1 ARQUITETURA DO CLEAN PIPES

O CLEAN PIPES é uma plataforma em nuvem e é entregue ao cliente sem a necessidade de adquirir ou instalar qualquer equipamento de segurança da informação no perímetro do cliente, este tipo de serviço é denominado *Serviço em nuvem de Segurança (Security as a Service – SecaaS* em inglês*)*.

A solução está fisicamente instalado no **Data Center Telefônica – Tamboré 1**, um dos maiores e mais modernos Data Center do Brasil.

1.1 UTM – UNIFIED THREAT MANAGEMENT

O **CLEAN PIPES** oferece um conjunto robusto de tecnologias avançadas de segurança baseada em assinaturas, heurística, e em um núcleo de firewall e VPN de alta velocidade. Este conjunto inclui prevenção de intrusão, controle de aplicativos, Anti Malware, Filtro Web, dentre outros.

As seguintes funcionalidades são oferecidas dentro do CLEAN PIPES:

1.1.1 Firewall

O firewall controla as comunicações que passam pela rede do cliente desde/até a Internet segundo as políticas definidas daquilo que é permitido/negado. Para permitir ou negar uma comunicação o firewall examina a origem e o destino da informação além do tipo de conexão estabelecida (porta).

O serviço proporciona uma medida de segurança adicional de maneira que não seja possível iniciar conexões diretamente da Internet até os equipamentos/servidores do cliente sem proteção, desta maneira apenas será permitido tráfego desde a Internet que seja resposta a uma petição autorizada e originada nas instalações do cliente.

1.1.1.1 Políticas de Firewall

O cliente terá a possibilidade de definir as políticas de firewall na hora de contratar o serviço ou alterar tais políticas abrindo chamado na central de relacionamento **Vivo Empresas**.

Perfis de política de firewall disponíveis no Plano UTM são:

- **Presença e navegação**

Esta política está desenhada para empresas que necessitem conexões desde a Internet até servidores localizados na rede do cliente, exemplo: servidores web ou servidores de correio eletrônico. Da mesma maneira, garante uma comunicação segura para os usuários da empresa que necessitam navegar na Internet, por isso esta política permite o acesso aos serviços básicos da Internet.

- **Navegação**

Esta política está desenhada para empresas que necessitam conexão maneira segura a serviços publicados na Internet.

- **Avançada**

Caso a empresa possua necessidades de navegação e presença mais complexas poderá ser criado um perfil específico em linha com os requerimentos de comunicação do cliente. Para isso será proposto como base o perfil Presença e Navegação onde o cliente poderá adicionar necessidades específicas para serviços como streaming, peer-to-peer, VoIP, etc.

Caso o cliente escolha o perfil avançada o cliente deverá preencher o formulário de ativação

Os detalhes das políticas de firewall se encontram especificados no ANEXO 1.

O Cliente terá até 30 dias após a implantação da solução de dados para escolher a configuração de firewall que melhor atenda as suas necessidades de negócio, caso isso não aconteça o firewall virtual será configurado atendendo a seguinte política:

- Todo o tráfego oriundo da internet (iniciado nela) será proibido
- Todo o tráfego de saída para a internet (http e https) será permitido

1.1.2 IPS – Intrusion Prevention System (Sistema de Prevenção de Intrusões) e Anti Botnets

1.1.2.1 IPS

Os clientes podem ser infectados quando navegam em sites aparentemente seguros que foram corrompidos anteriormente. Nestes casos, o código malicioso contido no site aproveita vulnerabilidades no navegador ou dos plugins (por exemplo: Java, Flash, etc.) instalando um código malicioso no computador infectado. Nossa solução ajuda a bloquear tais ataques ativando mais de 4.000 assinaturas maliciosas conhecidas e de “zero-day” garantindo a proteção do usuário que navega na Internet.

1.1.2.2 Anti-Botnets

Os equipamentos infectados podem estabelecer comunicação com servidores remotos desde os quais podem ser lançados ataques no futuro ou simplesmente pertencer a uma rede de Botnets para distribuir Malwares.

Nosso serviço consegue bloquear de maneira dinâmica as conexões dos equipamentos infectados com servidores remotos de duvidosa reputação. Através de atualizações de IPs o serviço bloqueia a comunicação com estes servidores que sejam parte de redes Botnets.

A solução tem a capacidade de inspecionar em nível de aplicação detectando aplicações maliciosas e bloqueando as mesmas independentemente da porta e IP por onde é feita a comunicação.

1.1.3 Anti-Malware

O serviço inspeciona em modo flow todo o trafego de navegação do cliente, tráfego de e-mail e FTP detectando, bloqueando, eliminando arquivos infectados com vírus, Spyware, Adware, trojans e outros Malwares antes deles chegarem ao ambiente do cliente.

- **Nota:** É importante destacar que a analise e bloqueio de arquivos infectados acontece no nível da navegação ou acesso a internet da plataforma de proteção da Telefonica | Vivo. Caso o cliente ou usuários da rede utilizem outro provedor de Internet ou façam uso de dispositivos de armazenamento (pendrive, HD externos, etc.) infectados a solução, não será efetivo o bloqueio destas ameaças. Nosso cliente pode solicitar à Telefonica | Vivo soluções específicas para esta situação (endpoint, antivírus, etc.).

