Обзор современных решений Cisco Security

Удвоение возможностей SD-WAN и искусственного интеллекта

Самый высокопроизводительный брандмауэр SD-WAN на рынке, работающий на основе искусственного интеллекта

Secure Firewall 1200 Series Compact

Firewall Threat Defense (FTD) версия 7.6

Ruslan Shaimardanov
ruslan.shaimardanov@figurait.kz

figura

ПОЧЕМУ МЫ?

IT-рынок Казахстана показывает уверенный рост на протяжении последних лет, на нём представлены крупные вендоры, оказывающие поддержку и предлагающие дополнительные услуги.
По этой причине для успешного ведения IT-проектов важно не иметь не только налаженные каналы продаж, но и надежную команду опытных технологических экспертов и инженеров, доступ к обновлениям ПО, возможность работы с вендорскими инструментами и базами знаний – всё это отличает интегратора от бокс-мувера.
У команды Figura IT – есть все необходимые ресурсы!

70% экспертов и инженеров компании обучены по стандартам и сертификациям вендоров - Cisco, HPE, Aruba, Dell и др.

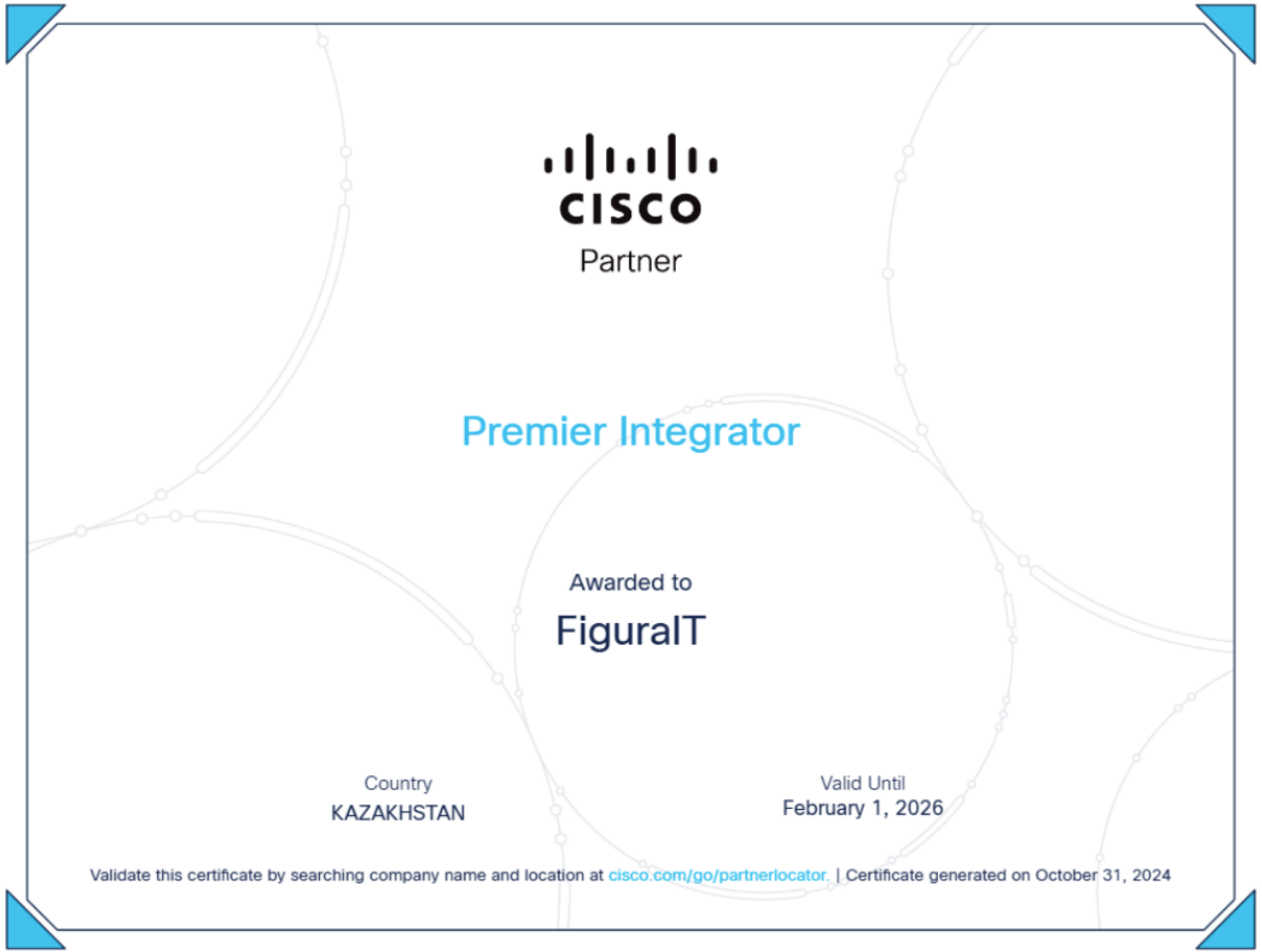
Оказываем **полный цикл** реализации проектов

Процессы системной интеграции выстраиваются с использованием лучших практик таких вендоров, как HP и Cisco

Область экспертизы:

cisco · Hewlett Packard Enterprise · hp UX · DELL EMC · HUAWEI · macrosan · CHECK POINT · Linux · MICRO FOCUS · BROCADE A Broadcom Company · VEEAM · citrix

vmware · UserGate · Nettrix宁畅 · Lenovo · aruba · xFUSION · MAIPU · FORTINET · Microsoft · Sugon · Synology



- Современные решения от Cisco сегодня это:
- более выгодные по цене - это уже не так дорого, как об этом мы знали ранее.
- могут быть доступны уже со склада в Казахстане.
- при размещении под заказ могут приехать к заказчику за 30-50 дней.
- можно построить надежное и безопасное решение на Cisco достаточно бюджетное и быстро.

