Projeto de Rede Corporativa

Empresa BRL

Integrantes:

Renan da Silva Oliveira Andrade
Leticia Maria Maia de Andrade Vieira
Brenda Gabrielli Barbosa

Orientador:

Prof. Dr. Ricardo Cassiano Nabhen

Outubro de 2025

Conteúdo

1 Apresentação do Projeto

O projeto tem como seu principal objetivo o design e implementação de uma rede corporativa de campus para a empresa BRL. A rede conectará duas localidades, a Matriz localizada em São Paulo e a Filial localizada em Curitiba, por meio de uma conexão segura através da Internet. O design hierárquico de redes será aplicado em ambos os site, dividindo a infraestrutura em camadas lógicas pensadas para otimizar o desempenho, a segurança e a escalabilidade da empresa.

2 Objetivos do Projeto

- Implementar um design de rede hierárquico: Separar a rede em camadas de acesso, distribuição e núcleo para melhor gerenciamento e desempenho.
- Garantir conectividade segura e redundante: Estabelecer uma conexão principal via VPN sobre a Internet e um link de backup para assegurar a continuidade do serviço entre os dois sites.
- Segregar o tráfego de rede: Utilizar VLANs para criar redes independentes para os dois departamentos em cada site, mantendo a interconectividade.
- Centralizar serviços corporativos: Consolidar serviços essenciais como VoIP, DNS e web no datacenter da Matriz.
- Assegurar alta disponibilidade e segurança: Implementar regras de firewall e NAT/NAPT para controlar o acesso à Internet e proteger a rede interna contra ameaças externas.

3 Descrição do Cenário de Rede

A empresa BRL opera em duas unidades: a Matriz (São Paulo) com 150 usuários, e a Filial (Curitiba) com 100 usuários. Em ambos os sites, a rede interna é segmentada em dois departamentos. Havendo participantes de ambos os departamentos em cada switch presente na rede.

3.1 Aplicações e Serviços

- **ERP**: Servidores em ambos os sites (HTTP).
- **DNS**: Servidor hospedado na Matriz responsável pelos sites, www.brl.com.br (Matriz) e www.brlfilial.com.br (Filial).
- **Telefonia IP (VoIP)**: Utiliza o protocolo SIP (UDP 5060, 5061) e RTP (UDP 10000-11000) para comunicação interna e entre as unidades. Há um servidor VoIP no datacenter de cada site.
- **Acesso à Internet**: O tráfego de saída dos usuários é restrito aos serviços HTTP, HTTPS, DNS e ICMP (ping).

4 Projeto Lógico da Rede

4.1 Topologia da Rede

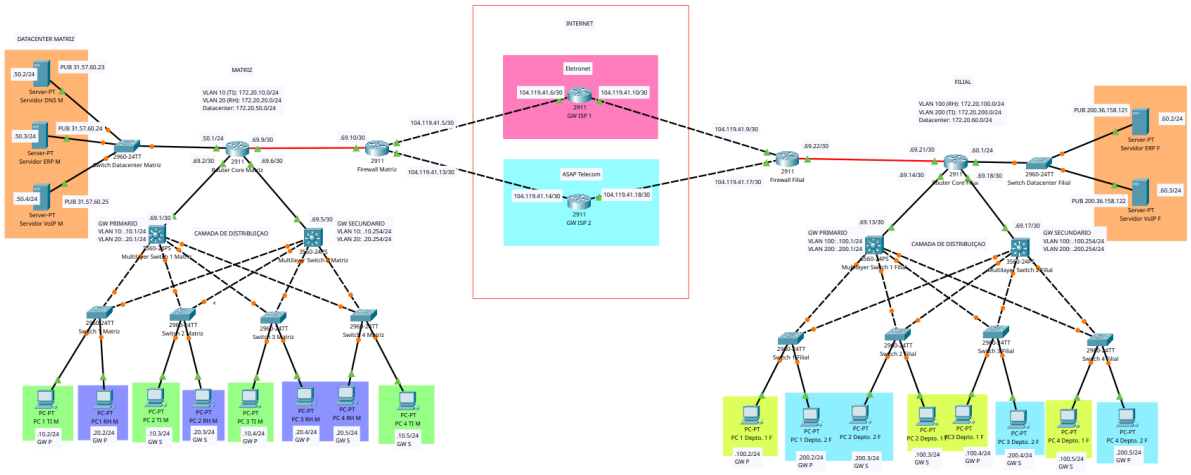

Figura 1: Diagrama Geral das Topologias das Redes

A topologia foi implementada no modelo hierárquico de três camadas (Núcleo, Distribuição e Acesso) em ambos os sites (Matriz e Filial). A conectividade entre os sites é garantida por um enlace VPN Site-to-Site sobre a Internet (apenas descrito em relatório, não implementado), com links redundantes para provedores de serviços.

