DIGITRIX - SOLUÇÕES EM TI

INFRAESTRUTURA DE TI

O básico para empreendedores

Digitrix®
Soluções em TI

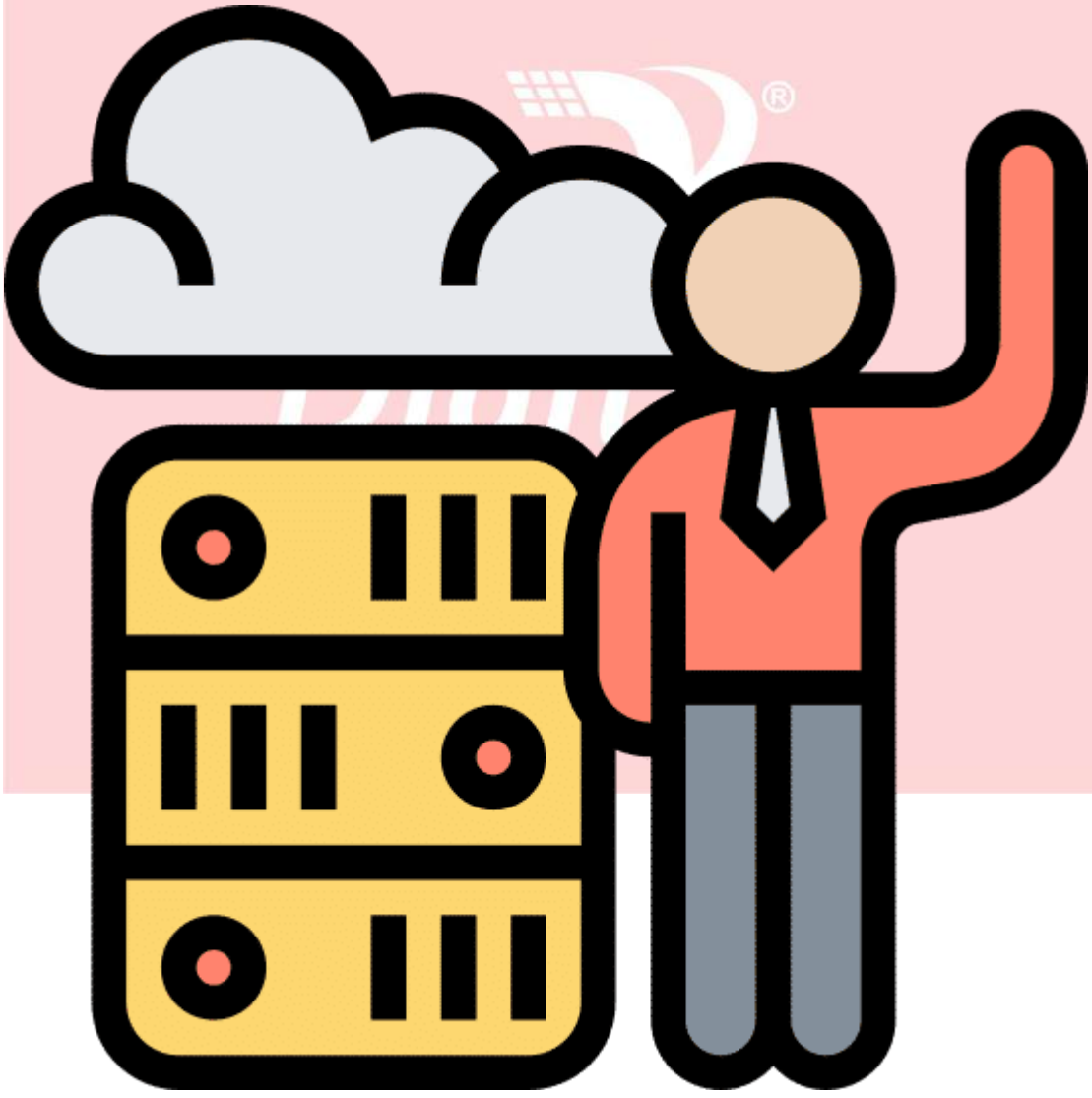
Conteúdo

Introdução

A sustentabilidade e o desempenho da infraestrutura de TI estão na agenda de muitas empresas. A dependência do sucesso da empresa na função e disponibilidade dos sistemas de TI é grande demais para que esse problema seja ignorado a longo prazo com impunidade.

Mas nem todos os empreendedores e tomadores de decisão também são especialistas em TI e podem encontrar o caminho dos inúmeros termos técnicos usados no setor de TI.

Com este ebook, gostaríamos de fornecer uma visão geral dos componentes mais importantes de uma infraestrutura de TI moderna. E com o mínimo de termos técnicos possíveis e explicados da forma mais clara possível. Dividimos o tópico da infraestrutura de TI em 6 áreas principais.



Acesso à Internet, largura de banda e email

Atualmente, os sistemas de TI que não estão conectados à Internet são dificilmente imagináveis. Sem a Internet, não há serviços em nuvem, downloads de dados, acesso remoto pelos funcionários e, certamente, nenhum e-mail.

É fácil ter a impressão de que as conexões de Internet de alto desempenho estão quase completamente disponíveis no Brasil, mas infelizmente isso está longe de ser o caso.

Não apenas em muitas regiões rurais, mas também em áreas metropolitanas supostamente bem desenvolvidas, ainda existem muitos pontos negros nos mapas de suprimentos.

Conexão com a Internet

Tenha cuidado: as informações de velocidade aqui são sempre "até" e indicam a velocidade máxima durante o download. As velocidades de upload e download que podem ser alcançadas em operação normal dependem de como e por quanto a respectiva linha é usada.

A velocidade de upload também é importante para todos os usuários de serviços em nuvem e geralmente é apenas um quinto ou um décimo da velocidade de download.

