



10 DICAS ESSENCIAIS PARA AQUISIÇÃO DE **FIREWALLS**

Recursos unificados de segurança para controle do uso da internet, gerenciamento de links e disponibilização de acesso remoto seguro (VPN), com interface intuitiva e prática.



ÍNDICE

3	INTRODUÇÃO
4	O PROBLEMA A SER RESOLVIDO
5	IDENTIFIQUE AS SOLUÇÕES
6	PLATAFORMA DE UTILIZAÇÃO
7	PRECIFICAÇÃO DA SOLUÇÃO
8	CAPACIDADE DE CRESCIMENTO
9	SUORTE E DESENVOLVIMENTO
10	SOLUÇÕES GRATUITAS
12	IMPLEMENTADOR
13	VENDER INTERNAMENTE
14	EQUIPE DE SEGURANÇA OU PROFISSIONAL ESPECIALIZADO



“ O objetivo deste e-book é orientá-lo com dicas essenciais, permitindo que você, verdadeiramente, **agregue valor** ao seu negócio ”

INTRODUÇÃO

A decisão de compra de um firewall passa por uma série de etapas: técnicas, comerciais, aprovação de orçamento e tantas outras. Implementações novas tendem a ser menos onerosas, enquanto, implantações que envolvem migração de estrutura, podem elevar de maneira substancial a complexidade de projetos, exigindo maior investimento em planejamento de implantação, conformidade de mudanças e análise de riscos.

O objetivo deste e-book é orientá-lo com dicas essenciais, permitindo que você, verdadeiramente, agregue valor ao seu negócio, independente do momento ou particularidades existentes no ambiente da empresa, facilitando a percepção de melhoria e retorno sobre o investimento.

Para facilitar a leitura, organizamos os itens de maneira segmentada, que vão desde o mapeamento dos problemas a serem resolvidos, até o convencimento e argumentação dentro da empresa para aprovação de orçamento para soluções com foco em segurança.

Aconselhamos profundamente leituras complementares do assunto para maior ambientação sobre o conceito, terminologia, tipos de arquitetura e soluções de firewall. Isso, sem dúvidas, facilitará o processo de aquisição e implantação da solução. Abaixo algumas leituras recomendadas:

[FIREWALL: HISTÓRIA](#)

[FIREWALL: CONCEITO E TERMINOLOGIA](#)

[ENTENDA AS PRINCIPAIS TOPOLOGIAS DE FIREWALL](#)

Esperamos que este material lhe auxilie na aquisição da sua primeira ou próxima solução de firewall.

BOA LEITURA!

[DICA #1]**REGISTRE
CLARAMENTE
QUAIS OS
PROBLEMAS
QUE DEVEM SER
RESOLVIDOS
PELA NOVA
SOLUÇÃO DE
FIREWALL****O PROBLEMA A SER RESOLVIDO**

O primeiro item importante trata-se do problema a ser resolvido, e embora possa parecer simples, é fundamental para delimitar a necessidade de sua empresa e não cair em armadilhas ou tentações comerciais.

A melhor solução para seu negócio não necessariamente passa pelo quadrante mágico do Gartner ou empresas que tem participação de mercado expressivas.

A reputação, solidez e maturidade da solução são importantes, mas comprar marca (ou grife) na maioria dos casos não significa satisfação. Você precisa entender sua necessidade e momento de compra.

Portanto, antes de iniciar a pesquisa sobre produtos, liste quais são as necessidades demandadas para o seu negócio. Caso a empresa possua uma solução de firewall em produção, destaque os pontos que necessitam ser melhorados. Os pontos registrados na checklist, serão utilizados na etapa de comparação das soluções.

A checklist pode ser um documento simples ou, dependendo da maturidade do negócio, um documento mais completo, podendo posteriormente evoluir para uma RFI (Request for Information). Independente do formato do documento, o mais importante é seu conteúdo, que deve expor de maneira clara as necessidades do negócio.

