Documentação Técnica do Projeto de Rede Hospitalar

1. Introdução

Este documento apresenta a infraestrutura de rede projetada para um hospital de grande porte, com foco em segurança, alta disponibilidade e desempenho. O projeto foi concebido para ser implementado no Cisco Packet Tracer, simulando um ambiente real de rede hospitalar.

2. Pesquisa e Fundamentação

Para o desenvolvimento deste projeto, foi realizada uma pesquisa aprofundada sobre as necessidades e melhores práticas de infraestrutura de rede em ambientes hospitalares. Um hospital de grande porte é caracterizado por possuir **acima de 150 leitos, podendo chegar a mais de 500 leitos** [1]. A complexidade e a criticidade dos serviços de saúde exigem uma rede robusta e segura.

2.1. Equipamentos de Rede

Em um hospital de grande porte, a quantidade de equipamentos de rede é significativa para garantir a conectividade em todas as áreas. As estimativas indicam a necessidade de:

- **Roteadores:** 2 a 4 roteadores, incluindo roteadores de borda para conexão com a internet e roteadores internos para roteamento entre VLANs. A redundância é crucial para evitar pontos únicos de falha.
- **Switches:** Uma arquitetura hierárquica é essencial, com switches na camada de núcleo (core), distribuição e acesso. Um hospital com 500 leitos pode demandar **centenas de switches de acesso** (24 a 48 portas cada) para conectar todos os dispositivos finais, além de **10 a 20 switches de distribuição** e **2 switches core** de alta capacidade.
- **Access Points (APs) Wireless:** A cobertura Wi-Fi é vital em hospitais. Estima-se que um hospital de grande porte possa ter **centenas a milhares de APs** (ex: 200 a 1500+), dependendo da área e da densidade de dispositivos móveis e equipamentos médicos sem fio [2].

2.2. Servidores Essenciais

Os servidores desempenham um papel central na operação de um hospital moderno. Os principais tipos e suas funções são:

- **Servidor de Prontuários Eletrônicos (PEP/EHR):** Sistema central para armazenamento e gerenciamento de dados clínicos dos pacientes, incluindo histórico, exames, diagnósticos e prescrições. É um sistema crítico que exige alta disponibilidade e segurança dos dados.
- **Servidor PACS (Picture Archiving and Communication System):** Dedicado ao armazenamento, recuperação e distribuição de imagens médicas digitais (raio-X, tomografias, ressonâncias magnéticas). Requer grande capacidade de armazenamento e alta largura de banda para acesso rápido às imagens.
- **Servidor de Domínio (Active Directory/LDAP):** Gerencia a autenticação e autorização de usuários e dispositivos na rede, garantindo controle de acesso e segurança.
- **Servidor DNS (Domain Name System) e DHCP (Dynamic Host Configuration Protocol):** Serviços essenciais para a resolução de nomes de domínio para endereços IP e para a atribuição automática de endereços IP aos dispositivos na rede, respectivamente.

- **Servidor de Aplicações:** Hospeda diversas aplicações hospitalares, como sistemas de gestão hospitalar (HIS), sistemas de agendamento, faturamento, farmácia e laboratório.
- **Servidor de Banco de Dados:** Armazena os dados de todas as aplicações hospitalares, exigindo alta performance e redundância para garantir a integridade e disponibilidade das informações.
- **Servidor de Backup:** Responsável pela realização de backups regulares de todos os dados críticos do hospital, fundamental para a recuperação de desastres e conformidade com regulamentações de dados.
- **Servidor de Virtualização (Hypervisor):** Permite a criação e gerenciamento de máquinas virtuais, otimizando o uso de recursos de hardware e facilitando a escalabilidade e o gerenciamento de múltiplos servidores lógicos.
- **Servidor de Segurança (Firewall/IDS/IPS/Proxy):** Implementa políticas de segurança, filtra tráfego malicioso e detecta/previne intrusões, protegendo a rede contra ameaças cibernéticas.
- **Servidor de E-mail:** Gerencia a comunicação por e-mail interna e externa do hospital.
- **Servidor Web:** Hospeda o site institucional do hospital, portais para pacientes e outras aplicações web.
- **Servidor de Monitoramento:** Monitora o desempenho da rede, servidores e aplicações, alertando sobre problemas e auxiliando na manutenção proativa.