A largura de banda define o limite

A largura de banda disponível é um fator limitante importante para a terceirização de TI na nuvem. Em resumo: quanto maior a largura de banda, mais fácil e confiável a transferência de dados funciona e mais funções podem ser hospedadas em data centers externos.

Se o software também for usado na nuvem (por exemplo, sistemas operacionais, programas como SAP ou bancos de dados entre empresas), a conexão com a Internet também funcionará da maneira mais estável possível. Se a conexão falhar, os funcionários não poderão mais fazer logon no próprio PC.

Se a terceirização de TI estiver sendo considerada, ou seja, de modo que não haja mais um servidor local, será necessária uma linha de fibra óptica dedicada.

Isso oferece uma largura de banda - mais ou menos garantida - de min. 100 Mbit / s, é muito mais estável e tem uma garantia de disponibilidade.

Se a largura de banda for muito baixa ou instável, também será usada uma solução híbrida que consiste em uma rede fixa e móvel. Se houver problemas na rede fixa, uma conexão 4G (ou no futuro 5G) entrará automaticamente. O mesmo se aplica se a rede fixa ainda estiver disponível, mas a largura de banda oferecida for muito baixa.

E-mails no datacenter ou na nuvem

A propósito, o servidor de email é uma função terceirizada clássica. Este é o servidor que recebe, encaminha, mantém ou envia emails. Ao mesmo tempo, é claro, ele também gerencia todas as caixas de correio da empresa (endereços de email). As empresas costumam terceirizar o servidor de e-mail para um data center externo de um provedor de serviços, a fim de economizar a operação tediosa e a manutenção regular.

Firewall e VPN

A internet também pode ser muito ruim, existem muitas pessoas querendo seus dados. Para mantê-los fora, o uso de um firewall poderoso é essencial.

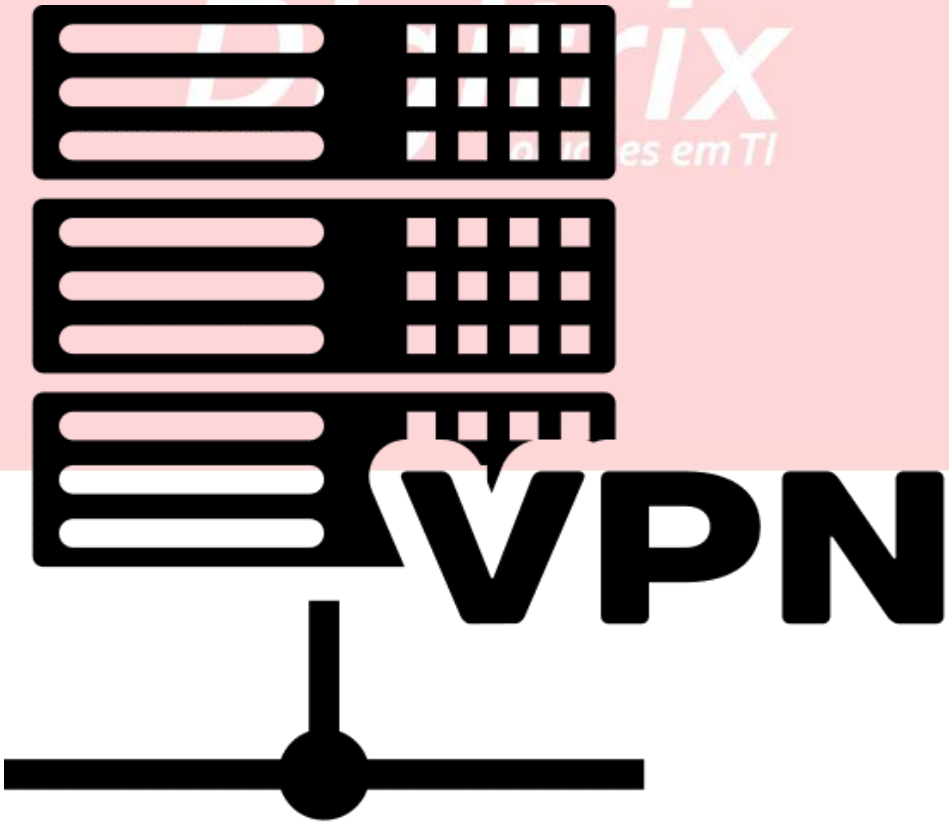
O fato é: assim que houver uma conexão entre a rede local e a Internet, os invasores podem tentar roubar, criptografar ou paralisar a rede da empresa.

O que é um firewall?

O "muro de fogo" é praticamente uma linha divisória entre a rede pública (desprotegida) (ou seja, a Internet) e a rede interna da empresa. Basicamente, você pode pensar em um firewall como uma última linha de defesa, na qual todas as regras de troca de dados são definidas e estabelecidas.

Aliás, isso pode ser entendido em ambas as direções: por um lado, o acesso indesejado a partir do exterior é bloqueado e, por outro lado, o acesso ao exterior também pode ser restrito - por exemplo, bloqueando sites com conteúdo pornográfico.

Parece fácil, mas não é realmente. Porque, é claro, enquanto os funcionários devem ter acesso a serviços da Internet, como WWW, email, FTP e conexões remotas, você deseja oferecer à Internet acesso público à sua própria página inicial ao mesmo tempo. E é aí que o firewall entra.



Papel central no conceito de segurança

Mesmo que um firewall esteja longe de ser suficiente para garantir um nível adequado de segurança na rede da empresa (scanners antivírus etc. também devem estar aqui, por exemplo), ele ainda desempenha um papel central no conceito geral de segurança.

Por conseguinte, a configuração do firewall deve ser realizada com cuidado. Sem o conhecimento especializado adequado, os erros podem surgir rapidamente e a “muralha de fogo” vai apagar.