Uma vez que esta listagem estiver pronta, pode-se então dar o próximo passo que é verificar a aderência das soluções de mercado para as necessidades que foram levantadas nessa etapa. Procure utilizar uma planilha para comparar lado a lado as soluções de acordo com as necessidades registradas.

Lembrando que sua checklist não deve conter somente aspectos técnicos, sendo importante levar em consideração validações complementares de serviços, experiência da equipe, formato de atendimento (fabricante/revenda), propriedade de produto (solução proprietária), modelo de pós-venda, faturamento, entre outros.



[DICA #2]

LISTE AS SOLUÇÕES QUE TENDAM SUA NECESSIDADE NÃO SOMENTE NO ASPECTO DE COMPARAÇÃO DE CARACTERÍSTICAS TÉCNICAS, USE A INTERNET E SUA REDE DE CONTATOS

IDENTIFIQUE AS SOLUÇÕES

Uma vez que os problemas estejam devidamente registrados, é hora de realizar uma pesquisa de aderência das soluções de mercado com as necessidades levantadas. A internet é um excelente ponto de pesquisa para fins de levantamento, e irá reduzir consideravelmente seu tempo.

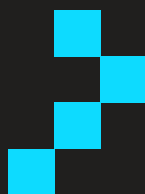
É interessante que sua checklist ou documento permita uma configuração lado a lado das soluções, assim sua comparação será mais eficiente. Tome bastante cuidado com nomenclaturas usadas por fornecedores para uma determinada característica de produto, em alguns casos pode causar a impressão de que o mesmo é o único detentor de tal funcionalidade.

Separe os recursos ou características que são mandatórios daqueles apenas desejáveis, isso certamente terá bastante diferença no momento de composição de valores.

Não esqueça da [DICA #1](#) e, portanto, crie um link entre as características como solução para os problemas que foram levantados.

Além dos aspectos técnicos, considere o país de origem da solução, a forma como a mesma será implantada em sua estrutura (terceiros, representantes comerciais etc), suporte técnico, capacidade de crescimento e licenciamento, entre outras informações importantes para o sucesso do seu projeto que estão ao longo deste material.

Sua rede de relacionamentos pode atuar de maneira muito favorável na recomendação e também comprovação de seu levantamento, mas seja criterioso ao obter as informações de indicação que realmente tirem suas dúvidas e agreguem valor ao levantamento que está sendo realizado.



[DICA #3]

**ESCOLHA
CRITERIOSAMENTE
QUAL A MELHOR
PLATAFORMA
PARA SUA
NECESSIDADE E
AMBIENTE**

PLATAFORMA DE UTILIZAÇÃO

Caso você ainda não saiba qual plataforma utilizará o produto, basicamente você encontrará três formatos para aquisição de firewall: software (openserver), appliance e virtual appliance.

SOFTWARE_A plataforma em software consiste em instalar a solução em um hardware próprio, novo ou reutilizado, não necessariamente de propósito específico (pode ser um servidor ou equipamento comum), onde os fabricantes têm compatibilidade de solução.

APPLIANCE_Os appliances representam soluções integradas de hardware e software embarcado, onde há uma grande sinergia e otimização do produto em uma plataforma de propósito específico. Geralmente, por conta do valor agregado, representam investimentos bem superiores às demais plataformas.

VIRTUAL APPLIANCE_Por outro lado, a plataforma de virtual appliance trata-se da utilização da solução em uma arquitetura virtualizada. Não podemos considerar uma estrutura totalmente especializada, mas em muitos cenários cumpre, juntamente com a plataforma em software, necessidades de diversas empresas, independente de porte.

Durante a etapa de levantamento das soluções não esqueça de registrar quais as plataformas suportadas pelos fabricantes. Você pode optar por uma solução em appliance, virtual appliance, software, e é importante que o fabricante tenha alinhamento com sua necessidade.

Se for sua primeira compra, ou o orçamento que você possui é um pouco mais limitado, as plataformas de software ou virtual appliance podem realmente ser bastante atraentes.

Nenhuma delas impede que você inicie a utilização com poucos recursos e escale conforme necessidade de crescimento no médio e longo prazo.

