Manual de Redes

Split Payment

Reforma Tributária

Manual de Redes
Versão 1.0.0 | Julho de 2026

SUMÁRIO

CAPÍTULO 1 – DISPOSIÇÕES INICIAIS

1.1 INTRODUÇÃO

Este Manual de Redes tem como objetivo orientar a configuração da conexão de rede entre os Prestadores de Serviços de Pagamento (PSPs) e a Plataforma Pública (PP). O foco é a conectividade por VPN IPsec Site-to-Site disponibilizada pela Plataforma Pública: o padrão técnico adotado, a segurança da rede e o passo a passo de configuração, validação e operação do túnel.

A Plataforma Pública disponibiliza a conectividade por VPN IPsec. Cabe ao time de redes da Plataforma Pública fornecer os parâmetros do lado remoto e o padrão criptográfico, bem como sua configuração; cabe ao PSP configurar o equipamento de borda da sua rede para estabelecer o túnel de forma segura e estável.

Este manual integra um conjunto de documentos do Split Payment, cada um com finalidade específica:

Documento	Finalidade
Manual de Operações	Funcionamento operacional, fluxos, regras de cálculo, experiência do usuário
Manual de Integração + Documento OpenAPI	Especificação técnica da API, contratos de mensagens, endpoints, dicionário de campos
Manual de Tempos	Prazos, janelas operacionais, ANS e marcos temporais
Manual de Redes	Arquitetura de conexão, topologia, capacidade e resiliência
Manual de Segurança	Autenticação, criptografia, auditoria e controles de proteção
Manual de Habilitação de Participantes	Checklist de conformidade para entrada de novos PSPs no Split Payment, playbooks de onboarding e offboarding, governança de incidentes
Regulamento (Ato Conjunto RFB/CGIBS)	Bases normativas, obrigações legais, penalidades

O conteúdo deste manual é complementar aos demais. Quando um tema for tratado em outro manual, este documento não reproduzirá o detalhamento técnico que pertence ao manual correspondente.

1.2 ESCOPO

Este documento concentra-se em:

- Modelo de conectividade por VPN IPsec Site-to-Site com a Plataforma Pública e sua topologia;
- Pré-requisitos de rede (links, IP fixo, equipamento, NTP e liberação de portas);
- Parâmetros da VPN fornecidos pela Plataforma Pública e os parâmetros sob responsabilidade do PSP;

- Configuração passo a passo do túnel IPsec (Fase 1/IKE e Fase 2/IPsec), roteamento e failover;
- Segurança da rede e da comunicação (VPN, TLS, firewall e boas práticas);
- Validação, testes de conectividade e solução de problemas (troubleshooting) do túnel.

1.3 PÚBLICO-ALVO

Destina-se a arquitetos e engenheiros de rede, equipes de segurança e responsáveis técnicos de infraestrutura dos PSPs, da Núclea e de eventuais Prestadores de Serviço de Conexão responsáveis pela configuração e operação do túnel VPN com a Plataforma Pública.

CAPÍTULO 2 – VISÃO GERAL DA CONECTIVIDADE VIA VPN

2.1 MODELO DE CONEXÃO

A conectividade com a Plataforma Pública é estabelecida por meio de uma VPN IPsec Site-to-Site entre o gateway de borda do PSP e o gateway da Plataforma Pública, cada VPN será configurada individualmente para o PSP. O túnel criptografa e autentica todo o tráfego de rede entre as duas pontas, isolando logicamente a comunicação.

O padrão criptográfico e os parâmetros do lado remoto são definidos e fornecidos pela Plataforma Pública; o PSP configura seu equipamento de borda em conformidade com esse padrão (ver Capítulos 4 e 5).

2.2 TOPOLOGIA DA CONEXÃO

A figura a seguir ilustra a topologia: os sistemas do PSP conectam-se ao(s) gateway(s) de borda, que estabelece(m) o(s) túnel(is) VPN IPsec com o gateway da PP.