De qualquer forma, as configurações básicas "Bloquear acesso da Internet à rede da empresa" e "Permitir acesso da rede da empresa à Internet" são praticamente inúteis. Não menos importante, porque pode ser útil e desejável para filiais e escritórios que possam existir,

Hardware e software

Simplificando, o termo firewall refere-se a um grupo de componentes de rede (hardware e software) que ficam na interface de duas redes. Todo o tráfego de dados entre uma rede pública e privada deve ser executado através desses componentes para garantir a conformidade com as diretrizes de segurança.

O firewall examina praticamente todos os pacotes de dados e apenas permite a passagem inesperada. Obviamente, o próprio firewall também deve ser imune a intrusos. Assim que um hacker entra, o firewall é inútil. Fiel ao lema: se o ladrão já estiver dentro, não ajuda mais trancar a porta do apartamento. Portanto, deve-se prestar tanta atenção à segurança do firewall quanto à segurança da própria rede privada.

Como já mencionado, um firewall protege o tráfego de dados entre LAN (rede privada) e WAN (Internet) e, portanto, verifica praticamente todo o tráfego de dados. Atualmente, isso quase sempre é executado nos protocolos da Internet HTTP e HTTPS.

Isso significa que esses protocolos e as portas associadas estão abertas em praticamente todos os firewalls. Como as transferências de dados mais diversas ocorrem dessa maneira, do messenger ao armazenamento em nuvem e serviços como o Microsoft Office 365, um firewall antigo que classifica apenas os fluxos de dados de acordo com a porta ou protocolo não tem mais chance de reconhecer se pragas são distribuídas ou dados roubados através da respectiva conexão. Por esse motivo, o bloqueio de serviços (ou portas) desnecessários não desempenha mais um papel importante.

Firewall Barracuda

Firewall de próxima geração

É aqui que os chamados "firewalls da próxima geração" entram em cena. O nome foi definido pelo Gartner Research (um instituto de pesquisa de mercado na área de TI).

Um firewall de última geração também pode identificar aplicativos e usuários no fluxo de dados. Isso inclui um sistema integrado de prevenção contra intrusões (IPS), a identificação de aplicativos e protocolos, independentemente da porta usada e a consideração de fontes de dados externas, como serviços de diretório com dados do usuário.

Em outras palavras, os firewalls de última geração examinam atentamente todas as transferências HTTP e HTTPS, examinam fluxos de dados, filtram dados infectados, analisam o comportamento do usuário e decidem quais transmissões são permitidas e quais não são, com base em regras predefinidas.

Novamente, que o respectivo nível de segurança depende das configurações (políticas). Se eles estiverem configurados corretamente, o sistema não será apenas mais seguro posteriormente, mas também causará menos aborrecimento para os funcionários (usuários), porque quase não existem "falsos alarmes".

Os limites de um firewall

Uma grande vantagem de um firewall central é que ele simplifica todo o gerenciamento de segurança - não é mais necessário configurar cada computador individualmente.

Como também serve como a única interface para a Internet, os ataques só podem ocorrer neste momento e, portanto, são mais fáceis de detectar. Os firewalls não são úteis, no entanto, quando ataques são realizados dentro de suas próprias fileiras.

Se os funcionários quiserem copiar dados para pendrives, eles poderão fazê-lo. Da mesma forma, os firewalls não ajudam contra vírus e cavalos de Troia, pois não podem procurar todos os pacotes de dados em busca de malware em potencial.

Os firewalls também não podem fazer nada contra os chamados ataques orientados a dados. São dados aparentemente inofensivos com códigos ocultos para alterar as configurações de segurança.

VPN - Acesso externo seguro

O acesso móvel seguro e criptografado aos dados da empresa ou à rede da empresa também é configurado no firewall - por exemplo, para funcionários no campo ou no escritório doméstico.

Uma rede virtual privada (VPN) permite que computadores remotos se comportem como se estivessem localizados diretamente na rede corporativa segura. Isso significa: você fica em casa com seu notebook e pode acessar a rede da empresa como se estivesse sentado em uma mesa no escritório.

Cada lado da conexão é um ponto de extremidade da VPN, a conexão entre eles é chamada de túnel da VPN. O software apropriado também deve ser instalado nos dois lados. Por causa da criptografia, é quase impossível que pessoas de fora interceptem os dados no túnel da VPN ou causem interferências.

Como um ponto de extremidade da VPN é o firewall da empresa, o seguinte se aplica: quanto mais poderoso o firewall, mais segura e estável a conexão VPN.

Rede, comutadores e WLAN

O servidor é a parte mais importante de uma rede de TI? De jeito nenhum! Sem a rede correta em segundo plano, até o servidor mais poderoso não tem valor. O "cabo na parede" é um dos componentes mais importantes e duradouros de uma rede de TI - e, portanto, deve ser planejado e escolhido com cuidado.

Cabeamento de rede estruturado

Afinal, o chamado cabeamento de rede estruturado constitui a base de qualquer rede de alto desempenho para a transmissão de dados e / ou voz.

Além dos componentes ativos, ou seja, os servidores ou computadores, as propriedades dos diferentes tipos de cabos e a estrutura do cabeamento são decisivas para o desempenho de uma rede.

Além disso, o fato de os componentes ativos (ou seja, o hardware) serem substituídos com muito mais frequência do que os cabos.

Um computador pode ser trocado rapidamente, mas a instalação (subsequente) de cabos significa um esforço logístico considerável e, portanto, também financeiro (levantar uma parede, interrupções nos negócios etc.).

O fato é: sem uma infraestrutura de rede passiva poderosa e segura, não há rede de TI estável, mesmo com os componentes de hardware ativo da mais alta qualidade.

Infelizmente, a importância de um cabeamento de TI limpo é subestimada: pontos fracos na rede da empresa e problemas com a confiabilidade do cabeamento geralmente impedem que os dados sejam transmitidos com eficiência. E isso afeta a produtividade de toda a empresa.

