Faculdade de Tecnologia Senac GO.
Gestão da Tecnologia da Informação 3º Período
Fundamentos de Serviços IP
Professor: Fernando Tsukahara
Alunos: Elson Cristino Farias, Lucas Eduardo Rodrigues Couto
Projeto Integrador

Documento Pré-Projeto para a Implantação de Serviços necessários para "Segurança e Desempenho do Sistema"

Objetivos:
Este documento pré-projeto tem por base esclarecer todas as dúvidas e receios acerca da implantação dos serviços de diretórios oferecidos por nossa empresa, onde será esclarecido as importâncias desses serviços para a empresa Visão Tech e seus Clientes, e quais os benefícios esses serviços irão oferecer, com o objetivo de segurança, redução de custos e organização.

Motivação:

Segurança digital é um assunto importante de extrema relevância no dia a dia das organizações pelo contínuo aumento dos ataques e das vulnerabilidades das redes. Hackers, os conhecidos invasores Digitais, vírus de computadores e worms "programas maliciosos que se propagam por máquinas sem a necessidade de se anexarem a arquivos", erros de configuração, ataques lançados externamente e internamente, dentre tantos outros. Com o passar do tempo, e por meio de pesquisas e monitoramento, ficou claro que a ameaça não é apenas externa. Muito do que pode acontecer nas redes corporativas, nos sistemas de informação, hoje tão expostos, dada a facilidade do acesso à informação, vem de ameaças causadas por agentes internos. Some-se isso aos altos custos de implementação de redes dedicadas, interligando datacenters e filiais, acaba por gerar enormes desperdícios de dinheiro à empresa. Melhoria significativa na infraestrutura, diminuição considerável nos custos, com aumento da segurança no tráfego das informações (ativo mais importante da empresa nos dias de hoje) é o objetivo primário dos trabalhos a serem executados. Não se pode deixar de verificar, contudo, que grande parte de ameaças externas também podem se tornar internas, caso não seja dada a devida atenção ao problema. Nesse quesito, a implantação de um Sistema de Gerenciamento Diretórios tem a solução ideal.

Com o controle do ambiente de trabalho, bem como de contas de usuários e contas de computadores, conectados à rede da empresa, fornecendo o gerenciamento e configuração centralizados de sistemas operacionais, aplicativos e configurações de usuários em um único ambiente: o SSO " Active Directory".

Dentro deste ambiente, há o controle do que o usuário pode ou não fazer dentro de um ambiente de trabalho, controle de seu acesso, suas permissões, monitoramento, com a centralização das políticas de tecnologia da informação da empresa, reduzindo drasticamente a possibilidade de ações que possam representar potenciais riscos à segurança digital da organização.

Com a diminuição dos custos relacionados à manutenção de redes dedicadas, e com a configuração/monitoramento de tráfego de dados, as perspectivas de novos investimentos, e redução dos custos, a melhoria dos serviços corporativos da empresa poderá ser sentida a curto prazo.

Justificativa:

Integrado com os serviços já existentes na empresa, como Serviços de Nomes de Domínio e Protocolos de Configuração de Host Dinâmicos, há um ganho considerável no quesito segurança dentro da rede corporativa.

Para configurar um servidor DNS que é executado em um controlador de domínio, visando a criação e gerenciamento de zonas de acesso, é preciso ser membro dos grupos de administradores de DNS,

administradores de domínio ou administradores da empresa. Nesse contexto, em vez de armazenar as informações de zona em um arquivo de texto, elas são armazenadas no Active Directory. As atualizações da zona são automaticamente realizadas durante a replicação do Active Directory. Crie uma zona integrada do Active Directory para simplificar o planejamento e a configuração de um espaço de nomes de DNS. Não é necessário configurar servidores DNS para especificar como e quando serão feitas as atualizações, já que o Active Directory mantém as informações da zona.

