Termo Específico do Produto

Vivo Filtro Web (Web Security Gateway – WSG)

1. Descrição do serviço Vivo Filtro Web

1.1. Sobre o serviço

Atualmente, as formas com que os ataques são planejados e executados tem como base o cenário atual encontrado nas empresas, que utilizam firewalls, IPS/IDS's, Proxy, Antivírus, etc, para contenção. O que as organizações criminosas tem feito é, baseado nas deficiências ou dificuldades operacionais das soluções acima, adequar suas ações para escapar das formas atuais de bloqueio, seja através da fragmentação de arquivos, utilização de novas formas de ataques, como DNS Tunneling e utilizando portas que não são habitualmente monitoradas para tráfego web, de forma a conseguir um by-pass nas soluções atuais

O WEB SECURITY GATEWAY é uma ferramenta complementar às utilizadas atualmente pelas empresas, sendo posicionada como primeira linha de defesa, e por atuar na camada DNS, por onde praticamente todos os ataques iniciam sua execução, apresenta uma eficiência muito grande na contenção dessas novas ameaças que tentam burlar as ferramentas convencionais. Um outro fator muito importante que contribui para a eficiência do WEB SECURITY GATEWAY é a sua capacidade de identificar novas ameaças se formando, e isso só é possível a partir do suporte de sua rede de Inteligência de ameaças, que possui um vasto conhecimento dos acontecimentos na Internet devido ao grande fluxo de informações que passam pela nossa rede, por nossos equipamentos e que recebemos de parceiros que são analisados por experts em cybersecurity que desenvolvem modelos probabilísticos e engines capazes de identificar a formação de novos ataques e domínios maliciosos. Com todas as suas funcionalidades combinadas, recebe aproximadamente 16 bilhões de requisições DNS por dia, 200 bilhões de e-mails analisados e 19.7 bilhões de ataques bloqueados diariamente

1.2. BenefÍcios ao cliente

- Proteção em Nuvem para os usuários e as organizações onde quer que estejam de qualquer local, com qualquer dispositivo ou porta, com disponibilidade e escalabilidade incomparáveis.
- Bloqueio proativo contra novas ameaças através da análise de diversos conjuntos de dados em tempo real para entender os padrões de atividade de Internet. Então, podemos identificar a infraestrutura do invasor sendo posicionada para o próximo ataque.
- Políticas de Segurança que permite a definição em como os controles de segurança e acesso são aplicados às identidades. Através das políticas, você determina se o tráfego é inspecionado e bloqueado ou permitido.
- Mecanismo de proteção atualizado que ordena dinamicamente todo o conteúdo com base na reputação do domínio que o serve e na natureza desse mesmo conteúdo. Incorporando informações provenientes de uma rede de organizações colaboradoras,

a nossa capacidade de reconhecer e bloquear conteúdo malicioso é reforçada, proporcionando aos nossos usuários uma medida confiável do risco de qualquer página web que visitam. Essa medida de risco é posteriormente usada para decidir sobre o bloqueio ou alerta aos usuários, com base no grau de risco que toda a organização esteja disposta a aceitar.

- Uma maneira de transformar Despesas de Capital, CapEx, em Gastos Operacionais previsíveis por usuário OpEx, ao facilitar os exercícios de orçamento e de planejamento, e, ao mesmo tempo, proporcionam um serviço de segurança de alto nível e atualizado que protege de forma confiável os utilizadores finais e não requer nenhuma evolução da plataforma e respectivos custos associados.
- Uma grande disponibilidade de serviços de computação baseados em nuvem, com um impacto mínimo sobre sua infra-estrutura de suporte de TI e serviços, ao ser totalmente gerenciado, e não necessitar nenhum hardware ou implantação de software, filtrando o conteúdo do usuário de forma transparente.
- Latência de processamento mínima garantida por SLA.
- Interface centralizada que permite o estabelecimento e controle das políticas de segurança e uso através de relatórios minuciosos atualizados, com a possibilidade de abranger através do painel, desde uma visão geral das informações mais recentes a uma interface de pesquisa com acesso a todas as informações de registro armazenadas.

1.3. Arquitetura do Serviço

O serviço tem uma arquitetura simples, porém poderosa, representada na figura a seguir:

Arquitetura do Serviço

Os usuários conectam-se ao serviço usando os seus dispositivos padrão. O tráfego que sai dos dispositivos de acesso é canalizado, usando qualquer um dos vários mecanismos poderosos, flexíveis e simples, para os nossos nós baseados em computação em nuvem que usam o conhecimento da fonte, grupo de usuários, e tempo para aplicar as políticas configuradas de forma centralizada para esse tráfego. Os nós usam as suas conexões de internet da camada superior para obter as informações de

interesse da Internet. As informações são filtradas de acordo com a política estabelecida, garantindo que todo o tráfego recebido pelo usuário final foi limpo e cumpre com os requisitos da empresa.

1.4. Principais Características

O serviço é composto de diversos módulos de funcionalidades que, em conjunto, proporcionam o acesso web seguros para usuários e organizações.

