CYLOCK / UFS

Infraestrutura de Redes Aplicada à Cibersegurança

Como redes, segmentação e controles de segurança influenciam a defesa, os testes autorizados e a investigação de incidentes.

DISPOSITIVOS • SEGMENTAÇÃO • FIREWALL • IDS / NSM

AULA DE 39 MINUTOS

Liga Acadêmica de Cibersegurança

Por que redes são essenciais para a cibersegurança?

Uma rede é um caminho de comunicação, uma superfície de ataque e uma fonte de evidências.

01

Superfície de ataque

Serviços expostos, configurações incorretas e acessos desnecessários.

02

Camada de defesa

Segmentação, políticas de acesso, criptografia e monitoramento.

03

Fonte de evidências

IPs, portas, horários, conexões e registros apoiam investigações.

BLUE TEAM

Proteger e responder

RED TEAM

Avaliar riscos autorizados

FORENSE DIGITAL

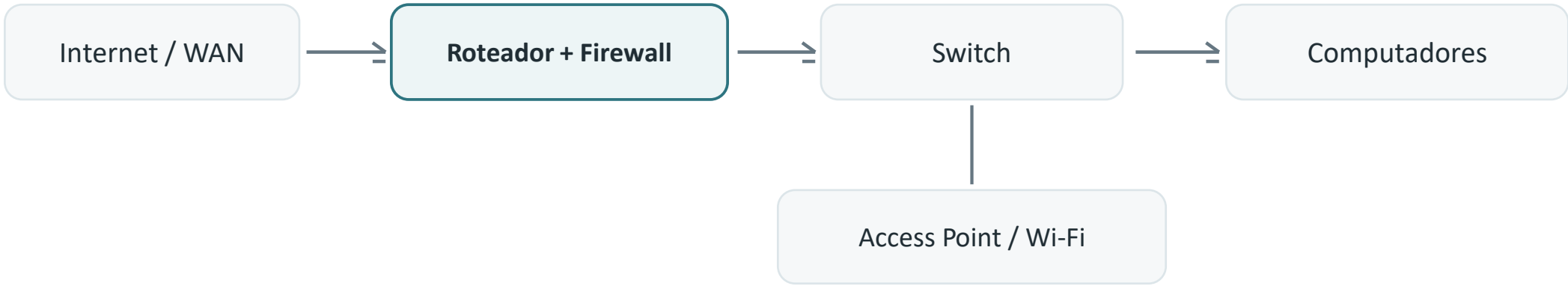
Reconstruir incidentes

PERGUNTA **Um computador comprometido permite acessar toda a empresa?**

Como os dispositivos de uma rede se comunicam?

Começamos com a estrutura mais simples da nossa empresa fictícia.

ETAPA 1 — REDE BÁSICA



SWITCH

Conecta dispositivos locais.

ROTEADOR

Liga redes diferentes.

ACCESS POINT

Disponibiliza Wi-Fi.

FIREWALL

Aplica regras de tráfego.

LAN, WLAN e WAN: três contextos diferentes

O meio de acesso e o alcance da rede mudam os riscos e os controles necessários.

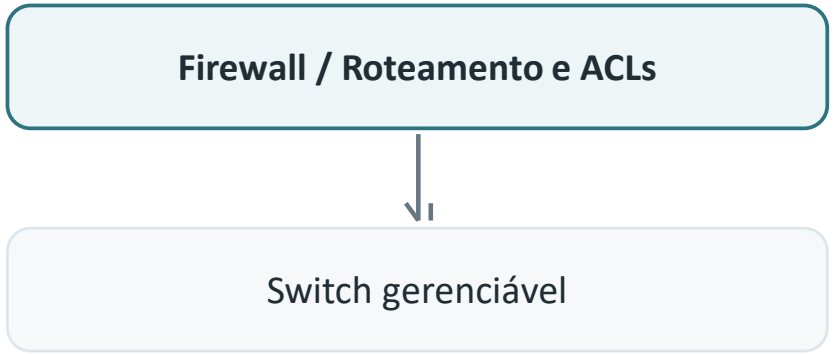
LAN	**Local Area Network** Rede local cabeada ou mista: casa, laboratório e escritório.	Segurança: segmentação e movimentação lateral.
WLAN	**Wireless Local Area Network** Rede local com conectividade sem fio por Wi-Fi.	Segurança: WPA2/WPA3, autenticação e APs não autorizados.
WAN	**Wide Area Network** Interliga redes distantes, como unidades em cidades diferentes.	Segurança: proteção de enlaces e disponibilidade.

