10 Atributos que o seu próximo Firewall precisa ter

Muito já foi feito para proporcionar visibilidade das aplicações e controle sobre a segurança da rede. A razão é óbvia: aplicações podem facilmente escapar dos firewalls tradicionais baseados em portas. E o valor é óbvio: funcionários usam qualquer aplicação que precisam para que seu trabalho seja realizado – geralmente, são indiferentes ao risco que este uso pode trazer ao negócio. Quase todo profissional que trabalha com segurança de rede admite que o controle de aplicações é uma parte cada vez mais crítica.

> **"Não se trata de bloquear aplicações, mas permiti-las de modo seguro. Aplicações garantem a continuidade dos negócios e os profissionais precisam estar cientes de que as utilizam de forma segura"**

Os firewalls de nova geração são definidos pelo Gartner como algo novo, diferenciado, focado nas necessidades corporativas, ao contrário do que afirmam alguns, de que esse tipo de solução é um subconjunto de outras funcionalidades (ex: UTM ou IPS). Oferecer visibilidade de aplicativos e conteúdo e ter o controle sobre o que circula em sua rede, mas utilizando um número limitado de assinaturas IPS ou uma base de dados externa não é a solução ideal. Essas funcionalidades não possuem uma integração total e sua matriz tecnológica ainda continua sendo a base Statefull.

A nova geração de *firewalls* é uma classe revolucionária e diferente de produtos, que tem como visão não bloquear aplicações, mas permiti-las de modo seguro e com controle. Aplicações garantem a continuidade dos negócios e os profissionais precisam estar cientes de que as utilizam de uma forma segura.

Para as empresas que procuram os firewalls da nova geração, a mais importante consideração a se fazer é: Essa nova tecnologia irá permitir que os times de segurança habilitem as aplicações que tragam benefícios para a organização? Outras perguntas-chaves para este tipo de tecnologia são:

- Aumentará a visibilidade e o entendimento do tráfego de aplicações?
- Expandirá as opções de controle de tráfego, para além do "autorizar/negar"?
- Ajudará a prevenir ameaças?
- Eliminará a necessidade de comprometer a performance em prol da segurança?
- Reduzirá custos para minha organização?
- Fará o gerenciamento de risco mais fácil ou simples?

Se a resposta a todas essas questões for sim, a transição é fácil de justificar

DEFINIÇÃO: NOVA GERAÇÃO DE FIREWALL
5 requisitos:

1. Identifica aplicações, independentemente da porta, protocolo, tática evasiva ou SSL;
2. Identifica usuários, independentemente de endereço IP;
3. Protege em tempo real contra ameaças incorporadas em aplicações;
4. Garante alta visibilidade e políticas de controle sobre o acesso a aplicações/ funcionalidades;
5. Multigigabit, implantação em linha, sem perda de performance.

Os 10 atributos que o seu Firewall precisa ter

Se o assunto for Firewalls, existem três pontos que a solução deve possuir – fácil operação, funções de segurança robustas e tudo isso com performance. As funções de segurança são elementos que correspondem à eficiência e controle sobre a segurança e a habilidade de gerenciar os riscos sobre o tráfego da sua rede. Na operação, o maior questionamento é: qual é a complexidade de gestão da solução? No quesito performance, a diferença é simples: a solução de Firewall faz todo o seu trabalho com o throughput e performance aceitáveis?

Agora, os 10 atributos que seu Firewall de nova geração deve possuir

1. Identificar e controlar aplicações em qualquer porta;
2. Identificar e controlar *circumventors**;
3. Descriptografar SSL de saída;
4. Possuir funções de controle de aplicações;
5. Procurar e prevenir vírus e malware em aplicações colaborativas permitidas em seu ambiente;
6. Ter o controle sobre o tráfego desconhecido a partir de políticas de segurança;
7. Identificar e controlar aplicativos que possuam a mesma conexão;
8. Permitir a mesma visibilidade de aplicações e controles para usuários remotos;
9. Tornar a segurança de rede mais simples, e não mais complexa, com a adição de controles de aplicações;
10. Oferecer o mesmo throughput e performance com o controle ativo das aplicações;