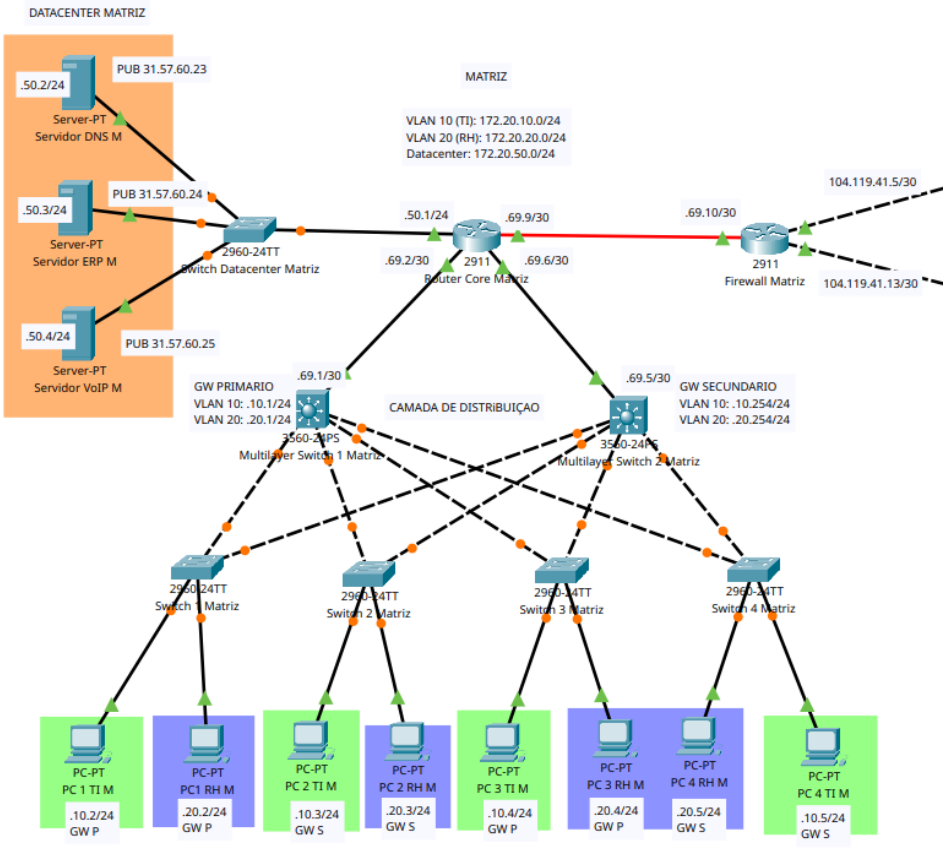

Figura 2: Diagrama da Topologia das Redes da Matriz

No diagrama da topologia da matriz, estão presentes 6 redes IPs: 1 rede IP designada ao data center, 2 redes IPs destinadas às VLANs (10 e 20), 2 redes ponto-a-ponto conectando os Multilayer Switches ao Roteador Core, e uma rede ponto-a-ponto conectando o Roteador Core ao Firewall.

Podemos identificar na topologia da rede as seguintes camadas do modelo hierárquico, onde os 4 Switches 2960-24TT representam a **Camada de Acesso**, que é a responsável por conectar os dispositivos de ponta à LAN.

Acima deles, estão posicionados 2 Multilayer Switches 3560-24PS, que compõem a **Camada de Distribuição**. Todos os switches da Camada de Acesso estão propositalmente conectados aos dois multilayer switches, para fornecer a redundância de link, distribuindo o acesso à rede.

Acima dos multilayer switches, está posicionado um Roteador 2911, responsável pela **Camada de Núcleo**, que tem como objetivo interconectar todos os dispositivos entre as LANs, entre si e às redes externas.

Em laranja, temos uma rede IP dedicada ao Data Center. Onde os servidores se conectam a um switch 2960-24TT, responsável por conectá-los ao roteador Core. Além de segregar as redes LAN da rede do data center, os servidores possuem acesso direto ao link de mais alta velocidade da rede.

Por último, temos um roteador segregado que aplica as **Regras de Firewall**, ele também é o Gateway Padrão do roteador core, e age como roteador de borda da rede, fornecendo conectividade à WAN.

Todos os aspectos topológicos comentados acima, podem ser visualizados na Figura 2.

