

Relatório Técnico: Proposta de uma Ferramenta para conexão VPN

Elaborador:	Thiago Luis Pimenta
Orientador:	Edson Gasetta

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS

Dados Internacionais de Catalogação-na-fonte

P697r PIMENTA, Thiago Luís

Relatório técnico: proposta de uma ferramenta para conexão VPN. / Thiago Luís Pimenta. – Americana, 2019.

21f.

Relatório técnico (Curso Superior de Tecnologia em Segurança da Informação) -
- Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica
Paula Souza

Orientador: Prof. Ms. Edson Roberto Gasetta

1 VPN – rede de computadores, I. GASETA, Edson Roberto II. Centro Estadual
de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

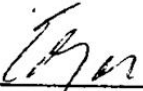
CDU: 681.519

Relatório Técnico: Proposta de uma Ferramenta para conexão VPN

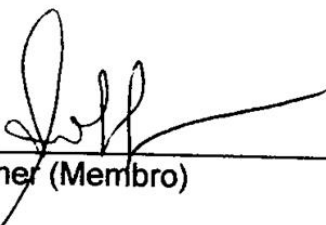
Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação, pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de Concentração: Segurança da Informação

Americana, 14 de junho de 2019.

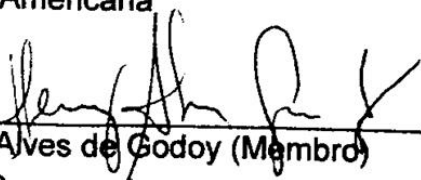
Banca Examinadora:



Edson Roberto Gaseta (Presidente)
Mestre
Fatec Americana



Renato Kraide Soffner (Membro)
Doutor
Fatec Americana



Henri Alves de Godoy (Membro)
Mestre
Fatec Americana

SUMÁRIO

1. Objetivo deste documento	05
2. Fundamentação teórica	06
2.1. Transferência de dados pela Internet	06
2.2. Criptografia	08
2.3. VPN	08
3. Cenários para implantação	08
3.1 Implantação da VPN.	10
3.2 Configuração VPN.	10
4. Resultados	19
5. Referências bibliográficas	21

Lista de figuras

Figura 1- Alguns Componentes da Internet.....	07
Figura 2- Cenário da rede corporativa.	09
Figura 3- Cenário das ilhas de edição.....	09
Figura 4- Cenário das ilhas de edição com o servidor VPN.	10
Figura 5- Configuração do Acesso Remoto.	11
Figura 6- Configuração do DirectAccess.....	11
Figura 7- Assistente de Configurações.	12
Figura 8- Assistente de Configurações VPN.....	12
Figura 9- Configuração do Roteamento e Acesso Remoto.	13
Figura 10- configurações personalizadas.....	13
Figura 11- Configurações personalizadas VPN.....	14
Figura 12- Iniciar Serviço.	14
Figura 13- Faixa de IP	15
Figura 14- Portas Habilitadas.....	16
Figura 15- Habilitar Firewall.	16
Figura 16- Habilitar Usuário	17
Figura 17- Configurar nova conexão VPN.....	18
Figura 18- Conectar.....	18

1. Objetivo deste documento

O objetivo da elaboração deste projeto é diminuir as ameaças de envio de arquivos de vídeos institucionais que são produzidos internamente na empresa que é uma provedora de tv a cabo, Internet e telefonia.

Os arquivos (vídeos) dizem respeito à informações sobre números e produtos da empresa e são direcionados apenas ao público interno, não devendo ser divulgados antes da permissão da diretoria responsável. Esses vídeos são capturados através de *camcorders* (câmera digital portátil que grava vídeo e áudio em dispositivos de armazenamento) e gravados em cartões de memórias do tipo SD criptografados, que depois são descarregados nas ilhas de edição (computadores de alta capacidade utilizados para edição de imagens e vídeos) para que a partir de então seja possível realizar sua finalização.

As ilhas de edição estão conectadas a Internet e estão fora da rede interna da empresa, ou seja, não contém as mesmas regras de *firewall* e *proxy* existentes na rede interna da companhia.

Após a edição, os mesmos são enviados em tamanho menor e baixa qualidade, para aprovação do departamento solicitante para possíveis alterações, estes que por muitas vezes nem sempre se encontram no mesmo prédio, cidade ou estado de onde está sendo realizado o procedimento e após a aprovação, os vídeos são enviados em alta qualidade e com tamanhos de variam de acordo com o tempo de duração de cada vídeo (normalmente os vídeos tem no mínimo uns de 500 a 700 Mb).

No primeiro momento para agilizar o processo de envio e recebimento, esses vídeos eram enviados para os solicitantes através de repositórios, como por exemplo: *Wetransfer*, *google drive*, *dropbox* e etc., porém afim de evitar o vazamento de dados esses repositórios foram bloqueados pelo departamento de segurança de informação que segundo a ABNT com sua norma ISO/IEC 17799:2001 é responsável pela:

"Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas".

Além dos repositórios, os dispositivos USB e de DVD também são bloqueados. Essas medidas foram tomadas após o levantamento da suspeita de que funcionários estariam negociando informações privilegiadas com concorrentes, o que acabou dificultando o trabalho do departamento de audiovisual ao precisar enviar ou receber grandes arquivos através da rede interna.

Como as ilhas de edição estão fora da rede interna, não há problema no envio e no recebimento dos arquivos, mas para o cliente que está na rede interna, o mesmo não conseguirá fazer o *download* dos *links* enviados desses repositórios.

