SONDA®
make it easy

DESCRITIVO FIREWALL

ÍNDICE

SONDA S.A. Copyright (c) 2025| Sua reprodução é proibida e qualquer cópia impressa deste documento é considerada não controlada. [NC-40]

1. Versão do Produto

Versão	Escopo	Data de Atualização
Versão 01	Criação do documento	-

2. Descrição Resumida

Os serviços de Firewall virtual dedicado oferecem aos **CLIENTES** da **SONDA** combinar as soluções de ponta do mercado, altamente reconhecidas, agregadas aos serviços profissionais **SONDA** especializados em segurança perimetral, para o controle aprimorado de segurança no acesso às suas aplicações e camada de rede.

Nesta oferta, o serviço é entregue através da solução de Firewall do Data Center **SONDA** e possui alta disponibilidade e redundância ao utilizar o modelo de implementação em cluster ATIVO/PASSIVO.

3. Objetivo

O serviço tem como objetivos:

- Disponibilizar firewall dedicado à necessidade de negócio;
- Satisfazer os requisitos de negócios do **CLIENTE** através de serviços disponíveis, confiáveis e seguros;
- Manter conformidade com os padrões do mercado;
- Cumprir com os níveis de serviços estabelecidos através dos SLAs;
- Agilizar o processo de criação de firewall e suas regras;
- Gestão de Governança baseadas nas melhores práticas e certificações.

4. Benefícios

A **SONDA** entende que com essa oferta é entregue aos **CLIENTES** os seguintes benefícios:

- O produto Firewall **SONDA** Virtual dedicado é ofertado aos **CLIENTES** por bundles de capacidade, desta forma os **CLIENTES** não têm a necessidade de aquisição de hardwares e licenças com alto valor de investimento;
- Acesso a um pool de profissionais especializados em firewall, assim se concentrando nos requisitos de negócio;
- Suporte 24x7x365;

5. Escopo de Atuação

Os Firewalls de Nova Geração (NGFW) ofertados pela **SONDA** oferecem abordagens abrangentes de segurança, que incorporam diversos módulos de proteção o para oferecer uma defesa robusta contra ameaças na rede.

Abaixo destacamos os principais módulos de segurança inclusos na oferta **SONDA** de NGFW.

1. **Detecção e Prevenção de Intrusões (IPS):**

Serviço de Detecção e Prevenção à Intrusão de Sistemas – IPS, composto por:

- Implementação e consultoria para desenho de arquitetura, testes, implantação de equipamentos, software e suporte técnico;
- Gerenciamento, operação e manutenção, contemplando monitoramento e análise de dados, configuração e atualização de sensores.

SONDA S.A. Copyright (c) 2025| Sua reprodução é proibida e qualquer cópia impressa deste documento é considerada não controlada. [NC-40]

O Data Center da **SONDA** adota procedimentos baseados nas melhores práticas de framework de segurança da Informação como NIST (*National Institute os Standard and Technology*) e CIS (*Center for Internet Security*) com o intuito de prover:

- Proteção preventiva contra ameaças de segurança conhecidas e emergentes;
- Minimização do risco e maior conformidade com normas e regulamentação;
- Níveis de serviço garantidos desenvolvidos para garantir a continuidade do negócio do **CLIENTE**;
- Suporte técnico 24x7 através de Equipe de Segurança Operacional, em caso de falhas ou acionamento.
- Geração e envio dos relatórios abaixo:

Ativo	Descrição do Serviço	Relatório	Periodicidade
IPS	Report do serviço	Top destinos Servidores TI	Mensal
		Top origens Servidores TI	Mensal
		Top aplicações Servidores TI	Mensal
		Top ameaças Servidores TI	Mensal

2. Firewall de Aplicação (WAF):

O módulo **WAF** oferece uma inspeção mais profunda do tráfego de aplicativos, permitindo uma visibilidade aprimorada e controle sobre as atividades específicas dos aplicativos.

