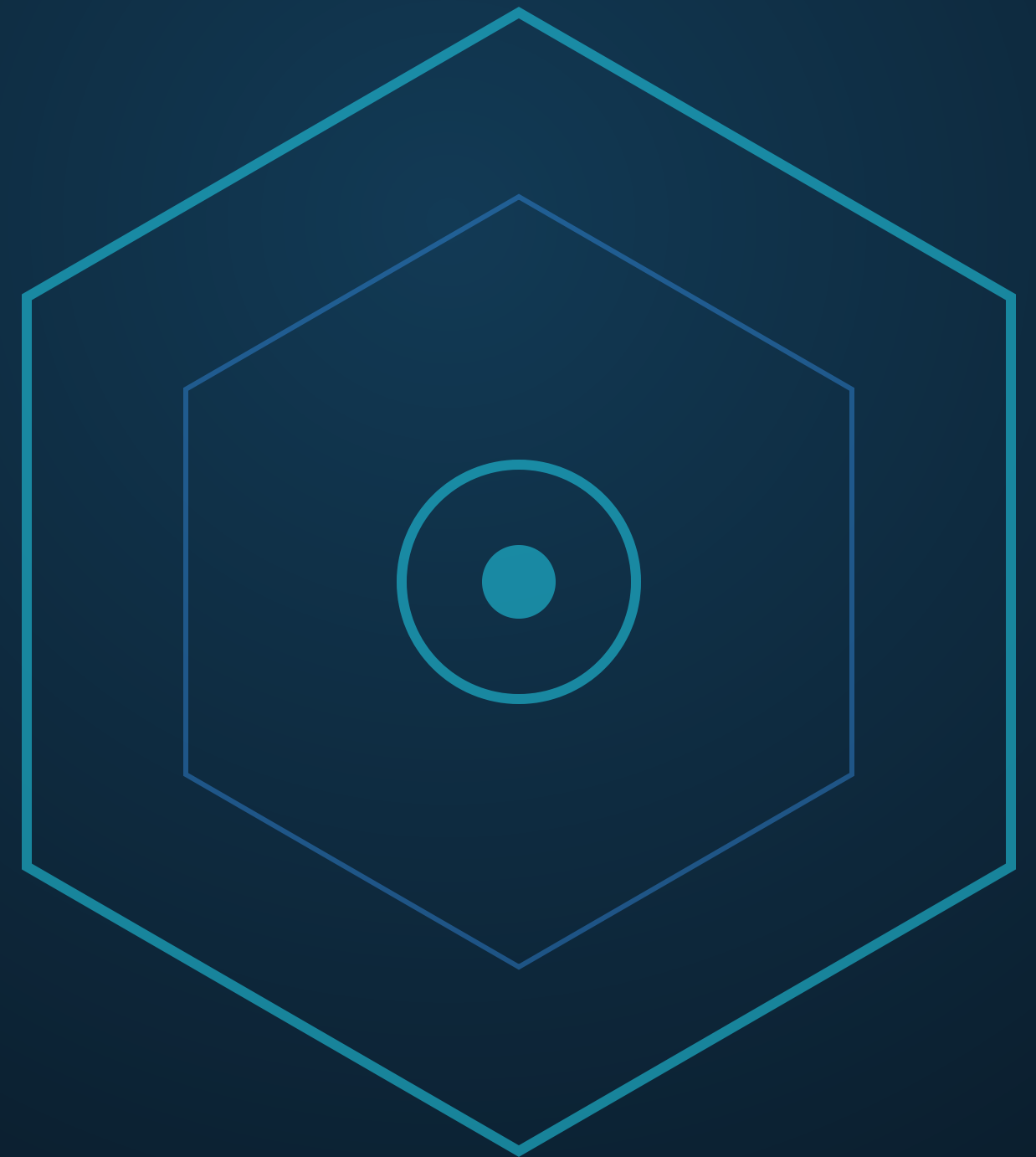


NETWORK ACCESS CONTROL

NAC **by** ROGIT

Controle de acesso à rede, do Wi-Fi ao switch, em uma única appliance.

RADIUS · TACACS+ · Portal de visitantes · Backup de configuração · Integração FortiGate



O DESAFIO

Quem está na sua rede agora?



