

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



Profit Security Day

Конференция по информационной безопасности



Руслан Шаймарданов
Figura IT

1 ноября 2024
пятница

InterContinental
Алматы, Казахстан

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.



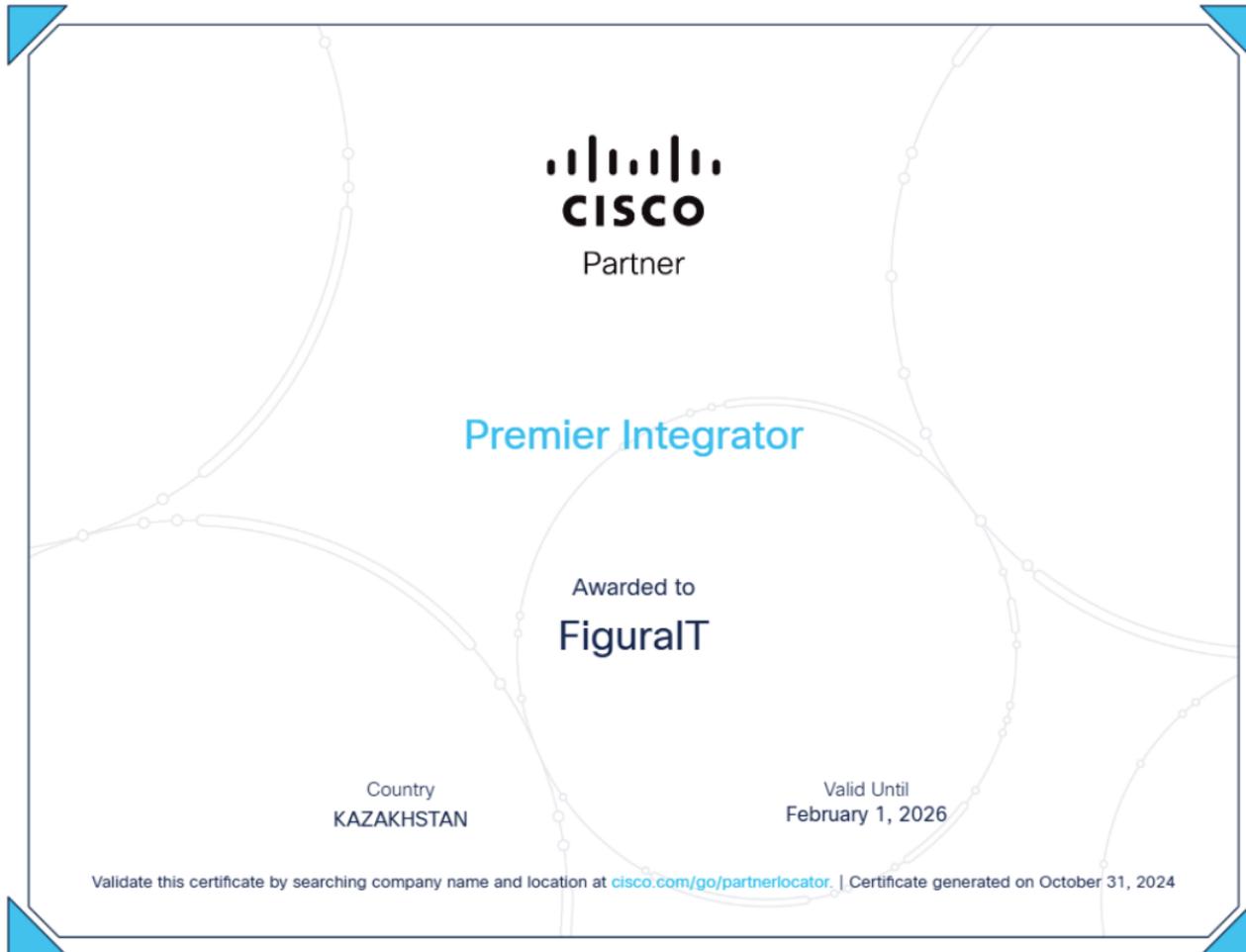
Оказываем **полный цикл** реализации проектов



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

Область экспертизы:





- 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.



