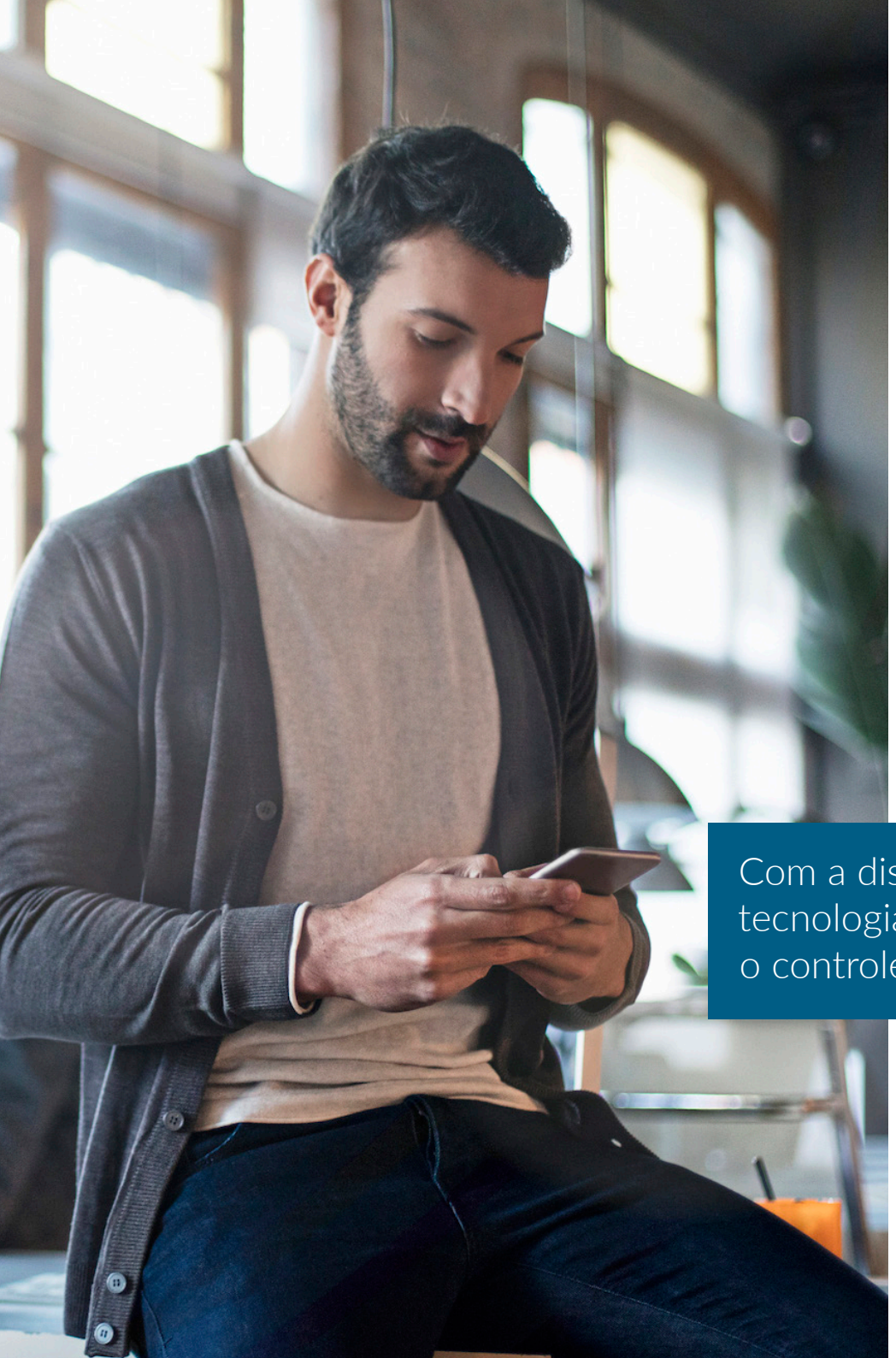
11 COISAS ÚTEIS QUE SEU FIREWALL DEVERIA FAZER

Vá além do bloqueio de ameaças de rede para proteger, gerenciar e controlar o tráfego de aplicações