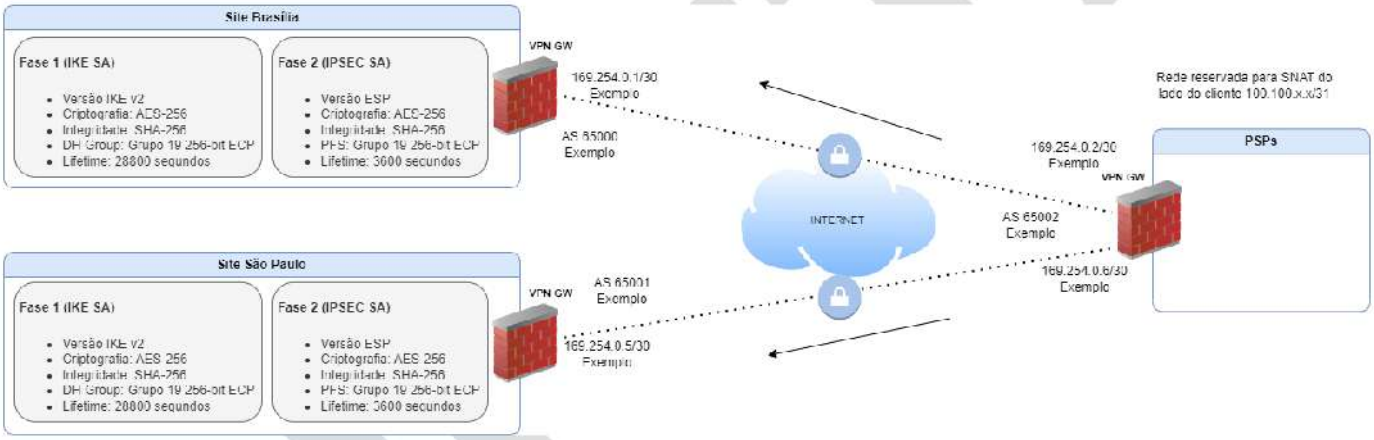

Figura 1 - Topologia da conexão VPN IPsec Site-to-Site e routing com a Plataforma Pública.

2.2.1 TOPOLOGIA LÓGICA (ROUTE-BASED / VTI COM BGP)

A conexão é estabelecida pela internet por meio de **interfaces de túnel virtual (Route-Based VPN / VTI)**, que permitem isolamento de tráfego e roteamento dinâmico baseado em **BGP**. O SERPRO disponibiliza a Plataforma Pública em **dois sítios geograficamente distintos (Brasília e São Paulo)**; cada PSP estabelece túneis para os gateways de VPN desses sítios.

Gateways de VPN: VPN GW da entidade parceira (IP público do PSP), VPN GW Brasília e VPN GW São Paulo (IPs públicos do SERPRO). Os túneis serão estabelecidos entre os links Primário / Secundário do PSP e da Plataforma Pública em cada site (Brasília e São Paulo). As sub-redes permitidas, ou tráfego de interesse, são definidas pela tabela de roteamento, e todo o tráfego é encaminhado via SNAT.

Endereçamento das interfaces de túnel (VTI): são usados endereços APIPA (faixa 169.254.0.0/16). Cada PSP recebe **duas redes /30** para a conexão ponto-a-ponto com o SERPRO, sendo uma para cada túnel; essa comunicação trafega por dentro dos túneis IPsec e garante o roteamento entre os sítios. Recomenda-se BGP para alta disponibilidade dinâmica; soluções com SD-WAN podem ser usadas para esse fim.

Identificação por SNAT: são reservadas redes 100.100.x.x/31para que os PSPs cheguem ao SERPRO com endereço conhecido e pré-definido, atribuído como **SNAT**, de forma que a rede interna do PSP fique "escondida" atrás dessa faixa, evitando sobreposição de endereçamento entre participantes. Esse endereçamento faz parte da faixa de CGNAT (Carrier Grade NAT), RFC 6598, e foi sugerido para evitar conflito com endereços privados, RFC 1918.

