**DESCRITIVO PROFESSIONAL SERVICES DE FIREWALL**

ÍNDICE

1. Versão do Produto 3

2. Descrição Resumida 3

3. Objetivo 3

4. Benefícios 3

5. Escopo de Atuação 3

5.1. Relatórios por Modalidade 4

6. Ofertas 4

7. Monitoramento 4

8. Premissas e Requisitos 4

8.1. Infraestrutura 4

8.2. Endereçamento IP 5

9. Matriz de Responsabilidades 5

10. Requisição de Serviço 5

1. Versão do Produto

|  |  |  |
| --- | --- | --- |
| **Versão** | **Escopo** | **Data de Atualização** |
| Versão 01 | Criação do documento | - |

1. Descrição Resumida

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 mais relevantes para que os nossos **CLIENTES** possam aprimorar seus mecanismos de segurança.

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 neste serviço a atualização constante dos componentes de Firewall que compõem a solução, assim como a execução de backups periódicos da configuração após a mudança de configuração do ambiente.

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.

1. Objetivo

Os principais objetivos desse serviço são:

* Criar um conjunto de regras de execução de segurança no modo ativo e inativo;
* Proteção proativa que incluem gerenciamento seguro de sessões, proteção de cookies, criptografia de URL;
* Atualização constante das regras básicas de proteção incorporadas por padrão;
* Proposta de um conjunto de regras automatizadas baseadas em algoritmos inteligentes de aprendizagem;
* Inspeção http bidirecional: análise completa de solicitações e respostas;
* Configuração automática da proteção do Microsoft Outlook Web Access;
* Estatísticas abrangentes e arquivos de log detalhados;
* Alarmes configuráveis (e-mail, HTTP POST, Logs) quando ocorrem eventos definidos;
* Exportar e importar as configurações de regra no caso de migrações de ambientes de teste para produção;
* Auditoria completa de todas as alterações nos conjuntos de regras e configuração;
* Proteção de IPS;
* Recursos SD-WAN.

1. Benefícios

Gerenciamento eficaz do Firewall aplicando as melhores práticas:

* Refino de Regras;
* Correção de Problemas;
* Reestabelecimento dos serviços em menor tempo.

1. Escopo de Atuação

O serviço é ofertado para realizar o gerenciamento do Firewall contratado da **SONDA** ou próprio do **CLIENTE**.

* Cisco;
* Fortigate;
* SonicWall;
* Palo Alto.
  1. Relatórios por Modalidade

Abaixo segue relacionado o escopo das modalidades ofertadas

|  |  |  |
| --- | --- | --- |
| **Escopo** | **Firewall SONDA** | **Firewall CLIENTE** |
| Relatório de utilização de banda - Sob demanda | X | X\* |
| Relatório de Regras - Sob demanda | X | X |
| Relatório de Tráfego na Interface - Sob demanda | X | X\* |
| Relatório de Log de acesso - Sob demanda | X | X\* |

Nota\*: Necessário que o **CLIENTE** possua a ferramenta Analyser do firewall.

1. Ofertas

O Professional Services de firewall oferece serviços especializados por profissionais de segurança cibernética para ajudar os **CLIENTES** a projetar, implementar, configurar e otimizar firewalls de rede. Isso inclui avaliação de requisitos de segurança, personalização da configuração do firewall, monitoramento de tráfego, análise de ameaças, resposta a incidentes e suporte contínuo para garantir a proteção eficaz da rede contra acessos não autorizados, malware e outras ameaças cibernéticas.

1. Monitoramento

Para uma gestão preventiva e preditiva, a **SONDA** disponibiliza relatórios para que o **CLIENTE** possa ficar seguro tendo a certeza que o ambiente é gerido e acompanhado a todo instante pela equipe **SONDA**.

### **Monitoramento automático**

Visando trabalhar de forma preventiva a **SONDA** disponibiliza a ferramenta de Enterprise Application Integration (EAI) para abertura automática de chamados ao detectar anomalia no ambiente diminuindo o tempo de resposta de qualquer anormalidade apresentada.

### **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).

1. Premissas e Requisitos
   1. Infraestrutura

Os equipamentos deverão ser do padrão 19’’ (rack mount) e/ou vir providos dos devidos kits de montagem e ou quaisquer elementos necessários para sua montagem em racks.

Os equipamentos a serem instalados no Data Center **SONDA** deverão disponibilizar os cabos de energia de acordo com os novos padrões de tomadas elétricas padrão 3 pinos de acordo com a NBR 14136.

* 1. Endereçamento IP

Os **CLIENTES** só poderão determinar o endereçamento IP das redes internas que compõe a sua solução quando comprarem a solução de Firewall Dedicado. Quando a opção for o Firewall compartilhado, a **SONDA** determinará todo o plano de conectividade utilizados no Data Center (VLAN ID, IPs).

Caso o **CLIENTE** necessite de designar VLAN ID deve ser tratado como Projeto Especial.

Deverão ser considerados na precificação do projeto os custos de conectividade de cada equipamento (servidores, roteadores, outros) físico e dedicado ao projeto do **CLIENTE**.

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;
* Identificação dos endereços IP LAN remoto (LAN do site do **CLIENTE**);
* O endereço IP Peer (Internet do site do **CLIENTE**) deverá ser fixo;
* Para os firewalls de propriedade do **CLIENTE** não se encontra no escopo deste serviço;
* Ferramenta de Analyzer do Firewall para geração relatório;
* Licenciamento do Firewall;
* Ferramenta de Syslog.

1. Matriz de Responsabilidades

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Contratação opcional?** | **Atividades** | **SONDA** | **CLIENTE** |
| Não | Criação de regras de Firewall | R | S/A |
| Não | Monitoramento do ambiente de segurança | R | I |
| Não | Criação das VLAN´S | R | S/A |
| Não | Alocar IP Válido (caso aplicável) e fazer o roteamento para o contexto a ser trabalhado | R | S |
| Não | Criação de VRF | R | S |
| Não | Inseris as VLAN´S criadas de acordo com o contexto a ser trabalhado (Produção e Gerência) | R | S |
| Não | Criação das VLAN´S nos Switches de Acesso | R | S |
| Não | Criação das VLAN´S no Firewall produção | R | S |
| Não | Criação VLAN'S no Firewall de gerência com as VLANs de gerência do **CLIENTE** | R | S |

1. Requisição de Serviço

No quadro abaixo são listadas todas as atividades possíveis a serem requeridas para um profissional do serviço.

|  |  |  |
| --- | --- | --- |
| **Requisição** | **Classificação** | **Tempo de Solução** |
| Criar regra | C | Conforme TS contratado |
| Alterar regra | C | Conforme TS contratado |
| Excluir regra | C | Conforme TS contratado |
| Criar VLAN | F | Conforme TS contratado |
| Alterar VLAN | F | Conforme TS contratado |
| Excluir VLAN | F | Conforme TS contratado |
| Gerar relatório | F | Conforme TS contratado |