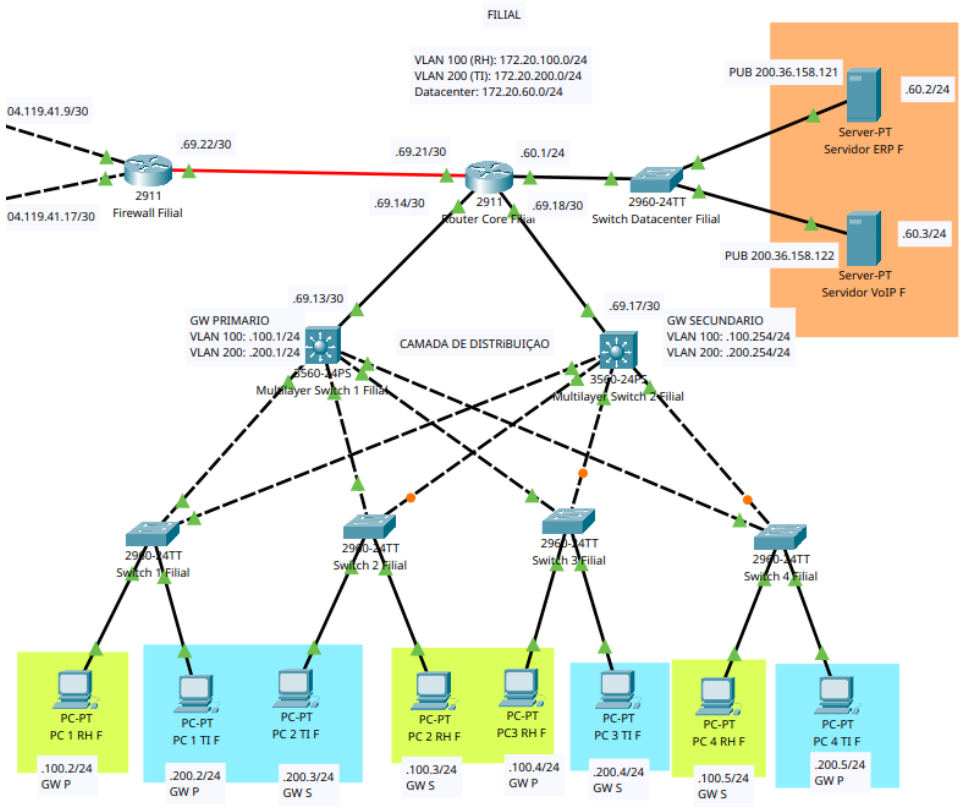

Figura 3: Diagrama da Topologia das Redes da Filial

A topologia da rede Filial é um espelho da rede Matriz, com a única exceção de conter um servidor a menos (servidor DNS), conforme demonstrado na Figura 3.

