RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 01/10/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

Arquiteturas de conectividade para pmes: segmentação de redes, vpns, virtualização e disponibilidade operacional

Connectivity Architectures for smes: Network Segmentation, vpns, Virtualization and Operational Availability

Arquitecturas de conectividad para pymes: segmentación de red, VPN, virtualización y disponibilidad operativa

Guilherme Gallo Zazeri

Profissional de Tecnologia da Informação, consultor e empreendedor em infraestrutura, conectividade e soluções tecnológicas, com mais de 25 anos de trajetória profissional.

Resumo

Redes corporativas de pequenas e médias empresas passaram a sustentar acesso a aplicações locais e em nuvem, trabalho remoto, telefonia IP, serviços virtualizados e comunicação entre unidades. Este artigo examina princípios de arquitetura para conectividade segura e disponível, abordando segmentação, firewalls, redes sem fio, VPNs, redundância de links, virtualização e documentação. A pesquisa utiliza revisão narrativa estruturada de livros clássicos de redes, publicações do NIST e dados do Verizon Data Breach Investigations Report. Os resultados mostram que desempenho e segurança não devem ser tratados como objetivos concorrentes: uma arquitetura coerente reduz superfície de exposição, limita propagação de falhas, melhora diagnóstico e cria condições para recuperação. Para PMEs, a padronização e a simplicidade operacional são especialmente relevantes porque ambientes excessivamente complexos podem ampliar custos e dependência de especialistas.
Palavras-chave: redes corporativas; conectividade; VPN; firewall; virtualização; pequenas e médias empresas; disponibilidade.

Abstract

Corporate networks in small and medium-sized enterprises now support access to local and cloud applications, remote work, IP telephony, virtualized services, and communication between locations. This article examines architectural principles for secure and available connectivity, addressing segmentation, firewalls, wireless networks, VPNs, link redundancy, virtualization, and documentation. The study uses a structured narrative review of established networking textbooks, NIST publications, and data from the Verizon Data Breach Investigations Report. Findings indicate that performance and security should not be treated as competing objectives: coherent architecture reduces exposure, limits failure propagation, improves troubleshooting, and creates conditions for recovery. For SMEs, standardization and operational simplicity are particularly relevant because unnecessarily complex environments can increase costs and dependence on specialists.
Keywords: corporate networks; connectivity; VPN; firewall; virtualization; small and medium-sized enterprises; availability.

Introdução

Redes corporativas deixaram de conectar apenas computadores dentro de um escritório. Hoje integram aplicações em nuvem, servidores virtualizados, telefonia IP, dispositivos sem fio, filiais e profissionais remotos. Tanenbaum e Wetherall (2021) mostram que a comunicação em rede é construída por camadas e protocolos interdependentes, característica que torna o desenho arquitetural decisivo para desempenho e confiabilidade.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 01/10/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

A expansão da conectividade amplia também a superfície de exposição. O Verizon DBIR 2025 identificou que, entre pequenas organizações consideradas no relatório, System Intrusion, Social Engineering e Basic Web Application Attacks responderam conjuntamente por 96% das violações. O dado demonstra que redes e acessos não podem ser administrados apenas sob a ótica de disponibilidade.

Este artigo analisa seis dimensões da arquitetura de conectividade para PMEs: desenho e segmentação, firewalls, VPNs, redundância, virtualização e documentação. A discussão procura mostrar como princípios técnicos consolidados podem ser aplicados sem pressupor estruturas equivalentes às de grandes corporações.

2. Metodologia

A pesquisa adota revisão narrativa estruturada, reunindo literatura de redes de computadores, segurança de perímetro, acesso remoto, virtualização e gestão de riscos.

Foram utilizados Tanenbaum e Wetherall (2021), Kurose e Ross (2021) e Stallings (2016) como bases conceituais de arquitetura, protocolos, desempenho e redes modernas.

As recomendações de segurança foram confrontadas com NIST SP 800-41 Rev. 1, NIST SP 800-46 Rev. 2, NIST CSF 2.0 e o guia do NIST para pequenos negócios.

O Verizon DBIR 2025 foi incorporado como fonte empírica sobre padrões de violações, com atenção específica ao recorte de pequenas organizações apresentado pelo relatório.

A análise não avalia marcas comerciais. Tecnologias de firewall, Wi-Fi, hipervisores e túneis são discutidas por função arquitetural, de modo a preservar neutralidade e aplicabilidade.