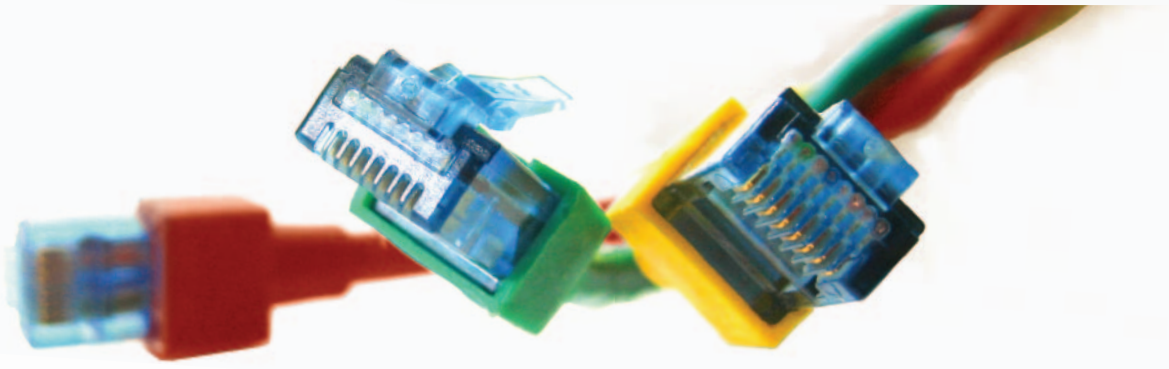
Saiba mais

1. O seu próximo firewall precisa identificar e controlar aplicações em qualquer porta e não apenas nas portas padrões (inclusive aplicações que usam HTTP ou outros protocolos).

Business case

Os desenvolvedores não se orientam mais pelos mapeamentos sobre padrão de portas, protocolos e aplicações. As aplicações são cada vez mais dinâmicas, tendo seu funcionamento em portas não padrão ou podem pular portas, como aplicações de mensagens instantâneas, arquivos peer-to-peer ou VOIP. Além disso, os usuários estão suficientemente experientes para forçar aplicações a rodar sobre portas não padrão (ex. MS RDP, SSH).

Para manter o controle das políticas específicas sobre aplicações em que as portas podem ser alteradas, seu próximo firewall deve assumir que qualquer aplicação pode rodar em qualquer porta. Essa é uma mudança fundamental que pode fazer do firewall de nova geração uma necessidade absoluta. Se qualquer aplicação pode ser executada em qualquer porta, um produto tendo como sua tecnologia a base Statefull deverá executar todas as assinaturas em milhares de portas.



É simples: seu próximo firewall precisa classificar o tráfego por aplicação, independente da porta, o tempo todo. De outra maneira, as políticas de segurança continuarão a ser burladas pelas mesmas técnicas que o atormentam há anos.

Requisitos

2. Seu próximo firewall precisa identificar e controlar circumventors: proxies, acesso remoto e aplicações *encrypted tunnel.*

Business case

Proxies, acesso remoto e aplicações *encrypted tunnel* são especialmente utilizados para contornar (*circumvent*) equipamentos de segurança como *firewalls*, filtragem de URL, IPS e *gateway web* de segurança. Sem ter como controlar esse *circumventors,* as organizações perdem a eficácia em suas políticas de segurança e se expõem a graves riscos no qual elas pensam ter conseguido mitigar pelos controles.

Nem todas as aplicações funcionam da mesma forma – aplicações de acesso remoto têm seu tráfego confiável, assim como aplicações em túneis VPN. Mas, *proxies* externos, anônimos, que se comunicam por SSL em portas randômicas, ou aplicações como Ultrasurf e Tor, têm apenas um propósito real: contornar controles de segurança.

Requisitos

Existem diferentes tipos de aplicações circumvention – cada uma delas utilizando técnicas sutilmente diferentes. Existem tanto proxies públicos e privados (para ter acesso a uma grande base de dados de proxies públicos veja proxy.org) que podem usar tanto HTTP e HTTPS. Proxies privados são geralmente estabelecidos como endereços IP não classificados (ex: computadores domésticos) com aplicações como PHProxy ou CGIProxy. Aplicações de acesso remoto como MS RDP ou GoToMyPC podem ter uso seguro, mas devido ao risco associado precisam ser gerenciadas. A maioria dos demais circumventors (ex. Ultrasurf, Tor, Hamachi) não possui uso para os negócios. E existe, claro, os circumventors desconhecidos.