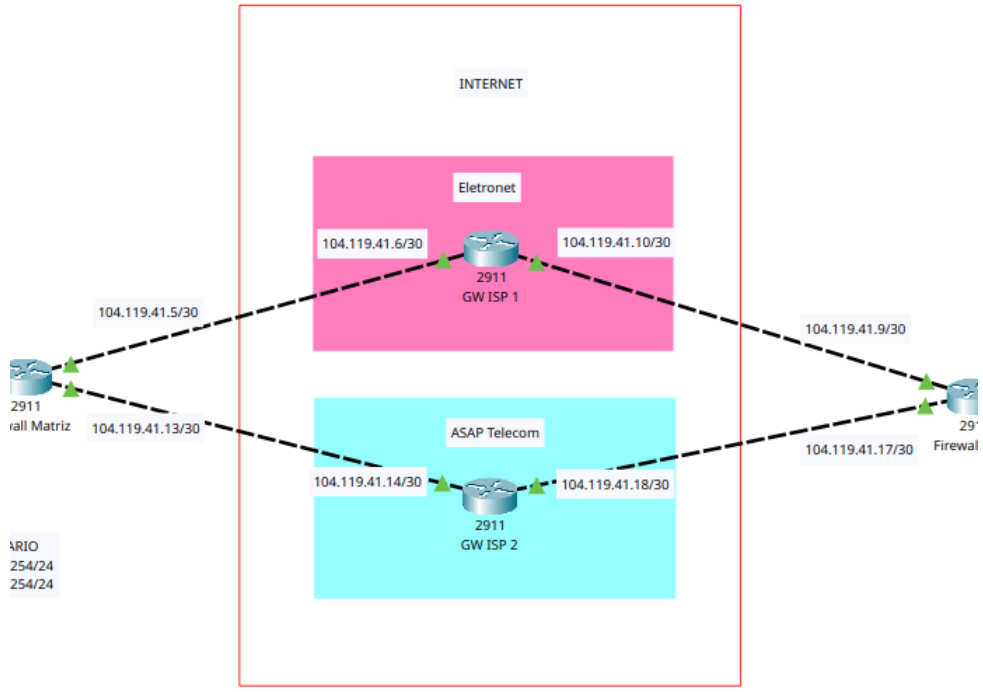

Figura 4: Diagrama da Topologia das ISPs

Para fins de redundância, o cenário leva em conta, a contratação de dois Provedores de Serviço de Internet (ISPs). Conforme observado na Figura 4, os dois ISPs são representados por dois roteadores distintos, que realizam o intermédio entre os dois sites Matriz e Filial, e (não demonstrado aqui) a conectividade à Internet. Os roteadores de borda de cada site (roteadores de firewall), se conectam diretamente ao roteador do provedor, estabelecendo assim a conexão dos sites à redes externas.

4.2 Divisão de VLANs e Esquema de Endereçamento IP

A segregação de tráfego é realizada através de VLANs, conforme detalhado na Tabela 1.

Tabela 1: Esquema de VLANs e Endereçamento IP

Local	**VLAN**	**Sub-rede**	**GW Primário**	**GW Secundário**
Matriz	TI (VLAN 10)	172.20.10.0/24	172.20.10.1	172.20.10.254
Matriz	RH (VLAN 20)	172.20.20.0/24	172.20.20.1	172.20.20.254
Filial	RH (VLAN 100)	172.20.100.0/24	172.20.100.1	172.20.100.254
Filial	TI (VLAN 200)	172.20.200.0/24	172.20.200.1	172.20.200.254
Matriz	Datacenter	172.20.50.0/24	172.20.50.1	N/A
Filial	Datacenter	172.20.60.0/24	172.20.60.1	N/A

Todos os VLAN IDs foram configurados nas VLAN DBs dos switches das camadas

de acesso, e dos multilayer switches das camadas de distribuição de ambas matriz e filial, onde a conexão entre switches e, entre switches e roteadores está configurada em modo TRUNK, enquanto as portas dos switches das camadas de acesso que estão conectadas a dispositivos de usuários, estão configuradas em modo ACCESS com a respectiva VLAN a qual pertence.

4.3 Endereçamento de Servidores

Os servidores corporativos possuem endereçamento estático, com mapeamento para IPs públicos via NAT, conforme mostra a Tabela 2.

Tabela 2: Endereçamento de Servidores e NAT

Serviço	**Local**	**IP Privado**	**IP Público (NAT Estático)**
DNS	Matriz	172.20.50.2/24	31.57.60.23
ERP	Matriz	172.20.50.3/24	31.57.60.24
VoIP	Matriz	172.20.50.4/24	31.57.60.25
ERP	Filial	172.20.60.2/24	200.36.158.121
VoIP	Filial	172.20.60.3/24	200.36.158.122

4.4 Links Ponto-a-Ponto e IPs Públicos

Todas as redes ponto-a-ponto utilizam CIDR /30. Para links ponto-a-ponto entre dispositivos internos utiliza-se a faixa 172.20.69.x/30. Os links para ISPs utilizam os seguintes endereçamentos públicos:

- **Firewall Matriz → ISP Eletronet**: 104.119.41.4/30
- **Firewall Matriz → ISP ASAP Telecom**: 104.119.41.12/30
- **Firewall Filial → ISP Eletronet**: 104.119.41.8/30
- **Firewall Filial → ISP ASAP Telecom**: 104.119.41.16/30

Para o NAPT (NAT Overload), são utilizados os IPs próprios das portas do roteador firewall. Portanto, os IPs compartilhados por hosts das LANs (exceto os servidores) são:

- **Hosts Matriz via ISP Eletronet**: 104.119.41.5/32
- **Hosts Matriz via ISP ASAP Telecom**: 104.119.41.13/32
- **Hosts Filial via ISP Eletronet**: 104.119.41.9/32
- **Hosts Filial via ISP ASAP Telecom**: 104.119.41.17/32

4.5 Projeto de Roteamento

A redundância é alcançada através da configuração de múltiplos caminhos, e da utilização de dois provedores de Internet. O protocolo de roteamento padrão do Cisco Packet Tracer, será utilizado para a troca dinâmica de informações de rota entre os dispositivos de camada 3 (Multilayer Switches e Roteador Core), garantindo assim a convergência da rede em caso de falhas.

Ambos os Multilayer Switches possuem como rota padrão o roteador core, e conhecem as redes das duas VLANs.