TALOS THREAT INTELLIGENCE

🔗 Actionable threat intelligence

👥 Collective responses

👁️ Comprehensive visibility

🔍 Signal identification

🔬 Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

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 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



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

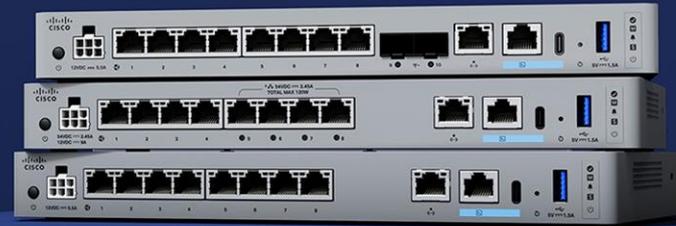
Немасштабируемая

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

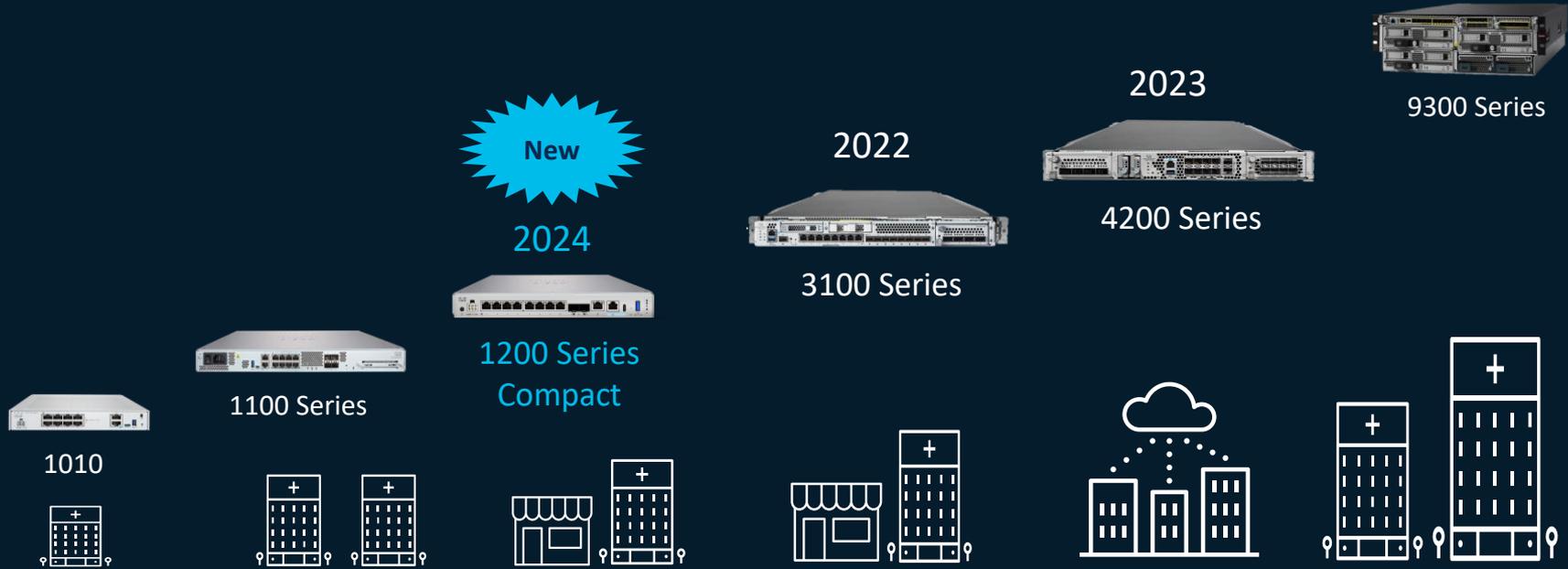
Сравнение производительности



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				
PoE	-	2 x PoE+	-	4 x UPoE+	2 x 10G SFP+

Портфолио оборудования Cisco Secure Firewall



Малый и средний
бизнес (МСБ)

