

Formação com Impacto

Liderar a Cibersegurança, transformar a Organização

Rui Duro

Data: 14/10/2026



Quem é (nome formador/professor) / Who I am



Rui Duro

Country Manager Check Point Portugal,
Especialista em Ciber Segurança

35 anos no sector das Tecnologias de Informação e mais de 25 anos dedicados à cibersegurança, num percurso diversificado, que combina experiência técnica e estratégica.

Antes de assumir funções de liderança na Check Point, iniciou o seu percurso profissional como **Engenheiro de Segurança** num integrador, integrou mais tarde uma das maiores operadoras de telecomunicações em Portugal, onde desempenhou funções como **Consultor de Segurança e Desenvolvimento de soluções na área de Segurança**, conduzindo projectos de transformação digital e implementação de soluções de segurança de grande escala.



Agenda

- Conceitos fundamentais
- Evolução das redes
- Tecnologias
- Monitorização e Controlo
- Porque são atacadas as empresas
- Boas praticas



Conceitos fundamentais

Definição de valor

...qualquer ativo digital ou acesso que possa ser explorado, vendido, trocado, monetizado ou usado para obter vantagem.....



Atores e os seus interesses



SCRIPT KIDDIES



HACKTIVISTAS



CIBER CRIMINOSOS



ESTADOS PATROCINADORES DE ATAQUES

Curiosidade e Aprendizagem

Prestígio e reputação

Desafiar autoridades ou sistemas

Diversão ou Tédio

Demonstrar que é capaz

Vingança ou retaliação pessoal

Atores e os seus interesses



SCRIPT KIDDIES



HACKTIVISTAS



CIBER CRIMINOSOS



ESTADOS PATROCINADORES DE ATAQUES

Político ou ideológico

Liberdade expressão

Justiça Social/Direitos Humanos

Exposição verdades ocultas

Antiglobalização/Anti
capitalismo

Solidariedade Internacional

Chamar atenção dos Media

Atores e os seus interesses



SCRIPT KIDDIES



HACKTIVISTAS



CIBER CRIMINOSOS



ESTADOS PATROCINADORES DE ATAQUES

Ganhos Financeiros

Espionagem corporativa

Espionagem Estatal

Venda de Exploits ou ferramentas de Hacking

Reputação e Status no submundo Hacker

Manipulação de Mercados Financeiros

Vingança pessoal ou profissional

Atores e os seus interesses



SCRIPT KIDDIES



HACKTIVISTAS



CIBER CRIMINOSOS



ESTADOS PATROCINADORES DE ATAQUES

Sabotagem Cibernética
(CyberWarfare)

Primeira vaga de ataque numa guerra

Guerra económica

Espionagem governamental

Espionagem industrial

Desinformação e repressão

Geração de receitas

Superfície de Ataque Vs Vetor de Ataque

Superfície de ataque	O que representa na rede	Vetores mais comuns
Email e colaboração	Mensagens, anexos, links e plataformas de comunicação	Phishing, BEC, links e anexos maliciosos
Utilizadores e identidades	Contas, credenciais, sessões e privilégios	Engenharia social, Password Spraying, Credential Stuffing, MFA fatigue
Endpoints e Mobile	PC, portátil, smartphone e tablet	Malware, ransomware, exploração de vulnerabilidades, USB malicioso, smishing
Rede Corporativa e Wi-Fi	LAN, WAN, filiais, acessos remotos e redes sem fios	Movimento lateral, serviços expostos, Man-in-the-Middle, rogue access point
Aplicações, SaaS e APIs	Portais web, serviços cloud e interligações entre aplicações	Falhas de autenticação, abuso de APIs, roubo de sessão, OAuth malicioso
Cloud e dados	Workloads, armazenamento e informação empresarial	Má configuração, credenciais comprometidas, exposição pública, exfiltração
IA generativa e agentes	Copilots, LLMs, prompts, conectores e agentes autónomos	Prompt Injection, Fuga de Dados, Shadow AI, abuso de privilégios
Terceiros, IoT e OT	Fornecedores, integrações, sensores e equipamentos ligados	Supply chain, firmware vulnerável, acessos indevidos, exploração remota

Do Perímetro à Identidade

Modelo Perimetral

Dentro da rede existe confiança implícita

A autenticação ocorre sobretudo na entrada

A VPN prolonga a rede até ao utilizador

Uma conta comprometida pode permitir o amplo movimento lateral

Modelo Orientado à Identidade

Cada pedido é avaliado segundo identidade, dispositivo, localização, contexto e risco

O acesso é limitado à aplicação necessária

A segurança é reavaliada durante a sessão



Evolução das redes

Da Firewall à HybridMesh

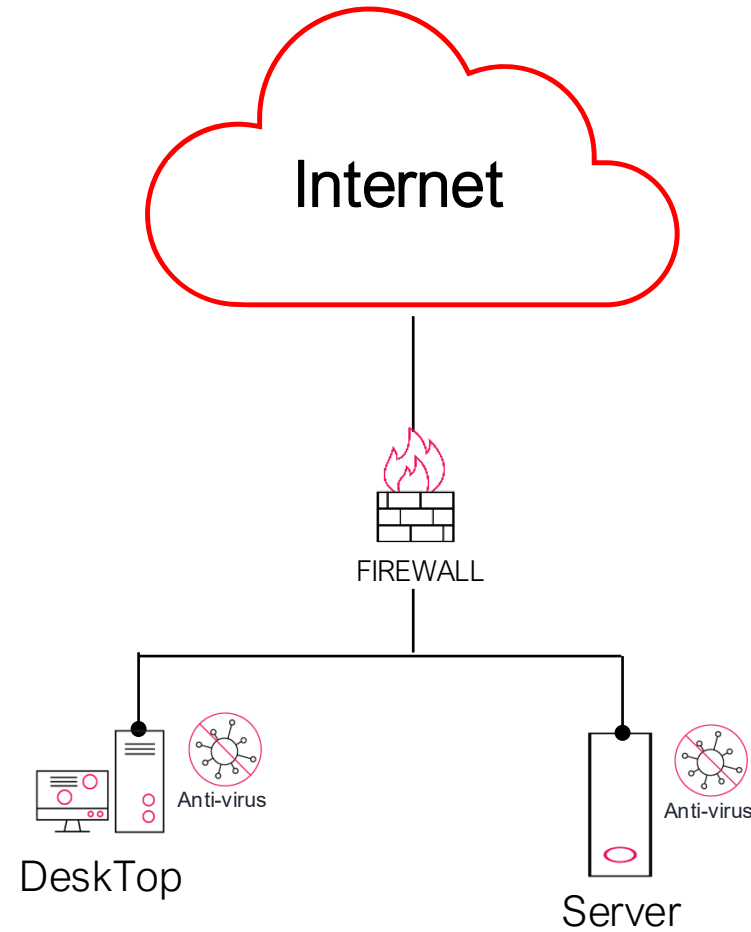
Proteção do Perímetro na Idade Média

Único ponto de entrada...
Concentrar forças na entrada
Não distribuímos as forças
Mais fácil defender
Mais fácil visualizar
Mais fácil controlar