O Active Directory é necessário para autorizar um Servidor DHCP. Com o Active Directory, os Servidores DHCP não autorizados não podem responder aos pedidos dos clientes. O serviço do Servidor DHCP, em um servidor membro do Active Directory, verifica o seu registro em um controlador de domínio do Active Directory. Se o Servidor DHCP não estiver registrado, o serviço não se iniciará e consequentemente o Servidor DHCP não designará endereços aos clientes. Sendo assim, clientes não autorizados não podem, por exemplo, acessar a rede de máquinas não autorizadas.

A infraestrutura atual, consistindo em conexões dedicadas e LANs virtuais geram custos demasiados à empresa, em vista de outro recurso que proporciona maior confiabilidade, segurança e melhores taxas de transferência de dados: as Redes Privadas Virtuais (Virtual Private Networks – VPN).

A ideia central da VPN é utilizar a internet, uma rede pública e de acesso irrestrito, para criar conexões privativas, visando a implementação de redes corporativas. Com isso, a transferência de dados de forma segura é garantida, como se as conexões fossem parte de uma intranet.

Com esse conceito, a criação de rede corporativa entre os clientes e a Visão Tech tem seus custos significativamente reduzidos, com os recursos de rede sendo acessíveis a toda empresa como se em uma rede privada estivesse.

Cabe lembrar que a rede virtual privada suporta múltiplos protocolos, entre eles o protocolo de internet (IP).

Quanto à questão de acessibilidade da informação, a instalação de servidores Proxy tende a aumentar exponencialmente a produtividade dos colaboradores da empresa. Um proxy de cache HTTP (Caching Proxy) permite que, pesquisando, um colaborador possa requisitar informações da rede externa, e o mesmo será buscado e entregue ao requisitante. Ao executar essa ação, o servidor guarda cópia da requisição em seu cache. Isso permite que, em uma futura busca, haja diminuição de latência, bem como redução no uso da banda utilizada na comunicação de dados, gerando melhoria nesse sentido.

Embora o conceito seja simples, sua implementação e execução passam por um quesito ainda mais crucial, que leva ainda maior importância à necessidade de implantação de uma estrutura virtualizada de rede: a disponibilidade a qualquer hora, em qualquer lugar.

A disponibilidade torna-se um diferencial quando o assunto é mobilidade. Todos sabemos que grandes decisões não possuem hora ou local para serem tomadas, e a necessidade do acesso a informações importantes é outro fator que não deve ser motivo de preocupações na empresa.

Tendo em vista estes fatores, apresentamos os serviços disponíveis para a empresa, visando acessibilidade, gerenciamento e disponibilidade de informações, dados e serviços em tempo real.

Os serviços VPN junto ao SSO, permite que terminais e o servidores da empresa possam ser acessados e configurados remotamente, diminuindo a necessidade de deslocamento de técnicos e administradores de serviços de TI até a instalação física do local. E ainda: em uma reunião de negócios ou visando planejamento estratégico, todos os dados necessários à sua execução estão disponíveis no momento necessário.

Com as configurações adequadas do serviço Active Directory, somente pessoas autorizadas poderão acessar determinadas informações, evitando assim que documentos possam ser visualizados por olhos não autorizados.

Enfim, existem inúmeras vantagens em se utilizar esse serviço, como a centralização de informações, prevenindo riscos de disponibilização não autorizada de logins e senhas; maior praticidade na manutenção, visto que a mesma pode ser feita remotamente; segurança e redução do desperdício de recursos; e maior agilidade e eficiência na replicação de matrizes do sistema.

Convém notar ainda que apesar das especificações mínimas, nada impede a implantação em hardwares mais velhos. Não seria viável, ou logicamente aceitável, contudo, que tanta informação pudesse trafegar desprotegida em um ambiente, por vezes, tão hostil quanto a internet. Exatamente por isso, a segurança das informações e dados é um item a ser tratado separadamente, e provavelmente o mais importante deles.

Segurança:

A questão primordial do acesso à informação nos dias atuais. Não pode haver qualquer risco à integridade das informações que trafegarão na rede virtual, seja ela a menor que for. Como sabemos, nos tempos atuais não existe método 100% seguro de prevenção ao acesso não autorizado à rede. No entanto, existem meios e métodos disponíveis para levar a quase 0 os riscos de tal situação.