Adjacência e prioridades BGP: A adjacência BGP é estabelecida entre as interfaces VTI do SERPRO e do PSP. Os ASNs devem pertencer à faixa privada (64512 a 65534), sendo atribuídos ao SERPRO e ao PSP conforme a arquitetura da solução. A priorização dos caminhos é realizada por meio de recursos do próprio protocolo BGP, como o AS prepend.

2.3 LINK ÚNICO E DUAL-LINK

O túnel VPN pode operar sobre um único link de internet ou sobre dois links de operadoras distintas (dual-link), para maior resiliência. No modelo dual-link, cada link estabelece um túnel IPsec independente com a PP, em arranjo Primário/Secundário ou Ativo/Ativo (detalhado na Seção 5.6). Ambos os túneis deverão ser tratados como produção, mesmo que usado o arranjo Primário / Secundário.

A configuração criptográfica do túnel é idêntica nos modelos de link único e dual-link. Da mesma forma, os endpoints, as obrigações operacionais e as diretrizes para envio de informações à Plataforma Pública permanecem inalterados.

2.4 RESPONSABILIDADES: PLATAFORMA PÚBLICA × PSP

Fornecido pela Plataforma Pública	Configurado pelo PSP
Padrão criptográfico da VPN (Fase 1 e Fase 2)	Equipamento de borda (roteador/firewall) compatível com IKEv2
IP público do gateway VPN da PP (um peer remoto por site)	IP público fixo do peer do PSP (um por link)
Sub-redes remotas (redes da PP a serem alcançadas)	Sub-redes locais a serem anunciadas via VPN
Gerar e disponibilizar a PSK de forma segura, individualizada para cada PSP.	Configurar a PSK durante a implantação da VPN.

CAPÍTULO 3 – PRÉ-REQUISITOS DE REDE

Antes de iniciar a configuração do túnel, o PSP deve atender aos pré-requisitos abaixo.

3.1 LINKS E ENDEREÇAMENTO IP FIXO

- **IP público fixo:** obrigatório para a VPN IPsec, pois o gateway remoto da PP precisa identificar o peer de forma estável. IPs dinâmicos (DHCP) não são aceitos.
- **Bloco de IP:** recomenda-se ao menos um bloco /30 (2 IPs) ou /29 (6 IPs) por link, documentado formalmente pela operadora.
- **Link de internet dedicada (ADI):** recomenda-se acesso dedicado, simétrico e com SLA; em dual-link, operadoras distintas e infraestrutura física diversa.

3.2 EQUIPAMENTO DE BORDA

O roteador/firewall de borda deve suportar IKEv2 e os algoritmos do padrão criptográfico (Capítulo 5). Devem ser registrados o modelo e a versão de firmware/IOS para validação de compatibilidade junto ao time de redes da Plataforma Pública. Em dual-link, recomenda-se equipamentos distintos por link, eliminando o roteador como ponto único de falha.

3.3 LIBERAÇÃO DE PORTAS E FIREWALL

As seguintes portas e protocolos devem ser liberados entre o peer do PSP e o gateway da PP:

Serviço	Porta / Protocolo	Finalidade
IPsec IKE / NAT-T	UDP 500 e 4500	Negociação e manutenção do túnel VPN (NAT-T quando houver NAT)
IPsec ESP	Protocolo IP 50	Tráfego cifrado da VPN (quando sem NAT-T)

As seguintes portas e protocolos devem ser liberadas nos firewalls que estabelecem túnel para permitir a comunicação da aplicação e roteamento. Aqui não se trata da liberação entre os peers públicos, mas sim das liberações após VPN estabelecida:

Serviço	Porta / Protocolo	Finalidade
BGP	TCP 179	Sessão de roteamento dinâmico entre as interfaces VTI (Route-Based)
Portas da aplicação	TCP 443	Comunicação HTTPS/REST com a API da Plataforma Pública, sobre o túnel

CAPÍTULO 4 – PARÂMETROS DA VPN

A configuração do túnel depende de dois conjuntos de parâmetros: os fornecidos pela Plataforma Pública e os fornecidos pelo PSP. Os valores concretos (endereços, sub-redes e ambientes) são fornecidos pelo time de redes da Plataforma Pública no processo de onboarding técnico e não devem ser presumidos.

