firewall ASA
- Talos

Целостная политика и осведомленность

- Secure Firewall Management Center
- Secure Firewall Device Manager
- Cisco Defense Orchestrator
- SecureX threat response
- Secure Network Analytics



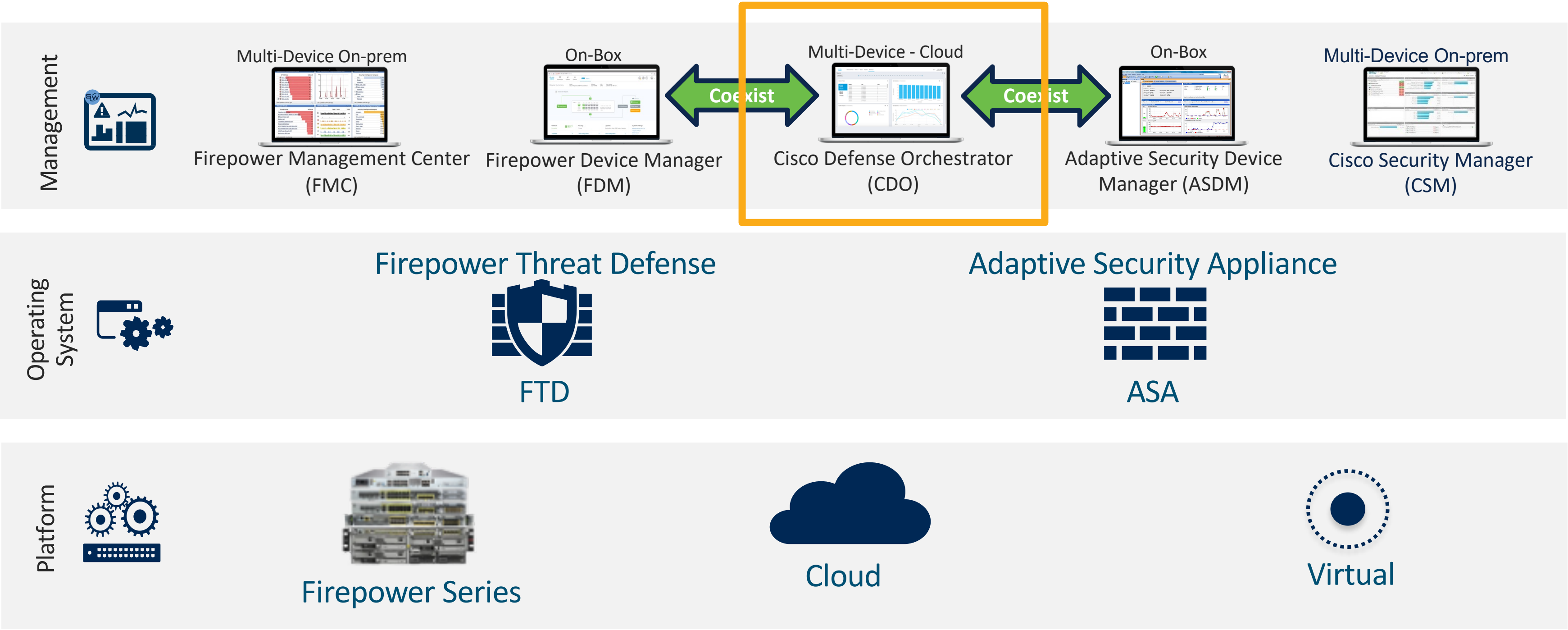
Интегрированное портфолио безопасности

- 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, Clientess, 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..

** CSM does not support AnyConnect 4.6*

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

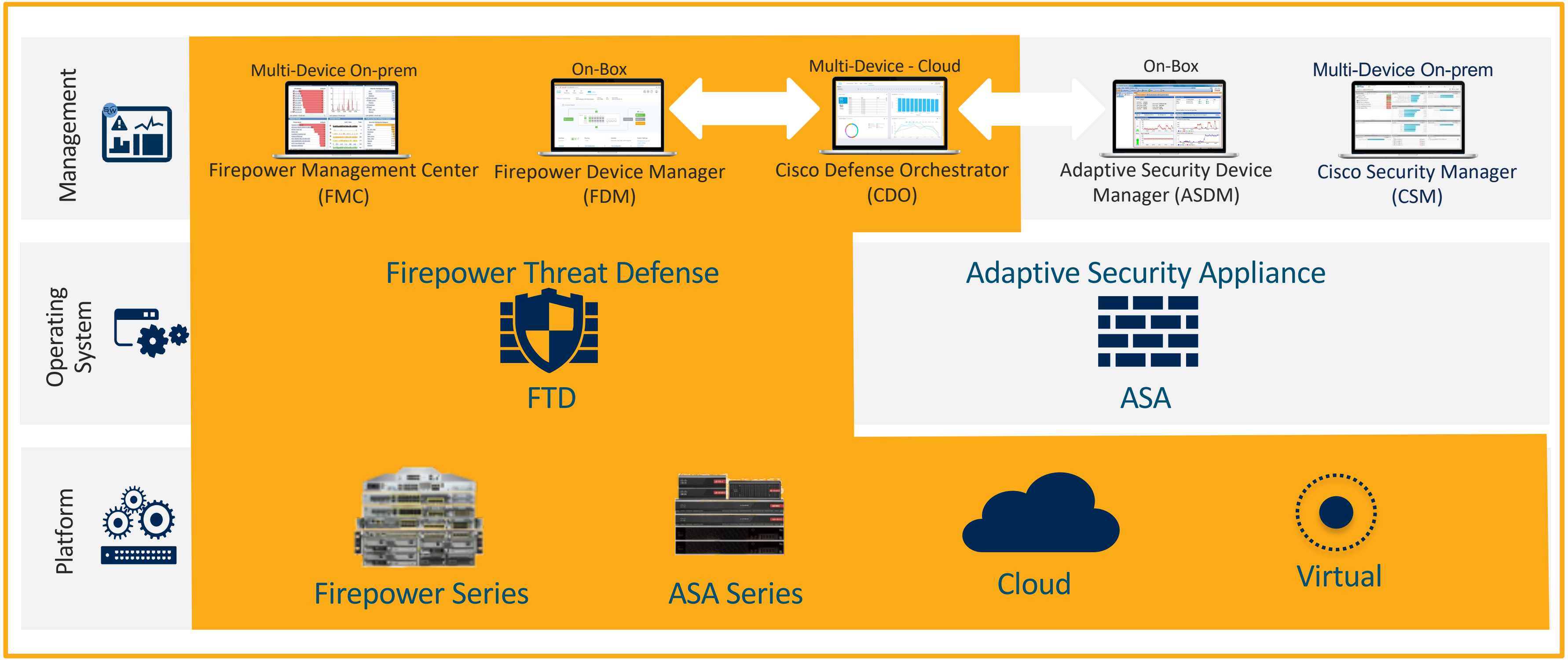
- Использование API's для автоматизации и оркестрации функций NGFW
- Интеграция с AMP EP, ISE, CTR, Tetration, SIEM и т.д.
- Использование API's для потребления информации и threat feeds
- Платформа для применения контролей

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

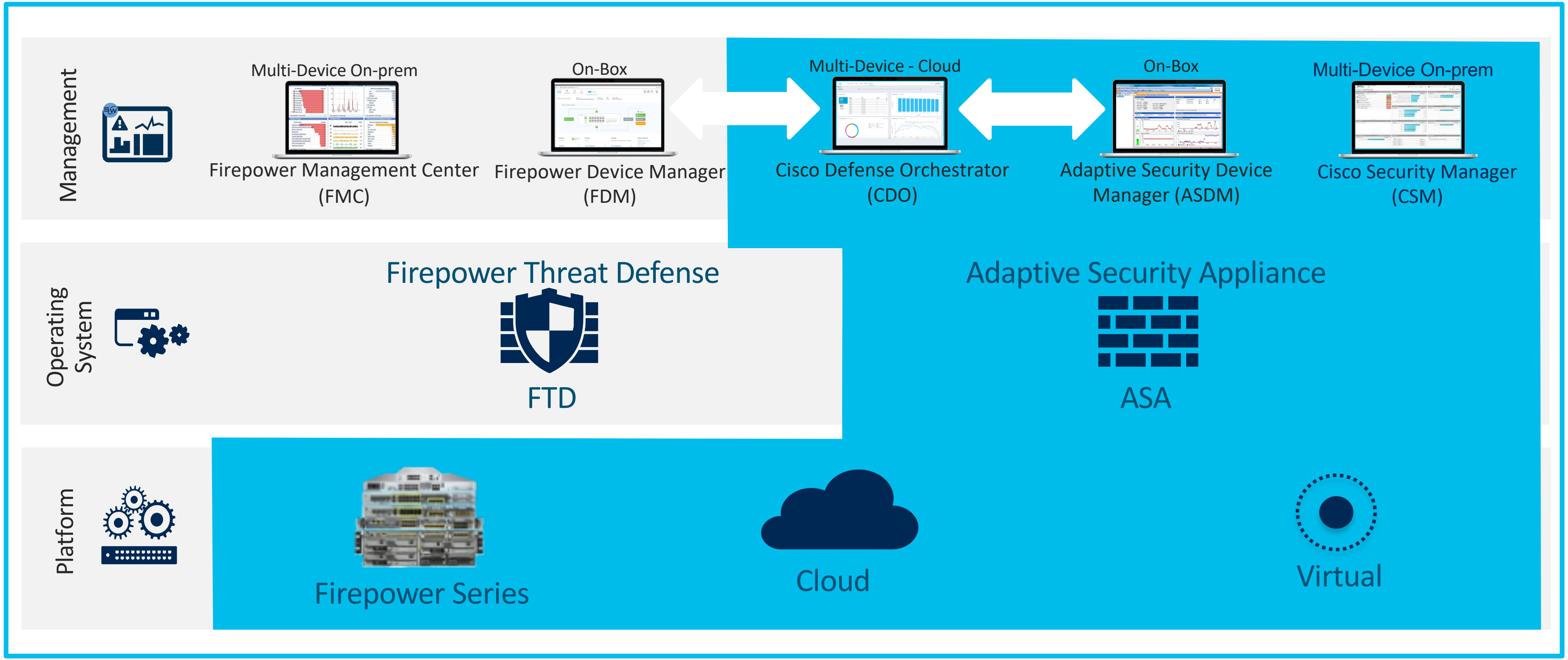
FTD : Опции платформы и управления

Platforms, Operating Systems and Management options



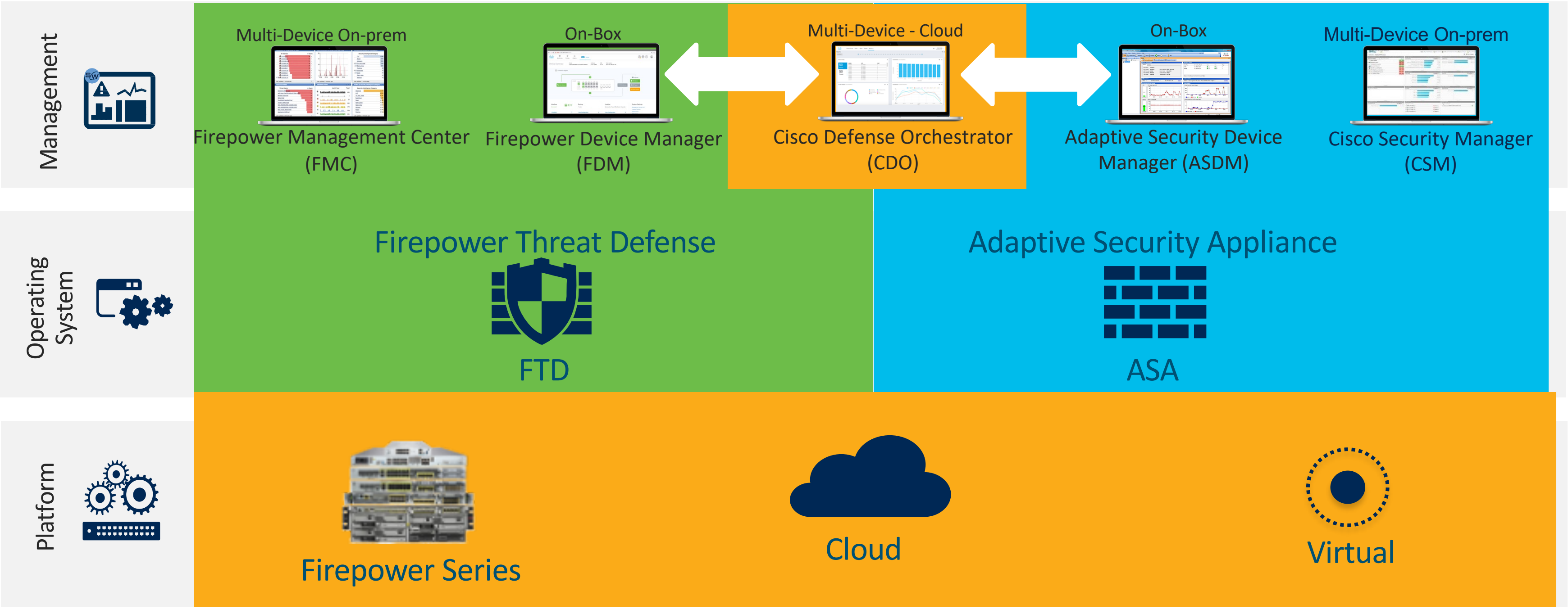
ASA: Опции платформы и управления

Platforms, Operating Systems and Management options



Собираем все вместе

Platforms, Operating Systems and Management options



Устройства и облачные платформы Firepower

Private Cloud*

vmware ESXi KVM

Public Cloud*

aws Azure

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

Six node cluster:
Up to 254 Gbps AVC
Up to 226 Gbps AVC+IPS

One Module:
55-70 Gbps AVC
53-68 Gbps AVC+IPS

Six node (2 chassis) cluster:
Up to 380 Gbps AVC
Up to 370 Gbps AVC+IPS

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

SOHO/ SMB	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

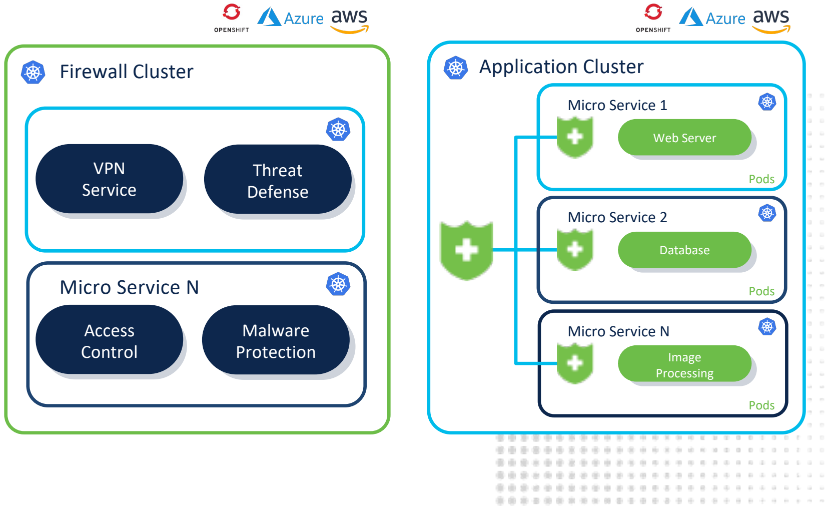
- Azure Application Insights для метрик FTD
- FMCv/FTDv ASAv в Google Cloud Platform и Oracle Cloud Infrastructure

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

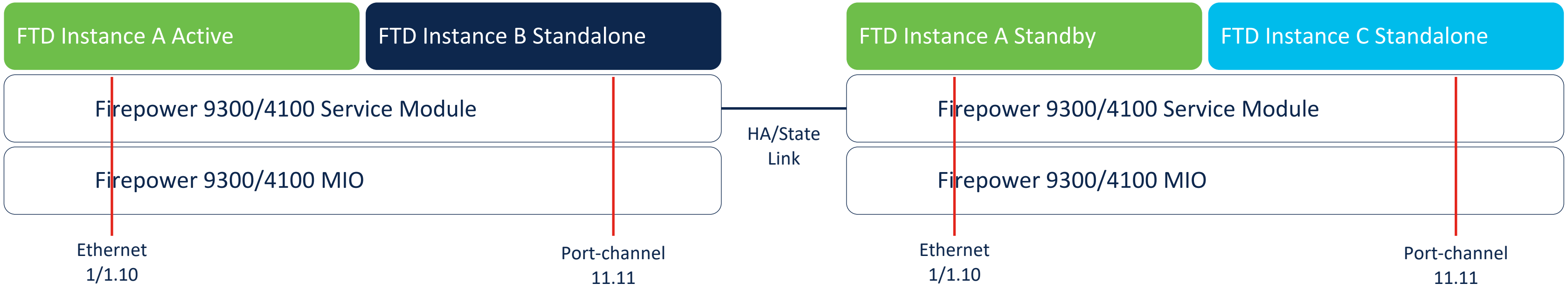
* FCS in May 2021 in AWS EKS, followed by Azure and Openshift this Fall

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

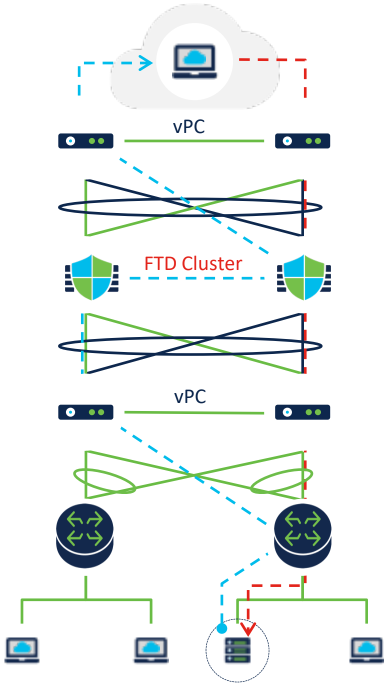
NEW



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 ассиметричный трафик

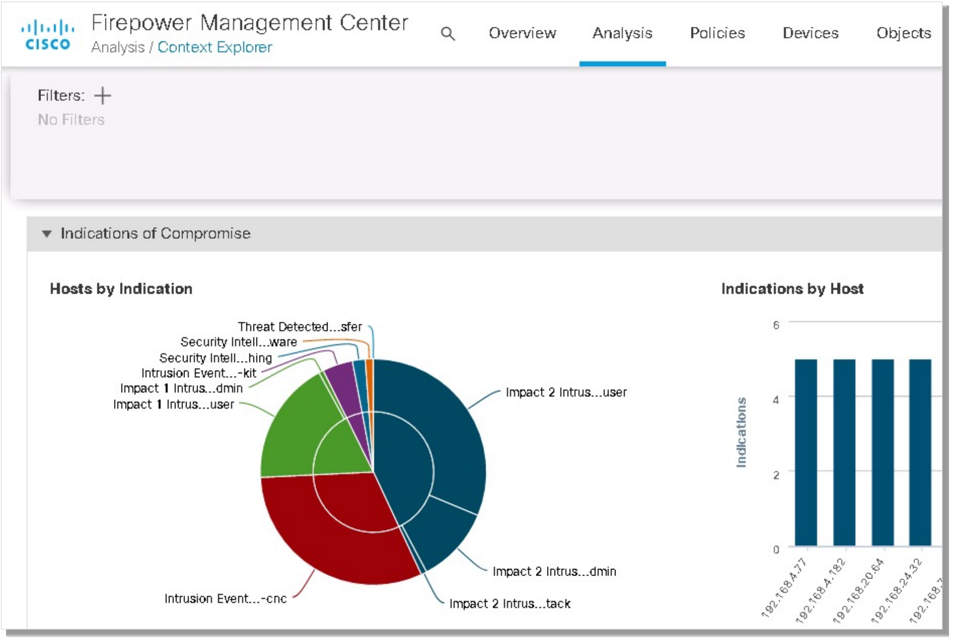


Secure Firewall Threat Defense

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	Динамические объекты для быстрых изменений	Проще в использовании	Улучшение обнаружения угроз	Публичные облака и виртуализация
Просмотр событий в реальном времени, масштабируемое хранение событий и логирование на площадке с использованием SAL	Политика на основе атрибутов добавляет динамические сетевые объекты в политику AC	Унифицированные метрики состояния (через SNMP), Дэшборд состояния для FMC, Управление изменениями (откат, просмотр изменений, улучшенный аудит, поиск и фильтрация)	Улучшено обнаружение угроз с важным архитектурным изменением: появление Snort 3 с FMC	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 пользовательских опыт, снижение операционной сложности и расходов	Заказчик получает лучшее обнаружение с меньшей затратой ресурсов	Поддержка гибридных облаков для любого развертывания заказчика

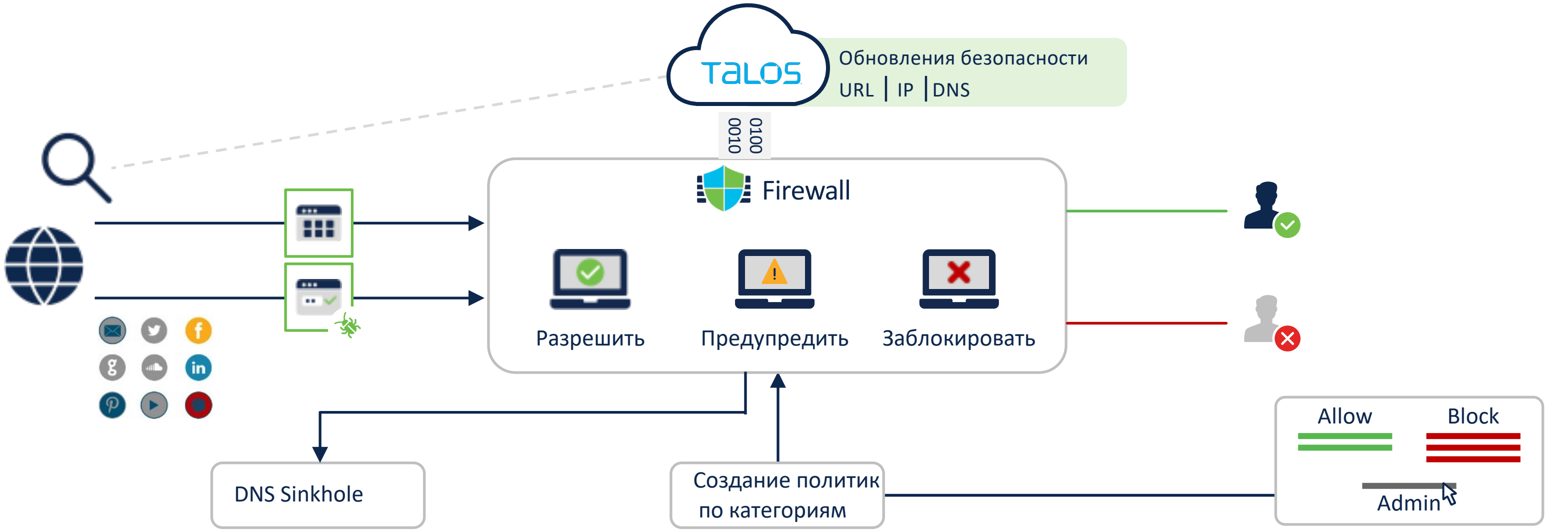
Много других улучшений в …

- 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

cisco SECURE

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

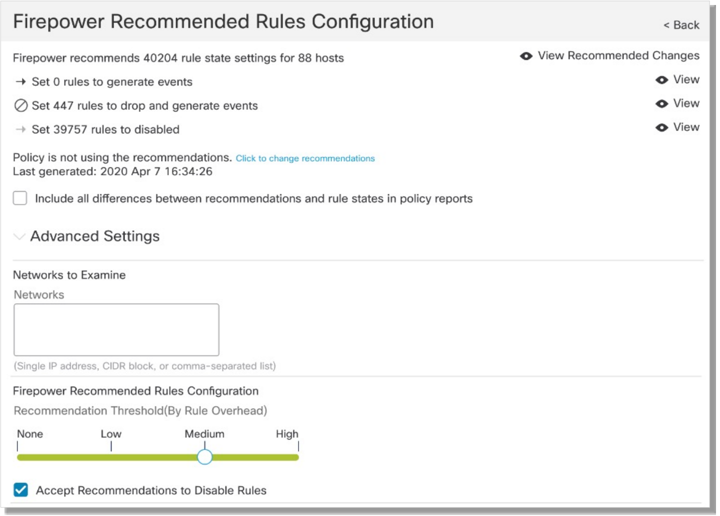
Обеспечивается Snort 3 – Лучшим IPS с открытым кодом

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	Атакуемый 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.