Филиал

Среднее
предприятие

Крупный корпоративный
центр обработки данных

Поставщик
услуг

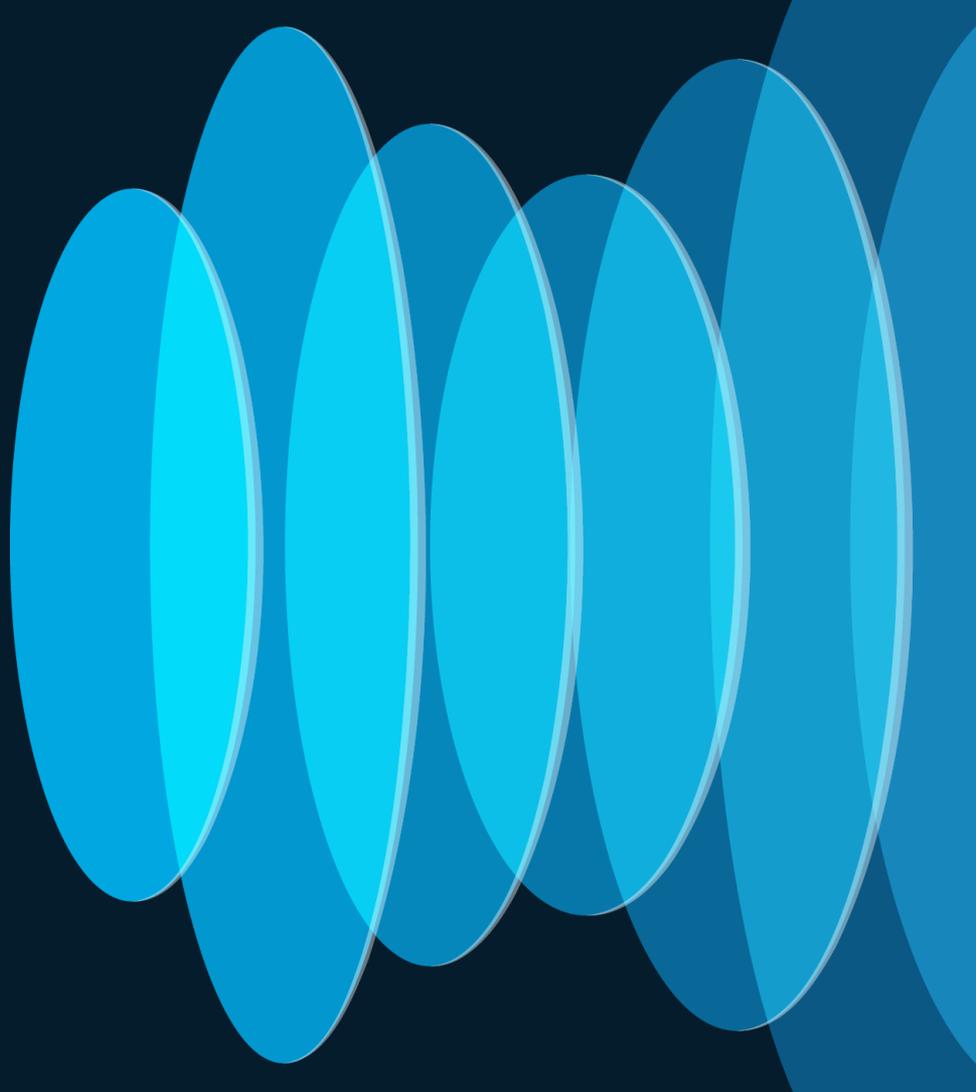


Новое в FTD 7.6

Шаблоны SD-WAN для

развертывания

Упрощение внедрения



Создание шаблона SD-WAN

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

The screenshot shows the 'Create VPN Topology' configuration page in the Cisco Firewall Management Center. The page is titled 'Create VPN Topology' and has a search bar in the top right corner. The left sidebar contains navigation options: Home, Overview, Analysis, Policies, Devices, Objects, and Integration. The main content area is divided into several sections:

- Topology Name ***: A text input field containing 'SDWAN'.
- VPN Type**: A section with four options, each with a radio button and a description:
 - SD-WAN Topology** (Selected): Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities. Below this, under 'Select VPN Topology', the 'Hub and Spoke' option is selected.
 - Route-Based VPN**: Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces. Below this, under 'Select VPN Topology', the 'Hub and Spoke' and 'Peer to Peer' options are available.
 - Policy-Based VPN**: Secures traffic between peers based on a static policy using protected networks. Below this, under 'Select VPN Topology', the 'Hub and Spoke', 'Peer to Peer', and 'Full Mesh' options are available.
 - SASE Topology**: A warning message states: 'You cannot configure a SASE topology without configuring Umbrella connection settings. More info Configure Umbrella Connector'. A 'Refresh' button is located below the warning.

At the bottom right of the configuration area, there are 'Cancel' and 'Create' buttons.