Референсная архитектура безопасности

figma cisco.com/go/sra

TALOS THREAT INTELLIGENCE — Actionable threat intelligence | Collective responses | Comprehensive visibility | Signal identification | Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

Cisco Vulnerability Management | Secure Analytics XDR | Secure Client | Talos Incident Response

SERVICES: Custom threat research on demand | Implement and manage | Incident response retainer | Managed detection & response | Strategy & assessment

CAPABILITIES: Network detection & response | Device discovery & insights | Endpoint detection & response | Open API platform & 3rd party native integrations | Risk-based vulnerability management | Identity Threat Detection & Response | SOAR | SIEM | Threat visibility, incident response & threat hunting

ZERO TRUST

SASE

User / Device Security

Cisco Secure Client (AnyConnect) | Umbrella | Secure Endpoint | Meraki Systems Manager | Duo | Secure E-mail | ThousandEyes

Cloud managed | VPN | Telemetry Visibility | Endpoint detection & response | DNS—layer security | Secure web | Anti-virus Anti-malware | Query | Host FW | Mobile device management | Risk-based MFA | Password-less | Device trust | Identity Intelligence | Email, Phishing, SPAM, BEC,DLP, content filtering | Digital experience monitoring

Cloud Edge Network

SASE/Security Service Edge

Duo | Secure Access | Umbrella | Secure Connect

- Browser access control
- Cloud access security broker
- Cloud malware detection
- Data loss prevention
- DNS-layer security
- FWaaS
- Identity / posture
- RAaaS
- Remote browser isolation
- Secure web gateway
- TLS decryption
- Zero Trust Network Access
- Tenant restrictions

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall | ThousandEyes | Catalyst

- Analytics
- Application performance optimization
- Cloud based orchestration
- Cloud OnRamp
- Digital experience monitoring
- Group tag propagation
- IPSecVPN
- Integrated security
- Middle mile optimization
- Segmentation
- Visibility

In the Office/Managed Location

Catalyst Center | ISE | Meraki | Secure Firewall | Secure Network Analytics | Secure Web Appliance

- Application network gateway
- Configuration orchestration
- Content filtering
- Encrypted visibility
- Zero Trust Network Access
- Group tag classification
- Identity/pxGrid Cloud
- Network access control
- Network security analytics
- NGFW
- NGIPS
- Security analytics & logging
- Segmentation
- Threat mitigation
- Profiling

Industrial Threat Defense

DNAC | CyberVision | Industrial Networking | ISE | Secure Firewall | Secure Network Analytics

- Anomaly detection
- Compliance
- Group tag classification
- Identity pxGrid
- Ruggedized
- Segmentation
- Threat mitigation
- Visibility

Workload, Application, and Data Security

ACI | Attack Surface Management | Panoptica | Radware | Secure Application | Secure Endpoint | Secure Firewall | Multicloud Defense | Secure Workload | Hypershield

Hybrid Multicloud Infrastructure

DDoS WAF/Bot | Identity pxGrid | Macro segmentation | Flow analytics | Threat mitigation | Deployment automation | Firewall NGIPS | Defense gateway

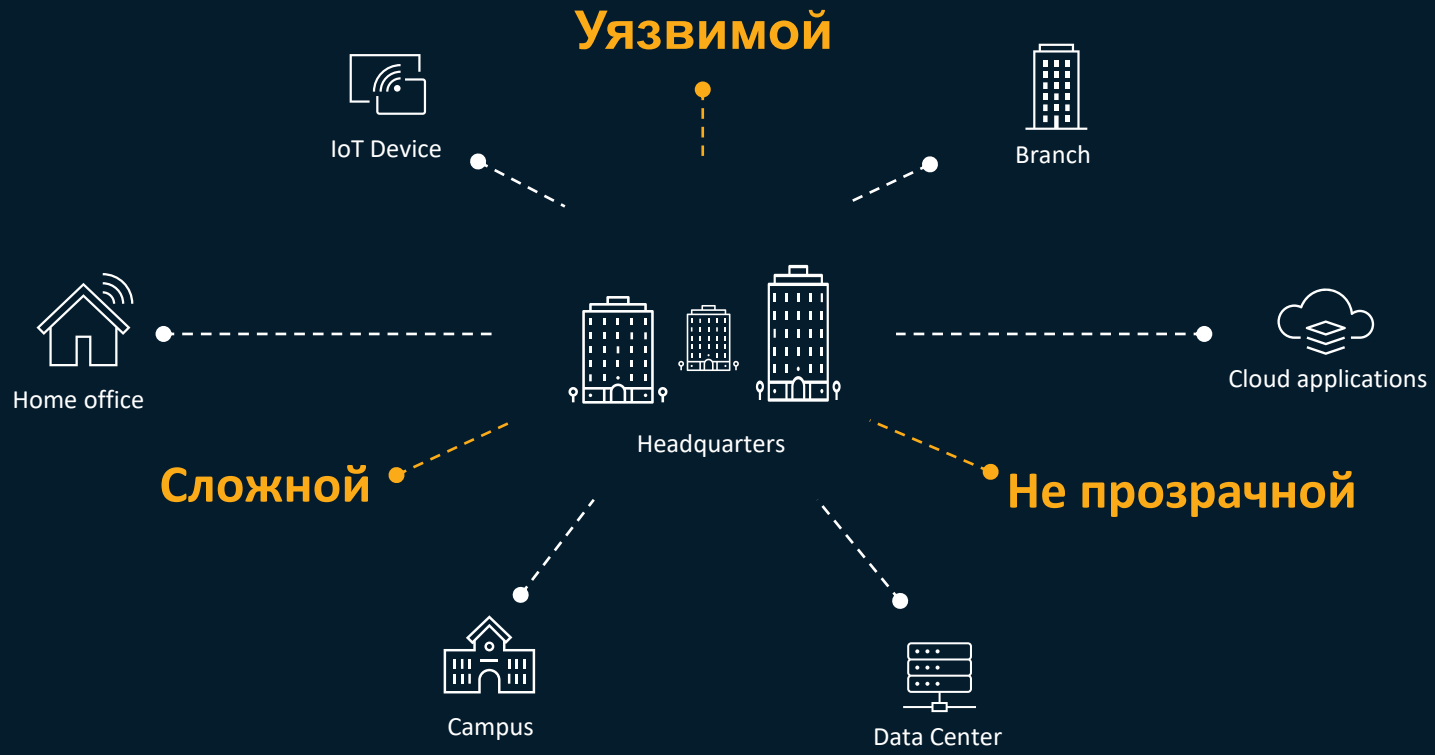
Cloud Native Application Platform

External Attack SM | CSPM/ CAASM | Micro segmentation | API security | App discovery & observability | Code+CI/CD security | Container security | DSPM | Run-time protection

Platform Capabilities
Cisco Security Cloud

CLOUD-BASED | Identity Intelligence | MULTICLOUD | UNIFIED MANAGEMENT & POLICY | AI / ML DRIVEN | OPEN & EXTENSIBLE

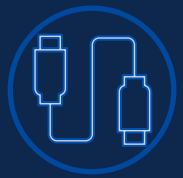
Ваша сеть расширяется и становится...



Ваша сеть расширяется и становится…

Проблемы распределенных филиалов

Больше устройств для покупки, больше капитальных затрат



Больше устройств для подключения по всему миру

Больше устройств для обновления и обслуживания

Больше людей, которых нужно найти, нанять и обучить

Несоответствие

Непрозрачная

Немасштабируемая

Безопасный межсетевой экран серии 1200 Compact

Самый производительный и компактный межсетевой экран для распределенных филиалов предприятий.

До
3-кратного
Превосходства
над конкурентами

2x
Цена/производительность
по сравнению с
другими решениями

Превосходная производительность при компактных размерах

Эффективность развертывания, устранение дополнительных аппаратных средств

Обнаружение и управление на основе AI/ML

Безопасный межсетевой экран серии 1200

Самый производительный компактный межсетевой экран с поддержкой SD-WAN для распределенных филиалов предприятия.