Planejamento é tudo

O cabeamento de TI não é apenas baseado em requisitos, mas também depende da localização ou do edifício - e, portanto, é sempre único. Por esse motivo, o planejamento concreto ou a implementação posterior DEVEM ser realizados profissionalmente e com cuidado.

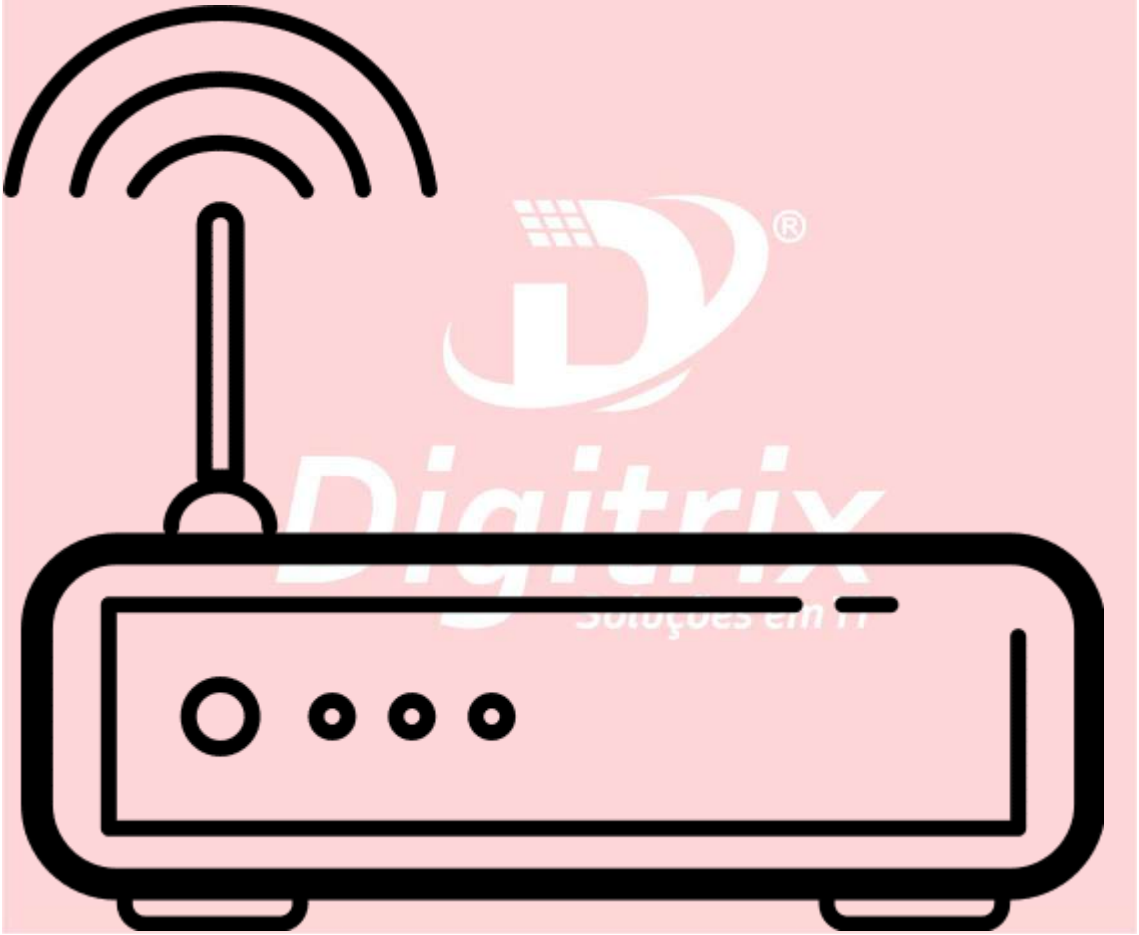
Intervenções subsequentes no sistema, por exemplo, devido a extensões ou reprojetos, só são possíveis com considerável esforço financeiro. Aliás, esses custos só podem ser reduzidos um pouco se já houver espaço planejado para

possíveis alterações no equipamento básico - por exemplo, com canos vazios ou - no início, supostamente desnecessários - cabos fictícios.

Se você quiser economizar dinheiro durante a fase de construção, pode ser muito caro posteriormente. Especialmente empresas com alta rotatividade de funcionários ou que estão crescendo

O objetivo do planejamento de rede não deve ser apenas configurar uma rede sem problemas, mas também torná-la o mais sustentável e escalável possível - palavra-chave: segurança futura.

Sem o conhecimento profissional, também no que diz respeito à experiência em termos de extensões posteriores, isso funcionará apenas nos casos mais raros.



Como funciona uma rede?

Pode-se imaginar uma rede de TI como uma rede. Existem inúmeras conexões e nós que, em conjunto, formam uma rede intacta. E não importa quantos nós estejam no meio, de alguma forma todos os dispositivos estão conectados - direta ou indiretamente - entre si.

Os nós podem ser computadores individuais (clientes), comutadores ou servidores. Eles são todos parte integrante das redes corporativas modernas.

Existem também outros dispositivos externos, como impressoras, scanners ou aparelhos de fax. Eles também são integrados à rede interna da empresa e, portanto, podem ser usados de maneira ideal por todos os funcionários - afinal, nem todo computador também precisa de sua própria impressora.

Switches - as grandes incógnitas

Ah, sim, embora você seja frequentemente confrontado com o termo "switch" em uma rede de TI, poucas pessoas realmente sabem o que realmente é - e elas geralmente são apenas uma caixa pequena e discreta na caixa de distribuição.

Basicamente, um switch é um elemento de conexão que conecta vários hosts em uma rede. Em uma rede Ethernet, um comutador serve como distribuidor dos pacotes de dados.