Pensando na segurança do envio e recebimento destes, foi criada uma VPN (Virtual Private Network) que segundo (CYCLADES,2014):

"A Rede Virtual Privada ou Virtual Private Network (VPN) é uma das maneiras de interligar diferentes redes de organização, onde se utiliza para isso a rede Internet. Sua principal característica é criar um "túnel virtual" de comunicação que possibilita a interligação das redes, de modo que os dados possam trafegar de forma segura, ou seja, criptografados através dos túneis, aumentando assim a segurança e a recepção dos dados."

2. Fundamentação teórica

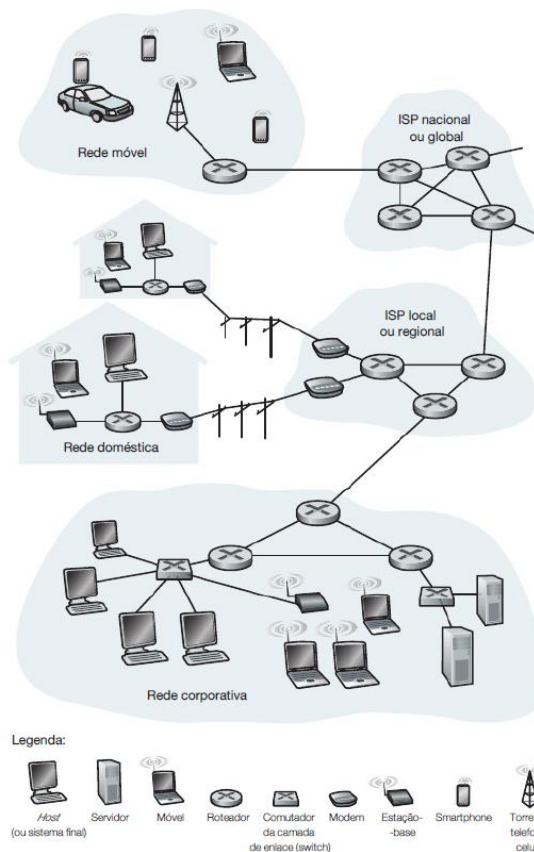
Neste capítulo serão abordados os conceitos, ferramentas e protocolos referentes a criação e execução de uma VPN, para facilitar o entendimento dos pontos que serão discutidos neste relatório técnico.

2.1. Transferência de dados pela Internet

Para entender o que é transferência de dados pela Internet, é necessário entender primeiro o que é Internet. Para isso apresenta-se como exemplo da figura 01, segundo Kurose, Ross (2015, p.2) existe diversas maneiras de descrevê-la:

“Primeiro, podemos descrever detalhadamente os aspectos principais da Internet, ou seja, os componentes de software e hardware básicos que a formam. Segundo, podemos descrever a Internet em termos de uma infraestrutura de redes que fornece serviços para aplicações distribuídas.”

Figura 1- Alguns Componentes da Internet



Fonte: KUROSE, Jim; ROSS, Keith (2013)

Resumidamente pode-se dizer que a Internet é um conjunto de computadores espalhados por todo o planeta, que através de um protocolo comum conseguem trocar dados e mensagens entre si.

Partindo desse princípio, a Internet é uma constante troca de informação entre máquinas e sistemas, e para isso ela utiliza alguns protocolos em comum que podem ser:

Toda essa estrutura de troca de dados é utilizada na transferência dos mesmos, desta forma, tornando-se mais segurança devido à configuração da VPN, onde os dados serão transmitidos de forma segura através do protocolo IPSEC, que é uma extensão de segurança do protocolo IP de criptografia da Internet para tunelamento, criptografia e autenticação. Para prover essa segurança que a VPN fornece no tráfego de dados, seria necessário criar uma rede a parte da rede pública, o que seria muito caro. Então para sintetizar o contexto deste relatório técnico, Kurose, Ross (2015, p.2) apresenta seguinte solução:

"Em vez de implementar e manter uma rede privada, hoje muitas instituições criam VPNs em cima da Internet pública. Com uma VPN, o tráfego interdepartamental é enviado por meio da Internet pública e não de uma rede fisicamente independente. Mas, para prover sigilo, esse tráfego é criptografado antes de entrar na Internet pública."

2.2. Criptografia

Embora seja um método muito antigo, de pelo menos a época de Júlio Cesar, a evolução da criptografia utilizada atualmente vem de progressos feitos somente de uns 40 anos atrás.

Sobre a criptografia, Kurose (2015, p. 34), declara:

"Técnicas criptográficas permitem que um remetente disfarce os dados de modo que um intruso não consiga obter nenhuma informação dos dados interceptados. O destinatário, é claro, deve estar habilitado a recuperar os dados iniciais a partir dos dados disfarçados."

2.3 VPN

Conforme já mencionado, VPN é um modo seguro de fazer a comunicação entre computadores ou entre filiais de empresas, utilizando a rede pública. E para que ela possa funcionar, são utilizadas duas ferramentas básicas de segurança:

- Tunelamento: O protocolo de comunicação estabelece um túnel por vários roteadores entre dois pontos que querem se comunicar.
- Encriptação dos Dados: As mensagens são enviadas de forma criptografadas por dentro desses túneis.