1.4.1. Plataforma na nuvem

A Telefônica | Vivo, visando oferecer serviços de segurança web na nuvem, construiu, junto com seus parceiros de negócio, uma plataforma para atender os requerimentos de latência, presença global e relatórios integrados que soluções de segurança na nuvem demandam.

O Filtro Web - WSG possibilita ao usuário final, de qualquer lugar, uma experiência segura de acesso à internet, forçando o cumprimento das políticas de segurança da empresa, descartando a necessidade de aquisição de equipamentos com funcionalidade de web proxy, filtro de conteúdo e antivírus de GATEWAY para cada site que as organizações possuam.

Para utilizar o serviço, as organizações somente precisam definir sua política de acesso e de conformidade web e redirecionar o tráfego web que sai de suas redes para um dos nossos data centers que possuem a infraestrutura global do serviço. Conforme a política definida, o acesso internet é bloqueado, controlado ou permitido. Além disso, o serviço verifica o tráfego contra uma grande variedade de ameaças, entregando um tráfego limpo e seguro para o usuário final.

O Filtro Web - WSG é um serviço que não requer nenhum hardware no local cliente para atender a estes desafios. Através do redirecionamento do tráfego do cliente para um dos nós do serviço, é possível autenticar usuários finais para aplicar políticas a usuários ou grupos em qualquer aparelho e em qualquer lugar em que esteja o usuário, possibilitando inspeção completa de tráfego http e https, para obter uma experiencia completa de integração com Active Directory e LPAD e visibilidade dos seus respectivos acessos é necessário a instalação de duas (2) Maquinas Virtuais (VMs).

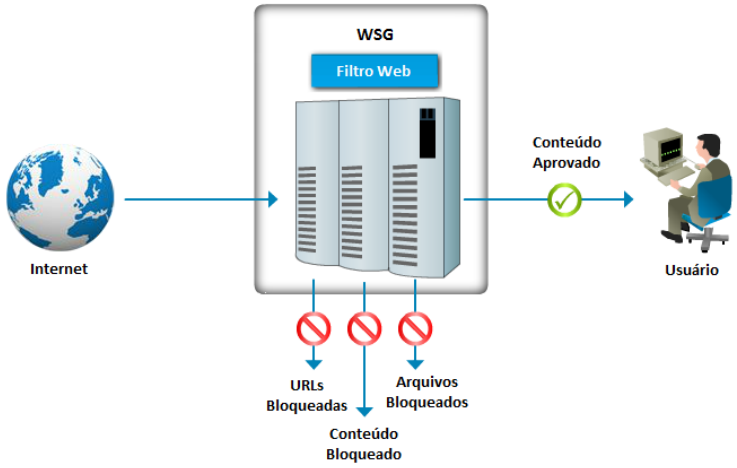
1.4.2. Filtro de conteúdo web

Este módulo permite a gestão da navegação internet dos usuários, garantindo a segurança através de detecção e bloqueio de acesso a páginas potencialmente perigosas e possibilitando a melhora da produtividade dos usuários com do controle de horário de navegação, através das seguintes funcionalidades:

- Granularidade: permite a criação de políticas de acesso por usuário, grupos de usuários e horário de navegação. Suporte integração com bases de usuários Active Directory que complementa os dispositivos virtuais (VAs) e os clientes móveis, fornecendo informações de nome de usuário, grupo ou computador do AD para cada solicitação de DNS aplicável.
- Filtros por categorias: visando oferecer uma maior flexibilidade na configuração de regras de acesso, o serviço disponibiliza até 60 categorias de páginas, permitindo a personalização das políticas de acesso de acordo com o conteúdo dos sites. Se um determinado site ainda não foi categorizado, o serviço realiza a categorização dinâmica do mesmo em tempo real;
- Notificação do usuário: o serviço envia ao usuário uma página sempre que o acesso a um determinado site é restrito (caution notification), não permitido ou está infectado (notification message). Se necessário, é possível customizar tais paginas de notificação conforme necessidades do cliente.

1.4.3. Políticas de Aplicações Web

Com o avanço da Web 2.0, uma nova geração de ferramentas de segurança que fosse muito além do tradicional filtro de conteúdo se fez necessária. Visando mitigar as ameaças provenientes deste novo modelo de navegação, o Filtro Web - WSG provê controles para o uso de redes sociais, webmail, mensagens instantâneas e streaming, possibilitando controles para estes acessos.



Metodologia de WEB SECURITY GATEWAY

- Mensagens instantâneas: controla o uso de ferramentas de mensagens instantâneas e a troca de arquivos;
- Webmail: gerencia o acesso a plataformas de webmail;
- Conteúdo multimídia: gerencia o acesso a conteúdo multimídia (como Youtube, radio streaming, etc);
- Redes sociais e blogs: gerencia o acesso aos mais famosos sites de redes sociais e blogs.

1.4.4. 3.4.4Proteção para malware, phishing, Ransomware, and C2 callbacks

Utilizando a abordagem de detecção baseada em assinaturas, com uma base de dados atualizada constantemente, o Filtro Web - WSG verifica o tráfego em tempo real e o conteúdo de arquivos, mesmo que estejam comprimidos.