1.1.4 Filtro web

O filtro web tem como finalidade permitir ou negar o acesso a páginas web segundo o tipo e conteúdo da informação . A solução oferece três perfis de filtro sendo que os sites dentro da categoria “Maliciosos”, “Phising” e “URLs de Spam” são bloqueados. A solução poderá ser configurada de maneira que seja mostrado um alerta ao usuário que está acessando a uma página com potencial de risco e decidir se continua ou não com a navegação (modelo “Aviso”). A solução também poderá ser configurada de maneira que os sites com potencial de risco sejam sempre bloqueados (modelo “Bloqueio”). O cliente escolherá o perfil de filtro web na hora da contratação do serviço .

Nota:

- Apenas é bloqueado o tráfego que sai do cliente a través do acesso a internet da Telefónica/Vivo.
- Se o cliente usar um dispositivo móvel da empresa fora da rede desta, o tráfego não será controlado.
- Se o cliente tem um link de redundância com outro ISP e está acessando a Internet por esse link, esse tráfego não será controlado.
- O cliente poderá alterar a lista de sites permitidos e bloqueados solicitando atendimento na central de relacionamento.

1.1.4.1 Grupos de Filtro Web

O Cliente poderá escolher grupos de filtro web pré-definidos na implantação. Tais grupos poderão ser customizados após a completa configuração do serviço.

Os perfis de filtro web pré-definidos para o serviço são:

- Navegação Segura
- Navegação Produtiva
- Restritiva

O Cliente terá até 30 dias após a implantação da solução de dados para escolher o grupo de filtro web que melhor atenda as suas necessidades de negócio, caso isso não aconteça será configurado a opção: “Navegação Segura”.

1.2 Provisionamento da Conectividade

Cada cliente terá direto a 1 (uma) VDOM provisionada exclusivamente para si, onde as regras de firewall e filtro web serão configurados.

Domínios virtuais (VDOMs) é um método de dividir uma unidade UTM em duas ou mais unidades virtuais que funcionam como múltiplas unidades independentes. Um único UTM é flexível o suficiente para atender a vários clientes.

VDOMs fornecem domínios de segurança separados que permitem zonas separadas, autenticação de usuários, políticas de segurança, roteamento e configurações VPN.

1.2.1 Topologia Fim-a-Fim

A topologia fim-a-fim para entregar o acesso seguro à internet com o CLEAN PIPES para o cliente PJ está representada na figura abaixo:

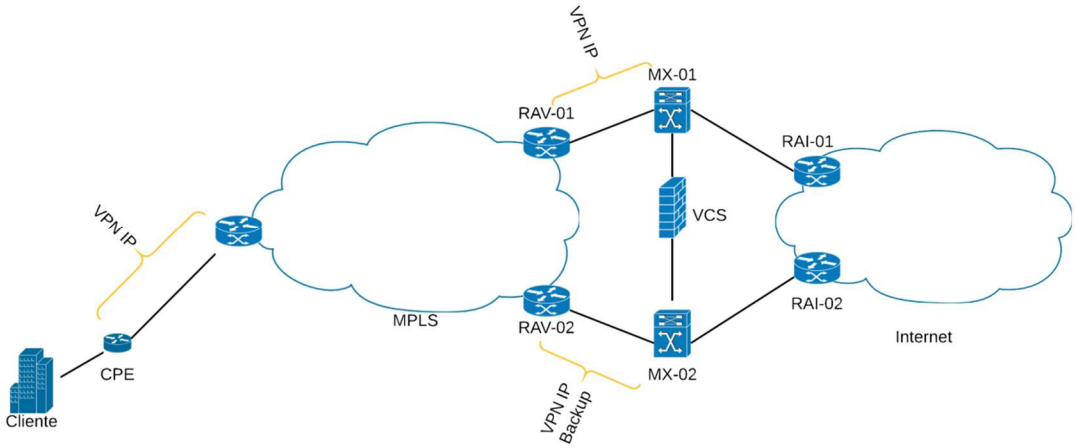

Figura 1. Topologia de implantação fim-a-fim do CLEAN PIPES e o acesso dados

1.2.2 Acesso de dados

O acesso entre o cliente o CLEAN PIPES é feito através de uma VPN IP pacote Light, com as seguintes características:

- Sem QoS
- Perfil bronze
    - Monitoramento de performance e utilização

1.2.2.1 Características da Implantação de Acesso de Dados VPN IP Light

Por padrão, o acesso de dados é implantação do acesso VPN IP Light com o seguinte cenário:

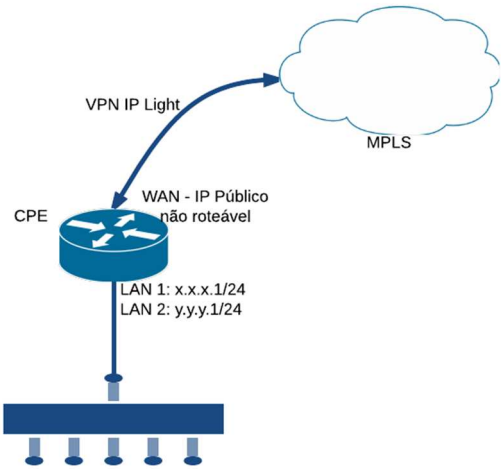

Figura 2. Cenário de Implantação VPN IP Light

Funcionamento:

- Toda a conectividade do cliente até o UTM será via rede segregada na MPLS da Telefônica| Vivo
- O roteador será instalado no cliente com a interface LAN configurada com 1 IP Privado de uma rede já definida pela Telefônica (X.X.X.X/24) e será alterada conforme solicitação a ser realizada pelo cliente com as seguintes opções de configurações na interface LAN do Roteador do cliente:
    - Alteração do IP privado na interface LAN do Roteador;
    - DHCP
    - VRRP (caso de links redundantes)
    - Rotas Estáticas na interface LAN do Roteador;
    - Trunk dot1q;
- Apenas os IP's das redes LAN's do cliente que tiverem conectividade IP com a interface LAN do roteador, terão políticas (acesso/segurança) no UTM para entrada/saída de tráfego com a Internet;
- Disponível para qualquer roteador homologado para VPN IP Light.

Restrições:

- Não será possível conectividade do UTM com qualquer outra rede LAN do cliente que não seja a que estiver diretamente conectada na LAN do Roteador do Cliente, devido a não existir conectividade IP.
- Não será possível criar políticas (acesso/segurança) no UTM para tráfego locais do cliente, devido a não existir conectividade IP com outras redes LAN;
- Não contempla projeto de migração ou reestruturação de redes. Ex.: Migração de regras de firewall, alterações na rede de L2 e L3 em relação a conectividade/roteamento;
- Todos os IP's Públicos serão configurados no firewall, não havendo a possibilidade de configuração de IP's públicos diretamente em hosts da rede LAN do Cliente, devido aos scripts padrões de ativação no roteador do cliente (definição de Produtos para facilitar a ativação);

1.3 Entregáveis

Os entregáveis do produto são:

- Acesso via **VPN IP** pacote **Light** que vai desde o endereço do cliente até o Novo Data Center de acordo com as características apresentadas no item 1.2. Cliente Provisionado na CLEAN PIPES de acordo com o perfil escolhido
- Acesso à internet através do POP do Novo Data Center

2 DEFINIÇÃO DAS RESPONSABILIDADES

2.1 Do Cliente

Clientes que por ventura venham a contratar serviços da **Vivo** estarão assumindo as seguintes as responsabilidades:

- Fornecer a **Vivo** as informações necessárias para ativação da solução dentro do prazo estabelecido no ponto 5.7.
- Informar a **Vivo** sobre qualquer mudança com relação à prestação dos serviços, com a devida antecedência permitindo que a mesma tenha tempo suficiente para preparar e implementar as alterações necessárias, conforme tais alterações ou mudanças afetem a prestação dos serviços. O Cliente deverá fornecer informações suficientes com relação às suas necessidades.
- Informar a **Vivo** com antecedência mínima de 30 (trinta) dias, sobre qualquer mudança que possa afetar a prestação de Serviços.
- Zelar pela conservação e correto manuseio da infraestrutura disponibilizada pela Telefônica | Vivo, responsabilizando-se pelos eventuais danos, pessoais e materiais, decorrentes de ações e utilizações indevidas por parte de seu pessoal ou de seus equipamentos.
- Definir prioridades/graus de severidade de atendimento
- Informar internamente e aos seus outros prestadores de serviços, o escopo de contrato com a Telefônica | Vivo, quando relacionado à suas atividades.
- Não gerenciar diretamente nenhum funcionário ou terceiros da **Vivo** alocados ou em atendimento nos sites do cliente
- Providenciar as autorizações de ingresso do pessoal da **Vivo** às suas instalações para executar o projeto contratado (caso for necessário).
- Designar um único interlocutor como responsável pelo projeto, e definir as pessoas de contato autorizadas a realizar consultas.
- Analisar o produto gerado e aprová-lo quando corresponder, garantindo a continuidade das diversas atividades do projeto e possibilitando seu fechamento quando os requisitos definidos para o projeto forem atendidos.
- Brindar a correspondente diligência nos trabalhos que lhe sejam próprios a executar dentro dos prazos do planejamento proposto.

- Designar o pessoal necessário, especializado nas funções a realizar e com dedicação suficiente a essas tarefas, para coordenar e entregar a **Vivo** a informação necessária para análise e resolução de eventos.
- Proporcionar, conforme corresponda, a infraestrutura necessária para instalação de equipes, cumprindo com as especificações indicadas nesta oferta.
- Manter atualizada junto à **Vivo** a lista de pessoas autorizadas a abrir chamados e solicitações de suporte.

2.2 Da Telefonica Vivo

A **Vivo** assume as seguintes responsabilidades perante os Clientes que venham a contratar seus serviços.