1. SSH

Todas as conexões remotas, sejam elas quais forem, serão feitas utilizando a aplicação/protocolo SSH, que consiste em um canal de comunicação segura, em um meio inseguro, visando comunicação de dados e comandos remotos, bem como outros serviços de rede entre duas estações conectadas, por meio de códigos autenticadores de mensagem fortemente confiáveis. Uma conexão utilizando esse protocolo é capaz de impedir, por exemplo, ataques de IP spoofing, IP source routing e DNS spoof. Todo o tráfego transmitido por uma conexão SSH (como senhas e todo o conteúdo, como arquivos sendo transmitidos entre os hosts) é fortemente criptografado, sendo virtualmente impossível para um atacante tentar observar ("sniffar") e conseguir decodificar as mensagens trocadas entre os participantes da conexão em tempo hábil para que aquele conteúdo decifrado seja de alguma utilidade;

2. SERVIDOR PROXY

Já observamos que a utilização de servidores proxy visam aumentar a produtividade dos serviços executados. Mas não apenas isso. Os servidores proxy tem como principal finalidade servir de intermediário na comunicação entre cliente-servidor, na conexão com outros servidores. Utilizando de suas capacidades de filtragem de conteúdo, ele promove controle administrativo sobre tudo o que poderá ser trafegado em uma ou ambas as direções através do proxy, utilizando de autenticação do usuário, exatamente visando evitar quaisquer acessos não autorizados a conteúdos tidos como secretos pela organização. Combinado com o serviço DNS, o serviço ainda restringe acesso a páginas da internet não autorizadas, que poderiam infectar a rede, ou simplesmente diminuir a produtividade (como redes sociais, por exemplo).

Além disso, ainda promove o controle de autenticação por horário, impedindo que mesmo pessoas autorizadas a acessar determinadas partes da rede não o façam fora do horário de expediente, por exemplo. Adicionalmente, ele mantém a estrutura de rede da companhia em segredo utilizando de tradução de endereços de rede, o que torna todas as requisições de máquinas e usuários na rede anônimas a olhos externos.

Importante salientar ainda sua capacidade de verificar a autenticidade das informações trafegadas, por meio da sua integração com o servidor DHCP, permitindo somente o tráfego de pacotes provenientes de máquinas autorizadas

A sua utilização torna a rede praticamente 100% segura, especialmente se utilizado junto com um software firewall, tendo em vista que não há conexão direta com a internet, o que torna a tentativa de um invasor externo de tomar o controle quase impraticável.