PERGUNTA Conectar-se ao Wi-Fi da empresa significa acessar a rede interna?

VLANs e rede de gerenciamento

Dispositivos diferentes não precisam compartilhar o mesmo domínio de comunicação.

ETAPA 2 — ZONAS LÓGICAS



VLAN 10

Funcionários

10.10.10.0/24

VLAN 20

WLAN convidados

10.10.20.0/24

VLAN 30

Servidores

10.10.30.0/24

VLAN 50

Gerenciamento

10.10.50.0/24

Rede de gerenciamento: acesso administrativo restrito, MFA, jump host e registros.

VLAN separa o tráfego em camada 2. O isolamento entre segmentos exige regras de acesso.

Servidores: ativos críticos de uma organização

Um servidor disponibiliza recursos e pode armazenar dados, credenciais ou registros importantes.

WEB	Sites e aplicações
DNS	Resolução de nomes
ARQUIVOS	Compartilhamento de dados
BANCO DE DADOS	Dados das aplicações
AUTENTICAÇÃO	Identidades e acessos

POR QUE PROTEGER?

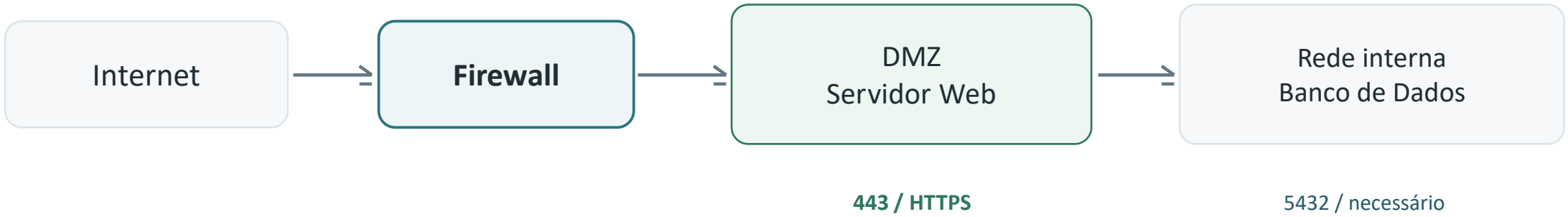
- Serviços expostos ampliam a superfície de ataque.
- Configurações e atualizações são críticas.
- Logs apoiam análise de incidentes.

PERGUNTA **Quais servidores precisam receber tráfego diretamente da Internet?**

DMZ: expondo serviços sem expor toda a empresa

A DMZ hospeda serviços públicos e restringe os caminhos para a rede interna.

ETAPA 3 — ACESSO PÚBLICO CONTROLADO



Internet → Web (HTTPS)

PERMITIR

Internet → Banco de Dados

BLOQUEAR

Web → Banco de Dados

RESTRINGIR

Se um servidor público for comprometido, o acesso à rede interna deve continuar limitado.

Firewall: quem pode se comunicar com quem?

Regras consideram origem, destino, protocolo, porta e, em alguns casos, estado e aplicação.

ORIGEM	DESTINO	PORTA	POLÍTICA
Internet	Servidor Web / DMZ	TCP 443	PERMITIR
Internet	Banco de Dados	TCP 5432	BLOQUEAR
Convidados	Rede de gerenciamento	Qualquer	BLOQUEAR
Admin autorizado	Jump Host	TCP 22	PERMITIR

STATELESS

Pacote isolado

STATEFUL

Estado da conexão

NGFW

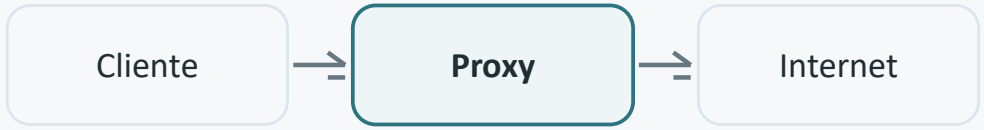
Controle avançado

Proxy: intermediário das comunicações

Duas arquiteturas com objetivos diferentes — controlar clientes ou proteger a publicação de serviços.