Snort 2 vs. Snort 3

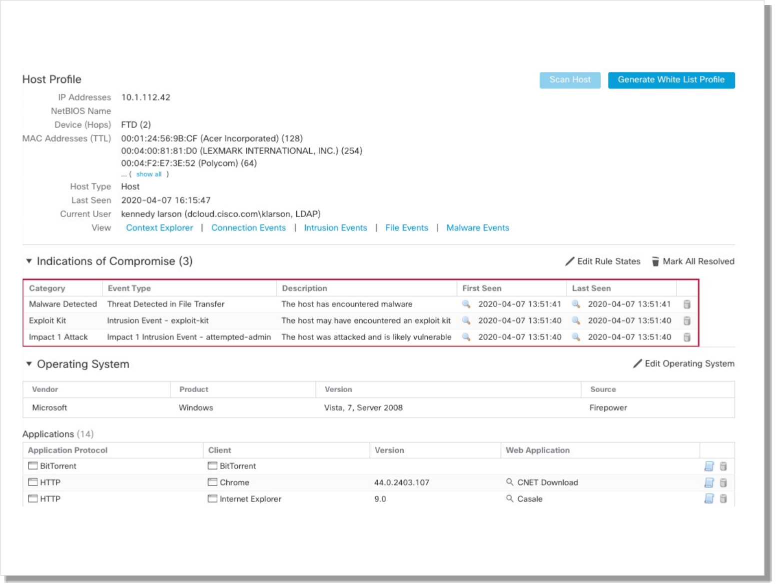
	Snort 2	Snort 3
Многоядерная архитектура		✔
Может запускать множество процессов Snort	✔	✔
Независимая от порта инспекция протоколов		✔
IPS Акселерация / поддержка Hyperscan		✔
Модульность – Проще обновлять для TALOS		✔
Масштабируемое выделение памяти		✔
Правила TALOS нового поколения – прим., Regex/Rule 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

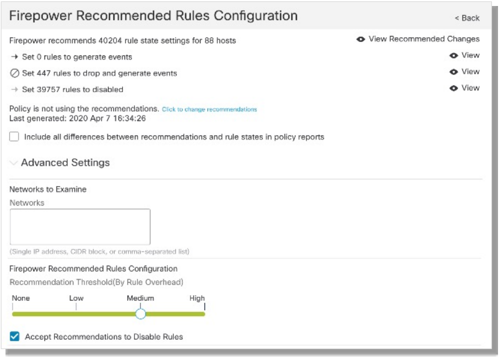
Корреляция Профилей Хоста и IPS

Проводите анализ воздействия и включайте рекомендованные правила



+ SNORT =

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



События индикаторов компрометации (IoC)

IPS События

События вредоносных активностей

События обнаружения malware

Вредоносы и трояны

Exploit-kit

Атаки на Web приложения

Атаки на Web приложения

Повышение привилегий

Соединения к известным CnC адресам: DNS Servers, Suspect URLs

Обнаружение вредоносов

Office/PDF/Java компрометация

Запуск вредоносов

Дропперы

▾ Indications of Compromise (3)

Edit Rule States | Mark All Resolved

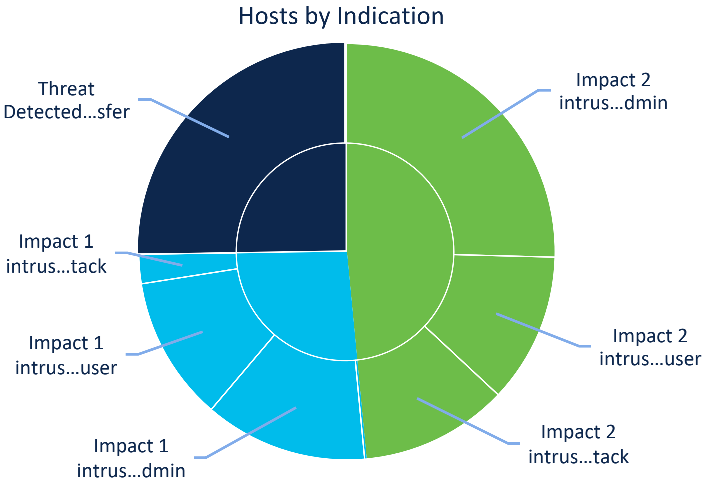
Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2020-04-07 13:51:41	2020-04-07 13:51:41
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2020-04-07 13:51:40	2020-04-07 13:51:40
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

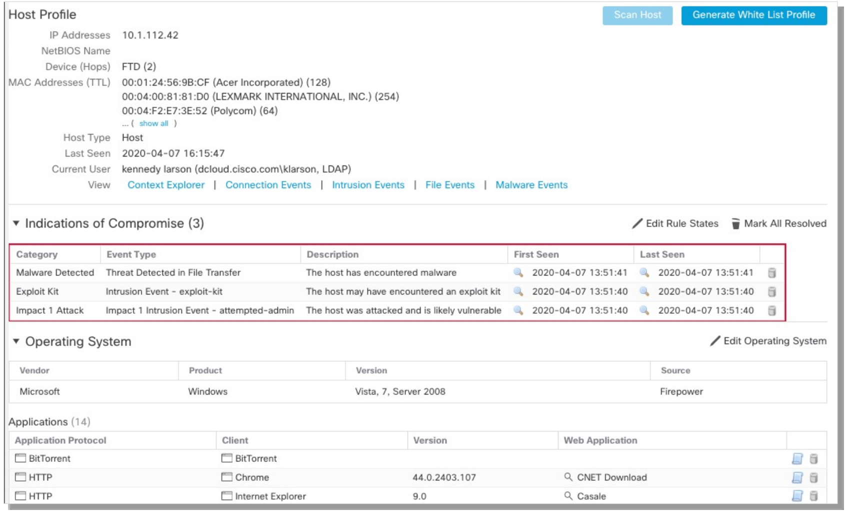
IoC содействуют исправлению состояния

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

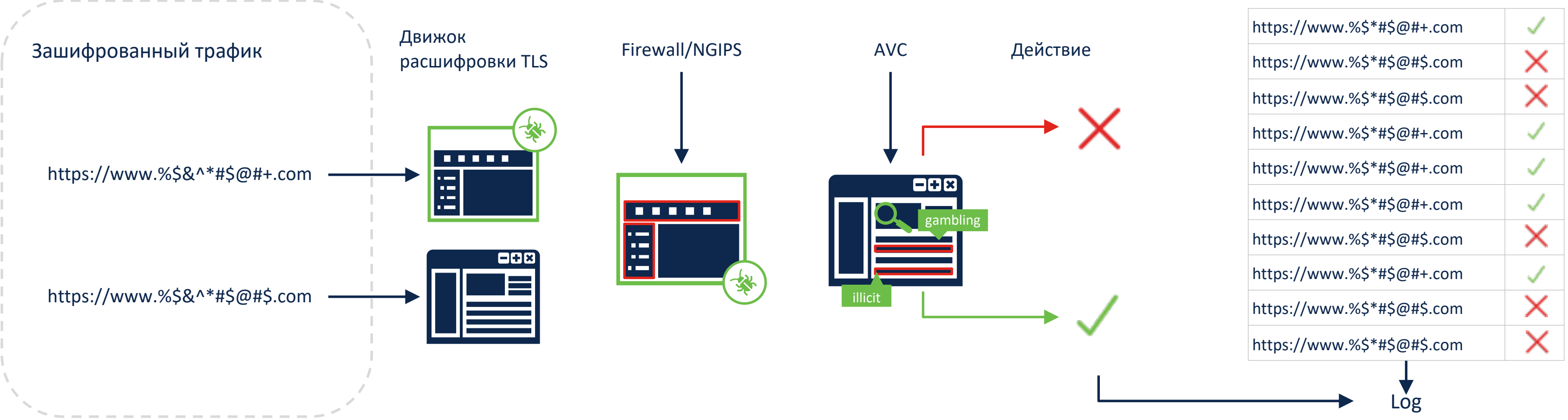




Интегрированная расшифровка TLS

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



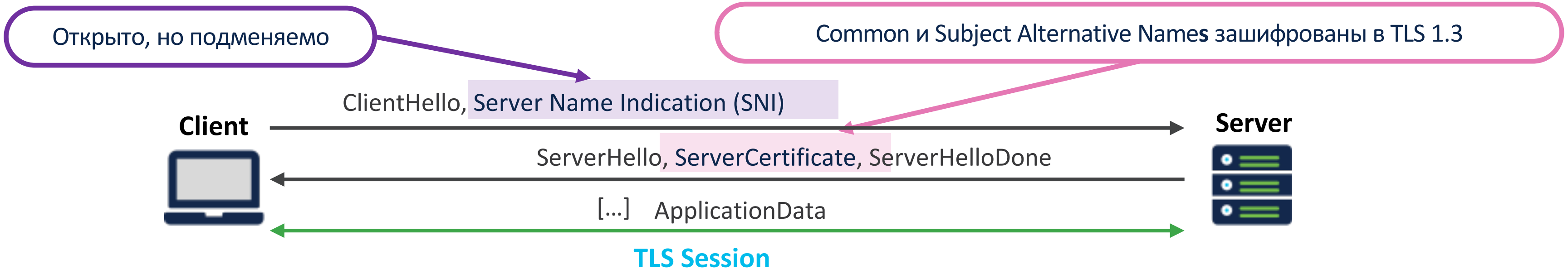
Расшифровка трафика аппаратная либо программная

Инспекция расшифрованных пакетов

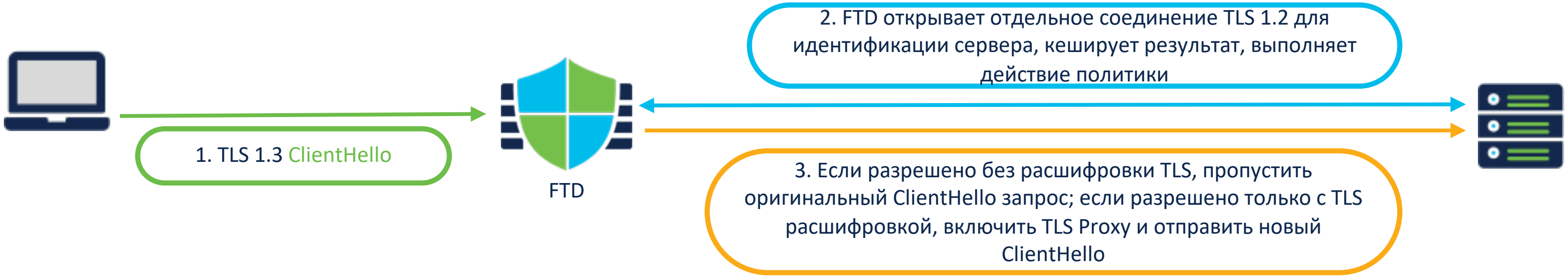
Отслеживание и логирование всех TLS сессий

Быстрое определение приложений и URL с TLS 1.3

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



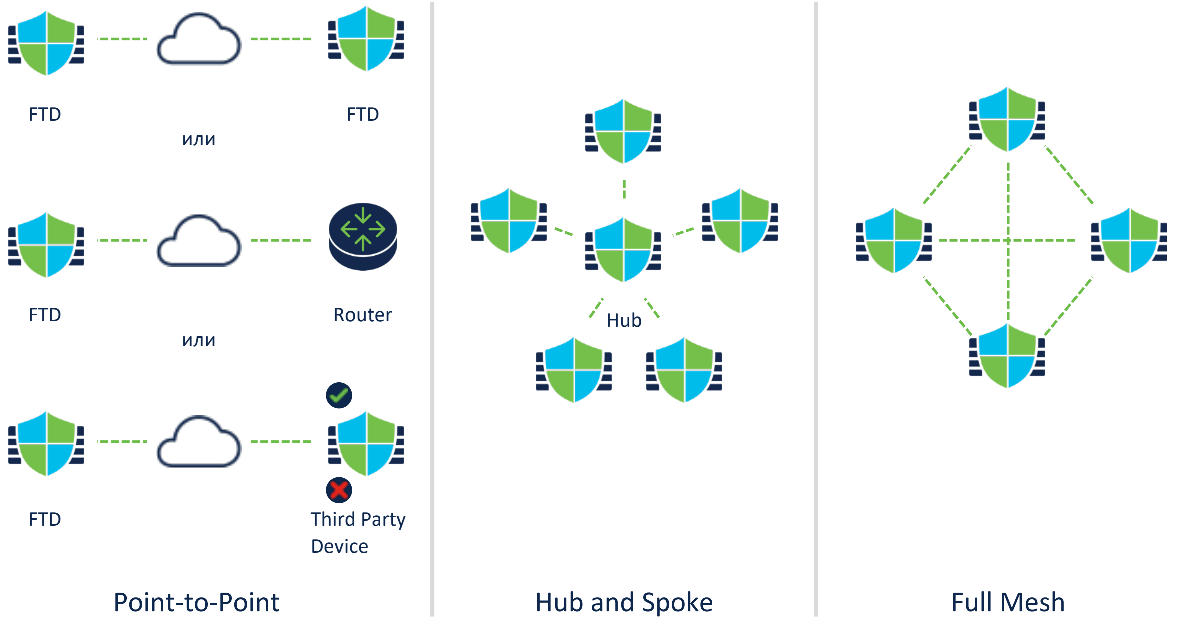
TLS Server Identity Discovery без расшифровки начиная с **FTD 6.7**



Site-to-Site VPN

Легко и безопасно соединять удаленные сайты

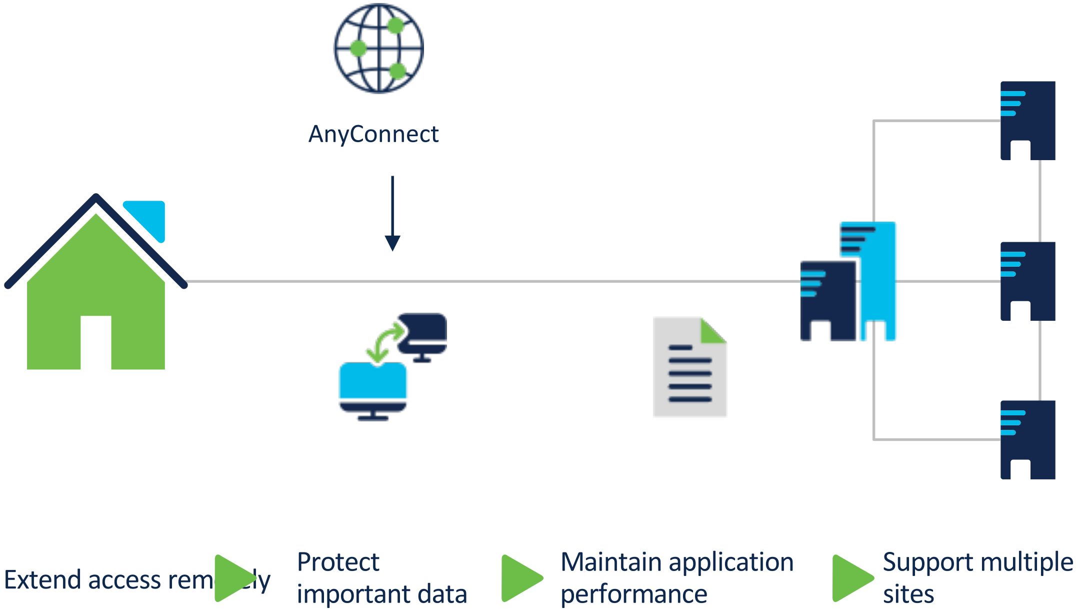
- IKEv1/IKEv2 policy-based VPN
- Простые конфигурации VPN с многими участниками в топологиях:
  - Point-to-point
  - Hub and Spoke
  - Full Mesh
- Гибкие опции аутентификации – общий ключ (автоматически) и сертификаты



Remote Access VPN

Provide ubiquitous secure access from remote and roaming users

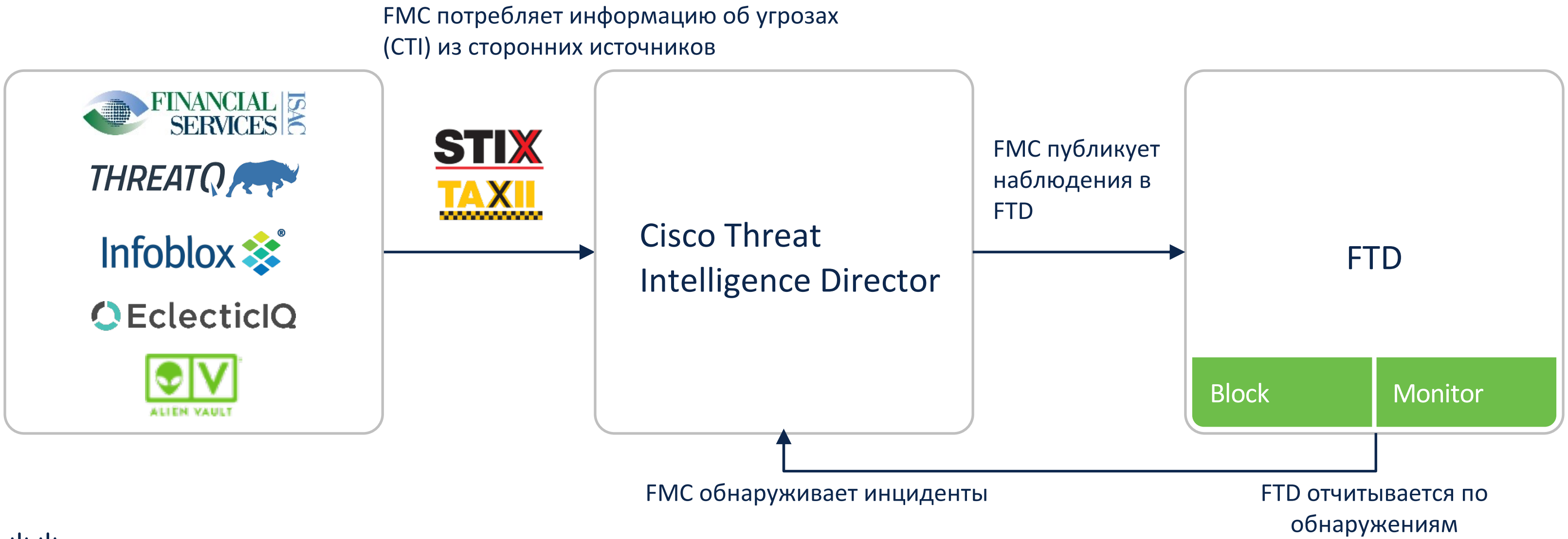
- Posture assessment
- Uses TLS, DTLS or IKEv2
- Easy wizard-based configuration
- Identity based security policies
- Enhanced security with 2 FA/MFA provided by Secure Access (Duo)
- Passwordless Authentication



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

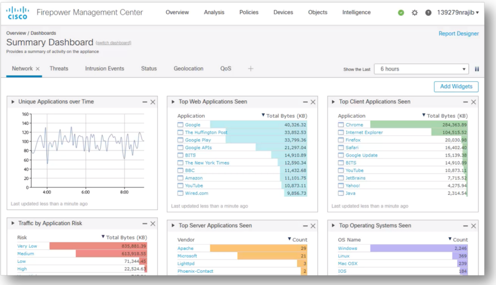
Целостная политика и осведомленность

Управления для любого пользователя

Гибкость облачного или локального развертывания

Интеграции безопасности

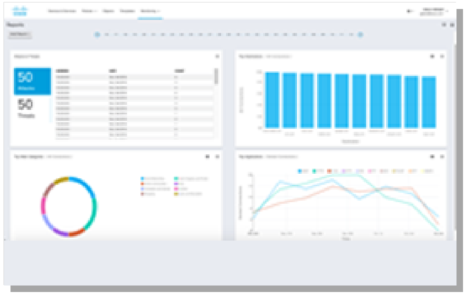
Firewall Management Center



Локальное централизованное управление с прицелом на безопасность

Общие API

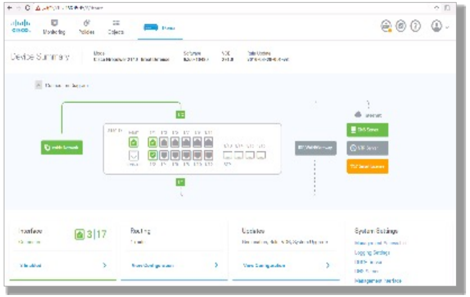
Cisco Defense Orchestrator



Облачное централизованное управление, с прицелом на сетевые функции

Coexist

Cisco Firewall Device Manager (FDM)



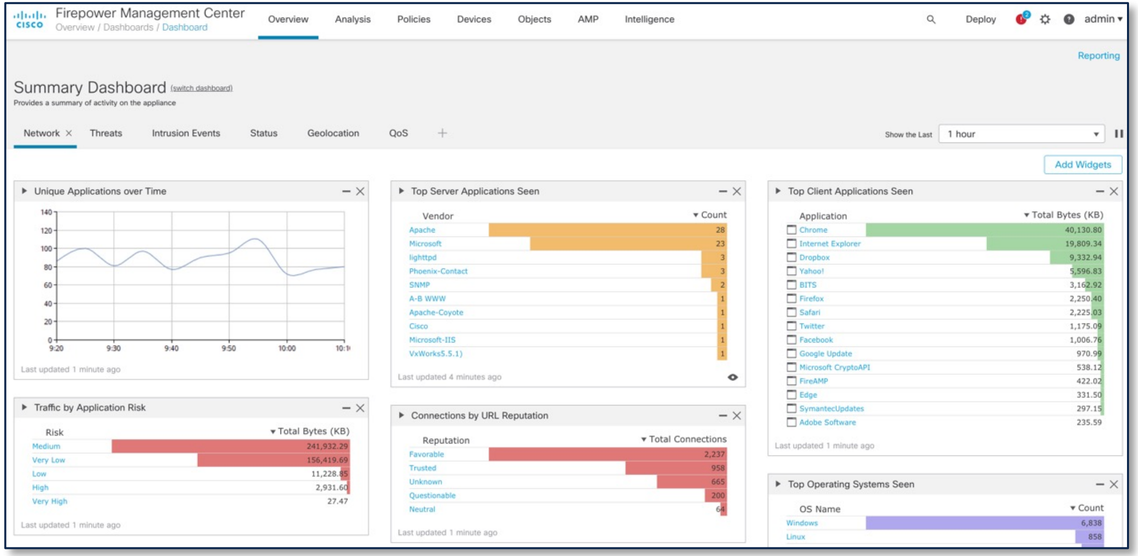
Локальное управление с прицелом на сетевые функции