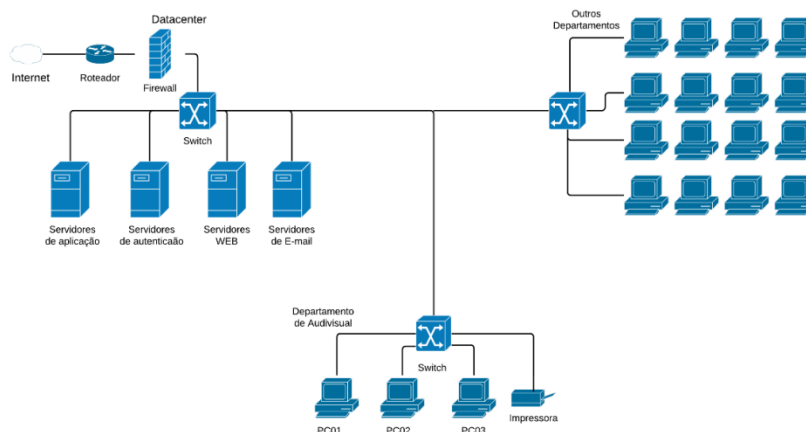
Com essas duas ferramentas são criadas duas camadas de segurança que se for identificado qualquer tentativa de quebra da segurança, o túnel inteiro é desfeito e é traçada uma nova rota através de roteadores diferentes.

Esses túneis VPN podem ser criados gateway-to-gateway que é dentro da rede da organização ou no próprio computador do usuário cliente-to-gateway que geralmente é utilizado para criar um extranet e conectar clientes e fornecedores que necessitam de acesso remoto.

3. Cenários para implantação

No cenário atual da empresa, encontra-se duas situações: na primeira os computadores ligados na rede interna da empresa conforme a figura 2, porém existe uma dificuldade de acesso por meio de dispositivos de armazenamento externo, já que as entradas de CD/DVD e USB são bloqueadas, além de o acesso aos sites de armazenamento em nuvens também serem bloqueados conforme já mencionado.

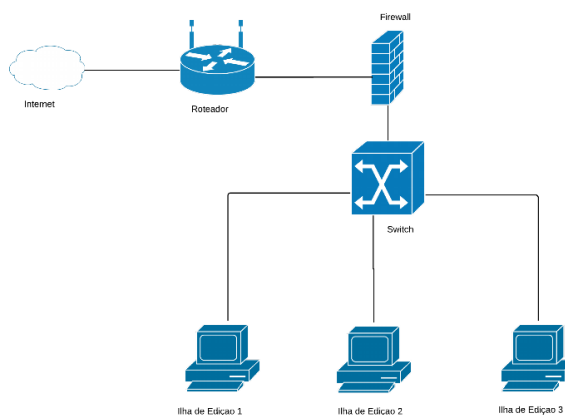
Figura 2- Cenário da rede corporativa.



Fonte: Próprio Autor

No outro cenário visto na figura 3, as ilhas de edição que são totalmente independentes da rede da empresa, estão ligadas apenas a um *switch*, *firewall* e um roteador. Essa rede é onde são editados e armazenados temporariamente os arquivos de vídeo requisitados pelas áreas da empresa. Após a finalização e entrega desses arquivos, as matrizes são apagadas e os arquivos finais são gravados em DVD's como forma de backup.

Figura 3- Cenário das ilhas de edição.



Fonte: Próprio Autor

3.1 Implantação da VPN.

Para implantar a VPN, será utilizado o segundo cenário, que é o das ilhas de edição, já que a troca de arquivos ocorre por lá e não influenciaria no andamento do trabalho do restante da empresa.

O servidor utilizado será um Windows Server 2012 r2, onde será implementada a VPN com armazenamento de arquivos e o *Active Directory* para o acesso dos usuários.

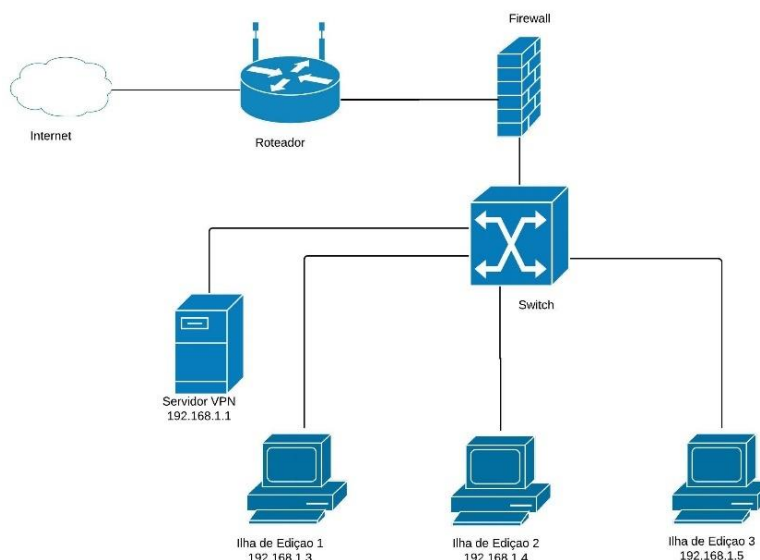
Sobre Active directory o site da Microsoft define que:

"AD armazena informações sobre contas de usuário, como nomes, senhas, números de telefone e assim por diante e permite que outros usuários autorizados na mesma rede acessem essas informações."