Se as portas dos dispositivos conectados (clientes) forem conhecidas, ele poderá alternar diretamente entre esses dispositivos. Se ele não conhece os dispositivos, ele simplesmente envia os pacotes de dados a todos os clientes e aguarda.

Quando os pacotes de resposta retornam dos destinatários, o comutador lembra os endereços MAC (endereços de dispositivo) dos pacotes de dados e a porta associada e envia os pacotes de dados apenas para o dispositivo correspondente.

Em princípio, um switch nada mais é do que um carteiro inteligente que recebe pacotes de dados e os entrega de maneira direcionada.

Aliás, essa inteligência também é a grande diferença para um hub. Por exemplo, se três computadores estiverem conectados a um hub por meio de um cabo LAN, eles poderão trocar dados entre si.

Se um computador enviar dados, eles serão distribuídos pelo hub para todos os outros computadores conectados. Por outro lado, um comutador pode identificar os computadores individuais e, portanto, enviar os dados apenas para determinados computadores, se necessário.

Além disso, um switch pode enviar e receber dados ao mesmo tempo, o que o torna muito mais rápido. Os switches estão disponíveis em uma ampla variedade de modelos e configurações.

Em geral, quanto maior e melhor um equipamento estiver equipado, mais caro ele será. Um switch simples possui 4 ou 5 portas - mas também há níveis de expansão com 8, 16, 24 e 32 portas. Switches empilháveis,

Importante: configure o WiFi

Para voltar à fiação do piso novamente. Isso também é frequentemente usado para implementar a conexão WLAN - em cada vez mais empresas, a famosa "última milha" já está sendo implementada sem fio.

Especialmente quando os funcionários trabalham principalmente com notebooks ou tablets. Note-se que uma WLAN é uma variante significativamente mais flexível, mas nem toda rede WLAN também é adequada para toda quantidade de dados.

Se grandes quantidades de dados tiverem que ser movidas, a conexão com fio é sempre preferível. A regra geral é: com um ponto de acesso WLAN de acordo com 802.11ac, são possíveis taxas de transmissão de até 1,3 Gbit.

Em um número cada vez maior de empresas, agora também é uma boa idéia oferecer aos visitantes e parceiros de negócios acesso sem fio à Internet o tempo todo.

De qualquer forma - apesar de toda a hospitalidade -, certifique-se de configurar seu próprio WiFi de convidado. Isso pode ser feito rapidamente e com pouco esforço e é altamente recomendado em termos de segurança de dados.

Uma rede de convidados é basicamente nada além de um ponto de acesso separado no roteador. Todos os dispositivos dos funcionários estão conectados à rede da empresa via WLAN - incluindo acesso a dados.

A rede de convidados, por outro lado, é um ponto isolado que oferece acesso à Internet, mas não à rede da sua empresa. Como o nome sugere, o WiFi para clientes é uma rede especial e isolada apenas para convidados.

Servidor e virtualização

As ambiguidades não estão necessariamente na agenda do setor de TI, mas o termo “servidor” é uma exceção. Existem servidores no lado do hardware e do software. A palavra mágica de TI "virtualização" também está permanentemente conectada aos "servidores".

Introdução ao mundo dos servidores

Pode ser um computador que disponibiliza seus recursos em uma rede ou apenas o software que é executado nesse computador. Por conseguinte, existem duas definições básicas de servidor.

Um servidor baseado em hardware é uma máquina (física) integrada em uma rede de TI, na qual um ou mais servidores baseados em software são executados além do sistema operacional.

Esses dispositivos são chamados de "host" no jargão de TI. Um servidor baseado em software, por sua vez, é um programa que oferece um serviço especial que pode ser usado por outros programas, os chamados clientes, localmente ou via rede. O serviço disponível depende do tipo de software para servidor.

Um exemplo clássico é um servidor de email. O correio é recebido e gerenciado por um computador (o host do servidor de correio), enquanto todos os outros computadores da rede (os clientes) o acessam.

Embora eles possam acessar e editar os e-mails, eles são salvos e permanecem no servidor. O mesmo sistema também funciona com bancos de dados ou espaços de armazenamento de dados.

Os sistemas centrais de armazenamento de dados, gerenciados por um servidor, são muito populares nas empresas. A grande vantagem: um backup é central para facilitar a implementação, do que se todos os computadores (clientes) da rede tivessem que ser processados individualmente.

Falando em clientes: em todos os casos, a base da comunicação é o modelo cliente-servidor.

Em uma rede, os servidores não são apenas “servidores”, eles também são responsáveis pelo gerenciamento de usuários e direitos.

Quem pode acessar quais dados ou quais ações (excluir, ler, salvar, alterar,...)? Na prática, a ferramenta "Active Directory" da Microsoft é quase sempre usada aqui.

Ele autentica usuários e suas autorizações individuais na rede. Trabalhar em uma rede com um servidor não é diferente de trabalhar em um computador de usuário único. Normalmente, no entanto, você tem acesso a pastas ou discos rígidos adicionais no servidor - mas somente quando você estiver conectado à rede.

Servidor Dell

Fisicamente e / ou virtualmente?

Vários servidores virtuais geralmente são executados em um servidor físico (ou seja, um computador em rede). Podem ser programas como um sistema ERP, servidor de correio, sistemas de telefone VoIP ou contabilidade.

Para garantir alta disponibilidade, esses aplicativos / programas às vezes são executados em paralelo em vários servidores físicos. A vantagem: se um único computador de rede falhar, você poderá continuar trabalhando sem perturbações pelo segundo (ou terceiro).

Mesmo se houver manutenção pendente, esse trabalho pode ser realizado sem perda de dados e / ou interrupção das operações em andamento. O software da VMware ou Microsoft é frequentemente usado para essa "virtualização".