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

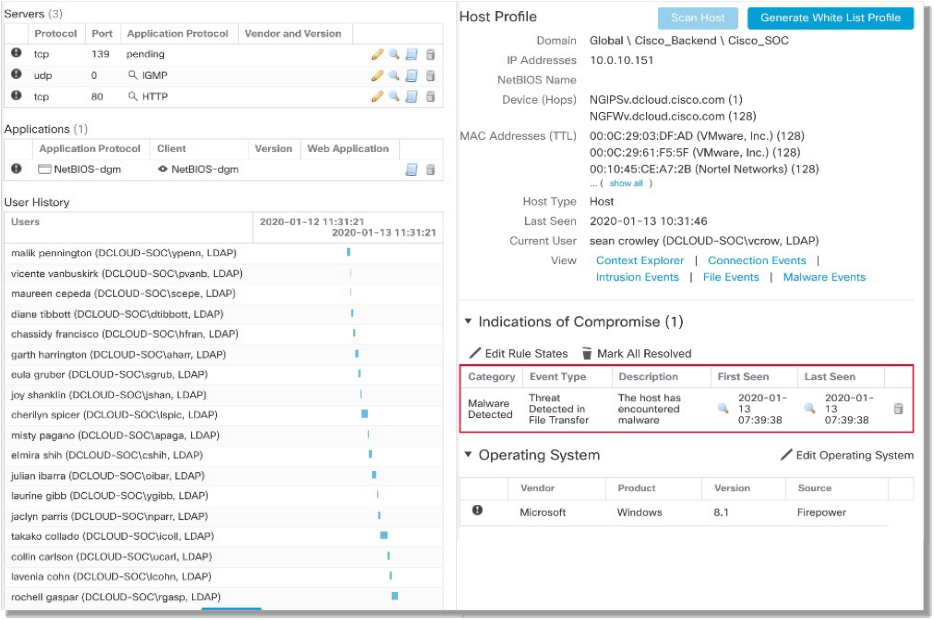
- Snort 3
- Динамические объекты
- Унифицированный просмотр событий
- Кросс-доменное доверие AD
- DNS репутационная фильтрация
- SecureX интеграция
- ACI интеграция – FMC Endpoint Update App

- 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

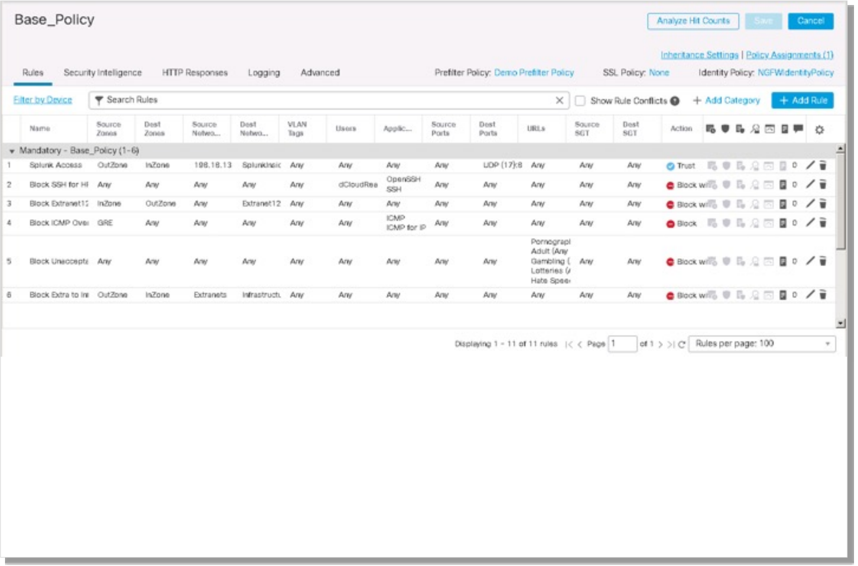
- Обнаруживает приложения, пользователей и хосты благодаря пассивному анализу трафика
- Собирает контекст и помогает понять степень воздействия атаки
- Настраивает набор сигнатур IPS на основании полученных данных
- Дополняет профили хостов данными, полученными от сторонних сканеров уязвимостей



Управление политикой

Снижение сложности управления политикой

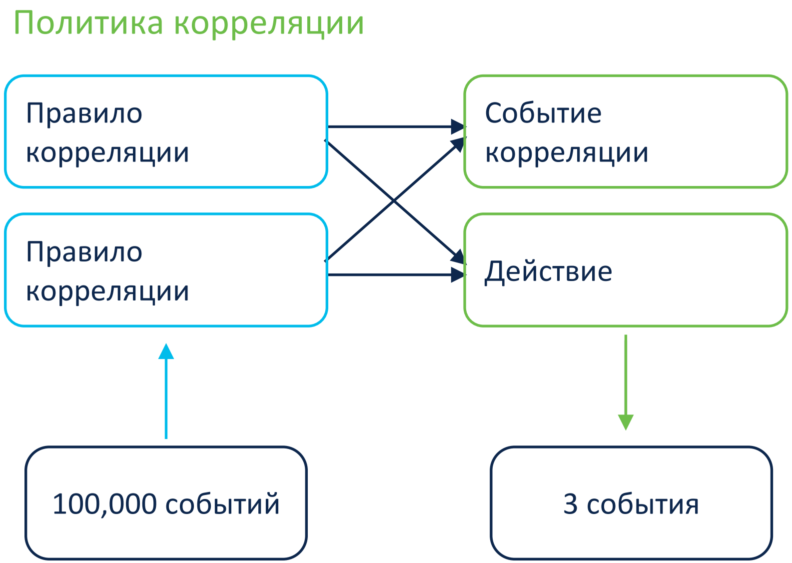
- Централизованное локальное управление политиками на различных платформах межсетевых экранов
- Интегрирует множество функций безопасности в единой политике доступа
- Снижает необходимость ручной настройки путем наследования и использования шаблонов.



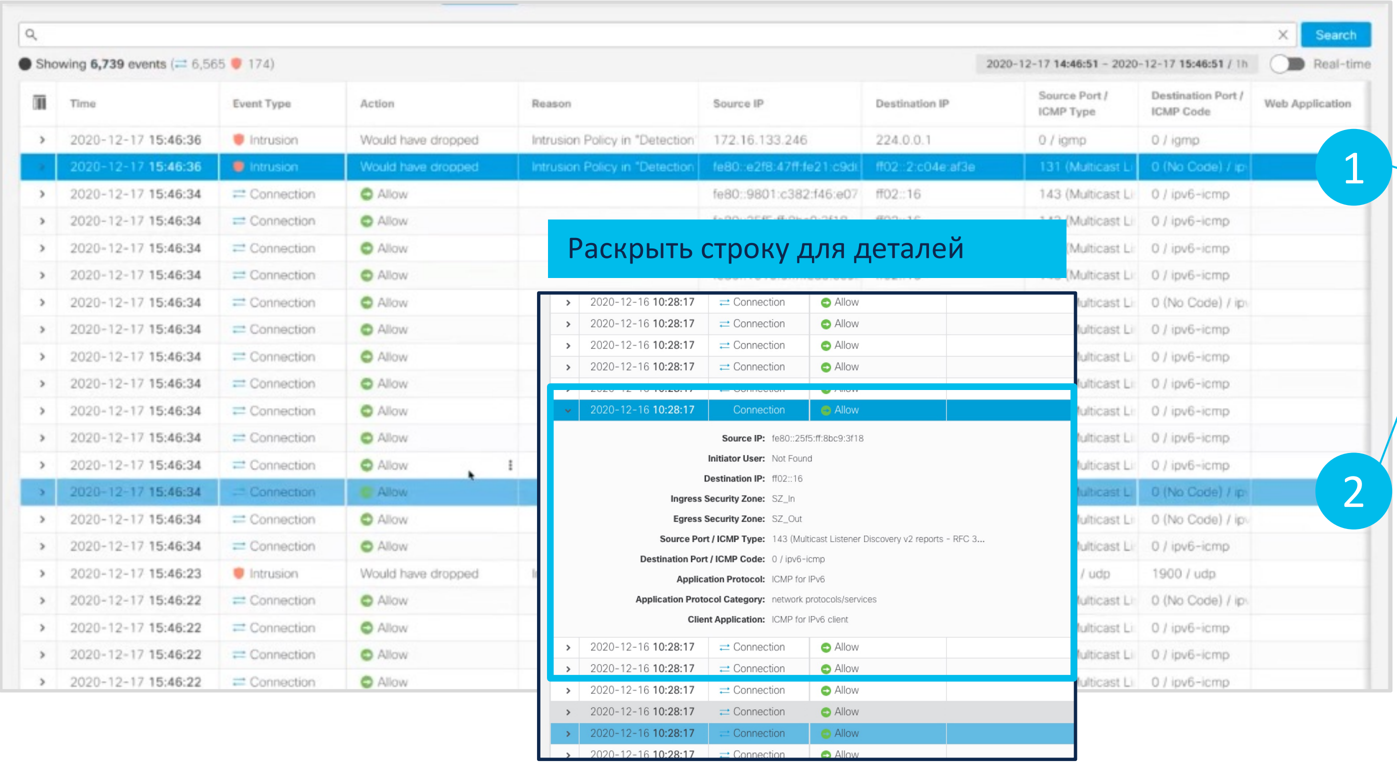
FMC: Автоматизация реагирования на угрозы

Снизить шум и точно среагировать

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



Унифицированный просмотр событий



Настоящая корреляция

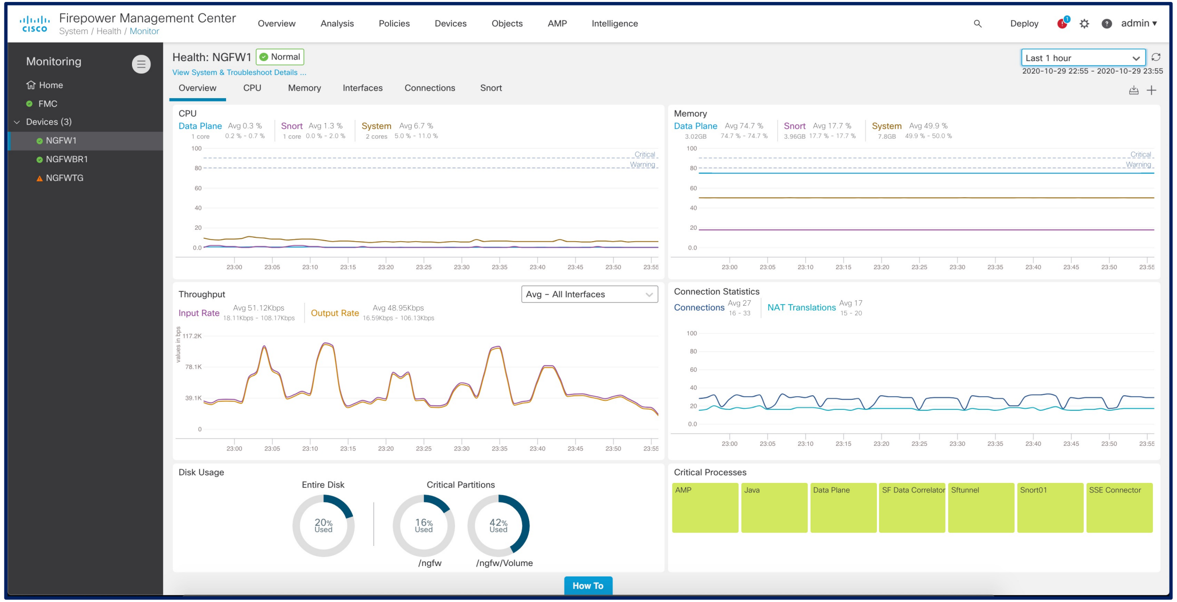
Нажатие на событие Intrusion подсвечивает ассоциированное событие соединения

Мониторинг состояния устройств

Унифицированная статистика из подсистем и критических процессов

Функции

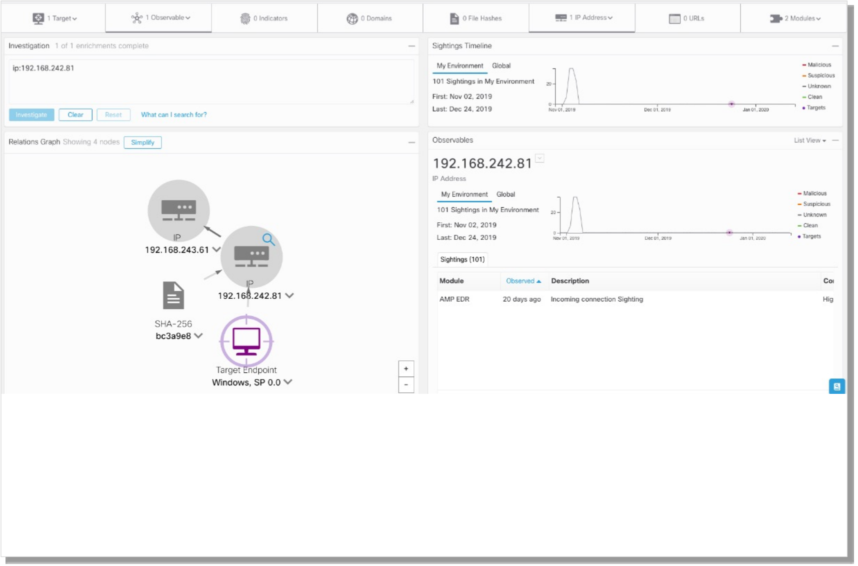
- Графики с трендами, наложение данных и собственные графики
- Улучшенный живой мониторинг включая статус отказоустойчивости и кластера
- Унифицированный Data plane и метрики Snort (прим. CPU, Memory)
- Отчетность по Snort, Настройкам, Соединениям и статистике Процессов
- Доступно через API



FMC Интеграции

Осведомленность и аналитика выходящие за рамки анализа сети

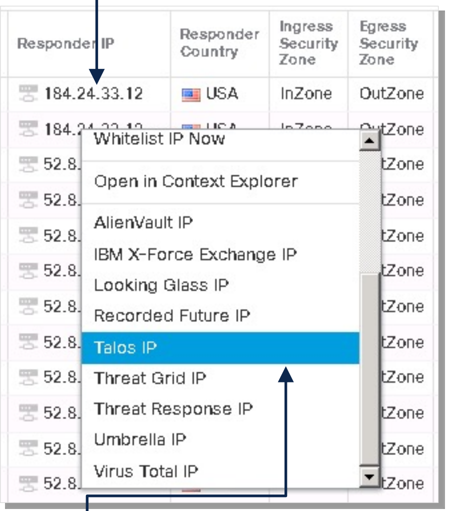
- Тесная интеграция FMC с Secure Endpoint
- Основанные на стандартах вектора угроз (STIX/TAXII)
    - Cisco Threat Intelligence Director (CTID)
- Снизить время на реагирование с широкими возможностями обнаружения и корреляции
    - SecureX Threat Response (CTR)
- Использовать другие продукты Cisco и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



Контекстный кросс-запуск

Тесная интеграция и кросс-запуск для поиска угроз

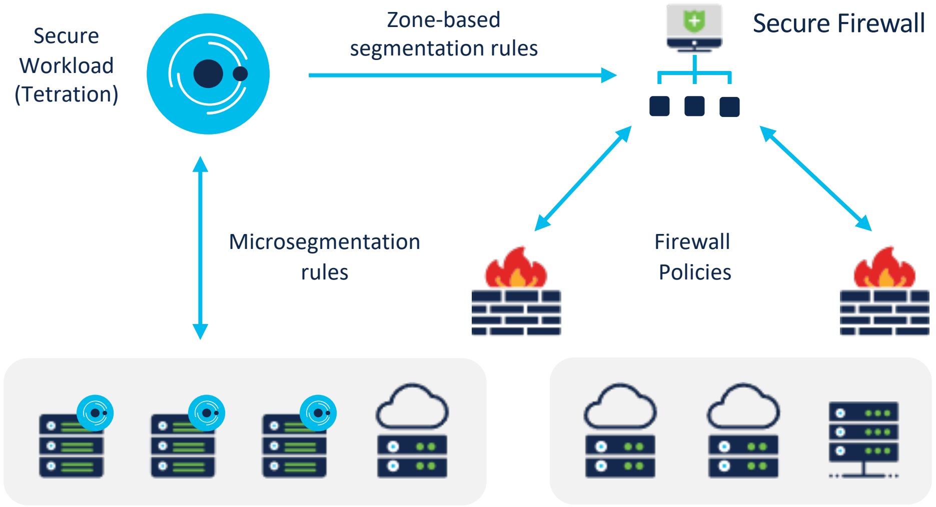
1 Правый клик на IP address



2 Выбрать просмотр в Talos по IP

- Навигация напрямую в архитектуре Cisco
- Навигация в сторонние утилиты 3rd
- Снизить время на анализ IoC для снижения времени реагирования
- Снизить сложность интеграции

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 multicloud позволит лучше выстраивать выстраивать безопасность в распределенной среде.”***

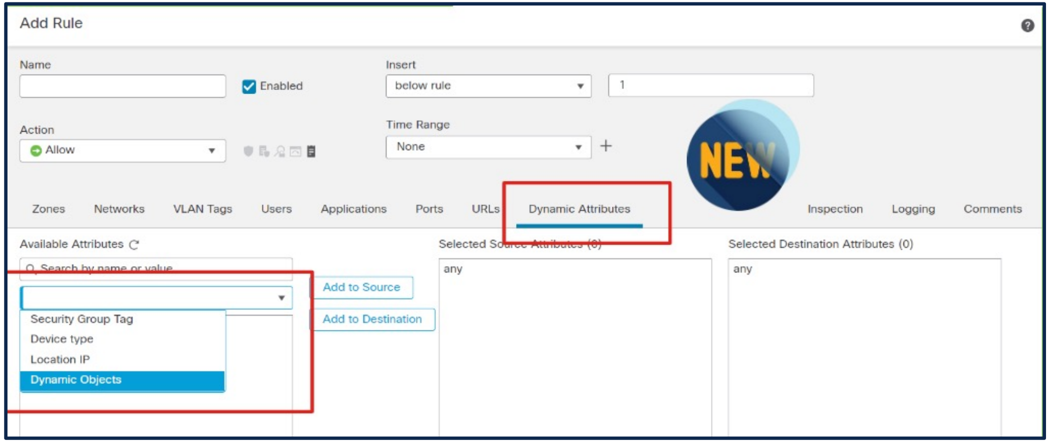
-- Global payments and fleet management enterprise

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.

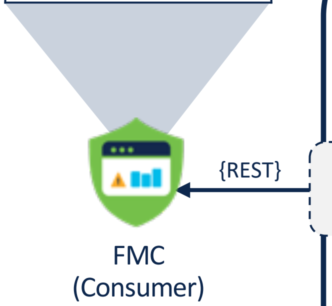
Решение: Cisco предоставляет программируемый метод создания, удаления и управления динамическими объектами. Работает для VMware, AWS, и Azure тегов в том числе.

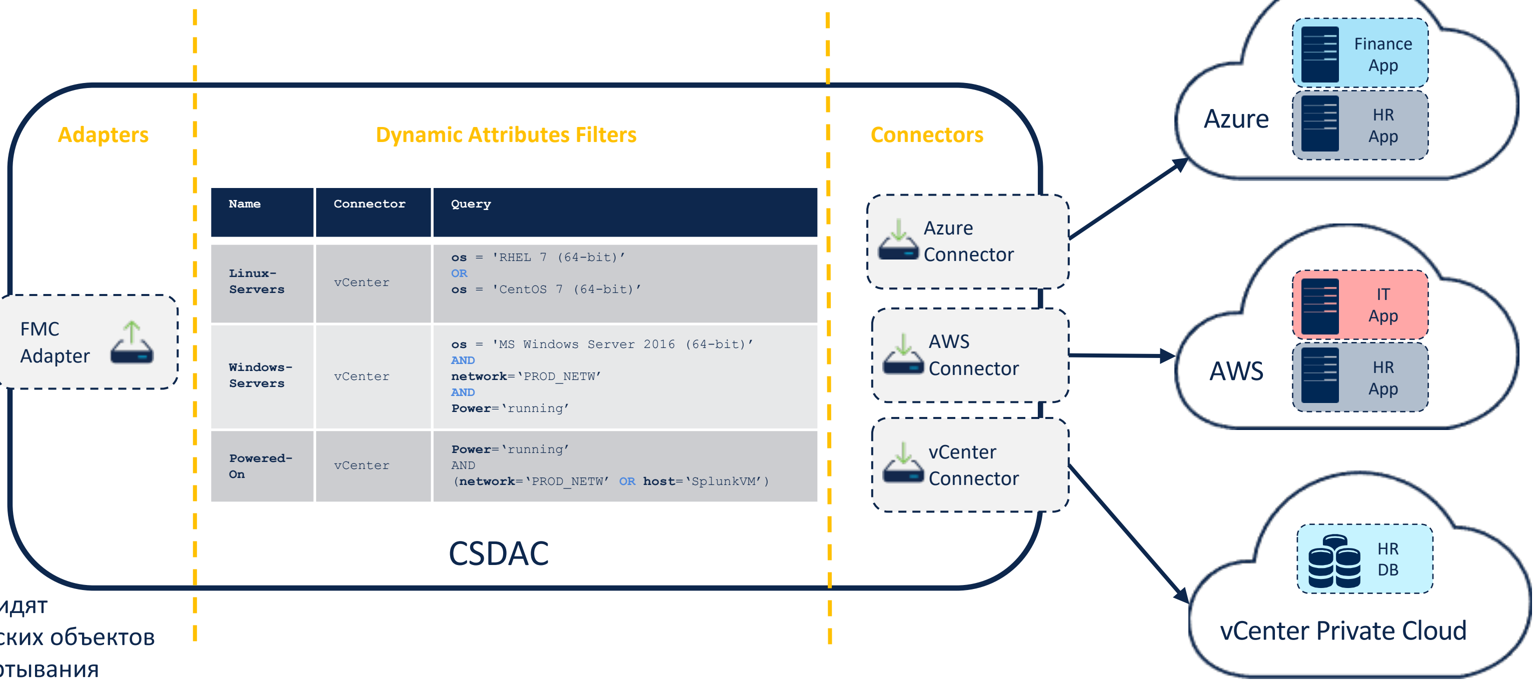
Преимущества: Категорически снизить загрузку администраторов по отслеживанию актуальности политик, предоставляет обновления политики по запросу без промедления и необходимости развертывания политики



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





Name	Connector	Query
Linux-Servers	vCenter	os = 'RHEL 7 (64-bit)' OR os = 'CentOS 7 (64-bit)'
Windows-Servers	vCenter	os = 'MS Windows Server 2016 (64-bit)' AND network='PROD_NETW' AND Power='running'
Powered-On	vCenter	Power='running' AND (network='PROD_NETW' OR host='SplunkVM')

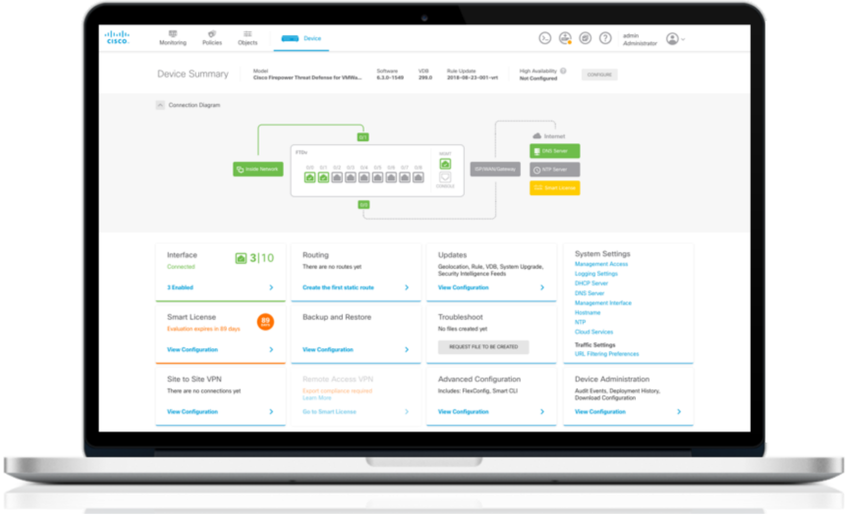
Преимущества:
- Сенсоры мгновенно видят изменения динамических объектов
- Изменения без развертывания политики

Secure Firewall Device Manager (FDM)

Что такое Secure Firewall Device Manager (FDM)

Управление одним устройство 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