SONICWALL®

Índice

SONICWALL®



O firewall amadureceu

Os firewalls tradicionais com inspeção dinâmica de pacotes concentram-se no bloqueio de ameaças na camada de rede, avaliando as portas e protocolos usados pelo tráfego na camada de rede. Os firewalls de Próxima Geração (NGFWs, next-generation firewalls) mais recentes utilizam a inspeção profunda de pacotes para examinar toda a carga de transmissão de dados do pacote e oferecer prevenção avançada de invasões, proteção contra malware, filtragem de conteúdo e proteção contra spam. Muitas aplicações são disponibilizadas pelas portas comuns de compartilhamento na Web e pelos protocolos HTTP ou HTTPS. Consequentemente, os firewalls tradicionais não conseguem examinar essas aplicações e tornam-se incapazes de priorizar um tráfego produtivo e seguro em lugar de um tráfego improdutivo e potencialmente inseguro. Os firewalls de Próxima Geração oferecem insight sobre as aplicações propriamente ditas, oferecendo um recurso importante aos profissionais de rede.

Com a disseminação da computação em nuvem e das tecnologias da Web 2.0, agora os firewalls têm outro desafio — o controle de aplicações.

SONICWALL®

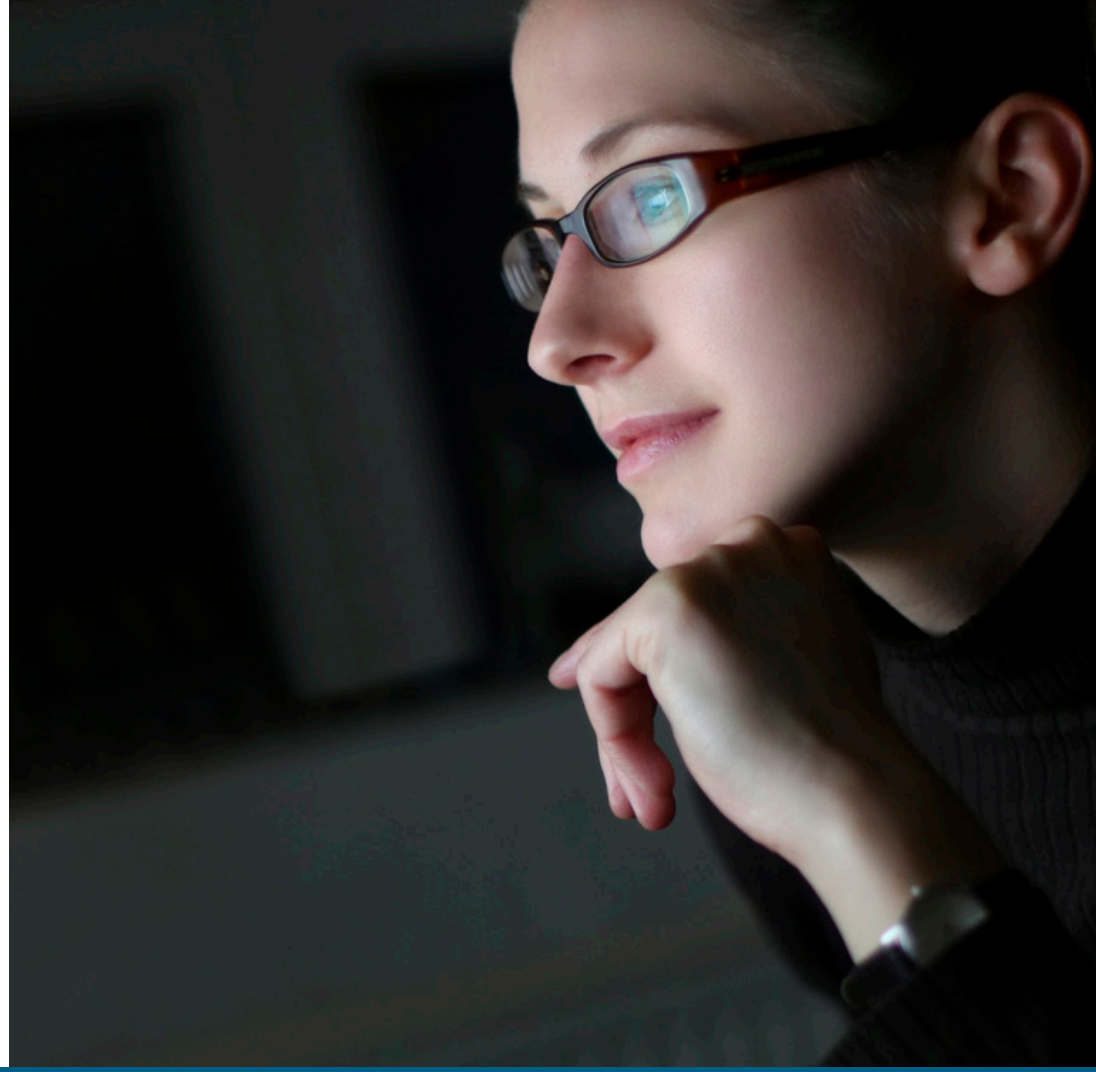
O que o SonicWall Application Intelligence and Control faz?