Visando aprimorar a experiência dos usuários que navegam na internet, os websites atuais não mais disponibilizam somente texto puro entre tags HTML, mas sim conteúdos sofisticados desenvolvidos com tecnologias Java, Flash, ActiveX, entre outros.

Usuários maliciosos frequentemente utilizam estas tecnologias para criar aplicações web com o objetivo de cometer as mais diversas variedades de crimes digitais. Entretanto, estas aplicações nem sempre ficam hospedadas nos sites destes usuários maliciosos. Cada vez mais tais usuários invadem site legítimos e instalam suas aplicações maliciosas, tornando a detecção deste tipo aplicação praticamente impossível para o usuário comum.

Visando proteger os usuários destas ameaças, o módulo proteção avançada está preparado para identificar uma grande variedade de aplicações e scripts maliciosos contidos nos websites, impedindo que o usuário faça o download destes conteúdos para suas estações de trabalho.

Este módulo possibilita proteção contra os mais diversos tipos de ataques como segue abaixo:

Malware: Sites e outros servidores que hospedam software malicioso, software, drive-by downloads/exploits, ameaças móveis e muito mais.

Ransomware: Tipo de ataque baseado em um software ou arquivo malicioso que, ao invadir o servidor, restringe o acesso ao sistema/arquivo infectado e cobra um resgate para que o acesso possa ser restabelecido. Caso não ocorra o pagamento do resgate, que geralmente é feito em criptomoedas, os arquivos podem ser perdidos e até mesmo publicados.

Domínios recém-vistos: Domínios que se tornaram ativos muito recentemente. Estes são frequentemente usados em novos ataques.

Command and Control Callbacks: Impedir que dispositivos comprometidos se comuniquem com a infraestrutura dos invasores.

Phishing Attacks: Sites fraudulentos que visam induzir os usuários a entregar informações pessoais ou financeiras.

DNS Dinâmico: Bloqueie sites que hospedam conteúdo DNS dinâmico.

Domínios potencialmente prejudiciais: Domínios que exibem comportamento suspeito e podem fazer parte de um ataque.

DNS Tunneling VPN: Serviços de VPN que permitem aos usuários disfarçar seu tráfego, encapsulando-o através do protocolo DNS. Eles podem ser usados para ignorar políticas corporativas relacionadas a acesso e transferência de dados.

Cryptomining: O Cryptomining permite que as organizações controlem o acesso do cryptominer a pools de mineração e mineradores da Web.

1.4.5. Mobile Security para IOS

O Security Connector fornece visibilidade e controle para dispositivos Apple iOS móveis de propriedade da organização e gerenciados por MDM, como iPhones e iPads. Direciona o tráfego DNS, incluindo a funcionalidade do proxy inteligente, para a nuvem, onde ocorre a filtragem contra sites maliciosos, como sites de phishing ou sites que filtram informações.

1.4.6. Mobile Security para Android

O Module de Conexão para Android OS é um cliente de roaming para dispositivos Android gerenciados que oferecem proteção contra ameaças da Internet na camada DNS. O módulo adiciona proteção de nível DNS ao perfil de trabalho do Android. Essa proteção se estende aos aplicativos e à navegação coberta pelo perfil de trabalho.

É necessário um sistema de gerenciamento centralizado de dispositivo móvel (MDM) para implantar esse cliente e enviar a configuração do Filtro Web - WSG para os dispositivos IOS e Android.

1.4.7. Lista de MDM homologados.

- Cisco Meraki
- Apple
- IBM Maas360
- Microsoft Intune
- JAMF
- MobiConnect
- MobileIron
- Workspace One
- Android (e.g., Samsung, Google Pixel) mobile devices with Android OS version 6.0.1 and above.

1.4.8. Administração

1.4.8.1. Gerência de Logs

O registro das atividades de suas identidades é definido por políticas quando você cria uma. Por padrão, o log está ativado e definido para registrar todas as solicitações que uma identidade faz para alcançar destinos. A qualquer momento após a criação de uma política, você pode alterar o nível de atividade de identidade que o Filtro Web - WSG registra.

1.4.8.2. Gerência de Domínios

O Gerenciamento de Domínio é usado para listar domínios e IPs que não devem ser enviados diretamente a ferramenta. Esses domínios usarão seus resolvedores locais ao em vez dos resolvedores do Filtro Web - WSG. A lista de domínios não pode exceder 5000 entradas. Os domínios podem ser aplicados a todos os sites, todos os dispositivos ou ambos. Por exemplo, você pode aplicar domínios a sites e não a dispositivos (ou vice-versa), para que apenas o tráfego dos sites use seus resolvedores locais.

1.4.8.3. Gerência de Proxy Inteligente

Quando ativado, o proxy inteligente do Filtro Web - WSG intercepta e solicita proxies para arquivos maliciosos incorporados em determinados domínios chamados "cinza". Você ativa e desativa o proxy inteligente ao criar uma política pela primeira vez e, uma vez configurado, na página Resumo da política.