Da FireWall à HybridMesh

Internet 1996



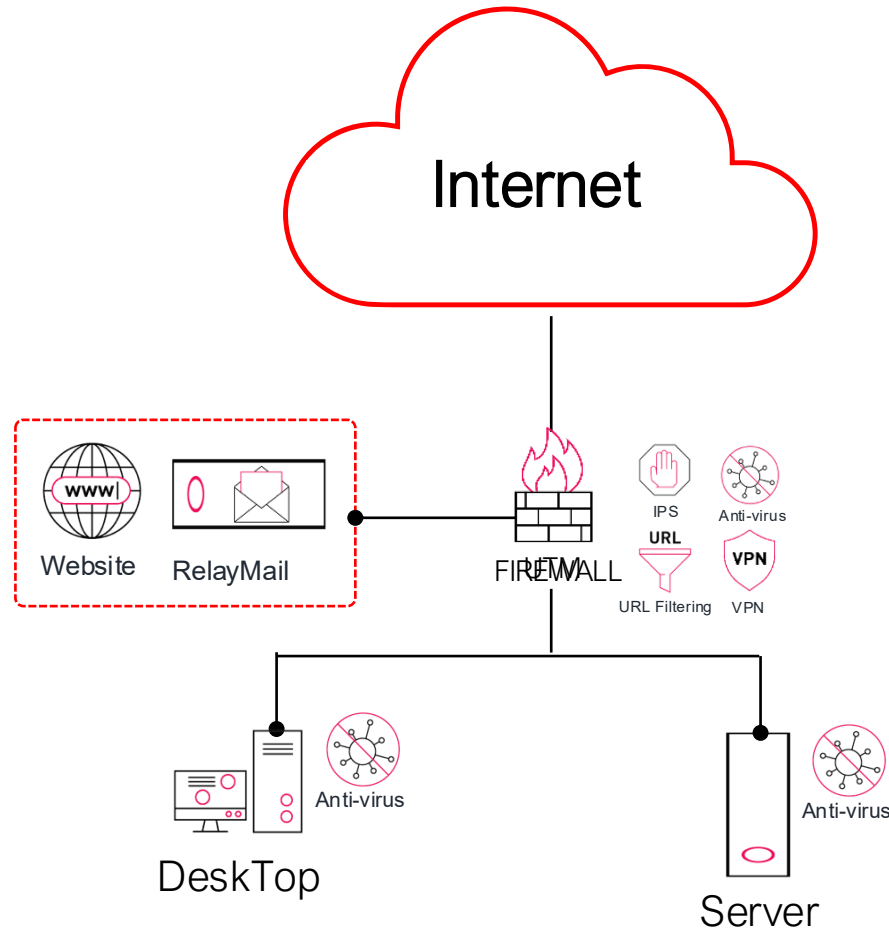
FireWall

Antivírus

..era quanto bastava...
Tínhamos um perímetro
único, dentro do edifício

Da FireWall à HybridMesh

WEB 1.0 2003



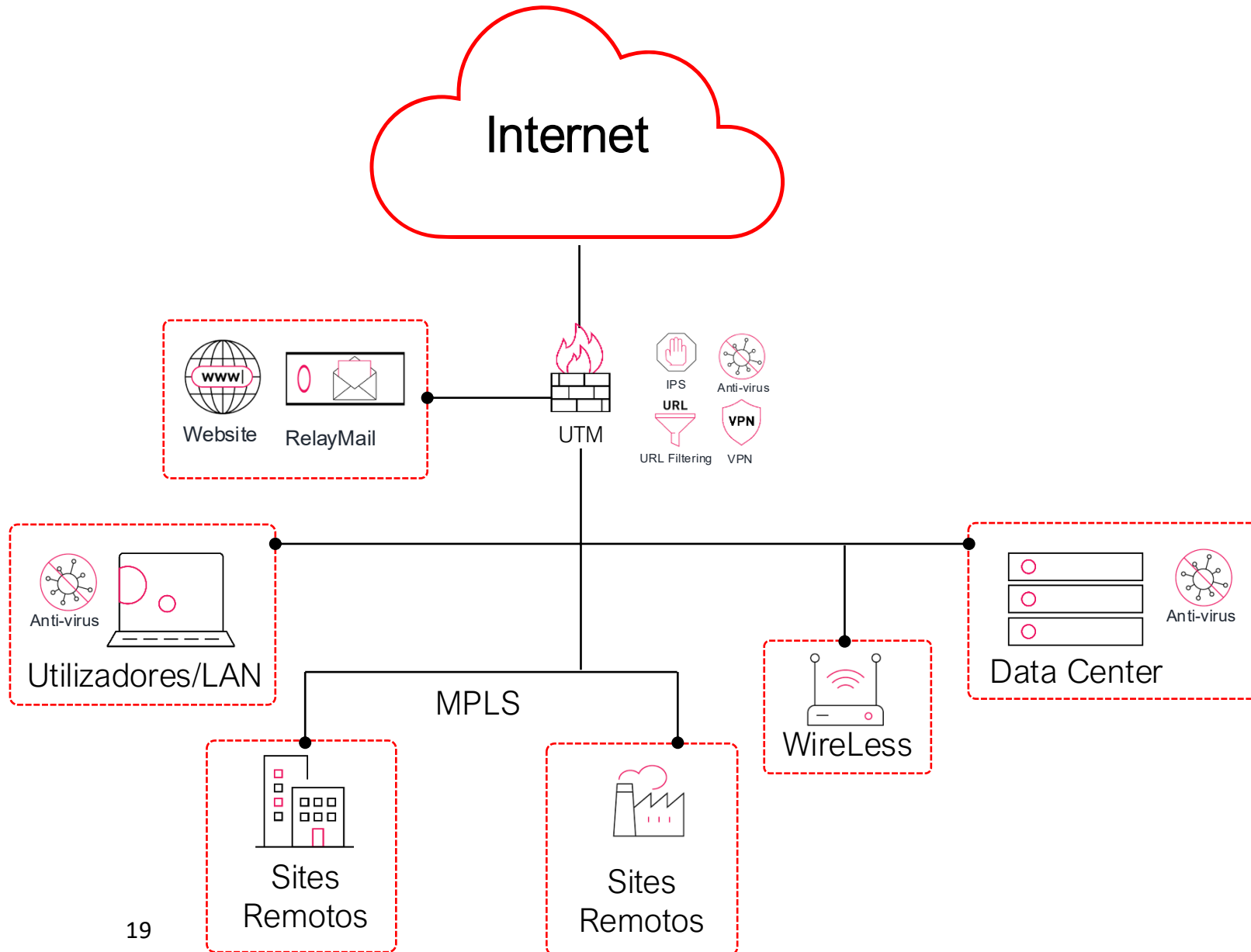
FireWall
IPS
URL Filtering
Antivirus
VPN