Os resultados foram organizados em seis eixos. Cada eixo considera disponibilidade, segurança, capacidade de manutenção e adequação ao porte da organização.

3.1 Desenho de rede e segmentação lógica

Tanenbaum e Wetherall (2021) explicam que redes são compostas por sistemas interligados cuja organização influencia desempenho e confiabilidade. Em empresas, o desenho precisa refletir funções distintas, como usuários, servidores, telefonia, visitantes e dispositivos especializados.

A segmentação lógica permite separar grupos de ativos e controlar a comunicação entre eles. Em vez de uma rede plana, na qual todos os dispositivos compartilham amplo alcance, segmentos reduzem a propagação de falhas e limitam caminhos desnecessários.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 01/10/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

Kurose e Ross (2021) destacam a importância do encaminhamento e das políticas que determinam como fluxos atravessam a rede. Em contexto corporativo, essas decisões devem ser documentadas e associadas a necessidades reais de comunicação.

Segmentar não significa criar complexidade ilimitada. Cada divisão adicional aumenta a necessidade de regras, testes e diagnóstico. Para PMEs, o equilíbrio entre isolamento e o administrativo é parte do desenho.

Redes sem fio também precisam integrar a arquitetura. A separação entre acesso corporativo e visitantes, por exemplo, evita que conveniência de conectividade resulte em exposição desnecessária de recursos internos.

Uma arquitetura bem segmentada cria uma base para políticas de firewall, monitoramento e resposta. O desenho da rede passa a expressar regras de negócio, e não apenas a disposição física dos equipamentos.

3.2 Firewalls e políticas de controle de tráfego

Firewalls atuam como pontos de aplicação de políticas entre redes ou zonas de confiança diferentes. Scarfone e Hoffman (2009), no NIST SP 800-41 Rev. 1, tratam política de firewall como parte essencial do planejamento e da administração desses controles.

A efetividade depende da qualidade das regras. Permissões acumuladas ao longo dos anos podem criar exceções cujo propósito já não existe. Revisões periódicas ajudam a remover regras obsoletas e reduzir exposição.

O princípio de permitir apenas o necessário é particularmente útil. Serviços publicados, portas abertas e acessos administrativos devem corresponder a uma necessidade identificada, com origem e destino definidos.

Logs de firewall fornecem evidências para diagnóstico e investigação, mas seu volume exige critérios. Eventos relevantes precisam ser retidos e analisados de forma compatível com o risco e a capacidade da equipe.

Firewalls também participam de funções de conectividade, como NAT, VPN e failover. Essa concentração torna a documentação de configurações e cópias de segurança do equipamento parte da continuidade operacional.

Portanto, o firewall não deve ser tratado como dispositivo que torna a rede automaticamente segura. Seu valor depende de arquitetura, regras, manutenção e monitoramento.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 01/10/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

3.3 VPNs e conectividade entre unidades e profissionais remotos

Acesso remoto e interligação de unidades exigem canais que protejam dados em trânsito e controlem quem pode alcançar recursos internos. Souppaya e Scarfone (2016), no NIST SP 800-46 Rev. 2, discutem segurança de teletrabalho e acesso remoto como combinação de tecnologias, políticas e gestão.

VPNs podem estabelecer túneis entre sites ou conectar usuários individuais. A escolha depende de topologia, aplicação, desempenho e modelo de autenticação.

Criptografia do túnel protege o tráfego, mas não resolve sozinha o risco do endpoint. Um dispositivo comprometido que possui acesso autorizado pode transportar ameaças para dentro da rede.

Por isso, o desenho de acesso remoto deve aplicar privilégio compatível com a função. Nem todo usuário remoto precisa alcançar todos os segmentos ou serviços.

A disponibilidade também precisa ser considerada. Dependência de um único link, equipamento ou serviço de autenticação pode transformar o acesso remoto em ponto de interrupção.

VPNs são, portanto, componentes de uma arquitetura maior. Segurança depende da combinação entre identidade, segmentação, atualização, monitoramento e regras de acesso.