Превосходная производительность при компактных размерах

- Повысьте производительность сотрудников за счет увеличения скорости подключения к головному офису или облачным приложениям почти в 3 раза.
- Включите устройства IoT напрямую с помощью UPoE+ или увеличьте производительность компактного межсетевого экрана с помощью портов SFP+.

Эффективность развертывания, устранение дополнительных аппаратных средств

- Развертывайте SD-WAN в нескольких филиалах быстрее с помощью встроенных шаблонов подключения и автоматической настройки.
- Устраните необходимость в приобретении, развертывании и управлении несколькими сетевыми устройствами в филиале.

Обнаружение и управление на основе AI/ML

- Обнаружение зашифрованных вредоносных программ, распространенных угроз и уязвимостей нулевого дня с помощью AI/ML.
- AI Assistant для оптимизированных операций брандмауэра и управления жизненным циклом политик для локальной или облачной среды.

Компактные модели Secure Firewall серии 1200

1220 CX
2x1G or10G SFP+
9 Gbps

1210 CP
4x UPoE+
6 Gbps

1210 CE
6 Gbps

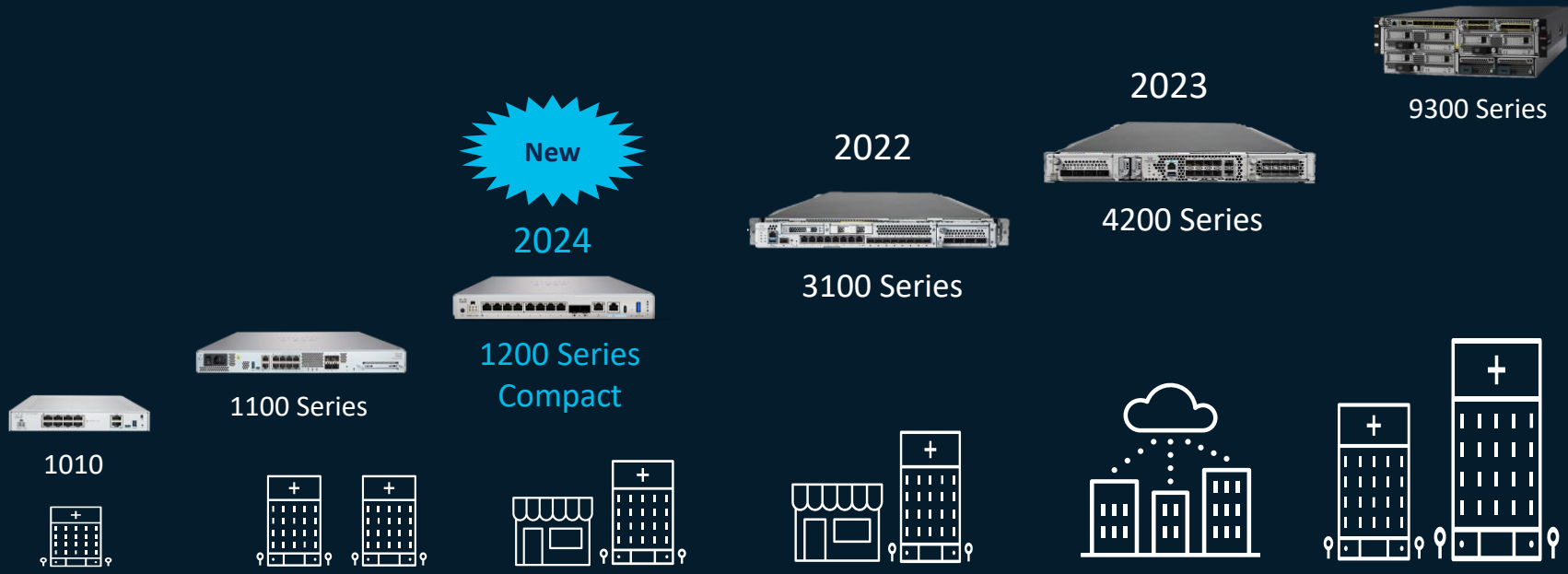
Компактные межсетевые экраны Cisco

Сравнение производительности

До
10 раз
производительность брандмауэра (1010 против 1220)

	1010	1010E	1210 CE	1210 CP	1220 CX
Firewall	0.9 Gbps	0.9 Gbps	6 Gbps	6 Gbps	9 Gbps
IPSec	0.4 Gbps	0.4 Gbps	5 Gbps	5 Gbps	10 Gbps
Ethernet	8 x 1000BASE-T	8 x 1000BASE-T	8 x 1000BASE-T	8 x 1000BASE-T	8 x 1000BASE-T
PoE	-	2 x PoE+	-	4 x UPoE+	2 x 10G SFP+