UTM

Antivírus

Da FireWall à HybridMesh

WEB 1.0 2003



FireWall
IPS
URL Filtering
Antivirus
VPN

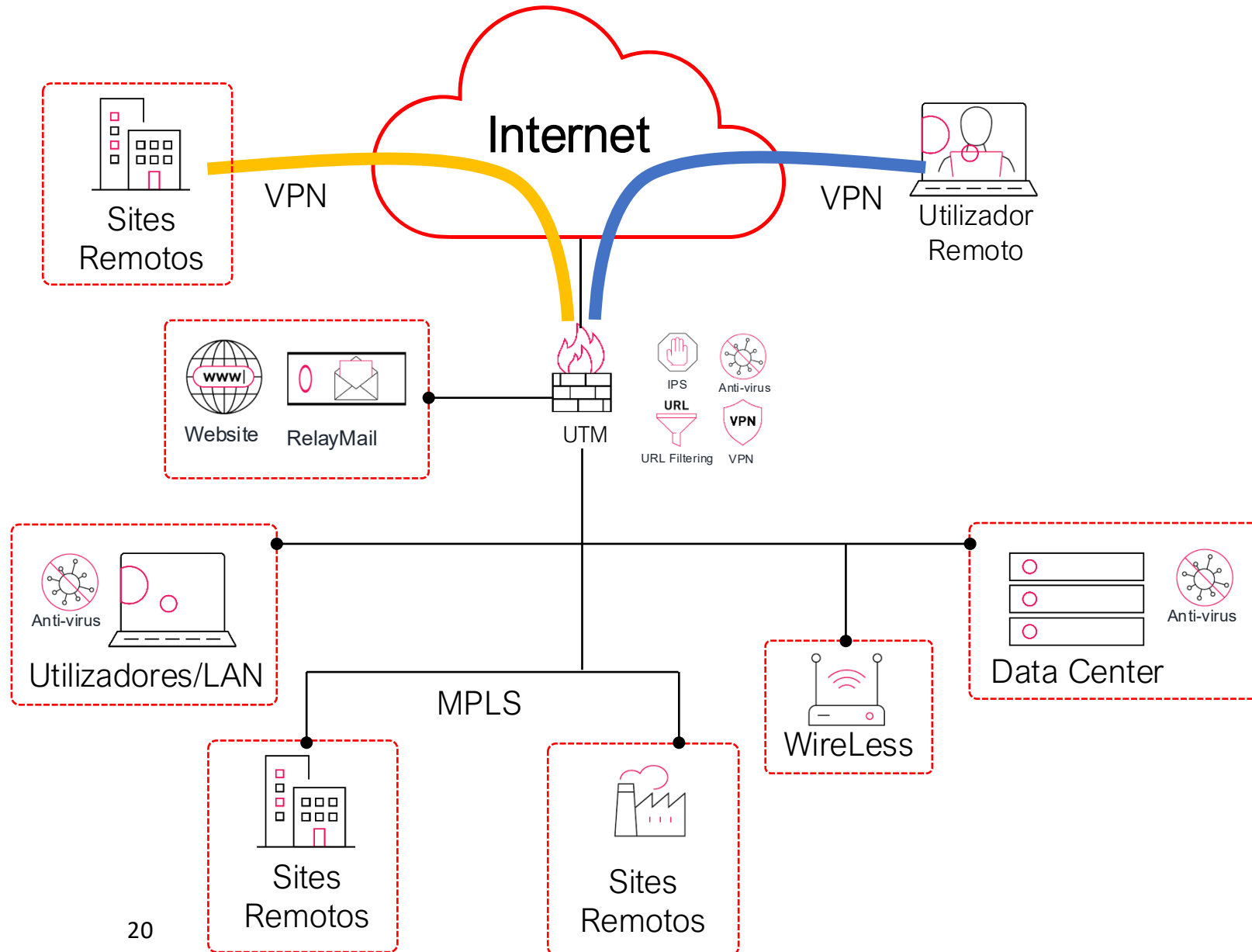
UTM

Antivírus

Redes privadas MPLS
Redes WireLess
Redes Industriais

Da FireWall à HybridMesh

WEB 1.0 2003



FireWall
IPS
URL Filtering
Antivirus
VPN

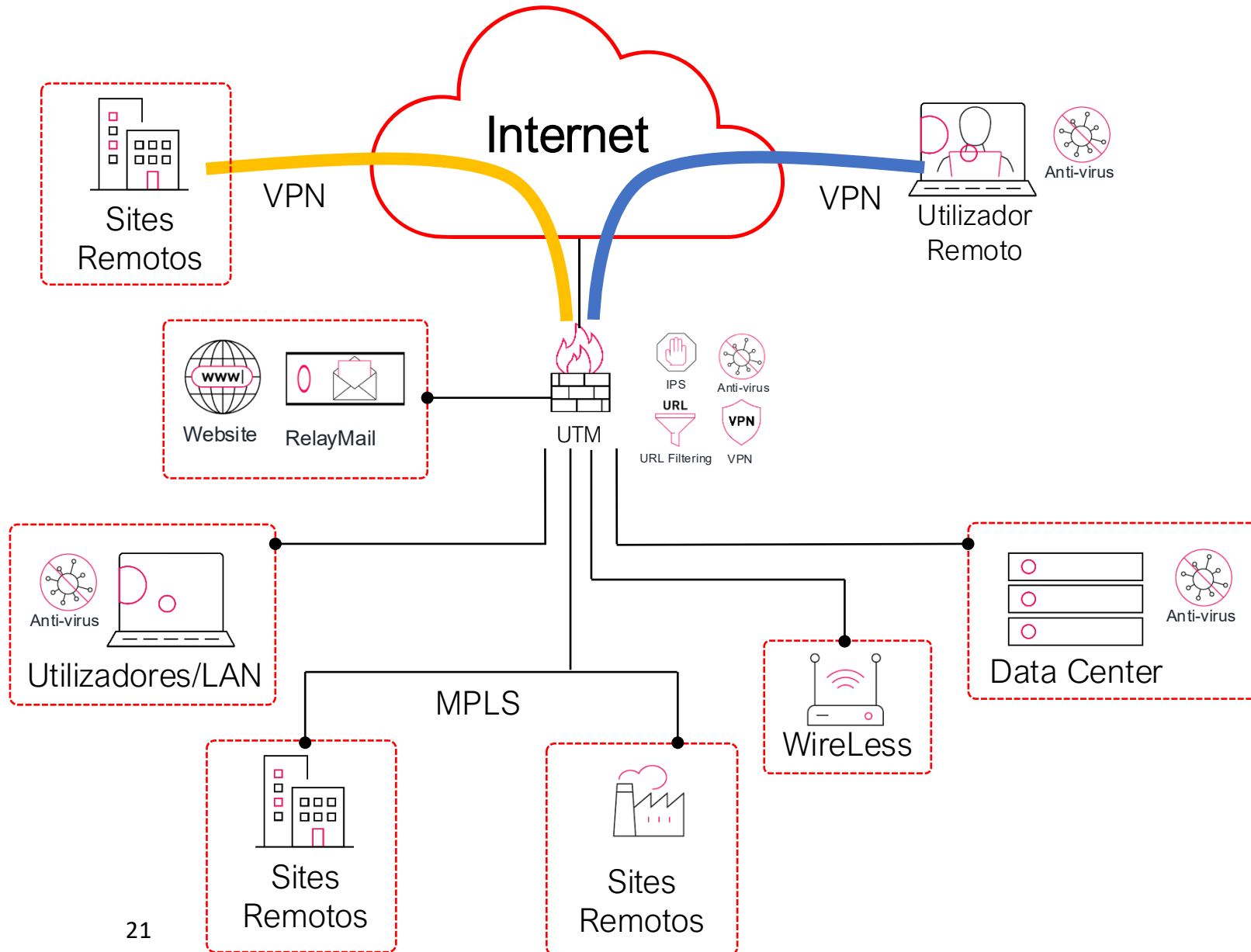
UTM

Antivírus

Redes privadas MPLS
Redes WireLess
Redes Industriais

Da FireWall à HybridMesh

WEB 1.0 2003



FireWall
IPS
URL Filtering
Antivirus
VPN

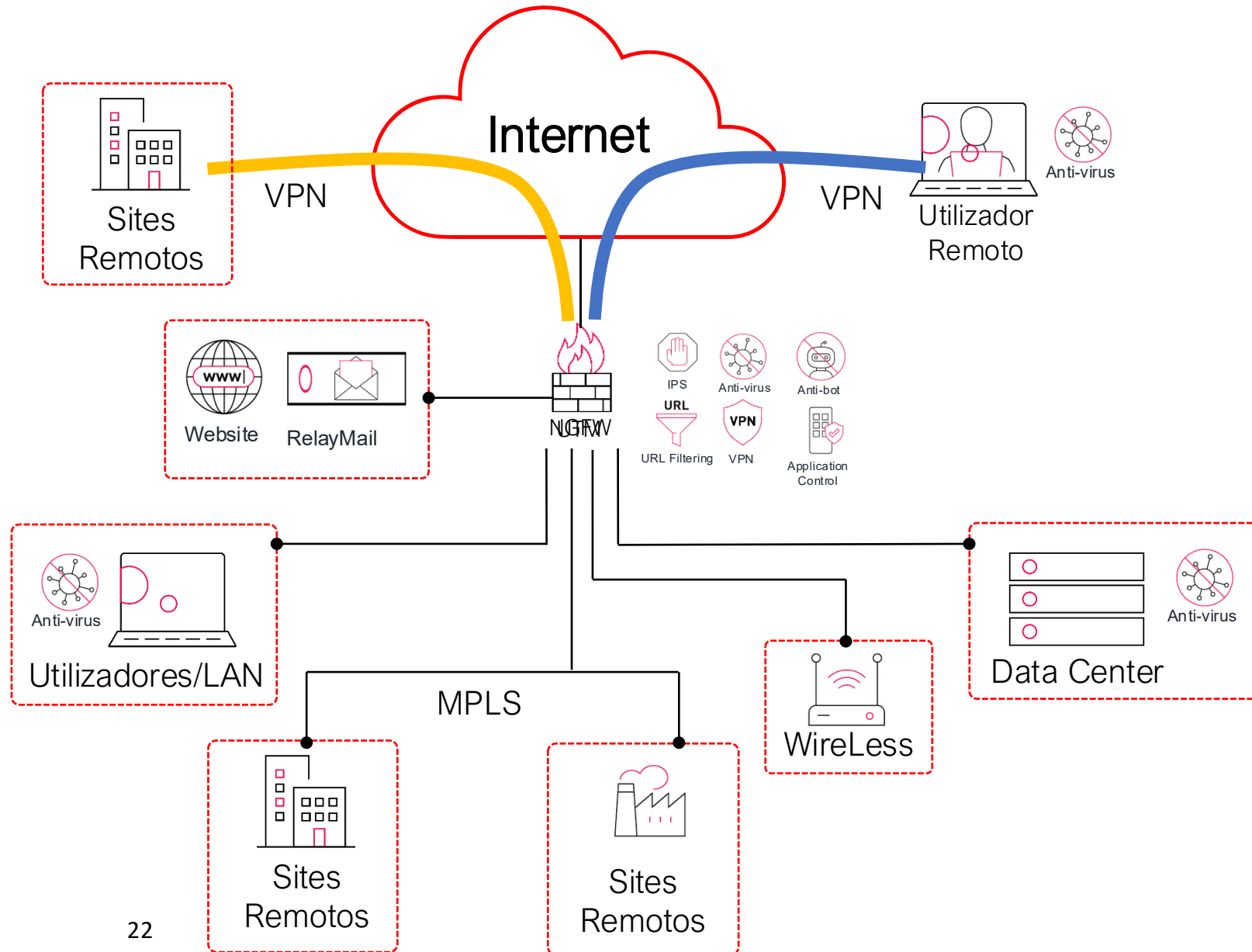
UTM

Antivírus

Segmentação