3. Antivírus:

O módulo de **Antivírus** do **NGFW** verifica o tráfego em busca de malware conhecido, utilizando assinaturas de vírus atualizadas regularmente. Além disso, pode empregar análise heurística para detectar ameaças desconhecidas com base em comportamentos maliciosos.

Ele usa mecanismos de detecção avançados patenteados e comprovados para impedir que malwares conhecidos e polimórficos se estabeleçam em sua rede.

4. Filtragem de URL (Web Filtering):

O módulo **Web Filtering** oferece proteção contra ameaças, incluindo ransomware, roubo de credenciais, phishing, spam e outros ataques transmitidos pela Web. Ele usa análise de comportamento orientada por Inteligência Artificial (IA), Aprendizado de Máquina (ML) e correlação de eventos para bloquear URLs mal-intencionados e desconhecidos quase imediatamente.

A filtragem de URL permite que os administradores controlem o acesso à web, bloqueando ou permitindo o acesso a categorias específicas de sites. Isso ajuda a proteger contra ameaças da web e a garantir conformidade com políticas de uso da internet determinadas por sua organização.

5. Controle de Aplicações:

O módulo **Controle de Aplicações** permite que os administradores controlem quais aplicativos são permitidos ou bloqueados na rede, com base em categorias, riscos e políticas específicas. Isso ajuda a prevenir o uso indevido de aplicativos e protege contra ameaças associadas a determinados tipos de tráfego.

6. Proteção contra Ameaças Avançadas (ATP):

SONDA S.A. Copyright (c) 2025| Sua reprodução é proibida e qualquer cópia impressa deste documento é considerada não controlada. [NC-40]

O módulo de **Proteção contra Ameaças Avançadas (ATP)** refere-se a soluções de segurança que protegem sua organização contra-ataques cibernéticos avançados e malware que visam extrair, corromper ou roubar dados confidenciais.
A **ATP** pode ajudar uma organização a ficar um passo à frente dos criminosos cibernéticos, prevendo até vetores de ataque, colocando a equipe de TI em melhor posição para se defender contra eles.
A **ATP** é projetada para detectar e bloquear ameaças avançadas e persistentes, utiliza análise comportamental, sandboxing, inteligência artificial (IA) e aprendizado de máquina (ML) contra ameaças para identificar atividades maliciosas.

7. **VPN (Virtual Private Network):**

Os NGFWs incluem funcionalidades de VPN para garantir a segurança nas comunicações remotas, permitindo a criação de túneis seguros e privados para comunicação entre filiais, usuários remotos e parceiros comerciais.

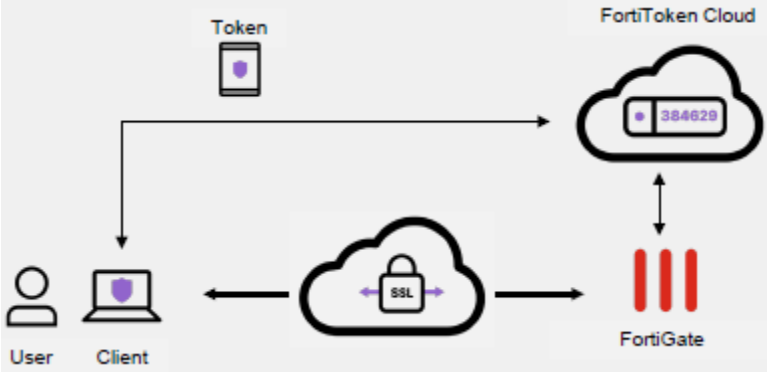
8. **Secure SD-WAN:**

Os NGFWs incluem funcionalidades de **SD-WAN** para oferecer conectividade de alto desempenho e ajuda a estender o acesso seguro independentemente de suas localizações geográficas.