1.4.8.4. Inspeção SSL

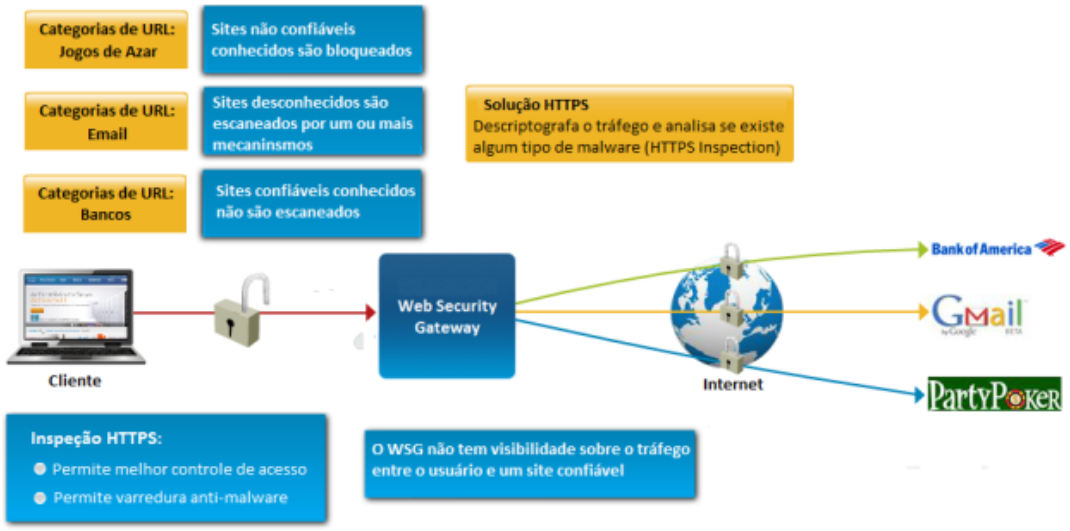
O SSL (Secure Socket Layer) é um conhecido protocolo utilizado para criptografar e proteger dados que trafegam pela internet. Quando um usuário estabelece uma conexão http com um web site através de um navegador, ocorre uma negociação para determinar se os dados trocados serão criptografados ou não. Uma vez que se decide que a criptografia será utilizada, o protocolo SSL é utilizado e conexão passa a ser https (o "s" significa "seguro").

O SSL é geralmente utilizado em sites financeiros (bancos e cartões de créditos), comercias (lojas virtuais) e outros sites que necessitam trocar informações pessoais legalmente protegidas, assim como é utilizado para proteger logins e senhas dos usuários contra interceptação não autorizada em webmails, redes sociais, etc.

Apesar deste uso benéfico do SSL, ele também pode ser usado por usuários maliciosos em alguns cenários, sempre visando prejudicar o usuário final.

- Esconder conteúdos perigosos como vírus, spyware e outros malwares;
- Usuários mal-intencionados podem inserir conteúdos maliciosos em sites SSL conhecidos e confiáveis;
- Pode-se utilizar o SSL para enviar informações para fora da organização (vazamento), já que este protocolo não é comumente inspecionado;

O Filtro Web - WSG possui a capacidade de interceptar conexões SSL com fim de evitar que o protocolo seja utilizado indevidamente. Com esta funcionalidade o tráfego é descriptografado quando chega na infraestrutura dos serviços e todas as políticas de segurança são aplicadas, assim como ocorre para conexões http. Uma vez que o tráfego é verificado e limpo, o mesmo é criptografado novamente e enviado para seu destino. O serviço também possibilita que para determinadas categorias ou lista de sites, como de internet banking, não sejam descriptografados pelo serviço, evitando que informações confidenciais dos usuários que são protegidas por lei sejam analisadas.



Inspeção HTTPS

Como o uso do SSL envolve certificados digitais, é necessário importar para todos navegadores dos usuários o certificado do serviço FILTRO WEB - WSG, visando evitar que os navegadores enviem para o usuário uma mensagem de que o certificado que está sendo usado não é confiável.

1.4.8.5. Virtual Appliance

Os appliances virtuais são máquinas virtuais leves, compatíveis com os hipervisores VMWare ESX / ESXi, Windows Hyper-V e KVM e as plataformas em nuvem Microsoft Azure, Google Cloud Platform e Amazon Web Services.

Quando utilizados como encaminhadores DNS condicionais na sua rede, os VAs do Filtro Web - WSG registram as informações internas do endereço IP das solicitações DNS para uso em relatórios, aplicação de segurança e políticas de filtragem de categoria. Além disso, os VAs criptografam e autenticam dados DNS para aumentar a segurança.

Os VAs também permitem a integração do Active Directory (AD), que expande a funcionalidade para incluir informações de identificação do AD, além de visibilidade interna do endereço IP e criptografia de DNS.

1.4.9. Portal de relatórios

Este módulo é responsável por gerar relatórios gráficos de cada uma das funcionalidades do serviço Filtro Web - WSG, como relatórios de urls/categorias mais acessadas e bloqueadas, utilização de webmail, relatórios sobre vazamento de informações, vírus bloqueados, entre outros. Trata-se de uma poderosa ferramenta que proporciona uma profunda visibilidade do tráfego web da organização.

Os relatórios podem-se aplicar filtros como intervalos de data, direção do tráfego, localização, departamento, entre outros. Pode-se também exportá-los em formato PDF.