3.2 Configuração VPN.

Para redea configuração da VPN será utilizada a faixa de IP 192.169.1.0/24, onde as ilhas de edição receberão os IP's 192.168.1.2 ao 192.168.1.4, o servidor ficara com o IP 192.168.1.1 conforme figura 4.

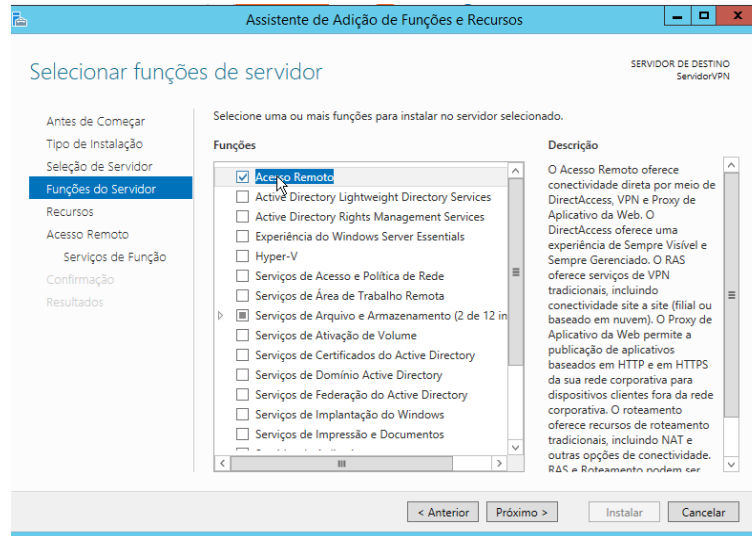
Figura 4- Cenário das ilhas de edição com o servidor VPN.



Fonte: Próprio Autor

No Gerenciador de Servidor do Windows Server 2012, selecionar a opção Ferramentas, em seguida selecionar Adicionar Funções e Recursos, após a seleção do servidor (192.168.1.1) selecionar Funções e Recursos e escolher a opção Acesso Remoto, conforme mostrado na figura 5.

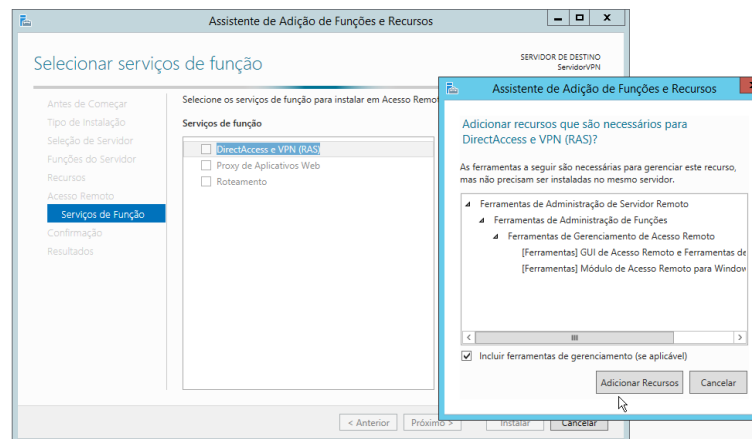
Figura 5- Configuração do Acesso Remoto.



Fonte: Próprio Autor

Em seguida selecione DirectAccess como visto na figura 6 e adicionar os recursos sugeridos na nova aba que abrirá. Clique em Avançar e depois em Instalar.

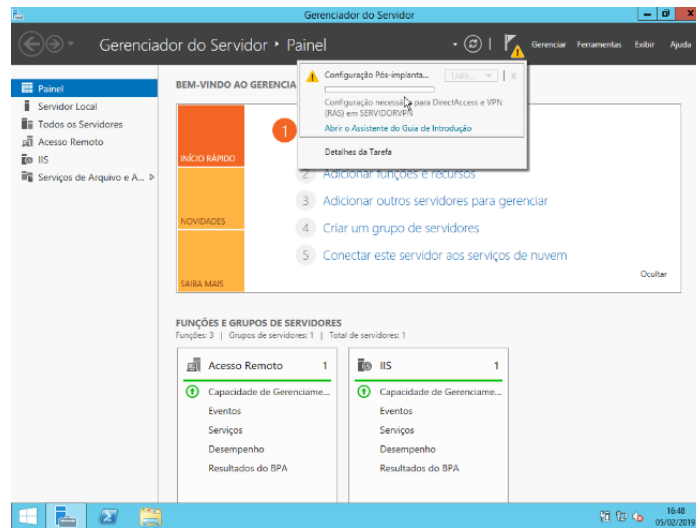
Figura 6- Configuração do DirectAccess.



Fonte: Próprio Autor

Após a instalação aparecerá um ícone amarelo na parte superior conforme figura 7, clique neste ícone para ver as configurações pendentes.