- Designar um profissional **Vivo** que será ponto focal para o projeto;
- Tornar disponíveis recursos **Vivo** necessários para execução dos serviços;
- Executar os serviços de acordo com os objetivos de níveis de serviço;
- Executar todas as atividades dentro dos padrões de qualidade **Vivo** e conforme estabelecido no contrato com o cliente;
- Cumprir os prazos estabelecidos nas atividades do projeto, desde que as responsabilidades do cliente sejam cumpridas;
- Gerenciamento proativo do serviço incluindo o fornecimento da Central de Atendimento.
- Dirigir, organizar e gerenciar o projeto.
- Participar nas reuniões de trabalho combinadas.
- Manter informado o pessoal do cliente sobre ações e resultados nas diferentes atividades.
- Garantir a confidencialidade dos dados informados pelo cliente para o desenvolvimento da atividade.
- O pessoal da **Vivo** que tiver acesso aos escritórios do cliente estará sujeito às normas de segurança que o cliente estabelecer para acesso e permanência em suas instalações.
- Comunicará e solicitará ao cliente, a aprovação explícita de qualquer mudança da equipe de trabalho, com uma antecipação mínima de sete (7) dias corridos.

3 NÍVEIS DE SERVIÇO

Este item tem como objetivo estabelecer e fornecer informações a respeito do acordo de nível de serviço que irá definir os padrões de qualidade para o CLEAN PIPES.

Tratam-se dos tempos de resposta do SOC para os chamados abertos.

Severidade	Definição
Crítico	Evento que indisponibiliza os serviços de um ativo classificado como crítico.
Alto	Evento que degrada os serviços de um ativo classificado como crítico ou que indisponibiliza os serviços de um ativo não crítico

Médio	Evento que degrada os serviços de um ativo classificado como não crítico
Baixo	Evento que não afeta os serviços, pouco ou nenhum impacto na operação.
Consulta/Solicitação	Consulta de dúvidas e solicitação de Inclusão/Alteração/Remoção das configurações

Tabela 1. Descrição das severidades.

3.1 SLO de Prestação de Serviços

O CLEAN PIPES é prestado considerando os seguintes objetivos de atendimento:

3.1.1 SLO de Incidentes

Definição	Crítico	Alto	Médio	Baixo
Tempo de atendimento a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC	30 min.	45 min.	1,5h (8X7).	2,5h. (8X5)
Tempo de resposta a partir da comunicação do cliente até que SOC faça o primeiro diagnóstico	1,5h.	2h.	3,5h. (8x7)	6,5h. (8x5)
Tempo de resolução a partir da comunicação do cliente até que o SOC comunique a resolução do mesmo	4,5h.	6,5h.	24h. (8x7)	36h. (8x5)

Tabela 2. SLO de Incidentes

O SLO de incidentes é medido em 24x7 (horas por dia x dias por semana), exceto quando explicitamente atendimento em horário comercial (8x5) ou horário comercial estendido (12x5).

3.1.2 SLO de Entrega dos Relatórios

Serão gerados os seguintes tipos de relatório segundo definido junto ao cliente e atendendo o seguinte SLO dos modelos apresentados no item 3.5:

Definição	Prazo
Tempo de entrega de relatórios mensais	Até o 10º dia útil do mês subsequente

Tabela 3. SLO de Entrega de Relatórios

3.1.3 SLO de Solicitações e Consultas

Todas as Solicitações e Consultas serão registradas pela **Vivo** com severidade “Baixa” e atendidas em regime de 8x5 e terão seu SLO medido em horas comerciais (úteis).

Considera-se que as Solicitações e Consultas utilizarão os mesmos valores de SLO’s que os incidentes de severidade baixa.

Indicadores de Consultas

São previstas as seguintes consultas para este serviço:

- Máquinas mais acessadas
- Serviços mais utilizados
- Usuários que mais utilizaram serviços
- URLs mais visualizadas
- Categorias Web mais acessadas
- Maiores emissores e receptores de e-mail
- Vírus mais detectados

Indicadores de Solicitações

Para atendimento de solicitações, o cliente deve preencher e enviar formulário específico corretamente preenchido. Em caso de falta do mesmo, ou de erro no preenchimento, o SOC devolverá o formulário ao solicitante com a indicação do problema e aguardará o seu retorno. Este período não será contabilizado no cálculo do SLO.

São previstas as seguintes solicitações para este serviço:

- Modificação na lista de contatos autorizados do cliente.
- Inclusão/Alteração/Remoção de usuários adicionais, em acordo com o plano contratado.
- Inclusão/Alteração/Remoção de regras de firewall, em acordo com o plano contratado.
- Inclusão/Alteração/Remoção de filtro de conteúdo (Filtro Web), em acordo com o plano contratado.
- Inclusão/Alteração/Remoção de configuração VPN Site-to-Site/Client-to-Site, em acordo com o plano contratado.
- Inclusão/Alteração/Remoção de configuração de IPS, em acordo com plano contratado.
- Inclusão/Alteração/Remoção de configuração de Controle de Aplicações, em acordo com plano contratado

Definição	SLO	
Tempo de atendimento **de solicitações e consultas: a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC**	2,5h. (8X5)	Úteis NBD[1]
Tempo de resolução **de consultas: a partir da comunicação do cliente até que o SOC comunique a resolução do mesma**	6,5h. (8x5)	Úteis NBD
Tempo de resolução **de solicitações: a partir da comunicação do cliente até que o SOC comunique a resolução da mesma**	36h. (8x5)	Úteis NBD

Tabela 4. SLO de Solicitações

3.1.3.1 Quantidade máxima de solicitações e consultas mensais

Este item refere-se a quantidade máxima de solicitações e consultas que o cliente pode realizar no período de 1 mês.