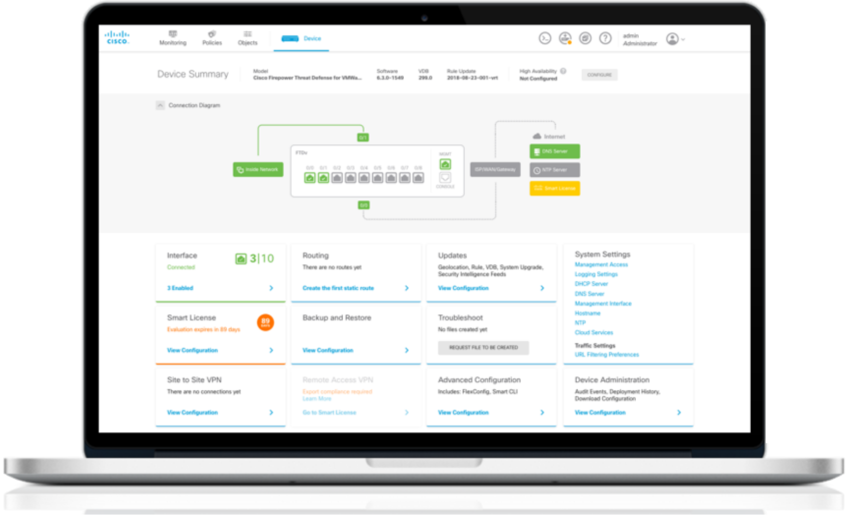
Простота настройки, управления, мониторинга

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

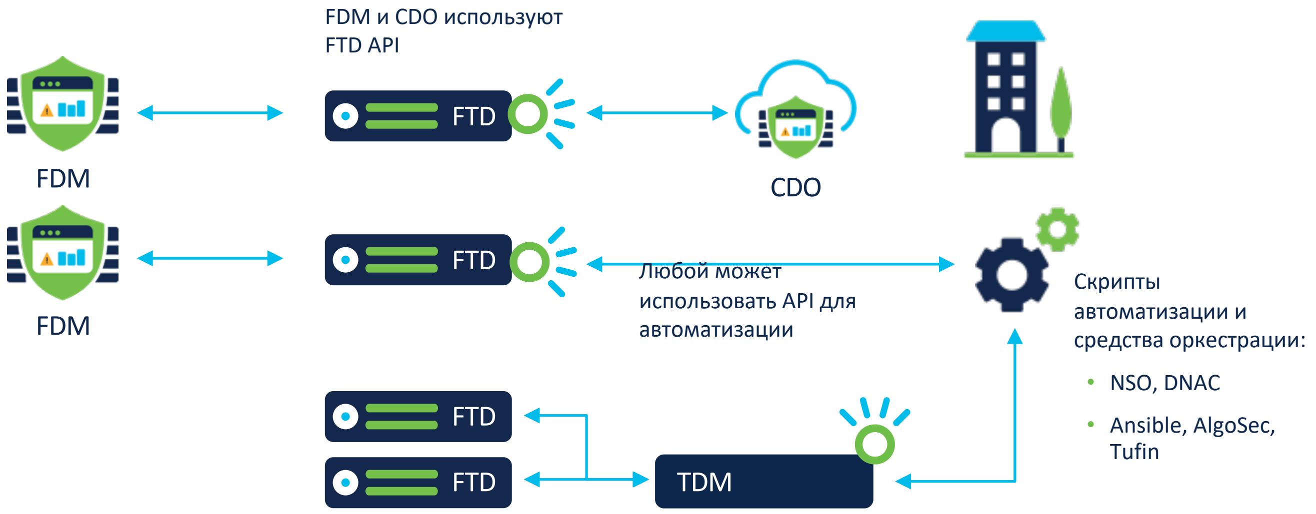
Повышайте операционную эффективность

Автоматизируйте сложные задачи в масштабе

Интегрируйтесь в экосистему

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

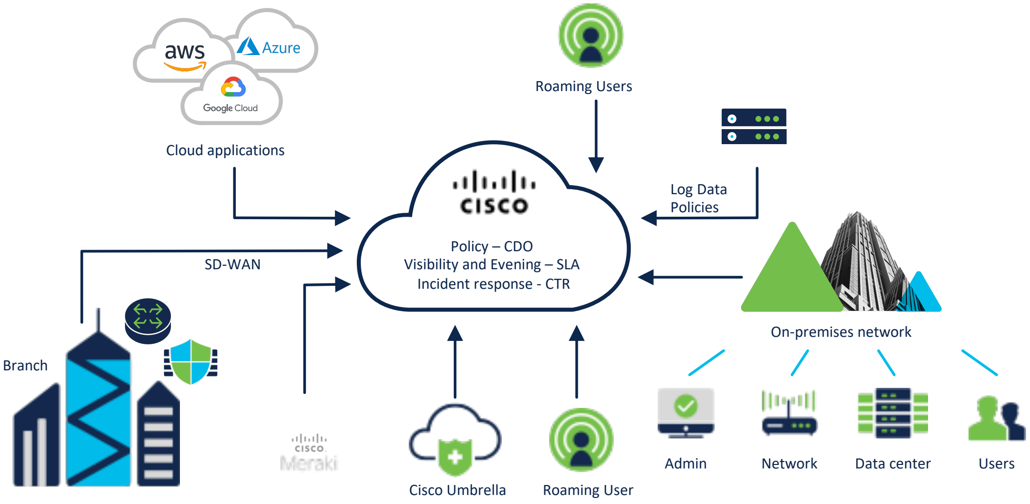
CDO это облачное приложение, которое абстрагирует сложность для экономии времени и поддерживает организацию защищенной от актуальных угроз.

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

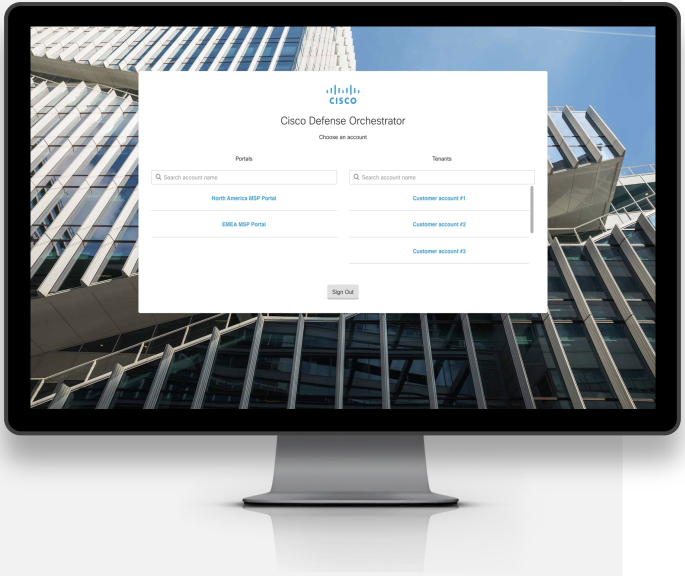
- Сервис уведомлений
- Поддержка интерфейса EtherChannel в FTD
- Поддержка Multi-tenant
- Low Touch Provisioning
- Secure Group Tags (SGT)
- Объекты AD Objects

CDO постоянно обновляется, здесь свежая информация

Cisco Defense Orchestrator

MSP портал

- Используйте CDO MSP портал для управления неограниченным количество 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

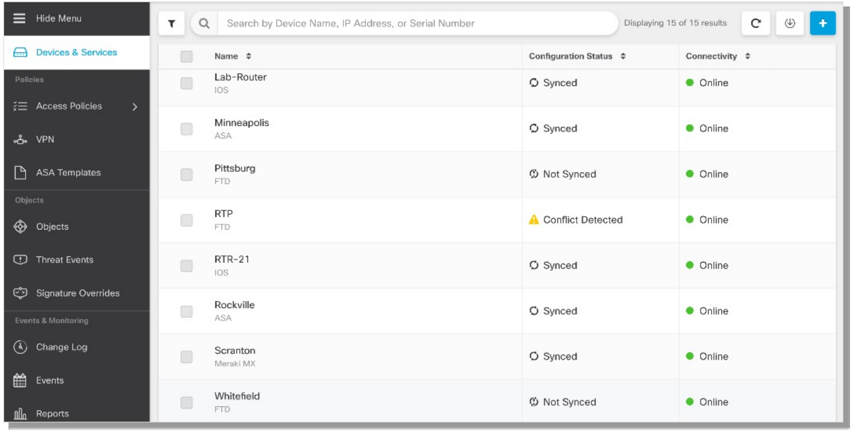
Модель подписки с моделью Pay as you Grow

Низкие расходы на содержание

Масштабируемое управление политиками

Простая гибкая платформа управления для смешанных окружений

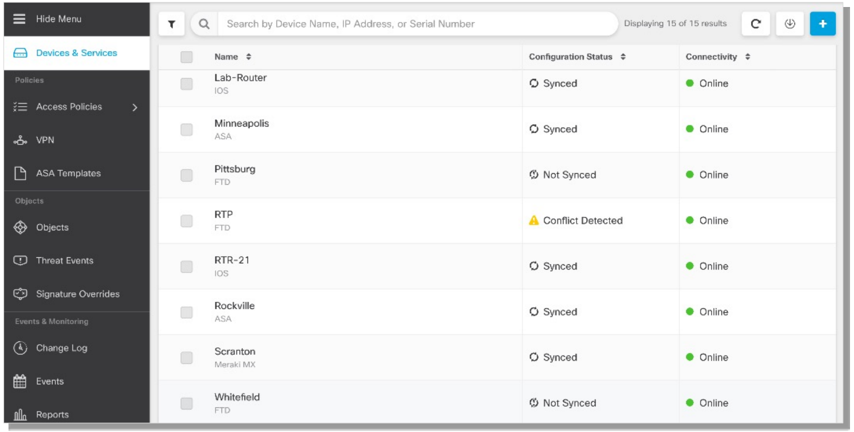
- Управление политиками в крупном масштабе
  - Шаблоны и макросы позволяют быстро создавать конфигурации для тысяч устройств
  - Простая миграция ASA в FTD
  - Интеграция различных функций безопасности в единую политику доступа



Простое и эффективное управление объектами

Простое графическое сравнение объектов

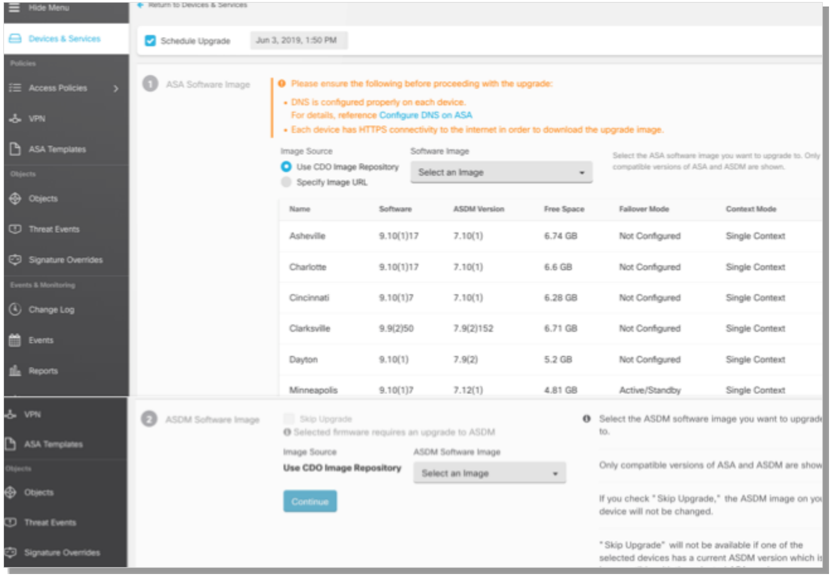
- Обнаружение конфликта объектов с простым исправлением ненужных объектов
  - Дубликаты
  - Не используемые
  - Не полные
- Анализ объектов снижает объем конфигураций



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

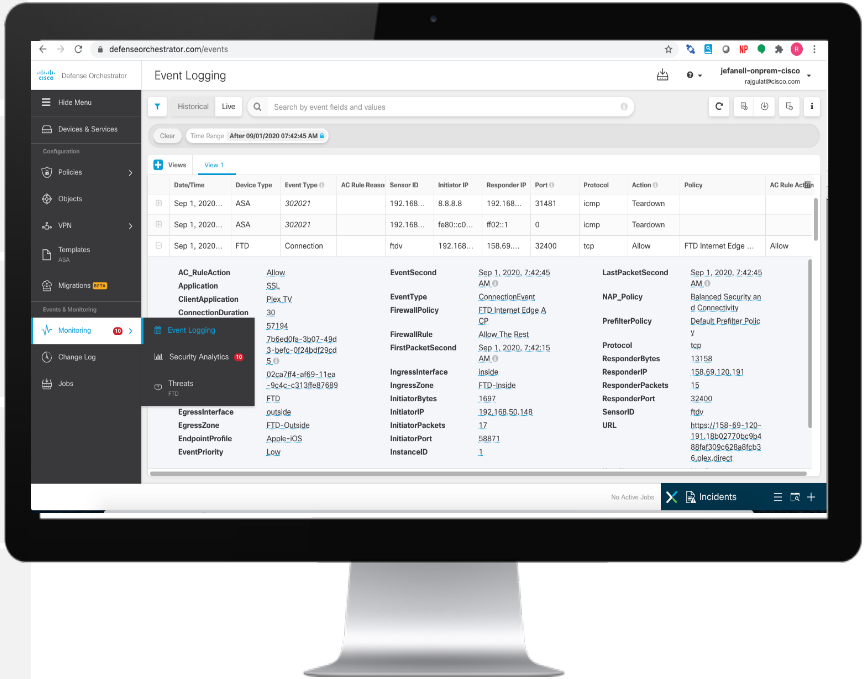
Платформы		Минимальный софт
ASA 5500-X		ASA 8.4 FTD 6.4
Firepower 1000		ASA 9.13 FTD 6.4
Firepower 2100		ASA 8.4 FTD 6.4
Firepower 4100		ASA 8.4 FTD 6.5
Firepower 9300		ASA 8.4 FTD 6.5
Virtual – Private Cloud	KVM, VMWare	ASA 8.4 FTD 6.4
Virtual – Public Cloud	AWS, Azure	ASA 8.4 FTD 6.5 (Azure)
Meraki MX	 	Последняя версия ПО

Cisco Security Analytics and Logging

Архитектура аналитики и логирования

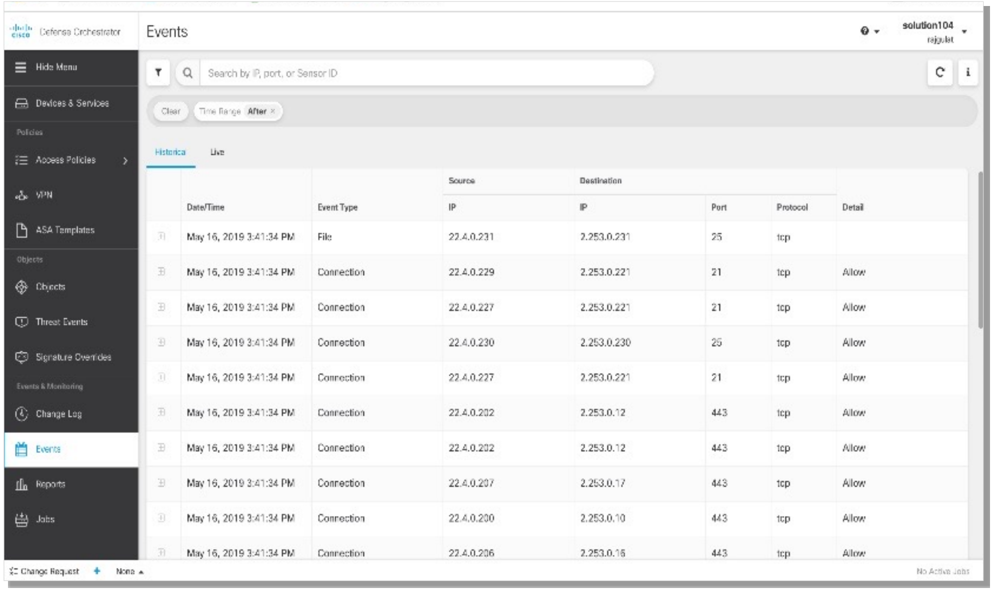
SAL (SaaS) Облачные функции

- 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



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

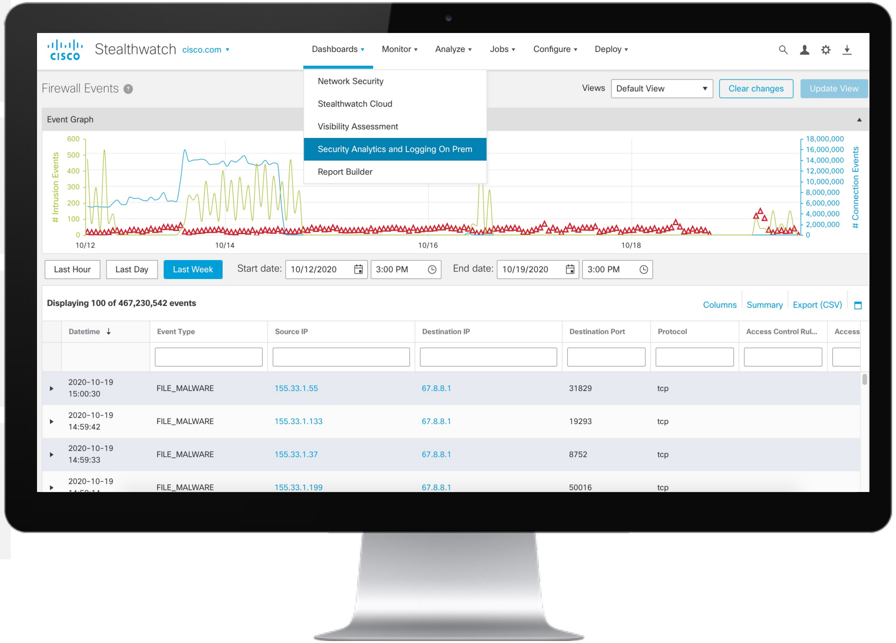
Идентифицировать и обогащать высокоприоритетные уведомления

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



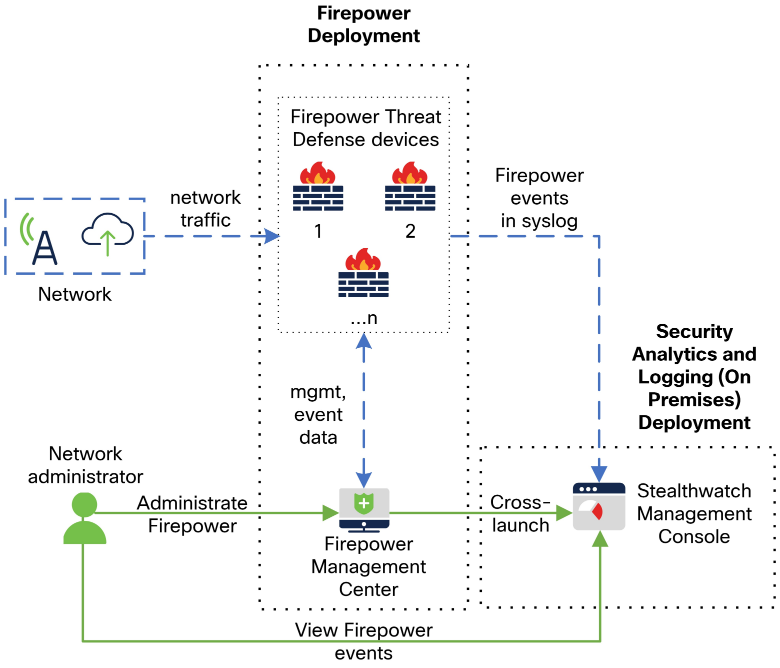
FMC интеграция с Cisco Security Analytics and Logging (On-Prem)

Кнопка для простой настройки

- В FMC настраиваются ссылки кросс-запуска для консоли аналитики Secure Analytics
- Настраиваются учетные данных 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 Clientess 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, Clientess, 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

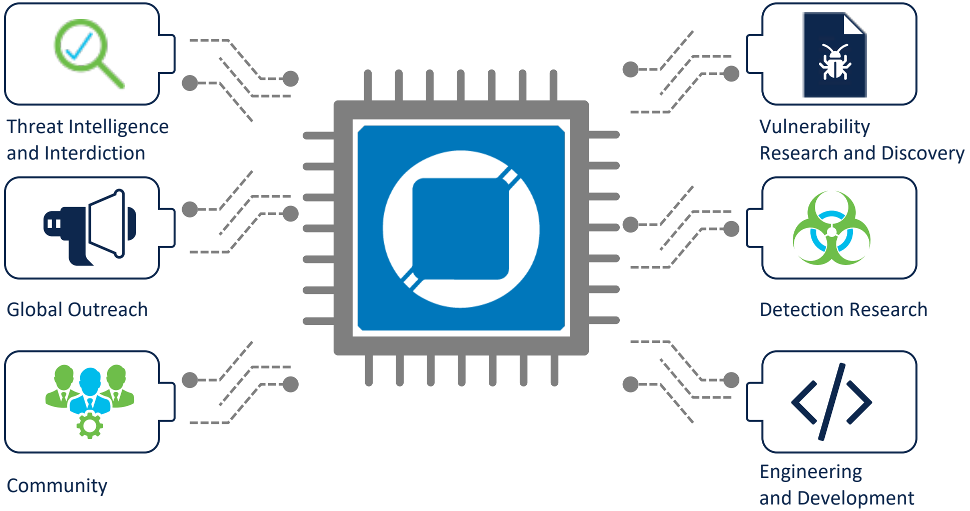
Безопасность

- 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.

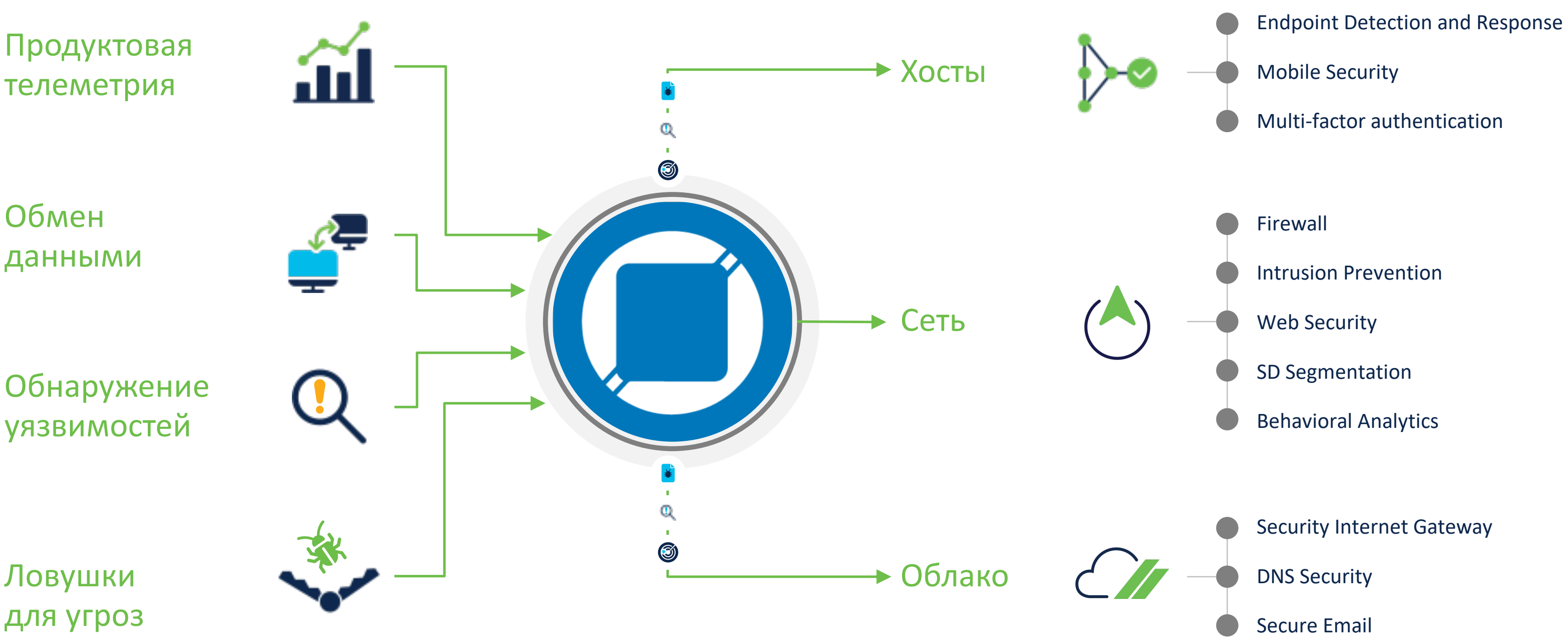
Talos

Что такое Talos?