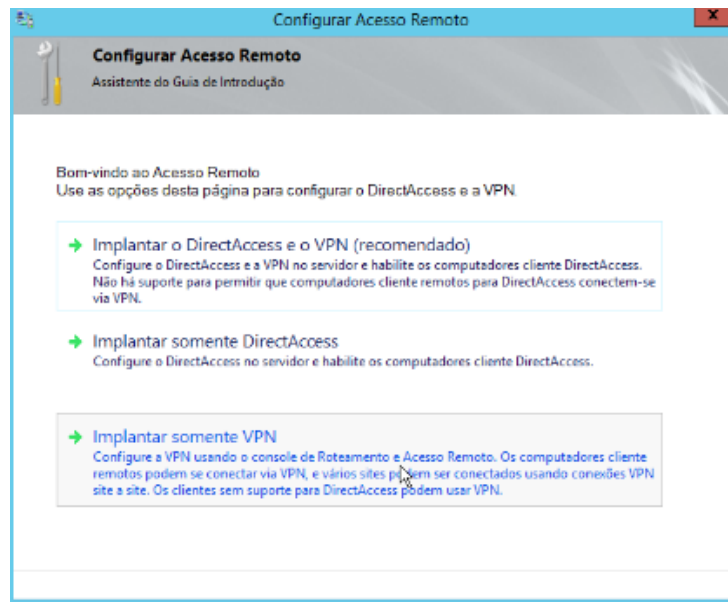
Figura 7- Assistente de Configurações.



Fonte: Próprio Autor

Na próxima janela como mostrado na figura 8 clique em Implantar somente VPN, já que será utilizado apenas este recurso.

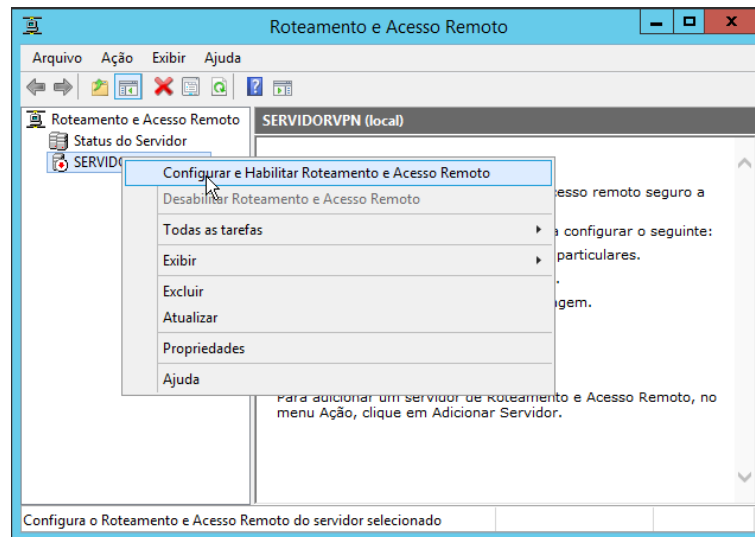
Figura 8- Assistente de Configurações VPN.



Fonte: Próprio Autor

Na janela de Roteamento e Acesso Remoto, clique com o botão direito em cima do Servidor e em seguida clique em Configurar e Habilitar Roteamento e Acesso Remoto como mostrado na figura 9.

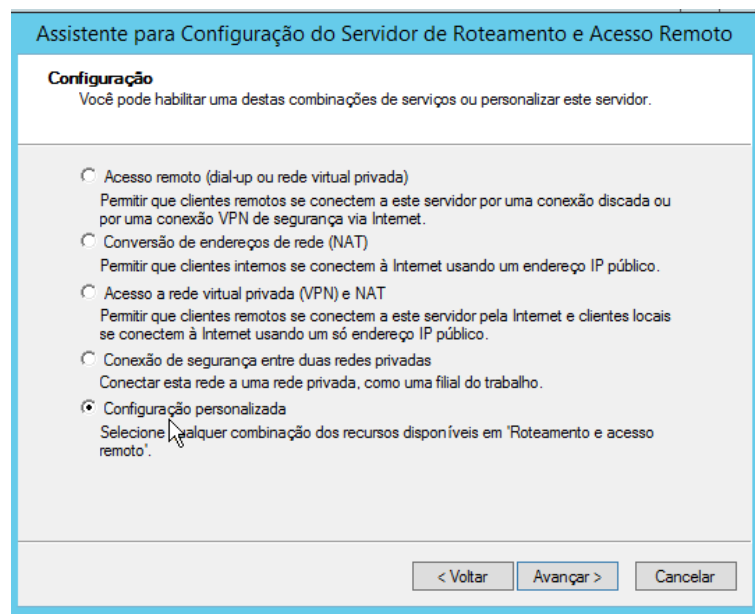
Figura 9- Configuração do Roteamento e Acesso Remoto.



Fonte: Próprio Autor

Em seguida abra uma janela com opções de serviços, clique em Configurações Personalizadas conforme figura 10.

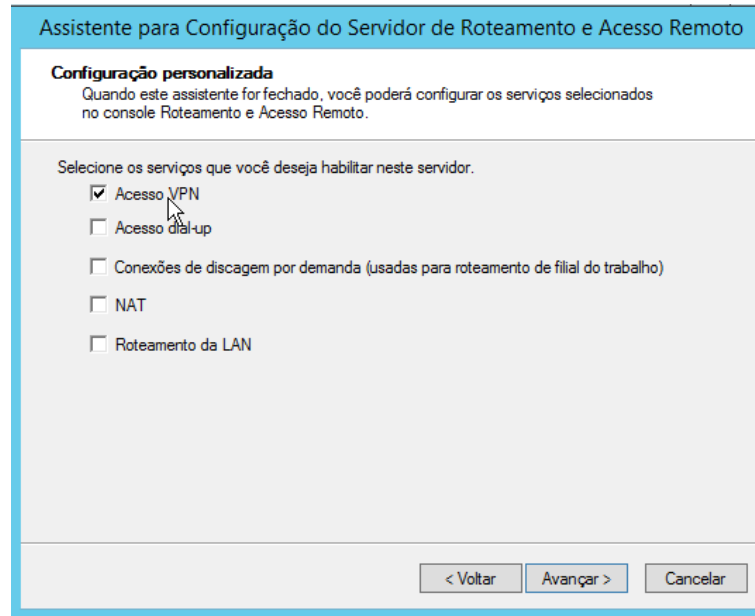
Figura 10- Configurações Personalizadas.