Gerenciado por meio de um portal baseado na Web intuitivo que permite aos clientes facilmente editar e ver os resultados em um ambiente familiar diretamente, proporcionando-lhes uma melhor visibilidade em seus negócios. Não será mais uma informação crítica comercial ambígua, o portal de relatórios vai mudar fundamentalmente a maneira como as decisões são tomadas em organizações de todos os tamanhos e levará a um melhor alinhamento, transparência, desempenho e, mais importante, informações para tomada de decisão.

1.4.9.1. Agendar relatórios

Vários relatórios no Filtro Web - WSG podem ser configurados para que o mesmo envie por e-mail regularmente um resumo desse relatório. E você configura filtros para que eles contenham apenas as informações que você deseja. Cada relatório enviado por email inclui uma versão HTML, um arquivo CSV anexado contendo todo o conjunto de dados e um link para a FILTRO WEB - WSG e o relatório.

1.5. Sobre o Parceiro Tecnológico – Cisco Umbrella

As formas com que os ataques são planejados e executados tem como base o cenário atual encontrado nas empresas, que utilizam firewalls, IPS/IDS's, Proxy, Antivírus, etc, para contenção. O que

as organizações criminosas tem feito é, baseado nas deficiências ou dificuldades operacionais das soluções acima, adequar suas ações para escapar das formas atuais de bloqueio, seja através da fragmentação de arquivos, utilização de novas formas de ataques, como DNS Tunneling e utilizando portas que não são habitualmente monitoradas para tráfego web, de forma a conseguir um by-pass nas soluções atuais

O Cisco Umbrella, é uma ferramenta complementar às utilizadas atualmente pelas empresas, sendo posicionada como primeira linha de defesa, e por atuar na camada DNS, por onde praticamente todos os ataques iniciam sua execução, apresenta uma eficiência muito grande na contenção dessas novas ameaças que tentam burlar as ferramentas convencionais. Um outro fator muito importante que contribui para a eficiência do Umbrella é a sua capacidade de identificar novas ameaças se formando, e isso só é possível a partir do suporte de sua rede de Inteligencia de ameaças, o Cisco Talos. Cisco Talos é a maior organização não governamental de segurança, com vasto conhecimento do que acontece na Internet devido ao grande fluxo de informações que passam pela nossa rede, por nossos equipamentos, que recebemos de parceiros, e são analisados por experts em cybersecurity que desenvolvem modelos probabilísticos e engines capazes de identificar a formação de novos ataques e domínios maliciosos. Com todas as suas funcionalidades combinadas, Cisco Talos recebe aproximadamente 16 bilhões de requisições DNS por dia, 200 bilhões de e-mails analisados e 19.7 bilhões de ataques bloqueados diariamente...

Cisco e Vivo tem atualmente uma forte relação de parceria, que reflete em investimentos de ambas as partes na capacitação, lançamento de produtos e ações de go to Market conjunta para aceleração de vendas dessas soluções. A forte presença da Cisco no mercado local e sua marca reconhecida faz com que seja o parceiro ideal para o lançamento de ofertas em conjunto

2. Modalidades do Serviço

2.1. Autogestão

O serviço esta disponível na modalidade Autogestão, do ponto de vista de gestão do serviço, o Autogestão é aquele no qual o **cliente será responsável pela gestão e configuração de suas regras de acesso e integração com o diretório ativo**.

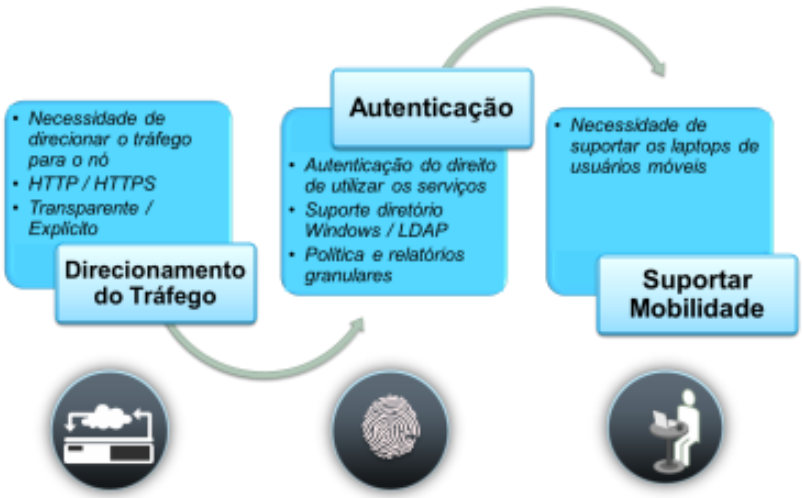
Nesta modalidade, o cliente é responsável pela gestão de configuração e mudanças de suas regras de acesso utilizando equipe própria, através do Portal de Administração do serviço. A equipe técnica do cliente é responsável pelo dia-a-dia e tratamento de incidentes, apoiando-se na Telefônica | Vivo para sanar dúvidas. O SOC suporta o cliente somente em incidentes relacionados à plataforma do serviço.