Definição	Quantidade	Período

[1] NBD - Next Business Day, ou seja, tempo de resposta descartado os finais de semana.

Quantidade máxima de solicitações e consultas por mês	5	Mensal[2]

Tabela 5. Quantide de solicitações mensais

3.2 SLA de Prestação de Serviço

3.2.1 Suporte ao Cliente

Garantir o atendimento de **95% dos SLOs definidos acima por mês**.

Severidade	Definição	SLA
Crítico	Evento que indisponibiliza os serviços de um ativo classificado como crítico.	95%
Alto	Evento que degrada os serviços de um ativo classificado como crítico ou que indisponibiliza os serviços de um ativo não crítico	95%
Médio	Evento que degrada os serviços de um ativo classificado como não crítico	95%
Baixo	Evento que não afeta os serviços, pouco ou nenhum impacto na operação.	95%
Consulta/Solicitação	Consulta de dúvidas e solicitação de Inclusão/Alteração/Remoção das configurações	95%

3.2.2 Disponibilidade da Plataforma

SLA de disponibilidade do produto: A disponibilidade do serviço seguirá o seguinte modelo:

Serviço	Disponibilidade
Porta do Firewall	95,2%
Porta do IPS	95,2%
VPN SSL / VPN IPSec	95,2%
Anti Malware	95,2%
Filtro de Conteúdo	95,2%
Controle de Aplicações	95,2%

[2] Período definido do primeiro ao último dia útil do mês.

Tabela 6. SLA de Disponibilidade do Serviço

3.2.2.1 Interrupções

A disponibilidade que garante o serviço obedece às seguintes condições:

- Não se contabilizarão dentro do tempo da não disponibilidade as interrupções do serviço que foram provocadas por causas imputáveis ao cliente;
- O cliente está comprometido a facilitar o acesso a suas dependências, das pessoas designadas pela Telefônica | Vivo, para a resolução dos problemas, ou a operação do serviço que seja necessária. O tempo necessário para obter esta permissão está fora do cálculo da disponibilidade;
- A **Vivo** se reserva no direito de efetuar, mediante aviso prévio ao cliente, paradas técnicas que não se contabilizam no cômputo da disponibilidade;
- São excluídas interrupções do serviço devidas a causas de força maior (por exemplo, desastres naturais, atentados, etc).

Períodos de Manutenção

Por necessidade de manutenção, pode ser necessário deixar sem serviço a rede do Cliente, com o objetivo de executar reconfigurações, atividades de manutenção, etc., na rede. Tais atividades serão executadas, necessariamente, durante um período pré-programado de manutenção.

Interrupções Programadas

As interrupções programadas de disponibilidade do serviço sejam elas pelas causas motivadas pelo item anterior, de períodos de manutenção, ou motivadas por alguma solicitação do Cliente, não serão contabilizadas para o cálculo da disponibilidade do serviço, constantes no Compromisso de Qualidade do Serviço.

4 PENALIZAÇÃO

Somente se considera para efeitos de penalização:

- Incidentes Críticos e Altos;
- As requisições categorizadas como Altas pelo cliente na abertura do chamado.

Assim, os itens que excedam não cumpram o SLA definido estarão sujeitos a um desconto, que serão liquidadas mensalmente pela fórmula:

$$\mathrm{Vpd} = \frac{(\mathrm{Te} \times 100)}{(1.440 \times \mathrm{Nd})}$$

Na qual:

Vpd = percentual de minutos excedidos no respectivo mês;

Te = tempo excedido em minutos além do determinado na tabela de SLO para o serviço em questão;

Nd = Número de dias no mês

Sendo constatado o não cumprimento do SLA, os índices de descontos, da tabela, abaixo, serão aplicados sobre o valor mensal a ser pago pelo cliente. Os descontos serão aplicados no mês subsequente ao mês da confirmação da ocorrência.

Percentual	Descontos %
0 < Vpd ≤ 2	0,5
2 < Vpd ≤ 4	1,0
4 < Vpd ≤ 6	2,5
6 < Vpd ≤ 10	5,0
10 < Vpd ≤ 20	7,5
Vpd > 20	10,0

Tabela 7. Definição dos descontos

5 IMPLANTAÇÃO

5.1 Prazo de instalação

O processo de implantação seguirá as seguintes etapas:

5.1.1 Reunião técnica

A **Vivo** irá se reunir com a equipe técnica do cliente no prazo máximo de **30 dias úteis** após a assinatura do contrato, para o planejamento da implantação do serviço a ser fornecido. Nesta reunião deverão ser discutidos e esclarecidos todos os questionamentos técnicos do serviço assim como as definições técnicas de configuração dos serviços e atividades de responsabilidade do cliente.