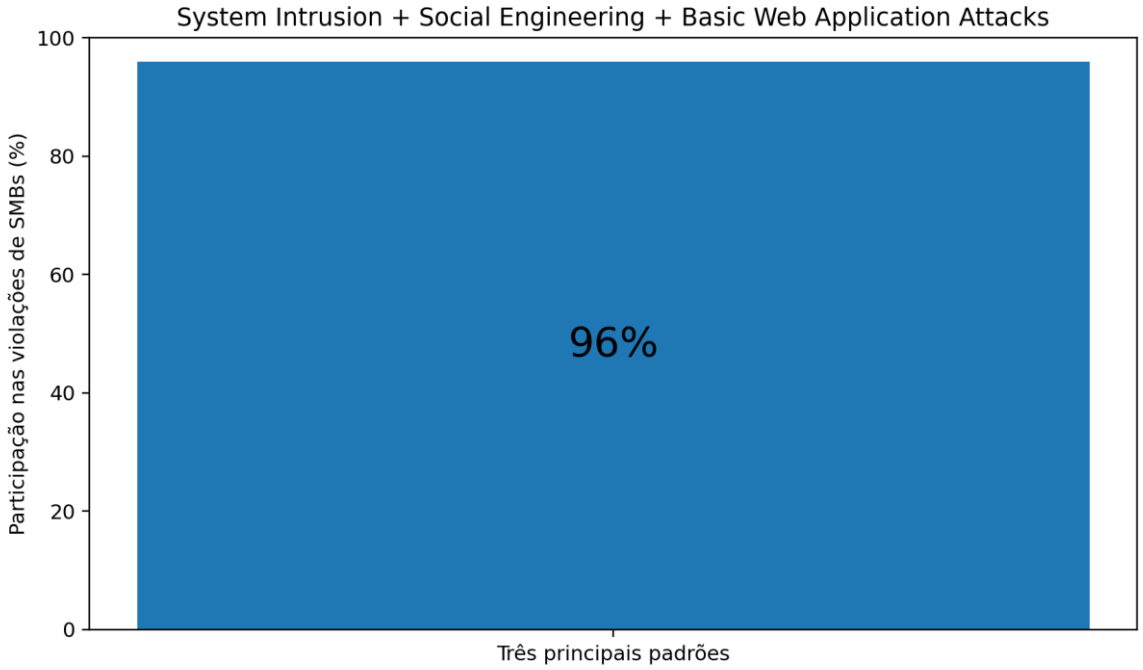

Figura 1. Participação conjunta dos três principais padrões de violações em pequenas organizações: System Intrusion, Social Engineering e Basic Web Application Attacks. Fonte: elaboração própria com base em Verizon (2025).

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 01/10/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

3.4 Redundância de links e continuidade da conectividade

Conectividade externa tornou-se dependência crítica para empresas que utilizam SaaS, e-mail em nuvem, telefonia IP e trabalho remoto. Uma falha de internet pode interromper múltiplos serviços simultaneamente.

Redundância de links reduz essa dependência quando provedores, rotas e equipamentos são planejados para evitar um ponto único de falha. A existência de dois contratos, porém, não garante independência física ou lógica.

Balanceamento de carga e failover possuem objetivos diferentes. O primeiro distribui tráfego; o segundo procura manter serviço quando um caminho deixa de funcionar. A arquitetura deve deixar claro qual comportamento é esperado.

Testes são necessários porque a troca automática pode falhar por DNS, sessão, roteamento ou dependência de endereço público. A disponibilidade precisa ser observada do ponto de vista da aplicação.

Telefonia IP evidencia esse desafio. Mesmo que o PABX permaneça operacional, perda de conectividade com troncos externos pode impedir chamadas. Kurose e Ross (2021) mostram como aplicações em tempo real são sensíveis a atraso, perda e disponibilidade de rede.

Redundância eficaz, portanto, depende de diversidade, configuração, teste e monitoramento. Duplicar componentes sem validar o caminho completo pode criar apenas uma aparência de resiliência.

3.5 Virtualização e consolidação de servidores

A virtualização separa a execução lógica de sistemas do hardware físico subjacente. Stallings (2016) relaciona virtualização à evolução de infraestruturas modernas, nas quais recursos computacionais podem ser abstraídos e administrados com maior flexibilidade.

Para PMEs, consolidar cargas pode reduzir quantidade de equipamentos e facilitar provisionamento. Máquinas virtuais podem ser copiadas, migradas e organizadas de maneira diferente de servidores exclusivamente físicos.

A consolidação também concentra risco. Quando múltiplos serviços dependem do mesmo host, uma falha física pode afetar várias funções. Capacidade, armazenamento, energia e estratégia de recuperação precisam acompanhar a densidade de cargas.