É preciso que o firewall tenha técnicas específicas para lidar com todas essas aplicações, independentemente de porta, protocolo, encriptação ou tática evasiva. Mais uma consideração: essas aplicações são regularmente atualizadas para tornar ainda mais difícil a detecção e o controle. Portanto, é importante entender que não apenas o seu próximo firewall pode identificar essas aplicações circumvention, mas também o quão frequente essa inteligência é atualizada e mantida.

3. O seu próximo firewall precisa descriptografar SSL de saída.

Business case

Atualmente, mais de 15% do tráfego de rede é SSL-encriptado (de acordo com a análise de mais de 2.400 exemplares de tráfego de rede – veja o relatório Palo Alto Networks' Application Usage and Risk para detalhes). Em

Business case

alguns mercados, como o de serviços financeiros, essa porcentagem sobe para mais de 50%. Devido ao aumento da adoção do protocolo HTTPS aplicações de alto risco, das aplicações utilizadas pelos usuários, como Gmail e Facebook, e da possibilidade dos usuários de forçar o uso do SSL em muitos sites, os times de segurança possuem um grande e crescente ponto cego ao não descriptografar, classificar, controlar examinar o tráfego SSL. Certamente, o firewall da nova geração precisa ser flexível para que alguns tipos de tráfego SSL-encriptado possam ser permitidos (ex: tráfego web, tráfego de serviços financeiros ou de organizações de saúde) enquanto outros tipos (ex: SSL em portas não padrão, HTTPS de websites não classificados da Europa Oriental) possam ser descriptografados via política de segurança.

Requisitos

A habilidade de descriptografar o tráfego SSL de saída é um elemento fundamental, não apenas porque a porcentagem de tráfego corporativo é significativa, mas também porque permite algumas outras funcionalidades-chaves que poderiam tornar-se incompletas, sem a habilidade de descriptografar o protocolo SSL (ex: controle de circumventors).

4. Seu próximo firewall precisa oferecer função de controle de aplicação (ex. SharePoint Admin vs. SharePoint Docs).

Business case

Muitas aplicações possuem diferentes funções, apresentando diferentes perfis de risco e valores, tanto para os usuários quanto para a organização. Bons exemplos disso são o WebEx vs. WebEx Desktop Sharing, Yahoo Instant Messaging vs. a funcionalidade de transferência de arquivos e o Gmail padrão vs. anexos enviados. Em ambientes regulados ou em empresas altamente dependentes de propriedade intelectual esse é um ponto crucial.

Requisitos

É preciso realizar a classificação contínua e obter o entendimento refinado de cada aplicação. Seu próximo firewall precisa avaliar continuamente o tráfego e observar as alterações: se uma nova função ou ferramenta for introduzida em uma sessão, o firewall precisa saber disso e realizar a checagem da política de controle.

Requisitos

Entender as diferentes funções de cada aplicação e os diferentes riscos a elas associados é extremamente importante. Infelizmente, muitos firewalls classificam o fluxo do tráfego uma vez e depois vão pelo caminho mais rápido, (leia-se: nunca mais olham para o fluxo novamente) isso para obter um melhor desempenho. Este método não acompanha as aplicações modernas e impede que esses firewalls encontrem o que é realmente necessário.

5. Seu próximo firewall precisa examinar ameaças em aplicativos de colaboração autorizados, como Sharepoint, Box.net, MS Office Online.

Business case

Empresas adotam cada vez mais aplicativos colaborativos localizados fora de seu Datacenter. Seja em Sharepoint, Box.net, Google Docs ou Microsoft Office Live, ou mesmo em uma extranet de algum parceiro, muitas organizações necessitam de uma aplicação que compartilhe arquivos – em outras palavras, esse é um vetor de alto risco.

Muitos documentos infectados estão armazenados em aplicativos de colaboração, juntamente com documentos que possuem informações sensíveis, por exemplo, informações pessoais de clientes. Além do mais, algumas dessas aplicações (Sharepoint) baseiam-se em tecnologias que são alvos regulares para exploits (ex., IIS, SQL Server). Bloquear a aplicação não é recomendado, mas também permitir tudo traz ameaças ao ambiente corporativo.