Diferentemente, se sua empresa está buscando

uma plataforma de ponta, o appliance é altamente recomendado, por que une hardware e software em uma única solução, com arquitetura especializada. Os fabricantes de appliances tem modelos para todos os tamanhos de negócios, portanto, appliance não está associado a negócios de maior porte.

PRECIFICAÇÃO DA SOLUÇÃO

Firewalls são precificados de diversas formas e entender o modelo de licenciamento é crítico para o sucesso do seu projeto, especialmente no que diz respeito a ROI e TCO. As licenças-base geralmente são comercializadas em formato perpétuo, onde pode-se utilizar o produto independente da existência de um contrato de desembolso mensal ou anual.

Modelos pay-per-use, baseados em receita recorrente, também estão se tornando comuns, e nestes casos, não há percepção de investimento inicial de licença, o valor na realidade é embutido na cobrança recorrente.

Além do licenciamento, outros produtos e serviços podem estar envolvidos nas propostas. Os mais comuns são planos ou subscrições de cobertura de suporte e atualização dos produtos, extensões (bundles) que não fazem parte do pacote básico de licenciamento, e até mesmo valores envolvendo serviços de implantação ou consultorias.

Para não cair em nenhuma armadilha, portanto, separe em seu documento de comparação qual o investimento único associado ao seu projeto de segurança, e quais são os custos fixos. O resultado trará uma visibilidade de custo de solução ao longo do tempo bastante interessante, e poderá ser um instrumento de apoio para tomada de decisão.

Muitas soluções tem o custo de aquisição baixo como estratégia de atrair o cliente, mas acabam praticando valores altos de manutenção não sendo competitivos no

[DICA #4]

**SEPARE O
INVESTIMENTO
INICIAL DOS
CUSTOS FIXOS
E AVALIE O
PREÇO TOTAL
AO LONGO DO
TEMPO**



[DICA #5]

ANALISE BEM O FORMATO DE LICENCIAMENTO PENSANDO NO CUSTO DE CRESCIMENTO AO LONGO DO TEMPO

tempo. Nenhuma organização compra um firewall com intuito de mantê-lo durante 12 meses, portanto pensar no médio e longo prazo é muito valioso. O contrário também ocorre, por isso a relevância em separar o investimento inicial dos custos fixos.

CAPACIDADE DE CRESCIMENTO

O custo de crescimento é outro item importante a ser avaliado durante o processo de seleção de sua solução de firewall. Entende-se por custo de crescimento qualquer valor desembolsado pela empresa decorrente do crescimento do seu parque ou em utilização de recursos que necessita de upgrades de licenciamento.

É importante validar todo o licenciamento da solução e verificar se há limitação de usuários ou dispositivos, e quando houver, se o valor de crescimento está de acordo com a expectativa de orçamento.

Essa é uma armadilha comercial, em muitas comparações, focadas somente em preço. Os compradores acabam igualando soluções que limitam, por exemplo, 5 usuários de VPN, com soluções que preveem usuários ilimitados para esse recurso.

O mesmo caso aplica-se para o crescimento no número de equipamentos (notebooks, desktops, etc) e, portanto, acessos simultâneos, ou dispositivos únicos utilizando ou sendo gerenciado pelo produto de firewall. Muitas licenças são referenciadas por conexões simultâneas, dispositivos e outras métricas que relacionam o crescimento sendo necessário a aquisição de novas licenças ou upgrades para manutenção do funcionamento dos recursos contratados, gerando novos investimentos para o cliente.

No caso da plataforma em appliance é interessante comprar modelos com capacidade de expansão, ou que permitam crescimento, caso sua empresa tenha esta expectativa. Isso por que, nos appliances, o crescimento muitas vezes envolve upgrade de hardware, e a troca do equipamento, exigindo novo investimento, o que não é interessante para o negócio. Bastante cuidado na

escolha do modelo de appliance, valide a estratégia de crescimento para não tornar o hardware precocemente obsoleto.

Além da avaliação de custo fixo ao longo do tempo, esteja muito atento ao custo de crescimento. Procure uma solução que esteja alinhada em suas expectativas de crescimento e orçamento, e que ao invés de limitar, permita que as necessidades e o negócio cresçam sem impeditivos.