5.1.2 Formulário de ativação

Após reunião técnica será disponibilizado um formulário técnico de ativação para identificação dos pré-requisitos e compatibilidades da solução, com as aplicações do cliente. O cliente deve preencher e retornar o formulário de ativação no prazo máximo de **30 dias** corridos caso contrário à solução será configurada conforme o seguinte padrão:

- Todo o tráfego de saída para a internet será permitido;
- Todo o tráfego oriundo da internet (iniciado nela) com destino à rede do cliente será proibido;
- Todo o tráfego web (HTTP) será controlado através de um grupo padrão de segurança, com características que inclui (a) todos os sites que conhecidamente trazem alto risco de segurança serão expressamente proibidos, (b) todos os sites ainda não categorizados serão permitidos e (c) a vasta maioria dos sites da internet serão permitidos;
- O IPS será configurado de acordo com o padrão sugerido pelo fabricante das soluções compostas pelo CLEAN PIPES;
- Nenhum usuário pode ser criado por padrão;

- Nenhum túnel VPN consegue ser criado;
- Apenas os contatos técnicos ou responsáveis informados nesta proposta podem entrar em contato com o SOC.

5.1.3 Instalação do serviço

O prazo previsto para instalação do serviço é de **até 60 dias corridos**, contados após a disponibilização dos dados necessários para a configuração da solução, através de cronograma a ser estabelecido de comum acordo entre as partes. Este prazo não contempla a disponibilização de equipamentos, no caso de vendas ou locação, assim como os prazos de instalação de links de dados, quando inclusos nos projetos. Limitações ou situações específicas de cada cliente e projeto podem causar variação nos prazos estabelecidos.

Ao finalizar o período de provisão do serviço, o cliente e **Telefônica|Vivo** acordarão testes de configuração para verificar o funcionamento correto de cada uma das funcionalidades do produto. Com o objetivo de customizar os limiares de detecção para aperfeiçoar o serviço ao cliente, a **Telefônica|Vivo** poderá solicitar ao cliente informações específicas de sua infraestrutura de rede interna e equipamentos de segurança existente. Tais informações serão confidenciais e não poderão ser divulgadas pela **Telefônica|Vivo**.

- Estes prazos também são aplicados nos seguintes cenários:
- Solicitação de Upgrade/Dowgrade do produto.
- Solicitação de baixa (cancelamento) do produto.
- Solicitação de reconexão do produto.

6 ANEXOS

ANEXO 1 - TABELA DE PERFIL DE POLÍTICAS DE FIREWALL

Perfil 1 - Presença e Navegação

Descrição	IP de origem	Puerto origem	IP de destino	Puerto de Destino / Servicio	L3 Protocolo	Ação
DNS server	ANY (External interface)	High ports	ANY (Internal interface)	Dns (53)	tcp/udp	Permitir
Presença Web	ANY (External interface)	High ports	ANY (Internal interface)	http, https (80, 443)	tcp	Permitir
Correio eletrônico entrante SMTP	ANY (External interface)	High ports	ANY (internal interface)	smtp (25)	tcp	Permitir
Correio eletrônico entrante SMTP SSL	ANY (External interface)	High ports	ANY (internal interface)	smtp ssl (465,587)	tcp	Permitir
IMAP (Acesso a correio interno)	ANY (External interface)	High ports	ANY (Internal interface)	imap (143)	tcp	Permitir
IMAP over SSL (acesso a correio interno)	ANY (External interface)	High ports	ANY (Internal interface)	imaps (993)	tcp	Permitir
POP3 (Acesso a correio interno)	ANY (External interface)	High ports	ANY (internal interface)	pop3 (110)	tcp	Permitir
POP3 over SSL (acesso a correio interno)	ANY (External interface)	High ports	ANY (internal interface)	pop3s (995)	tcp	Permitir
ICMP (gestão rede)	ANY (External interface)	N/A	Range externa roteador cliente telefônica	N/A	Icmp	Permitir
DNS	ANY (Internal interface)	High ports	ANY (External interface)	dns (53)	tcp/udp	Permitir
Navegação Web	ANY (Internal interface)	High ports	ANY (External interface)	http, https (80, 8080, 443)	tcp	Permitir
IMAP (Acesso a correio externo)	ANY (Internal interface)	High ports	ANY (External interface)	imap (143)	tcp	Permitir
IMAP over SSL (Acesso correio externo)	ANY (Internal interface)	High ports	ANY (External interface)	imaps (993)	tcp	Permitir
POP3 (Acesso a correio externo)	ANY (Internal interface)	High ports	ANY (External interface)	pop3 (110)	tcp	Permitir
POP3 over SSL (Acesso a correio externo)	ANY (Internal interface)	High ports	ANY (External interface)	pop3s (995)	tcp	Permitir

Descrição	IP de origem	Puerto origem	IP de destino	Puerto de Destino / Servicio	L3 Protocolo	Ação
Correio electrónico saliente SMTP	ANY (Internal interface)	High ports	ANY (External interface)	smtp (25)	tcp	Permitir
Correio electrónico saliente SMTP SSL	ANY (Internal interface)	High ports	ANY (External interface)	smtp ssl (465,587)	tcp	Permitir
NTP (Network Time Protocol)	ANY (Internal interface)	High ports	ANY (External interface)	ntp (123)	tcp/udp	Permitir
ICMP (gestão rede)	ANY (Internal interface)	N/A	ANY (external interface)	N/A	Icmp	Permitir
Conectividade Social e Receita Net	ANY (Internal interface)	High ports	200.201.174.0/24, 200.201.173.68, 161.148.0.0/16, 189.9.71.0/24, 200.198.239.0/24	ANY	tcp	Permitir
FTP (Passive)[3]	ANY (Internal interface)	High ports	ANY (External interface)	ftp (20,21, PASV Port)	tcp	Permitir
O que não se permite explicitamente se proíbe	ANY	ANY	ANY	ANY	ANY	Proibir