Para se ter um ambiente seguro, é necessário examinar as aplicações em busca de ameaças. Essas aplicações podem comunicar-se por meio de uma combinação de protocolos (ex. Sharepoint – HTTPS e CIFS, e requerem políticas mais sofisticadas do que o "bloqueio da aplicação"). O primeiro passo é identificar a aplicação (independentemente da porta ou da encriptação), permiti-la protegendo o ambiente de ameaças: exploits, vírus/malware ou spyware... Ou mesmo informações confidenciais, sensíveis e regulamentadas.

Requisitos

6. Seu próximo firewall precisa lidar com tráfego desconhecido a partir de políticas, e não deixar que ele simplesmente passe despercebido.

Business case

Sempre existirá um tráfego desconhecido e ele sempre representará riscos significativos para qualquer organização. Existem vários elementos importantes a se considerar em relação ao tráfego desconhecido – identificar facilmente aplicações personalizadas de forma que elas sejam "conhecidas" na política de segurança, e ter visibilidade previsível e políticas de controle sobre o tráfego que permanece desconhecido.

Requisitos

Primeiramente (por padrão), seu próximo firewall precisa tentar classificar todo o tráfego - essa é uma área em que as arquiteturas anteriores e a discussão sobre segurança tornam-se importantes. Para aplicações customizadas ou desenvolvidas pela própria organização, deve haver uma maneira de identificar esta personalização – de forma que o tráfego é contabilizado por "conhecido" e controlado.

7. Seu próximo firewall precisa identificar e controlar aplicações que compartilham a mesma conexão.

Business case

Aplicações compartilham seções. Para garantir que os usuários continuem usando plataformas de aplicações, seja Google, Facebook, Microsoft, SalesForce, LinkedIn ou Yahoo, os desenvolvedores integram diferentes aplicações – que geralmente possuem perfis de risco e valores de negócio diferenciados. Vamos observar o exemplo do Gmail – que possui a habilidade de rodar uma seção do Google Talk dentro do Gmail. São aplicações fundamentalmente diferentes, e o seu próximo firewall precisa reconhecer isso e permitir respostas apropriadas nas políticas de segurança para cada uma delas.

Requisitos

A simples classificação da plataforma ou do website não funciona. Em outras palavras, o "caminho mais rápido" não é a opção – a classificação "uma vez feita" ignora o fato que aplicações compartilham seções. O tráfego precisa ser continuamente avaliado para entendermos a aplicação, suas mudanças, quando o usuário muda para uma aplicação completamente diferente utilizando a mesma seção e reforçar as políticas de controle apropriadas.

Basta analisar de forma rápida os requisitos utilizados pelo Gmail/Google Talk, por exemplo: o Gmail é por default HTTPS, então, o primeiro passo é descriptografá-lo. Mas isso deve ser constante, assim como a classificação da aplicação, porque a qualquer momento o usuário pode iniciar um chat, que pode ter uma política completamente diferente associada a ele.

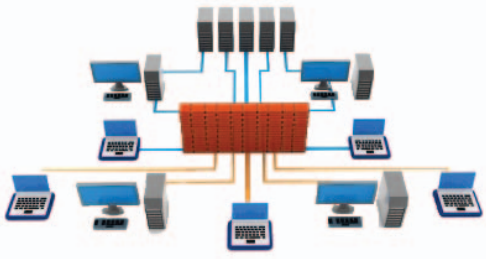
8. Seu próximo firewall precisa permitir a mesma visibilidade e controle de aplicativos para usuários remotos.

Business case

Cada vez mais, os usuários estão trabalhando longe dos escritórios. Uma parte significativa dos profissionais é capaz de trabalhar remotamente. Seja em um coffee shop, em casa, alocados no cliente, os usuários esperam conectar-se às aplicações via WiFi, 3G ou qualquer meio necessário. Independentemente de onde o usuário esteja, ou mesmo onde a aplicação que ele utiliza possa estar, o mesmo padrão de controle deve ser aplicado. Se o seu próximo firewall permite visibilidade de aplicativos e controle sobre o tráfego dentro do escritório, mas não fora, ele abre uma porta de ameaças ao ambiente.