Управление шаблонами SD-WAN

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

Firewall Management Center
Devices / VPN

Home

Overview

Analysis

Policies

Devices

Objects

Integration

Devices

Device Management	VPN	Troubleshoot
Template Management ✓	Site To Site	File Download
NAT	Remote Access	Threat Defense CLI
QoS	Dynamic Access Policy	Packet Tracer
Platform Settings		Packet Capture
FlexConfig		Snort 3 Profiling
Certificates		Troubleshooting Logs
		Upgrade
		Threat Defense Upgrade
		Chassis Upgrade

Template

Interfaces Inline Sets Routing DHCP **VPN** Template Settings Associated Devices

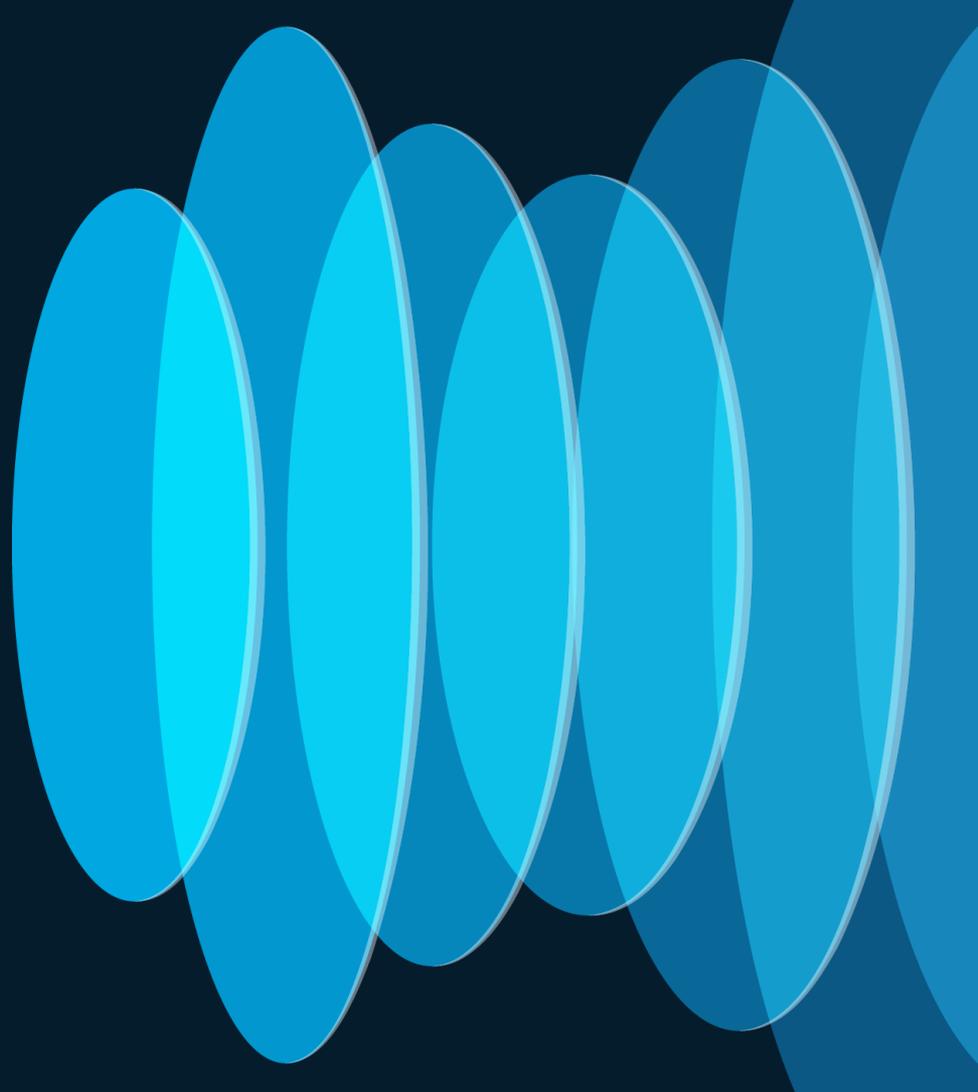
Site-to-Site VPN Connections ⓘ

VPN Topology	VPN Connections	
SDWAN-VPN-64512 Type: SD-WAN Topology Role: Spoke	VPN Interface	Outside1-lsp1
	Local Tunnel IKE ID	\$LocalIKE-S...
SDWAN2-VPN-64512-lsp2 Type: SD-WAN Topology Role: Spoke	VPN Interface	Outside2-lsp2
	Local Tunnel IKE ID	\$LocalIKE-S...



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



~800В 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.