Perfil 2 – Navegação

Descrição	IP de origem	Puerto origem	IP de destino	Puerto de Destino / Servicio	L3 Protocol	Ação
ICMP (gestão rede)	ANY (External interface)	N/A	Rango externo roteador cliente telefónica	N/A	Icmp	Permitir
DNS	ANY (Internal interface)	ANY	ANY (External interface)	dns (53)	tcp/udp	Permitir
Navegação Web	ANY (Internal interface)	ANY	ANY (External interface)	http, https (80, 8080, 443)	tcp	Permitir
IMAP (Acesso a correio externo)	ANY (Internal interface)	ANY	ANY (External interface)	imap (143)	tcp	Permitir
IMAP over SSL (Acesso correio externo)	ANY (Internal interface)	ANY	ANY (External interface)	imaps (993)	tcp	Permitir
POP3 (Acesso a correio externo)	ANY (Internal interface)	ANY	ANY (External interface)	pop3 (110)	tcp	Permitir

[3] Não se permitirá o modelo Active FTP onde o servidor estabelece uma conexão com o cliente na rede interna dele ate uma porta destino previamente acordada. Só estará permitido o modelo Passive FTP onde o cliente estabelece a conexão para transferência de dados ate uma porta destino previamente acordada. A solução monitora a comunicação com esta porta e permite dinamicamente esta conexão.

POP3 over SSL (Acesso a correio externo)	ANY (Internal interface)	ANY	ANY (External interface)	pop3s (995)	tcp	Permitir
Correio electrónico saliente SMTP	ANY (Internal interface)	ANY	ANY (External interface)	smtp (25)	tcp	Permitir
Correio electrónico saliente SMTP SSL	ANY (Internal interface)	ANY	ANY (External interface)	smtp ssl (465,587)	tcp	Permitir
NTP (Network Time Protocol)	ANY (Internal interface)	ANY	ANY (External interface)	ntp (123)	tcp/udp	Permitir
ICMP (gestão rede)	ANY (Internal interface)	N/A	ANY (external interface)	N/A	Icmp	Permitir
Conectividade Social e Receita Net	ANY (Internal interface)	High ports	200.201.174.0/24, 200.201.173.68, 161.148.0.0/16, 189.9.71.0/24, 200.198.239.0/24	ANY	tcp	Permitir
FTP (Passive) [4]	ANY (Internal interface)	ANY	ANY (External interface)	ftp (20,21, PASV Port)	tcp	Permitir
O que não se permite explicitamente se proíbe	ANY	ANY	ANY	ANY	ANY	Proibir

[4] Não se permitirá o modelo Active FTP onde o servidor estabelece uma conexão com o cliente na rede interna dele ate uma porta destino previamente acordada. Só estará permitido o modelo Passive FTP onde o cliente estabelece a conexão para transferência de dados ate uma porta destino previamente acordada. A solução monitora a comunicação com esta porta e permite dinamicamente esta conexão.

ANEXO 2 – FILTRO WEB

Modelo de Gestão

- Alerta: A solução não bloqueia o acesso ao site potencialmente perigoso apenas avisa ao cliente do risco existente e deixa a decisão com o usuário que esta navegando na Internet.
- Bloqueio: A solução bloqueia o acesso ao site potencialmente perigoso impedindo o acesso conforme especificado na política de filtro web escolhida pelo cliente.

Grupos de Filtro Web

Legenda:

- O acesso a esta categoria estará Permitido
- O acesso a esta categoria será Bloqueado
- ⚠ A solução avisará de potencial risco caso o usuário queira acessar a páginas web dentro desta categoria, o usuário decide o acesso ou não.

General Interest-Bussiness	**Interesse Geral - Negócios**	**Navegação Segura**	**Navegação Produtiva**	**RESTRITIVO**
Armed Forces	Forças Armadas	✓	✓	✓
Business	Negócio	✓	✓	✓
Finance and Banking	Finanças e Bancos	✓	✓	✓
General Organizations	Organizações gerais	✓	✓	✓
Government and Legal Organizations	Governo e organizações legais	✓	✓	✓
Information and Computer Security	Informatica e Segurança da informação	✓	✓	✓
Information Technology	Tecnologia Da Informação	✓	✓	✓
Search Engines and Portals	Sites de busca e portais	✓	✓	✓
Secure Websites	Sites seguros	✓	✓	✓
Web Hosting	Hospedagem Web	✓	✓	✓
Web-based Applications	Aplicações baseadas na Web	✓	✓	✓
Bandwidth Consuming	**Consumidores de largura de banda**	**Navegação Segura**	**Navegação Produtiva**	**RESTRITIVO**
File Sharing and Storage	Compartilhamento e armazenamento de arquivos	✓	✓	⊘⚠
Freeware and Software Downloads	Freeware e download de software	✓	✓	⊘⚠
Internet Radio and TV	Rádio Internet e TV	✓	✓	⊘⚠
Internet Telephony	Telefonia via Internet	✓	✓	⊘⚠
Peer-to-Peer File Sharing	Compartilhamento de arquivos(Peer-to-peer)	✓	✓	⊘⚠
Streaming Media and Downloads	Streaming Media and Download	✓	✓	⊘⚠
Security Risk	**Riscos de Segurança**	**Navegação Segura**	**Navegação Produtiva**	**RESTRITIVO**
Malicious Websites	Sites maliciosos	⊘	⊘	⊘
Phishing	Phishing	⊘	⊘	⊘
Spam URLs	URLs de spam	⊘	⊘	⊘