Já o roteador core, conhece todas as redes internas, incluindo as redes diretamente conectadas (redes do data center e do firewall), e rotas estáticas para as redes das VLANs, tendo como rota padrão o firewall (roteador de borda da rede).

O firewall conhece as redes das duas ISPs, bem como a rede ponto-a-ponto estabelecida com o roteador core. Além disso, possui também rotas estáticas para as redes VLANs, juntamente com a rede do data center.

A estratégia utilizada para estabelecer redundância de link entre o firewall e os ISPs, é estabelecer ambos os links como rotas padrão, porém estabelecendo um peso (*cost*) maior no ISP de backup (ASAP Telecom), fazendo assim com que o firewall prefira o ISP principal (Eletronet) e utilize o ISP secundário em caso de falha do primeiro link.

5 Serviços de Rede

5.1 Configuração de NAT/NAPT

O serviço de tradução de endereços de rede (NAT) é configurado no firewall de borda para:

- **NAT Estático**: Mapeamento one-to-one de IPs públicos para os servidores internos (Tabela 2), permitindo acesso externo controlado.
- **PAT (NAPT Overload)**: Tradução de todos os IPs privados das VLANs de usuários para os IPs públicos das interfaces de saída do firewall, permitindo o acesso múltiplo e simultâneo à Internet.

5.2 Regras de Firewall

A política de segurança "Default Deny" é implementada, negando explicitamente todo o tráfego não permitido. As regras são baseadas no princípio do menor privilégio, garantindo a segurança da rede.

5.2.1 Política de Firewall Matriz

O firewall da Matriz adota uma política de permitir comunicações essenciais entre a rede interna, a filial e serviços externos, conforme descrito:

- **HTTP/HTTPS:** é permitido o tráfego de saída e entrada para navegação web segura, com portas 80 e 443.
- **DNS:** consultas DNS são liberadas tanto para saída quanto para retorno de respostas, utilizando UDP na porta 53

- **ICMP:** pacotes ICMP são autorizados para permitir testes de conectividade (ping) entre as redes internas e externas.
- **ERP:** comunicação bidirecional entre o servidor ERP da Matriz (172.20.50.3) e os IPs de clientes da Filial de ambas as ISPs, com portas 80 e 443 para aplicação.
- **DNS Interno:** é permitido o acesso de IPs de clientes da Filial ao servidor DNS interno da Matriz para resolução de nomes internos (brl.com.br e brlfilial.com.br).
- **SIP/RTP (Voz sobre IP):** é permitido o tráfego de voz (SIP nas portas 5060–5061 e RTP entre 10000–11000) entre o servidor VoIP da Matriz e o servidor VoIP da filial (200.36.158.122), garantindo comunicação VoIP exclusiva entre os dois sites.

.

MATRIZ											
SERVIÇO	REGRA	TIPO	AÇÃO	ROTEADOR	INTERFACE	SENTIDO	PROTOCOLO	IP_ORIGEM	IP_DESTINO	PORTA_ORIGEM	PORTA_DESTINO
HTTP	1.1	EGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	IN	TCP	.10.0/24, .20.0/24	*	>1023	80
HTTP	1.3	INGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	OUT	TCP	*	.10.0/24, .20.0/24	80	>1023
HTTPS	2.1	EGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	IN	TCP	.10.0/24, .20.0/24	*	>1023	443
HTTPS	2.3	INGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	OUT	TCP	*	.10.0/24, .20.0/24	443	>1023
DNS	3.1	EGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	IN	UDP	.10.0/24, .20.0/24	*	>1023	53
DNS	3.3	INGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	OUT	UDP	*	.10.0/24, .20.0/24	53	>1023
ICMP	4.1	EGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	IN	ICMP	.10.0/24, .20.0/24	*	-	-
ICMP	4.3	INGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	OUT	ICMP	*	.10.0/24, .20.0/24	-	-
ERP	5.1	EGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	IN	TCP	172.20.50.3	IPS_FILIAL	80	>1023
ERP	5.3	INGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	OUT	TCP	IPS_FILIAL	172.20.50.3	>1023	80
ERP	6.1	EGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	IN	TCP	172.20.50.3	IPS_FILIAL	443	>1023
ERP	6.3	INGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	OUT	TCP	IPS_FILIAL	172.20.50.3	>1023	443
SER. DNS	7.1	EGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	IN	UDP	172.20.50.2	IPS_FILIAL	53	>1023
SER. DNS	7.3	INGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	OUT	UDP	IPS_FILIAL	172.20.50.2	>1023	53
SIP	8.1	EGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	IN	UDP	172.20.50.4	200.36.158.122	5060~5061	>1023
SIP	8.3	INGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	OUT	UDP	200.36.158.122	172.20.50.4	>1023	5060~5061
SIP	8.4	EGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	IN	UDP	172.20.50.4	200.36.158.122	>1023	5060~5061
SIP	8.6	INGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	OUT	UDP	200.36.158.122	172.20.50.4	5060~5061	>1023
RTP	9.1	EGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	IN	UDP	172.20.50.4	200.36.158.122	10000~11000	10000~11000
RTP	9.3	INGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	OUT	UDP	200.36.158.122	172.20.50.4	10000~11000	10000~11000

