

FUNDAÇÃO DE ASSISTÊNCIA E EDUCAÇÃO – FAESA
CURSO DE GRADUAÇÃO EM REDES DE COMPUTADORES

MATHEUS H. DUTRA RANGEL

PROJETO INTEGRADOR V-B

VITÓRIA
2023

MATHEUS H. DUTRA RANGEL

PROJETO INTEGRADOR V-B

Trabalho acadêmico do Curso de Graduação em Redes de Computadores, apresentado às Faculdades Integradas São Pedro como parte das exigências da disciplina projeto integrador V-B, sob orientação do(a) professor(a) Lorena Piza.

VITÓRIA
2023

Tarefas Solicitadas

- Análise das necessidades da empresa em termos de conectividade e segurança.
- Seleção dos equipamentos de rede adequados para implementar a rede de longa distância.
- Configuração dos equipamentos de rede, como roteadores, switches e firewalls, para garantir a segurança e eficiência da rede.
- Escolha do tipo de conexão de rede adequado para cada localidade, como fibra ótica, cabo de cobre ou conexão sem fio.
- Configuração de segurança, incluindo firewalls, VPNs e outros mecanismos de proteção.
- Testes de desempenho e solução de problemas na rede de longa distância.
- Apresente um relatório detalhado sobre a implementação da rede de longa distância, incluindo um cronograma de atividades, um diagrama de rede, desenho da rede lógica e física (como deve ser e segmentar), uma descrição da configuração dos equipamentos e uma análise dos resultados dos testes de desempenho e segurança.

Análise de requisitos

A empresa precisará possuir toda uma infraestrutura básica em cada um de seus três escritórios, contendo switches, roteadores e firewalls para ter a devida segurança, será necessário também a instalação da infraestrutura de rede sem fio com WLC (Wireless LAN Controller) ou apenas com um roteador à depender do tamanho do espaço físico dos escritórios em cada localidade.

Além disso dependendo da forma de trabalho dos colaboradores, caso for utilizado modelos de trabalho híbrido, onde podem trabalhar de home office, será necessário configuração de acesso dos mesmos via VPN à infraestrutura local dos respectivos escritórios. Além disso será necessária implantação de telefonia do tipo VOIP para a intercomunicação dos escritórios e comunicação externa.

Seleção de equipamentos

Para a rede em questão, deverão ser utilizados equipamentos recentes e que suportem os mais novos tipos de protocolos e tecnologias trazendo benefícios financeiros à empresa no que tange a troca destes componentes, pois terão um excelente desempenho além de longa vida útil.

Lan interna podem ser utilizados switches Cisco Catalyst 9200 ou Hp Aruba 2930 como switches de borda. Servidores para o gerenciamento dos usuários on premise, ou ainda a utilização de soluções em nuvem ou híbrido.

Segurança: deverá ter também uma aplicação firewall, para garantir que a rede fique segura e não haja nenhum problema relacionado à invasão, ou perda de dados. O mais indicado atualmente disponível no mercado e líder de vendas é o firewall Fortinet, porém existem outras opções no mercado, uma delas é o Pfsense, que é uma aplicação open source.

Dependendo da forma como será realizada a comunicação entre os escritórios, será necessário que a empresa invista em roteadores caso queria receber em um link direto as LAN's de cada filial por meio por exemplo de cabos de fibra ótica.

Configuração dos equipamentos de rede

Roteador: roteador realizará a conexão de Internet e configure a interface WAN com as informações fornecidas pelo provedor de serviços de Internet (ISP).

Switch: irá conectar os dispositivos locais (como computadores, impressoras, telefones VoIP) ao switch.

VLAN: para segmentar o tráfego de rede. Por exemplo, existirá uma VLAN para os computadores, e uma VLAN para os telefones VOIP.

Servidor DHCP: irá atribuir endereços IP automaticamente aos dispositivos da rede.

Firewall: Serão criadas regras de firewall para proteger a rede contra ameaças externas e internas.

VPN: entre as filiais, serão configuradas as informações da VPN no roteador para permitir a comunicação segura entre as redes.

