

Relatório Técnico de Análise de Segurança – Lab Segmentação de Rede

Autor: Lucas Rocha **Data:** 27 de julho de 2025 **Versão:** 1.1

Sumário Executivo

A análise de segurança da rede corporativa revelou falhas arquiteturais críticas que comprometem a confidencialidade, integridade e disponibilidade dos dados e serviços da empresa. Foi identificada uma inversão completa da política de segmentação de rede, onde servidores de infraestrutura crítica foram encontrados operando na rede de visitantes (`guest_net`), enquanto dispositivos pessoais de usuários foram alocados na rede de infraestrutura (`infra_net`). Adicionalmente, foi detectado o uso de protocolos inseguros (FTP), a presença de software obsoleto (OpenLDAP) e configurações de serviço permissivas. As recomendações prioritárias focam na re-segmentação imediata da rede e na implementação de regras de firewall para mitigar os riscos mais urgentes.

Objetivo

Analisar a topologia e configuração da rede corporativa simulada para identificar vulnerabilidades, falhas de segmentação e riscos operacionais que possam expor a organização a ameaças cibernéticas.

Escopo

O escopo do teste abrangeu o ambiente simulado, incluindo três segmentos de rede distintos: `corp_net` (10.10.10.0/24), `guest_net` (10.10.30.0/24) e `infra_net` (10.10.50.0/24), e todos os ativos de TI contidos neles.

Metodologia

A análise foi conduzida através de uma abordagem de reconhecimento ativo na rede. As seguintes ferramentas foram utilizadas para mapeamento de rede, descoberta de hosts, escaneamento de portas e identificação de serviços:

- **Ferramentas:** `nmap`, `rustscan`, `telnet`, `smbclient`, `ldapsearch`.
- **Processo:**
 1. Descoberta de hosts ativos em cada sub-rede.
 2. Escaneamento completo de portas TCP (`1-65535`) para cada host identificado.
 3. Análise de banners e versões dos serviços para identificar tecnologias e potenciais vulnerabilidades.
 4. Testes de autenticação anônima nos serviços expostos.
 5. Consolidação e análise dos dados para elaboração do diagnóstico.

Diagrama de Rede

Os diagramas abaixo ilustram a arquitetura de rede encontrada e a arquitetura recomendada para correção das falhas de segurança.

