# Firewalls vs. SBCs

Entendendo o modelo de acamadas OSI e as implicações para a RTC

White Paper

## Introdução

Empresas de todos os portes estão implementando soluções de voz sobre IP (VoIP, do inglês Voice over Internet Protocol) para melhor atender a negócios globalizados e equipes de trabalho móveis. Apesar da lenta adoção nos primórdios da tecnologia VoIP, estudos indicam que o mercado para esses serviços deve atingir US$ 204,8 bilhões até 2020. A adoção da tecnologia VoIP não apresenta sinais de desaceleração, mas sua implementação e gestão não estão livres de desafios.

Infraestruturas tradicionais de telefonia sofreram com problemas de desvio de chamadas, direcionamento e interceptação quando hackers assumiam o controle das redes empresariais de forma ilegal. As redes públicas de telefonia comutada (PSTNs, do inglês Public Switched Telephone Network) estão dando lugar para as soluções VoIP, mas isso não significa que as considerações tradicionais de segurança ficaram para trás. Em vez disso, os chamados criminosos cibernéticos aproveitam a disposição das empresas de abrir suas comunicações para a Internet com as soluções VoIP.

Muitas empresas acreditam que firewalls são medidas de segurança suficientes para proteção contra várias ameaças diferentes. Na realidade, a melhor opção de segurança para os serviços VoIP é com os controladores de borda de sessão (SBCs, do inglês Session Border Controllers).

Embora possa parecer que firewalls e SBCs tenham as mesmas metas de segurança, avaliar suas diferenças em como as tecnologias processam comunicações em tempo real revela a necessidade de empregar ambas as soluções para alcançar uma proteção adequada.

## A evolução dos firewalls

Tradicionalmente, firewalls operam na camada 2 (camada de enlace de dados), camada 3 (camada de dados) e camada 4 (camada de transporte) do modelo de camadas de interconexão de sistemas abertos (OSI, do inglês Open System Interconnection) e bloqueiam tráfego com base em portas na sua rede. Embora isso ainda faça parte da equação, firewalls modernos possuem recursos elevados com supervisão de aplicativos.

Atualmente, não importa o tipo de tráfego que circula na rede. Cas seja baseado em IP, o firewall moderno pode identificar assinaturas de aplicativos, entender o contexto de pacotes de dados e bloquear malware de forma inteligente.

Em vez de definir políticas difusas baseadas em portas, os firewalls modernos podem atualizar listas de malwares conhecidos com rapidez para se antecipar aos criminosos. E, no caso de detecção de malware, os novos firewalls podem enviar pacotes de dados para uma área restrita a fim de examinar arquivos e códigos potencialmente maliciosos. E não para por aí: quando os firewalls modernos operam em linha com proteção de endpoint, você conta com uma solução de segurança flexível capaz de se adaptar a praticamente qualquer tráfego de dados.

Migrar de firewalls baseados em portas e antivírus que funcionam com assinaturas para essas soluções flexíveis e modernas pode parecer a maneira perfeita para cobrir todas as necessidades de segurança. No entanto, essas soluções não são otimizadas para tratar das vulnerabilidades emergentes em comunicações de voz e vídeo em tempo real.

## Modelo de OSI

| | Dados | Camada |
|---|---|---|
| Camadas | **Dados** | **Aplicativo**<br>Proceso de rede para aplicativo |
| | **Dados** | **Apresentação**<br>Representação e criptografia de dados |
| | **Dados** | **Sessão**<br>Conexões de ponta a ponta e confiança |
| | **Segmentos** | **Transporte**<br>Conexiones y Contabilidad de Extremos a Extremo |
| Camadas de | **Pacotes** | **Rede**<br>Determinação de caminho e IP (endereçamento lógico) |
| | **Quadros** | **Enlace de Dados**<br>MAC e LLC (Endereçamento físico) |
| | **Bits** | **Físico**<br>Mídia, sinal e transmissão binária |

## Firewalls x SBCs: implicações para soluções de comunicações em tempo real

Os sistemas de comunicações empresariais são essenciais e precisam estar disponíveis 24 horas por dia, 7 dias por semana. Os profissionais de segurança da informação não podem se dar ao luxo de desligar e ligar tráfego em portas específicas sem esperar que uma empresa pare.

Na verdade, firewalls podem ser implantados como um servidor proxy de protocolo de iniciação de sessão (SIP, do inglês Session Initiation Protocol) e podem transmitir e controlar as informações de sinais SIP. No entanto, uma vez que o servidor não está envolvido ativamente no caminho de mídia de protocolo de transporte em tempo real (RTP, do inglês Real-Time Transport), não é possível controlar comunicações em tempo real de forma a assegurar conexões de voz e vídeo seguras e de qualidade.

Os SBCs, por outro lado, foram projetados especificamente para segurança e gestão de comunicações IP e proporcionam vantagens importantes para qualidade e segurança em RTC:

• Transcodificação de protocolos

• Visibilidade para indicadores-chave de desempenho (KPIs) de chamadas de voz e vídeo, como variação de sinal, latência, taxa de transferência e muito mais

• Controle dinâmico de políticas para aplicativos de comunicação

O principal problema com firewalls modernos para proteção de tráfego de comunicação é que foram projetados especificamente para ignorar fluxos em tempo real. Seus gateways de camada de aplicativo (ALGs, do inglês Application Layer Gateways) não são otimizados para tráfego de comunicação, o que significa que eles costumam interromper o fluxo de dados para qualquer coisa além de chamadas básicas. E fica pior: eles não são projetados para processar a criptografia de RTC. Dessa forma, se você estiver usando criptografia em seu tráfego de voz e vídeo, os firewalls não poderão proporcionar proteção contra intrusos, independentemente de quão avançado o dispositivo seja.