Dispositivos desconhecidos

Notebooks pessoais, câmeras e IoT entram em qualquer porta ou Wi-Fi.



Senha única nos switches

Todos usam o mesmo admin. Ninguém sabe quem digitou cada comando.



Alterações sem rastro

Uma VLAN muda e ninguém sabe quando, por quem nem como voltar.



Visitantes no Wi-Fi

A senha do Wi-Fi circula entre convidados e nunca expira.

Cada ponto vira um risco de segurança e de auditoria, e costuma pedir uma ferramenta diferente.

A SOLUÇÃO

Uma appliance, seis módulos



Acesso à rede

802.1X, PEAP, EAP-TLS e MAB com VLAN dinâmica.



Visitantes e BYOD

Vouchers, portal com sua marca e aprovação pelo anfitrião.



TACACS+

Login nos equipamentos com o AD, comando a comando.



Backup de configuração

Versões, diferenças e autor de cada alteração.



Integração FortiGate

Identidade por IP e quarentena automática.



Visibilidade e alertas

Painel, auditoria, relatórios e avisos no celular.

COMO FUNCIONA

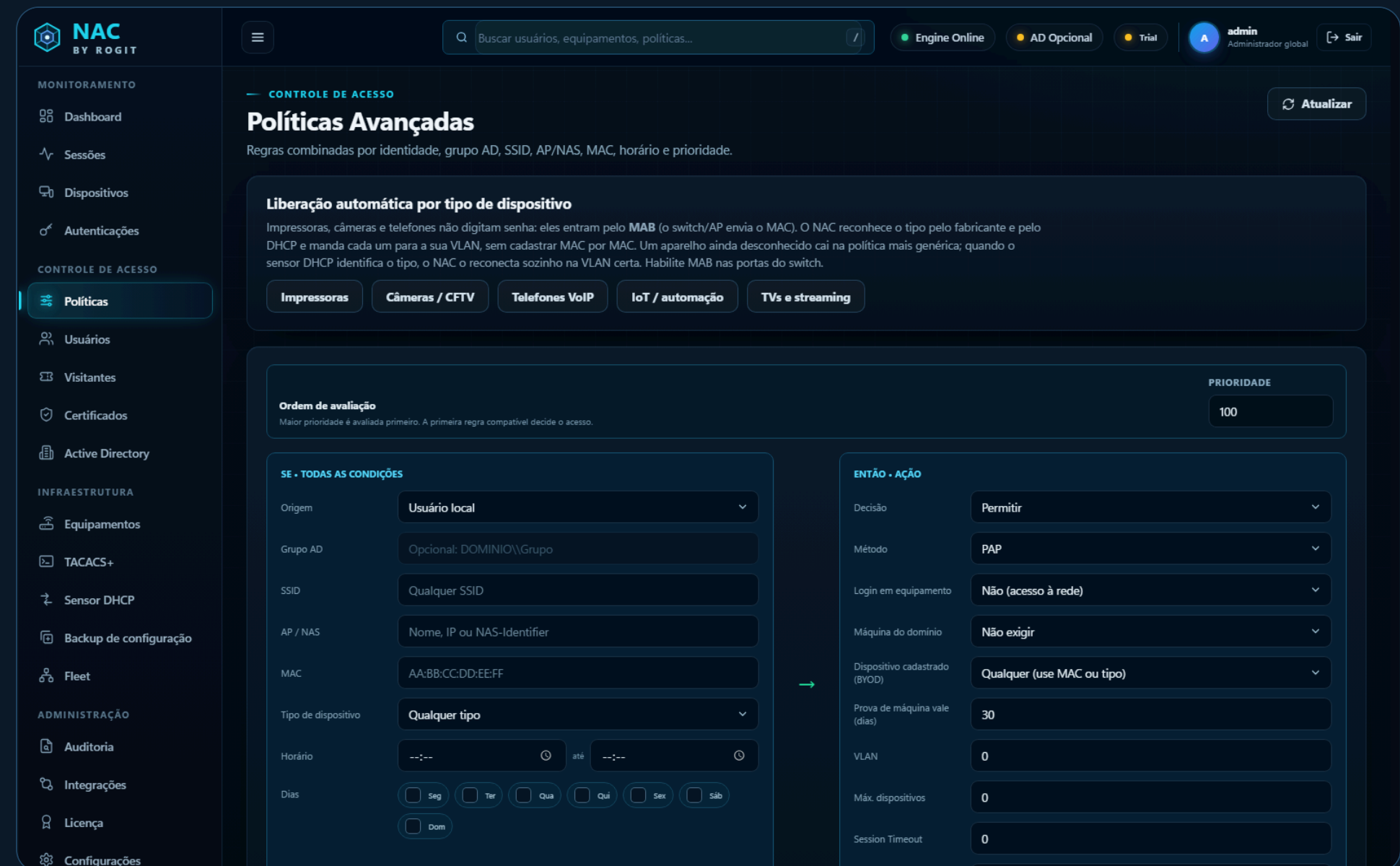
O NAC no centro da sua rede



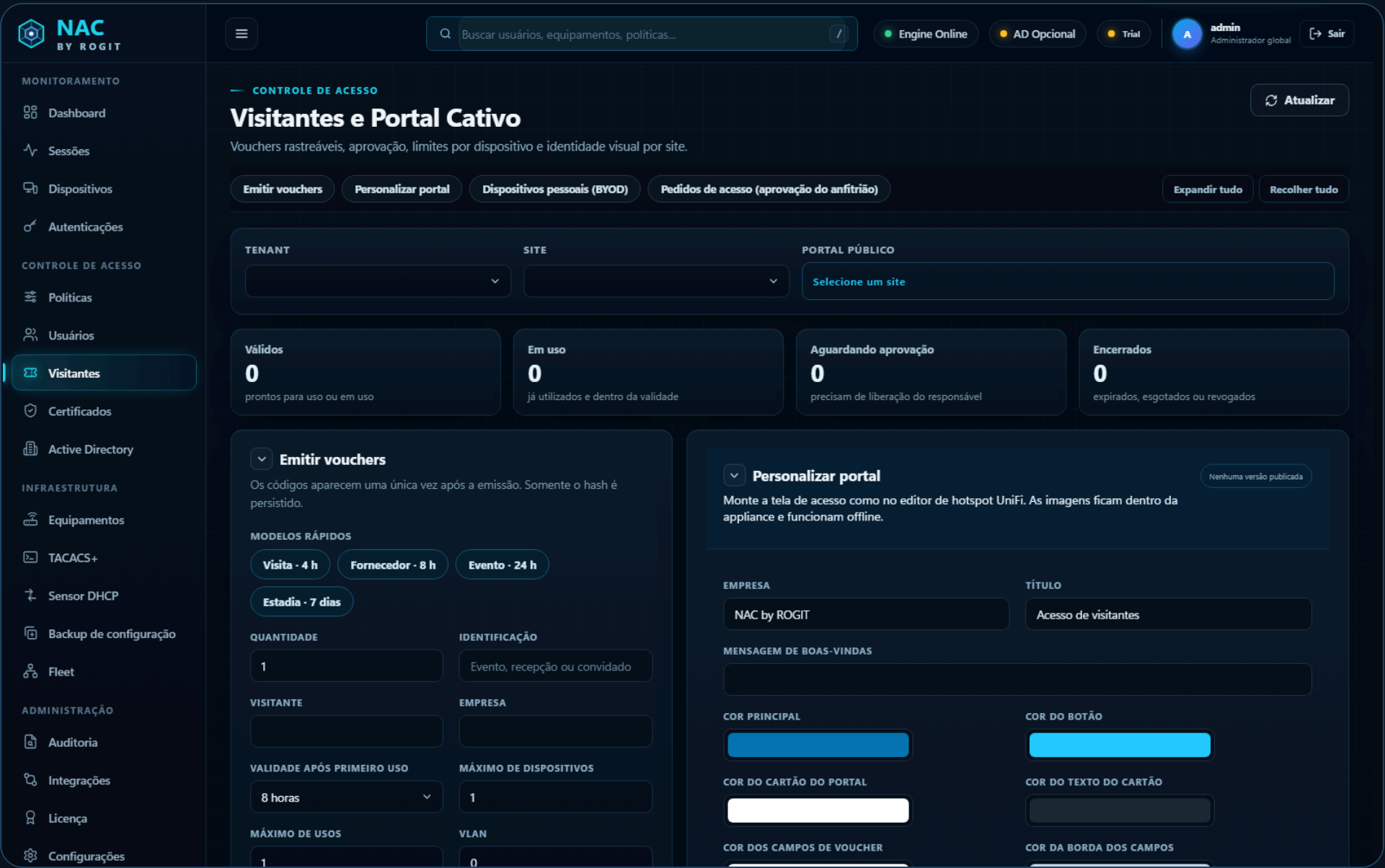
Tudo roda na sua infraestrutura: os dados de acesso não saem da empresa.