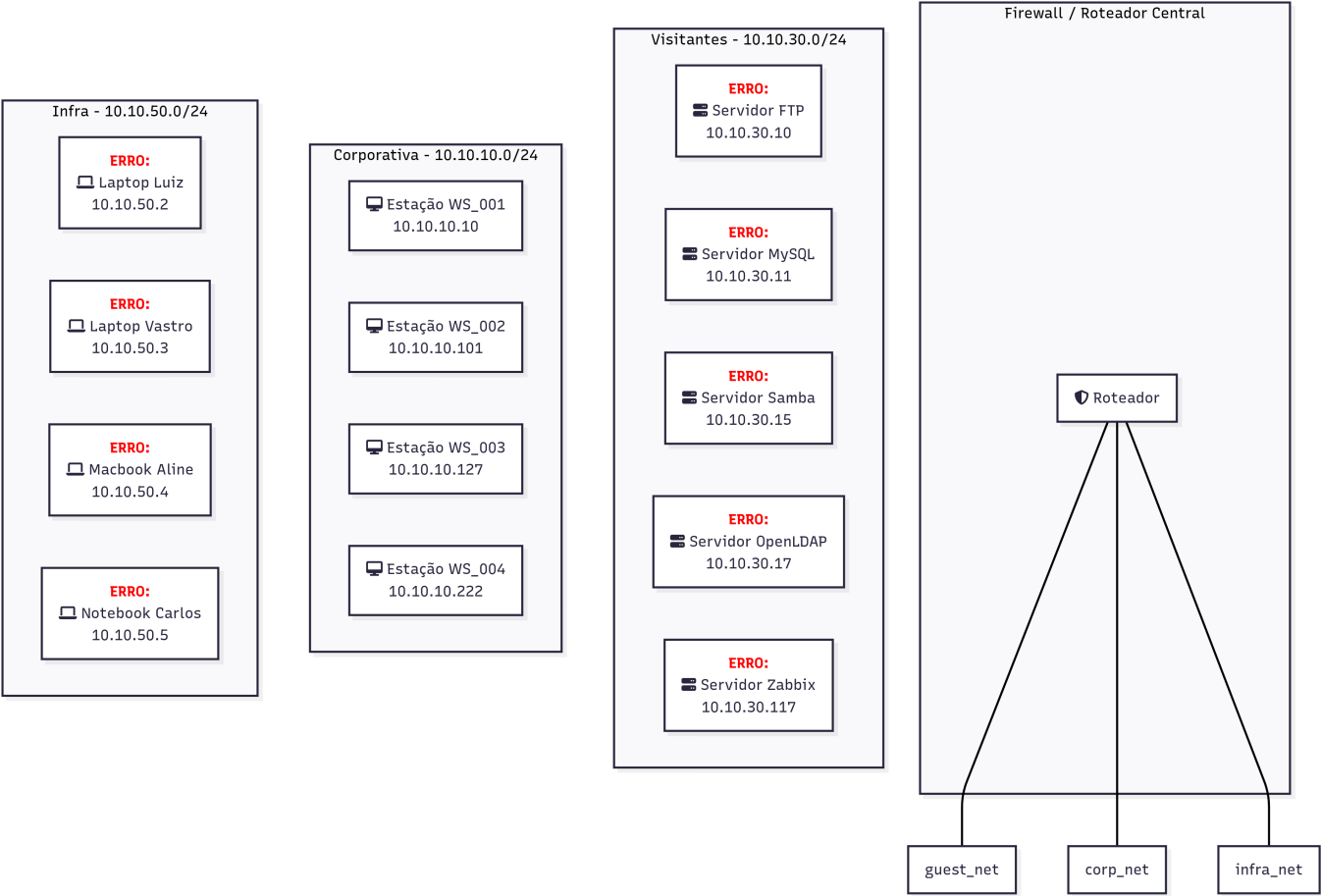


Figura 1: Arquitetura atual da rede, demonstrando as falhas críticas de segmentação.

Diagnóstico (Achados)

Achado 1: Falha Crítica de Segmentação – Servidores de Infraestrutura na Rede de Visitantes