Produto líder no **Gartner® Magic Quadrant™ 2023** para **SD-WAN** em alta capacidade de execução.

5.1. Autenticação de dois fatores – FortiToken Mobile

O Firewall **SONDA** oferece a função de autenticação em dois fatores através do aplicativo FortiToken Mobile, gerando senhas provisórias de acesso único. Ele possui servidor de autenticação integrado para validação OTP (one-time password), sendo o segundo fator de autenticação para VPN SSL. Isso elimina a necessidade de servidor RADIUS externo que é normalmente necessário ao implementar soluções de dois fatores.
O aplicativo FortiToken Mobile está disponível para as plataformas iOS, Android e Windows Phone.
Abaixo o diagrama de funcionamento do serviço de Firewall com a autenticação em dois fatores do FortiToken Mobile.



Nota: O FortiToken Mobile está disponível apenas para a oferta de bundle de Firewall C2S (client-to-site).

6. Escopo de Atuação

Com o suporte especializado da **SONDA** e a parceria com os fabricantes, nossos **CLIENTES** usufruem das facilidades de licenciamento, processos de instalação customizados, suporte e entrega de serviços, relatórios que apresentam os dados relevantes para que os nossos **CLIENTES** possam aprimorar seus mecanismos de segurança.

SONDA S.A. Copyright (c) 2025| Sua reprodução é proibida e qualquer cópia impressa deste documento é considerada não controlada. [NC-40]

Neste serviço o Firewall é monitorado 24x7x365 garantindo para os **CLIENTES** da **SONDA** o atendimento de SLA de disponibilidade contratado e o suporte operacional.

A **SONDA** garante a atualização constante dos componentes de Firewall que compõem a solução, assim como a execução de backups diários com retenção de 60 dias através da ferramenta de monitoramento.

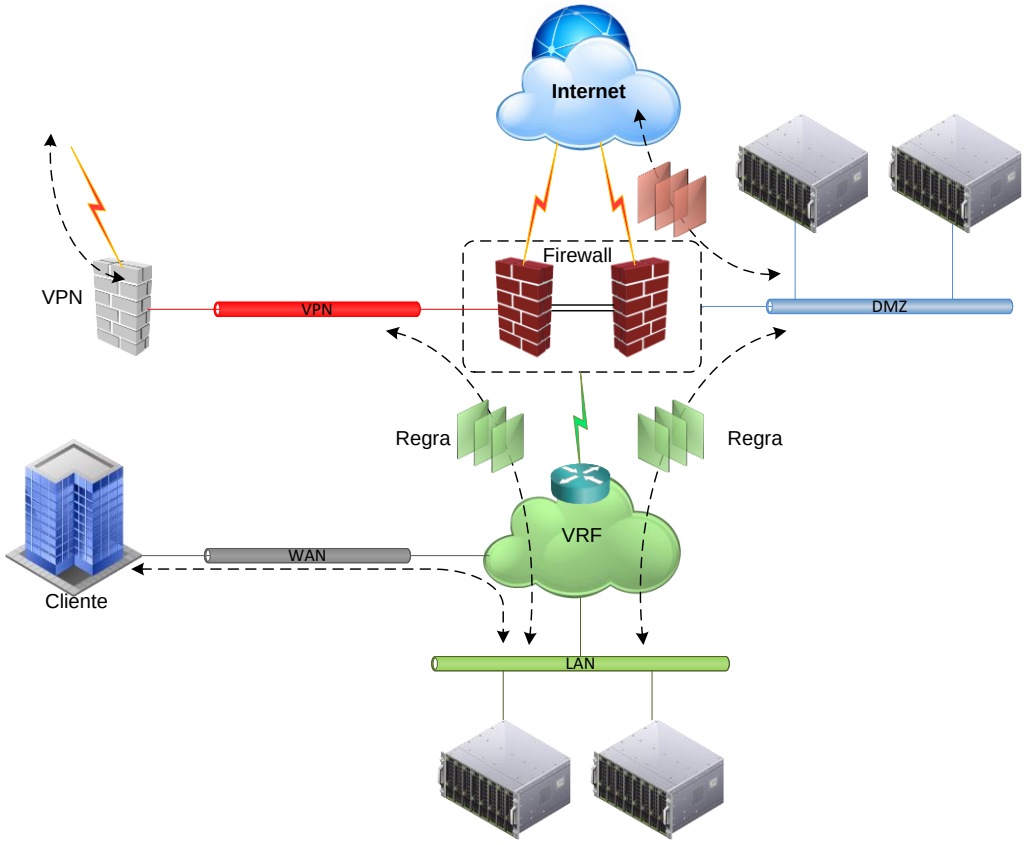
Em caso de eventuais falhas, o atendimento é contínuo até que o ambiente se restabeleça nas situações normais. Por padrão, são utilizadas tecnologias de Camada 2 e Camada 3, de acordo com a demanda do projeto.