Портфолио оборудования Cisco Secure Firewall

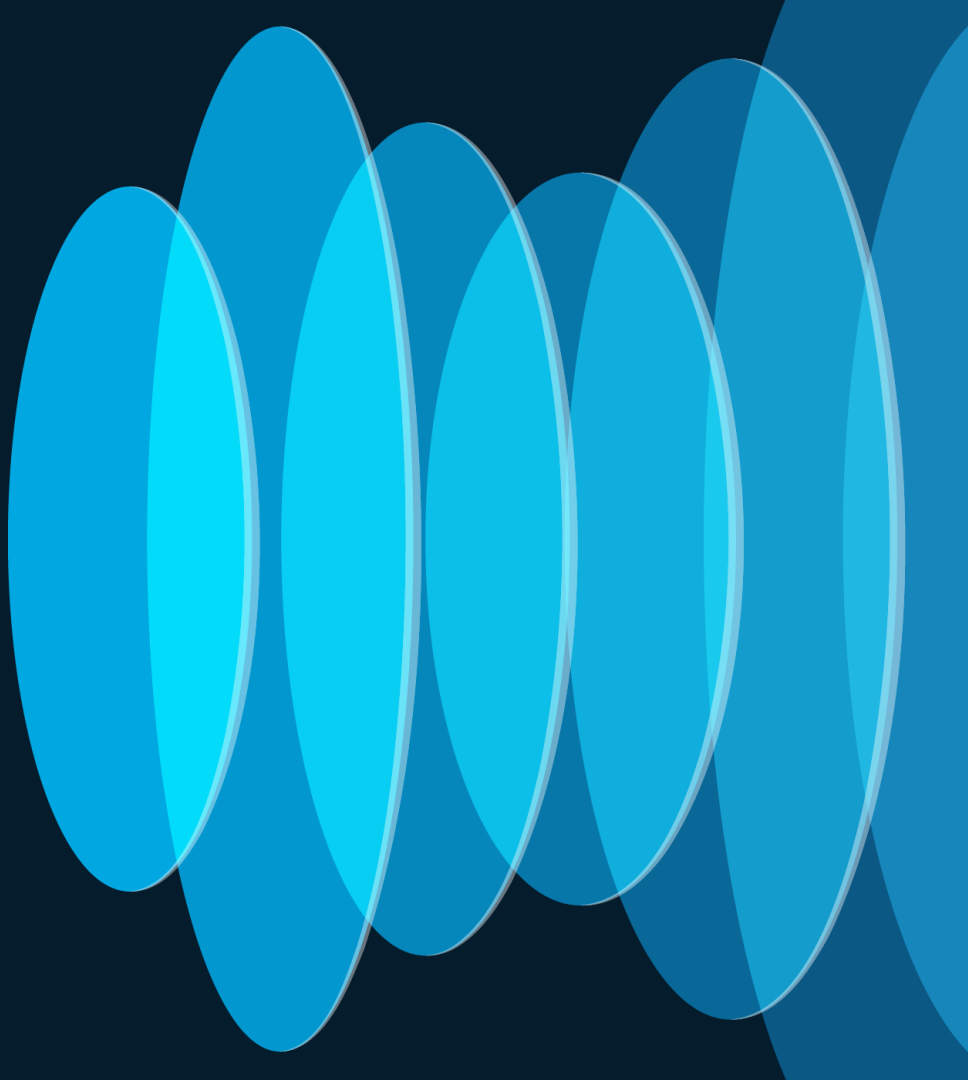


figma

Новое в FTD 7.6

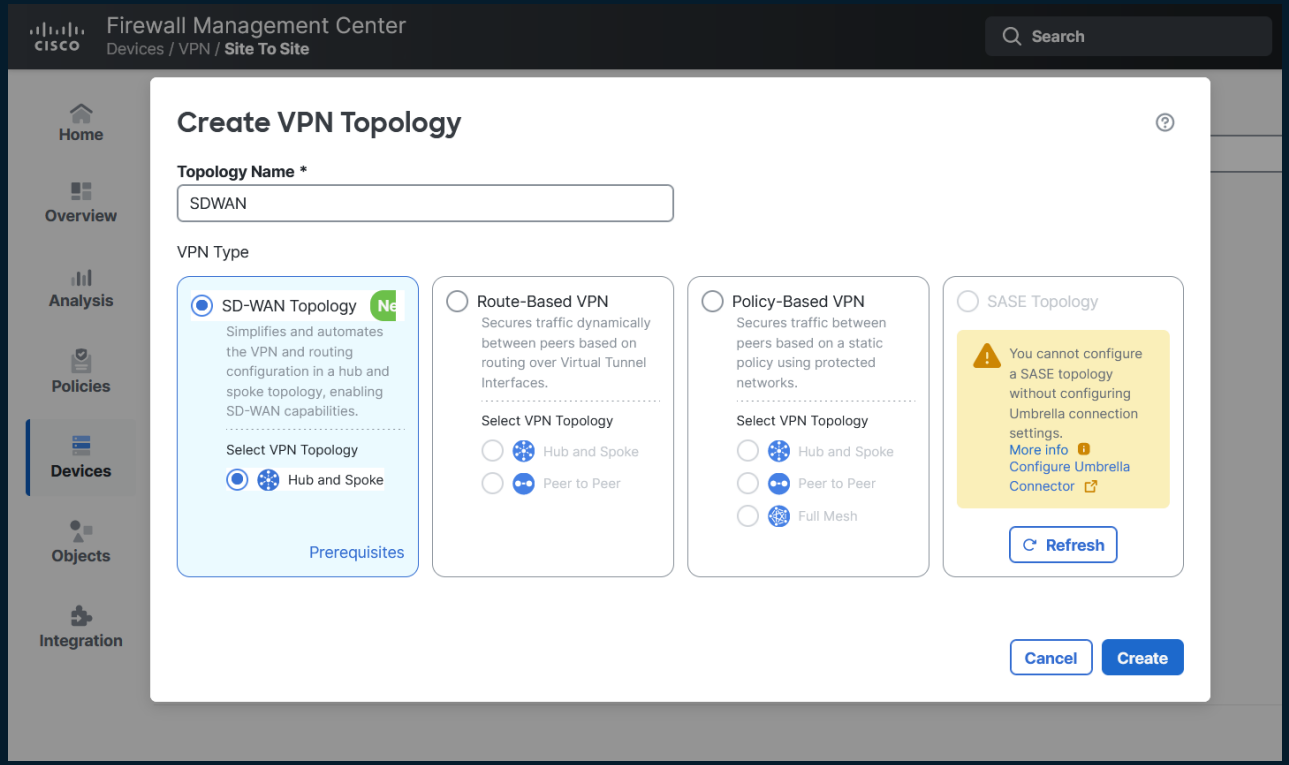
Шаблоны SD-WAN для развертывания

Упрощение внедрения



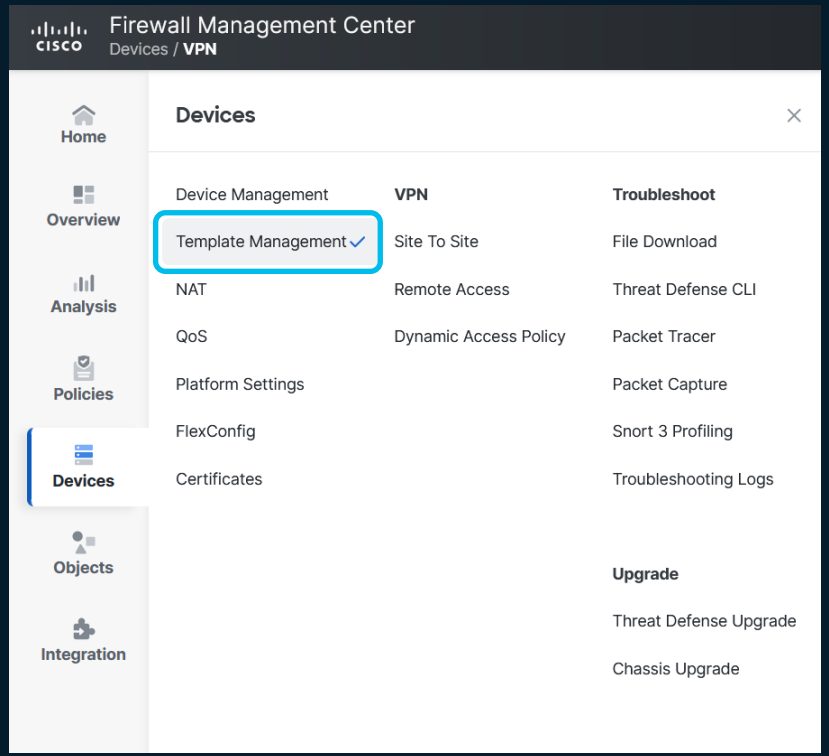
Создание шаблона SD-WAN

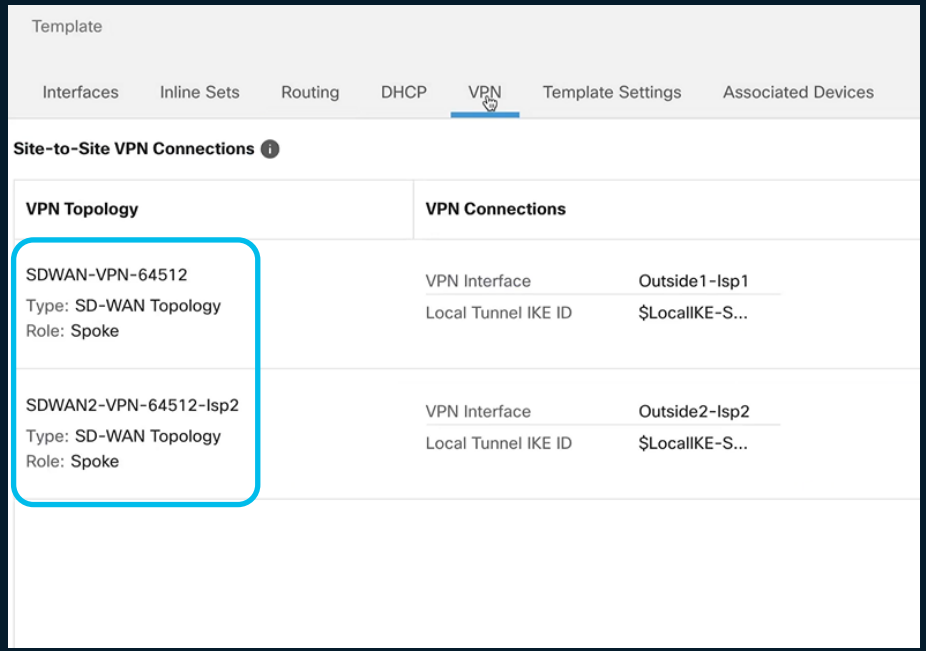
Легко включайте SD-WAN на всех существующих межсетевых экранах Cisco с автоматической настройкой.



Управление шаблонами SD-WAN

Легко подключите SD-WAN ко всем существующим брандмауэрам Cisco с помощью функции инициализации «в одно касание».

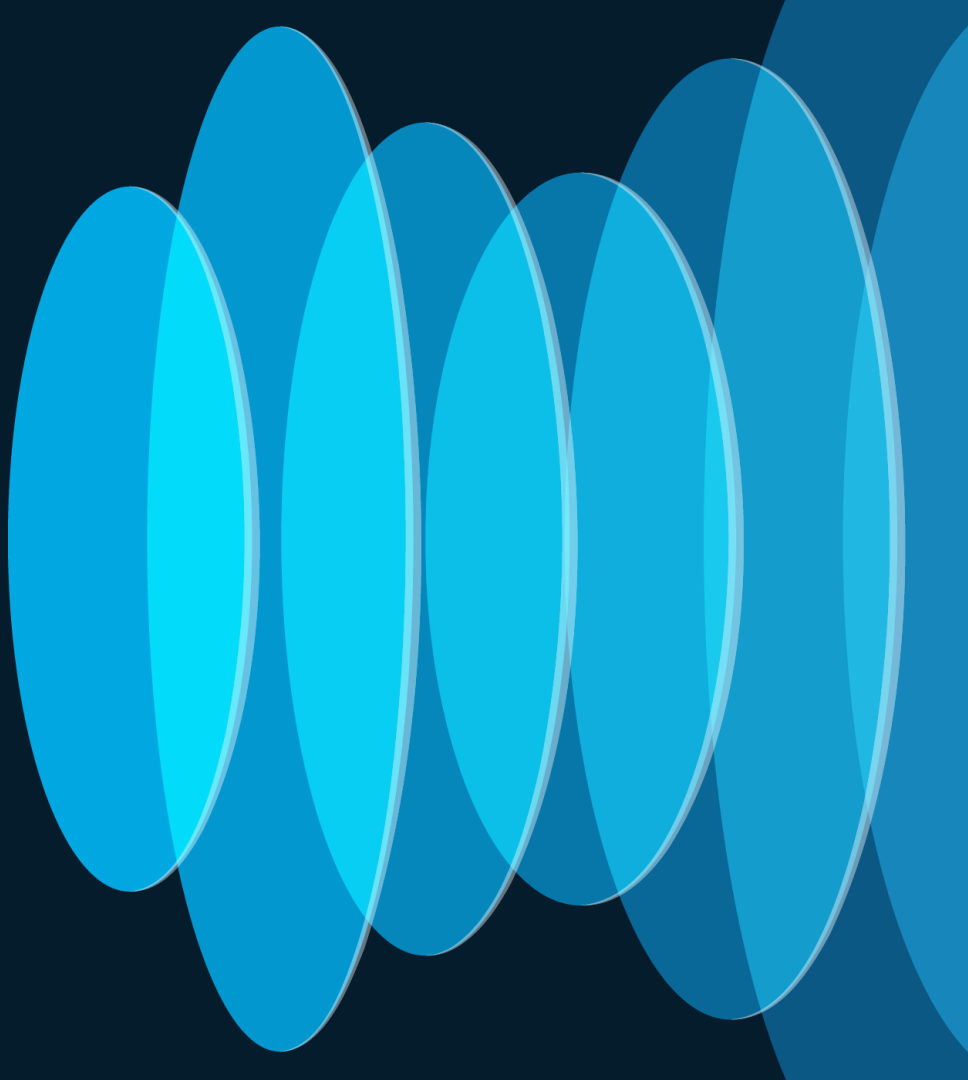




figura

Новое в FTD 7.6

Обнаружение угроз 0-дня и зашифрованных угроз с использованием AI/ML-технологий