- **Hosts:** ftp-server, mysql-server, samba-server, openldap, zabbix-server
- **IPs:** Segmento 10.10.30.0/24 (guest_net)
- **Risco Identificado (CRÍTICO):** Toda a infraestrutura de TI crítica, incluindo o servidor de autenticação (OpenLDAP), banco de dados MySQL e servidor de arquivos Samba, está localizada na rede menos confiável da empresa. Isso elimina a proteção que a segmentação deveria oferecer.
- **Evidência:** Os scans do nmap da guest_net mostram os hosts com nomes *_infra_net possuindo IPs na faixa 10.10.30.0/24.

```
root@486ef7dc9d31: /home/analyst

15 A analyst está conectada na rede guest_net com IP Dinâmico em 10.10.30.0/24.
16 A analyst está conectada na rede infra_net com IP Dinâmico em 10.10.50.0/24.
17
18 ---
19
20 ## 📶 Acesso às Redes
21
22 O ambiente está segmentado em 3 redes principais:
23
24 | Rede | Subnet | Descrição |
25 |-----|-----|-----|
26 | corp_net | 10.10.10.0/24 | Rede corporativa (estações e web server) |
27 | guest_net | 10.10.30.0/24 | Rede de visitantes e dispositivos pessoais |
28 | infra_net | 10.10.50.0/24 | Rede de infraestrutura crítica (servidores) |
29
30 Você pode testar o acesso às redes e suas máquinas com:
31
32 ping 10.10.10.10 # Teste uma estação corporativa
33 ping 10.10.30.11 # Teste o MySQL da infraestrutura
34
35 > Para explorar de forma mais avançada, utilize nmap, fustscan, fig, telnet, etc.
36
37 ---
38
39 NORMAL main formacao-cybersec README.md gj < 0 1 74% 05:35 @ 10:30
```

```
13 ## Escopo
14
15 O escopo do teste abrangeu o ambiente, incluindo três segmentos de rede distintos:
16 corp_net (10.10.10.0/24), guest_net (10.10.30.0/24) e infra_net (10.10.50.0/24), e
17 todos os ativos de TI contidos neles.
18
19 ## Metodologia
20
21 A análise foi conduzida através de uma abordagem de reconhecimento ativo na rede. As
22 seguintes ferramentas foram utilizadas para mapeamento de rede, descoberta de hosts,
23 escaneamento de portas e identificação de serviços:
24
25 - Ferramentas: nmap, fustscan, telnet, smbclient, ldapsearch.
26
27 - Processo:
28 1. Descoberta de hosts ativos em cada sub-rede.
29 2. Escaneamento completo de portas TCP (1-65535) para cada host identificado.
30 3. Análise de banners e versões dos serviços para identificar tecnologias e
31 potenciais vulnerabilidades.
32 4. Testes de autenticação anônima nos serviços expostos.
33 5. Consolidação e análise dos dados para elaboração do diagnóstico.
34
35 ## Diagrama de Rede
36
37 ---
38
39 NORMAL README.md 0 1 24% 27:60 @ 10:30
```

```
root@486ef7dc9d31: /home/analyst
# cat scan-guest.txt
# Nmap 7.95 scan initiated Sun Jul 27 17:42:44 2025 as: /usr/lib/nmap/nmap -sV -o -p -iL guest.txt -oN scan-guest.txt
Host is up (0.000079s latency).
Not shown: 65535 closed top ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
MAC Address: 42:93:1A:57:EA (Unknown)
Device type: general purpose router
Running: Linux 4.XIS.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenMT 21.02 (Linux 5.4), Mikrotik RouterOS 7.2 - 7.6 (Linux 5.4.3)
Network Distance: 1 hop

Nmap scan report for mysql-server-projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000025s latency).
Not shown: 65535 closed top ports (reset)
PORT STATE SERVICE VERSION
3306/tcp open mysql MySQL 8.0.43
33060/tcp open mysql MySQL X protocol listener
MAC Address: F4:77:0B:CA:C2:04 (Unknown)
Device type: general purpose router
Running: Linux 4.XIS.X, Mikrotik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenMT 21.02 (Linux 5.4), Mikrotik RouterOS 7.2 - 7.6 (Linux 5.4.3)
Network Distance: 1 hop

Nmap scan report for samba-server-projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.000049s latency).
Not shown: 65535 closed top ports (reset)
PORT STATE SERVICE VERSION
139/tcp open netbios-ssn Samba smbd 4
445/tcp open netbios-ssn Samba smbd 4
MAC Address: 62:64:0A:5F:5C:10 (Unknown)
Device type: general purpose router
Running: Linux 4.XIS.X, Mikrotik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenMT 21.02 (Linux 5.4), Mikrotik RouterOS 7.2 - 7.6 (Linux 5.4.3)
Network Distance: 1 hop

Nmap scan report for openldap-projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000025s latency).
Not shown: 65535 closed top ports (reset)
PORT STATE SERVICE VERSION
389/tcp open ldap OpenLDAP 2.2.X - 2.3.X
636/tcp open ldaps OpenLDAP
MAC Address: AA:7A:1A:5B:54:FD (Unknown)
Device type: general purpose
Running: Linux 4.XIS.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop

Nmap scan report for snmp-server-projeto_final_opcao_1_infra_net (10.10.30.177)
Host is up (0.000049s latency).
Not shown: 65535 closed top ports (reset)
PORT STATE SERVICE VERSION
80/tcp open http
10061/tcp open snmp/snmp-trapper?
10062/tcp open unknown
MAC Address: 46:20:5B:4D:2E:27 (Unknown)
Device type: general purpose router
Running: Linux 4.XIS.X, Mikrotik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenMT 21.02 (Linux 5.4), Mikrotik RouterOS 7.2 - 7.6 (Linux 5.4.3)
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 27 17:43:15 2025 -- 5 IP addresses (5 hosts up) scanned in 28.68 seconds

root@486ef7dc9d31: /home/analyst
```