Para a infraestrutura de rede são utilizados equipamentos e/ou tecnologias com performance compatíveis com os atuais padrões de mercado.

O escopo deste serviço é oferecer Bundle de firewall que contempla firewall e VPN.

6.1. Topologia Firewall

Na topologia abaixo vimos que o Firewall e suas regras são destinados a infraestrutura do **CLIENTE**.
As regras de VPN e de Firewall são exclusivamente entregues ao **CLIENTE**.



6.2. Relatórios Entregáveis

Escopo	Dedicado
Relatório de utilização de banda geral - Sob demanda	Sim
Relatório de Regras - Sob demanda	Sim

SONDA S.A. Copyright (c) 2025| Sua reprodução é proibida e qualquer cópia impressa deste documento é considerada não controlada. [NC-40]

Relatório Gerenciais (detalhamento dos outros relatórios)	Não*
Relatório de Tráfego na Interface geral - Sob demanda	Sim
Relatório de Log de acesso geral - Sob demanda	Sim

Nota: * Para ofertar os relatórios gerenciais deve ser acrescentado o produto de Monitoramento.

7. Ofertas

O serviço gerenciado de Firewall é ofertado por capacidade em duas modalidades de oferta, sendo a diferença entre elas o suporte ou não a VPN Client to Site.

1. **Modalidade com VPN S2S**
   - Bundle Firewall Unified Threat Protection – S2S
2. **Modalidade com VPN S2S e C2S**
   - Bundle Firewall Unified Threat Protection – S2S and C2S

Abaixo segue o quadro comparativo entre as duas modalidades.

Escopo	1 Bundle de Firewall UTP + S2S	1 Bundle de Firewall UTP + S2S and C2S
Máximo 400 Políticas de Firewall	Sim	Sim
Máximo 40 Usuários VPN Client to Site Simultâneos	Não	Sim
Máximo 80 Túneis VPN	Sim	Sim
Máximo 100.000 Sessões Correntes	Sim	Sim
Monitoramento Disponibilidade	Sim	Sim
Logs de Acesso Internet	Sim	Sim
Criação de Políticas, NAT, VPN e Roteamento	Sim	Sim
Atendimento a Solicitações e Incidentes	Sim	Sim
Política de backup de configuração	Sim	Sim
Evolução da versão do software do Firewall	Sim	Sim
Implantação de Rede Segregadas por LAN, DMZ, DEVQA, BD, ETC	Sim	Sim
Hardware em Cluster Ativo/Standby	Sim	Sim
Políticas de segurança definidas e/ou aprovadas pelo **CLIENTE**	Sim	Sim
Aplicação de endereçamento IP local definido pelo **CLIENTE**	Sim	Sim
Conexões de links WAN	Sim	Sim
Usuário com acesso leitura para o **CLIENTE**	Sim	Sim
Usuário com acesso escrita para o **CLIENTE**	Não*	Não*
Alta disponibilidade de Conectividade	Sim	Sim
Configuração de solução em SD-WAN	Sim	Sim
Geração de senha única de acesso através do FortiToken	Sim	Sim
Criar, Alterar e Excluir regras de IPS, WEB FILTER, APLICATION, ANTIVIRUS e SSL INSPECTION (Security Profiles Custom)	Sim	Sim
Fortitoken Mobile	Não	Sim