Fonte: Próprio Autor

Escolha a opção Acesso a VPN conforme figura 11.

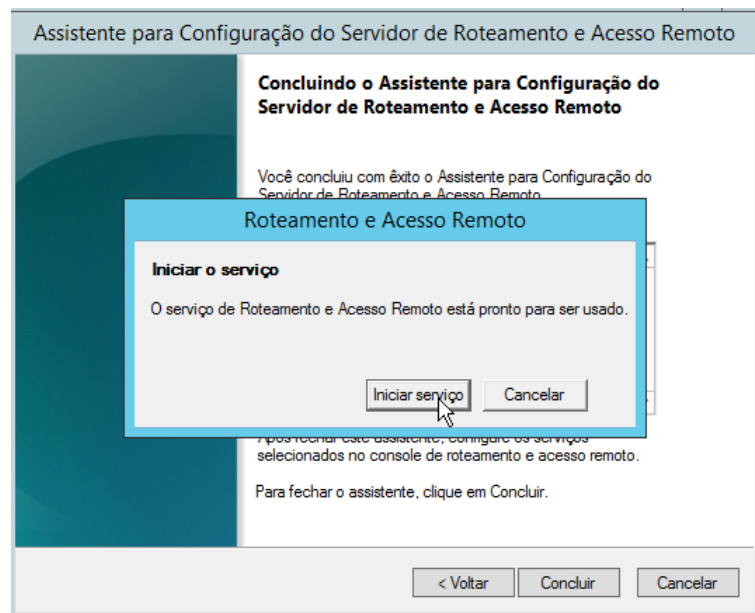
Figura 11- Configurações personalizadas VPN.



Fonte: Próprio Autor

Na próxima tela depois de Concluir inicie o serviço conforme figura 12.

Figura 12- Iniciar Serviço.

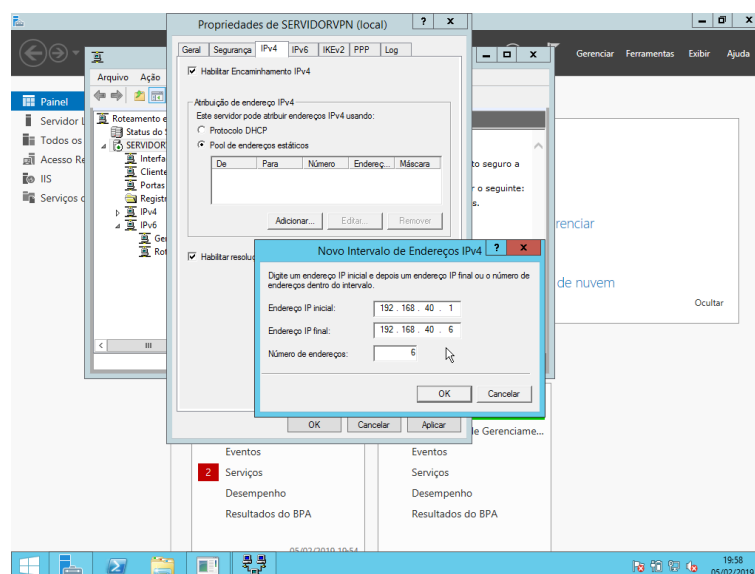


Fonte: Próprio Autor

Após a instalação, é necessário configurar a VPN, começando pela configuração da faixa de IP's que serão utilizados.

Clique novamente com o botão direito em cima do Servidor e vá em Propriedades, em seguida selecione a aba IPV4, nesta aba selecione a Pool de endereços estáticos ao invés de deixar no DHCP para dar mais segurança. Selecionando essa opção adicionar um intervalo de Ip's para apenas 6 máquinas para limitar o acesso. O intervalo de Ip's será do 192.168.40.1 ao 192.168.40.6 conforme figura 13. Note que a faixa de IP's é diferente dos da rede que está sendo utilizada, mas isso não tem problema, pois esses IP's serão os que vão ser atribuídos as máquinas que conectarão ao servidor VPN.

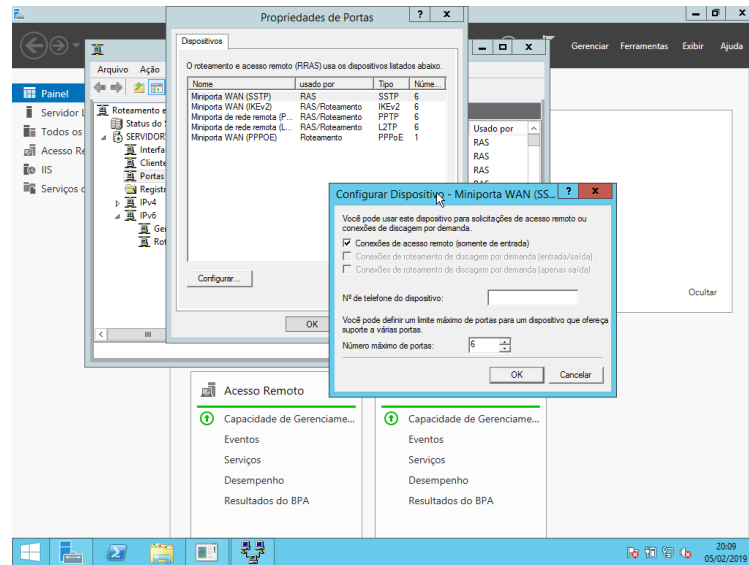
Figura 13- Faixa de IP.



