PRINCIPAIS DESAFIOS NA IMPLEMENTAÇÃO DE VPNs

O **HOME OFFICE** você já conhece mas e o

HOME ENTER PRISE,

VOCÊ ESTÁ PREPARADO?

PINPOINT®
Made to Measure

A repentina mudança no modo de trabalho das empresas levou os funcionários a trabalhar remotamente. Mas, como garantir a conectividade no ambiente corporativo por meio de VPNs?

O Home Enterprise hoje é uma necessidade latente e a qualidade desta solução está impactando diretamente na produtividade da força de trabalho das organizações.

QUAIS SÃO OS DESAFIOS DE MONITORAR E ESCOLHER A MELHOR SOLUÇÃO DE VPN?

A falta de monitoração das soluções de VPN pode trazer grandes problemas:

- **Vazamento de informações**
- **Baixa produtividade dos colaboradores**
- **Problema de acesso a ambientes críticos**
- **Impacto negativo no nome das empresas**

MELHORES PRÁTICAS PARA SOLUÇÕES DE VPN

Listamos pontos chaves na escolha da plataforma de VPN, levando em conta software, hardware e processos.

- **Criptografia de ponta**
- **Autenticação**
- **Gestão de equipamentos nas pontas**
- **Alta disponibilidade**
- **Conectividade**
- **Capacidade**
- **Monitoração**
- **Operação**

Criptografia de ponta

Todo o tráfego precisa ser criptografado para impedir que terceiros tenham acesso a ele na Internet. É comum encontrarmos no mercado implementações de VPN que criptografam apenas parte do tráfego, normalmente o tráfego direcionado ao(s) servidor(es) da empresa. Este tipo de implementação, apesar de ter um processamento menor, pode trazer um risco grande, pois abre brechas para ataques por outros protocolos.

Como exemplo, um redirecionamento feito por um ataque de DNS pode levar o usuário a enviar dados sensíveis para o atacante.

Esta prática também facilita que erros de configuração não sejam percebidos a curto prazo, deixando o ambiente vulnerável. Outro ponto a se destacar é a utilização cada vez maior de serviços na Nuvem, o ajuste dos equipamentos para criptografar o tráfego necessário é extremamente oneroso.

Por esses pontos, a recomendação é criptografar todo o tráfego dos usuários remotos, e fazer a liberação dos acessos todos em um firewall corporativo passando por regras de bloqueio e identificação de ameaças (IDS/IPS).

Autenticação

Garantir que apenas pessoas autorizadas possam se conectar a VPN.

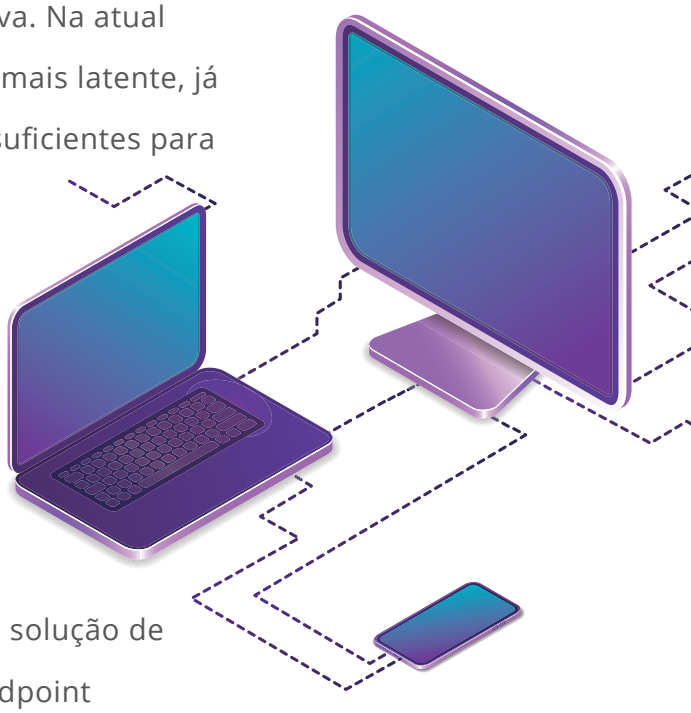
Neste quesito, a recomendação é utilizar uma solução de autenticação de dois fatores, ou seja, além da senha, utilizar um segundo método (como por exemplo a utilização de tokens).

Existem nos mercados diversas soluções de autenticação de dois fatores, que vão desde equipamentos físicos (aqueles chaveiros) até soluções baseados em Aplicativos, como Google Authenticator e o 1Password.

Gestão de equipamentos nas pontas

Quando ligamos a rede da empresa até o dispositivo pessoal (laptop, tablet ou celular), precisamos garantir requisitos mínimos de conformidade com o ambiente da empresa, por exemplo, antivírus atualizado, atualizações críticas aplicadas.

Várias empresas nos últimos anos vêm aderindo a políticas de B.Y.O.D. (Bring Your Own Device), ou seja, possibilitar que o usuário utilize seus próprios equipamentos para conectar a rede corporativa. Na atual situação que estamos vivendo essa alternativa é ainda mais latente, já que muitas empresas não contavam com dispositivos suficientes para colocar toda sua força de trabalho em Home Office.