Com os firewalls da SonicWall, é possível identificar e controlar todas as aplicações em uso na rede. Esse controle adicional melhora a conformidade e prevenção de vazamento de dados por meio da identificação de aplicações com base em suas assinaturas exclusivas, em vez de portas ou protocolos. Isso é feito pela visualização do tráfego de aplicações para determinar padrões de uso e, em seguida, pela criação de políticas detalhadas para aplicações, usuários ou até mesmo grupos de usuários, bem como horário e outras variáveis, para um controle flexível que possa se adaptar a qualquer requisito de rede.

Atribuir largura de banda para aplicações críticas ou sensíveis a latência.

Como o SonicWall Application Intelligence and Controle funciona?

Com o uso de um amplo banco de dados de assinaturas de aplicações em crescimento constante e atualizado automaticamente, a SonicWall identifica aplicações com base em seu “DNA”, em vez de atributos menos exclusivos, como porta de origem, porta de destino ou tipo de protocolo. Por exemplo, é possível permitir mensagens instantâneas, mas bloquear a transferência de arquivos, ou permitir o acesso ao Facebook, mas bloquear o acesso a jogos do Facebook. Esses controles também estão disponíveis para todo o tráfego TLS/SSL criptografado, que deve ser inspecionado assim como conexões não criptografadas. E é possível visualizar os resultados dos seus controles facilmente, permitindo ajustar o uso de aplicações e otimizar a largura de banda da rede.



Controle categorias de aplicações, aplicações individuais e recursos específicos dentro das aplicações.

A visualização de aplicações permite “ver” quais navegadores estão sendo usados antes da criação da política.

1ª Utilidade:

Controlar as aplicações permitidas na rede

Você precisa ter certeza de que todos os seus funcionários estejam usando a última versão do Internet Explorer. Sua missão é garantir que todos os funcionários que usarem o IE9 ou IE10 sejam redirecionados automaticamente para o site de download do IE11 e restritos de qualquer outro acesso à Web. Estas são algumas soluções possíveis:

- Verificar fisicamente a versão do navegador da Web de cada sistema diariamente
- Criar um script personalizado para verificar automaticamente as versões de navegador
- Estabelecer uma política com o SonicWall Application Intelligence and Control — e parar de se preocupar

Crie uma política para redirecionar os usuários do IE9 ou IE10 para fazer o download da versão mais recente do navegador IE e bloquear o acesso à Internet do IE9 ou IE10

1. O mecanismo de Inspeção Profunda de Pacotes (DPI, Deep Packet Inspection) procura “User Agent = IE 9.0” ou “User Agent = IE 10.0” no cabeçalho HTTP
2. A política redireciona os usuários do IE9 ou IE10 para o site de download do IE11, bloqueando ao mesmo tempo o acesso do IE9 ou IE10 a todos os outros sites

SONICWALL®

2ª Utilidade:

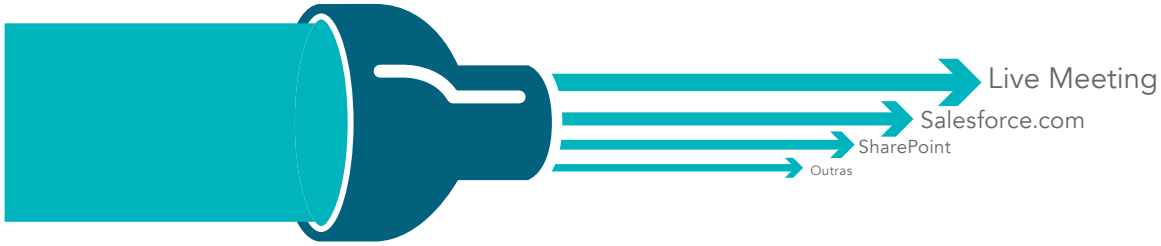
Gerenciar a largura de banda para aplicações críticas

Muitas aplicações críticas, como Live Meeting, Salesforce.com® e SharePoint®, são hospedadas na nuvem ou executadas em redes geograficamente dispersas. A garantia de que essas aplicações tenham prioridade sobre a navegação improdutiva na Web melhora a produtividade do negócio.®

Crie uma política para dar prioridade de largura de banda para a aplicação Live Meeting

1. O mecanismo de Inspeção Profunda de Pacotes procura a assinatura ou o nome da aplicação
2. Atribua à aplicação Live Meeting uma prioridade de largura de banda mais alta

A prioridade da aplicação pode se basear em datas (por exemplo, prioridade de final de trimestre para aplicações de vendas).



SONICWALL®

3ª Utilidade:

Bloquear aplicações peer-to-peer

Aplicações improdutivas peer-to-peer (P2P) como o BitTorrent são usadas com frequência para fazer o download de versões não licenciadas de conteúdo protegido por direitos autorais e podem consumir a largura de banda rapidamente ou transmitir malware. Entretanto, novas aplicações P2P, ou alterações simples (por exemplo, números de versão) nas aplicações P2P atuais, surgem o tempo todo; por isso, é difícil bloquear manualmente cada aplicação P2P.

A SonicWall atualiza constantemente a inteligência de aplicações e o banco de dados de controle para adicionar novas aplicações P2P assim que elas são disponibilizadas. De agora em diante, você pode simplesmente criar uma política para bloquear todas as aplicações P2P.

Crie uma política para bloquear o uso de aplicações P2P

1. O mecanismo de Inspeção Profunda de Pacotes usa assinaturas de aplicações P2P predefinidas da lista de assinaturas de aplicações
2. Escolha as aplicações P2P na lista de assinaturas predefinidas
3. Aplique a política a todos os usuários
4. Bloqueie as aplicações P2P por meio de restrições de largura de banda e horário

Lista de Assinaturas Aplicações

BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
BitTorrent-6.0.1
... e inúmeras outras

+

Lista de Assinaturas Aplicações

As atualizações da SonicWall são recebidas e aplicadas

=

Lista de Assinaturas Aplicações

BitTorrent-6.1.1
BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
... e inúmeras outras

Resultados

- Você pode gerenciar e controlar aplicações P2P
- Você não precisa gastar tempo atualizando regras de assinaturas de IPS

4ª Utilidade:

Bloquear componentes improdutivos das aplicações

As aplicações de redes sociais como Facebook, Instagram e YouTube tornaram-se novos canais de comunicação para as pessoas e empresas. Embora o bloqueio de todas as aplicações de redes sociais possa ser contraproducente, é necessário controlar como elas podem ser usadas no local de trabalho.

Por exemplo, você pode permitir que o pessoal de marketing atualize a página da empresa no Facebook, mas não permitir jogos do Facebook como Texas HoldEm Poker ou Candy Crush Saga. Com a inteligência e controle de aplicações, é possível criar uma política para permitir o acesso ao Facebook e bloquear jogos.

Crie uma política para permitir o Facebook, mas bloquear jogos do Facebook

1. Selecione “Todos” os usuários
2. Selecione a categoria “aplicações de jogos do Facebook”
3. Crie uma única regra para “Bloquear” o acesso de todos os usuários a jogos no Facebook

Você também pode permitir o chat, mas bloquear transferências de arquivos dentro do chat.

