SONICWALL

# RESUMO DE SOLUÇÃO: MELHORES PRÁTICAS PARA OBTER ACESSO MÓVEL SEGURO

**Mantenha-se operacional, independentemente do que esteja nas notícias amanhã.**

## Resumo

Fornecer suporta às metas organizacionais para o espaço de trabalho digital de hoje exige acesso móvel seguro, mas existem obstáculos no caminho para equilibrar segurança, acesso, desempenho e valor. As práticas recomendadas para implementar efetivamente uma força de trabalho móvel protegida incluem a manutenção de alta segurança, conectividade, desempenho robusto e baixo custo total de propriedade. Este Resumo de Solução detalha as etapas para alcançar essas práticas recomendadas.

### Introdução

Seja para garantir a continuidade dos negócios ou melhorar a retenção e a produtividade da força de trabalho, mais organizações estão adotando mobilidade, trabalho remoto e tempo flexível para seus funcionários. Para atingir as metas de negócios com uma força de trabalho móvel e remota, ter um serviço de segurança de acesso robusto e confiável nunca foi tão crítico. Um elemento essencial para garantir o acesso móvel confiável é manter as atualizações de segurança, mas a manutenção pode prejudicar o serviço e o desempenho.

As organizações precisam manter um ambiente de trabalho flexível sem perder a acessibilidade. Mas, implantar um serviço altamente acessível pode ser complexo, caro e demorado.

### Uma cibersegurança eficaz deve incluir acesso móvel seguro

Fornecer acesso móvel no mundo de hoje em qualquer lugar / a qualquer hora, hiper-distribuído, aumenta os pontos de exposição em uma infinidade de dispositivos móveis potencialmente inseguros.
A falibilidade humana e os riscos online fazem com que os funcionários não consigam garantir a segurança de seus próprios dispositivos móveis.
Além disso, a variedade de tipos de ameaças está se expandindo, se aprofundando e ficando mais inteligentes, incluindo ransomware direcionado, ameaças nunca antes vistas, malware baseado na memória, ataques de canal lateral e ameaças criptografadas.
Por fim, a segurança da sua rede móvel deve corresponder à da sua rede com fio.

Mantenha-se operacional, independentemente do que esteja nas notícias amanhã.

**Melhores Práticas: Simples, seguro e mobilidade ágil**

Para ser eficaz, a cibersegurança deve fornecer aos funcionários móveis acesso fácil e seguro 24 horas por dia, 7 dias por semana, aos principais recursos comerciais, de maneira ágil, fácil de usar, econômica e escalável.

Isso requer uma postura zero-trust em relação a qualquer dispositivo móvel que tente se conectar aos recursos corporativos, estejam eles no local ou na nuvem. O acesso móvel seguro é um componente essencial de uma abordagem zero-trust para acesso a qualquer lugar e a qualquer hora.

A TI também deve proteger o acesso desses endpoints móveis com orçamentos limitados e recursos de equipe qualificados.

Isso significa otimizar a implantação, a disponibilidade e o suporte, para reduzir o custo total de propriedade.

**SonicWall Secure Mobile Access**

A Solução SonicWall Secure Mobile Access (SMA) permite acesso em qualquer lugar, a qualquer hora, em empresas hiper-distribuídas. Isso dá à sua empresa a agilidade para permanecer operacional, independentemente do que será apresentado nas notícias futuras.

O SonicWall SMA 1000 Series fornece às corporações distribuídas acesso remoto seguro abrangente de ponta a ponta a recursos corporativos hospedados em datacenters om-prem, na nuvem e híbridos.Aplica identidade, controle de acesso impostos por política, autenticação do dispositivo com reconhecimento de contexto e VPN no nível da aplicação para conceder acesso aos dados, recursos e aplicações após estabelecer a identidade e a confiança do usuário e do dispositivo. Implantado de forma flexível como um dispositivo Linux reforçado ou virtual em nuvens privadas no ESXi ou Hyper-V ou em ambientes de nuvem pública da AWS ou Microsoft Azure. Ele suporta até 20.000 conexões simultâneas com uma única unidade e aumenta a escala de centenas de milhares de usuários por meio de cluster horizontal.

SMA simplifica as iniciativas de trabalho flexível da sua empresa com:

- VPN sempre ativa
- Login único (SSO) usando o provedor de identidade SAML
- Alta Disponibilidade
- Autentificação de Multifator (MFA)
- Capture Advanced Threat Protection (ATP) sandboxing
- Suporte TLS 1.3
- Implantação flexível e escalável
- Gerenciamento Centralizado
- Baixo TCO

## Conclusão

As práticas recomendadas para segurança móvel incluem controle de acesso zero-trust, confiabilidade perfeita e baixo custo total de propriedade. Felizmente, existe uma solução viável para ajudá-lo a implementar todas essas práticas recomendadas.

Para saber como você pode ter mais sucesso em manter um ambiente de segurança de acesso saudável e, ao mesmo tempo, se manter londe da inatividade, visite www.sonicwall.com/pt-br/products/secure-mobile-access.

## Sobre SonicWall

A SonicWall vem lutando contra a indústria do crime cibernético há mais de 29 anos, defendendo empresas de pequeno e médio portes, grandes corporações e órgãos governamentais no mundo todo. Respaldadas pela pesquisa do SonicWall Capture Labs, nossas premiadas soluções de detecção e prevenção de violações em tempo real protegem mais de um milhão de redes e seus e-mails, aplicações e dados em mais de 215 países e territórios. Essas organizações operam com mais eficácia e com menos receios quanto à segurança. Para obter mais informações, acesse visite www.sonicwall.com ou no sita no Twitter, LinkedIn, Facebook e Instagram.

Se você tiver alguma dúvida sobre o uso potencial deste material, entre em contato com:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Consulte o nosso site para obter informações adicionais.
**www.sonicwall.com**