General Interest-Personal	**Interesse Geral - Pessoal**	**Navegação Segura**	**Navegação Produtiva**	**RESTRITIVO**
Advertising	Publicidade	✓	✓	✓

Arts and Culture	Arte e Cultura	✓	✓	✓
Brokerage and Trading	Sites de pregão na bolsa	✓	✓	✓
Child Education	Educação Infantil	✓	✓	✓
Content Servers	Servidores de Conteúdo	✓	✓	✓
Digital Postcards	Cartões postais digitais	✓	✓	✓
Domain Parking	Domain Parking	✓	✓	✓
Dynamic Content	Conteúdo Dinâmico	✓	✓	✓
Education	Educação	✓	✓	✓
Entertainment	Entretenimento	✓	✓	⊘⚠
Folklore	Folclore	✓	✓	✓
Games	Jogos	✓	⊘⚠	⊘⚠
Global Religion	Religião Global	✓	✓	✓
Health and Wellness	Saúde e Bem Estar	✓	✓	✓
Instant Messaging	Mensagens Instantâneas	✓	✓	✓
Job Search	Pesquisa de emprego	✓	✓	✓
Medicine	Medicina	✓	✓	✓
Meaningless Content	Conteúdo sem sentido	✓	✓	✓
News and Media	Notícias e Mídia	✓	✓	✓
Newsgroups and Message Boards	Grupos de notícias e Fórum	✓	✓	✓
Personal Privacy	Personal Privacy	✓	✓	✓
Personal Vehicles	Veículos pessoais	✓	✓	✓
Personal Websites and Blogs	Sites pessoais e blogs	✓	✓	✓
Political Organizations	Organizações políticas	✓	✓	✓
Real Estate	Imobiliária	✓	✓	✓
Reference	Referência	✓	✓	✓
Restaurant and Dining	Restaurante e Gastronomia	✓	✓	✓
Shopping and Auction	Compras e Leilão	✓	✓	✓
Social Networking	Redes Sociais	✓	✓	⊘⚠
Society and Lifestyles	Sociedade e Estilo de Vida	✓	✓	✓
Sports	Esportes	✓	✓	✓
Travel	Viagem	✓	✓	✓
Web Chat	Web Chat	✓	✓	⊘⚠
Web-based Email	Web-mail	✓	✓	⊘⚠

Adult/Mature Content	Adulto / Conteúdo Adulto	Navegação Segura	Navegação Produtiva	RESTRITIVO
Abortion	Aborto	✓	✓	✓
Adult Materials	Materiais Adulto	✓	⊘⚠	⊘⚠
Advocacy Groups	Organizações de advocacia	✓	✓	✓
Alcohol	Alcool	✓	✓	⊘⚠
Alternative Beliefs	Crenças alternativas	✓	✓	✓
Dating	Namoro	✓	⊘⚠	⊘⚠
Extremist Groups	Grupos extremistas	✓	✓	✓
Gambling	Jogos de azar	✓	✓	⊘⚠
Lingerie and Swimsuit	Roupas intimas e trajes de banho	✓	✓	✓
Marijuana	Maconha	✓	✓	✓
Nudity and Risque	Nudez	✓	✓	✓
Pornography	Pornografia	✓	✓	⊘⚠
Sex Education	Educação Sexual	✓	⊘⚠	⊘⚠
Sport Hunting and War Games	Esportes de caça e Jogos de Guerra	✓	✓	✓
Tobacco	Tabaco	✓	✓	✓
Weapons	Armas (Vendas)	✓	✓	⊘⚠
Potencially Liable	**Potencialmente punitivo**	**Navegação Segura**	**Navegação Produtiva**	**RESTRITIVO**
Child Abuse	Abuso Infantil	✓	⊘⚠	⊘⚠
Discrimination	Discriminação	✓	✓	⊘⚠
Drug Abuse	Abuso de Drogas	✓	⊘⚠	⊘⚠
Hacking	Hacking	⊘⚠	⊘⚠	⊘⚠
Illegal or Unethical	Ilegal ou antiético	✓	✓	⊘⚠
Plagiarism	Plágio	✓	✓	⊘⚠
Proxy Avoidance	Sites de proxy	⊘⚠	⊘⚠	⊘⚠
Violence	Violência explícita	✓	⊘⚠	⊘⚠