Redes privadas MPLS
Redes WireLess
Redes Industriais

Da FireWall à HybridMesh

WEB 2.0 2009



FireWall
IPS
URL Filtering
Antivirus
VPN
Anti-Bot
Application Control

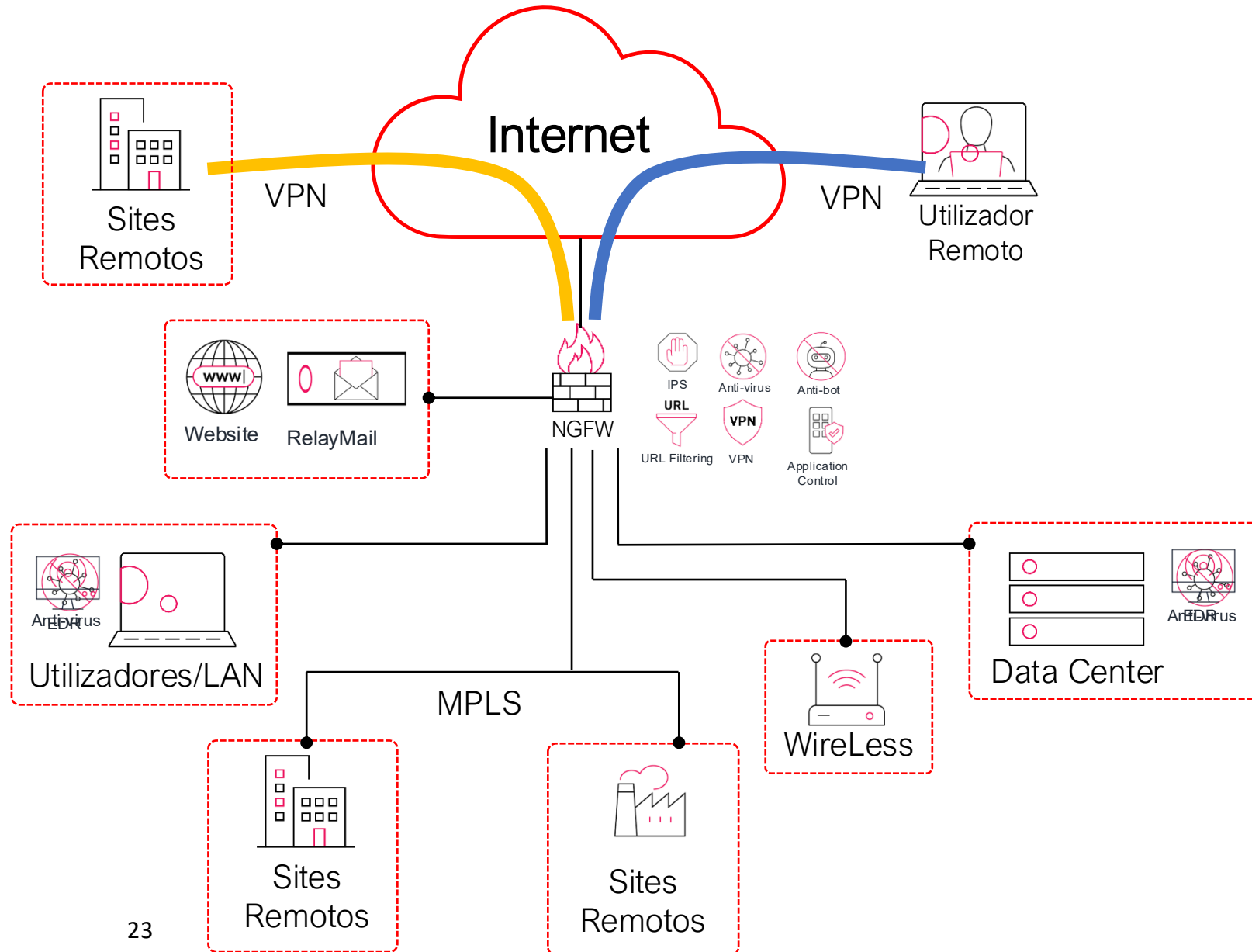
Antivírus

Aplicações
Colaboração Online
Google e Facebook

Da FireWall à HybridMesh

SaaS

2013



FireWall

IPS

URL Filtering

Antivirus

VPN

Anti-Bot

Application Control

NGFW

~~Antivírus~~

Vírus evoluem para Malware

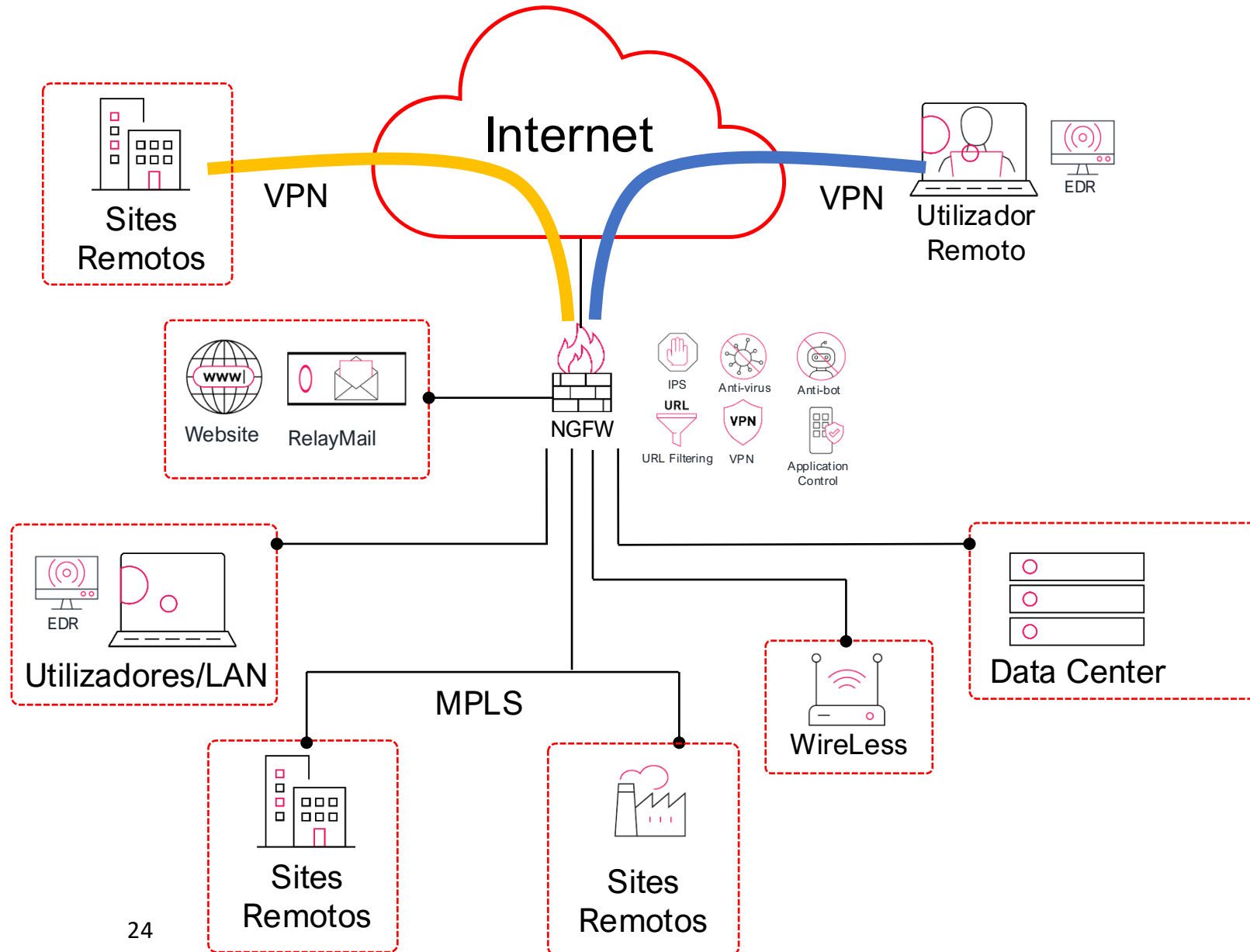
Aplicações

Colaboração Online

Google e Facebook

Da FireWall à HybridMesh