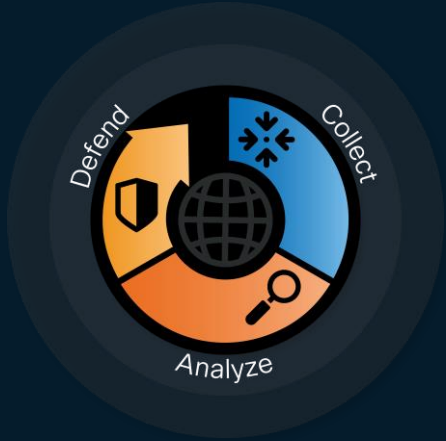
Cisco Talos расширяет возможности межсетевых экранов с помощью интеллектуальных технологий AI/ML

~800B событий безопасности в день

~9 млн заблокированных писем в час

~2 000 новых экземпляров в минуту

~2 000 заблокированных доменов в секунду



AI Cisco для безопасности обучается на одном из крупнейших в мире наборов данных о безопасности

60+
Партнерство с государственными и правоохранительными органами

200+
Уязвимости, обнаруженные за год

Получите контроль над зашифрованными угрозами

Механизм контроля зашифрованных угроз v2.0, не требующий расшифровки, использует AI/ML для блокировки зашифрованных угроз, обеспечивая полную безопасность, простоту, конфиденциальность и производительность.