Tipo de conexão

Para a implantação do cabeamento estruturado dos escritórios devem ser utilizados cabeamento UTP-CAT6 de cobre. Já para a ligação destes escritórios como descrito anteriormente deverá ser utilizado cabeamento de fibra ótica.

Configuração de segurança

Como comentado anteriormente, existem diversas soluções atualmente no mercado, podemos citar como as mais conhecidas a solução proprietária da fortinet, e também a versão open source da Pfsense.

Relatório de implementação

CONFIGURAÇÃO DAS VLANS

Será separado as VLANs dentro do restaurante, uma para a rede empresarial e outra VLAN para a disponibilização de acesso à Internet para os clientes. Essas VLAN terão seus tráfegos bloqueados entre elas através de configuração de firewall do Mikrotik, para haver uma maior segurança e a inibição de tentativas de invasão na rede principal, tanto da filial quanto da matriz. As VLANs utilizadas serão:

ID da VLAN	Utilização
1	Padrão
100	Rede empresarial
42	Rede para clientes
999	<i>Black hole</i>

No switch, será inserido como VLAN 100 modo access todas as portas em que equipamentos de rede empresarial irão se conectar diretamente. Nos pontos de acesso sem-fio iremos colocar como modo TRUNK e as VLANs 100 e 42, pois o único método de entrega de Internet para os clientes será por meio de conexão sem fio. Todas as outras portas que não forem utilizadas deverão entrar no modo shutdown e apontadas para a VLAN de black hole, que será a 999. Essa VLAN não possuirá gateway e não será roteável, para aumentar a segurança e não ser mais conectados nenhum equipamento adicional sem o conhecimento da equipe técnica de TI.

- **Configuração do dhcp**

A utilização do DHCP irá diferir entre as redes corporativa e a de clientes. Na rede corporativa, os equipamentos deverão ter os seus IP's fixados para prever um possível problema no roteador ou conflito de entrega de IP's. Se por algum motivo o roteador parar o seu funcionamento, a rede corporativa, através do switch e dos IP's fixos corretamente e na mesma subrede, poderão continuar comunicando-se entre si, já que os equipamentos locais estarão na mesma rede e não será necessário o roteamento dos pacotes.

Pensando dessa forma, o pool de DHCP não precisará ser grande, pois ele não poderá contemplar o range dos IP's dos equipamentos fixados. Outra configuração também que deve ser vista é o lease do DHCP, que no caso da rede corporativa poderá ser alto, sendo aproximadamente de 3 dias, pois os mesmos equipamentos serão sempre utilizados no mesmo local físico.

- **Configuração do roteador**

Dentro da infraestrutura, o roteador servirá como gateway da rede e o responsável com a conexão via VPN com a matriz. A rede da filial será apenas roteável com a matriz, não sendo configurada nem permitida o roteamento entre as filiais. Por padrão e regulação, o gateway terá o IP final de 254. Esse mesmo roteador também servirá de firewall e também como servidor DHCP da rede.

- **Conexão via pontos de acesso sem fio**

As conexões via wi-fi na rede da filial se dará de duas maneiras diferentes, uma forma para a conexão na rede corporativa e outra para a rede de clientes. A conexão com a rede de clientes se dará por método simples, utilizando uma SSID padrão para todas as filiais, pois todas as filiais terão a mesma rede. Com isso, caso o cliente quando sair de uma filial e for visitar uma outra, não será necessária uma nova tentativa de conexão, já que o dispositivo, se assim programado, poderá se conectar automaticamente na wifi. Será utilizado para essa conexão o padrão WPA2 Personal. com uma senha pré-definida e padrão, que poderá ser fornecida para o cliente se assim for necessário.

Referências

COMER, Douglas E. **Interligação de redes com TCP/IP**. Vol. 1 princípios, protocolo e arquitetura. 5ª. ed. Rio de Janeiro: Campus, 2006.

FILIPPETTI, Marco Aurélio., **CCNA 4.1: Guia Completo de Estudo**. Florianópolis: Editora Visual Books, 2008.

KUROSE, James F. **Redes de computadores e a Internet**. 5ª. ed. São Paulo: Pearson, 2010.