Requisitos

Conceitualmente isso é simples: seu próximo firewall precisa ter visibilidade e controle consistentes sobre o tráfego, independentemente de onde o usuário esteja – dentro ou fora. Isso não quer dizer que as empresas terão as mesmas políticas de segurança – algumas organizações podem querer que seus empregados usem Skype quando estão fora, mas não dentro da sede, enquanto outras podem ter uma política que diga que se estiver fora do escritório, usuários não podem fazer download de anexos do sales-force.com a não ser que tenham o disco rígido encriptado. Isso pode ser obtido em seu próximo firewall sem introduzir latência significativa para o usuário final, ou pro-blemas operacionais indevidos ao administrador, ou custo significa-tivo para a organização.



9. Seu próximo firewall precisa tornar a segurança de rede mais simples, e não mais complexa, com a aplicação de controles de aplicativos.

Business case

Muitas empresas lutam para incorporar mais fontes de alimentação, mais políticas e mais regras no já sobrecarregado processo de gerenciamento de segurança e de pessoas. Em outras palavras, se os times não podem gerenciar o que eles já possuem, adicionar mais gerência, políticas e informações não ajudarão. Além do mais, quanto mais distribuída for a política (ex. Firewall baseado em portas, tráfego autorizado em porta 80, análise de IPS para bloqueio de ameaças e aplicações, reforço de segurança em portões web, filtragem URL), mais difícil é para gerenciar essa política. Onde os admins irão para permitir WebEx? Como eles resolvem conflitos de políticas de segurança sobre tantos equipamentos?

Dado que os firewalls típicos, baseados em portas, possuem bases de regras que incluem milhares de regras, adicionando milhares de assinaturas de aplicações por entre dezenas de milhares de portas (veja #3) a complexidade aumentará em muito.

Requisitos

Políticas de firewall precisam ser baseadas em usuários e aplicações. Análises de conteúdo subsequentes podem ser realizadas em tráfego permitido, mas o controle fundamental de acesso precisa ser baseado em elementos relevantes (aplicações, usuários ou grupos). Isso pode ter um efeito simplificador efetivo. Políticas de Firewall baseadas em portas em endereço IP, seguidas de análises subsequentes para entendimento da aplicação tornam as coisas mais complicadas do que já são.

10. Seu próximo firewall precisa oferecer o mesmo rendimento e desempenho com o controle ativo das aplicações.

Business case

Muitas empresas se esforçam para garantir a segurança, sem comprometer a performance. Muito frequentemente, transformar recursos de segurança em domínio de segurança de rede significa desassociar rendimento e performance. Se a sua próxima geração de firewall é desenvolvida da maneira certa, esse comprometimento é desnecessário.

Requisitos

A importância da arquitetura é óbvia aqui também, mas de uma maneira diferente. Associar um firewall baseado em porta a outras funções de segurança de diferentes origens tecnológicas e a outras funções de segurança em geral, indica a existência de camadas de rede redundantes, ferramentas de exame e políticas, que se traduzem em uma baixa performance. Da perspectiva do software, o firewall precisa ser desenvolvido para fazer
isso do começo. Além do mais, dadas as requisições para tarefas computacionais intensas (ex: identificação de aplicações) realizadas em alto volume de tráfego e com pouca tolerância à latência associada em infraestrutura crítica, seu próximo firewall precisa do hardware desenvolvido para a tarefa também – significando processamento de rede, segurança (incluindo terminações SSL – veja #3), e exame de conteúdo dedicado.

Conclusão

Seu próximo Firewall deve permitir aplicações e o desenvolvimento dos negócios de forma segura.

Usuários continuam adotando novas aplicações e tecnologias – e as ameaças advindas com elas. Em algumas empresas, impedir a adoção de novas tecnologias pode ser um movimento limitador. Mesmo quando não o é, aplicações geram produtividade. Portanto, a permissão cuidadosa e segura é cada vez mais a postura da correta política corporativa. Mas, para permitir essas aplicações e tecnologias de forma segura e, consequentemente, os negócios que giram em torno delas, os times de segurança precisam determinar políticas apropriadas que governem o seu uso, mas que também sejam capazes de controlar e se auto reforçarem.

Os dez atributos aqui descritos apresentam capacidades críticas para garantir os controles necessários – especialmente diante de um panorama de aplicacões cada vez mais variado e ameaçador. Sem uma infraestrutura de segurança de rede que lide com a variedade e a amplitude, os times de segurança não podem permitir de forma segura as aplicações necessárias e gerenciar os riscos em suas empresas.