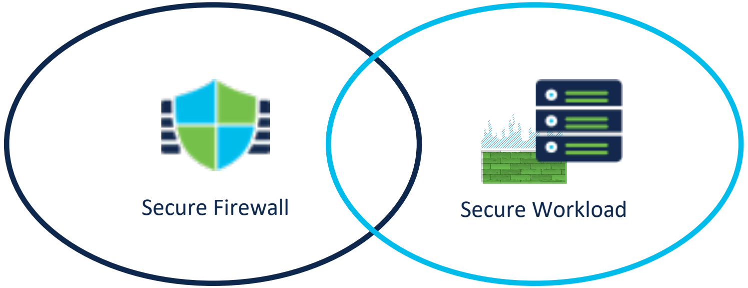
Talos это большая интеллектуальная группа в Cisco. Мы здесь чтобы сражаться на светлой стороне – мы работаем чтобы защищать от угроз наших заказчиков и пользователей в целом.



От непонятного к известному



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 полит[illegible]и

Локальный

SaaS

Увидеть всю сетевую активность приложений

Автоматически обнаружить группу и идентификацию приложения

Валидировать и симулировать политику до применения

Secure Workload (Tetration)

Сдерживание последовательного продвижения

Постоянное отслеживание соответствия безопасности

Идентификация поведенческих аномалий

Снижение поверхности атаки

Интеграция cSecureX, унифицированная видимость и автоматизация

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.

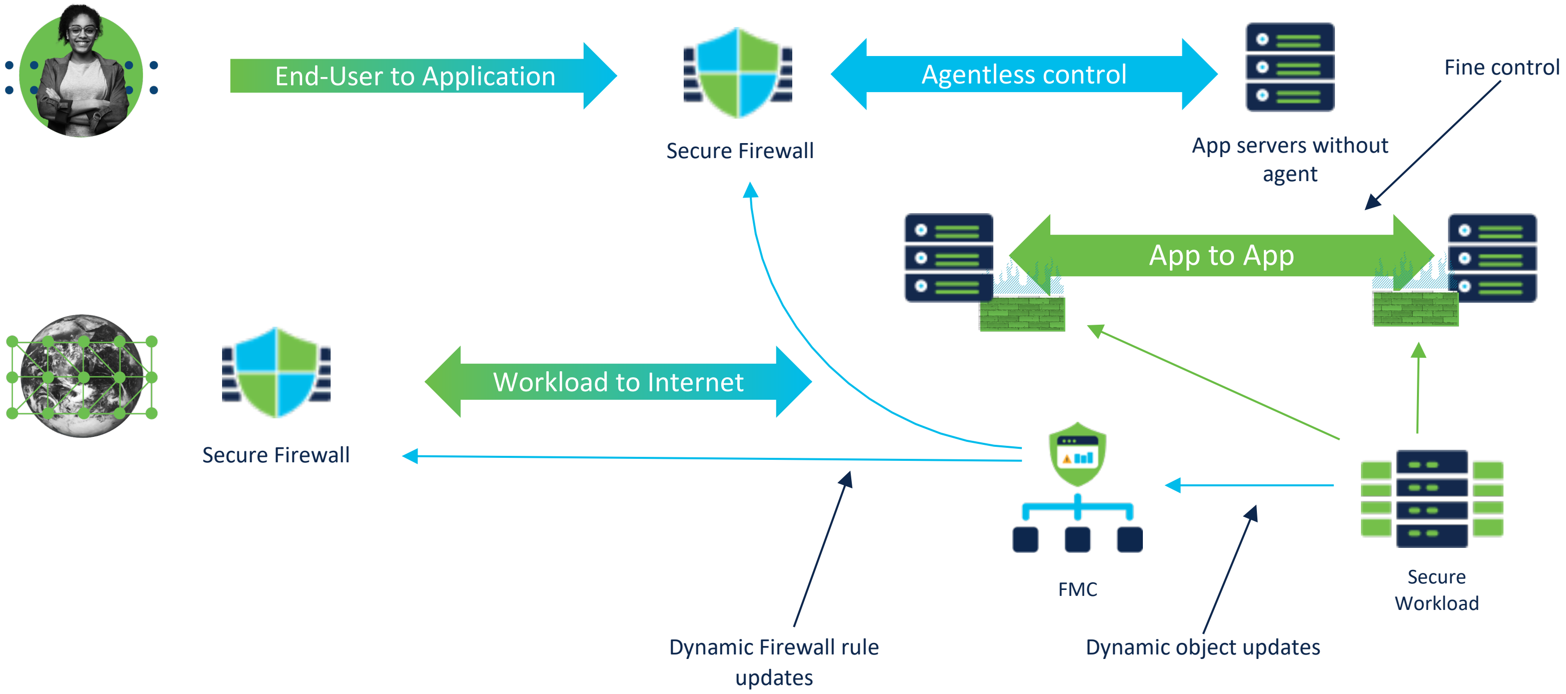
Ключевые функции

- 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

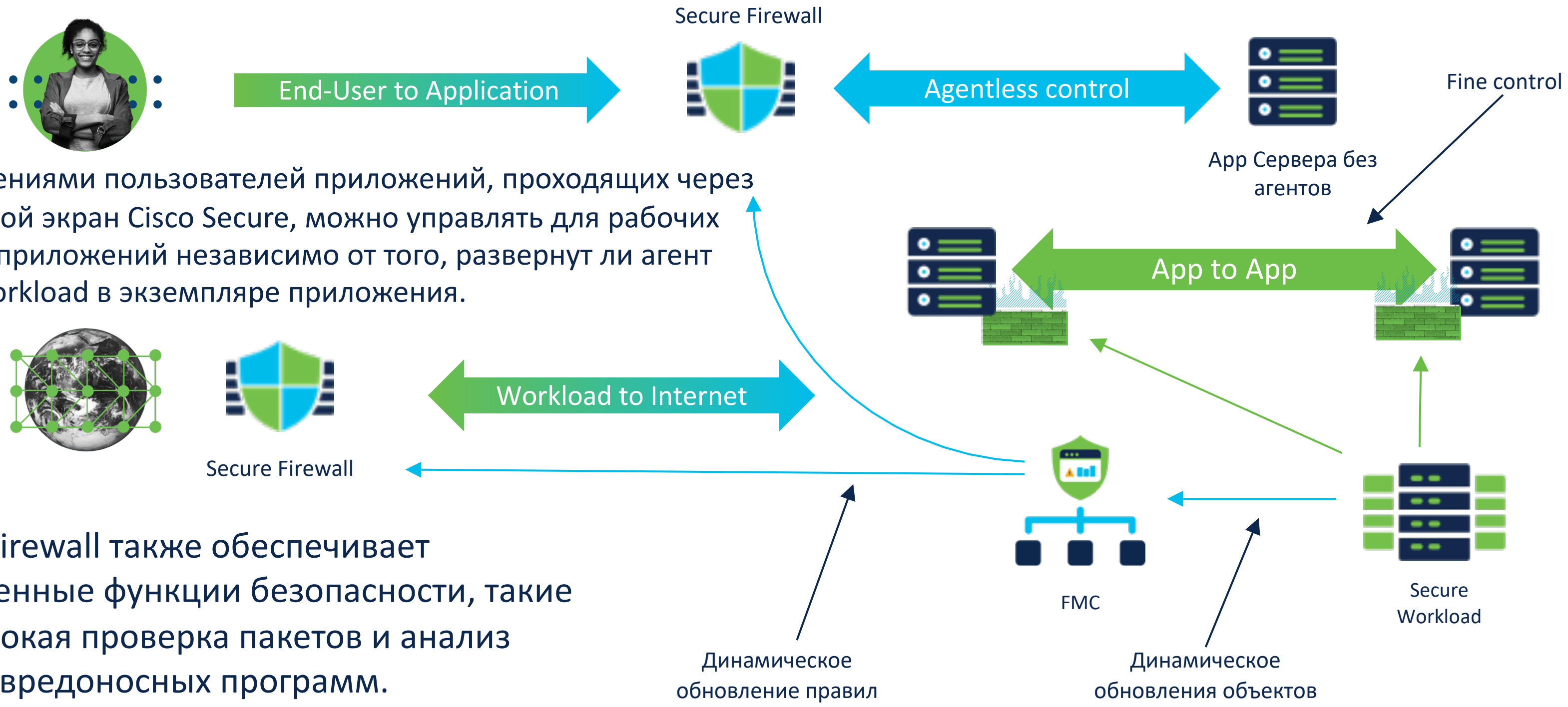
Key Capabilities

- 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



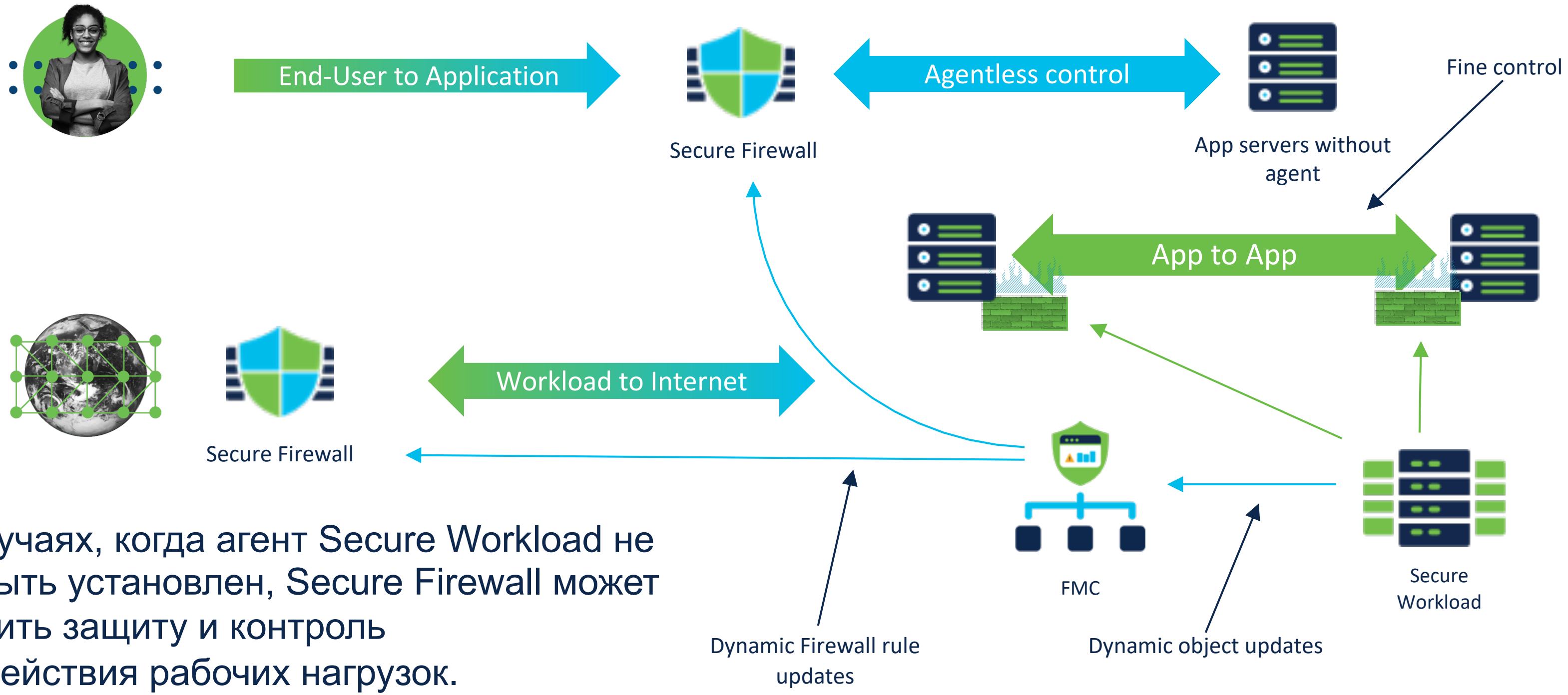
Secure Workload Integration



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

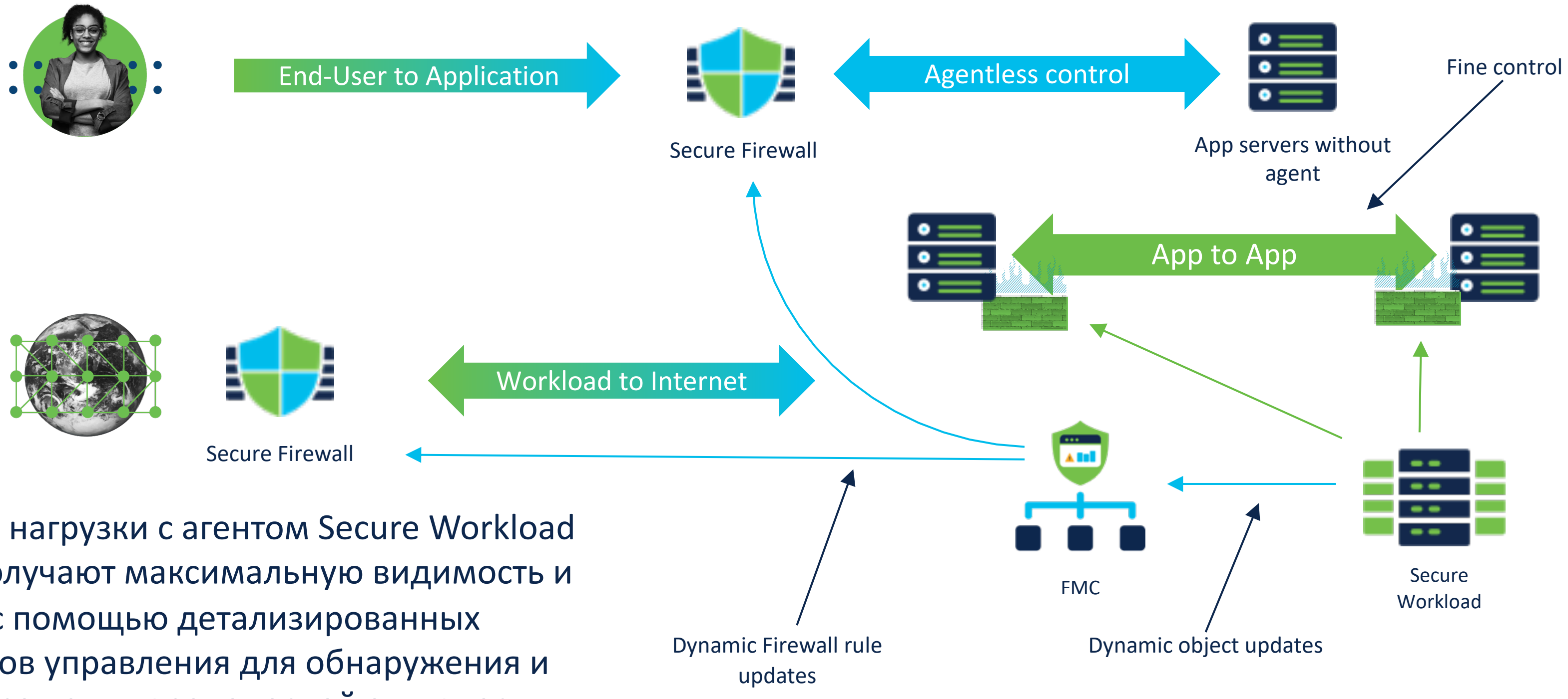
Secure Firewall также обеспечивает расширенные функции безопасности, такие как глубокая проверка пакетов и анализ файлов вредоносных программ.

Интеграция Secure Workload



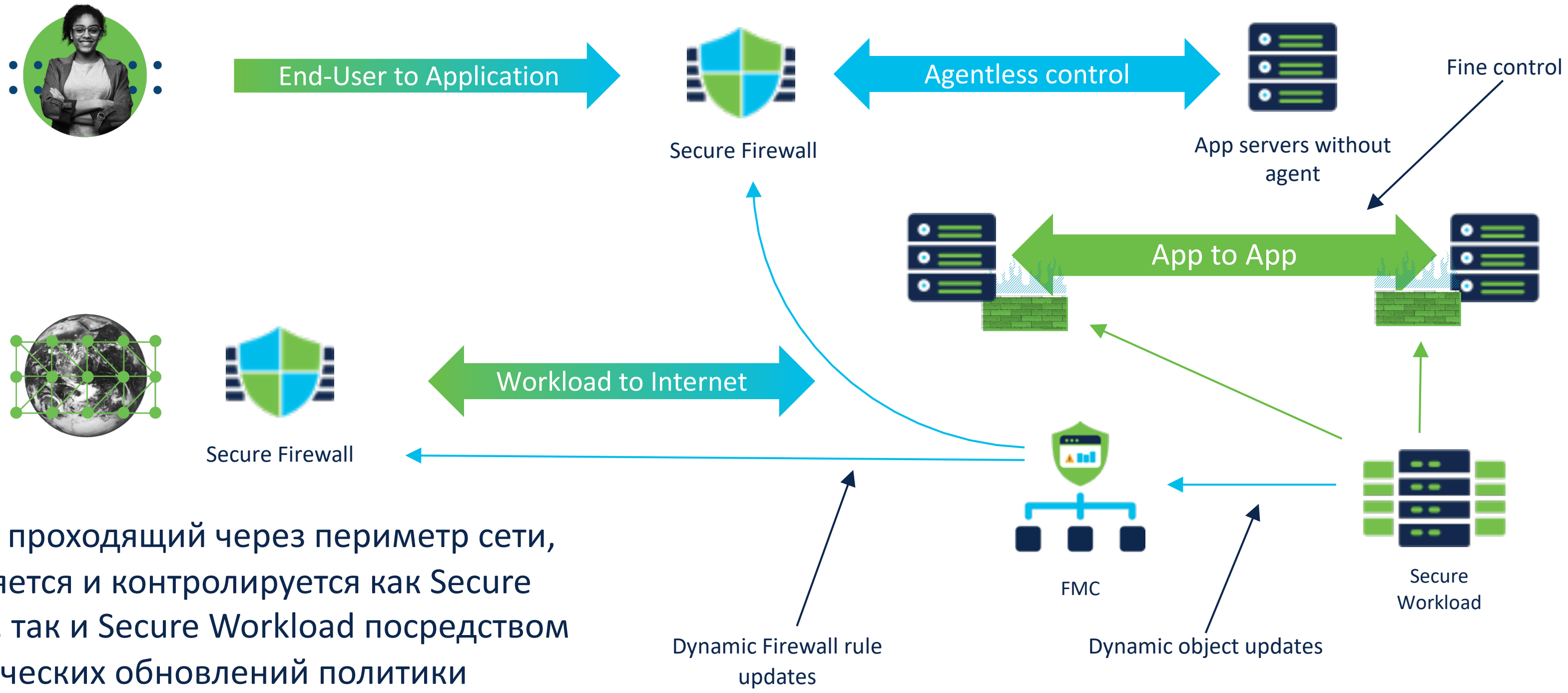
В тех случаях, когда агент Secure Workload не может быть установлен, Secure Firewall может обеспечить защиту и контроль взаимодействия рабочих нагрузок.

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.

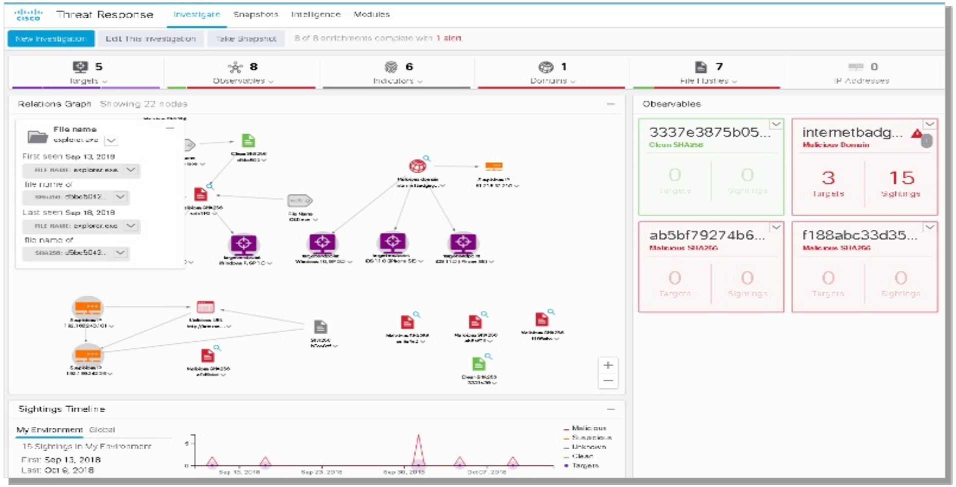
SecureX

Платформа безопасности

Что такое SecureX threat response?