Virtualização não substitui backup. Snapshots podem apoiar manutenção ou reversão de curto prazo, mas não devem ser confundidos automaticamente com uma estratégia independente de proteção e retenção.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 01/10/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

A padronização do ambiente facilita suporte. Templates, nomenclatura, documentação e critérios de alocação tornam mudanças mais previsíveis e reduzem configurações improvisadas.

Assim, a virtualização produz valor quando integra capacidade, continuidade e governança. O objetivo não é maximizar o número de máquinas por host, mas obter uma infraestrutura administrável e recuperável.

3.6 Monitoramento, documentação e diagnóstico operacional

Redes complexas produzem sinais em roteadores, firewalls, pontos de acesso, servidores e aplicações. Monitoramento converte parte desses sinais em informação operacional, permitindo reconhecer indisponibilidade, saturação e comportamento anômalo.

Tanenbaum e Wetherall (2021) mostram que problemas de rede podem surgir em diferentes camadas. Diagnóstico eficiente exige distinguir falha física, endereçamento, roteamento, resolução de nomes, transporte e aplicação.

Documentação reduz o tempo necessário para essa investigação. Diagramas, inventários, endereçamento, regras essenciais e dependências ajudam a reconstruir o caminho do tráfego.

O Verizon DBIR 2025 reforça a relevância de manter visibilidade sobre o ambiente. No recorte de pequenas organizações, três padrões — System Intrusion, Social Engineering e Basic Web Application Attacks — representaram 96% das violações.

Esse dado não significa que todo incidente seja causado por arquitetura de rede. Ele demonstra, porém, que conectividade, sistemas e identidade estão inseridos em um cenário no qual exposição e acesso precisam ser observados continuamente.

Monitoramento e documentação completam o ciclo arquitetural. Uma rede bem desenhada, mas não observável ou compreensível por quem a administra, perde parte importante de sua capacidade de permanecer disponível e segura.

3.7 Telefonia IP, qualidade de serviço e convergência de comunicações

A convergência de voz e dados alterou o papel da rede corporativa. Sistemas de telefonia IP compartilham infraestrutura com aplicações, acesso à internet e serviços internos, fazendo com que uma degradação de conectividade possa afetar simultaneamente comunicação e sistemas de negócio.

Kurose e Ross (2021) explicam que aplicações em tempo real apresentam requisitos próprios de atraso, variação de atraso e perda de pacotes.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 01/10/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

Em uma rede sem critérios de priorização, tráfego volumoso pode disputar recursos com chamadas de voz. A percepção do usuário é imediata: atrasos, cortes e perda de inteligibilidade. A gestão de qualidade de serviço procura tratar essa diferença de sensibilidade sem presumir que toda aplicação necessita do mesmo comportamento da rede.

Stallings (2016) relaciona Quality of Service e Quality of Experience à evolução das redes modernas. Em ambientes corporativos, isso significa que métricas técnicas precisam ser interpretadas a partir do efeito sobre a atividade: uma conexão pode estar disponível e, ainda assim, oferecer experiência inadequada para voz ou videoconferência.

A telefonia IP também amplia a importância da segmentação. Separar logicamente dispositivos e fluxos de voz pode facilitar aplicação de políticas, diagnóstico e controle de broadcast. A decisão, contudo, deve permanecer compatível com a capacidade de administração da equipe.

Outro aspecto é a dependência externa. Troncos SIP, DNS, internet e energia podem integrar a cadeia de funcionamento da telefonia. Redundância precisa considerar essas relações; manter o PABX ativo não resolve uma indisponibilidade se a rota externa necessária às chamadas permanecer inacessível.

A documentação torna-se particularmente relevante em ambientes com grande quantidade de ramais. Numeração, grupos, rotas, regras de entrada e saída e dependências de operadora precisam ser registradas para que alterações e incidentes possam ser tratados com previsibilidade.

A convergência também muda o diagnóstico. Problemas percebidos como falhas de telefonia podem ter origem em perda de pacotes, saturação, DNS, roteamento, firewall ou configuração do endpoint. Tanenbaum, Feamster e Wetherall (2021) mostram por que uma análise por camadas continua útil mesmo em arquiteturas modernas.

Assim, telefonia IP não deve ser administrada como sistema isolado. Ela integra a arquitetura de conectividade e precisa compartilhar os mesmos princípios de disponibilidade, segmentação, monitoramento, documentação e recuperação aplicados ao restante da infraestrutura.