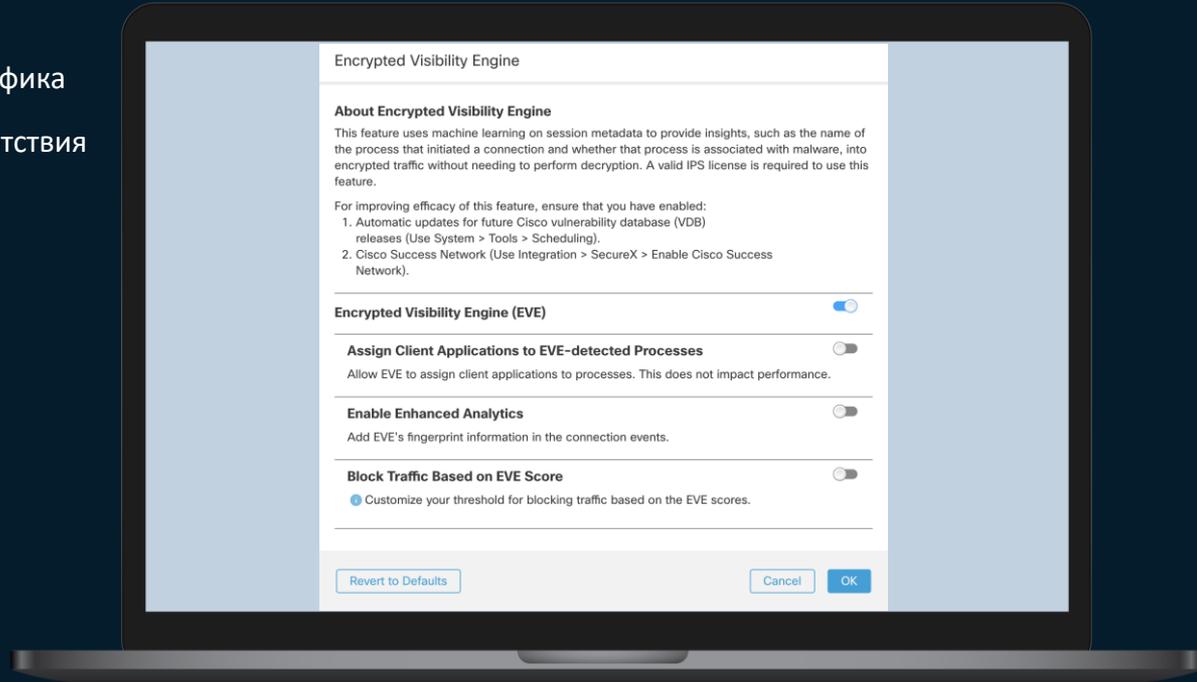
Упрощение проверки зашифрованного трафика

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

The screenshot displays the Cisco Firewall Management Center (FMC) interface. At the top, there is a navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, Integration, and Deploy. A search bar and user profile (admin) are also visible. Below the navigation bar, there are links for Bookmark This Page, Create Report, Dashboard, View Bookmarks, and Search. A dropdown menu for Predefined Searches is open. The main content area is titled "Events By Priority and Classification" and shows a time range of 2024-05-01 00:00:00 to 2024-05-31 15:11:31. The "Packets" tab is selected, and the event information is displayed as follows:

- Message: (snort_ml) potential threat found in HTTP parameters via Neural Network Based Exploit Detection (411:1:1)
- Time: 2024-05-06 13:28:55
- Classification: Unknown Traffic
- Priority: low
- Ingress Security Zone: BPInline
- Egress Security Zone: BPInline
- Device: 10.7.117.156
- Ingress Interface: 10.20.0.1
- Egress Interface: 10.30.0.1
- Source IP: 10.20.34.251
- Source Port / ICMP Type: 5793 / tcp
- Destination IP: 10.30.10.157
- Destination Port / ICMP Code: 80 (http) / tcp
- HTTP Hostname: 10.30.10.157
- HTTP URI: /joomla/index.php?option=com_saxumastro&view=savedreading&publicid=1'+AND+EXTRACTVALUE(66,CONCAT(0x5c,CONCAT_WS(0x203a20,USER()),DATAB