Achado 2: Falha Crítica de Segmentação – Dispositivos Pessoais na Rede de Infraestrutura

- **Hosts:** laptop-luiz, macbook-aline, notebook-carlos, laptop-vastro
- **IPs:** Segmento 10.10.50.0/24 (infra_net)
- **Risco Identificado (CRÍTICO):** Dispositivos de usuários finais, vetores comuns de infecção, estão na rede que deveria ser a mais protegida, permitindo acesso direto a ativos críticos se comprometidos.
- **Evidência:** O scan da rede infra_net confirma a presença de dispositivos pessoais incorretamente alocados.

```
root@486ef7dc9d31: /home/analyst

12 ## 🖥️ Máquina Analyst
13
14 Você realizará as análises a partir do container analyst, que já possui ferramentas como
15 nmap, fustscan, net-tools e dig.
16
17 Acesse com:
18 docker exec -it analyst bash
19
20 A analyst está conectada na rede corp_net com IP Dinâmico em 10.10.10.0/24.
21 A analyst está conectada na rede guest_net com IP Dinâmico em 10.10.30.0/24.
22 A analyst está conectada na rede infra_net com IP Dinâmico em 10.10.50.0/24.
23
24 ---
25
26 ## 📶 Acesso às Redes
27
28 O ambiente está segmentado em 3 redes principais:
29
30 | Rede | Subnet | Descrição |
31 |-----|-----|-----|
32 | corp_net | 10.10.10.0/24 | Rede corporativa (estações e web server) |
33 | guest_net | 10.10.30.0/24 | Rede de visitantes e dispositivos pessoais |
34 | infra_net | 10.10.50.0/24 | Rede de infraestrutura crítica (servidores) |
35
36 NORMAL main formacao-cybersec README.md gj < 0 1 59% 52:1 @ 10:31
```

```
1 Relatário Técnico de Análise de Segurança - Lab Segmentação de Rede
2
3 Autor: Lucas Rocha
4 Data: 27 de julho de 2025
5 Versão: 1.0
6
7 ## Sumário Executivo
8
9 A análise de segurança da rede corporativa revelou falhas arquiteturais críticas que
10 comprometem a confidencialidade, integridade e disponibilidade dos dados e serviços da
11 empresa. Foi identificada uma inversão completa da política de segmentação de rede, onde
12 servidores de infraestrutura crítica (incluindo autenticação, banco de dados e arquivos)
13 foram encontrados operando na rede de visitantes (guest_net), enquanto dispositivos
14 pessoais de usuários foram alocados na rede de infraestrutura (infra_net).
15 Adicionalmente, foi detectado o uso de protocolos de comunicação inseguros (FTP) e a
16 presença de software obsoleto (OpenLDAP). As recomendações prioritárias focam na re-
17 segmentação imediata da rede e na implementação de regras de firewall para isolar os
18 segmentos, mitigando assim os riscos mais urgentes.
19
20 ## Objetivo
21
22 Analisar a topologia e configuração da rede corporativa simulada para identificar
23 vulnerabilidades, falhas de segmentação e riscos operacionais que possam expor a
24
25 NORMAL README.md 0 1 24% 27:60 @ 10:31
```

```
root@486ef7dc9d31: /home/analyst
# cat scan-infra.txt
# Nmap 7.95 scan initiated Sun Jul 27 17:43:43 2025 as: /usr/lib/nmap/nmap -sV -o -p -iL infra.txt -oN scan
-infra.txt
Nmap scan report for laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.2)
Host is up (0.000057s latency).
All 65535 scanned ports on Laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.2) are in ignored states.
Not shown: 65535 closed top ports (reset)
MAC Address: F6:4D:05:0F:18:87 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.3)
Host is up (0.000020s latency).
All 65535 scanned ports on macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.3) are in ignored states.
Not shown: 65535 closed top ports (reset)
MAC Address: A2:C1:71:0F:10:55 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.4)
Host is up (0.000022s latency).
All 65535 scanned ports on notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.4) are in ignored state
s.
Not shown: 65535 closed top ports (reset)
MAC Address: 92:E2:10:46:15:48 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for laptop-vastro.projeto_final_opcao_1_guest_net (10.10.50.5)
Host is up (0.000021s latency).
All 65535 scanned ports on laptop-vastro.projeto_final_opcao_1_guest_net (10.10.50.5) are in ignored states.
Not shown: 65535 closed top ports (reset)
MAC Address: FA:F6:1A:13:1E:3A (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 27 17:43:47 2025 -- 4 IP addresses (4 hosts up) scanned in 4.43 seconds

root@486ef7dc9d31: /home/analyst
```