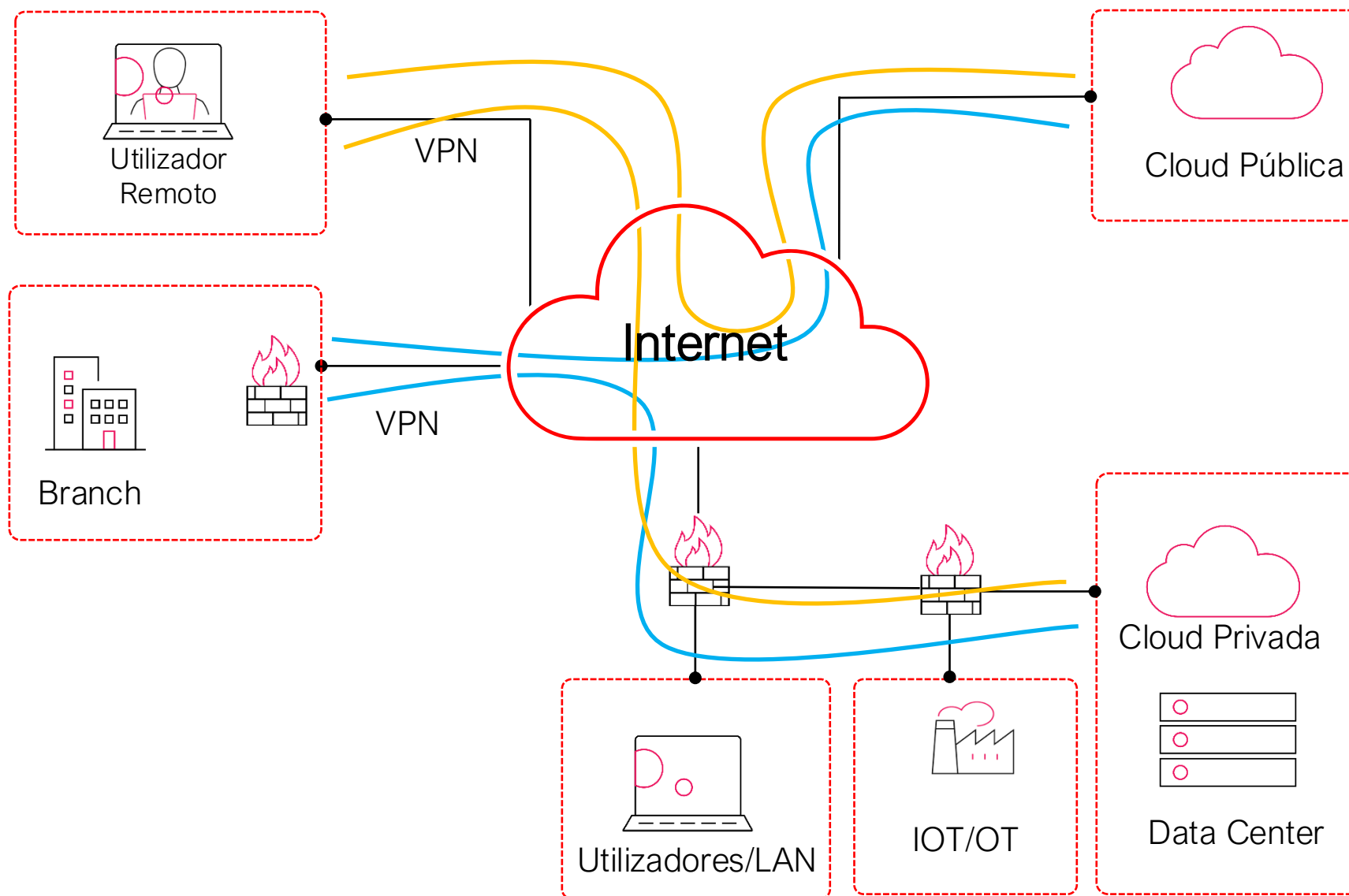
Cloud 2015



FireWall
IPS
URL Filtering
Antivirus
VPN
Anti-Bot
Application Control

NGFW

EDR
Cloud MainStream
Aplicações
Colaboração Online
Google e Facebook

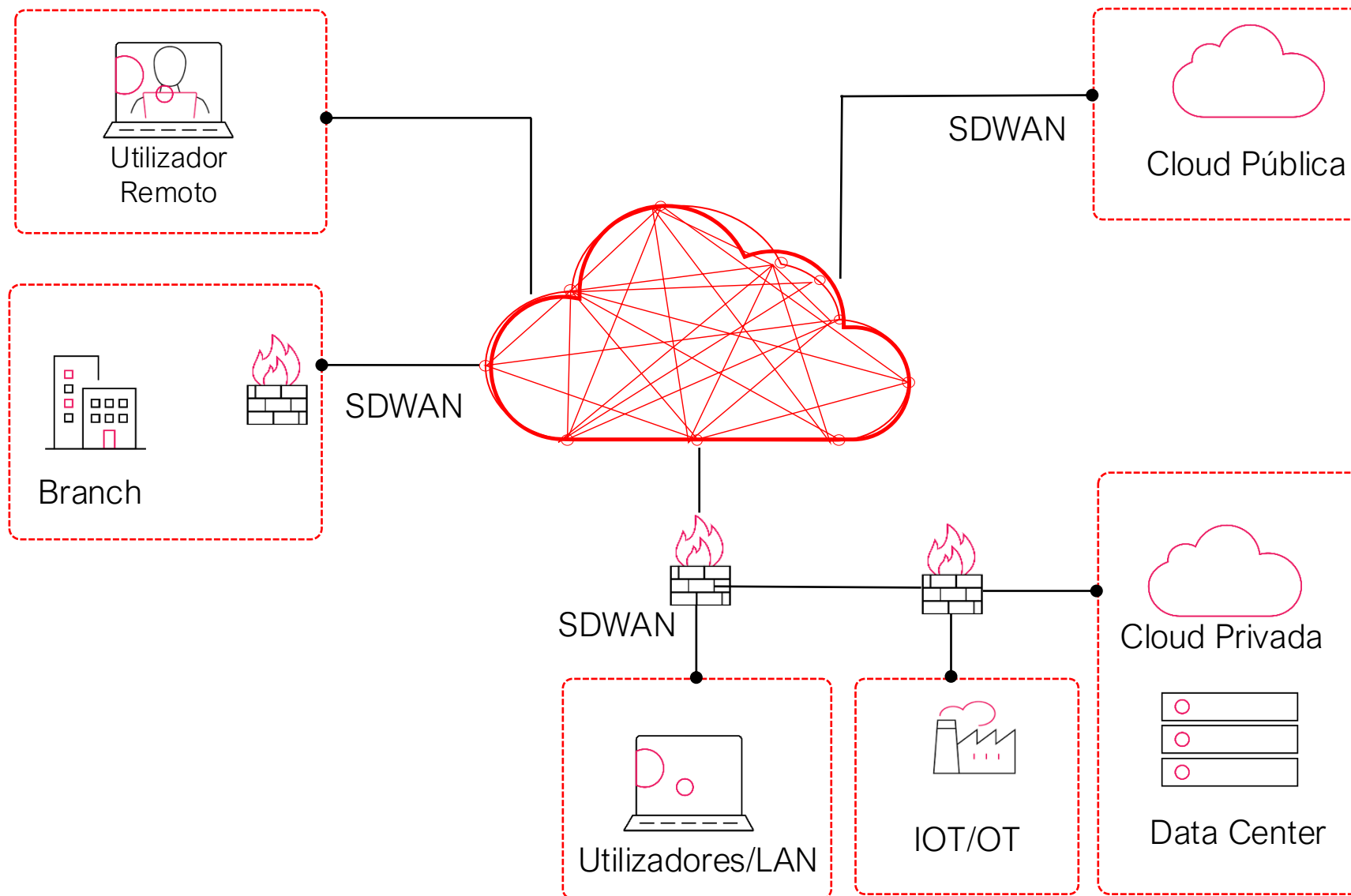


Perímetro estendido

**Recursos no
Datacenter e na
Cloud**

**Falta de visibilidade
Falta de Controlo**

**Muitos sistemas
para gerir**



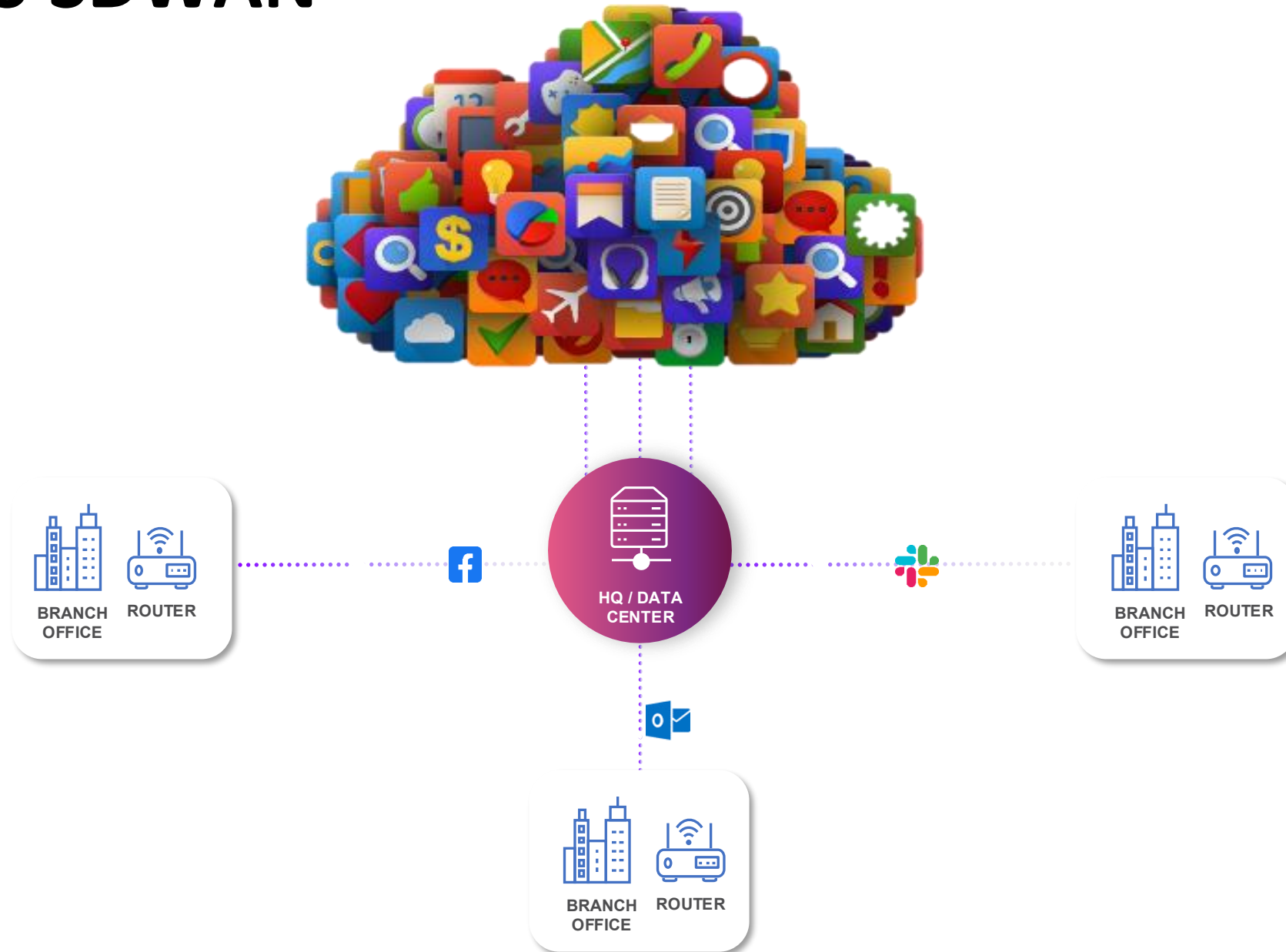
Perímetro estendido

**Recursos no
Datacenter e na
Cloud**

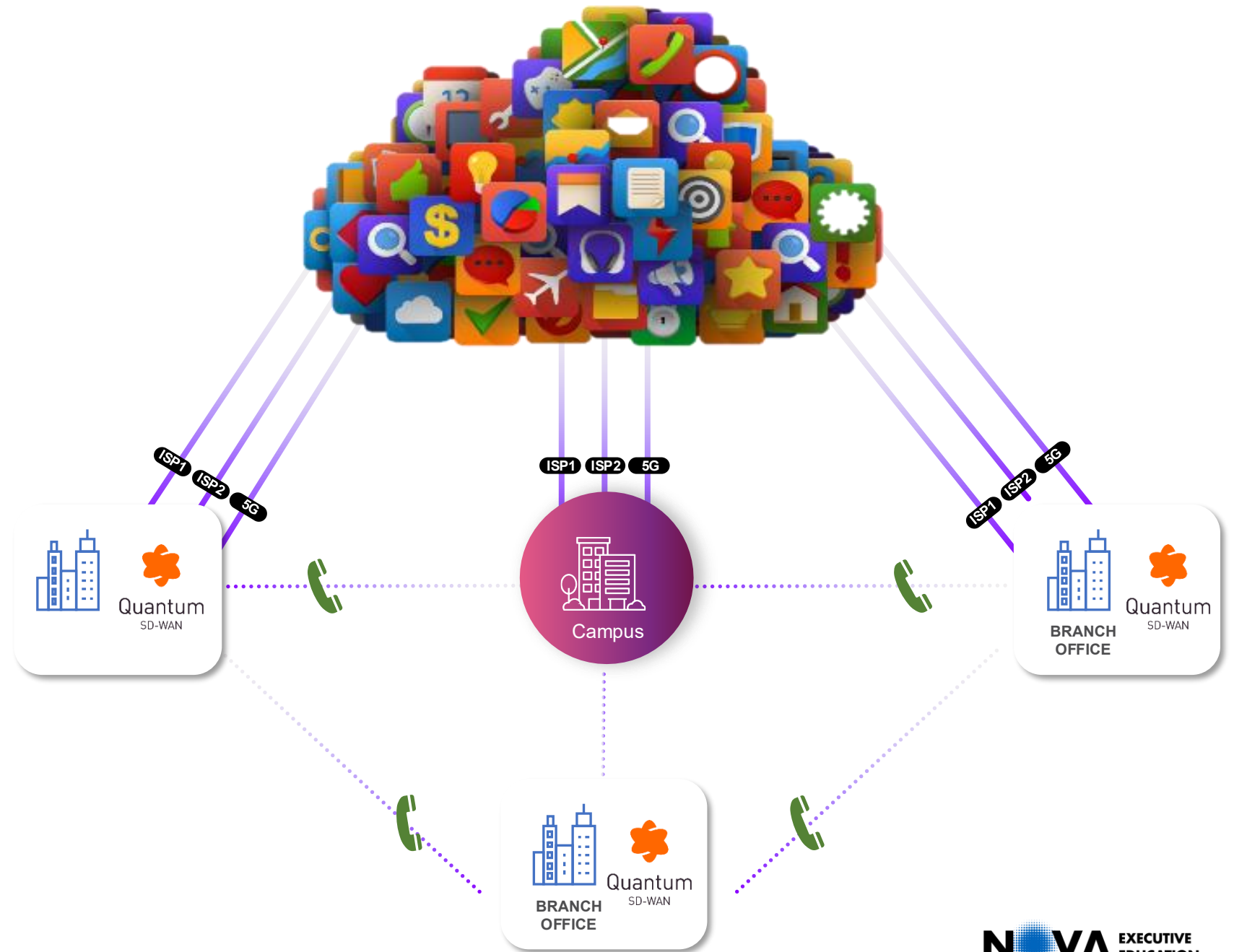
**Falta de visibilidade
Falta de Controlo**