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

Детектор приложений генеративного AI

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

Firewall Management Center
Policies / Application Detectors

Filters: Category: generative ai

Create Custom Detector

Name	Detection Type	Details	Port(s)	Type	State
AutoGPT Provides a generative AI platform to autonomously complete a range of tasks.	TCP	1 AutoGPT		Basic	<input checked="" type="checkbox"/>
Bing AI Offers an AI based search engine.	TCP	1 Bing AI		Basic	<input checked="" type="checkbox"/>
ChatGPT An AI which is trained to follow an instruction in a prompt and provide a detailed response.	TCP	1 ChatGPT		Basic	<input checked="" type="checkbox"/>
ChatGPT An AI which is trained to follow an instruction in a prompt and provide a detailed response.	TCP	1 ChatGPT		Basic	<input checked="" type="checkbox"/>
Chatsonic Offers a conversational AI chatbot.	TCP	1 Chatsonic		Basic	<input checked="" type="checkbox"/>
CodeGeex Provides an AI-based coding assistant.	TCP	1 CodeGeex		Basic	<input checked="" type="checkbox"/>

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%».

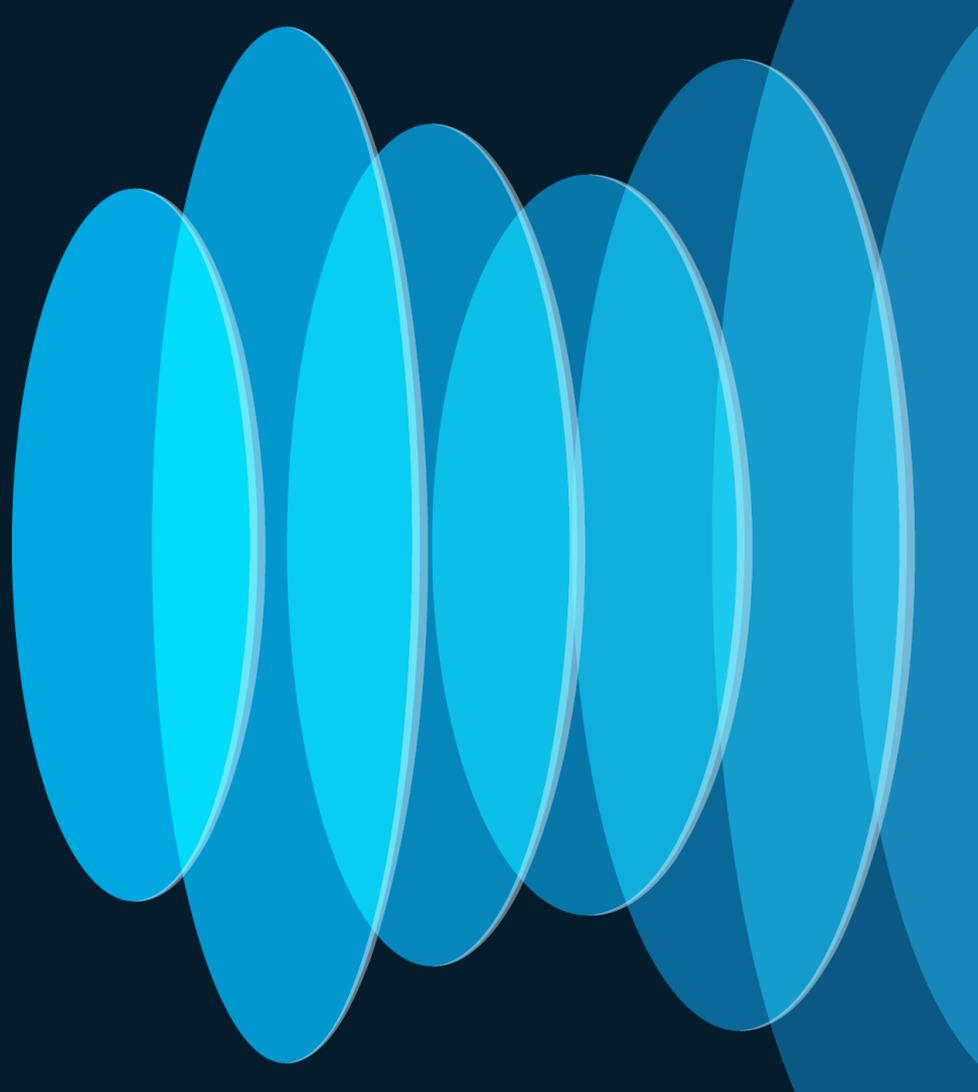
-Gartner

Поддерживает обнаружение и контроль 70+ приложений GenAI.