Palavra mágica "virtualização de servidores"

O que nos leva ao termo mágico de TI "virtualização". Nesse contexto, virtual significa que algo realmente não existe, mas existe teoricamente ou é simulado por um computador.

Então, o que é um servidor virtual? Um pequeno exemplo para explicar: imagine um host que não seja poderoso o suficiente para lidar com determinadas tarefas.

Computadores (físicos) adicionais deverão, portanto, ser usados para poder fornecer a potência computacional necessária. Os programas (da VMware ou Microsoft) agora estão instalados nessa "rede de computadores", o que faz com que essa rede apareça como um "servidor" único para os clientes.

O usuário então não sabe qual computador do cluster está processando o trabalho, mas - e esse é o ponto crucial - o trabalho é realizado com a máxima satisfação. Em outras palavras, muitos hosts aparecem como um host que fornece o serviço que desejam.

Isso também impede que a utilização do hardware de um serviço afete o desempenho de outros serviços.

Obviamente, também funciona o contrário: se um host poderoso estiver disponível, ele poderá executar várias tarefas sem que o usuário perceba que todas as tarefas são executadas por um único computador.

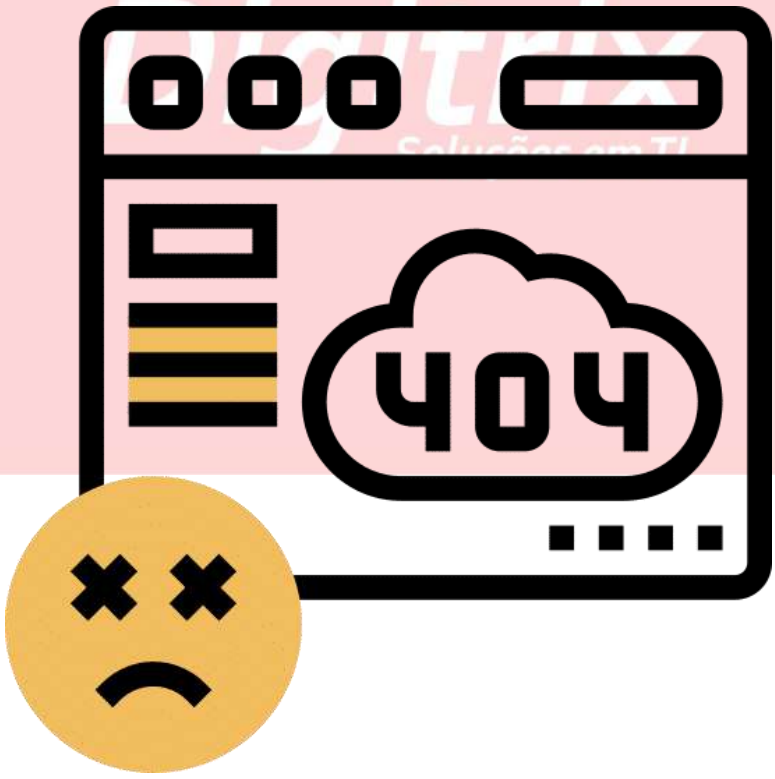
O princípio de um servidor virtual é, portanto, conectar computadores para poder gerenciar o software do servidor ou executar vários softwares em um host para utilizar seu desempenho Servidor.

Falha no servidor... e agora?

Servidores (físicos ou virtuais) desempenham um papel importante na rede da empresa. Por exemplo, se um servidor de email falhar, ninguém na empresa poderá receber ou enviar email.

Consequentemente, esses componentes de rede também devem ser bem mantidos e altamente disponíveis.

Nesse caso, o tempo de resposta do fabricante do hardware ou do provedor de serviços de TI é essencial. Como regra, um serviço no local 24 horas é usado para servidores, mas em casos extremos também um serviço no local durante 4 horas.



Sistemas de telefone VoIP

A transformação digital também não para no sistema telefônico. O protocolo Voice over Internet (VoIP) oferece vantagens consideráveis de custo às empresas, é quase infinitamente escalável e permite rotas de trabalho e comunicação mais flexíveis.

O sistema telefônico clássico ainda pode ser encontrado em muitas empresas. No entanto, os sinais dos tempos estão claramente no IP (Internet Protocol).

Tudo já está funcionando nas redes de computadores hoje, então por que não a telefonia vocal também? Especialmente porque os sistemas VoIP trazem muitas vantagens - por exemplo, no lado dos custos.

Vantagens de um sistema de telefone VoIP

Mas não é só isso: a telefonia IP também oferece às empresas inúmeras vantagens nos negócios cotidianos. Especialmente quando os funcionários costumam estar na estrada ou no escritório em casa, por exemplo.

Graças ao alto nível de flexibilidade, eles podem trabalhar onde quer que estejam, mas ainda podem ser alcançados pelo número de telefone fixo habitual e podem fazer chamadas pela Internet.

O único requisito aqui é que um telefone de software (um aplicativo) seja instalado no notebook, tablet ou smartphone do respectivo funcionário.

O sistema também é muito fácil de gerenciar, que geralmente é baseado na Web através de um navegador. O encaminhamento de chamadas pode ser configurado com o clique de um mouse, números de telefone bloqueados, informações de presença enviadas ou reuniões telefônicas agendadas.

O sistema VoIP também pode ser vinculado ao Microsoft Exchange ou a um sistema de CRM, ou seja, o respectivo banco de dados de clientes, por meio de interfaces.

Se o funcionário tocar no telefone, todos os dados importantes do cliente serão exibidos na tela - com base no número de telefone que está ligando.

Isso significa que as conversas com os clientes podem ser conduzidas de forma mais rápida, pessoal e eficiente.