[DICA #6]

**NÃO COMPRE
SOMENTE O
PRODUTO,
BUSQUE A
SOLUÇÃO, QUE
COMPREENDE
PRODUTO, PÓS-
VENDA E MUITO
MAIS**

SUPORTE E DESENVOLVIMENTO

Muitos consumidores não compram produtos considerando a estrutura de pós-venda do fornecedor, e isso ocorre com qualquer produto, não necessariamente falando de segurança da informação. Infelizmente problemas acontecem e isso não está necessariamente vinculado a qualidade da solução, especialmente quando falamos de tecnologia, onde existem diversas variáveis envolvidas. Além de problemas, o acesso à um suporte de qualidade traz comodidade, agilidade e, conseqüentemente proporciona melhor uso da solução, trazendo experiência diferenciada ao cliente.

Por isso, além da aderência de necessidades técnicas, custos de licenciamento e crescimento, considere com peso razoável a avaliação do pós-venda tanto do produto quanto da empresa que está oferecendo-o (no caso de venda de produtos via representantes, distribuidores e outros). Utilize a internet, sua rede de relacionamento e outros meios para obter informações a respeito do serviço de pós-venda, você vai precisar.

Quem oferece o suporte da solução? Se for um representante, verifique qual o grau de abertura o mesmo possui com o fabricante da solução, uma vez que, em momentos específicos, pode ser necessária a intervenção deste na resolução de problemas. Se for uma multinacional, muito provavelmente você entrará em uma fila de atendimento, com tempo maior de resolução.

Um representante comercial de multinacional, na maioria dos casos, possui relacionamento mais próximo com o distribuidor nacional, e exerce muito pouca influência, ou realmente nenhuma, com o fabricante em si. Isso quer dizer que, independente de portais, bases de conhecimento, documentação, FAQ, etc. A facilidade de acesso ao fabricante é algo importantíssimo a ser considerado na compra, por que certamente, em algum momento, problemas ou necessidades irão surgir.

Mesmo que não ocorra nenhum problema, contar com a experiência direta do fabricante no deploy de suas soluções representam alguns passos expressivos no sucesso do projeto. Se o seu projeto precisa de alguma customização de característica, estar próximo do fabricante é basicamente o fator crítico de sucesso.

SOLUÇÕES GRATUITAS

Existem diversas soluções de firewall gratuitas na internet disponíveis para download, e você deve certamente incluí-las em seu processo de avaliação com todos os critérios e dicas que estamos colocando para reflexão neste material. São soluções verdadeiramente interessantes e potencialmente atrativas para implantação, pois um dos grandes impedimentos em muitos projetos de segurança, é a indisponibilidade de orçamento.

Não esqueça que implantar uma solução de firewall, com todos os recursos disponíveis, não trata-se de um processo plug and play. É necessário experiência tanto no mercado de segurança, para melhor aproveitamento da solução, e muita profundidade e conhecimento também da solução, para proporcionar um uso mais adequado para o ambiente.

[DICA #7]

**CUIDADO COM
OS RISCOS
OCULTOS NA
ESCOLHA DE
SOLUÇÕES
DE FIREWALL
GRATUITAS**

Portanto, para as soluções gratuitas é interessante responder, dentre tantas outras, algumas perguntas fundamentais:

1. Quem ou qual empresa realizará a implantação da solução? Qual o nível de especialização da mesma?

2. Qual o país de origem da solução e que plataformas de acesso são oferecidas para suporte? Os níveis de acordo de serviço (SLA) para este propósito atendem a expectativa da organização?

3. Qual a frequência de lançamento e atualização do produto? Trata-se de uma solução ativa no mercado?

A solução pode ser gratuita, mas sem dúvidas a implantação, suporte e outras necessidades não serão. A falta de expertise na implantação, bem como a falta de suporte com o ambiente em produção, podem ser traumáticos. Assumir que não será necessário suporte é um risco enorme para a continuidade do ambiente.