Fonte: Próprio Autor

A próxima configuração é a configuração das portas que ficarão abertas, por padrão ele vem com 128 portas de cada protocolo aberta (SSTP, IKEv2, PPTP, L2TP), mas será deixada apenas 6 portas de cada. Para isso ainda em Roteamento e Acesso remoto clicar com o direito em cima Portas >Propriedades em seguida selecione cada um dos protocolos e em configurar, no lugar de 128 coloque 6 conforme figura 14. Repita esse procedimento em todos os protocolos que estão com 128 portas.

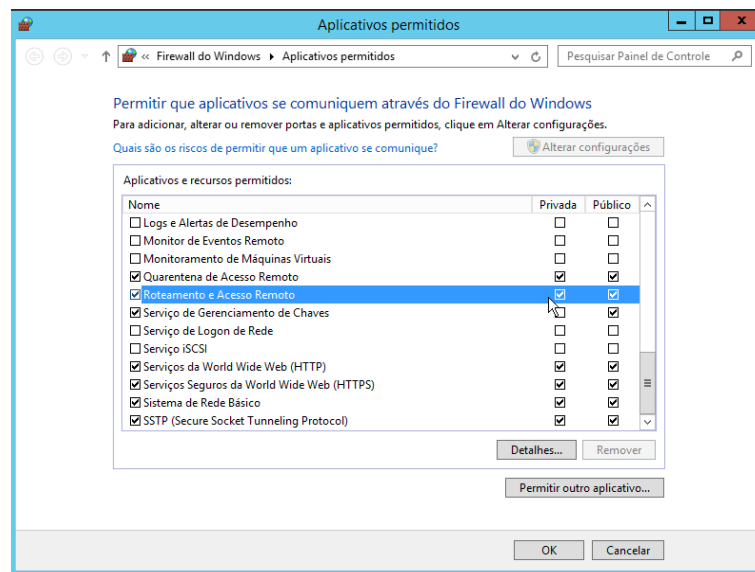
Figura 14- Portas Habilitadas.



Fonte: Próprio Autor

Após as configurações de portas é necessário a configuração do Firewall, para isso vamos em pesquisa e entrar em Permitir um aplicativo pelo firewall, em seguida procure Roteamento e Acesso Remoto visto na figura 15, selecione privada e público;

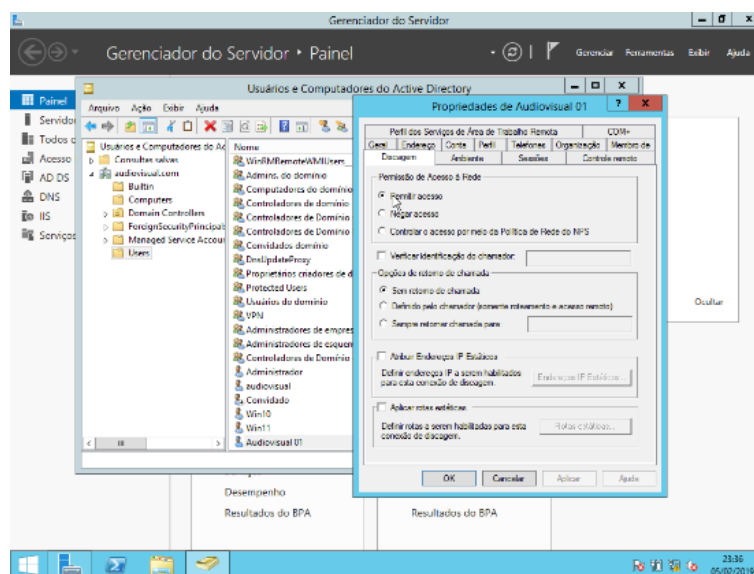
Figura 15- Habilitar Firewall.



Fonte: Próprio Autor

Com a VPN configurada é preciso confirmar os usuários que terão acesso ao servidor VPN. Para isso é necessário acessar o Gerenciador do Servidor > Ferramentas > Usuários e Computadores do Active Directory, no lado esquerdo clique em users e selecione no lado o usuário que poderá acessar a VPN (neste caso já havia um usuário para o audiovisual, caso necessário clique com o botão direito em user > novo > usuários e configure um novo usuário); com o botão direito nesse usuário e selecione propriedade, em seguida selecione a aba discagem e permitir acesso conforme figura 16. Após este procedimento clique em ok e o servidor VPN estará pronto para o acesso.