FORWARD PROXY

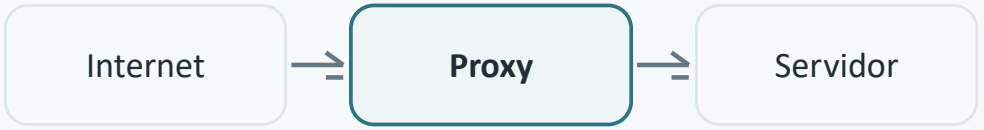
Intermedeia a saída de clientes



Filtragem web, autenticação e logs de navegação.

REVERSE PROXY

Intermedeia a entrada para servidores



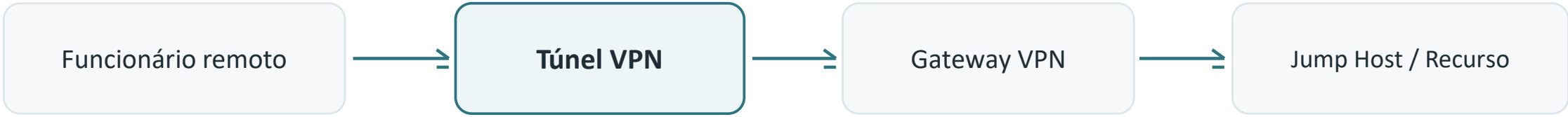
Publicação de aplicações, TLS, WAF e balanceamento.

NA NOSSA REDE Reverse proxy na DMZ, intermediando conexões externas para a aplicação.

VPN: túnel protegido não é confiança automática

VPNs conectam usuários ou redes por um túnel criptografado sobre infraestrutura não confiável.

ETAPA 4 — ACESSO REMOTO



MFA Exigir autenticação forte.

MENOR PRIVILÉGIO Liberar somente os recursos necessários.

POSTURA DO DISPOSITIVO Verificar se o endpoint atende aos controles.

MONITORAMENTO Registrar sessões e acessos.

PERGUNTA **Se o computador remoto estiver infectado, o túnel torna esse dispositivo seguro?**

IDS, IPS e NSM: identificar, agir e investigar

Ferramentas diferentes fornecem níveis distintos de prevenção e visibilidade.

IDS

DETECTA

Monitora tráfego ou eventos e gera alertas.

Suricata / Snort em modo IDS

IPS

PREVINE

Atua em linha e pode bloquear comunicações.

Suricata / Snort em modo IPS

NSM

INVESTIGA

Coleta e interpreta evidências de comunicação.

Zeek e análise de logs

Um alerta exige contexto: falsos positivos existem, e ausência de alerta não prova ausência de ataque.

Onde posicionar sensores de segurança?

A cobertura de detecção depende do ponto de observação e da disponibilidade do tráfego.

SENSORES DE REDE — PONTOS DE COLETA

SENSOR 1

PERÍMETRO

Entrada e saída da Internet.

SENSOR 2

DMZ

Serviços publicados.

SENSOR 3

SEGMENTOS

Comunicações internas.

COMO O SENSOR RECEBE O TRÁFEGO?

- Cópia por SPAN / espelhamento ou TAP, entre outros mecanismos.
- Criptografia pode limitar o conteúdo inspecionável; o ponto de captura importa.

Um incidente, três perspectivas de trabalho

Cenário: um servidor web tenta acessar a rede de gerenciamento sem autorização.

BLUE TEAM

Defesa

O tráfego foi bloqueado? Houve alerta? Precisamos conter o servidor?

RED TEAM

Avaliação autorizada

A segmentação limita o avanço? Há caminhos indevidos ou controles insuficientes?