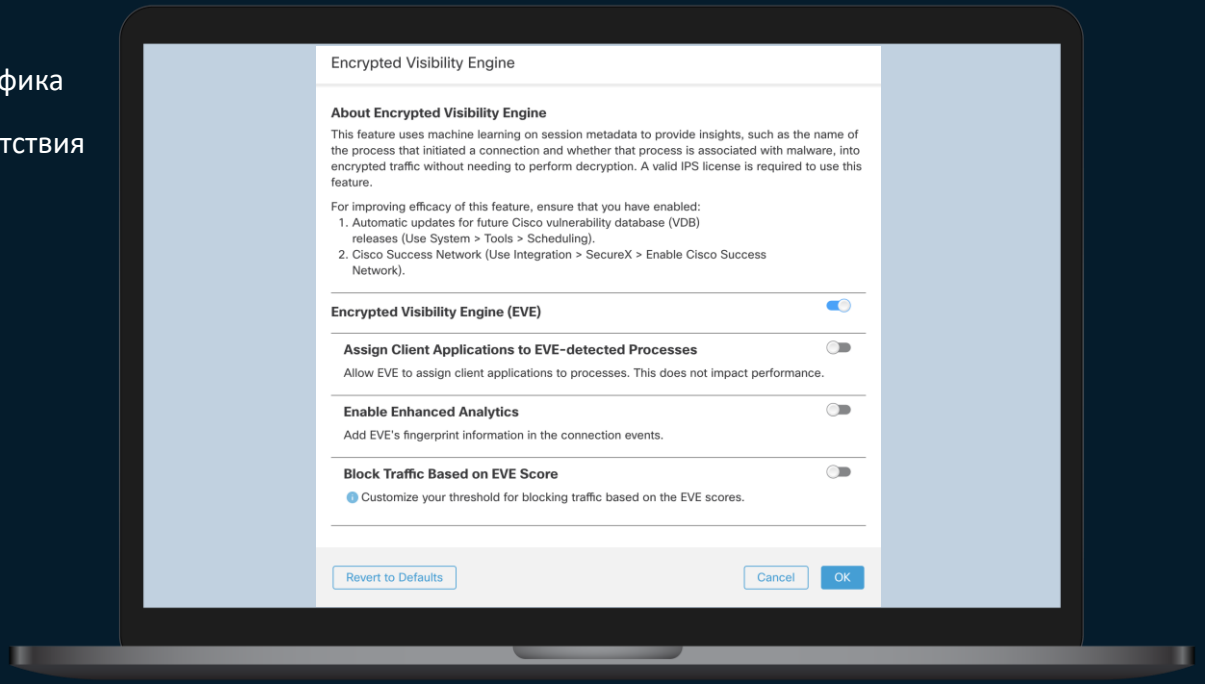
Упрощение проверки зашифрованного трафика

Сохранение конфиденциальности и соответствия требованиям.