4.1 PARÂMETROS FORNECIDOS PELA PLATAFORMA PÚBLICA - VPN

Parâmetro	Descrição
IP público do gateway VPN da PP	Endereço(s) do peer remoto (Plataforma Pública)
Pre-Shared Key (PSK)	Mínimo de 20 caracteres;
Sub-redes remotas	Redes da PP a serem alcançadas pelo PSP
Padrão criptográfico	Algoritmos de Fase 1 e Fase 2 (ver Capítulo 5)
Ambiente	Homologação e produção, com seus respectivos endereços. Ambos devem ser tratados como produção.
Endpoints da API	URLs base por ambiente (HTTPS), conforme Manual de Integração

4.2 PARÂMETROS FORNECIDOS PELA PLATAFORMA PÚBLICA - ROUTING

Parâmetro	Descrição
Sub-redes a anunciar	Rede criada para fazer o SNAT, enviada pela PP. Rede 10.x.x.x/31
Rede VTI	IPs que devem ser configurados nas interfaces de túnel. Rede APIPA (Faixa 169.254.0.0/16) e serão usados para estabelecer vizinhança BGP
Parâmetros BGP	Todos os parâmetros que serão usados para estabelecer conexão BGP
Sistema Autônomo de Rede (ASN)	ASN privado correspondente ao ponto de conexão da Plataforma Pública.
Saltos para “AS prepend”	Número de saltos “AS prepend” usados para definir Primário / Secundário.
Bidirectional Forwarding Detection (BFD)	Habilitado ou não, para comutação praticamente instantânea
capability-graceful-restart	Habilitado ou não. Preserva o encaminhamento das rotas durante o reinício/restabelecimento da sessão BGP, evitando interrupção do tráfego enquanto a adjacência se restabelece.

4.3 PARÂMETROS FORNECIDOS PELO PSP - VPN

Parâmetro	Descrição
IP público fixo do peer (PSP)	IP da interface WAN do roteador/firewall - um por link
Equipamento de borda	Modelo e versão de firmware/IOS

4.4 PARÂMETROS FORNECIDOS PELO PSP - ROUTING

Parâmetro	Descrição
Parâmetros BGP	Todos os parâmetros que serão usados para estabelecer conexão BGP
Sistema Autônomo de Rede (ASN)	Informar o ASN privado do PSP ou de cada datacenter, quando aplicável.

CAPÍTULO 5 – CONFIGURAÇÃO DA VPN IPSEC - PASSO A PASSO

5.1 VISÃO GERAL DO PROCESSO

A configuração do túnel segue a sequência abaixo, executada no equipamento de borda do PSP em conformidade com o padrão fornecido pela PP:

- Reunir os parâmetros da VPN (Capítulo 4) e validar a compatibilidade do equipamento;
- Liberar as portas e protocolos no firewall (Seção 3.3);
- Configurar a Fase 1 (IKE) com os algoritmos do padrão (Seção 5.2);
- Configurar a Fase 2 (IPsec) e os seletores de tráfego (Seção 5.3);
- Definir a autenticação por “Pre-Shared Key” (Seção 5.4);
- Configurar o roteamento das sub-redes locais e remotas (Seção 5.5);
- Habilitar o Dead Peer Detection e, em dual-link, o failover via BFD, se for o caso (Seção 5.6);
- Validar e testar a conexão.