FORENSE DIGITAL

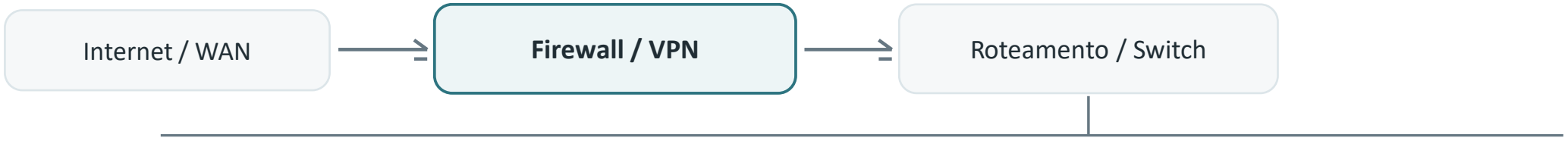
Investigação

Quando e de onde partiu a conexão? Que registros corroboram a sequência?

Os mesmos fluxos de rede servem como superfície de teste, pontos de bloqueio e evidências.

Desafio: você é responsável por esta empresa

Arquitetura completa. Sua missão: definir acessos e interpretar os sinais de um incidente.



LAN — funcionários
10.10.10.0/24

WLAN — convidados
10.10.20.0/24

Servidores internos
10.10.30.0/24

DMZ — servidor web
10.10.40.0/24

Rede de gerenciamento
10.10.50.0/24

VPN — acesso remoto
10.10.60.0/24

IDS / NSM: sensores na DMZ e nos segmentos internos, com registros para análise.

Missão 1 — Você é o firewall

Para cada fluxo, a turma decide: permitir, bloquear ou restringir?

COMUNICAÇÃO	PORTA	DECISÃO DA TURMA
Internet → Servidor Web	443 / HTTPS	□ permitir □ bloquear
WLAN convidados → Banco de Dados	5432 / TCP	□ permitir □ bloquear
Servidor Web → Banco de Dados	5432 / TCP	□ permitir □ bloquear
Internet → Rede de Gerenciamento	22 / SSH	□ permitir □ bloquear
Administrador via VPN → Jump Host	22 / SSH	□ permitir □ bloquear
Servidor da DMZ → Rede de Gerenciamento	22 / SSH	□ permitir □ bloquear

Justifiquem as escolhas: origem, destino, porta e necessidade de negócio.

Missão 2 — O SOC recebeu quatro eventos

Analisem os registros e decidam o que é esperado, anômalo e quais evidências faltam.

10:02	**REVERSE PROXY**	Acesso HTTPS externo recebido pelo servidor web da DMZ.
10:04	**FIREWALL · DENY**	Servidor Web (10.10.40.10) → Gestão (10.10.50.10), porta 22.
10:05	**FIREWALL · ALLOW**	Servidor Web (10.10.40.10) → Banco de Dados (10.10.30.20), porta 5432.
10:06	**IDS · ALERT**	Tentativas de conexão do servidor web para vários dispositivos da LAN.

DEBATAM EM GRUPOS

1. Qual alerta priorizar? 2. O que pode ser legítimo? 3. Quais logs buscar?

O que os registros realmente demonstram?

Um alerta é o início da investigação — não uma prova isolada de comprometimento.

10:02	**Conexão pública**	Acesso esperado em um serviço web, mas necessita contexto.
10:04	**Bloqueio de gestão**	A política funcionou; a tentativa pode indicar risco.
10:05	**Banco de Dados**	Fluxo potencialmente legítimo: conferir aplicação e origem.
10:06	**Anomalia interna**	Investigar a série de conexões e procurar outros sinais.

Conclusão da atividade: correlacionar firewall, IDS, proxy e logs de servidores.

Laboratório recomendado e preparação para OSI

Consolidar a arquitetura antes de estudar formalmente a comunicação em camadas.

PRÁTICA COMPLEMENTAR

TryHackMe

Secure Network Architecture

Segmentação, zonas de segurança e políticas de acesso.

tryhackme.com/room/introtosecurityarchitecture

PARA A PRÓXIMA AULA

Modelo OSI

- As sete camadas e suas funções.
- Protocolos associados a cada camada.
- Ataques e controles por camada.

Pergunta para estudar: em quais camadas um firewall pode atuar?