E para finalizar, caso possa ser tentador para você implantar por conta própria uma solução desse tipo, pense bem se isso é uma responsabilidade sua e se está no seu pleno domínio. Firewalls apresentam-se nas arquiteturas de rede como pontos únicos de falha (desconsiderando ambientes clusterizados), por isso, em caso de falha, toda a operação da empresa pode ser comprometida.



A solução pode ser gratuita, mas sem dúvidas a implantação, suporte e outras necessidades não serão.





[DICA #8]

**ALÉM DO
PRODUTO,
VALIDE COMO
SE DÁ O
PROCESSO DE
IMPLANTAÇÃO
E A EXPERTISE
DOS TIMES
ENVOLVIDOS**

IMPLEMENTADOR

Como citado na [DICA #7](#), soluções de firewall não são plug and play, e por conta disso é essencial que a empresa e os consultores envolvidos nesse projeto tenham conhecimento de segurança e também do produto, para potencializá-lo de acordo com as necessidades do ambiente.

Muitas empresas compram produtos baseados na marca, especialmente de multinacionais, acreditando que tal atitude minimiza a ocorrência de problemas e ampliará as chances de sucesso do projeto na organização.

Comprar produtos de grandes players internacionais traz algumas vantagens, contudo, é importante não se deixar levar por promessas difíceis de serem cumpridas.

Por isso, mantenha o foco na entrega da solução, para atendimento das necessidades do seu negócio, essa deve ser sua prioridade.

Avalie se a proposta oferecida inclui a entrega completa da solução através de uma metodologia e estrutura de projeto, para garantir que não seja simplesmente a compra de uma caixa ou de um software pela internet. Se não existir, verifique se realmente a sua equipe tem capacitação suficiente para extrair o que há de melhor da solução adquirida, do contrário, você estará subutilizando o produto.

Se não tiver equipe interna, e também a proposta não cobrir a implantação de acordo com as necessidades do seu ambiente, descarte-a ou solicite alinhamento. O sucesso do seu projeto não é somente a compra do produto, mas sim a resolutividade dos seus problemas.

E para finalizar, questione ao contato comercial qual a experiência da equipe de projetos, ou do implementador propriamente dito.

Certifique-se que você irá contar com um profissional altamente capacitado, com grande bagagem, para implantar a solução de firewall selecionada no ambiente de sua empresa.

[DICA #9]**TANGIBILIZE
QUANTO OS
PROBLEMAS
CUSTAM PARA
A EMPRESA
E MOSTRE
O RETORNO
SOBRE O
INVESTIMENTO****VENDER INTERNAMENTE**

Existem diversas possibilidades de vender o projeto de segurança internamente mas, sem conhecer os problemas, quaisquer sugestões mais direcionadas podem ser arriscadas ou não aplicadas à sua realidade. Por isso, como dica, basicamente a argumentação pode ser desenhada em produtividade e perda ou vazamento de informações.

É muito importante que independente da base de argumentação, você consiga tangibilizar, usando números para mostrar o quanto a falta de produtividade afeta o negócio, bem como os prejuízos financeiros e de imagem que um vazamento de informação poderia causar ao negócio.

Uma vez que consiga transformar em números estas perdas, tendo o valor do projeto, fica bastante fácil calcular o tempo de retorno do investimento e levar essa informação para os setores ou pessoa competente, com um argumento forte e quase infalível.

Quanto em média um funcionário perde com o uso da internet por dia? Essa pergunta pode ser um ponto de partida interessante. Se sua empresa tem 200 funcionários que usam regularmente computadores para exercer suas funções, e tem acesso à internet. Considerando que cada funcionário desperdice 1 hora por dia em atividades improdutivas, ao final de uma semana, serão 1000 horas que poderiam ser melhor empregadas.

Considerando um valor médio de hora na folha de pagamento em R\$ 15,00 existe um desperdício de aproximadamente R\$ 15.000,00 por semana. Certamente seu projeto de segurança seria rapidamente aceito e também traria um resultado espetacular para a organização se conseguisse reduzir esse número.