5.2 FASE 1 IKE (INTERNET KEY EXCHANGE)

Os parâmetros abaixo devem ser configurados de forma idêntica em ambos os túneis (em dual-link):

Parâmetro	Valor
Versão	IKEv2 (obrigatório; IKEv1 não será aceito)
Criptografia	AES-256
Integridade / Hash	SHA-256
Grupo Diffie-Hellman	Grupo 19 (ECP-256) como linha de base (NIST SP 800-77); Grupo 14 (2048 bits) aceitável.
Lifetime da SA	28.800 segundos (8 horas)
Autenticação	Pre-Shared Key (PSK), mínimo de 20 caracteres alfanuméricos contendo maiúsculas, minúsculas, números e símbolos
DPD (Dead Peer Detection)	Habilitado - intervalo (a definir) s / (a definir) tentativas

5.3 FASE 2 IPSEC

Parâmetro	Valor
Protocolo	ESP (Encapsulating Security Payload)
Criptografia	AES-256
Integridade / Hash	SHA-256
PFS (Perfect Forward Secrecy)	Habilitado - Grupo 19 (ECP-256) como linha de base (NIST SP 800-77); Grupo 14 aceitável.

Parâmetro	Valor
Lifetime da SA	3.600 segundos (1 hora)
Modo de encapsulamento	Tunnel Mode
Seletores de tráfego	Sub-redes locais (PSP) ↔ sub-redes remotas (PP), conforme Capítulo 4

5.4 AUTENTICAÇÃO (PRE-SHARED KEY)

A autenticação do túnel é feita por Pre-Shared Key (PSK) de no mínimo 20 caracteres, contendo letras maiúsculas e minúsculas, números e símbolos.

5.5 ROTEAMENTO

O tráfego destinado às sub-redes da PP deve ser roteado pelo túnel, por roteamento dinâmico (BGP), conforme a política definida com o time de redes da Plataforma Pública. Devem ser anunciadas apenas as sub-redes locais estritamente necessárias ao acesso à Plataforma, observando o princípio do menor privilégio. Deverão ser usadas as redes designadas para estabelecimento do BGP e SNAT para tráfego de dados conforme envio pela Plataforma Pública (ver Seção 4.1). Será usado também o parâmetro “AS prepend” para definição de qual rota é principal ou secundária.

5.6 DEAD PEER DETECTION E FAILOVER (DUAL-LINK)

O Dead Peer Detection (DPD) detecta a indisponibilidade do peer remoto e, em dual-link, aciona o failover automático para o link secundário. Mecanismos complementares de teste (IP SLA, Link-Monitor, Track, BFD) permitem chaveamento mais rápido. As duas modalidades de redundância são:

Primário/Secundário: O link primário transporta 100% do tráfego em condições normais, enquanto o secundário mantém o túnel VPN estabelecido e em prontidão. Em caso de indisponibilidade do caminho primário, o tráfego é direcionado automaticamente para o link secundário, conforme os mecanismos de roteamento e failover configurados.

Com DPD configurado com intervalo de (a definir) segundos e (a definir) tentativas, o tempo de detecção da falha pode chegar a aproximadamente (a definir) segundos, dependendo da implementação. Para uma detecção mais rápida e uma convergência mais previsível, recomenda-se utilizar BFD associado ao mecanismo de roteamento, quando suportado por ambas as extremidades.

Ativo/Ativo: Ambos os links carregam tráfego simultaneamente, com balanceamento. Dobra a banda disponível, mas exige roteamento avançado no equipamento do PSP; cada link deve suportar todo o tráfego na falha do outro.

