ATUALIZAÇÃO 2025-2026

Novidades do Secure Firewall

O que mudou de 2025 para 2026

Versões 7.7 e 10.x | Jan/2025 até hoje | Fontes oficiais Cisco

Fernando Mantovani Pierobon · CCIE Security #63268

CIBERSEGURANÇA CISCO

NESTA AULA

O que você vai ver

01 **Novos firewalls**

Modelos 220, 1200 e 6100, novos FMC e virtuais

02 **Proteção e criptografia**

EVE, decriptação, Shadow Traffic e SnortML

03 **VPN, SD-WAN e gerência**

Menos trabalho manual no dia a dia

04 **Hybrid Mesh Firewall e IA**

Security Cloud Control e AgenticOps

LINHA DO TEMPO

Versões lançadas no período

2025

Versão 7.7

Recovery CLI e fim do Snort 2

2025

Versão 7.7.10

Universal ZTNA

Fim de 2025

Versão 10.0

Nova numeração e novos modelos

2026

Versão 10.1

Versão mais recente listada pela Cisco

CIBERSEGURANÇA CISCO

NOVIDADE · VERSÃO 10.0

Por que pulou da 7.7 para a 10.0?

Cada série agora tem só duas versões com recursos novos. Para o suporte completo (até 66 meses), vá para a versão final.

10.0

Versão inicial

Primeira versão da série, com recursos novos

10.5

Versão final

Última com recursos novos. Vai para certificação de governo

10.x.2

Manutenção

Só correções de bugs e vulnerabilidades

Fernando Mantovani Pierobon · CCIE Security #63268

01

Novos firewalls

220 · 1200 · 6100 · FMC 1800/2800/4800

Fernando Mantovani Pierobon · CCIE Security #63268

CIBERSEGURANÇA
CISCO

NOVIDADE 01 · APPLIANCES

Um modelo novo para cada cenário

220

Pequena filial

Desktop, até 1,5 Gbps. A partir da 10.0

1200 Compact

Filial e campus

Até 9 Gbps, opção com PoE. A partir da 7.6

1200 rack

Campus e empresa

1230, 1240 e 1250, até 18 Gbps. A partir da 7.7

6100

Data center

Até 630 Gbps, cluster de até 16. A partir da 10.0

NOVIDADE 01 · GERÊNCIA E VIRTUAL

FMC novo, FTD virtual maior

FMC

1800 · 2800 · 4800

Nova geração. O maior gerencia até 1.500 FTDs

FTDvU

Virtual sem limite

32 ou 64 vCPUs no VMware e KVM (antes: até 16)

Nuvem

Cluster e autoscale

Autoscale no GCP e Azure, ARM na OCI

EOL

Hora de migrar

ASA 5500-X e Firepower antigos: vá para 1200, 3100 ou 4200

Fernando Mantovani Pierobon · CCIE Security #63268

02

Proteção e tráfego criptografado

EVE · Decriptação · Shadow Traffic · SnortML

Fernando Mantovani Pierobon · CCIE Security #63268

CIBERSEGURANÇA
CISCO

NOVIDADE 02 · VERSÃO 10.0

Encrypted Visibility Engine mais simples

O que é

Identifica app e malware no tráfego criptografado sem decriptar, pela "impressão digital" do TLS.

Por que importa

Ficou fácil de ligar: modos Monitor e Protect e só dois níveis de bloqueio (High e Very High).

Onde encontrar

Agora direto na Access Control Policy. Antes ficava em Advanced Settings.

Fernando Mantovani Pierobon · CCIE Security #63268

CIBERSEGURANÇA CISCO

NOVIDADE 02 · VERSÃO 10.0

Decryption Policy: antes e depois

ATÉ A VERSÃO 7.7

- Só política baseada em regras
- Exceções criadas à mão
- Muitos passos para configurar

A PARTIR DA VERSÃO 10.0

- Modo Standard guiado, sem regras
- Exceções já prontas
- Usa o veredito do EVE (Client Threat)

Fernando Mantovani Pierobon · CCIE Security #63268

CIBERSEGURANÇA CISCO

NOVIDADE 02 · SHADOW TRAFFIC

Tráfego que tenta se esconder do firewall

Novo dashboard no FMC e nova coluna nos eventos: Shadow Traffic Type.