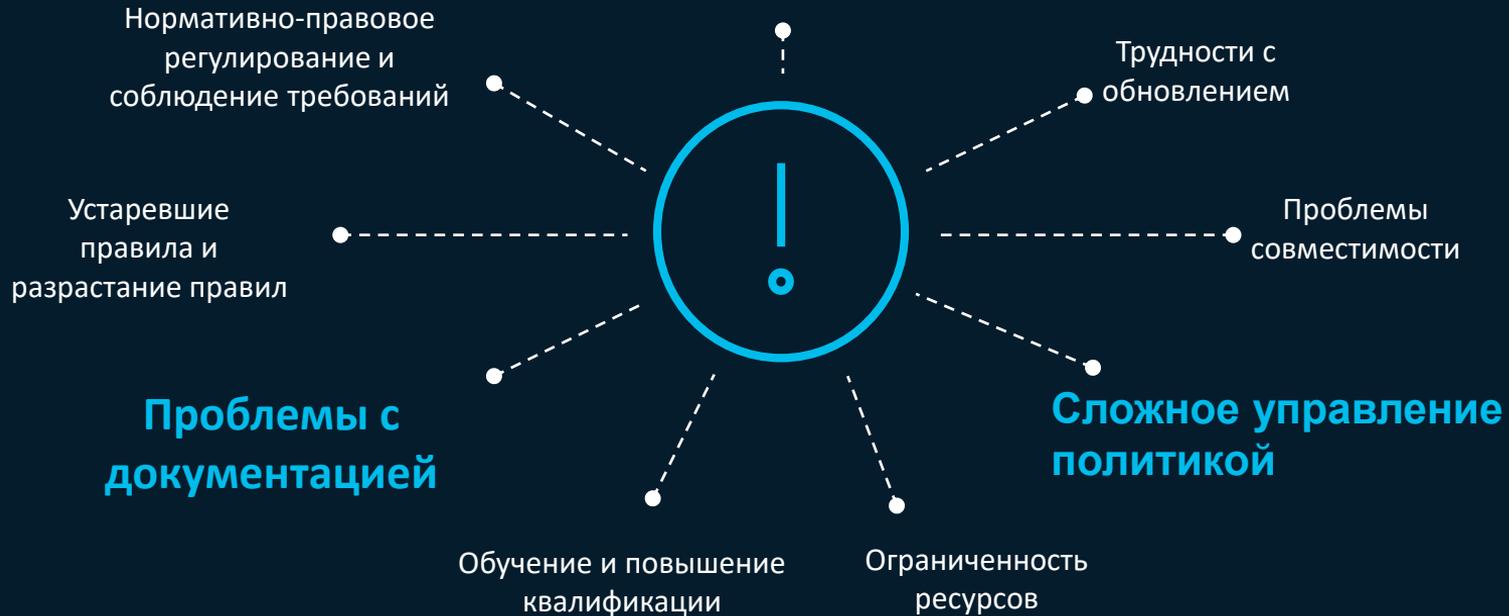
Новое в FTD 7.6

AI ассистент на FMC для
упрощения работы



Управление брендмауэром – это сложно!