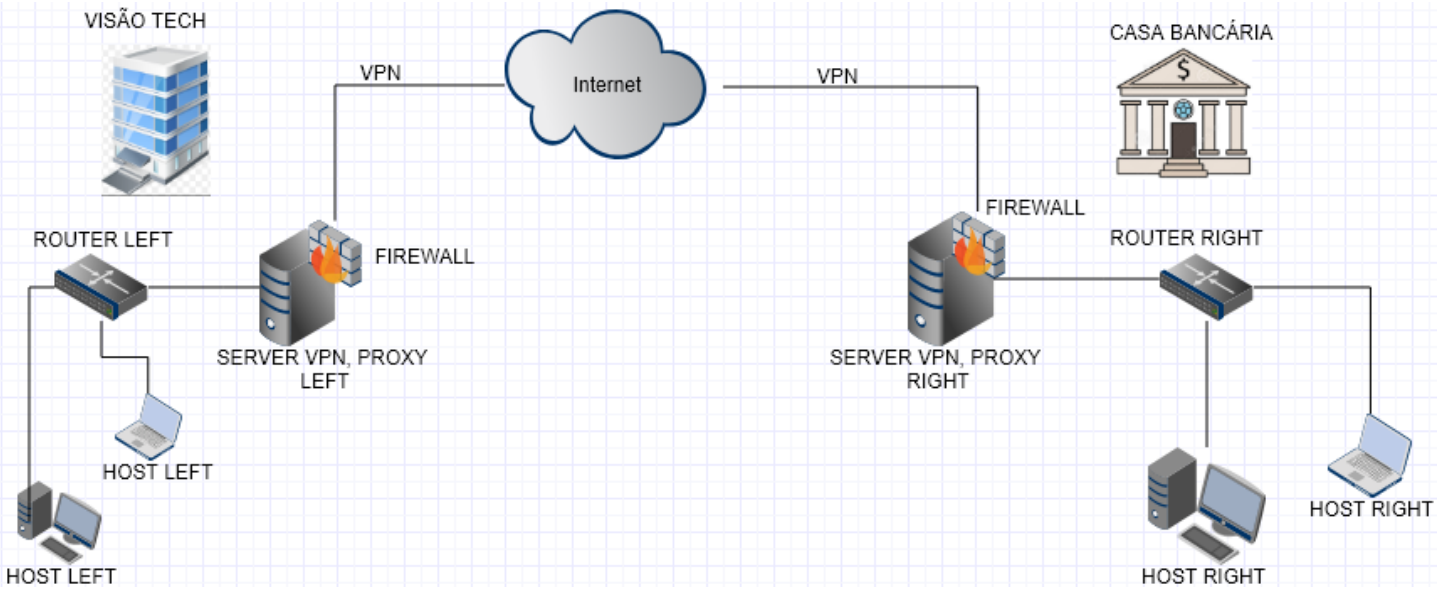
Uma grande quantidade de tráfego criptografado, seguro, em um ambiente não seguro, muito provavelmente irá atrair atenção indesejada de olhos curiosos e maliciosos. É certo que, independente dos esforços empreendidos para assegurar a integridade das informações de uma empresa, pode ainda haver momentos em que nem mesmo tais medidas de segurança são suficientes para barrar intrusos. Neste caso, uma solução seria utilização do método Honeypot,

Honeypots são métodos utilizados para atrair e capturar, identificar e, por vezes, contra-atacar tentativas não-autorizadas de utilizar os sistemas de informação disponíveis na rede da corporação. Sugerimos que o mesmo implantado já dentro do banco de dados implementado na empresa, tendo em vista que o firewall presente nele permite que haja configuração para honeypot.

Uma vez funcional, o mesmo irá direcionar toda tentativa de ataque identificada para ele, visando verificar, e capturar informações (endereço IP, por exemplo) do suposto invasor, enquanto mantém a rede segura, com a vantagem de capturar ataques que têm maior possibilidade de não serem percebidos, bem como reduzir falsos positivos.

Lembrando sempre que essa tática foi criada para ser comprometida. Não deve, de forma alguma, substituir nenhum dos serviços aqui listados.

ILUSTRAÇÃO DE CENÁRIO



Conclusão:

Esses serviços são de grande importância em termos de segurança e rapidez nas comunicação da empresa com os clientes, onde apresentam uma redução de custos e aumento de desempenho em seus serviços, é importante ressaltar que com os serviços da VPN, a empresa terá benefícios em tecnologia e uma melhora de serviços entre os demais departamentos que serão interligados entre os sistemas da empresa.

Os servidores proxy tem como principal finalidade servir de intermediário na comunicação entre cliente-servidor, na conexão com outros servidores. Utilizando de suas capacidades de filtragem de conteúdo, ele promove controle administrativo sobre tudo o que poderá ser trafegado em uma ou ambas as direções através do proxy, utilizando de autenticação do usuário, exatamente visando evitar quaisquer acessos não autorizados a conteúdos tidos como secretos pela organização. Combinado com o serviço DNS, o serviço ainda restringe acesso a páginas da internet não autorizadas, que poderiam infectar a rede, ou simplesmente diminuir a produtividade (como redes sociais, por exemplo).

O cliente terá os serviços VPN, DNS, DHCP, PROXY e SSH, mas só será garantido um bom funcionamento desses serviços com uma estrutura de SSO para fazer uma autenticação única no sistema. A empresa conseguirá alcançar boas medidas de produtividade com o alto ganho de eficiência que será oferecido pelo SSO que permite que o funcionário não perca tempo com múltiplos login de acessos aos sistemas implantados, permitindo assim que se obtenha mais agilidade nos serviços.