VPNs evasivas
Mais de 70 apps de VPN

Proxies multi-hop
Anonimizam a origem

DNS cifrado
Esconde a resolução de nomes

Domain fronting
Nome falso no SNI

Fake TLS
Finge ser TLS ou QUIC

Fernando Mantovani Pierobon · CCIE Security #63268

CIBERSEGURANÇA CISCO

NOVIDADE 02 · DETECÇÃO

O que evoluiu na detecção de ameaças

SnortML

IA contra exploits novos

Na 10.0 também pega XSS e command injection, além de SQL injection

QUIC

Decriptação de HTTP/3

Um clique para ligar, mesma lógica do TLS 1.3

Snort 3

Snort 2 aposentado

Desde a 7.7, só Snort 3. Com Snort 2 o upgrade é bloqueado

03

VPN, SD-WAN e gerência

Menos trabalho manual no dia a dia

Fernando Mantovani Pierobon · CCIE Security #63268

CIBERSEGURANÇA
CISCO

NOVIDADE 03 · VPN E SD-WAN

VPN mais rápida e mais automática

ECMP + BFD

Troca de caminho rápida

Balanceia no hub e muda de link em até 150 ms

SGT na VPN

TrustSec no túnel

A tag SGT atravessa o túnel VTI

ACME

Certificado automático

Renova sozinho o certificado da RA VPN e do ZTNA

4200

VPN distribuída no cluster

Túneis IPsec divididos entre os nós

NOVIDADE 03 · GERÊNCIA

FMC e FDM no dia a dia

Novo menu do FMC

Mesma navegação do Security Cloud Control

Edição simultânea

Várias pessoas na mesma ACP, com merge

Assistente do Splunk

Syslog para SIEM em uma tela só

Recovery CLI

Arruma interface, rota e VPN se perder o FMC

TACACS+ no FDM

AAA centralizado também no FDM

Dynamic Firewall

Política usa o nível de confiança do usuário

04

Hybrid Mesh Firewall e IA

Security Cloud Control · AgenticOps

Fernando Mantovani Pierobon · CCIE Security #63268

CIBERSEGURANÇA
CISCO

NOVIDADE 04 · ESTRATÉGIA CISCO

Hybrid Mesh Firewall



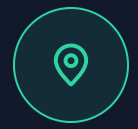
O que é

Firewall em todo lugar: físico, virtual, nuvem, switch e workload, com uma política só.



Por que importa

Você define a política uma vez e aplica em firewalls Cisco e de terceiros.



Onde encontrar

Security Cloud Control, a console em nuvem da Cisco.

Fernando Mantovani Pierobon · CCIE Security #63268

CIBERSEGURANÇA CISCO

NOVIDADE 04 · AGENTICOPS

IA cuidando da operação do firewall

Tudo no Security Cloud Control. O AI Assistant ainda responde dúvidas de política em linguagem natural.

Policy Analyzer

Acha regras duplicadas, vencidas e que podem ser unidas

Best Practices

Compara sua config com as boas práticas Cisco

Feature Adoption

Mostra quais recursos você realmente usa

Upgrade Planner

Versões disponíveis e CVEs corrigidas

EOL Planner

Avisa fim de vida e sugere o substituto

IMPACTO NO CURSO

O que muda no que você aprendeu

Continua valendo

- ACP, NAT, IPS e VPN
- FMC + FTD, HA e cluster

Mudou

- Menus do FMC na 10.0
- Decriptação e EVE mais simples
- Só Snort 3

É novo

- Modelos 220, 1200 e 6100
- Shadow Traffic e AgenticOps
- Numeração 10.x

FONTES

Documentação oficial da Cisco

Technical Decision Maker · versão 10.0
Cisco Secure Firewall 10.0 - Technical Decision Maker (TDM)

Plataformas 220, 1200 e 6100
Cisco Secure Firewall 220, 1200 Series e 6100 Platform - TDM

Novidades por versão · cisco.com
Cisco Secure Firewall Management Center New Features by Release

Bons estudos!

Cursos completos e labs práticos em

cibersegurancacisco.com.br



Fernando Mantovani Pierobon · CCIE Security #63268