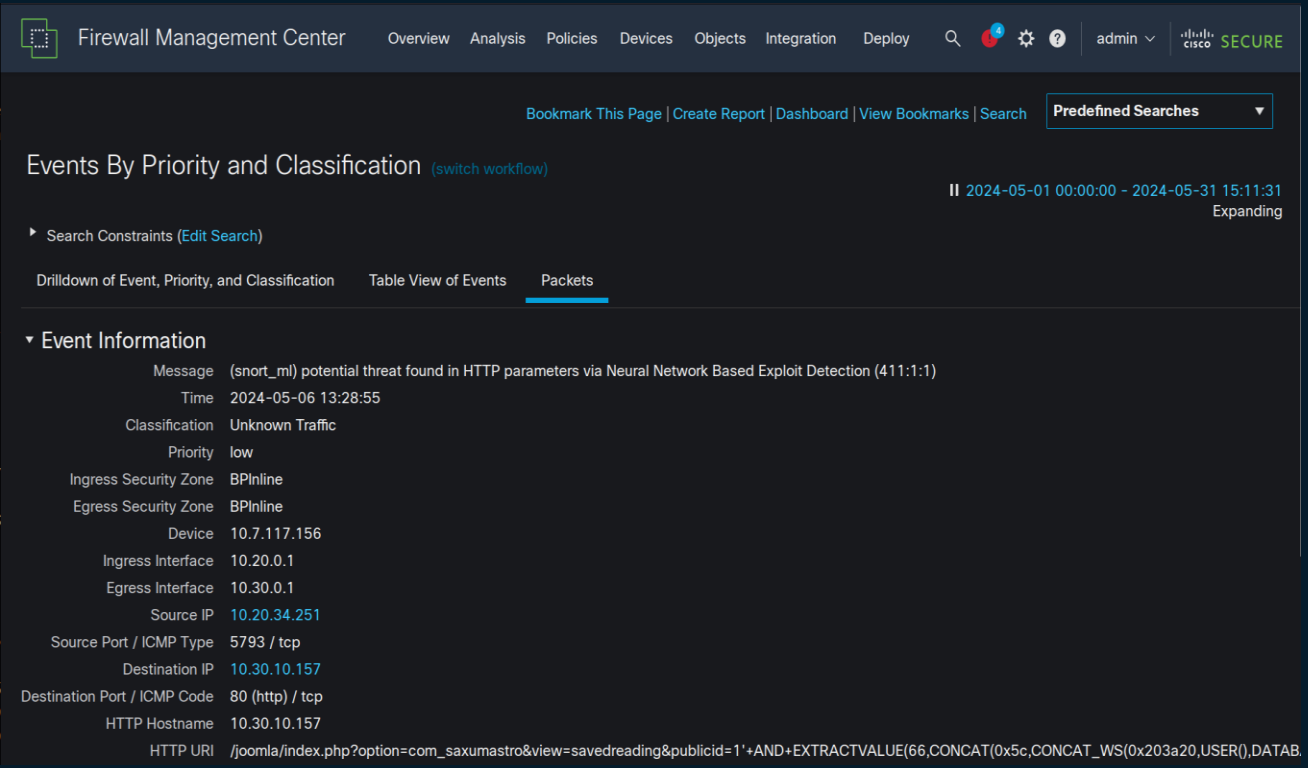
Ускорение работы брандмауэра

Видимость и контроль приложений в зашифрованных потоках

Поддержка протоколов TLS 1.3 и QUIC



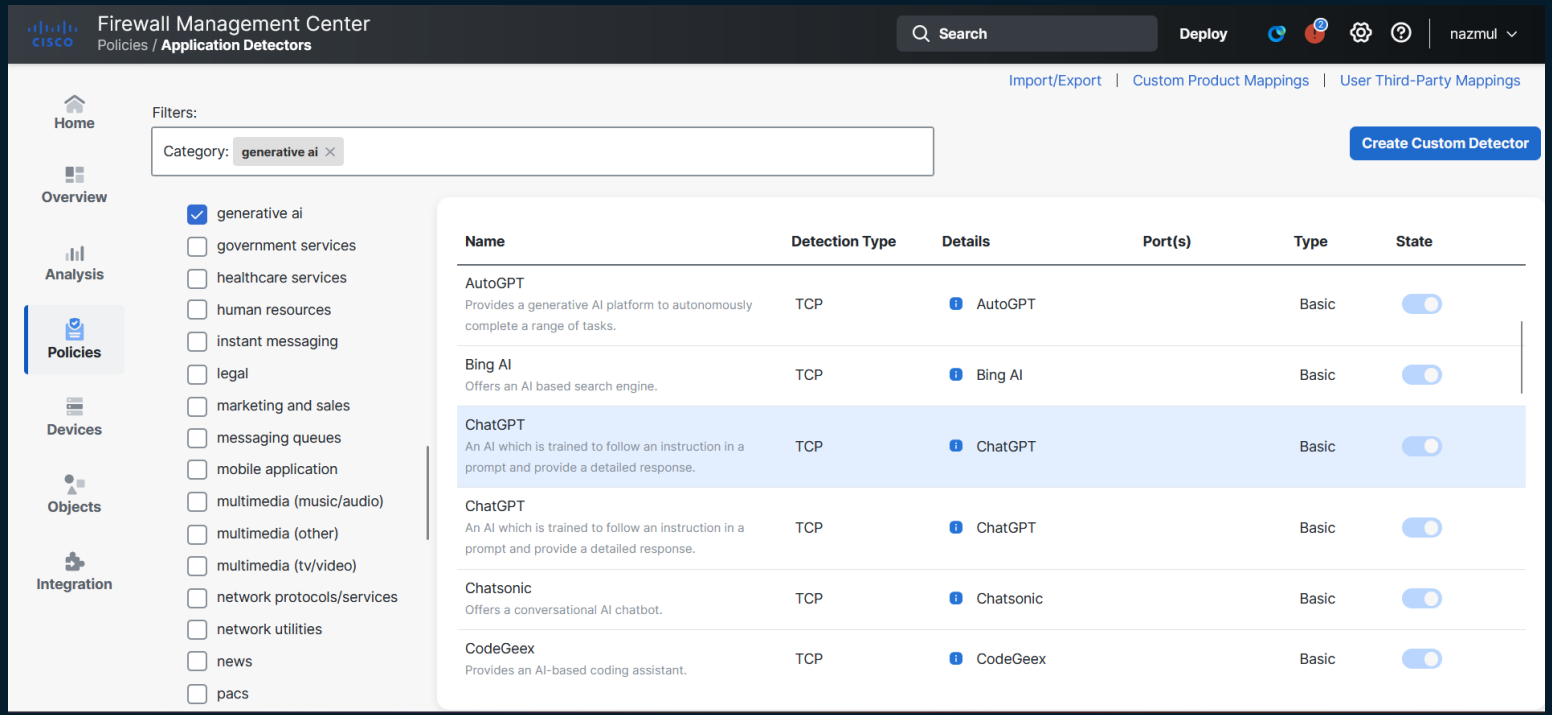
SnortML: Защита от атак нулевого дня



- Механизм машинного обучения, обнаруживающий известные типы уязвимостей
- Проактивное блокирование эксплойтов 0-дня
- Выявление вариаций атак

Детектор приложений генеративного AI

Устранение рисков, связанных с передачей конфиденциальной информации в платформе GenAI.



К 2025 году генеративный ИИ приведет к увеличению ресурсов кибербезопасности, необходимых для его защиты, что приведет к увеличению расходов на безопасность приложений и данных более чем на 15 %».

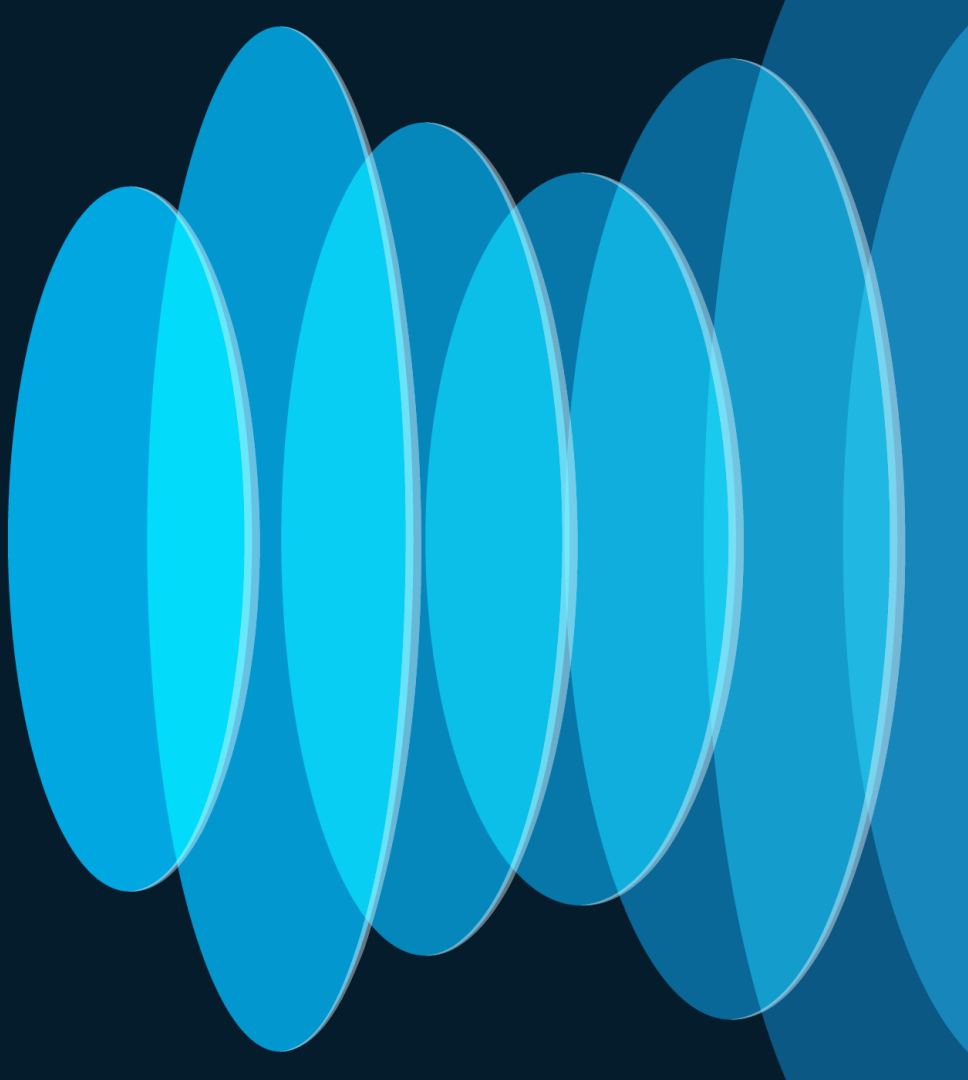
-Gartner

Поддерживает обнаружение и контроль 70+ приложений GenAI.

figura

Новое в FTD 7.6

AI ассистент на FMC для упрощения работы



Управление брандмауэром – это сложно!