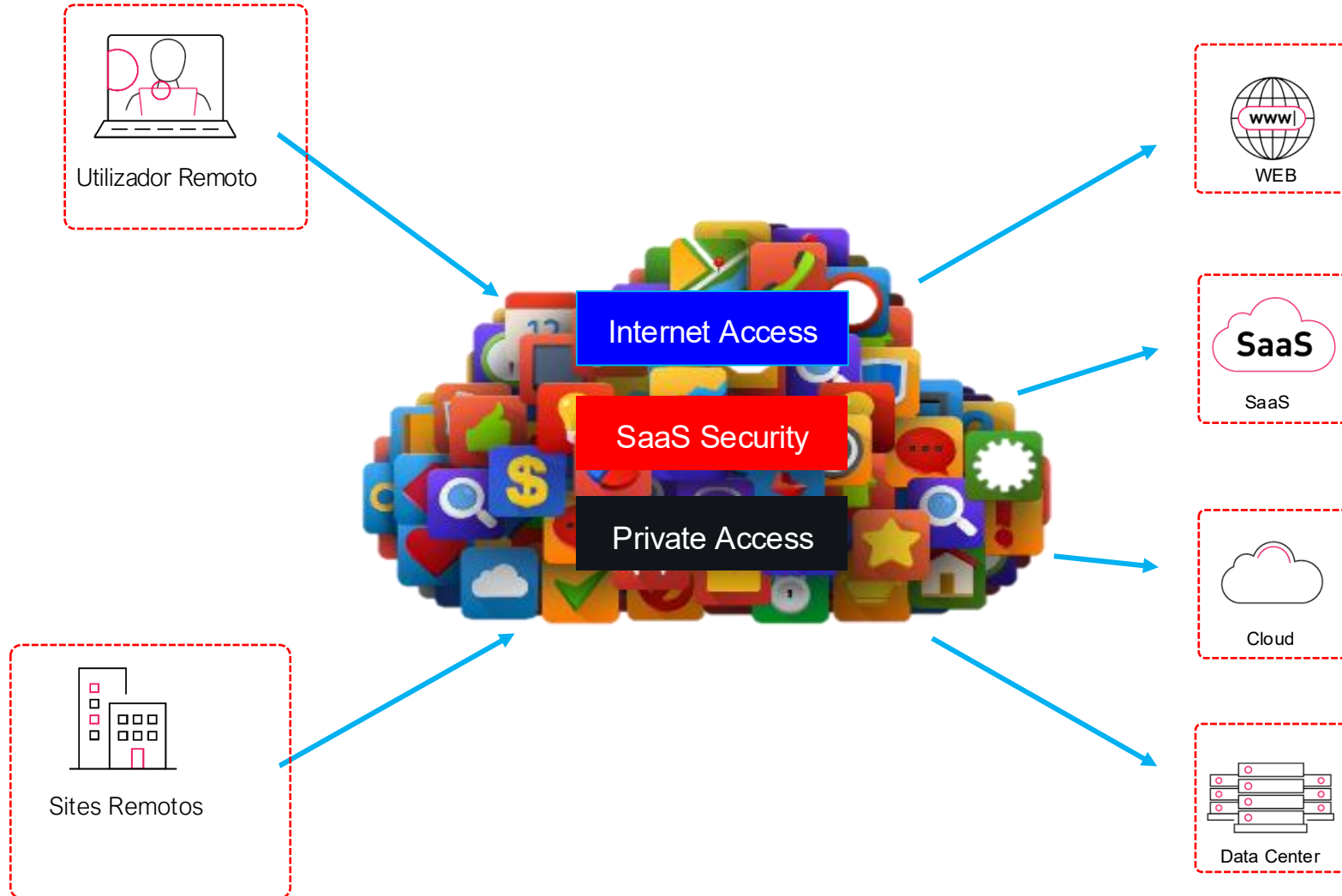
**Muitos sistemas
para gerir**

Antes do SDWAN



Com SDWAN

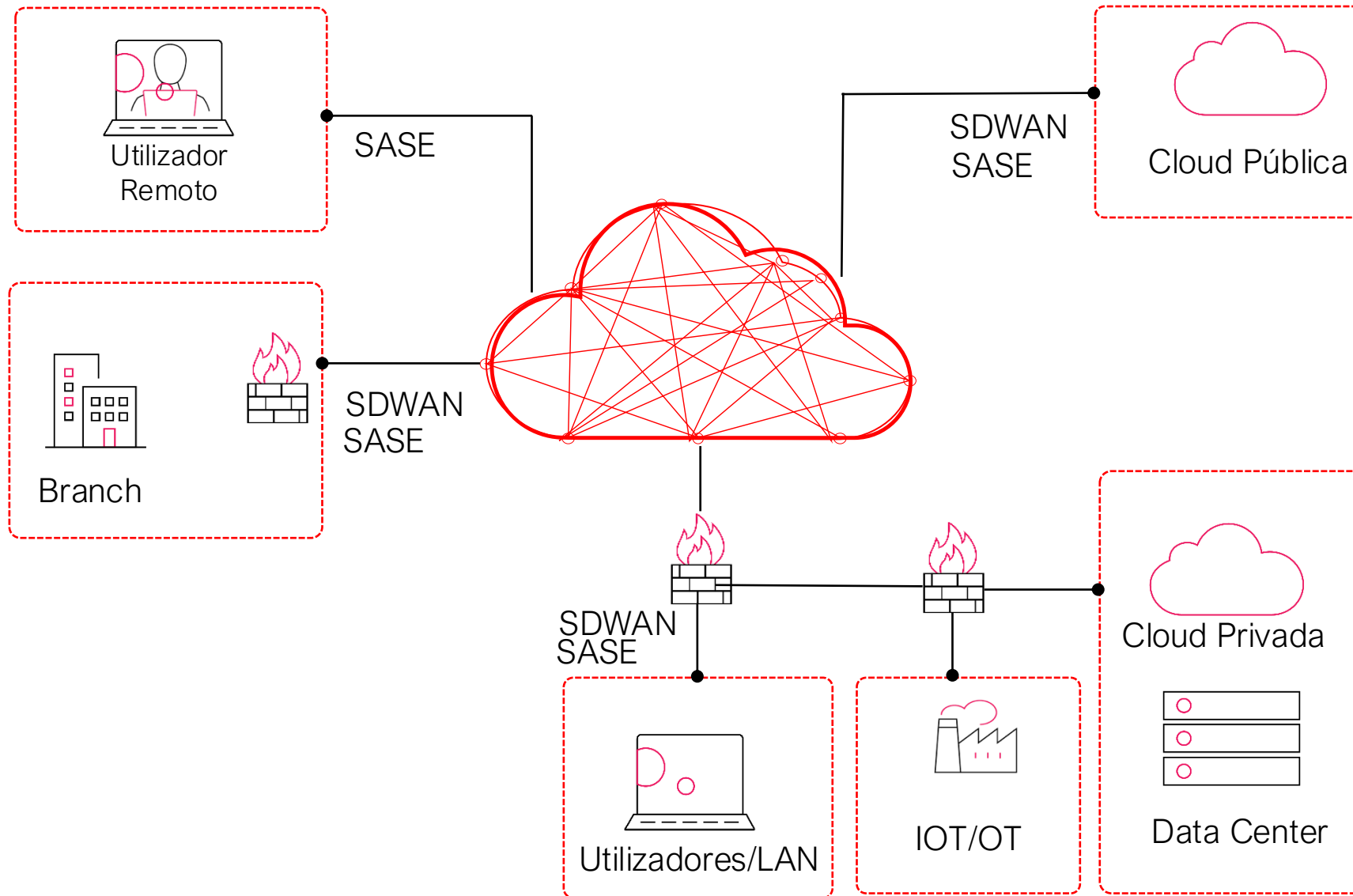




Da FireWall à HybridMesh

Covid

2020



Vamos todos para casa

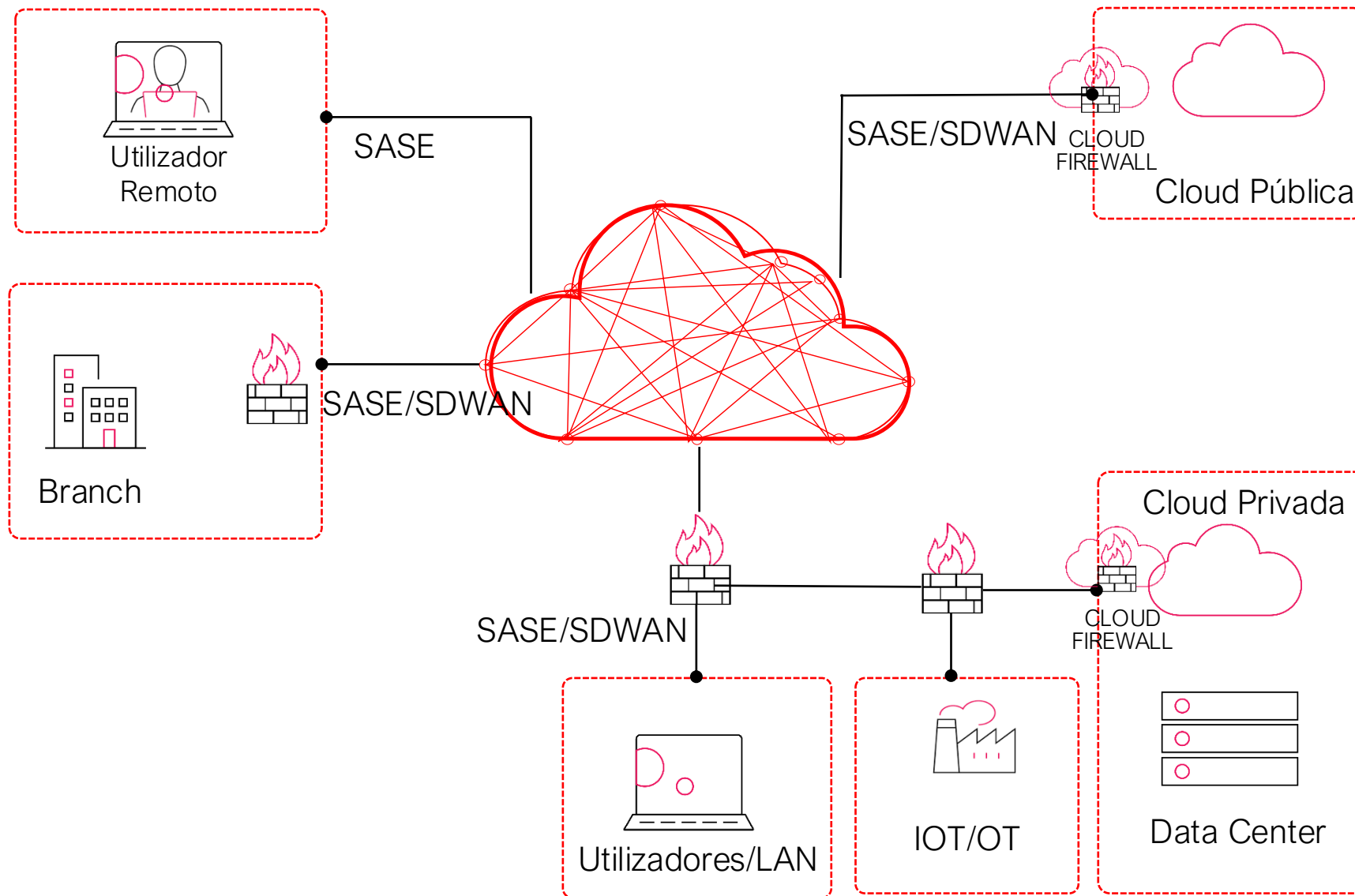
Trabalho remoto

**Falta de visibilidade
Falta de Controlo**

**Muitos sistemas
para gerir
SDWAN/SASE**

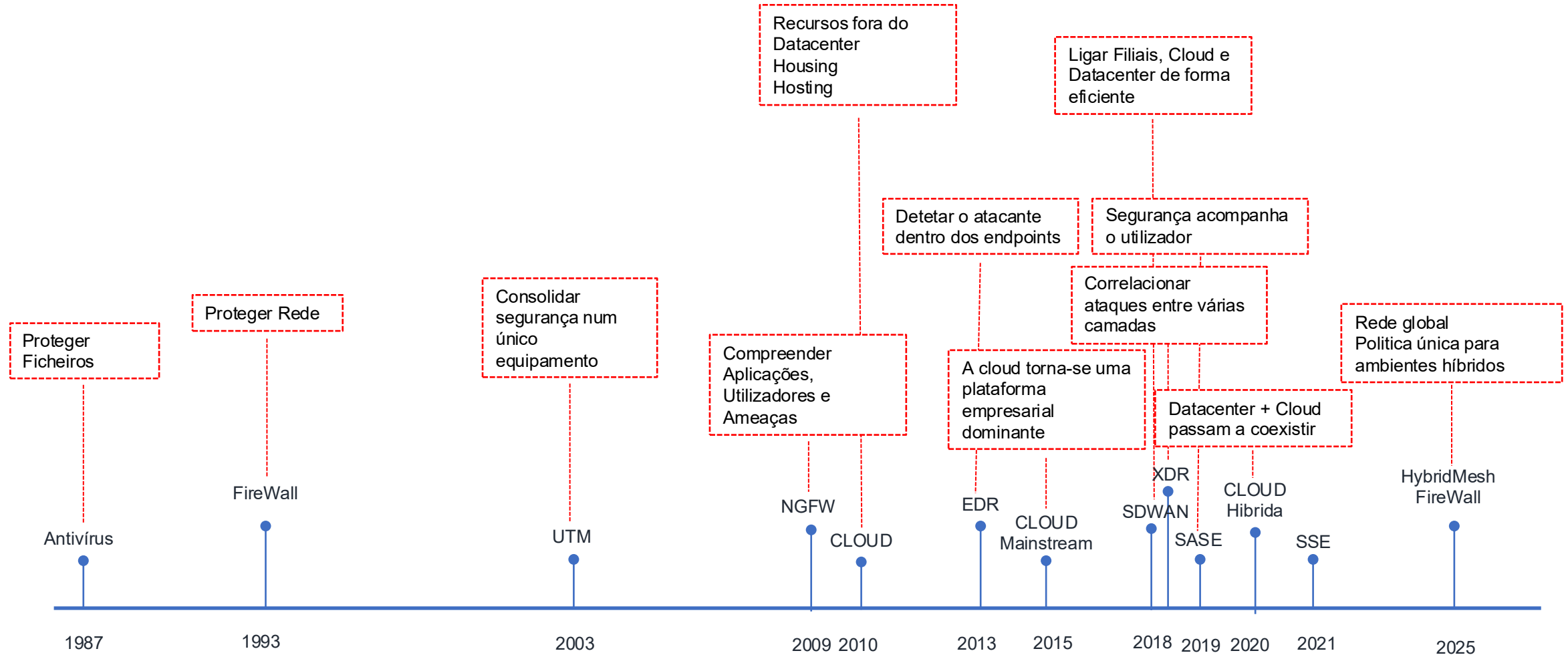
Da FireWall à HybridMesh

HybridMesh 2025



Gestão Centralizada
Politica Única
Gestão Identidades
Gestão Dispositivos
MFA
Inspeção total
Mesma Segurança
Segmentação
ZTNA

Da FireWall à HybridMesh





Tecnologias

NGFW Next Generation Firewall

- **Deep Packet Inspection (DPI)**

Inspeção profunda de pacotes: Conteúdo | Aplicações | Padrões Maliciosos

- **Application Awareness**

Redes sociais | Aplicações SaaS | Ferramentas de colaboração | IoT

- **Intrusion Prevention System (IPS)**

Bloqueia ataques e vulnerabilidades passíveis de serem exploradas

- **SSL Inspection**

Inspeção de tráfego encriptado

- **User Awareness**

Políticas baseadas no utilizador através da integração com diretórios como: Microsoft Active Directory | LDAP

- **Threat Intelligence**

Integração com feeds de inteligência para bloquear: Malware | Botnets | Ataques conhecidos

EDR - Endpoint Detection and Response

- **MONITORIZAÇÃO CONTÍNUA DO ENDPOINT**

Processos | Actividades do Utilizador | Alterações em Ficheiros | Conexões de Rede

- **DETEÇÃO COMPORTAMENTAL**

Atividades anómalas | Técnicas usadas por atacantes | Movimentos laterais

- **INVESTIGAÇÃO FORENSE**

Origem do ataque | Cadeia de eventos | Impacto na infraestrutura

- **RESPOSTA A INCIDENTES**

Isolamento de máquinas | Bloqueio de processos maliciosos | Remoção de malware

- **VISIBILIDADE COMPLETA DO ENDPOINT**

XDR – Extended Detection and Response

- **Correlação multi-domínio**

Analisa eventos provenientes de diferentes sistemas: phishing por email | login suspeito | execução de malware

- **Deteção avançada de ameaças**

Identifica atividades maliciosas por: análise comportamental machine learning | inteligência de ameaças

- **Investigação automatizada**

Cria automaticamente: timelines de ataque | análise de causa raiz | contexto do incidente

- **Resposta automatizada**

Executa ações como: isolamento de endpoint | bloqueio de utilizador | bloqueio de IP

- **Redução de ruído de alertas**

Consolida múltiplos alertas num incidente único

IAM & MFA - Identity and Access Management + Multi-Factor Authentication

- **Gestão do ciclo de vida das identidades**