Figura 5: Regras de Firewall - Matriz

Nota: `IPS_FILIAL` entende-se como os IPs públicos dos dois provedores utilizados pela Filial no NAPT (104.119.41.9 e 104.119.41.17); portanto, existem regras de egressos e ingressos para ambos os IPs públicos.

Em resumo, a Matriz atua como ponto principal da rede corporativa, controlando fluxos com a filial e o provedor VoIP, e liberando serviços web, DNS e ERP de forma controlada.

5.2.2 Política de Firewall Filial

O firewall da Filial segue uma política espelhada, com foco em acesso controlado à Matriz e à Internet:

- **HTTP/HTTPS:** libera acesso web de saída e retorno de respostas para toda a rede local (100.0/24, 200.0/24).
- **DNS:** permite consultas e respostas DNS via UDP, tanto internas quanto externas.
- **ICMP:** autoriza pacotes ICMP para verificação de conectividade.

- **ERP:** garante comunicação segura entre o servidor ERP da Filial (172.20.60.2) e os hosts da Matriz, nas portas 80 e 443, para sincronização e acesso de dados e de sistemas corporativos.
- **SIP/RTP:** permite comunicação de voz entre o servidor VoIP da Filial (172.20.60.3) e o servidor VoIP da Matriz (31.57.60.25), estabelecendo uma conexão bidirecional exclusiva entre Matriz e Filial.

Assim, a Filial mantém conectividade segura com a Matriz e com a Internet, restringindo o tráfego apenas a protocolos e portas estritamente necessárias.

FILIAL											
SERVIÇO	REGRA	TIPO	AÇÃO	ROTEADOR	INTERFACE	SENTIDO	PROTOCOLO	IP_ORIGEM	IP_DESTINO	PORTA_ORIGEM	PORTA_DESTINO
HTTP	1.1	EGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	IN	TCP	.100.0/24, .200.0/24	*	>1023	80
HTTP	1.3	INGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	OUT	TCP	*	.100.0/24, .200.0/24	80	>1023
HTTPS	2.1	EGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	IN	TCP	.100.0/24, .200.0/24	*	>1023	443
HTTPS	2.3	INGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	OUT	TCP	*	.100.0/24, .200.0/24	443	>1023
DNS	3.1	EGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	IN	UDP	.100.0/24, .200.0/24	*	>1023	53
DNS	3.3	INGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	OUT	UDP	*	.100.0/24, .200.0/24	53	>1023
ICMP	4.1	EGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	IN	ICMP	.100.0/24, .200.0/24	*	-	-
ICMP	4.3	INGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	OUT	ICMP	*	.100.0/24, .200.0/24	-	-
ERP	5.1	EGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	IN	TCP	172.20.60.2	IPS_MATRIZ	80	>1023
ERP	5.3	INGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	OUT	TCP	IPS_MATRIZ	172.20.60.2	>1023	80
ERP	6.1	EGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	IN	TCP	172.20.60.2	IPS_MATRIZ	443	>1023
ERP	6.3	INGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	OUT	TCP	IPS_MATRIZ	172.20.60.2	>1023	443
SIP	7.1	EGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	IN	UDP	172.20.60.3	31.57.60.25	5060~5061	>1023
SIP	7.3	INGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	OUT	UDP	31.57.60.25	172.20.60.3	>1023	5060~5061
SIP	7.4	EGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	IN	UDP	172.20.60.3	31.57.60.25	>1023	5060~5061
SIP	7.6	INGRESSO	ALLOW	FIREWALL FILIAL	Gig0/3/0	OUT	UDP	31.57.60.25	172.20.60.3	5060~5061	>1023
RTP	8.1	EGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	IN	UDP	172.20.60.3	31.57.60.25	10000~11000	10000~11000
RTP	8.3	INGRESSO	ALLOW	FIREWALL MATRIZ	Gig0/3/0	OUT	UDP	31.57.60.25	172.20.60.3	10000~11000	10000~11000

Figura 6: Regras de Firewall - Filial

Nota: `IPS_MATRIZ` entende-se como os IPs públicos dos dois provedores utilizados pela Matriz no NAPT (104.119.41.5 e 104.119.41.13); portanto, existem regras de egressos e ingressos para ambos os IPs públicos.