3.8 Padronização arquitetural e escalabilidade em ambientes distribuídos

Empresas que crescem por novas unidades, trabalho remoto ou adoção de serviços em nuvem enfrentam um problema adicional: configurações criadas caso a caso tendem a produzir ambientes difíceis de manter. A padronização reduz variações desnecessárias e cria referências para implantação e diagnóstico.

Padronizar não significa tornar todas as unidades idênticas. Significa estabelecer princípios repetíveis para endereçamento, segmentação, acesso remoto, nomenclatura, registros, atualização e cópias de

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 01/10/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

configuração. Kurose e Ross (2021) mostram que a previsibilidade do comportamento da rede depende de regras claras de encaminhamento e comunicação.

Templates e checklists podem reduzir omissões durante novas implantações. Em redes distribuídas, a repetição disciplinada de critérios também facilita comparar desempenho entre locais e identificar desvios.

O NIST CSF 2.0 (PASCOE; QUINN; SCARFONE, 2024) enfatiza que resultados de segurança devem ser compreendidos, priorizados e comunicados. Uma arquitetura padronizada facilita esse processo porque permite associar controles a padrões conhecidos em vez de reconstruir o ambiente a cada avaliação.

Escalabilidade inclui capacidade de operação humana. Uma solução que exige intervenção artesanal para cada novo usuário, túnel ou unidade pode funcionar em pequena escala e tornar-se insustentável com o crescimento. Automação e padronização devem ser avaliadas também por esse efeito.

A documentação padronizada reduz ainda a dependência do profissional que realizou a implantação original. Quando topologia, regras e parâmetros essenciais seguem um modelo comum, outros integrantes conseguem compreender o ambiente com menor custo de transição.

Por fim, padronização cria uma base mais segura para inovação. Novas tecnologias podem ser avaliadas sobre uma arquitetura conhecida, permitindo comparar benefícios e riscos sem introduzir mudanças simultâneas em todas as camadas.

Escalar conectividade, portanto, não é apenas adicionar equipamentos e links. É preservar compreensibilidade, segurança e capacidade de manutenção à medida que a rede se torna maior e mais distribuída.

Conclusão

A conectividade de uma PME sustenta serviços que antes eram independentes e, por isso, precisa ser tratada como arquitetura crítica.Segmentação ajuda a organizar fluxos e limitar exposição, desde que o nível de complexidade permaneça administrável.Firewalls são mecanismos de aplicação de política; sua eficácia depende da qualidade e da manutenção das regras, não apenas da presença do equipamento.VPNs ampliam mobilidade e integração entre unidades, mas precisam ser combinadas com identidade, privilégio e segurança dos dispositivos.Redundância de links deve ser testada pelo caminho completo da aplicação. Dois circuitos não representam continuidade se compartilham dependências ocultas.A virtualização oferece flexibilidade e consolidação, ao mesmo tempo em que exige atenção à concentração de cargas, capacidade e recuperação.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 01/10/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

Monitoramento e documentação tornam a arquitetura observável e reduzem o tempo de diagnóstico, além de diminuir dependência de conhecimento individual.Conclui-se que redes resilientes para PMEs são construídas pela combinação de simplicidade, segmentação, controles de acesso, redundância proporcional e operação disciplinada. O desenho técnico ganha valor quando permanece compreensível, testável e sustentável ao longo do tempo.

Referências

TANENBAUM, Andrew S.; FEAMSTER, Nick; WETHERALL, David J. Computer Networks. 6. ed. Harlow: Pearson, 2021.
KUROSE, James F.; ROSS, Keith W. Computer Networking: A Top-Down Approach. 8. ed. Hoboken: Pearson, 2021.
STALLINGS, William. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Boston: Addison-Wesley, 2016.
PASCOE, Cherilyn; QUINN, Stephen; SCARFONE, Karen. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg: National Institute of Standards and Technology, 2024.
ELIOT, Daniel. NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide. NIST SP 1300. Gaithersburg: National Institute of Standards and Technology, 2024.
VERIZON. 2025 Data Breach Investigations Report. Basking Ridge, 2025.
SCARFONE, Karen; HOFFMAN, Paul. Guidelines on Firewalls and Firewall Policy. NIST SP 800-41 Rev. 1. Gaithersburg: National Institute of Standards and Technology, 2009.
SOUppAYA, Murugiah; SCARFONE, Karen. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security. NIST SP 800-46 Rev. 2. Gaithersburg: National Institute of Standards and Technology, 2016.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.