Planos e características	Básico	Avançado
Performance		
100% cloud — nenhum hardware para instalar ou software para manter	✔	✔

100% uptime — resolve solicitações de mais de 80 bilhões diariamente, sem latência adicional	✔	✔
Mais de 7 milhões de destinos maliciosos aplicados simultaneamente em 25 data centers	✔	✔
Proteção		
Camada adicional de segurança preditiva para qualquer dispositivo, em qualquer lugar	✔	✔
Proteção para malware, phishing, and C2 callbacks em qualquer porta de acesso	✔	✔
Aplicação de políticas de uso aceitável usando 60 categorias de conteúdo	✔	✔
Execução		
Bloqueio de solicitações de domínio malicioso e respostas de IP na camada DNS	✔	✔
Bloqueio de caminhos de URL maliciosos e conexões IP diretas na camada IP		✔
Domínios com Proxy Risky para inspeção de URL e arquivo usando mecanismos AV e Advanced Malware Protection (AMP)		✔
Visibilidade		
Pesquisa das atividades de toda a empresa em tempo real e relatórios programados	✔	✔
Identifique ataques direcionados comparando atividade local x global		✔
Identifique os riscos de uso de nuvem e IoT relatando mais de 1800 serviços		✔
Gestão		
Listas personalizadas de bloqueio/permissão, páginas de bloqueio internas e opções de desvio	✔	✔
Aplicação e visibilidade por rede interna ou usuário/grupo do AD		✔
Mantenha os logs para sempre integrando-se ao seu bucket do Amazon S3		✔

3. REQUISITOS DO SERVIÇO

Para que o serviço seja ativado, dois requisitos básicos devem ser definidos: modelo de redirecionamento de tráfego para a nuvem e identificação do usuário. A correta identificação destes requisitos é essencial para o correto funcionamento do serviço.



Requisitos do Serviço

3.1. Identificação do usuário

Uma solução de segurança não é completa se a mesma não possibilitar identificação do usuário através do modelo AAA (authentication, authorization e accouting). Sem o modelo AAA, não é possível associar um usuário a uma transação específica, e desta forma os relatórios não irão apresentar informações de nome de usuários ou grupos.

Dentro do perímetro de rede da organização, prover serviços de AAA é relativamente simples, pois as credenciais do usuário permanecem dentro dos limites da organização. Na outra ponta, para os serviços na nuvem, talvez a autenticação seja o maior problema a ser endereçado, devido à questão de que as credenciais dos usuários também precisam existir fora dos limites da organização. Assim, os serviços na nuvem precisam possuir um método para sincronizar as informações dos usuários que somente existem na infraestrutura AAA local da organização. Esta questão é uma das maiores preocupações e dúvidas das equipes de TI e segurança das organizações, pois a sincronização dos usuários com serviços na nuvem só pode ocorrer de duas maneiras: permitir que o provedor do serviço acesse a base local de usuários ou a enviar literalmente para o provedor.

Uma vez que a base de usuários está sincronizada, o provedor de serviços poderá autenticar cada sessão do usuário, verificar se o mesmo possui autorização para aquele tipo de acesso e registrar o acesso, visando situações de auditoria ou análise forense. Sem o modelo AAA, não é possível disponibilizar estes serviços para as organizações.

3.2. Método de Autenticação de Usuários

O método de autenticação pode ser feito de duas maneiras para se obter a granularidade dos acessos, autenticação via AD/ LDAP ou através de um agente instalado “Roaming Client”

Quando feita a autenticação através da integração com AD/LDPA, o controlador de domínio e acessos do cliente (e.g. Microsoft AD) é integrado com o serviço, através da internet. Será necessário que o cliente possua os Hipervisores, VMWARE /ESXI , HYPER-V, ou as plataformas em nuvem Microsoft

Azure, Google Cloud Platform e Amazon Web Services. Necessário duas maquinas virtuais na infraestrutura, para orquestramento entre o DNS internos e externos

Quando não há integração com o AD (active Directory), será necessário instalar os agentes (Roaming Client) em todas as estações de trabalho, para obter a granularidade com o dispositivo.

3.3. Conector de Autenticação

Componente fundamental do serviço implantação do Filtro Web - WSG. Instalado em um controlador de domínio do Active Directory ou servidor membro, é um agente de autenticação que executa o seguinte.

- Encaminha o usuário e grupo informações para o Filtro Web - WSG para permitir que política personalizada com base em grupo e / ou nomes de usuário antes de começar a gerar tráfego; sem ele, você deve esperar até que os usuários / grupos de gerar tráfego e, em seguida, reativamente criar uma política.
- Monitora o login e atividade de logout de usuários do domínio para construir uma matriz de IP e nome de usuário.
- Relatório de atividades de login e logout de usuários para manter a matriz de IP e nome de usuário atualizado; ou mantém esta matriz em si no controlador de domínio e empurra a matriz atualizada regularmente para a nuvem.