Em uma época na qual invasores percebem que um malware simples pode passar direto por uma rede se for enviado por uma porta de vídeo, as empresas não podem contar com firewalls modernos para proteger tráfego de comunicação de missão crítica. É aí que os SBCs entram em cena.

## Como os SBCs garantem a segurança de VoIP

Os SBCs vão além da conversão de endereço de rede e terminação de SIP simples. Eles estão amplamente envolvidos na sinalização de tráfego de comunicação e foram projetados para funcionar com todos os recursos avançados de voz e vídeo. Diferente dos firewalls, os SBCs atuam como pontos de demarcação de borda, o que significa que podem descriptografar tráfego para analisar a existência de atividade maliciosa sem interromper os fluxos em tempo real.

Contar com SBCs é essencial para a segurança e qualidade de tráfego único de comunicações. Diferentemente da maioria do tráfego de dados, fluxos de voz e vídeo são divididos em uma camada de sinalização e uma camada de mídia. Enquanto os firewalls são projetados para tráfego de fluxo único, os SBCs podem entender o contexto de camadas de sinalização e mídia para supervisionar o fluxo em tempo real.

Como resultado, os SBCs cuidam de cinco considerações importantes de segurança onde os firewalls não oferecem proteção:

• **Proteção contra ataques maliciosos:** Quando ataques de negação de serviço (DoS, do inglês Denial of Service) e DoS distribuído (DDoS, do inglês Distributed DoS) ocorrem, eles sobrecarregam as redes com tráfego malicioso em uma tentativa de derrubar sistemas e sondar fraquezas. Os SBCs podem separar facilmente tráfego VoIP de atividades maliciosas, permitindo que apenas tráfego de voz autorizado passe e descartando o resto. Os SBCs podem ajustar dinamicamente a alocação de recursos para isolar sistemas de comunicação contra quedas na qualidade de serviço (QoS, do inglês Quality of Service) que ocorram com picos de tráfego por DoS e DDoS.

• **Proteção contra fraudes de tarifas:** Um número crescente de hackers está invadindo sistemas de VoIP empresariais para direcionar chamadas internacionais de alto custo, o que pode levar a dezenas de milhares de dólares em cobranças. Com um SBC instalado, organizações podem programar a solução VoIP para negar tons de discagem secundária.
• **Criptografia:** É relativamente fácil interceptar mensagens de comunicação em tempo real. No entanto, de acordo com Zeus Kerravala, Analista Chefe na ZK Research: "Os SBCs usam o protocolo de camada de segurança [TLS] para proteger o tráfego de sinalização e torná-lo invisível aos hackers. Para proteger pacotes de mídia e adicionar outra camada de proteção, os SBCs usam o protocolo de transporte seguro e confiável [SRT]."
• **Ocultação de topologia:** A comunicação entre duas redes pode proporcionar a usuários não autorizados acesso à topologia de rede empresarial. Os SBCs eliminam esse risco ao ocultar a topologia nas comunicações.
• **Gestão de tráfego de IP:** Basicamente, SBCs limitam o número de sessões que podem ocorrer ao mesmo tempo. Assim como a proteção contra DDoS, a gestão de tráfego de IP assegura uma qualidade de serviço mitigando os efeitos que grandes volumes de chamadas podem ter no sistema como um todo.

## Conclusão: quando o assunto é segurança, ambos SBCs e firewalls são necessários

Conforme organizações de todos os portes implementam soluções de VoIP, assegurar a segurança e a qualidade precisa ser uma prioridade. Embora firewalls e SBCs pareçam realizar metas de segurança a princípio similares, suas diferenças no processamento de comunicações em tempo real corroboram que há diferenças significativas. As soluções de comunicações em tempo real possuem requisitos únicos. Até mesmo a menor interrupção no nível de rede pode levar a distorção de fala, chamadas de conferência com muita estaticidade, pixelização de vídeo e problemas de som.

Entender como firewalls e SBCs controlam o tráfego e implementam políticas de segurança é o primeiro passo para criar um design de rede que protege sistemas de comunicação vitais enquanto proporciona aos usuários os níveis de QoS necessários para realizar seus trabalhos diariamente. Sem um SBC funcionando com firewalls, os grupos de TI vão acabar respondendo continuamente a queixas de usuários e procurandoproblemas que podem ser extremamente de serem solucionados em longo prazo.

## Sobre a Ribbon Communications

A Ribbon é uma empresa com duas décadas de liderança em comunicações em tempo real. Fundada com base em tecnologia e propriedade intelectual de ponta, a Ribbon leva comunicações em tempo real integradas, seguras e inteligentes para o mundo moderno. Ela transforma redes fixas, móveis e empresariais de ambientes de legado em arquiteturas na nuvem e IP seguro, possibilitando comunicações altamente produtivas para consumidores e empresas. Com unidades em 28 países nos quatro cantos do mundo, o portfólio inovador e líder de mercado da Ribbon emprega provedores de serviço e empresas com criação rápida de serviço em um ambiente totalmente virtualizado. A Plataforma de Comunicações como um Serviço (CPaaS) Kandy da empres proporciona um conjunto vasto de recursos avançados e integrados de comunicações que possibilita essa transformação.

Para mais informações, acesse rbbn.com