Nota *:

SONDA S.A. Copyright (c) 2025| Sua reprodução é proibida e qualquer cópia impressa deste documento é considerada não controlada. [NC-40]

- Para acesso de escrita ao usuário do **CLIENTE** na VDOM do Firewall, é necessária análise prévia do time de Segurança da **SONDA** e emissão de carta para compartilhar responsabilidades sobre acesso.

Notas:

- Caso a necessidade do **CLIENTE** não se enquadre nos serviços entregues deve ser tratado como Projeto Especial com análise e aprovação da **SONDA**.

8. Monitoramento

Para atuar de forma preventiva e preditiva, a **SONDA** oferece o serviço de Monitoramento que coleta dados dos itens monitorados e identifica condições que indicam a saúde do ambiente, sinalizando possíveis riscos ou sucessos operacionais.

O **CLIENTE** tem acesso ao portal da ferramenta de monitoramento, onde pode visualizar dados e relatórios detalhados, garantindo total transparência e a certeza de que o ambiente está sendo continuamente gerido e acompanhado pela equipe **SONDA**.

Além disso, o serviço conta com integração entre nosso ITSM e o Monitoramento por meio da ferramenta de Enterprise Application Integration (EAI), permitindo a abertura automática de chamados sempre que uma anomalia for detectada. Isso reduz significativamente o tempo de resposta a qualquer irregularidade no ambiente.

Monitoramento Padrão

O Monitoramento consiste no acompanhamento em tempo real de qualquer dispositivo utilizando o protocolo SNMP (Simple Network Management Protocol). Verifica o estado (up/down) dos dispositivos, níveis de consumo de memória e processamento, bem como tempo de resposta. É possível também supervisionar os acessos/links de rede, e monitoramento de URLs e Portais.

Itens monitorados:

- UP/Down de equipamentos;
- Monitoramento de Performance;
- Monitoramento de Disponibilidade;
- Monitoramento de redes (Vlan);
- Monitoramento de Conexões;
- Monitoramento de Consumo de banda;
- Monitoramento de Disponibilidade;
- Monitoramento de LOG.

Itens passiveis de monitoramento de acordo com a demanda do **CLIENTE**:

- Monitoramento de CPU, Memória e sessões por segundo;
- Monitoramento de VPN Site to Site; (up, down) – recebimento de alerta;
- Monitoramento e Gestão de controle de aplicações (camada 7);
- Monitoramento e Gestão de SDWAN;

Recebimento de alertas de Patchs de segurança "vulnerabilidades de firmware e etc.".

9. Premissas e Requisitos

9.1. Endereçamento IP

SONDA S.A. Copyright (c) 2025| Sua reprodução é proibida e qualquer cópia impressa deste documento é considerada não controlada. [NC-40]

Os **CLIENTES** só poderão determinar o endereçamento IP das redes internas que compõe a sua solução quando comprarem a solução de “Firewall Dedicado”.

Premissas:

- Uso de blocos válidos AS **SONDA**;

Cada link contará com 2 (dois) IPs válidos, sendo que qualquer quantidade adicional deverá ser analisada dentro de um Projeto Especial.

9.1. Relatórios

Este escopo não oferta relatórios gerenciais ou detalhados, para contratação do serviço deve ser adicionado as ferramentas conforme quadro abaixo. Para a emissão de relatórios customizados é necessário a aquisição de ferramenta Gerencial de Relatório, variando de tecnologia, por exemplo:

Fabricante	Ferramenta
Fortigate	FortiAnalyzer

10.Matriz de Responsabilidade

Para um melhor entendimento a matriz de responsabilidade será classificada com base na metodologia RASICO, onde: **R** - Responsável; **A** - Aprovador; **S** - Suporte; **I** – Informado; **C** – Consulta e **O** - Opcional.