5ª Utilidade:

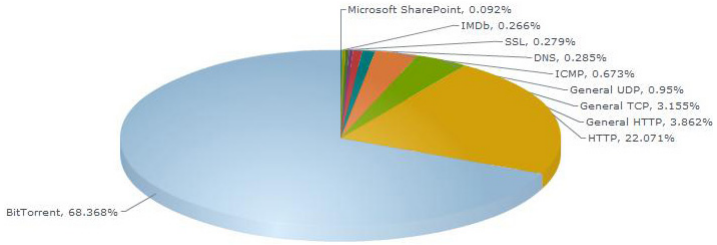
Visualizar o tráfego das aplicações

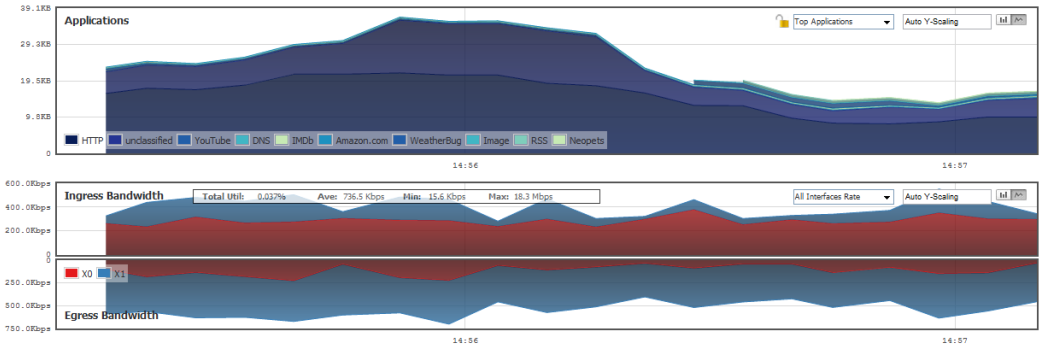
O que está acontecendo na rede? Quem está desperdiçando a largura de banda? Por que a rede está tão lenta? Você já fez alguma dessas perguntas? Você pode usar uma combinação de ferramentas distintas para tentar achar as respostas, mas esse processo é demorado e só revelará as informações após o ocorrido. Com a visualização do tráfego de aplicações em tempo real da SonicWall, é possível responder a essas perguntas imediatamente, diagnosticar problemas rapidamente, detectar inconformidade de uso de rede, criar políticas adequadas e ver imediatamente a eficácia dessas políticas.

Visualize todo o tráfego em tempo real, fazendo login no Monitor de Fluxo de Aplicações

1. Visualize gráficos em tempo real de todo o tráfego de aplicações
2. Visualize gráficos em tempo real da largura de banda de entrada e saída
3. Visualize gráficos em tempo real dos sites visitados e de toda a atividade dos usuários
4. Crie sua própria filtragem para obter as informações mais relevantes

A visualização dá aos administradores um feedback instantâneo sobre os fluxos de tráfego na rede.





SONICWALL

6ª Utilidade:

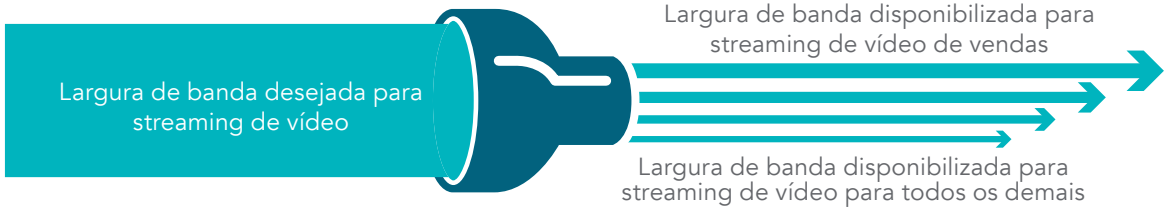
Gerenciar a largura de banda para um grupo de usuários

O que você faz quando seu CEO reclama de que os vídeos de notícias sobre negócios que ele quer ver pela manhã são instáveis e não são reproduzidos corretamente? Após uma investigação, constata que o problema é uma política de gerenciamento de largura de banda que você implementou em toda a empresa para todo o streaming de vídeo. Você poderia aliviar as restrições de largura de banda para todos, mas existe uma solução melhor: gerenciamento de largura de banda para grupos.