Achado 3: Risco Alto – Uso de Protocolo Inseguro (FTP)

- **Host/IP:** `ftp-server` (10.10.30.10)
- **Porta:** 21/tcp
- **Risco Identificado (ALTO):** O serviço de FTP transmite credenciais em texto puro, permitindo a captura por um atacante na rede.
- **Evidência:**

```
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net
(10.10.30.10)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPd
```

Achado 4: Risco Alto – Software de Autenticação Obsoleto

- **Host/IP:** `openldap` (10.10.30.17)
- **Porta:** 389/tcp
- **Risco Identificado (ALTO):** O servidor OpenLDAP (`2.2.X – 2.3.X`) está severamente desatualizado, expondo o serviço de autenticação central a múltiplas vulnerabilidades conhecidas.
- **Evidência:**

```
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
PORT      STATE SERVICE VERSION
389/tcp    open  ldap      OpenLDAP 2.2.X – 2.3.X
```

Achado 5: Risco Médio – Permissão de Conexão Anônima no LDAP

- **Host/IP:** `openldap` (10.10.30.17)
- **Observação:** O servidor LDAP, embora bloqueie a listagem do diretório, permite conexões anônimas (anonymous bind). Esta permissão pode ser abusada para validar a existência de nomes de usuário ou para realizar ataques de força bruta e *password spraying*.
- **Evidência:** O teste com `ldapsearch` confirmou que a conexão inicial é aceita, mas a busca pelo conteúdo falha, enquanto a busca pelo `namingContexts` tem sucesso, validando a política.

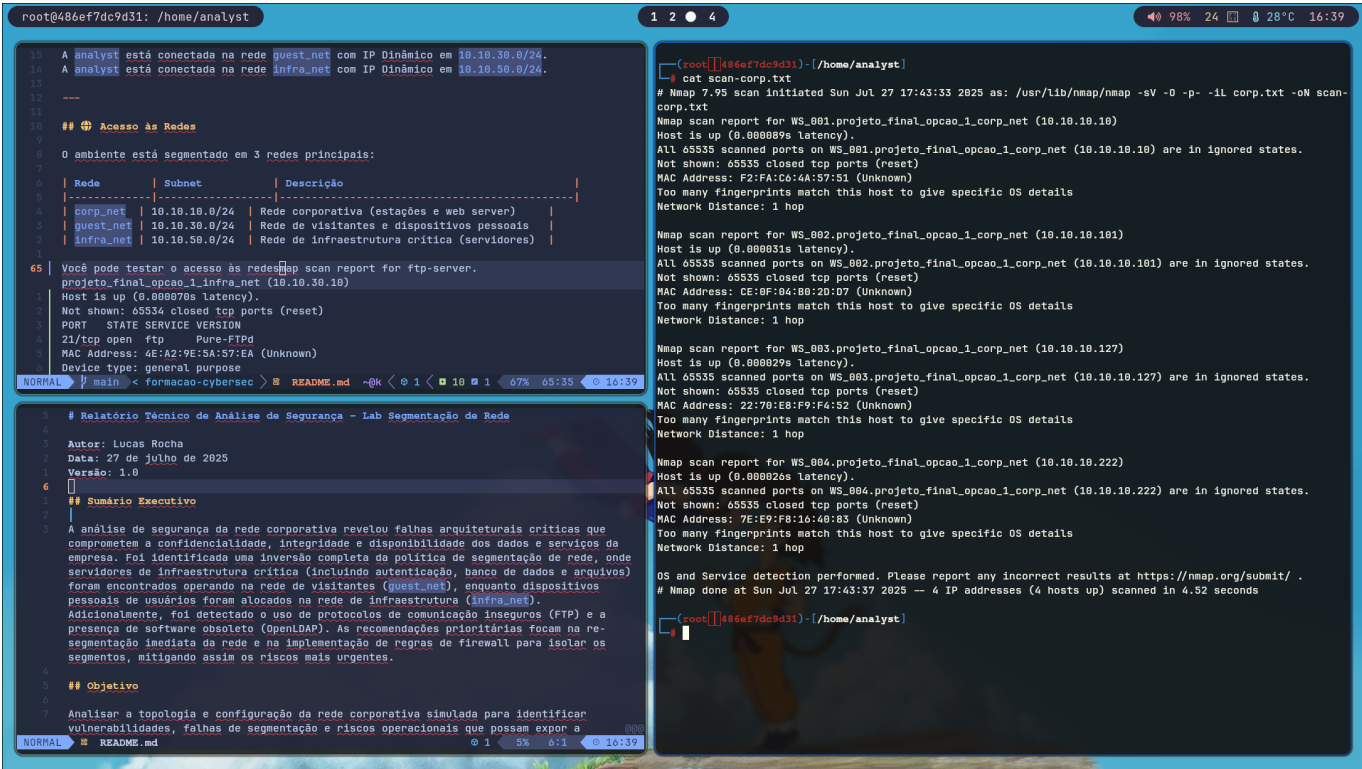
```
# Teste de busca no diretório (falhou)
ldapsearch -x -H ldap://10.10.30.17 -b "dc=example,dc=org"
result: 32 No such object

# Teste de busca pelo namingContext (sucesso)
ldapsearch -x -H ldap://10.10.30.17 -s base "(objectclass=*)"
namingContexts
namingContexts: dc=example,dc=org
result: 0 Success
```