Criação | alteração | revisão | remoção de contas e acessos.

- **Autenticação multifator**

Combina dois ou mais fatores: algo que sabe | tem | é.

- **Autorização e menor privilégio**

Acesso baseado em função, política e necessidade de negócio.

- **Single Sign-On e federação**

Uma identidade para aceder de forma controlada a várias aplicações.

- **Auditoria e governação de acessos**

Registo de atividades | revisões de acesso | apoio à conformidade.

NAC - Network Access Control

- **Descoberta e identificação de dispositivos**

Reconhece equipamentos geridos, BYOD, convidados, IoT e OT.

- **Avaliação da postura de segurança**

Verifica sistema operativo | atualizações | proteção de endpoint | certificados.

- **Autenticação e aplicação de políticas**

Decide quem e que dispositivo pode ligar-se, segundo identidade e contexto.

- **Segmentação e acesso diferenciado**

Coloca cada dispositivo na rede ou segmento adequado ao respetivo perfil.

- **Visibilidade e resposta**

Inventário | monitorização | isolamento ou bloqueio de dispositivos não conformes.

WAF – Web Application Firewall

- **Proteção contra ataques a aplicações**

Analisa e bloqueia: comandos maliciosos | payloads de ataque exploração de vulnerabilidades

- **Proteção contra ataques do OWASP Top 10**

Injection | Broken Authentication | Cross-Site Scripting

- **Proteção contra bots**

Deteta e bloqueia: Scraping automatizado | Ataques de bots | Abuso de aplicações.

- **Mitigação de ataques DDoS a aplicações**

Protege aplicações contra: Tráfego malicioso | Ataques volumétricos

- **Monitorização e visibilidade**

Permite: analisar padrões de tráfego | identificar tentativas de ataque | melhorar postura de segurança.

SDWAN - Software Defined Wide Area Network

- **Orquestração centralizada**

Configuração automática | Deployment rápido de filiais | Gestão centralizada

- **Dynamic Path Selection**

Seleção automática do melhor caminho: Latência | Jitter | Perda de pacotes

- **Utilização de múltiplos links**

Suporte para: MPLS | Internet broadband | 4G / 5G | Fibra

- **Application-aware routing**

Prioriza aplicações críticas: VoIP | ERP | SaaS | Videoconferência

- **Segurança integrada**

Muitas soluções incluem: Firewall | Segmentation | VPN

Integração com SASE

ZTNA - Zero Trust Network Access

- **Identidade e autenticação forte**

Validação do utilizador através de: IdP / SSO | MFA | função e grupo.

- **Avaliação do dispositivo e do contexto**

Verificação de: postura de segurança | localização | horário | nível de risco.