Устранение неисправностей занимает много времени



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

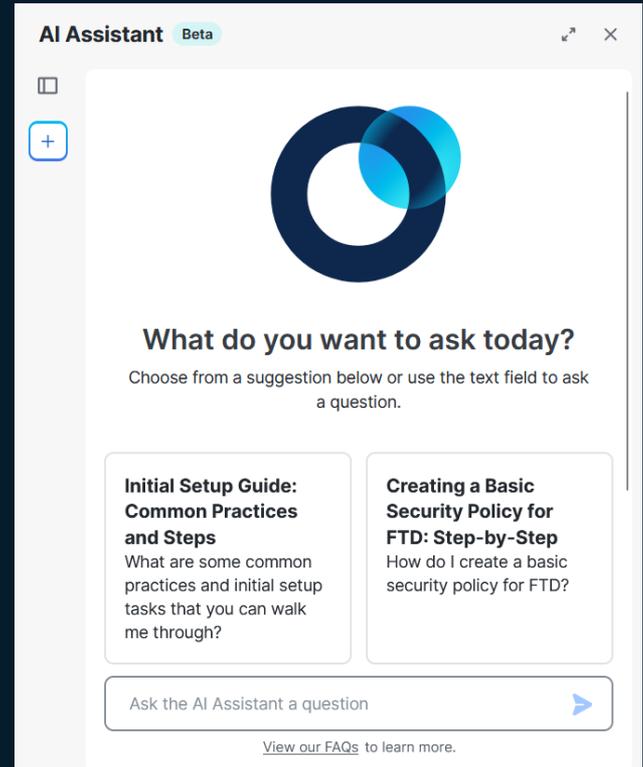
Поиск и устранение неисправностей

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

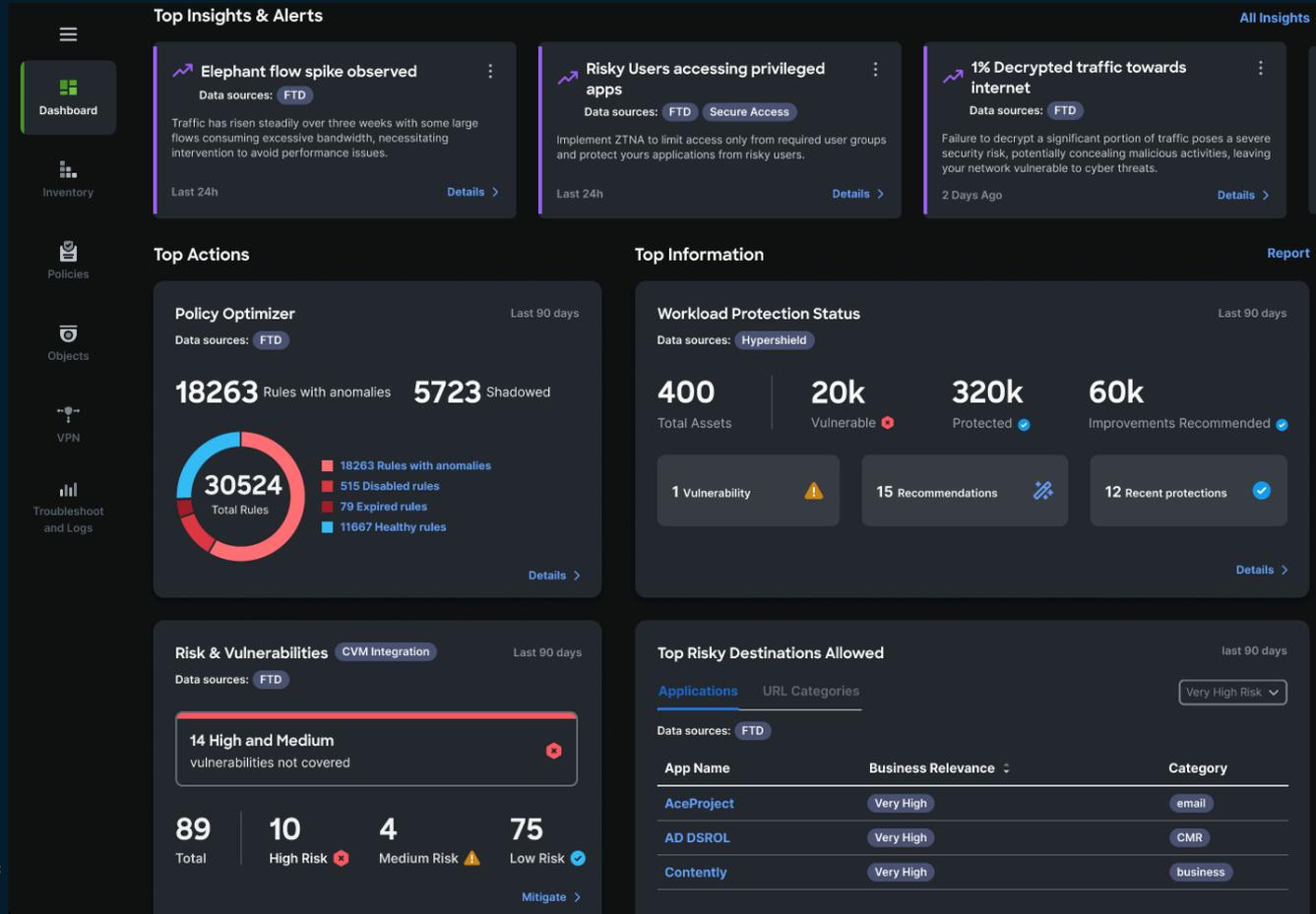


Доступно для всех решений FMC, начиная с версии 7.6 программного обеспечения FTD.

Security Cloud Control (панель CDO)

Архитектура AI-Native для:

- Упрощенные операции
- Улучшенная безопасность
- Улучшенная ясность





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

 it@figurait.kz

 www.figurait.kz

 +7 (727) 310-20-59