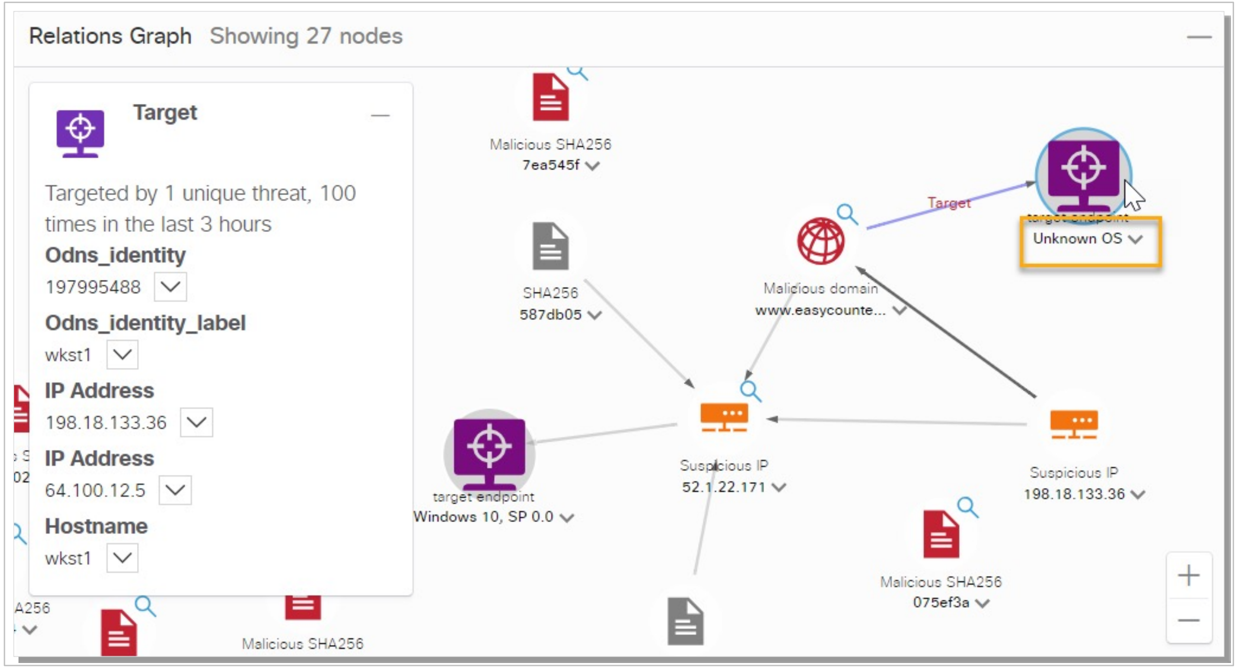
Автоматизирует интеграцию между сетями, узлами и облачными средами

- 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



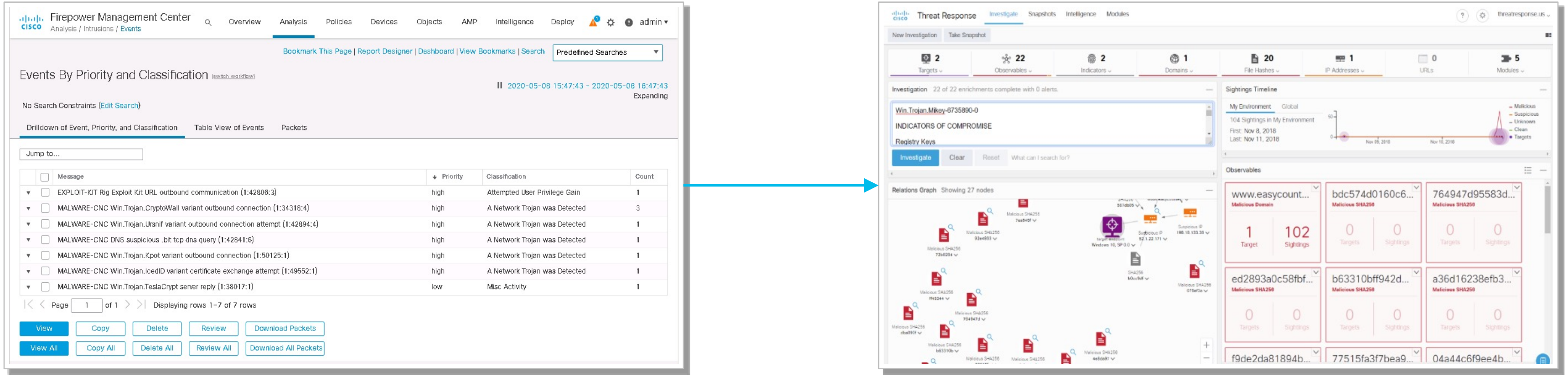
Расследуйте любой объект: Endpoint

Снижение сложности и времени, необходимого для поиска угроз



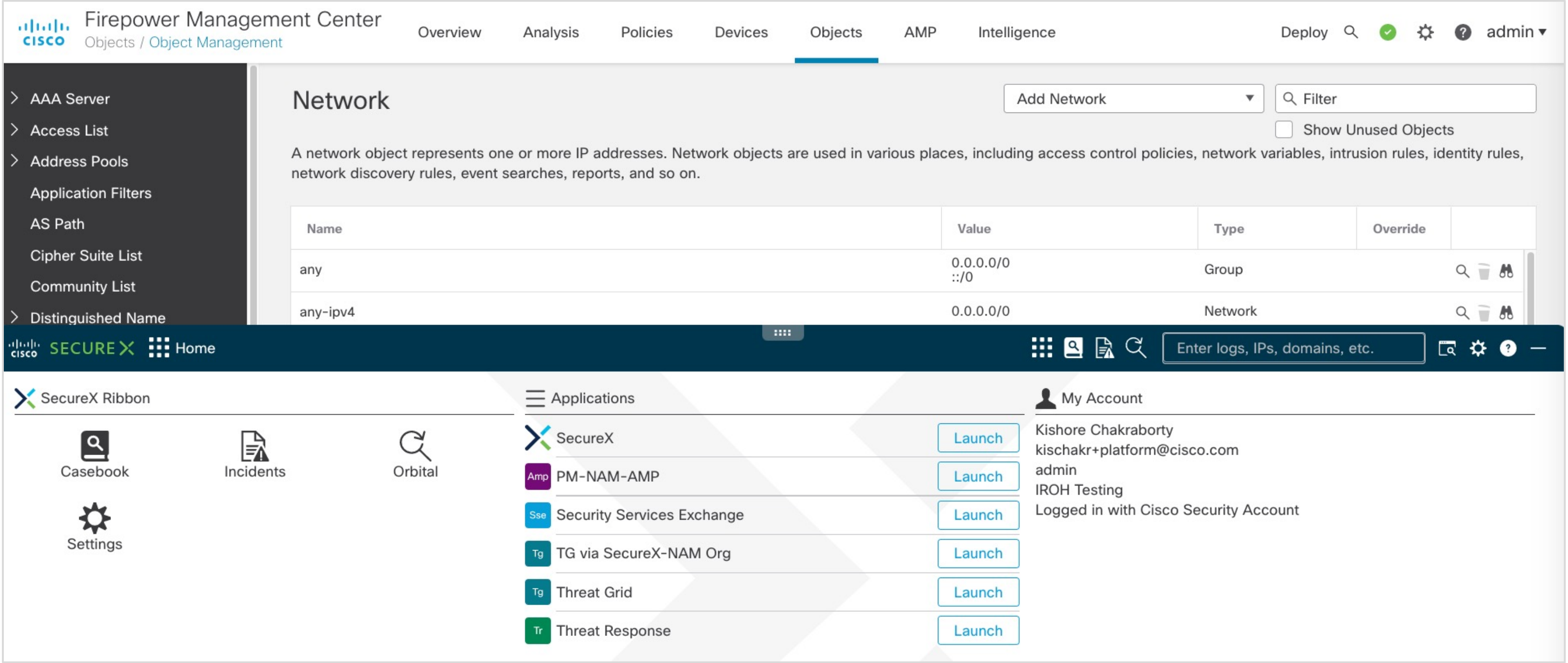
Используйте бесшовный рабочий процесс

FTD предоставляет события безопасности для реагирования на угрозы SecureX



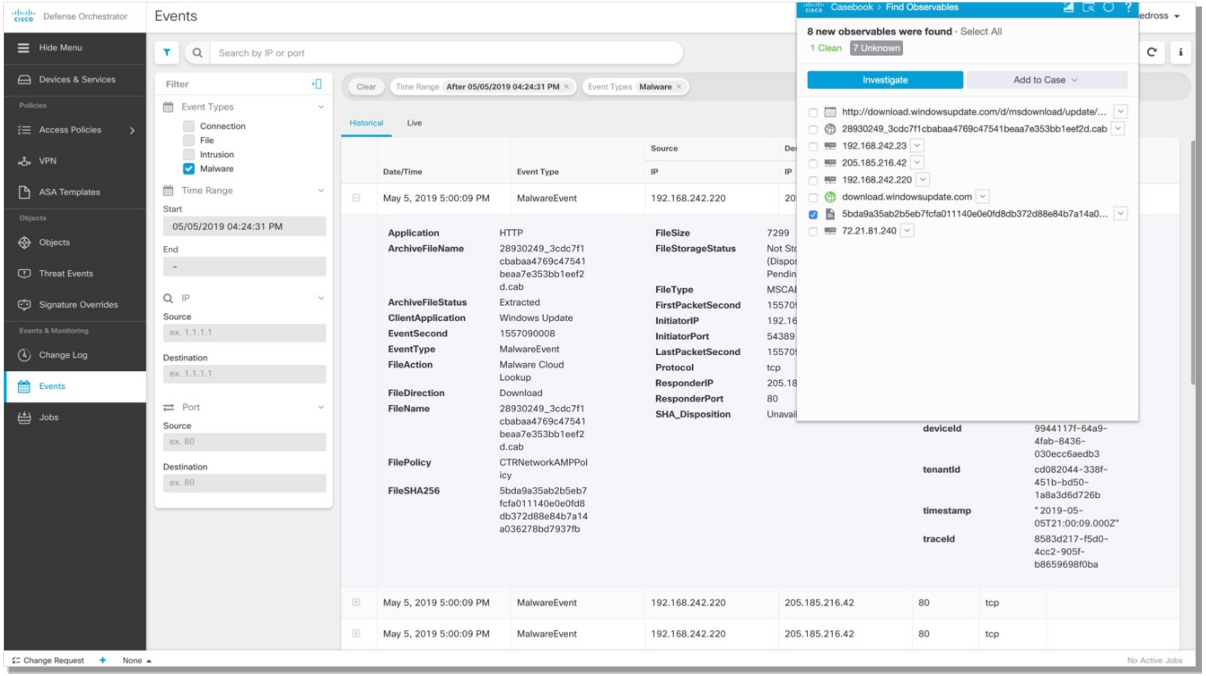
- В облаке хранятся ограниченные данные
- FMC может отправлять события IPS в SecureX threat response
- Любой IP, домен, файловый хеш или IoC в FMC может быть запрошен в SecureX threat response, снижая сложность и время поиска угроз
- Непрерывный анализ с ретроспективой облегчает исправление и расширяет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

Расширение FMC SecureX Ribbon



SecureX threat response и интеграция CDO

Переход к threat response из CDO с помощью event viewer



Дополнительная информация по SecureX

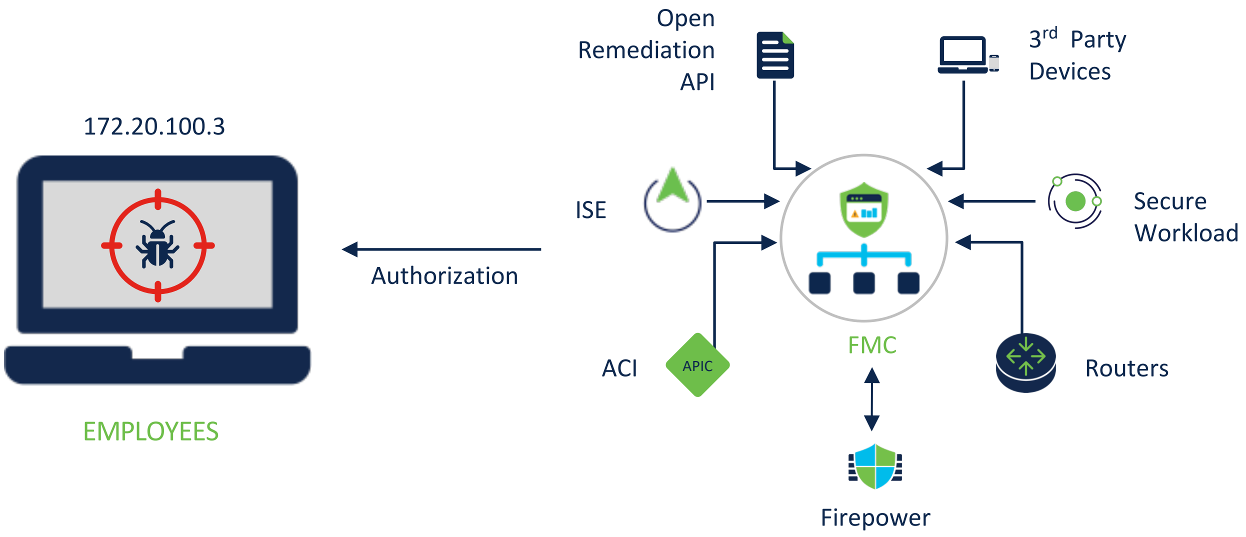
- Вебинар XDR. Как мы это себе представляем
  - Запись вебинара https://youtu.be/E_Sq4VdFKcg

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)

Extend access remotely ▶ Protect important data ▶ Maintain application performance ▶ Support multiple sites

Protect Your Network Using AMP

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

Breadth and Control points

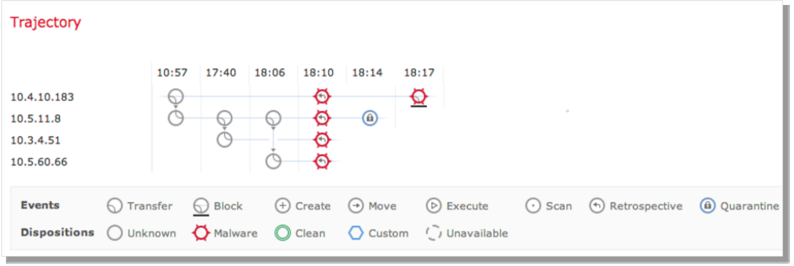
Email
Endpoints
Web
Network
IPS
Devices

Threat Visibility

Retrospective Detection
Behavioral IoCs
File Trajectory
Threat Hunting

Telemetry Stream

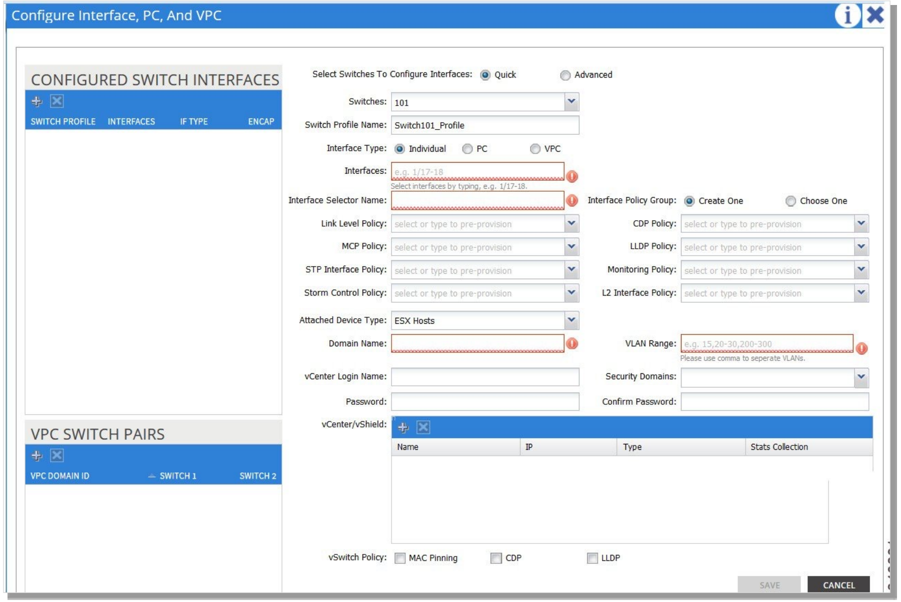
File and Network I/O
File Fingerprint and Metadata
Process Information
Talos and Malware Analytics Intelligence



Application-Centric Infrastructure

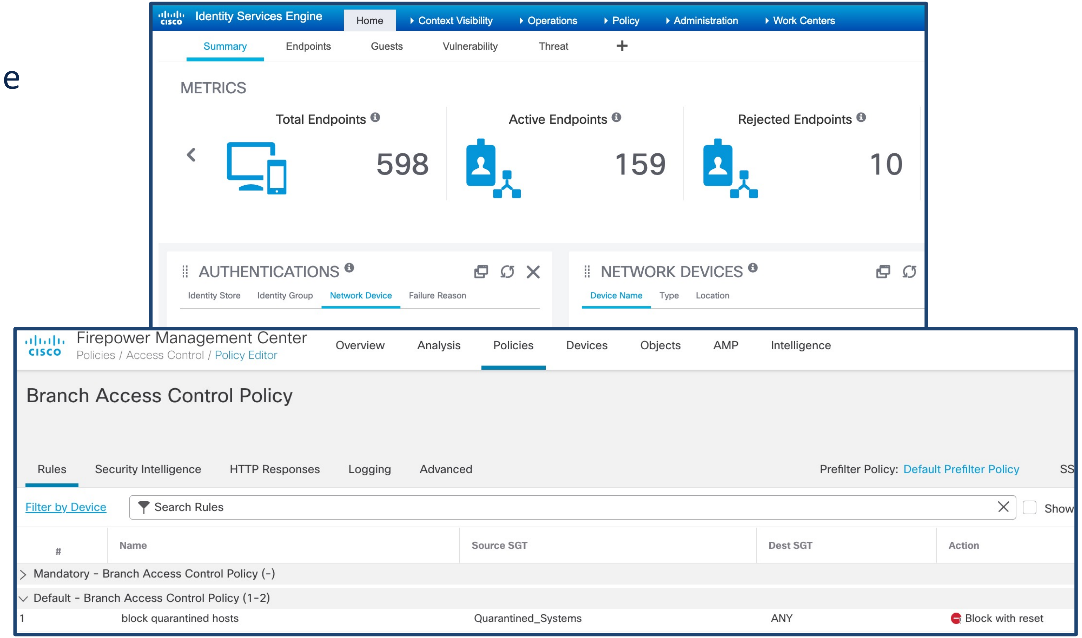
Transparent policy-based security for both physical and virtual environments

- 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

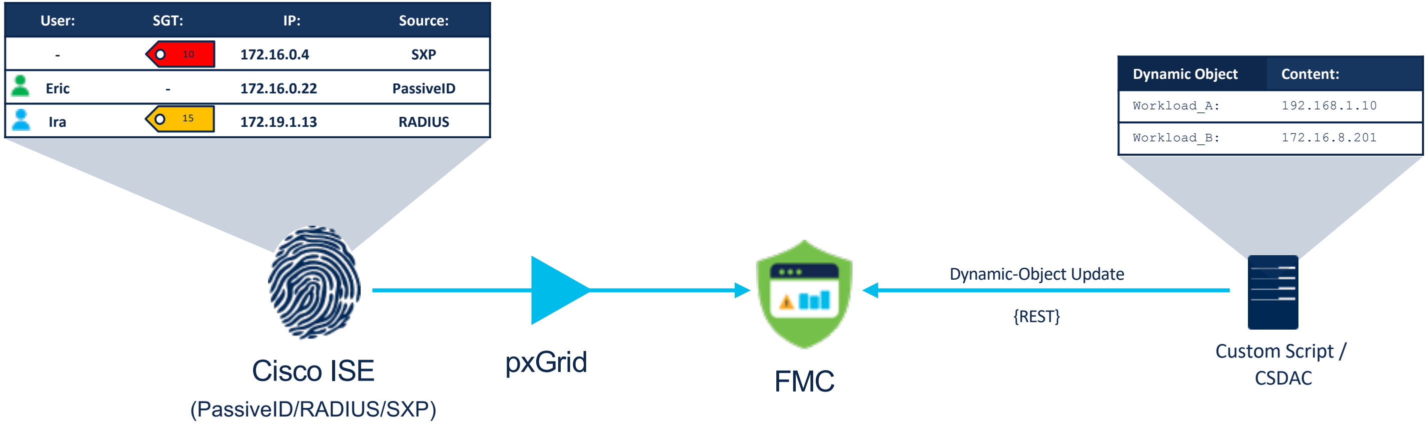


Control Traffic Based on User Awareness

- 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



Identity Mapping Propagation



Simplify Security Management with TrustSec

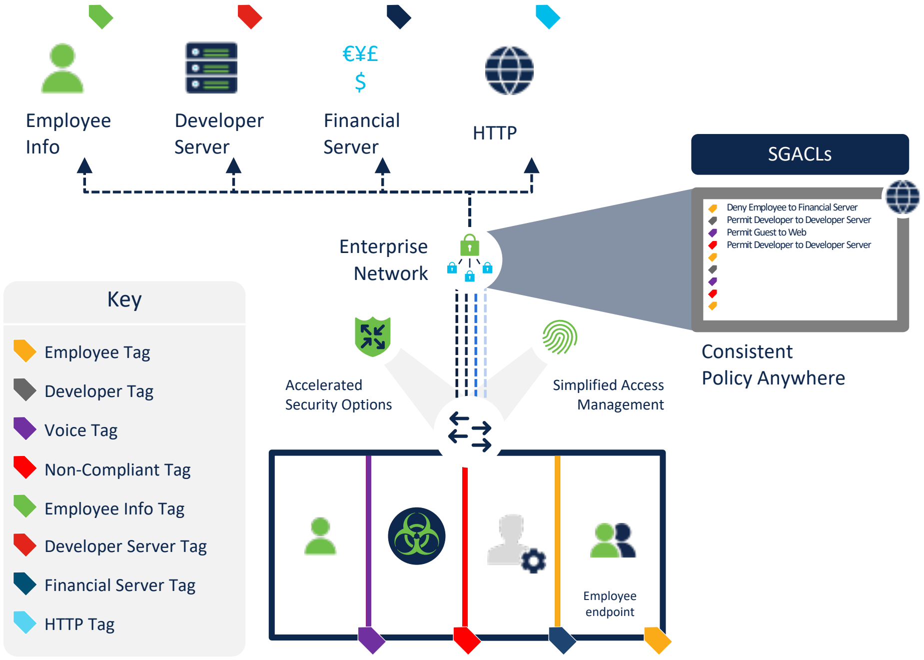
Leverage the network and investment

- 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

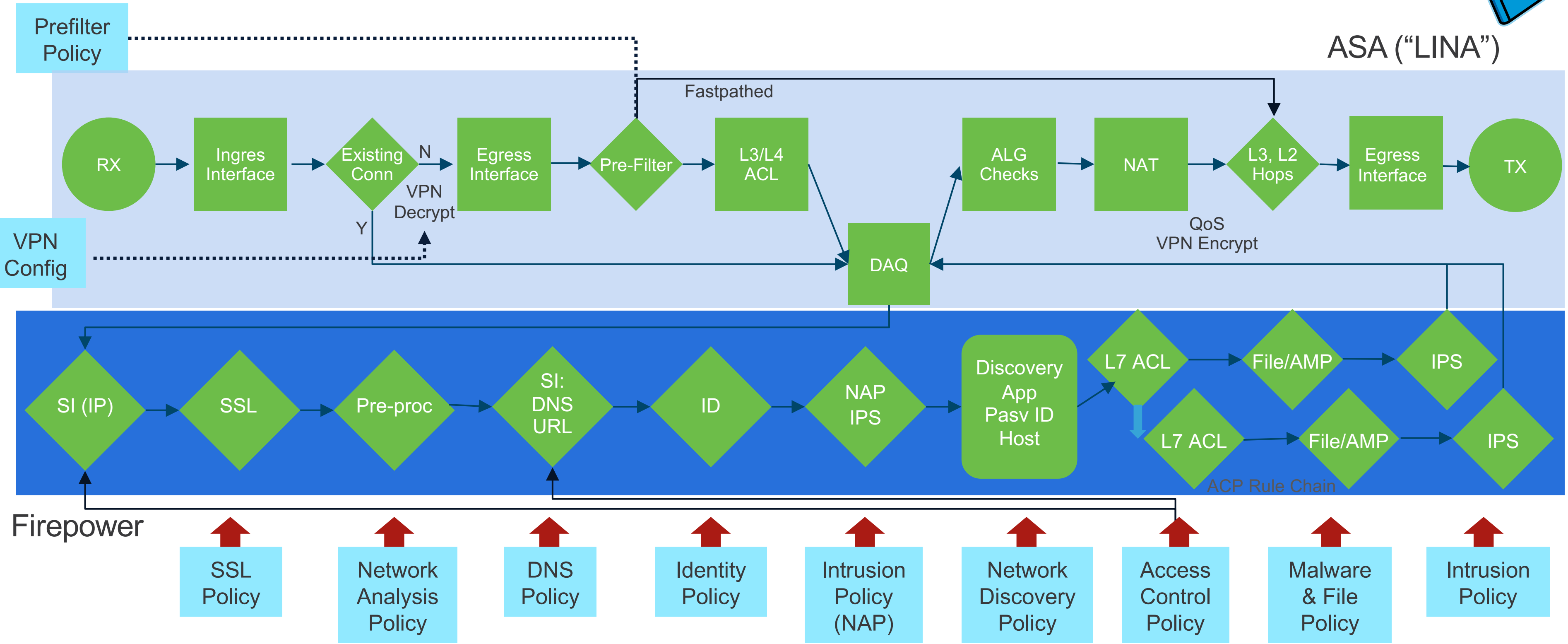
Rapid Security Administration
Speed-up adds, moves, and changes, simplifying firewall administration to speed up
server onboarding