5.3 Especificações do Link de Internet e SLA

Para garantir conectividade robusta e em conformidade com as necessidades empresariais, foram selecionados dois provedores de telecomunicações com atuação nacional e reconhecida qualidade em links corporativos de alta disponibilidade: **Eletronet** e **ASAP Telecom**. As principais características dos serviços estão resumidas na Tabela 3.

Tabela 3: Especificações dos Provedores de Internet

Provedor / Serviço	**Largura de Banda**	**SLA (Acordo de Nível de Serviço)**
Eletronet (Principal)	Link Dedicado IP Corporativo – até 400 Gbps (Fibra Óptica DWDM)	Disponibilidade de 99,95%, latência média nacional <15 ms, suporte 24x7, tempo de reparo <4h
ASAP Telecom (Backup)	Link Dedicado de Internet – até 10 Gbps (Fibra Óptica ponto a ponto)	Disponibilidade de 99,5%, latência média nacional <25 ms, suporte 24x7, tempo de reparo <6h

O *Service Level Agreement* (SLA) define os parâmetros de desempenho e disponibilidade contratados com os provedores. O serviço da Eletronet [4] utiliza rede óptica baseada em tecnologia *DWDM* (Dense Wavelength Division Multiplexing), com backbone próprio de mais de 17 mil km interligando os principais pontos de troca de tráfego (PTTs) do Brasil, permitindo conexões de até 400 Gbps com baixa latência e suporte corporativo contínuo.

Já o serviço da ASAP Telecom [5] é implementado sobre fibra óptica dedicada (*link ponto a ponto*), oferecendo redundância ao link principal com banda contratual de até 10 Gbps, gerenciamento proativo de falhas e monitoramento em tempo real.

O SLA de 99,95% ofertado pela Eletronet implica em até cerca de 4h22min de indisponibilidade anual, enquanto o SLA de 99,5% da ASAP Telecom representa até 1 dia e 19h de possível inatividade ao ano — valores aceitáveis dentro de um cenário de contingência empresarial.

As métricas de desempenho incluem latência, *packet loss*, tempo de resolução de falhas e disponibilidade contínua do serviço, elementos essenciais para a estabilidade de aplicações críticas como ERP, VPN e VoIP.

5.4 Especificações da VPN Site-to-Site

Para garantir a comunicação segura entre a Matriz e a Filial, interligadas por meio de provedores de Internet distintos e potencialmente inseguros, é proposta a implementação de uma **VPN (Virtual Private Network)** no modelo Site-to-Site utilizando o protocolo IPSec em modo túnel.

Essa abordagem permite encapsular e criptografar todo o tráfego IP entre as duas redes locais corporativas, garantindo confidencialidade, integridade e autenticação ponta a ponta entre os roteadores/firewalls de borda de ambas as unidades.

5.4.1 Arquitetura e Topologia de Comunicação

A VPN será estabelecida entre os firewalls de borda de cada localidade:

- **Firewall Matriz:** IPs públicos 104.119.41.5 (Eletronet) e 104.119.41.13 (ASAP Telecom)
- **Firewall Filial:** IPs públicos 104.119.41.9 (Eletronet) e 104.119.41.17 (ASAP Telecom)

Ambos os firewalls estarão configurados como *peers* IPSec, estabelecendo um túnel direto através da Internet pública. Cada firewall atuará simultaneamente como gateway local para suas redes privadas internas:

- Redes internas da Matriz: 172.20.10.0/24, 172.20.20.0/24, 172.20.50.0/24
- Redes internas da Filial: 172.20.100.0/24, 172.20.200.0/24, 172.20.60.0/24

O tráfego destinado de uma rede à outra será roteado automaticamente pelo túnel criptografado, com o firewall realizando *encapsulation/decapsulation* conforme a direção do tráfego.

5.4.2 Configurações Técnicas da VPN IPSec

- **Modo de Operação:** Túnel (Tunnel Mode).
- **Protocolo de Segurança:** IPSec (Internet Protocol Security).
- **Camada de Implementação:** Camada de Rede (Camada 3 – Modelo OSI).
- **Criptografia:** AES-256 GCM (Advanced Encryption Standard Galois/Counter Mode, chave de 256 bits) para proteção de dados em trânsito.
- **Integridade e Autenticação:** SHA-256 (Secure Hash Algorithm 256-bit) para verificação de integridade e autenticação do pacote.
- **Troca de Chaves:** IKEv2 (Internet Key Exchange, versão 2), utilizando Diffie-Hellman Group 14 (2048 bits).
- **Tempo de Vida da SA (Security Association):** 8 horas para rekeying automático.
- **Modo de Transporte:** ESP (Encapsulating Security Payload), operando sobre o protocolo IP (protocolo 50).
- **Protocolos Suportados:** Compatibilidade com *OpenVPN* e *L2TP/IPSec* para interoperabilidade futura.