Crie uma política para excluir a equipe executiva do gerenciamento de largura de banda para streaming de vídeo

1. Escolha o grupo executivo importado do servidor do protocolo LDAP
2. O mecanismo de Inspeção Profunda de Pacotes usa assinaturas de aplicações de streaming de vídeo predefinidas da lista de assinaturas de aplicações
3. Aplique a restrição de largura de banda ao tráfego com esse cabeçalho

Muitas empresas descobriram que os funcionários ficam mais felizes quando você dá a eles pleno acesso à Web, mesmo com largura de banda reduzida para sites improdutivos.



SONICWALL

7ª Utilidade:

Bloquear ataques de ransomware e violações

A segurança da rede deve ser a prioridade do foco de todo administrador de TI. A capacidade de bloquear ataques, como ransomware e violações, gerados por malware e tentativas de invasão, protege a organização contra um grande risco e evita o potencial desperdício de recursos. Os serviços de segurança da SonicWall, em execução na arquitetura de alto desempenho e latência ultrabaixa dos firewalls de Próxima Geração da SonicWall, são capazes de impedir que milhões de ameaças conhecidas e desconhecidas entrem na rede antes que elas se tornem um perigo para sua organização. O SonicWall Capture estende os recursos de prevenção de ameaças do firewall por meio da detecção e prevenção de ataques desconhecidos e zero-day, com um serviço de sandboxing multimotor na nuvem.

Bloqueie ataques de malware e invasões antes que eles entrem na rede!

SONICWALL®

8ª Utilidade:

Identificar conexões por país

Uma conexão a um IP em um país estrangeiro feita em seu escritório local ou em uma filial é apenas uma conexão inofensiva de alguém que está navegando na Web ou é uma atividade de botnet? Você pode usar a identificação GeoIP de tráfego por país para identificar e controlar o tráfego na rede relacionado a países específicos, para proteger-se contra ataques de origens conhecidas ou suspeitas de atividades de ameaças ou para investigar o tráfego suspeito proveniente da rede.

Visualize conexões por país ou crie filtros específicos a um país

1. Verifique quais aplicações estão se conectando a IPs em outros países
2. Veja quais usuários e quais computadores estão se conectando a IPs em outros países
3. Crie filtros para restringir o tráfego para países especificados por você, com listas de exclusão

Depois de descobrir a resposta, você pode conversar com o usuário, inspecionar a máquina com o endereço IP ilícito ou ativar um utilitário de captura de pacotes no firewall para analisar exatamente o que está acontecendo nessa conexão. Com a identificação GeoIP de tráfego por país da SonicWall, é possível identificar e resolver problemas que de outra forma você poderia não tomar conhecimento.

9ª Utilidade:

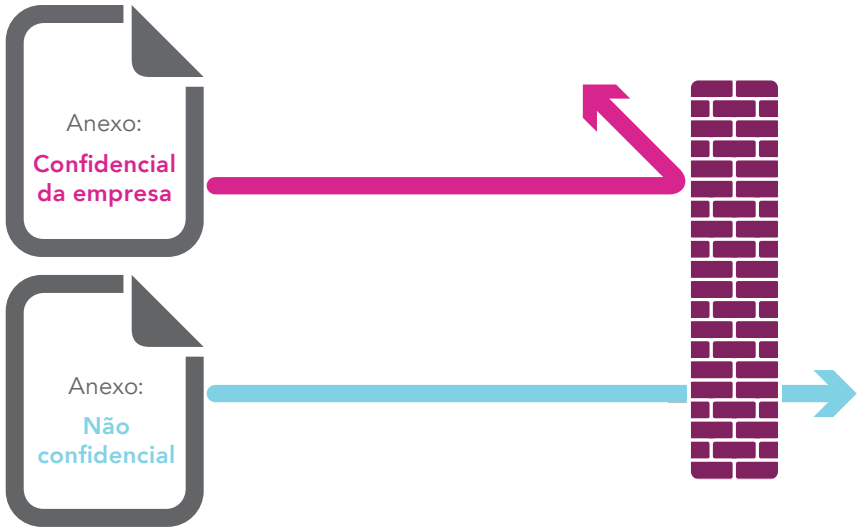
Prevenir vazamentos de dados por e-mail

Em algumas empresas, os e-mails enviados não passam pelo sistema de segurança de e-mail, ou o sistema não verifica o conteúdo dos anexos de e-mail. Em todo caso, os anexos "confidenciais da empresa" podem sair da organização facilmente. Como o envio de tráfego na rede passa pelo firewall, você pode detectar e bloquear esses "dados em movimento".

Crie uma política para bloquear anexos de e-mail identificados como "confidenciais da empresa"

O mecanismo de Inspeção Profunda de Pacotes procura:

1. Conteúdo de e-mail = "Confidencial da Empresa";
2. Conteúdo de e-mail = "Propriedade da Empresa"
3. Conteúdo de e-mail = "Propriedade particular", etc.



SONICWALL®

10ª Utilidade:

Prevenir vazamentos de dados por webmail

Agora, vamos supor que sua proteção contra spam atual possa detectar e bloquear um e-mail normal enviado com informações “confidenciais da empresa”. Porém, e se um funcionário usar um serviço de webmail, como o Yahoo® ou o Gmail®, para enviar informações “Confidenciais da Empresa”?

Crie uma política para bloquear anexos “confidenciais da empresa” no tráfego da Web

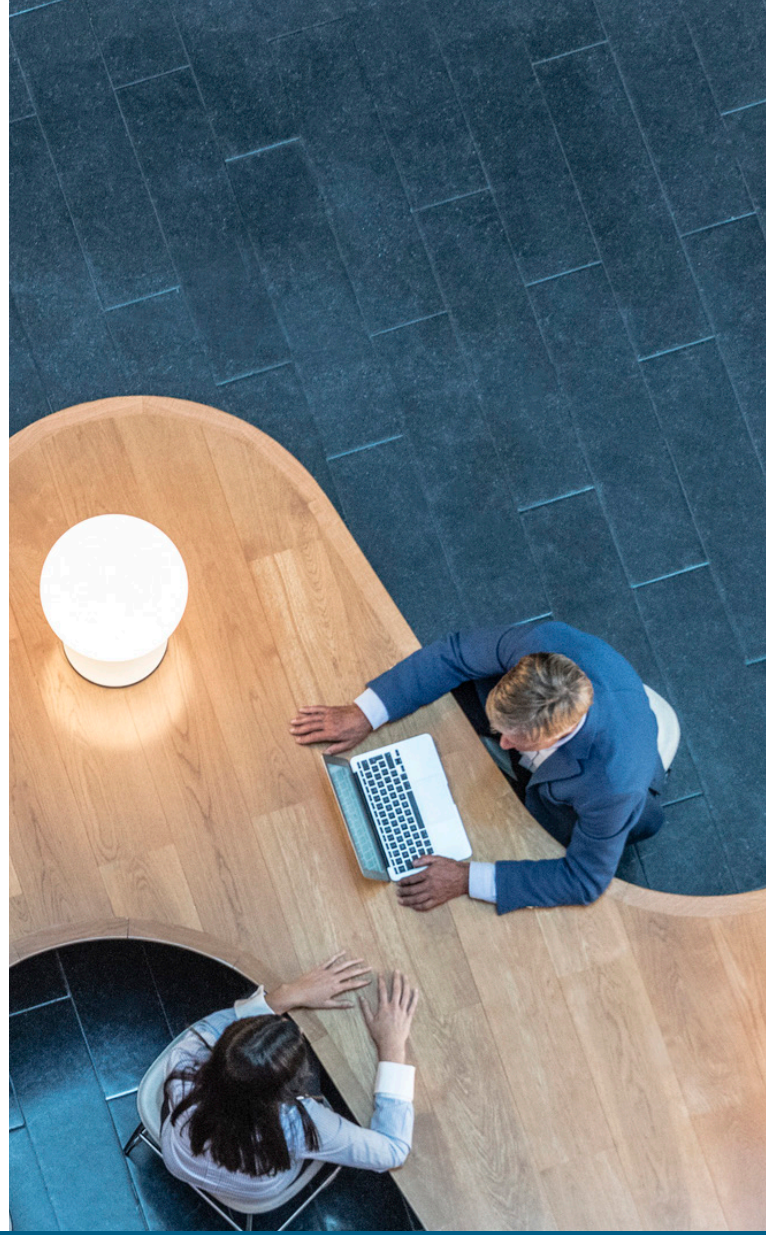
1. O mecanismo de Inspeção Profunda de Pacotes procura a identificação “confidencial da empresa” nos arquivos transferidos por HTTP ou HTTPS
2. Bloqueie a mensagem e notifique o remetente de que a mensagem é “confidencial da empresa”