Achado 6: Boa Prática – Segurança na Rede Corporativa

- **Hosts:** `WS_001`, `WS_002`, `WS_003`, `WS_004`

- **IPs:** Segmento 10.10.10.0/24 (corp_net)
- **Observação (POSITIVA):** As estações de trabalho da rede corporativa não expõem nenhuma porta TCP, indicando uma política eficaz de firewall de host.
- **Evidência:** O scan da rede corp_net mostrou todos os 65535 ports em estado "closed/ignored".



Recomendações

1. **Re-segmentação Imediata da Rede:** Realocar todos os servidores para a sub-rede de infraestrutura (infra_net) e os dispositivos de usuários finais para a guest_net, que deve operar com DHCP.
2. **Implementação de Regras de Firewall (ACLs):** Configurar Access Control Lists para impor o isolamento total da guest_net em relação às redes internas (corp_net, infra_net).
3. **Descomissionar o Protocolo FTP:** Substituir o serviço de FTP por uma alternativa segura como SFTP (SSH File Transfer Protocol).
4. **Atualização de Software Crítico:** O servidor OpenLDAP deve ser atualizado para a versão estável mais recente.
5. **Revisão de Configuração dos Serviços (Hardening):** Após a realocação, revisar as configurações dos serviços para seguir o princípio do menor privilégio. Para o OpenLDAP, isso inclui desabilitar o anonymous bind. Para MySQL e outros, garantir senhas fortes.