3.4. Redirecionamento de tráfego

Por trata-se de um serviço na nuvem, prestado através da internet, deve-se redirecionar o tráfego web do cliente para a infraestrutura do serviço. O Filtro Web - WSG não requer nenhum hardware adicional na rede do cliente, o direcionamento do tráfego é feito através de Consultas DNS (plataforma do WSG) que é realizado pelo apontamento nos servidores DNS internos e dispositivos Gateways de rede Layer 3 para os servidores DNS externos da plataforma do Filtro Web - WSG.

4. Condições Gerais

A presente documentação é propriedade da Telefônica | Vivo. Tem caráter confidencial e não poderá ser objeto de reprodução total ou parcial, tratamento por meios de informática nem transmissão por qualquer meio, seja eletrônico, mecânico, por fotocópia, gravação ou qualquer outro.

Também não poderá ser objeto de empréstimo, locação ou qualquer forma de cessão de uso sem a permissão prévia e escrita da Telefônica, titular do copyright. O não cumprimento das limitações determinadas acima por qualquer pessoa que tenha acesso à documentação será punido conforme a lei.

4.1. Condições de prestação do serviço

4.1.1. Abertura de Chamados

As solicitações sobre o serviço deverão ser efetuadas a Central de Relacionamento da Telefônica | Vivo pelo telefone 0800 151551. O atendimento é realizado 24 horas por dia, 7 dias por semana, 365 dias por ano.

O cliente poderá designar até 03 (três) administradores de sua empresa, unidade de negócio ou filial para contato com a Central de Relacionamento, os nomes deverão ser informados durante o processo de implantação do Serviço. A Central de Relacionamento da Telefônica não efetua atendimento ao usuário final.

O SOC efetuará o acompanhamento das solicitações e das soluções dadas ao cliente. A cada solicitação será associado um número de registro da chamada e quando for o caso, um nível de severidade, conforme o grau crítico do problema avaliado.

No caso de necessidade de interação com o cliente para a resolução de algum problema do serviço, a equipe de suporte do SOC entrará em contato com um dos três administradores designados pelo cliente, que serão os pontos focais.

4.1.2. Fechamento de Chamado

O chamado somente será concluído com o "de acordo" dado por um dos três administradores designados, anteriormente, pelo cliente, sendo o contato efetuado por telefone ou e-mail.

4.1.3. Quantidade de Usuários Aferidos

A quantidade de usuários é definida pelo número total de usuários que acessam a internet, não realizamos propostas para acessos simultâneos (número de máquinas).

Caso o cliente não realizará a autenticação de seus usuários, a proposta deverá ser feita com base no número total de usuários.

Em ambos os casos, autenticados ou não dos usuários, a quantidade de usuários está sujeita ao pico de banda larga por usuário do cliente, não deve superior a uma média de 15 Kbs em qualquer mês do ano e com margem de 5% no mês aferido.

4.2. Compromisso de Qualidade de Serviço

São definidos os parâmetros de qualidade do serviço, envolvendo disponibilidade e retardo.

4.2.1. Disponibilidade do serviço em nuvem

4.2.1.1. Disponibilidade

A disponibilidade do serviço é distinguida entre **Serviço In-line** e **Serviço Não In-line**. O Serviço In-line é definido como o processamento ou a execução de dados em trânsito destinados e oriundos do usuário final para a Internet. O Serviço Não In-line é qualquer serviço que não processa nem executa dados em trânsito destinados e oriundos do usuário final para a Internet (tais como as ferramentas de emissão de relatórios usadas pelo administrador). O Serviço In-line geralmente estará disponível 99,999% do tempo. O Serviço Não In-line estará disponível 99,5% do tempo. A disponibilidade é calculada por mês-calendário da seguinte maneira:

$$\frac{\boldsymbol{Total - Paradas\ não\ programdas - Paradas\ programadas}}{\boldsymbol{Total - Paradas\ programadas}} \times \mathbf{100} \geq (\boldsymbol{meta\ da\ disponibilidae})$$

- Indisponibilidade de serviço não será avaliada em função de: (i) uma falha do Cliente para configurar corretamente o serviço de acordo com a documentação de serviço

aplicável ou adesão ao CONTRATO; (ii) a indisponibilidade de uma página web específica ou de um aplicativo em nuvem de terceiro(s); (iii) indisponibilidade de um um data center individual; ou (iv) indisponibilidade de um ou mais específicas características, funções, ou equipamento de hospedagem locais dentro do serviço, enquanto outras características fundamentais permanecem disponíveis.

- "Total" significa o número de minutos para o mês calendário.
- “Paradas não programadas” significada indisponibilidade não planejada do serviço.
- “Paradas programadas” inclui:
  - Tempo de parada planejado. Com relação ao tempo de parada planejado, a CONTRATADA avisará o Cliente com a máxima antecedência possível, conforme as circunstâncias permitirem, e buscará fazê-lo com no mínimo 72 horas ou mais de antecedência. A CONTRATADA aplicará os esforços comercialmente cabíveis para agendar o tempo de parada planejado fora dos horários de pico (horário do datacenter local). O cliente reconhece que a CONTRATADA poderá, em determinadas situações, realizar manutenções de emergência (tempo de parada não planejado) com menos de 24 horas de prévio aviso.
  - Qualquer indisponibilidade causada por circunstâncias que fujam do controle cabível da CONTRATADA, incluindo, porém sem se limitar a casos fortuitos, atos do governo, enchentes, incêndios, terremotos, agitações civis, atos terroristas, greves ou outros problemas trabalhistas (excluindo aqueles envolvendo os funcionários da CONTRATADA), defeitos ou atrasos envolvendo hardware, software, invasões de rede ou ataques de negação de serviço que não se encontram sob a posse ou o controle cabível da CONTRATADA.