É claro que existem diversas outras variáveis que devem ser colocadas no papel para montar uma linha de argumentação e viabilidade orçamentária consistente, mas o exemplo é somente uma inspiração de como você pode começar a trabalhar em números para aprovar seu projeto.

Outro exemplo que pode ser utilizado, caso sua empresa

dependa muito da internet e sofra com quedas contínuas deste serviço, é indicado a inserção dos custos associados a indisponibilidade do recurso, em seu documento para viabilização de aquisição da solução de firewall.

Para auxiliar em sua defesa, faça a leitura desse artigo:

[QUANTO SUA EMPRESA PERDE COM A INDISPONIBILIDADE DE INTERNET?](#)



[DICA #10]

**PROCURE
PARCEIROS DE
SEGURANÇA
QUE SEJAM
ESPECIALISTAS
NO ASSUNTO**

EQUIPE DE SEGURANÇA OU PROFISSIONAL ESPECIALIZADO

Qual é o negócio que sua empresa atende e qual a importância da segurança? Muito embora segurança da informação seja fundamental para todos os negócios atualmente, e será cada vez mais, isso não significa e nem justifica manter uma equipe dentro da própria empresa.

Ter um parceiro especializado em segurança da informação na maioria dos casos é uma solução financeiramente interessante, e também de maior valor agregado, pois as equipes estão em contato com diversas demandas de segurança no mercado, e trazem toda essa bagagem para dentro de projetos, pós-venda ou incidentes ocorridos em sua empresa.

É importante ter um conhecimento superficial dentro do negócio para permitir maior facilidade de argumentação com os fornecedores, estar atento às novidades de mercado, mas ter um apoio de parceiro especializado neste segmento é um passo extremamente importante para o sucesso das estratégias de segurança ao longo do tempo.

Para organizações, especialmente financeiras, onde a confidencialidade e privacidade das informações é totalmente estratégico para sobrevivência do negócio, ter times de segurança próprios é basicamente um pré-requisito de sobrevivência. E mesmo nestes casos, as equipes internas tem contatos fortes com o mercado e

com fornecedores que suportam as soluções e plataformas de segurança utilizadas por estas empresas.

Pelo contrário, o dinamismo do mercado é muito alto, vulnerabilidades que podem comprometer milhões de ambientes, são lançadas diariamente. Produtos devem resolver a maioria das necessidades operacionais, mas jamais vão substituir a expertise de um time ou empresa especializada. Por isso, sempre antes de adquirir um produto de segurança, não somente um firewall, analise criteriosamente tudo aquilo que está ao redor do produto e fornecedor. Faça o movimento correto!

CONTINUE LENDO

SE VOCÊ GOSTOU DO ASSUNTO E GOSTARIA DE NOVAS LEITURAS, FIQUE A VONTADE PARA CONSULTAR ATRAVÉS DOS LINKS ABAIXO TEMAS RELACIONADOS EM NOSSO PORTAL.



FILTRO DE CONTEÚDO WEB

Gerir de maneira eficiente o uso da internet é um passo importante, que não somente aumenta a segurança do ambiente corporativo e das pessoas, mas promove ganhos de produtividade.



RANSOMWARE

5 DICAS FUNDAMENTAIS PARA EVITAR SEQUESTRO DE DADOS

O material traz informações essenciais sobre ataques Ransomware, que vem causando danos expressivos a empresas e usuários no Brasil e no mundo.



TUDO QUE VOCÊ PRECISA SABER SOBRE FIREWALLS

Gerir de maneira eficiente o uso da internet é um passo importante, que não somente aumenta a segurança do ambiente corporativo e das pessoas, mas promove ganhos de produtividade.



VOCÊ SE INTERESSOU PELO CONTEÚDO?

ESCLAREÇA SUAS DÚVIDAS COM ESPECIALISTAS NO ASSUNTO

CONVERSE COM ESPECIALISTA





facebook.com/ostec



linkedin.com/company/ostec-security



contato@ostec.com.br



www.ostec.com.br



ostec.blog



ostec
Segurança digital de resultados