Servidor em vez de sistema telefônico

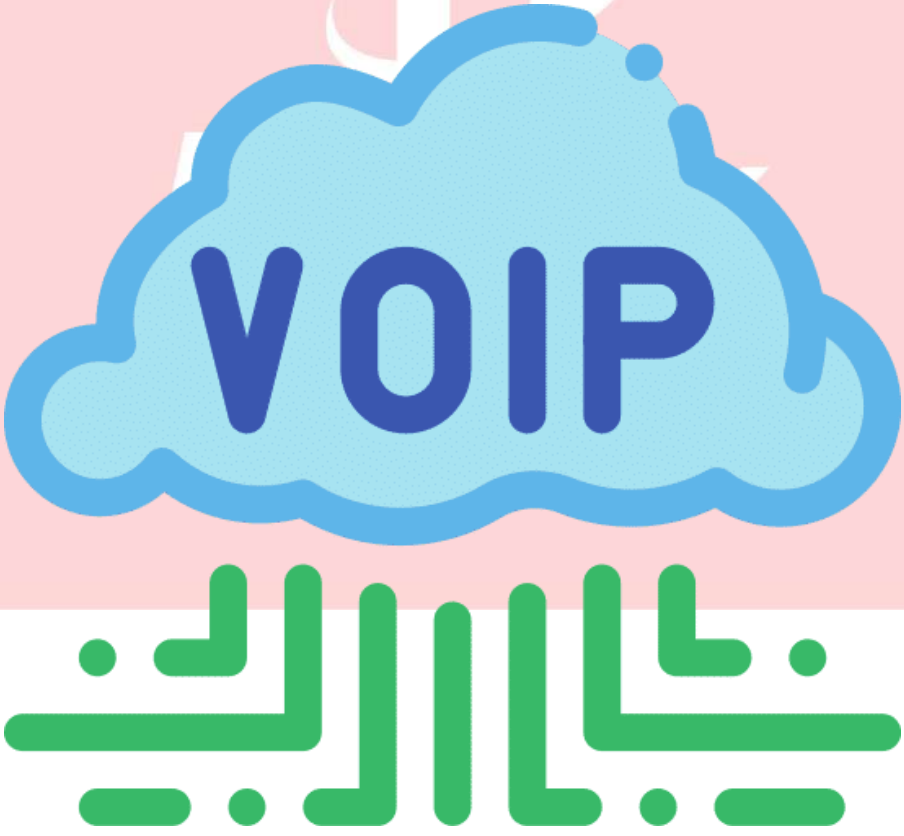
A escalabilidade flexível do sistema também é muito interessante para as empresas. As conexões do sistema IP, os chamados troncos SIP, fornecem um número variável de canais de voz sem precisar conectar um novo dispositivo ou colocar novos cabos.

Se mais canais forem necessários, eles podem simplesmente ser reservados - e mais tarde, é claro, cancelados novamente sem problemas. Simplificando, um tronco SIP conecta um sistema telefônico compatível com VoIP a um provedor de telefonia com base em uma linha de dados.

Também possibilita configurar várias conexões telefônicas paralelas a partir de ramais diferentes ao mesmo tempo. O Session Initiation Protocol (SIP) assume a tarefa de controlar as conexões de voz baseadas em IP.

Em vez de um sistema telefônico, a própria empresa possui um servidor de telefonia incorporado à infraestrutura de rede da empresa. Este servidor é responsável por todos os processos de comutação e solicitações de conexão.

Ele assume as tarefas que praticamente correspondem às de um sistema telefônico clássico. Um gateway VoIP adicional também estabelece uma conexão com a rede telefônica clássica. Servidor e gateway são frequentemente combinados como hardware e software.



Interface web 3CX

A largura de banda deve estar disponível

Na telefonia VoIP, um terminal VoIP (um telefone de mesa VoIP ou um telefone de software VoIP) converte a fala em pequenos pacotes de dados e os comprime.

Os pacotes de dados são então transmitidos ao outro assinante via rede de computadores (interna) ou pela Internet (externa). O dispositivo VoIP instalado lá converte os pacotes de dados novamente em som e os emite.

Desde que a largura de banda esteja correta, a qualidade da voz VoIP também se ajusta. A chamada VoIP deve compartilhar uma linha de dados com centenas de outros aplicativos.

Se houver pouca largura de banda disponível, não haverá mais espaço suficiente para os dados da chamada VoIP.

Falhas como interrupção de fala ocorrem ou a conversa pode até parar completamente. No entanto, existem mecanismos chamados QoS (Qualidade de Serviço) para evitar esses problemas.

Usando a tecnologia QoS, você pode configurar sua rede para que as chamadas VoIP, por exemplo, tenham sempre a maior prioridade e sejam transmitidas antes de todos os outros dados. Isso resulta em uma qualidade de voz consistentemente alta, mesmo com chamadas VoIP.

Não tenha medo de mudar

No geral, os sistemas VoIP oferecem muito mais funcionalidade do que os sistemas telefônicos tradicionais - e também são consideravelmente mais baratos e flexíveis de operar.

Também é fato que, no futuro, não haverá maneira de contornar o VoIP. Por esse motivo, é aconselhável planejar uma migração para telefonia IP hoje.

A maneira mais fácil de mudar é se a empresa já usa o chamado sistema híbrido. Isso pode ser feito com capacidade de IP com esforço gerenciável.

No entanto, se for um sistema ISDN puro, existem várias opções para a troca. Uma delas é conectar um gateway externo com o qual o sistema existente possa continuar sendo usado.

No entanto, esta opção está longe de ser ótima e não é recomendada. É melhor substituir o sistema telefônico antigo por um novo sistema IP. Se a nova

solução IP for a sucessora do sistema ISDN antigo, talvez seja possível continuar usando os dispositivos existentes.

Uma terceira variante é a mudança completa para uma solução baseada em nuvem - em comparação com o sistema telefônico local, a alternativa mais barata e mais flexível.