SIGA

De: mocinho@sua_empresa.com
Para: mocinho@parceiro.com
Assunto: Aprovação do Cartão de Ponto de Jim
Aprovo as horas de seu cartão de ponto desta semana. Joe

PARE

De: vilão@sua_empresa.com
Para: vilão@concorrente.com
Assunto: Roadmap de projetos
ui está o Roadmapp
9 de janeiro – Versão 7.0
Este documento é **Confidencial da Empresa**



Isso também pode ser feito para conteúdo de FTP.

11ª Utilidade:

Gerenciar a largura de banda para o streaming de áudio e vídeo

O acesso ao streaming de vídeo de sites como o YouTube às vezes é útil, mas costuma ser exagerado. O bloqueio desses sites pode funcionar, mas uma abordagem preferível seria limitar a largura de banda total direcionada ao streaming de vídeo, independentemente da origem. Isso também se aplica a sites de streaming de áudio, como estações de rádio de música on-line e serviços de streaming de música, como Spotify e Apple Music. Esse tráfego não precisa necessariamente vir de sites conhecidos, mas também pode ser hospedado por blogs. Portanto, o objetivo é identificar o tráfego por aquilo que ele é, em vez de sua origem. A Inspeção Profunda de Pacotes se sobressai nesse processo.

Crie uma política para limitar o streaming de áudio e vídeo por uma lista de assinaturas predefinidas

1. Selecione as categorias de aplicações Streaming de Vídeo e Streaming de Áudio
2. Defina a largura de banda que você deseja alocar para essas categorias de aplicações (por exemplo, 10%)
3. Crie uma regra que obrigue o Streaming de Vídeo e o Streaming de Áudio a consumir no máximo 10% da largura de banda para todos (talvez excluindo alguns grupos de departamentos, como os integrantes do grupo de treinamento)
4. Opcionalmente, programe a regra para funcionar durante o horário comercial padrão, mas não no horário de almoço ou após as 18 horas
5. Confirme a eficácia da nova política com a visualização em tempo real, fazendo login no Monitor de Fluxo de Aplicações

SONICWALL®

Quando você soma tudo isso

Plataforma de alto desempenho
+ Inspeção profunda de pacotes
+ Prevenção de invasões
+ Inteligência, controle e visualização de aplicações

Firewalls de Próxima Geração da SonicWall

Segurança, desempenho e controle

SONICWALL®

Quem Somos

A SonicWall luta contra a indústria do cibercrime há mais de 27 anos, protegendo empresas de pequeno e médio porte e empresas no mundo todo. Nossa combinação de produtos e parcerias viabilizou soluções automatizadas em tempo real de detecção e prevenção de violações sintonizadas às necessidades específicas de mais de 500 mil empresas em mais de 215 países e territórios, para que possam fazer mais negócios com menos relutâncias. Para obter mais informações, acesse www.sonicwall.com ou siga-nos no Twitter, LinkedIn, Facebook e Instagram.

Em caso de dúvidas sobre o possível uso deste material, escreva para:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Consulte nosso website para obter informações adicionais.
www.sonicwall.com

Ebook-11CoolThings-Firewall-US-VG-MKTG5084

SONICWALL