Atividades	SONDA	CLIENTE
Criação, alteração e exclusão de regras de firewall	R	S/A
Monitoramento do ambiente de segurança	R	I
Implementação/ execução de política de backup	R	I
Atualização da versão de Software do Firewall	R	I
Alocar IP Válido	R	S
Criação de VRF	R	S
Inseris as VLAN´S criadas de acordo com o contexto a ser trabalhado (PRODUÇÃO E GERÊNCIA);	R	S
Criar as VLAN´S nos Switches de Acesso	R	S
Criar as VLAN´S no Firewall produção;	R	S
Criar VLAN'S no Firewall de gerência com as vlans de gerencia do **CLIENTE**	R	S

11.Requisição de Serviço

A tabela abaixo lista as requisições de serviços disponíveis para solicitações dos **CLIENTES** assim como seu tempo de solução e horário de cobertura.

Requisição	Classificação	Tempo de Solução
Criar regra de Acesso	C	Conforme TS contratado
Alterar regra de Acesso	C	Conforme TS contratado
Excluir regra de Acesso	C	Conforme TS contratado
Criar regra de NAT	C	Conforme TS contratado
Alterar regra de NAT	C	Conforme TS contratado
Excluir regra de NAT	C	Conforme TS contratado
Criar regra de Roteamento	C	Gestão de Mudança
Alterar regra de Roteamento	C	Gestão de Mudança

SONDA S.A. Copyright (c) 2025| Sua reprodução é proibida e qualquer cópia impressa deste documento é considerada não controlada. [NC-40]

Excluir regra de Roteamento	C	Gestão de Mudança
Criar regra de IPS	C	Conforme TS contratado
Alterar regra de IPS	C	Conforme TS contratado
Excluir regra de IPS	C	Conforme TS contratado
Criar regra de Web Filter	C	Conforme TS contratado
Alterar regra de Web Filter	C	Conforme TS contratado
Excluir regra de Web Filter	C	Conforme TS contratado
Criar regra de Aplication Control	C	Conforme TS contratado
Alterar regra de Aplication Control	C	Conforme TS contratado
Excluir regra de Aplication Control	C	Conforme TS contratado
Criar regra de Antivírus	C	Conforme TS contratado
Alterar regra de Antivírus	C	Conforme TS contratado
Excluir regra de Antivírus	C	Conforme TS contratado
Criar regra de SSL Inspection	C	Conforme TS contratado
Alterar regra de SSL Inspection	C	Conforme TS contratado
Excluir regra de SSL Inspection	C	Conforme TS contratado
Criar vlan	F	Gestão de Mudança
Alterar vlan	F	Gestão de Mudança
Excluir vlan	F	Gestão de Mudança
Gerar relatório	F	Conforme TS contratado
Inserir usuário ao Fortitoken	C	Conforme TS contratado
Alterar usuário ao Fortitoken	C	Conforme TS contratado
Excluir usuário ao Fortitoken	C	Conforme TS contratado

12.Nível de Serviço

Serviço	Nome	Descrição	Meta
Firewall	Disponibilidade	Percentual de tempo que o serviço estará disponível, incluindo acessibilidade e funcionalidade, excluindo desse tempo as atividades de paralisação programada e demais exceções mencionadas em contrato.	99,98%

Nota:
O SLA de disponibilidade acima só é válido mediante ao cumprimento de TODAS as premissas descritas neste documento.

SONDA S.A. Copyright (c) 2025| Sua reprodução é proibida e qualquer cópia impressa deste documento é considerada não controlada. [NC-40]


SONDA
make it easy