Algumas soluções de VPN tem a opção de fazer uma validação de compliance (conformidade), como resultado dessa validação a solução de VPN pode permitir a conexão, rejeitar ou ainda colocar esse dispositivo em uma rede de “quarentena”, passando assim por regras mais rígidas.

Outro ponto a se destacar, que trabalha em conjunto à solução de VPN são os sistemas para gestão de computadores (Endpoint Management) e celulares (MD).

Estes sistemas visam garantir integridade e padronização do parque de equipamentos que estão remotos, de forma rápida e padronizada.

É recomendado uma operação conjunta entre a VPN e a solução de gerenciamento de Endpoint para garantir que os equipamentos conectados a rede não causem potenciais danos de perda de dados ou invasões.

Alta disponibilidade

A alta criticidade das comunicações gera a necessidade de soluções de VPN com alta disponibilidade. As funções do concentrador precisam estar preservadas e uma análise do tipo de redundância é fundamental e diferente para cada ambiente. No mercado, existem as seguintes opções (listas em ordem de resiliência a falhas):

Standalone: Apenas uma instância do equipamento de VPN instalada e configurada. Em caso de falha, o serviço ficará totalmente indisponível até que uma outra instância seja configurada. Com essa configuração, em caso de falha, haverá uma interrupção de tráfego de longo prazo.

Backup: Uma instância ligada e configurada, e uma outra (que pode ser física ou virtual) está pronta para entrar em operação. A caixa ativa precisa sofrer um backup constante, e esses dados de backup guardados em local apropriado. Se ocorrer um problema com a instância ativa, o último backup será restaurado na outra instância. Neste caso, haverá uma interrupção de tráfego de médio prazo.

Cluster Ativo/Backup: Nesta configuração são necessários dois equipamentos que irão realizar um sincronismo online de configurações e status internos. Caso o nó ativo falhe, ou outro automaticamente identifica essa falha e assume suas funções. Na grande maioria das empresas, esse tempo de chaveamento não gera impactos ao ambiente produtivo.

Cluster Ativo/Ativo: No modo ativo/ativo, todos os equipamentos (que podem ser mais que dois) vão trabalhar juntos. Cada um tratando uma porção do tráfego. O importante neste caso é garantir que em caso de falha de um nó haja sobra de processamento nos demais para assumir esse tráfego sem impactar na performance para os usuários conectados.

Geo-Distribuído: Este é o cenário mais complexo, mas que em certos projetos precisam ser utilizados para garantir um SLA agressivo. Ele é composto normalmente por dois ou mais clusters, onde cada um é instalado em um datacenter/nuvem diferentes. Este modelo é muito utilizado quando a corporação precisa operar com um DRP (Disaster Recovery Plan) ou tem sua planta descentralizada (por exemplo, envolvendo várias nuvens). Neste caso, é altamente aconselhável uma gestão de rede WAN e internet muito bem implementada.

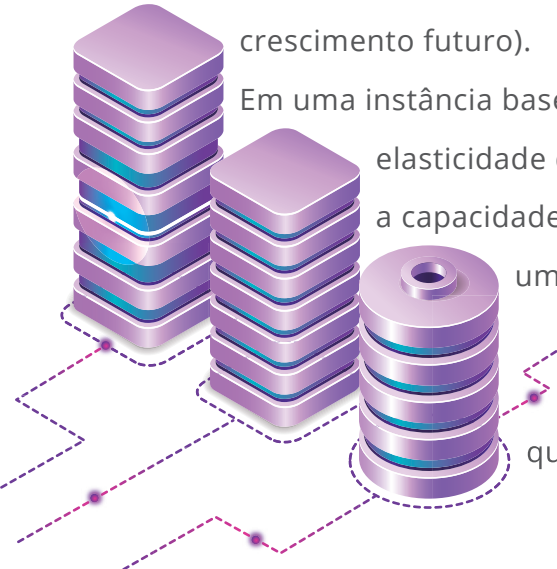
Conectividade

A qualidade, estabilidade e performance da VPN está diretamente ligada às operadoras que entregam Internet para as pontas (concentrador e usuários finais). Principalmente no Brasil, que possui uma diversidade de regiões enorme, uma análise da melhor combinação de provedores é fundamental para garantir uma experiência de uso que o negócio requer. É necessário um mapeamento da localização dos usuários e onde estão localizados os serviços. Em alguns casos, é

Capacidade

A escolha de software e hardware para as soluções de VPN devem impactar diretamente na capacidade de uso do ambiente. O mapeamento correto dos modelos de equipamentos é fundamental para não gerar problemas de performance ou investimento acima do necessário. O ponto crucial no desenho da solução de VPN é a escolha entre um equipamento físico (baseado em máquina virtual) ou ainda VPN como serviço.