Cisco AI Assistant for Security теперь на FMC

Помощь

Политика и отчетность

Поиск и предоставление информации о политиках для ускорения запросов, аудита и создания отчетов.

Дополнения

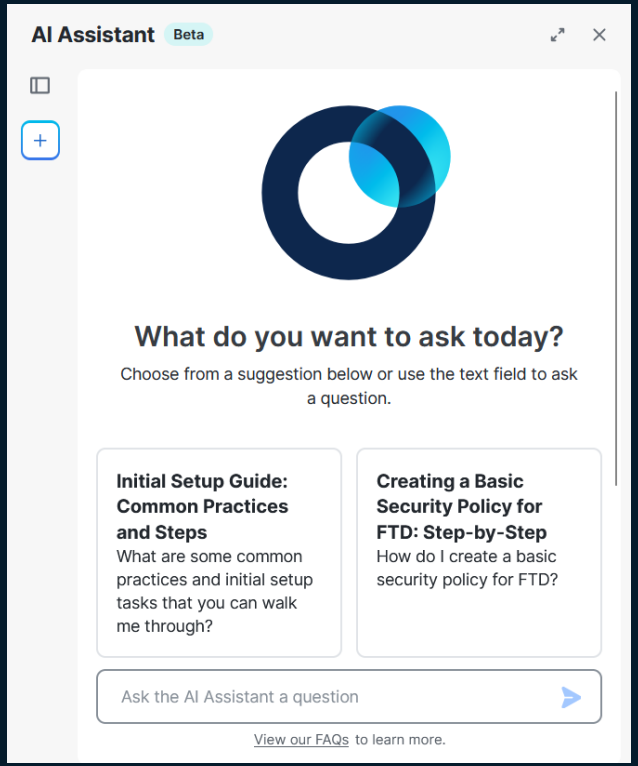
Поиск и устранение неисправностей

Объедините все руководства пользователя для ускоренного решения проблемы

Автоматизация

Управление жизненным циклом политики

Поиск и устранение ошибок в правилах брандмауэра для повышения безопасности и производительности

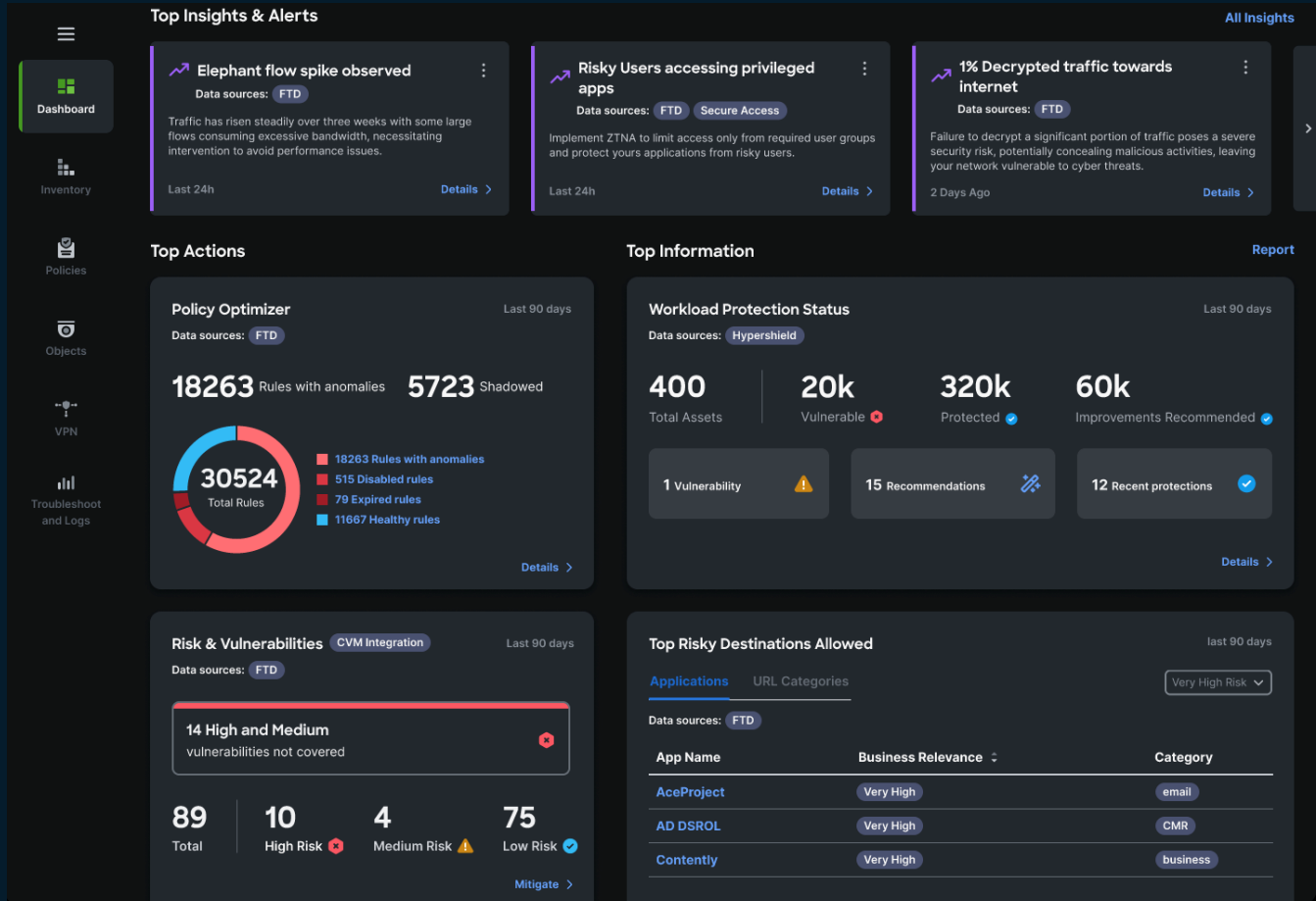


Доступно для всех решений FMC, начиная с версии 7.6 программного обеспечения FTD.

Security Cloud Control (ранее CDO)

Архитектура AI-Native для:

- Упрощенные операции
- Улучшенная безопасность
- Улучшенная ясность



figura

050013, г.Алматы, Бостандыкский район,
Бульвар Бухар жырау 33, офис 7

it@figurait.kz

www.figurait.kz

+7 (727) 310-20-59