O acesso certo para cada um

- Políticas por grupo do AD, SSID, equipamento, MAC e horário
- VLAN dinâmica e limite de dispositivos por usuário
- Exige máquina do domínio quando preciso
- Impressoras, câmeras e telefones liberados pelo tipo
- Bloqueio derruba a sessão na hora (CoA)



Wi-Fi de visitante sem senha



- Vouchers com validade, limite de aparelhos e VLAN própria
- Portal com a marca da empresa, editado no painel
- O visitante pede acesso e o anfitrião aprova por e-mail
- Funcionários cadastram o próprio celular (BYOD)

Login individual nos equipamentos

1

Quem entra

Login nos switches com a conta do AD e nível pelo grupo.

2

O que pode

Autorização comando a comando: bloqueie o que é perigoso.

3

O que fez

Todo comando registrado, mais o syslog dos equipamentos.

Funciona com Dell, Cisco, Huawei, HP, Aruba, Fortinet, MikroTik e Juniper.

Toda alteração guardada e explicada

- Cópia diária e logo após cada alteração detectada
- Histórico com as diferenças linha a linha
- Quem alterou, quando e por onde
- Alerta no celular quando a configuração muda

Exemplo · SW-CORE · versão 12

vlan 30

+ name VISITANTES

interface Gi1/0/12

- switchport access vlan 10

+ switchport access vlan 30

alterado por admin.rede via TACACS+

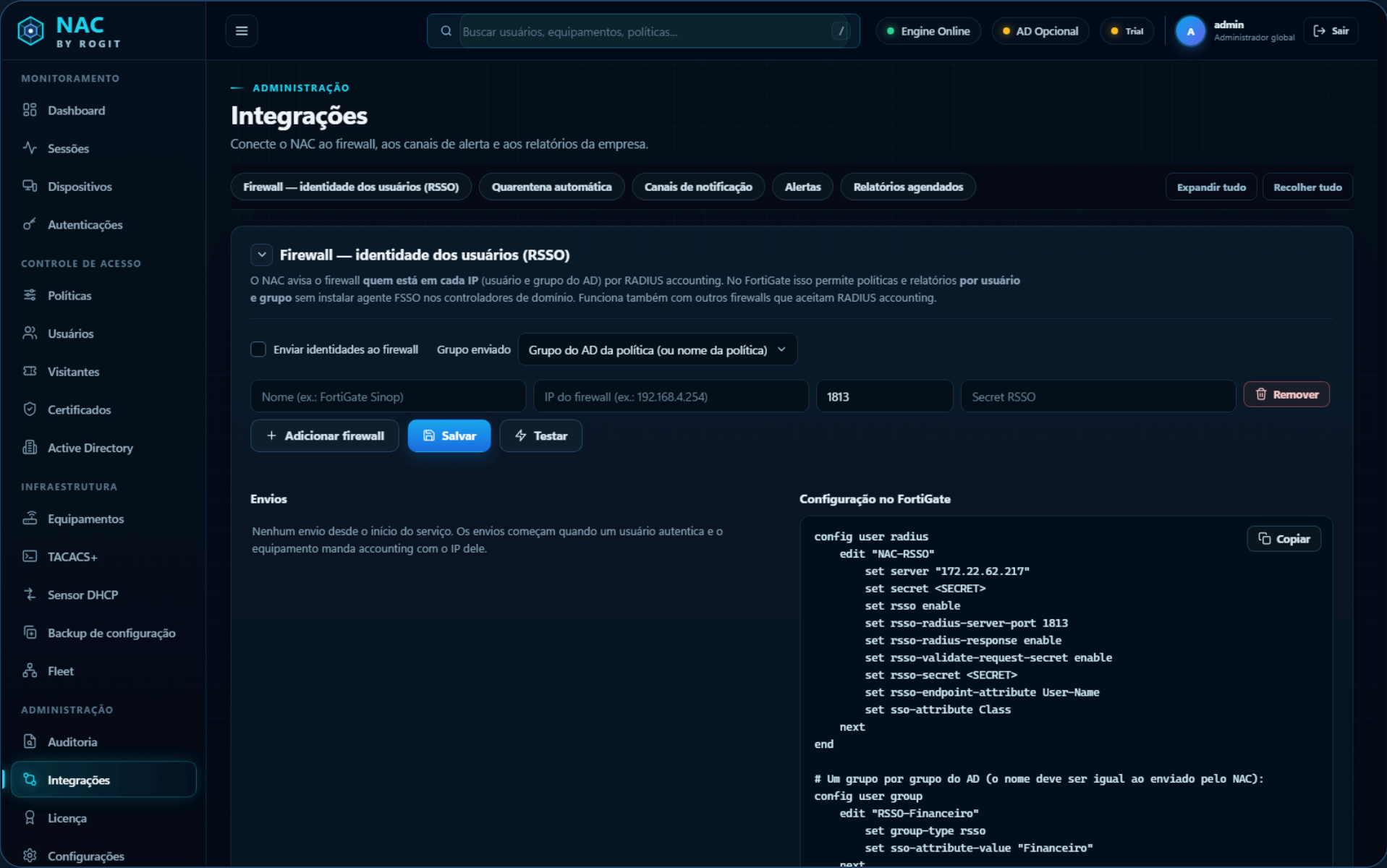
O firewall sabe quem é cada IP

Identidade por IP (RSSO)

Usuário e grupo do AD chegam ao FortiGate sem agente FSSO. Regras e relatórios por pessoa.

Quarentena automática

O FortiGate detecta a ameaça, o NAC acha o aparelho pelo IP e o isola na hora.



VISIBILIDADE

Saiba antes de virar problema

Painel em tempo real

Sessões, autenticações, falhas e uso por SSID.

Auditoria completa