5.7 CHECKLIST DE CONFIGURAÇÃO

Item	Critério de conclusão
Portas liberadas no firewall (UDP 500/4500, ESP)	Testado com tcpdump ou equivalente

Item	Critério de conclusão
Fase 1 (IKE) configurada	Status ESTABLISHED; algoritmos conforme Seção 5.2
Fase 2 (IPsec) configurada	Status ESTABLISHED; seletores e PFS corretos
Pre-Shared Key configurada	PSK ≥ 20 caracteres; enviada por canal seguro
Roteamento configurado	Tráfego das redes da PP roteado pelo túnel
DPD / failover habilitado	Intervalo (a definir) s / (a definir) tentativas (detecção em torno de (a definir) s);
NTP sincronizado	Diferença de relógio < 5 s
BFD Habilitado	(a definir)

CAPÍTULO 6 – SEGURANÇA DA REDE E DA COMUNICAÇÃO

6.1 PADRÃO CRIPTOGRÁFICO DO TÚNEL

O túnel utiliza IKEv2 com AES-256 e SHA-256 na Fase 1, e ESP com AES-256, SHA-256 e PFS (Grupo 19 / ECP-256, ou Grupo 14) na Fase 2, em Tunnel Mode (ver Seções 5.2 e 5.3). Os parâmetros devem ser idênticos em ambos os túneis no modelo dual-link. IKEv1 não é aceito. O padrão tem base no NIST SP 800-77 Rev.1 e no RFC 8247.

6.2 FIREWALL E CONTROLE DE ACESSO

Recomenda-se restringir as regras de firewall ao estritamente necessário: liberar apenas as portas da Seção 3.3 e, sempre que possível, restringir a origem/destino aos endereços do peer e às sub-redes acordadas com o time de redes da Plataforma Pública (allowlisting). O acesso à API deve ser limitado às redes que efetivamente realizam a integração.

6.3 BOAS PRÁTICAS DE SEGURANÇA OPERACIONAL

- Manter o NTP sincronizado em todos os equipamentos de borda;
- Anunciar apenas as sub-redes necessárias, aplicando o princípio do menor privilégio;
- Registrar e analisar logs de IKE/DPD e de renegociação de SA para detecção precoce de instabilidades;
- Configurar alertas para queda de túnel e degradação de banda;
- Segregar as redes internas que acessam a Plataforma das demais redes corporativas.

6.4 GESTÃO DO CICLO DE VIDA DA PSK

A Pre-Shared Key (PSK) que autentica o túnel (Seção 5.4) é gerada pela Plataforma Pública, individualmente para cada PSP e por ferramenta criptograficamente segura (CSPRNG), com PSKs distintas para homologação e produção. A tabela a seguir resume os procedimentos de compartilhamento, rotação e revogação da chave.

Procedimento	Resumo
Compartilhamento	A PP gera a PSK e a entrega de forma segura previamente acordada. Opções, em ordem de preferência: cofre de senhas com link de acesso único e expiração; e-mail cifrado (PGP/S-MIME); videoconferência privada com autenticação; ferramentas que apagam a mensagem após a leitura; ou SharePoint com MFA. A PSK não é armazenada em ticketing, e-mail ou formulários abertos.
Revogação	Invalidação imediata da PSK. Em incidente (vazamento, equipamento comprometido, ex-funcionário com acesso), a PP desativa o peer nos dois sítios, gera nova PSK e revalida o túnel após a reconfiguração. No offboarding, a PP remove o peer, revoga firewall e allowlist, libera SNAT (100.100.x.x/31) e VTI (APIPA /30) e descarta a PSK sem recuperação.

CAPÍTULO 7 – OPERAÇÃO E SOLUÇÃO DE PROBLEMAS

7.1 MONITORAMENTO DOS TÚNEIS

Recomendações:

- Manter dashboard em tempo real com o status dos túneis e dos links (em dual-link, dos dois);
- Configurar alertas para queda de túnel, degradação de banda acima de 5% e latência acima do limiar;
- Coletar logs de DPD e de renegociação de SA para análise de instabilidades.