Sobretudo porque os altos investimentos iniciais, bem como os custos de administração e manutenção, são eliminados.

Noções básicas de segurança de TI

Aumentar a digitalização está desafiando a segurança de TI. Mais e mais dispositivos na rede e mais funcionários móveis estão sempre criando novos pontos de ataque. Um firewall sozinho não é mais suficiente hoje.

E até o software antivírus tradicional não é mais suficiente para garantir totalmente a segurança das empresas. Em vez disso, aparecem soluções integradas que oferecem proteção no nível do dispositivo e da rede, além de modernas funções de análise e ferramentas de prevenção.

Simplificando, trata-se de implementar uma estratégia holística de segurança de dispositivos que combina e coordena uma série de contramedidas.

Isso inclui o programa antivírus clássico, bem como contramedidas com base em assinaturas ou análises contínuas de comportamento. Note-se que cada tipo de dispositivo possui seus próprios requisitos e recursos de segurança. Quando você fala sobre um "ponto final" hoje em dia, precisa considerar muito mais dispositivos do que alguns anos atrás.

Agora, eles incluem servidores, PCs, laptops, smartphones, tablets, dispositivos IoT e ambientes em nuvem tradicionais. Cada um desses pontos pode ser um gateway para invasores, que geralmente não se concentram em apenas um dispositivo, mas têm vários deles à vista.

Em particular, dispositivos IoT, como impressoras ou scanners, geralmente não possuem funções de segurança integradas, motivo pelo qual deve ser dada atenção especial a eles.

Gerenciamento de segurança central

Portanto, as empresas precisam aumentar a segurança do dispositivo com a combinação certa de tecnologias avançadas. Uma possibilidade é chamada de Unified Threat Management Solutions (UTM).

Eles fornecem uma variedade de funções de segurança diferentes em um único produto. Eles geralmente trabalham entre a Internet e a rede local e analisam as transferências de dados.

A vantagem das soluções UTM é o controle central, que fornece uma visão geral do status de segurança da rede a qualquer momento e pode criar relatórios.

Uma grande vantagem sobre soluções individuais é que o departamento de TI não precisa lidar com diferentes consoles de gerenciamento.

No entanto, a abordagem uniforme não apenas garante um nível mais alto de segurança, por causa disso, os erros de configuração são (em grande parte) evitados.

Além disso, as funções de segurança individuais da solução UTM geralmente são bem coordenadas. Um dispositivo UTM pode, por exemplo, descriptografar conexões VPN de entrada e verificar o tráfego de dados por meio de seu sistema de detecção de intrusões (sistema de detecção de ataques), que seria muito mais complicado de implementar com componentes individuais.

Um sistema UTM também economiza custos porque é mais barato de manter do que um cenário complexo de segurança de TI.

Monitoramento em tempo real com SIEM

Parte de uma solução UTM é, obviamente, sempre um firewall. No entanto, isso por si só está longe de ser suficiente para garantir um nível adequado de segurança.

No entanto, o firewall e sua configuração ainda desempenham um papel central no conceito geral de segurança. No entanto, o monitoramento proativo da segurança de TI que monitora todos os processos na rede é quase ainda mais importante.

A ferramenta de segurança coleta dados de eventos de diferentes níveis operacionais e os analisa em tempo real. Se houver alguma anomalia na rede, elas serão reconhecidas e relatadas. Usando essas análises, medidas direcionadas podem ser tomadas para conter o ataque.

Essas técnicas são resumidas no termo SIEM (Gerenciamento de informações e eventos de segurança) e são baseadas na avaliação de dados relevantes para a segurança em um banco de dados central.

Com a ajuda desse banco de dados, processos relevantes à segurança podem ser controlados, eventos correlacionados, análise de erros e análises forenses realizadas em caso de incidentes de segurança.

Basicamente, esse monitoramento de segurança de TI também é a única maneira de detectar invasores cibernéticos antes que eles possam causar danos em uma empresa.

Software desatualizado e funcionários descuidados

As atualizações regulares de segurança de software também não devem ser negligenciadas. Isso fecha as brechas de segurança que - assim que a atualização foi publicada pelo fabricante - são conhecidas por praticamente todos.

Essas lacunas de segurança devem ser resolvidas o mais rápido possível pela atualização correspondente, antes que um hacker possa tirar proveito da situação.

Funcionários desatentos também são um gateway popular. Muitas vezes, o tratamento negligente de e-mails abre a possibilidade de invasores injetarem malware no sistema.

Os funcionários devem, portanto, ser treinados e sensibilizados de acordo. Para que eles não caiam no "spear phishing", no qual os emails direcionados são usados para se infiltrar em software malicioso.

Os aplicativos do departamento de RH, por exemplo, que contêm arquivos maliciosos direcionados a vulnerabilidades no Microsoft Word ou Adobe Acrobat, em vez do currículo de um funcionário em potencial, são muito populares aqui. Os programas antivírus podem interceptar muito aqui, mas infelizmente nem tudo.

Sobre a Digitrix

A DIGITRIX é uma empresa especializada em Serviços e Soluções de TI. Desde 2003 ajuda empresários e gestores a vencer seus desafios com apoio da Tecnologia da Informação.

Somos especializados em:

=> Administração de ambientes e recursos de TI;

=> Suporte de TI com Service Desk;

=> Segurança e Proteção de Dados;

=> Venda de Hardware e Software;

=> Soluções em Nuvem;

=> Redes;

=> Virtualização;

=> DLP Gerenciado;

=> Antivírus Gerenciado;

=> Backup Gerenciado;

=> Firewall Gerenciado;

=> HotSpot Gerenciado.

Temos nossos serviços e soluções focados em três importantes perspectivas:

- Mitigação de riscos

- Redução de custos

- Produtividade

Saiba +

www.Digitrix.com.br