- **Acesso específico por aplicação**

O utilizador acede apenas às aplicações autorizadas, sem entrar na rede completa.

- **Menor privilégio e microsegmentação**

Limitação do acesso ao estritamente necessário, reduzindo exposição e movimento lateral.

- **Verificação contínua e visibilidade**

Reavaliação da sessão | registo da atividade | revogação do acesso se o contexto mudar.

SASE - Secure Access Service Edge

- **SD-WAN**

Gestão inteligente da conectividade entre: Filiais | Cloud | Utilizadores remotos

- **Secure Web Gateway (SWG)**

Protege acesso à internet: Filtragem de URL | Proteção contra | Malware | Controlo de navegação

- **Cloud Access Security Broker (CASB)**

Controla utilização de aplicações Cloud. Visibilidade de SaaS | Controlo de acesso | Proteção de dados

- **Zero Trust Network Access (ZTNA)**

Acesso privado baseado em Identidade, dispositivo e contexto

- **Data Loss Prevention (DLP)**

Identificação e control de saída indevida de informaçãno sensível

- **Firewall as a Service (FWaaS)**

Firewall entregue via Cloud: Inspeção de tráfego | Políticas de segurança | Proteção contra ameaças

HMF - Hybrid Mesh Firewall

- **Gestão centralizada de políticas**

Firewalls físicos | Firewalls virtuais | Firewalls Cloud

- **Consistência de segurança entre ambientes**

On-premise | Cloud | Edge | Workloads

- **Integração com ambientes Cloud**

Amazon Web Services | Microsoft | Google | Outros

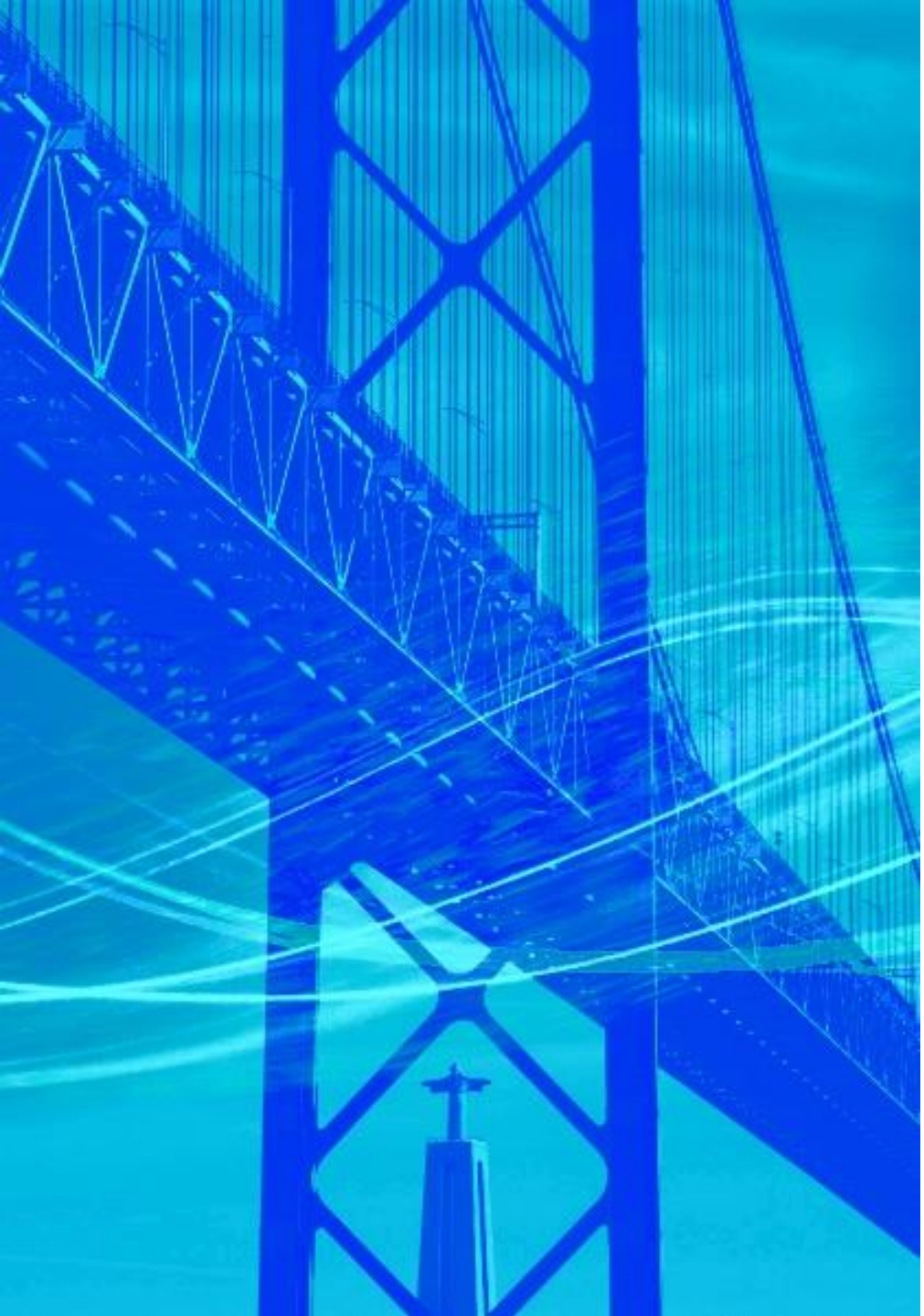
- **Segmentação de rede**

Permite segmentar: Aplicações | Workloads | Ambientes

- **Integração com Arquiteturas Zero Trust**

Permite aplicar políticas baseadas em: Identidade | Contexto | Localização

Estas tecnologias produzem sinais, bloqueiam comportamentos e registam atividade. O desafio seguinte é transformar toda essa informação em decisões.



Monitorização e Controlo

Transformar sinais dispersos em decisões de
segurança.

Porque monitorizamos?



Quem entrou?

Identidade, origem e método de autenticação



A que acedeu?

Aplicações, dados, serviços e segmentos consultados.



O que fez?

Ações, alterações, transferências e ligações realizadas.



O que mudou?

Configurações, privilégios, ficheiros e postura do dispositivo.



O que parece anómalo?

Comportamento fora do padrão ou incompatível com o contexto.

Do registo ao incidente

1

LOG

Registo técnico de uma ação ou comunicação.
Ex.: início de sessão, ligação, alteração de ficheiro.

2

EVENTO

Atividade interpretada dentro de um sistema.
Ex.: várias tentativas de autenticação falhadas.

3

ALERTA

Sinal que ultrapassa uma regra, limiar ou padrão.
Ex.: acesso invulgar seguido de transferência elevada.

4

INCIDENTE

Atividade maliciosa ou risco relevante confirmado.
Ex.: conta comprometida com acesso indevido.

Do registo ao incidente

Rede

NGFW | IDS/IPS | DNS | SD-WAN

Fluxos, aplicações, destinos e comunicações.

Endpoint

EDR | Proteção de Endpoint

Processos, ficheiros, comportamento e ligações.

Identidade

IAM | MFA | ZTNA

Autenticações, privilégios, contexto e sessões.

Cloud e SaaS

Cloud logs | CASB | aplicações

Atividade, configurações, dados e utilização.

Email e colaboração

Email Security | plataformas

Mensagens, anexos, links e partilhas.

Dados e aplicações

WAF | API | DLP

Pedidos, operações, exposição e saída de dados.



**Porque são
atacadas as
empresas**

Porque são atacadas as empresas?

Complexidade

- Superfície de ataque muito extensa
- Âmbito muito grande de soluções
- Falta de controlo e visibilidade de todas as soluções
- Hardware e software Legacy
- Vulnerabilidades Ocultas
- Dificuldade de aplicar uma política única
- Cultura organizacional fragmentada
- Diferentes equipas, com diferentes visões
- Equipa operacional sem sensibilidade de segurança
- Shadow IT

Porque são atacadas as empresas?

Governança (Governance)

- Falta de liderança e prioridades
- Políticas pouco claras, muito permissivas ou inexistentes
- Responsabilidades mal distribuídas, ou sem responsável claro
- Utilizadores com privilégio na máquinas

Porque são atacadas as empresas?

Procrastinação

- Não atualização dos sistemas
- Vulnerabilidades continuam disponíveis
- Muitas invasões acontecem dias ou semanas depois da divulgação de falhas — justamente porque as empresas demoram a agir.
- Adiar projectos de segurança
- Auditorias, conformidade e melhorias negligenciadas

Porque são atacadas as empresas?

Falta de princípios básicos de segurança

- Falta de Segmentação
- Falha por falta de KnowHow
- Procrastinação
- Governação fraca
- Pass Admin para vários sistemas (Password AD = Password Backup)
- Passwords Fracas
- Não implementação de MFA
- Falta de Política segurança unificada

Porque são atacadas as empresas?

Falta de recursos

- Profissionais qualificados
- Ferramentas desatualizadas ou inadequadas
- Resposta lenta a incidentes

Falta de Know-How

- Falha de configurações
- Políticas permissivas



Boas práticas

Boas práticas

Identidade

- MFA;
- Menor privilégio;
- Gestão de passwords;
- Revisão de acessos.

Boas práticas

Infraestrutura

- Segmentação;
- Atualizações;
- Proteção de Endpoint;
- Configuração segura.

Boas práticas

Resiliência

- Backups;
- Monitorização;
- Plano de resposta;
- Testes regulares.

Boas práticas

Pessoas e governação

- Formação;
- Responsabilidades claras;
- Políticas simples;
- Melhoria contínua.

...ideias para levar:

- 1. A cibersegurança é como as cebolas, feita de camadas;***
- 2. Proteger começa por saber o que tem valor;***
- 3. A rede moderna já não tem um único perímetro;***
- 4. Identidade, dispositivo e contexto condicionam o acesso;***
- 5. Prevenção sem visibilidade é insuficiente;***
- 6. Segurança exige pessoas, processos, tecnologia e melhoria contínua.***

Keep Learning. Keep in touch.

✉ info.executive@fct.unl.pt