5.4.3 Mecanismos de Estabelecimento do Túnel

O processo de inicialização do túnel ocorre em duas fases:

1. **Fase 1 (IKE SA):** Estabelece um canal seguro para troca de parâmetros de autenticação e negociação das chaves criptográficas. Ambas as partes autenticam-se mutuamente via *pre-shared key* (PSK) ou certificados digitais X.509.
2. **Fase 2 (IPSec SA):** Define os parâmetros do túnel (endereços locais/remotos, algoritmos de criptografia e integridade). A partir dessa fase, o tráfego entre os sub-redes é criptografado e transmitido de forma segura.

5.4.4 Fluxo de Comunicação

O funcionamento da VPN segue a sequência abaixo:

1. Um dispositivo de umas das redes da Filial (por exemplo, 172.20.10.2) envia um pacote destinado à uma das redes da Matriz (por exemplo, 172.20.100.0/24).
2. O firewall da Filial identifica o tráfego como pertencente à política IPSec e encapsula o pacote original em um cabeçalho IPSec.
3. O pacote criptografado é transmitido pela Internet (link da Eletronet ou ASAP Telecom) até o firewall da Matriz.
4. O firewall da Matriz valida a integridade e autenticidade do pacote, descriptografa o conteúdo e encaminha-o internamente à rede de destino.
5. O processo inverso ocorre para o tráfego no sentido oposto.

5.4.5 Redundância e Monitoramento

O túnel IPSec será configurado com suporte a failover automático via roteamento dinâmico (*Dead Peer Detection – DPD*) e integração com protocolos de alta disponibilidade como *VRRP* ou *HSRP*, permitindo que o túnel seja restabelecido automaticamente em caso de falha de um dos links ou firewalls.

Além disso, será implementado monitoramento ativo SNMP e syslog para auditoria e registro de eventos, com geração de alertas automáticos em caso de desconexão do túnel ou anomalias de latência.

5.4.6 Segurança e Benefícios

A VPN Site-to-Site IPSec proporciona:

- Confidencialidade total do tráfego corporativo entre Matriz e Filial.
- Autenticação mútua entre os gateways, prevenindo ataques de spoofing.
- Integridade dos pacotes de dados, protegendo contra alterações não autorizadas.
- Compatibilidade com múltiplas plataformas de firewall (Cisco ASA, FortiGate, pfSense, entre outros).

6 Conclusão

Este relatório detalha o projeto completo de rede corporativa para a empresa BRL, abrangendo desde a topologia física e lógica até as especificações de segurança e conectividade. A implementação proposta segue um modelo hierárquico com redundância, políticas de segurança robustas e uma VPN IPSec site-to-site, fornece uma base sólida para uma infraestrutura de rede escalável, eficiente e segura. O projeto atende às necessidades atuais e futuras das operações da empresa fictícia BRL em sua Matriz e Filial, garantindo alta disponibilidade e proteção para os dados corporativos.

Referências

[1] Cisco Systems. (2023). *Cisco Hierarchical Network Model*. Disponível em: `https://www.cisco.com`

[2] IETF. (2023). *IP Security Protocol (ipsec)*. RFC 4301-4309. Disponível em: `https://www.ietf.org`

[3] Microsoft. (2023). *VPN Gateway design*. Disponível em: `https://learn.microsoft.com`

[4] Eletronet. (2024). *Serviços IP e Conectividade Corporativa*. Disponível em: `https://www.eletronet.com/servicos/`. Acesso em: 13 out. 2025.

[5] ASAP Telecom. (2024). *Link Dedicado Empresarial e Conectividade*. Disponível em: `https://www.asaptelecom.com.br/link-dedicado`. Acesso em: 13 out. 2025.

[6] Cisco. (2023). *Configuring NAT on Cisco Routers*. Disponível em: `https://www.cisco.com`

[7] Tanenbaum, A. S.; Wetherall, D. J. (2011). *Computer Networks*. 5ª ed. Pearson.

[8] IEEE 802.1Q. (2018). *VLAN Tagging*. IEEE Standards.

[9] ITIL. (2019). *Service Level Agreements Best Practices*. Axelos.