4.2.2. Latência média específica para os serviços

4.2.2.1. Serviços de Segurança na Web

A latência média no caso de operações que passem pelo VIVO WEB SECURITY GATEWAY baseia-se no tempo de processamento atribuído à infraestrutura em nuvem. A latência média para os Serviços de Segurança na Web é definida como o tempo médio que o serviço leva para verificar, processar e aplicar a política do Cliente aos dados do conteúdo da Web, considerando uma página da Web de 1MB, não incluindo o tempo consumido pelas comunicações fora do datacenter do serviço. A Latência Média é de 100 milissegundos ou menos, sendo determinada pela média mensal das amostras coletadas pela CONTRATADA em um determinado mês.

4.2.2.2. Análise de Malware

Não está sujeita ao cálculo da latência média

4.2.2.3. Atendimento

Trata-se do tempo de espera para atendimento através da Central de Relacionamento.

Tipo	Descrição	Objetivo	SLA

Atendimento	Tempo máximo de espera para atendimento	10 segundos	80%

4.2.2.4. Suporte

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

Severidade	Descrição	Objetivo	SLA
Crítico	Evento que impede a realização de funções críticas frequentemente ou por um período prolongado.	2 horas	95%
Alto	Evento permanente que impede a realização de funções não-críticas.	4 horas	95%
Médio	Evento ocasional que impede a realização de funções não-críticas.	24 horas	95%
Baixo	Evento que impacta operações administrativas, não-críticas ou funções secundárias.	36 horas	95%
Solicitações	O serviço não está afetado. Dúvidas sobre algum aspecto técnico ou característica do serviço.	48 horas	95%

4.2.3. Penalidade

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.

Vpd	Desconto %
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

4.3. Gestão Operacional Do Contrato

A prestação dos serviços pela Telefônica | Vivo e o cumprimento do contrato a ser firmado, deverá ser fiscalizado, monitorados e geridos pelas partes para fins de contínua avaliação e melhoria dos serviços prestados.

A gestão operacional do futuro contrato será feita através da gerência técnico-operacional da Telefônica | Vivo, que deverá zelar pelo bom desenvolvimento de todos os projetos e processos ligados aos serviços prestados ao Cliente, mantendo um canal de alto nível para comunicação entre as empresas.

4.4. Prestadoras de Serviço contratadas pela Telefônica| VIVO

A Telefônica | Vivo poderá contratar terceiros para a prestação dos serviços, sendo que, neste caso, ela será a única e diretamente responsável perante ao Cliente por todos os serviços prestados por terceiros.

4.5. Responsabilidades do Cliente

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

- Informar a Telefônica | 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 Telefônica | 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.
- Informar internamente e aos seus outros prestadores de serviços, o escopo de contrato com a Telefônica | Vivo, quando relacionado a suas atividades.
- Não gerenciar diretamente nenhum funcionário ou terceiros da CONTRATADA alocados ou em atendimento nos sites da CONTRATANTE.
- A CONTRATADA é responsável pela gestão e configuração de suas regras de acesso e integração os equipamentos internos de sua empresa, como diretório ativo.

4.6. Responsabilidades Da Telefônica | Vivo

- Designar um profissional que será ponto focal para o projeto;
- Tornar disponíveis recursos Telefônica | 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 Telefônica | Vivo e conforme estabelecido no contrato com a CONTRATANTE;

- Cumprir os prazos estabelecidos nas atividades do projeto, desde que as responsabilidades da CONTRATANTE, 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 da CONTRATANTE, sobre ações e resultados nas diferentes atividades.
- Garantir a confidencialidade dos dados informados pela CONTRATANTE, para o desenvolvimento da atividade.
- O pessoal da Telefônica | Vivo que tiver acesso aos escritórios da CONTRATANTE, estará sujeito às normas de segurança que a CONTRATANTE, estabelecer para acesso e permanência em suas instalações.
- Comunicará e solicitará à CONTRATANTE, a aprovação explícita de qualquer mudança da equipe de trabalho, com uma antecipação mínima de sete (7) dias corridos.

4.7. Prazo de Implantação

- A CONTRATADA irá se reunir com a equipe técnica da CONTRATANTE, no prazo máximo de 15 dias corridos 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 da CONTRATANTE.
- - Como produto desta reunião, a CONTRATADA deverá disponibilizar os serviços na nuvem, credenciais de acesso e manuais, em até 7 dias corridos após a conclusão das definições técnicas e do cronograma de implantação;
- - A CONTRATANTE fará a implementação das configurações necessárias nos equipamentos de sua propriedade em até 20 dias corridos após a disponibilização do serviço;
- - A CONTRATADA prestará suporte técnico durante a fase de implantação intrínseca a esta atividade.