Quem fez o quê no painel e na rede, com exportação CSV.

Sensor DHCP

Reconhece o tipo de cada aparelho que entra na rede.

Diagnóstico da rede

Mostra o que falta configurar em cada equipamento.

Alertas no celular

Telegram, e-mail e WhatsApp, com regras e horários.

Relatórios agendados

Resumo periódico por e-mail para a gestão, com CSV.

PRONTO PARA PRODUÇÃO

Feito para não parar



Alta disponibilidade

Dois appliances ativos, configuração replicada.



Segredos cifrados

Senhas e secrets protegidos em repouso.



API e webhooks

Integração com ITSM e automações.



MFA e perfis de acesso

TOTP no painel e papéis por função.



Atualização assinada

Pacotes verificados, também sem internet.



Várias filiais

Tenants e sites com administração separada.

Uma appliance. Toda a rede sob controle.

Quem entra, quem administra e o que muda, num só painel.

IMPLANTAÇÃO

Da instalação à rede protegida

01

Instalar

Appliance em VM ou servidor da empresa.

02

Conectar

Ingresso no Active Directory.

03

Cadastrar

Switches, APs e firewalls no painel.

04

Definir

Políticas por grupo, local e horário.

05

Ativar

802.1X e TACACS+ nos equipamentos.

Assistente de configuração no primeiro acesso e diagnóstico que mostra o que falta em cada equipamento.

LICENCIAMENTO

Simple de contratar e crescer

Plano 1

R\$ 5.000

Até 100 equipamentos

Plano 2

R\$ 8.500

Até 300 equipamentos

Plano 3

R\$ 15.000

Equipamentos ilimitados

Licença por número de equipamentos. Todos os módulos incluídos em todos os planos.

PRÓXIMO PASSO

Vamos proteger a sua rede?

Agende uma demonstração no seu ambiente.

CONTATO

Rogério Carvalho

E-MAIL

rogeriosampaiox@gmail.com

WHATSAPP

(66) 99632-8178

SITE

www.rogit.com.br