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



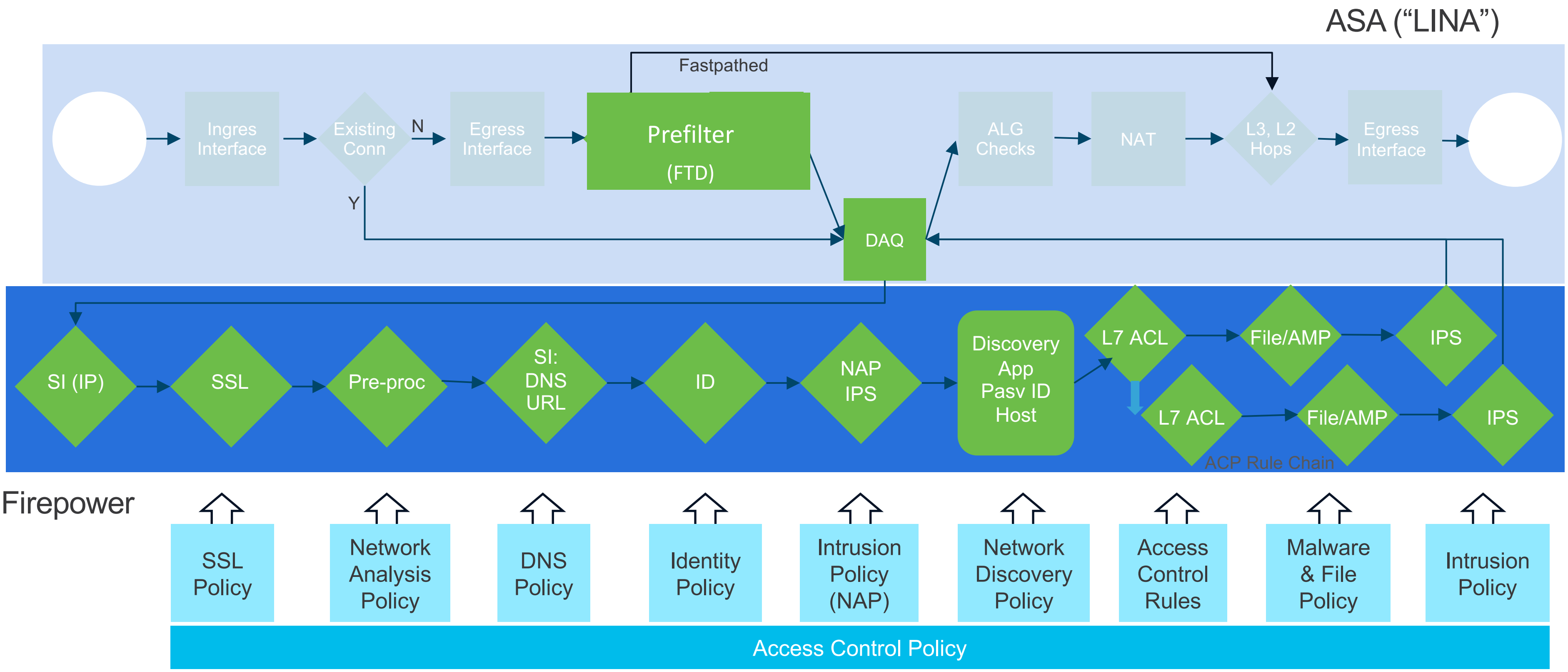
Отдельные заметки по работе с политиками

Пакеты и политики: как знать, где что происходит



106

Пакеты и политики: как знать, где что происходит



107

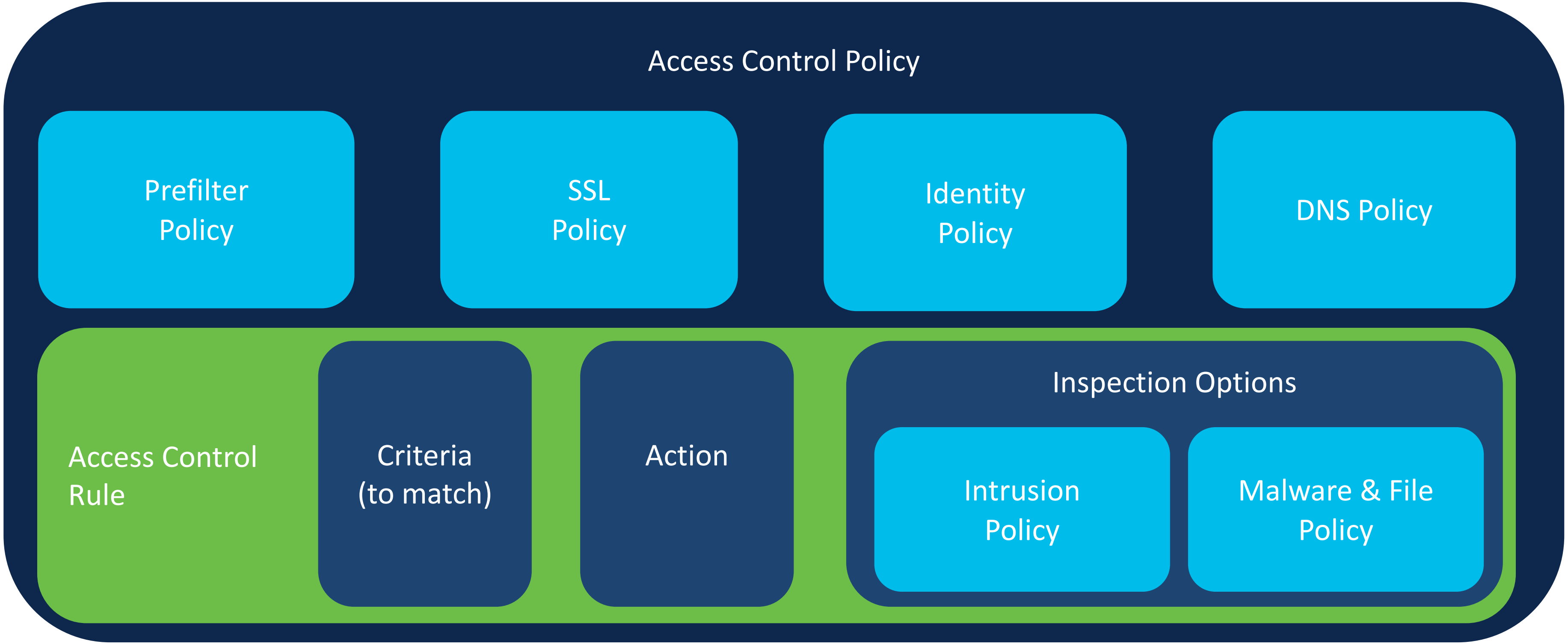
Политики Firepower

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



109

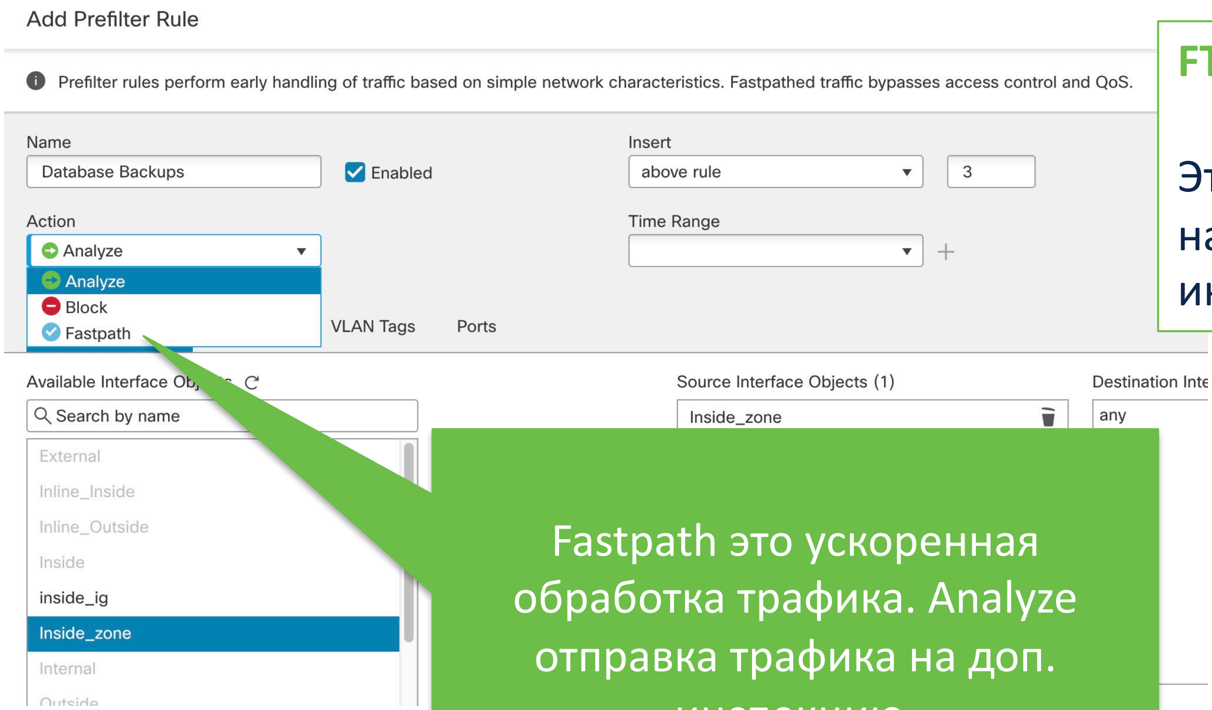
Типы политик NGFW в FTD

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

110

Prefilter Policy



FTD-Only Feature

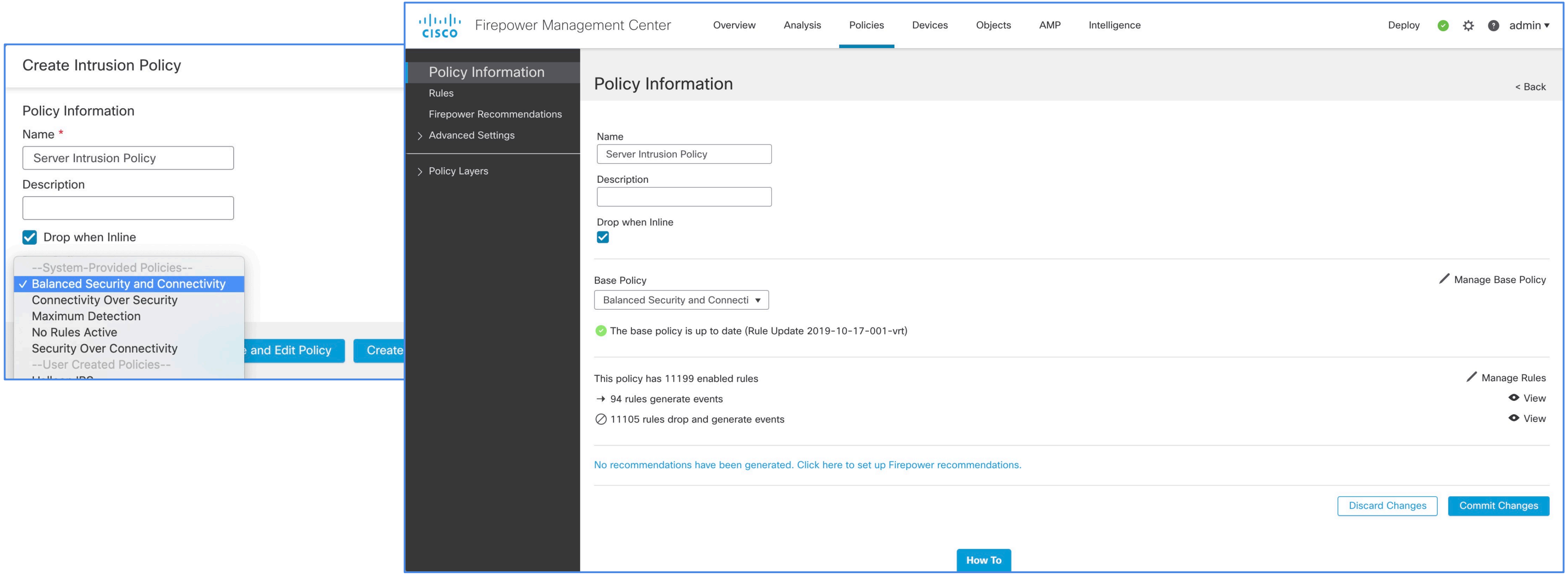
Это первый набор правил, на основании которых инспектируется трафик

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

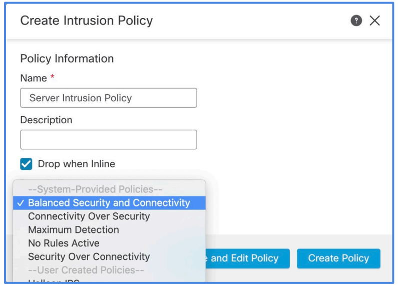
111

Intrusion Policy

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



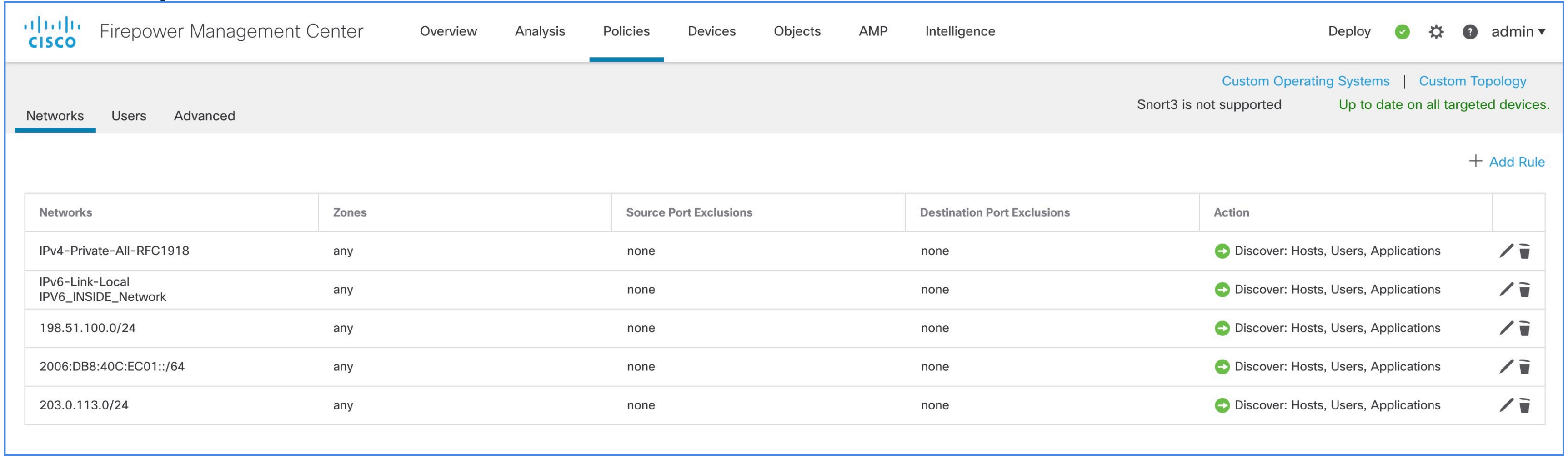
Базовые политики



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

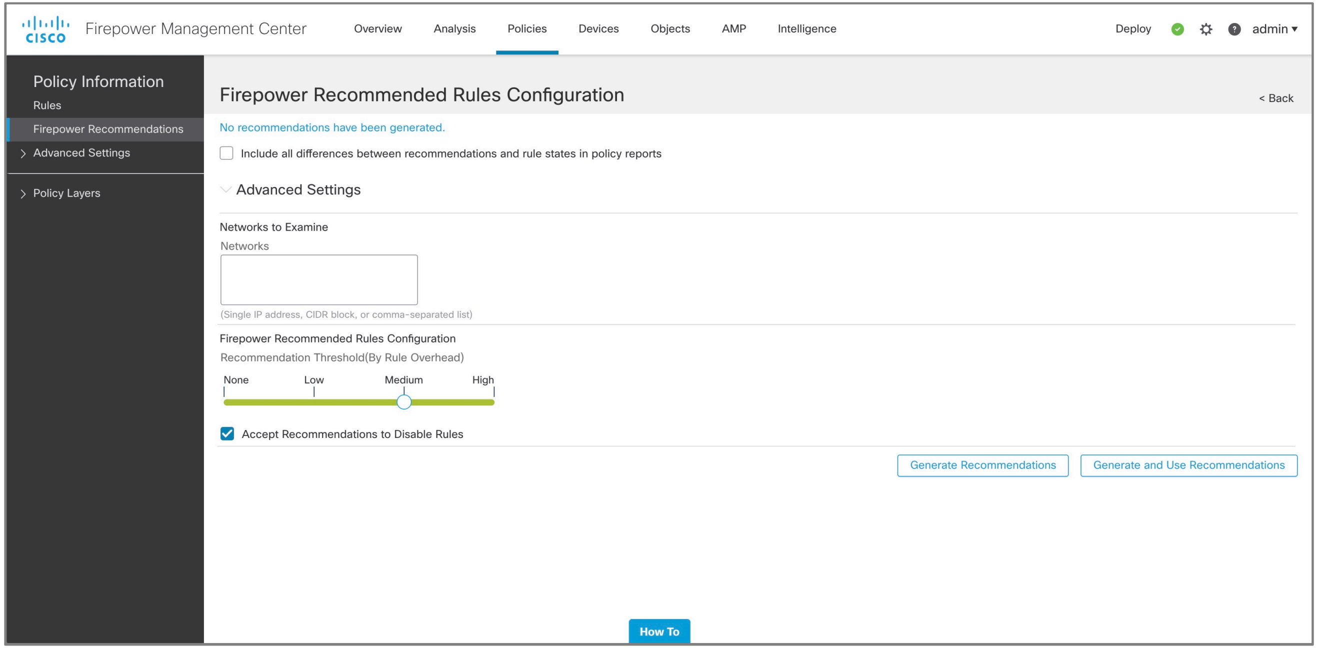
Network Discovery Policy

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



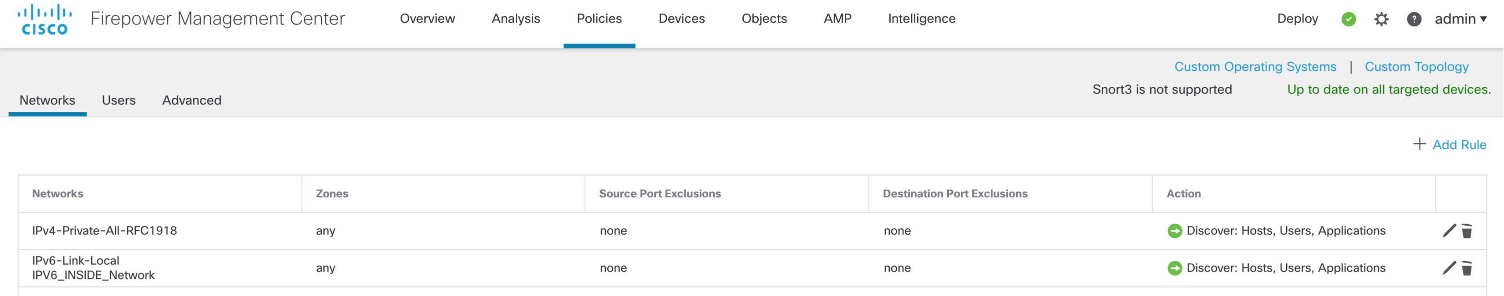
Intrusion Policy и Network Discovery Policy

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



Impact Flags

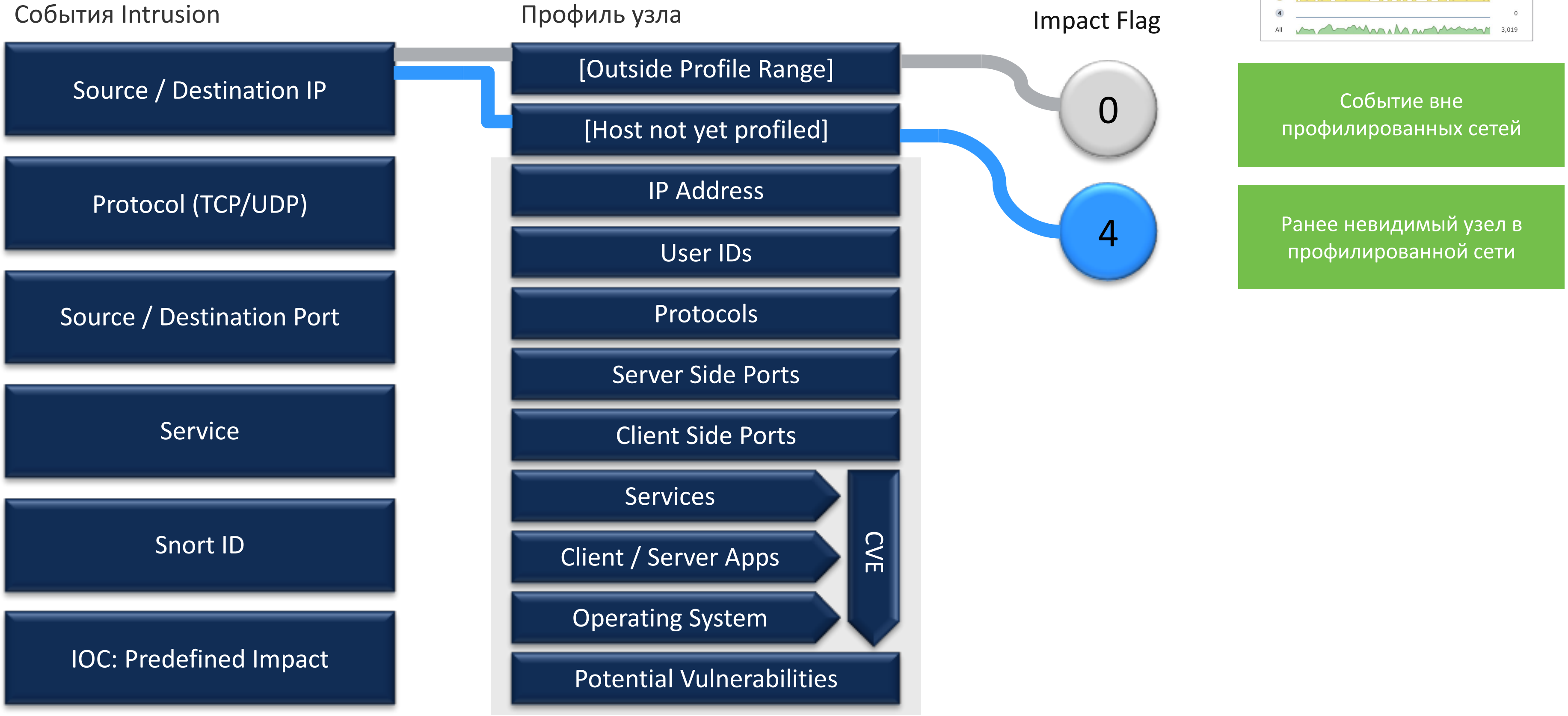
Мы настраивали Network Discovery Policy…

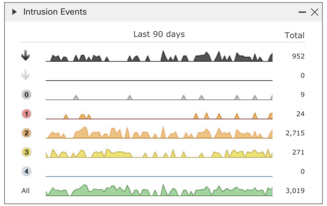


Это включает Impact Flags для анализа.

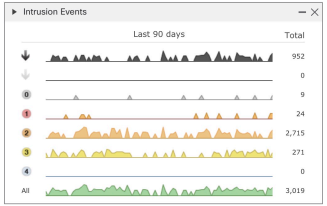
Что это значит?