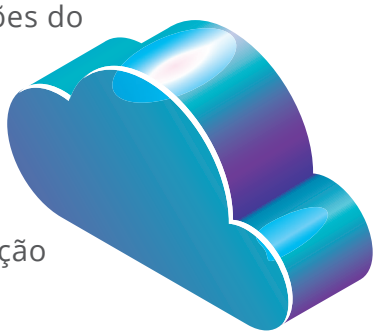
Quando optamos por um equipamento físico temos a vantagem de trabalhar com uma solução padronizada (software foi desenvolvido pensando naquele hardware), sem adaptações e em muitos casos, utilizando-se de ASICs e aceleradores especializados. A desvantagem desse modelo é a amarração do CAPEX versus capacidade, ou seja, é preciso fazer um investimento bem superior ao necessário no momento (prevendo o crescimento futuro).



Em uma instância baseado em máquina virtual temos a vantagem da elasticidade de crescimento, onde possivelmente podemos aumentar a capacidade de forma simples (algumas vezes, o crescimento requer um aumento no licenciamento do software de VPN/Firewall. Em oposto à utilização de um hardware dedicado e específico, neste modelo precisamos tomar cuidado quanto aos recursos disponibilizados pelo virtualizador. Há

uma necessidade garantir recursos dedicados e seguir todas as orientações do fabricante a risca.

Ainda existe a opção de se contratar VPN como serviço. Neste caso, a princípio, não precisa se levar em consideração os aspectos de crescimento. Ponto a se levar em consideração neste modelo é a localização (onde está conectado) em termos de rede.



Monitoração

Assim que implementado, o ambiente precisa ser monitorado. Essa monitoração visa garantir o pleno funcionamento da solução, identificar e prever gargalos e minimizar riscos de vazamento de informações. Os provedores de Internet também precisam ser monitorados para garantir sua conectividade entre as pontas.

Cada plataforma tem suas próprias métricas e pontos que precisam ser monitorados. Quando utilizamos um hardware dedicado para o concentrador de VPN, além dos monitores de status do software é necessário a monitoração do hardware (temperatura, ventoinha (fan), status de discos, etc). A maior recomendação é alinhar expertise em monitoração com dos administradores da solução. Cada um desses profissionais tem uma visão diferente, e que juntas, irão aumentar as capacidades e precisão dos alarmes.

Para a gestão de segurança, além das métricas estatística e de status dos equipamentos é importante a monitoração de duas outra visões: Configuração e Logs.

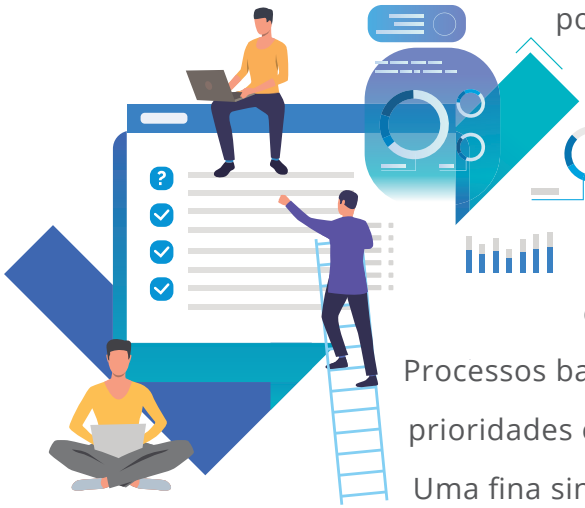
Configuração: A monitoração de configuração visa garantir, além de um backup consistente, a validação desta configuração quanto a política de segurança empresarial. Como exemplo, podemos monitorar para que todos os usuários criados na plataforma estejam com o perfil correto aplicado.

Logs: É importante monitorar os logs enviados pelos sistemas de VPN. Além dos logs relacionado ao sistema, também é possível monitorar os logs de uso dos usuários, transformando o NOC em um SOC.

Além da monitoração do ambiente tecnológico, também é possível monitorar a produtividade de cada indivíduo, não só através do tempo de conexão, mas também pela atividade final de cada um.

Operação

A operação precisa atender de forma rápida e precisa as demandas de novas requisições, bem como resolver incidentes com a plataforma no menor tempo possível. A operação precisa estar finamente alinhada com o processo de monitoração.



O desenho dos processos de operação deve sempre levar em consideração o SLA esperado e combinado com o negócio. Processos baseados em ITIL ajudam a controlar as prioridades e atender prazos.

Uma fina sintonia entre o time do NOC e de suporte ajudam a melhorar os tempos de atendimento e resolução de incidentes. O empoderamento do NOC, executando ações rápidas e pré definidas, melhora os tempos e diminui custos de operação.

Conclusão

Para uma escolha adequada da solução de VPN, todos esse pontos precisam ser levados em consideração durante um processo de engenharia e desenho e operação do ambiente. Mais do que garantir a conectividade remota, as organizações precisam garantir a continuidade do negócio, levando-se em conta a força de trabalho remota e impactos que vazamentos de dados irão ocasionar a marca.

PINPOINT®
Made to Measure

www.pinpoint.com.br
comercial@pinpoint.com.br
(11) 2359-0440
/pinpointbr