7.2 PROBLEMAS COMUNS E SOLUÇÕES

Sintoma	Causa provável	Ação
Fase 1 (IKE) não estabelece	IP do peer/PSK incorretos; IKEv2 não habilitado; UDP 500/4500 bloqueado; relógio dessincronizado	Conferir peer e PSK; habilitar IKEv2; liberar portas; sincronizar NTP
Fase 2 (IPsec) não estabelece	Propostas/PFS divergentes; seletores de tráfego incompatíveis; lifetimes incompatíveis	Alinhar algoritmos (Seção 5.3), seletores e lifetimes com o padrão da PP
Túnel sobe, mas não há tráfego	Rotas ausentes; sub-redes locais não anunciadas; firewall interno	Revisar roteamento (Seção 5.5) e regras de firewall
Quedas/perdas intermitentes	MTU/MSS (fragmentação); NAT-T ausente atrás de NAT; DPD mal ajustado	Ajustar MTU/MSS; habilitar NAT-T (UDP 4500); revisar DPD
Failover lento (dual-link)	Ausência de IP SLA/Track; threshold de DPD elevado	Habilitar testes de link; reduzir intervalo/retries do DPD

CAPÍTULO 8 – CONFIGURAÇÃO DE CONECTIVIDADE COM A PLATAFORMA PÚBLICA

Para habilitação da conectividade com a Plataforma Pública, o PSP deverá encaminhar ao time de redes as informações necessárias para configuração do respectivo peer.

Informações obrigatórias

O PSP deverá informar:

- Identificação do participante (razão social e ISPB);
- Ambiente de destino (Homologação ou Produção);
- Endereço(s) IP(s) público(s) que serão utilizados para iniciar o estabelecimento da VPN;
- Dados técnicos do equipamento concentrador VPN do PSP, quando aplicável;
- Janela desejada para realização da configuração e testes;
- Contatos técnicos responsáveis pela implantação e suporte da conectividade.

Configuração pela Plataforma Pública

Com base nas informações fornecidas pelo PSP, o time de redes da Plataforma Pública realizará:

- O cadastramento do peer correspondente ao participante;
- A configuração, nos equipamentos de borda, dos endereços IP autorizados a iniciar tentativas de estabelecimento da VPN;
- O encaminhamento do tráfego autorizado ao concentrador VPN responsável pela negociação do túnel seguro;
- A validação dos parâmetros técnicos definidos para a conexão;
- A liberação da conectividade para execução dos testes de homologação.

Observações

- A autorização dos endereços IP possui finalidade exclusiva de permitir o encaminhamento do tráfego até o concentrador VPN da Plataforma Pública.
- O simples cadastramento dos endereços IP não caracteriza estabelecimento da conexão nem concessão automática de acesso aos serviços da Plataforma Pública.
- O acesso efetivo aos ambientes estará condicionado à conclusão bem-sucedida das etapas de autenticação e validação previstas no processo de estabelecimento da VPN.
- Qualquer alteração nos endereços IP previamente cadastrados deverá ser comunicada formalmente pelo PSP para atualização das configurações do peer.

CAPÍTULO 9 – ROTEAMENTO DINÂMICO E ENDEREÇAMENTO (BGP, VTI E SNAT)

Esta seção consolida o modelo de roteamento e endereçamento adotado pela Plataforma Pública (SERPRO) para a interconexão com os PSPs, em complemento ao Capítulo 2.

9.1 TIPO DE VPN E INTERFACES VTI

- **Tipo de VPN:** Route-Based (VTI). Interfaces de túnel virtual ponto-a-ponto, que permitem roteamento dinâmico e isolamento de tráfego.
- **Endereços das VTIs:** APIPA, faixa 169.254.0.0/16, com duas redes /30 por PSP para a conexão ponto-a-ponto com o SERPRO. A comunicação trafega por dentro dos túneis IPsec.
- **Alta disponibilidade:** recomenda-se BGP; soluções com SD-WAN podem ser usadas, caso seja viável. O tráfego é manipulado por roteamento dinâmico entre os sítios.

9.2 BGP E IDENTIFICAÇÃO POR ASN

- **Adjacência BGP** estabelecida entre as interfaces VTI do SERPRO e do PSP.
- **ASN privados (64512–65534):** exemplos como SERPRO Brasília 65000, SERPRO São Paulo 65001, PSP 65002.
- **Manipulação de rotas:** uso de AS-path prepend para definir prioridades de caminho (primário/secundário).