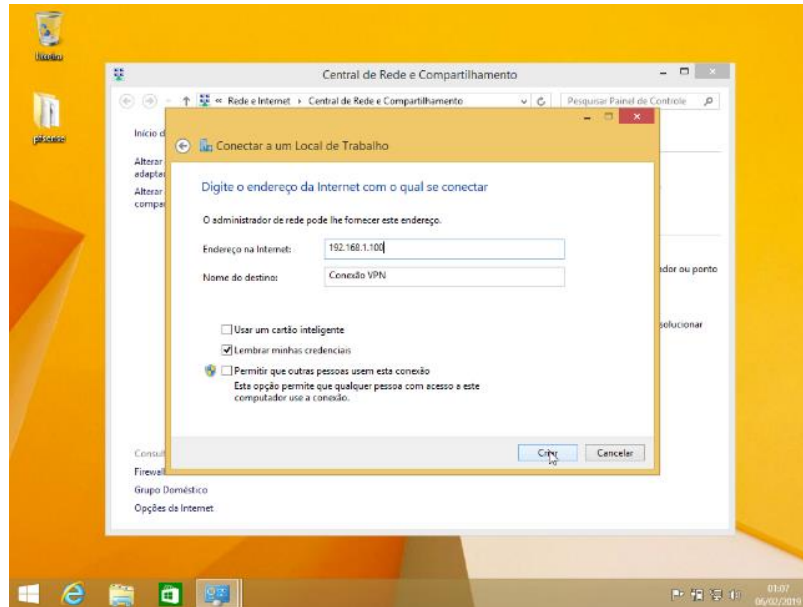
Figura 16- Habilitar Usuário.



Fonte: Próprio Autor

Após a configuração do servidor, é necessário configurar o computador do cliente que terá acesso aos arquivos pela VPN, para o acesso a ele, selecione Central de Rede e Compartilhamento e em seguida Configurar uma nova conexão ou rede. Na próxima janela basta eleger " Conectar a um local de trabalho" na próxima opção selecione em "Usar minha conexão com a Internet (VPN)". Após esses procedimentos resta configurar com o IP do servidor, se ele estiver diretamente ligado a Internet, ou o IP do seu roteador como no nosso caso conforme figura 17.

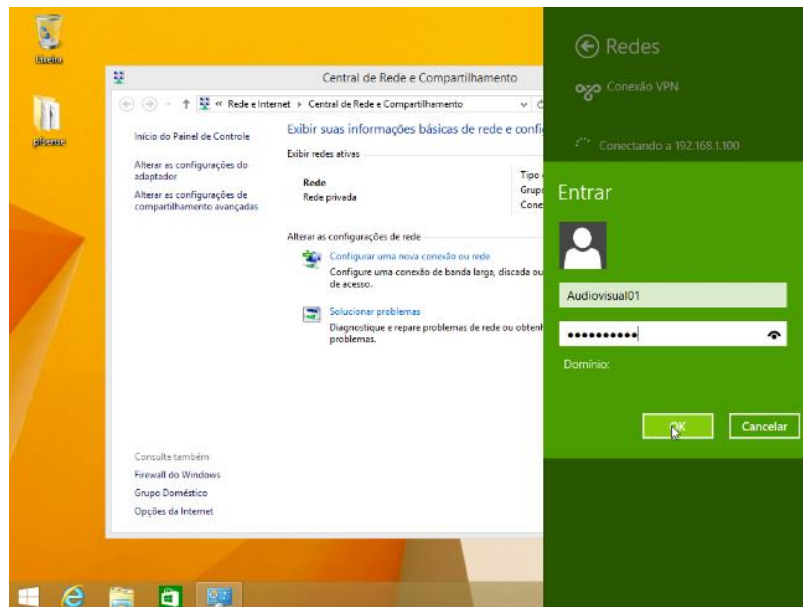
Figura 17- Configurar nova conexão VPN.



Fonte: Próprio Autor

Após as configurações, basta logar com o usuário e senha conforme figura 18 criado no AD do Servidor VPN e ter acesso as pastas compartilhadas de arquivos.

Figura 18- Conectar.



Fonte: Próprio Autor

4. Considerações finais

Após a implantação do servidor VPN nota-se uma maior autonomia do departamento de audiovisual e os departamentos clientes, pois haverá uma diminuição no número de chamados para liberação de portas e repositórios para a troca de arquivos.

Além disso, também uma melhora no desempenho da troca de arquivos, o que antes levava um tempo maior para subir o arquivo de um lado e baixar pelo outro, poderá ser feito apenas por um rumo, já que o servidor se encontra dentro do próprio departamento. A localização deste dentro do próprio departamento também ajudará na maior confiabilidade da segurança dos arquivos que não precisam mais passar por sites de terceiros antes de chegarem ao destino.

O nível de segurança da troca das informações também foi um fator preponderante, pois com os dados sendo trafegados em um túnel VPN criptografado garante a confidencialidade e a integridade da informação.

O custo da implantação deste projeto seria apenas para licença de Windows server, pois os equipamentos e infraestrutura de rede já encontram-se prontos, o valor segundo o site da Microsoft está em torno de \$ 500 dólares a versão Essentials para pequenas empresas de com até 25 usuários e 50 dispositivos.

5. Referências bibliográficas

KUROSE, Jim; ROSS, Keith. **Redes de computadores e a Internet: uma abordagem top-down**. 6ª Edição. São Paulo: Pearson, 2015.

Redes Privadas Virtuais VPN. Disponível em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2015_2/Seguranca/conteudo/Redes-Privadas-Virtuais-VPN/IPSec.html> Acessado em 08 Set. 2018

Moraes, Alexandre Fernandes de. **Firewalls Segurança no Controle de Acesso** 1ª Edição. São Paulo: Érica, 2015.

Visão geral do Active Directory Domain Services. Disponibilizado em : <<https://docs.microsoft.com/pt-br/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>> Acessado em Jun. 2019