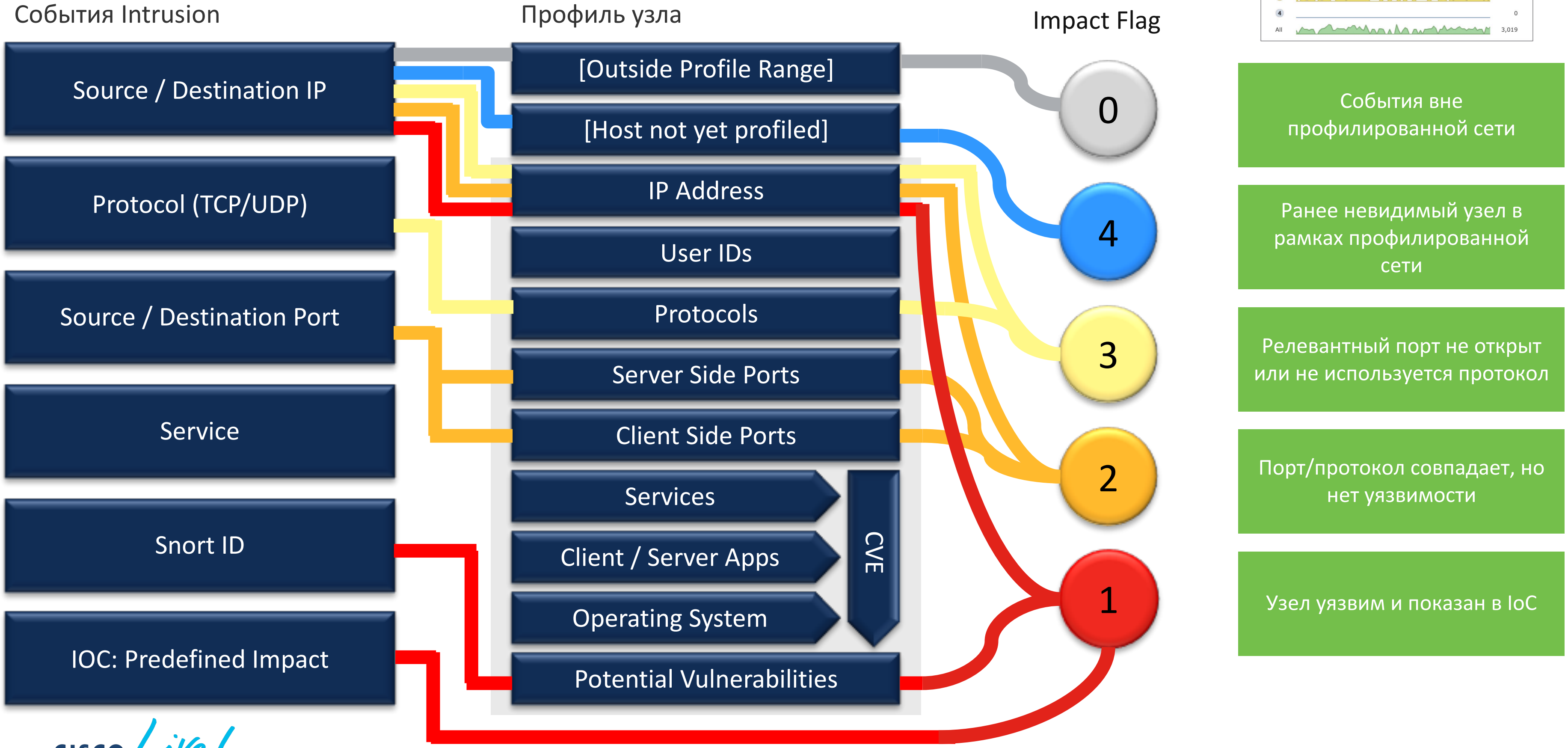
Понимание Impact Flags



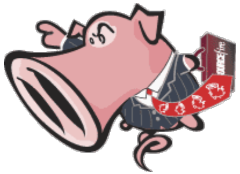


Понимание Impact Flags





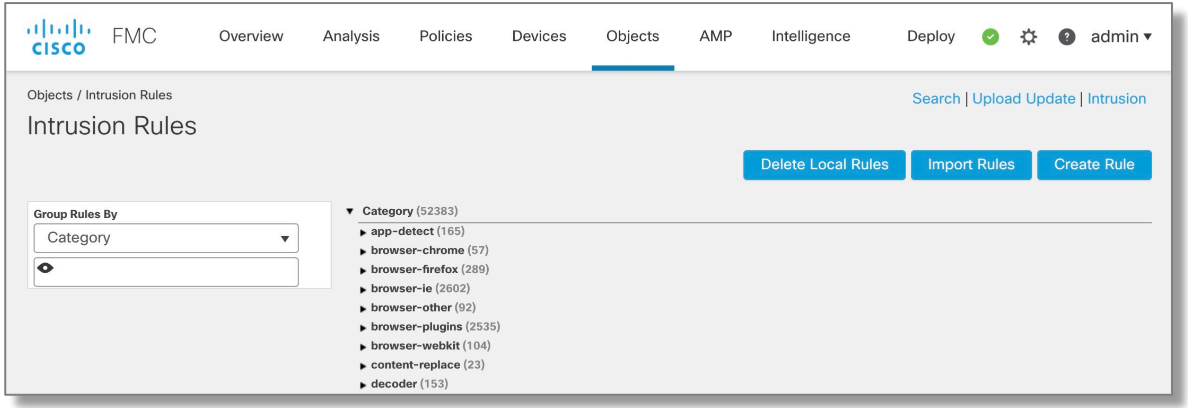
Snort правила



Firepower использует Snort правила для Intrusion Prevention.

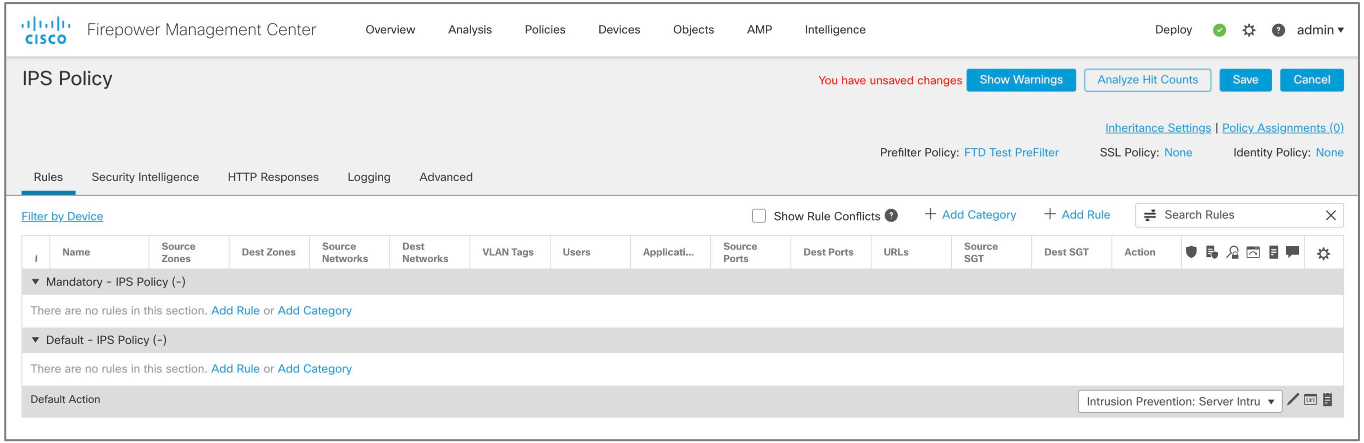
Cisco обеспечивает регулярные обновления правил. Большинство клиентов обновляется автоматом.

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



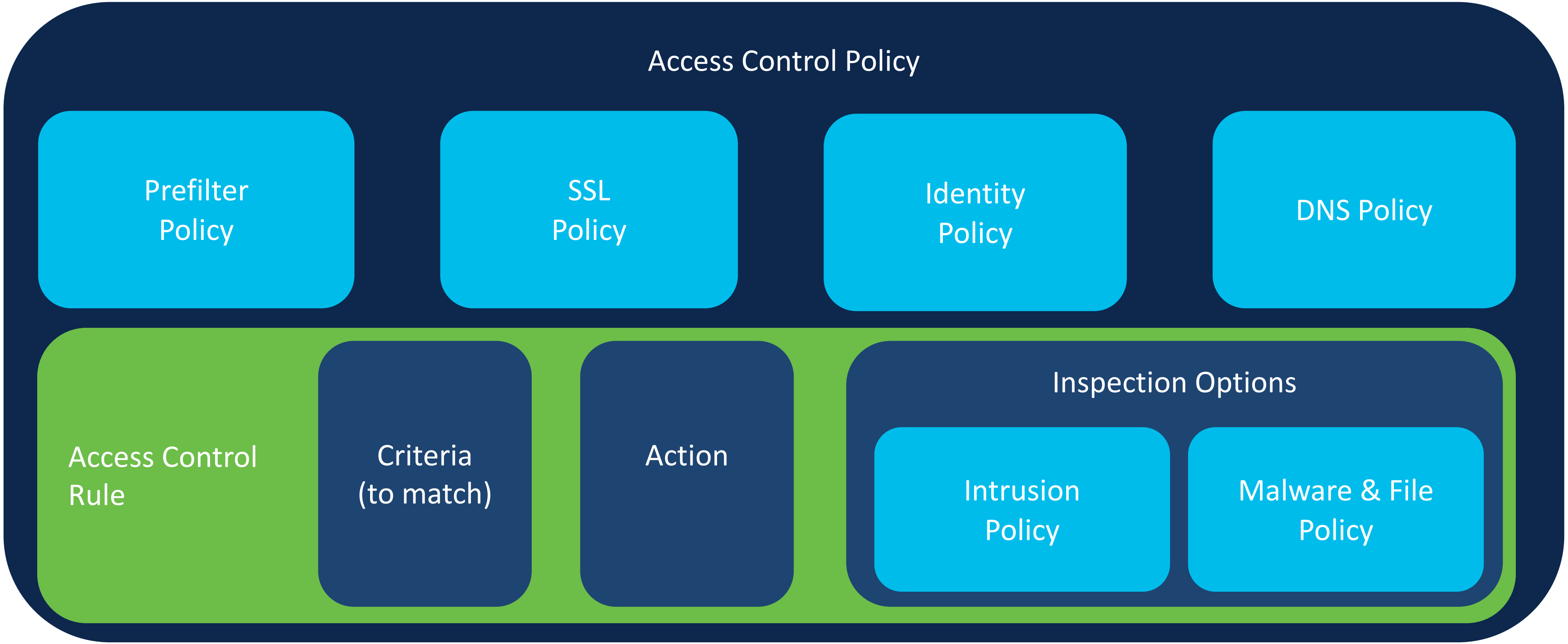
Access Control Policy

Для инспекции трафик должен попасть в Access Control Policy



Access Control Policy

Ключ, который все объединяет

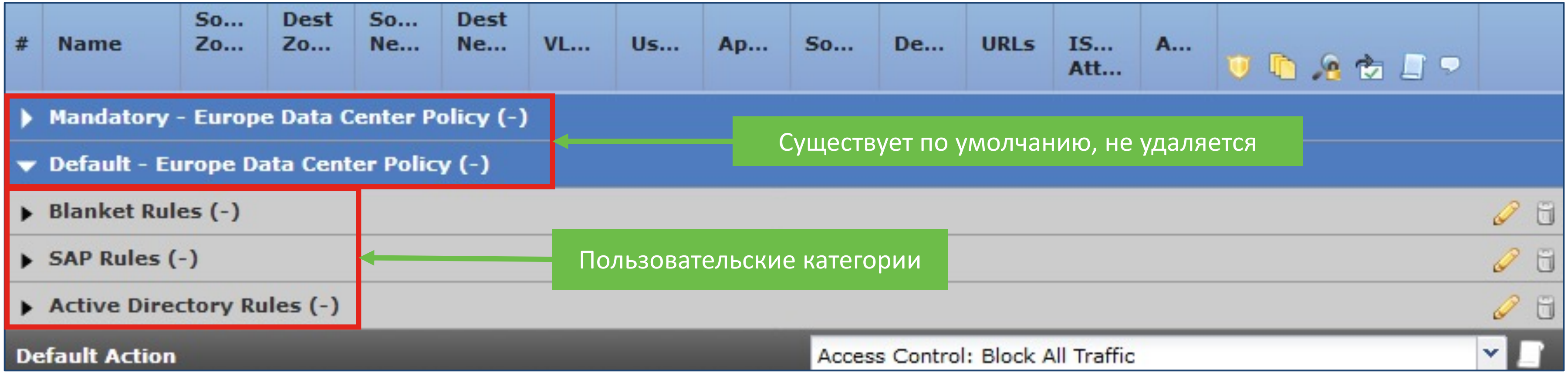


121

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…



123

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 копи, 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

Policy Management Table of Contents:

NGFW Policy Order of Operations

NGFW Policy Order of Operations

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

Table of Contents

NGFW Basic Policy Creation for Firepower

Basic Policy Creation for Firepower

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

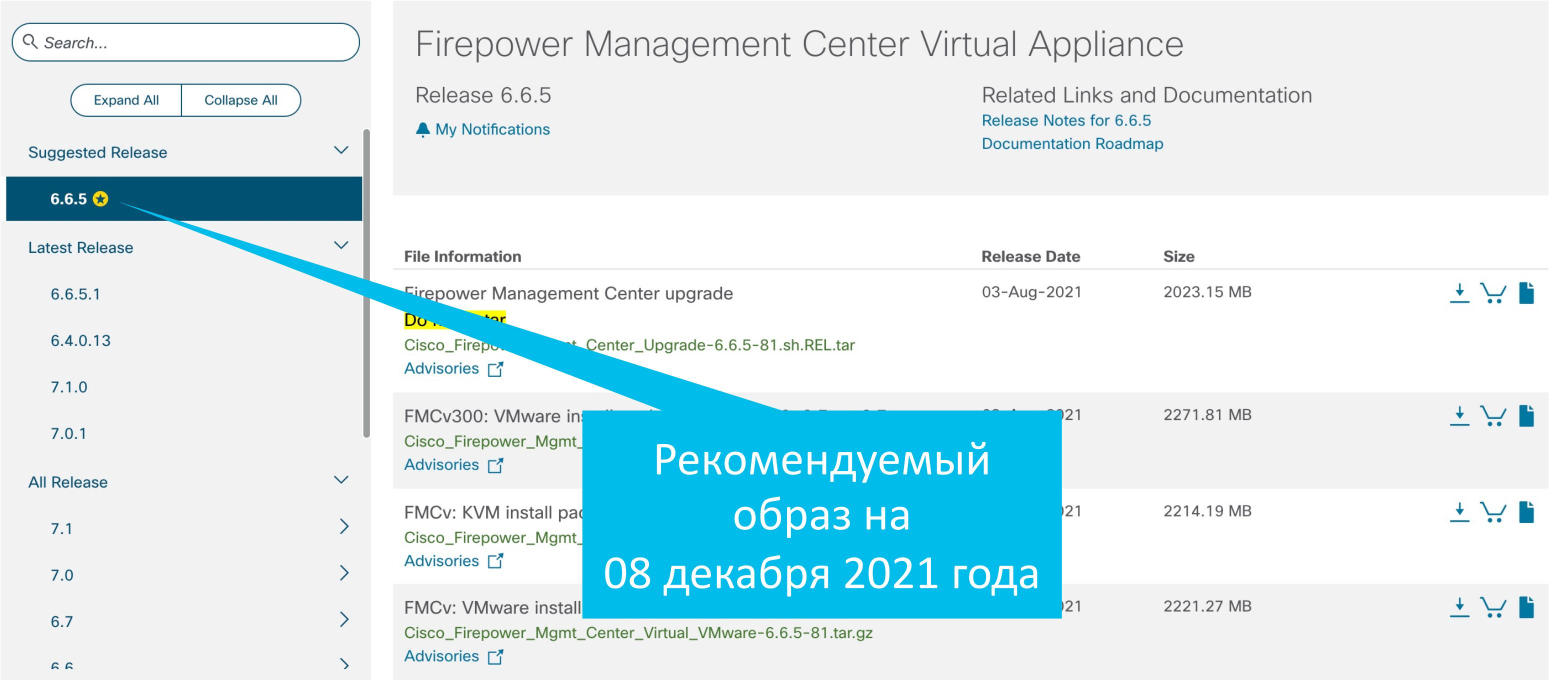
Table of Contents

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

SECURE

Новые и рекомендуемые релизы ПО

Рекомендуемый образ FTD



Firewall Threat Defense 7.0

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

Scalable Eventing and Logging	Динамические объекты для быстрых изменений	Проще в использовании	Улучшение обнаружения угроз	Публичные облака и виртуализация
Просмотр событий в реальном времени, масштабируемое хранение событий и логирование на площадке с использованием SAL	Политика на основе атрибутов добавляет динамические сетевые объекты в политику АС	Унифицированные метрики состояния (через SNMP), Дэшборд состояния для FMC, Управление изменениями (откат, просмотр изменений, улучшенный аудит, поиск и фильтрация)	Улучшено обнаружение угроз с важным архитектурным изменением: появление Snort 3 с FMC	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 пользовательских 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

CISCO SECURE

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 (VTIдля 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

Snort 3

- Elephant flow visibility
- Encrypted Visibility Engine
- Intrusion Rule Recommendations
- Additional rule actions

VPN Management

- 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

Public Cloud

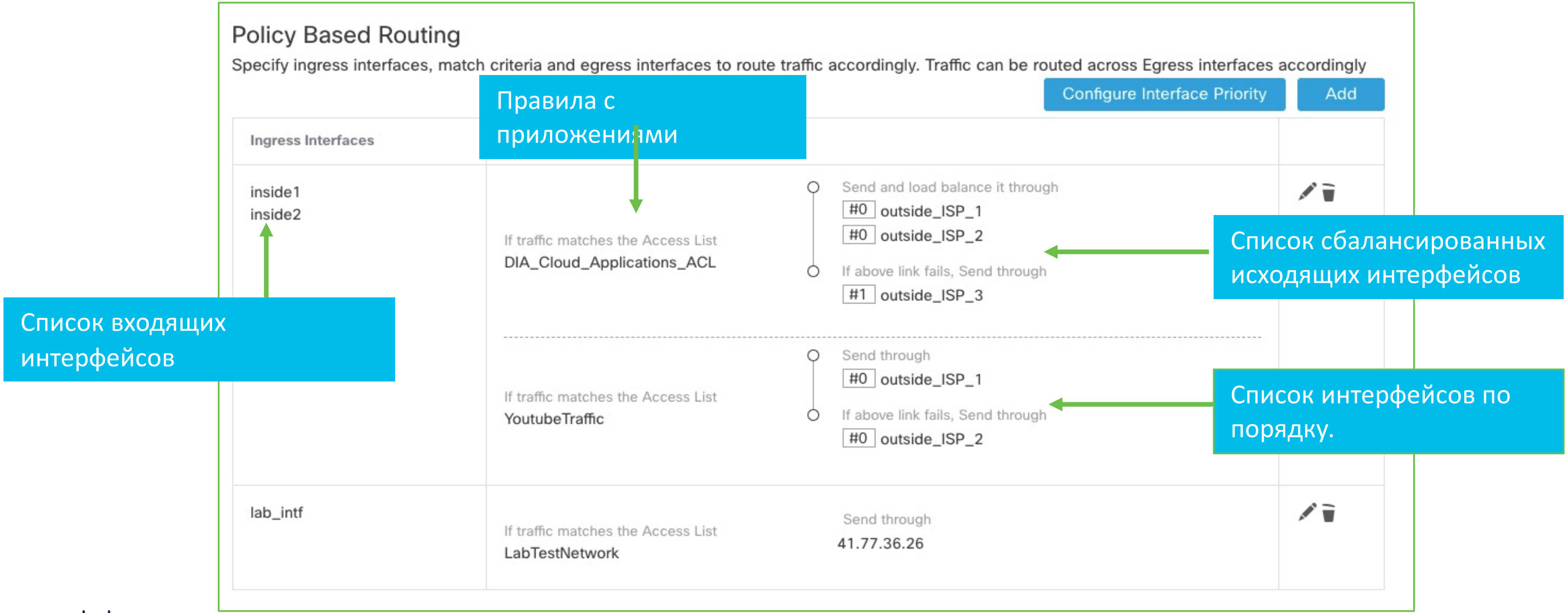
- Additional instance type support in AWS, Azure
- FMCv HA and FMCv300 in AWS and OCI
- Geneve AWS proxy support
- Automated FTDv horizontal scaling in OCI
- AWS CloudWatch health monitoring integration

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.



Упрощенное развертывание для региональных офисов

Secure Elastic Connectivity

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

Высокая доступность с около нулевым временем восстановления

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

Увеличение полосы пропускания (7.1)

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

Прямой доступ в Internet и для гостевого трафика (7.1)

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

Упрощенное управление

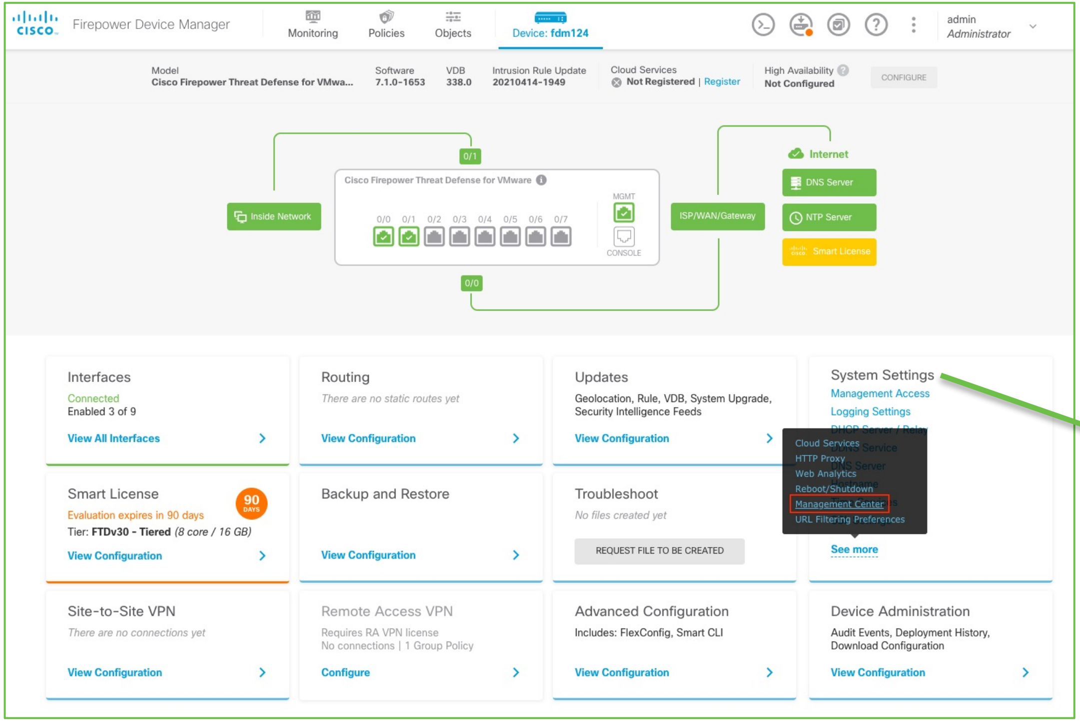
- Low Touch Provisioning
- Data Interface Management
- Auto Config Rollback (7.1)
- FDM Driven Onboarding (7.1)

Обзор функционала

How it Works

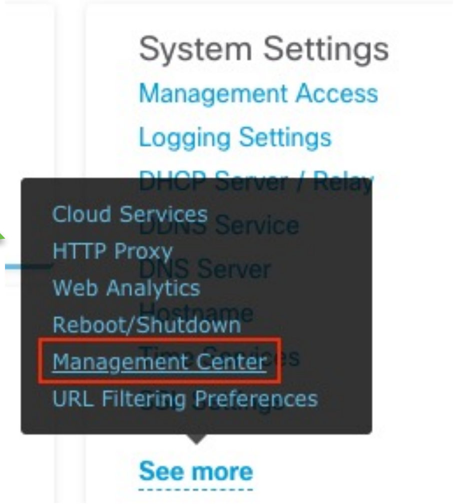
- FTD API (и FDM) могут использоваться для настройки FMC
  - Использует доступ к интерфейсу данных
  - Использует доступ к интерфейсу управления
- Какой менеджер: FDM и FTD REST API
- Ограничения
  - Не поддерживаются FTD в HA режиме
  - Не поддерживаются FTD с Universal PLR
  - FTD с FlexConfig не поддерживается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

Device > System Settings > Management Center



Management Center может запуститься:

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



Готовы начать?

Обновите свой Firewall сегодня!

Подпишитесь на бесплатный trial:

Тестирование и Heath Check Firepower

Тестирование Cisco Defense Orchestrator

Спасибо