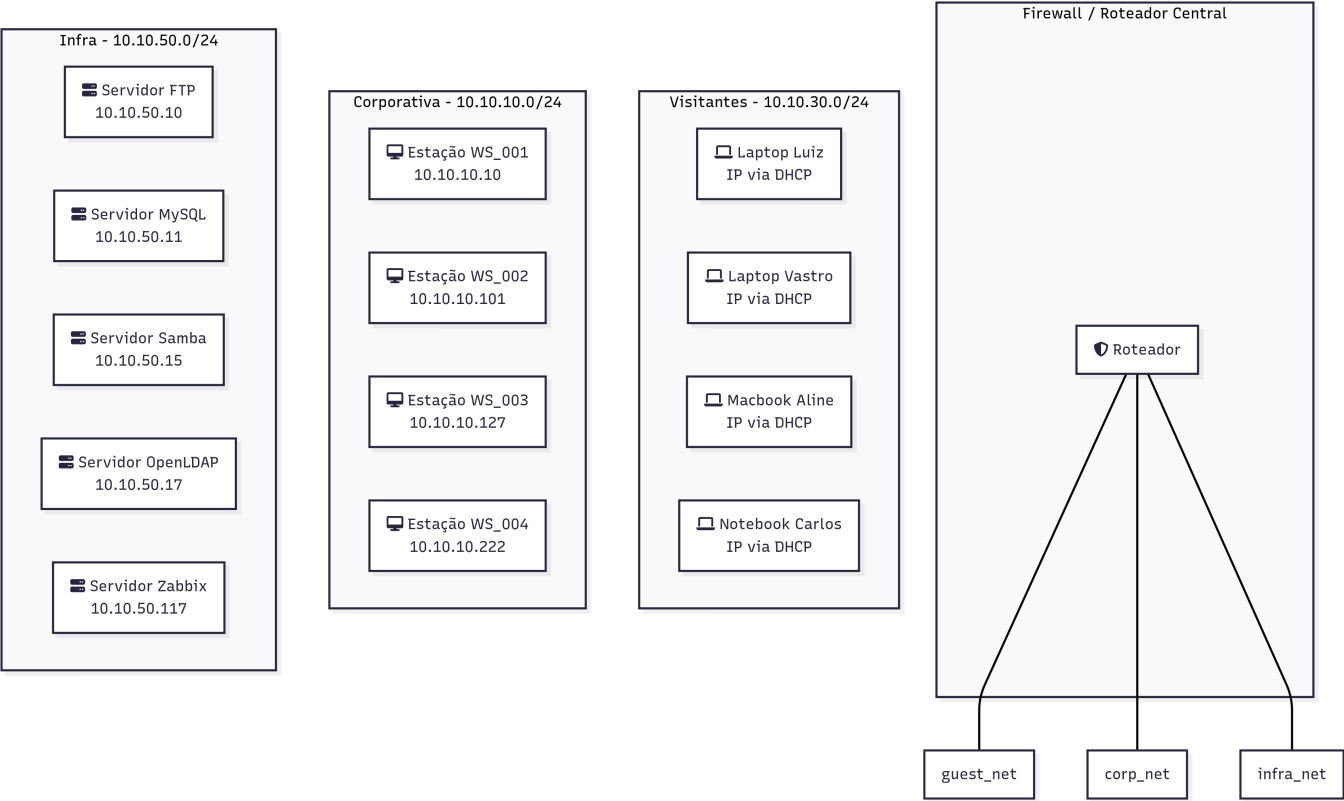


Figura 2: Arquitetura recomendada, com os ativos alocados em seus respectivos segmentos de segurança.

Plano de Ação (80/20)

Ação	Impacto no Risco	Facilidade	Prioridade
Mover servidores para <i>infra_net</i> e laptops para <i>guest_net</i>	Crítico	Média	1 - Máxima
Implementar regras de firewall para isolar redes	Crítico	Média	2 - Máxima
Desativar o serviço de FTP (porta 21)	Alto	Alta	3 - Alta
Fortalecer configuração do LDAP (desativar bind anônimo)	Médio	Média	4 - Média
Atualizar o servidor OpenLDAP	Alto	Baixa	5 - Média

Conclusão

A análise de segurança revelou uma arquitetura de rede fundamentalmente insegura, com falhas de segmentação que expõem os ativos mais críticos da organização a riscos imediatos. Embora existam pontos positivos, como o hardening das estações de trabalho, eles são ofuscados pela exposição sistêmica dos servidores. A implementação do plano de ação, começando pela re-segmentação da rede, é mandatória para estabelecer um nível mínimo de segurança e proteger a empresa contra comprometimentos.

Outros Anexos

- Saídas completas dos scans do Nmap (*scan-corp.txt*, *scan-guest.txt*, *scan-infra.txt*);

- [Logs smbclient](#);
- [Logs ldap](#);
- [Ips encontrados](#).