9.3 SNAT E FAIXA RESERVADA

São reservadas redes **100.100.x.x/31** para que cada PSP alcance o SERPRO com endereço conhecido e pré-definido. Esse endereço é atribuído como **SNAT**, “escondendo” a rede interna do PSP e evitando sobreposição de endereçamento entre participantes. Cada PSP recebe um endereço de SNAT para sua identificação.

Elemento	Definição
Tipo de VPN	Route-Based (VTI)
Endereços das VTIs	APIPA 169.254.0.0/16 - /30 por PSP
Protocolo de roteamento	BGP (ASN privado por sítio e por PSP)
Manipulação de rotas	AS-path prepend
Identificação do PSP	Endereço de SNAT em faixa 100.100.x.x/31

CAPÍTULO 10 – REFERÊNCIAS NORMATIVAS

10.1 NIST

- NIST SP 800-77 Rev.1 — Guide to IPsec VPNs

10.2 IETF / RFCS

- RFC 7296 — Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 4301 — Security Architecture for IP
- RFC 8247 — Algorithm Implementation Requirements for ESP and AH
- RFC 4307 — Cryptographic Algorithms for use in IKEv2 (e correlatas de IPsec)
- RFC 4271 e RFC 6286 — BGP (Border Gateway Protocol)
- RFC 6996 — Autonomous System (AS) Reservation for Private Use
- RFC 3022 — Traditional IP Network Address Translation (NAT)
- RFC 3927 e RFC 6890 — Endereçamento link-local / APIPA e blocos de uso especial
- FIPS 203 — referência para evolução à criptografia pós-quântica (futuro)

CAPÍTULO 11 – HISTÓRICO DE REVISÃO

Data	Versão	Descrição das Alterações
27/07/2026	1.0.0	Versão Inicial

APÊNDICE A – GLOSSÁRIO

Termo	Definição
VPN IPsec	Rede privada virtual que cifra e autentica o tráfego entre o PSP e a PP.
Site-to-Site	Modelo de VPN que conecta duas redes (gateways), e não usuários individuais.
IKEv2	Internet Key Exchange v2, protocolo de negociação das chaves/SA da VPN (obrigatório).
Fase 1 (IKE)	Etapa que estabelece o canal seguro de negociação entre os peers.
Fase 2 (IPsec)	Etapa que estabelece as SAs que cifram o tráfego de dados (ESP).
ESP	Encapsulating Security Payload, protocolo IPsec que cifra e protege a integridade do tráfego.
SA	Security Association, conjunto de parâmetros e chaves de uma sessão IPsec.
PSK	Pre-Shared Key, chave compartilhada de autenticação do túnel (mínimo de 20 caracteres; ver Seção 5.4).
PFS	Perfect Forward Secrecy, renovação de chaves que impede a decifração retroativa do tráfego.
DPD	Dead Peer Detection, detecta a queda do peer remoto e aciona o failover.
NAT-T	NAT Traversal, encapsula o IPsec em UDP 4500 para travessia de NAT.
Tunnel Mode	Modo de encapsulamento IPsec que protege todo o pacote IP original.
Grupo DH	Diffie-Hellman, define a força da troca de chaves (Grupo 14 = 2048 bits).
AES-256 / SHA-256	Algoritmos de criptografia e de integridade adotados no túnel.
TLS 1.3	Transport Layer Security 1.3, cifragem da sessão HTTPS.
IP fixo / ADI	Endereço público estático; Acesso Dedicado à Internet (link dedicado e simétrico).
ECMP	Equal-Cost Multi-Path, balanceamento entre rotas de mesmo custo (modo ativo/ativo).
MTU / MSS	Tamanho máximo de pacote/segmento; ajuste evita fragmentação no túnel.
RTT	Round-Trip Time, tempo de ida e volta de um pacote (latência).
Gateway PP	Ponto de entrada da Plataforma Pública.