3. Arquitetura de Rede Proposta

A arquitetura de rede segue um modelo hierárquico de três camadas para otimizar o desempenho, a segurança e a escalabilidade:

- **Camada de Núcleo (Core):** Composta por dois switches Layer 3 redundantes, responsáveis pelo roteamento de alta velocidade entre as VLANs e pela interconexão com a internet.
- **Camada de Distribuição:** Agrega o tráfego da camada de acesso e aplica políticas de segurança e roteamento inter-VLAN. Cada switch de distribuição atende a um grupo de setores ou andares.
- **Camada de Acesso:** Conecta os dispositivos finais à rede, fornecendo portas com e sem PoE para computadores, telefones IP, Access Points e equipamentos médicos.

3.1. Esquema de Endereçamento IP e VLANs

O esquema de endereçamento IP utiliza a faixa privada **10.0.0.0/8** com VLSM para segmentação eficiente. A tabela a seguir detalha as VLANs e sub-redes para cada setor:

ID VLAN	Nome da VLAN (Setor)	Endereço de Rede	Máscara de Sub-rede	Endereço de Broadcast	Faixa de Hosts Úteis	Nº de Hosts
10	Administração	10.10.0.0	255.255.252.0 (/22)	10.10.3.255	10.10.0.1 - 10.10.3.254	1022
20	Clínico/Médico (Enfermarias)	10.20.0.0	255.255.248.0 (/21)	10.20.7.255	10.20.0.1 - 10.20.7.254	2046
30	UTIs	10.30.0.0	255.255.254.0 (/23)	10.30.1.255	10.30.0.1 - 10.30.1.254	510
40	Bloco Cirúrgico	10.40.0.0	255.255.254.0 (/23)	10.40.1.255	10.40.0.1 - 10.40.1.254	510
50	Emergência/Pronto Atendimento	10.50.0.0	255.255.252.0 (/22)	10.50.3.255	10.50.0.1 - 10.50.3.254	1022
60	Laboratórios	10.60.0.0	255.255.254.0 (/23)	10.60.1.255	10.60.0.1 - 10.60.1.254	510
70	Radiologia (PACS)	10.70.0.0	255.255.252.0 (/22)	10.70.3.255	10.70.0.1 - 10.70.3.254	1022
80	Farmácia	10.80.0.0	255.255.255.0 (/24)	10.80.0.255	10.80.0.1 - 10.80.0.254	254
90	Equipamentos Médicos (IoT)	10.90.0.0	255.255.248.0 (/21)	10.90.7.255	10.90.0.1 - 10.90.7.254	2046
100	Rede de Visitantes (Wi-Fi)	10.100.0.0	255.255.240.0 (/20)	10.100.15.255	10.100.0.1 - 10.100.15.254	4094
110	Voz (VoIP)	10.110.0.0	255.255.252.0 (/22)	10.110.3.255	10.110.0.1 - 10.110.3.254	1022
120	Segurança (CFTV)	10.120.0.0	255.255.252.0 (/22)	10.120.3.255	10.120.0.1 - 10.120.3.254	1022
200	Datacenter/Servidores	10.200.0.0	255.255.255.0 (/24)	10.200.0.255	10.200.0.1 - 10.200.0.254	254

3.2. Configuração dos Servidores

Os servidores estarão localizados na VLAN 200 (Datacenter) e terão as seguintes configurações:

Servidor	IP	Máscara	Gateway	Serviços
Servidor de Domínio (AD) / DNS / DHCP	10.200.0.10	255.255.255.0	10.200.0.1	Active Directory, DNS, DHCP
Servidor de Prontuários Eletrônicos (PEP)	10.200.0.11	255.255.255.0	10.200.0.1	Aplicação PEP, Banco de Dados
Servidor PACS	10.200.0.12	255.255.255.0	10.200.0.1	Armazenamento e comunicação de imagens médicas
Servidor de Aplicações (HIS)	10.200.0.13	255.255.255.0	10.200.0.1	Sistema de Gestão Hospitalar (HIS)
Servidor de Banco de Dados	10.200.0.14	255.255.255.0	10.200.0.1	Banco de dados para HIS e outras aplicações
Servidor de Backup	10.200.0.15	255.255.255.0	10.200.0.1	Software de Backup
Servidor de Virtualização	10.200.0.16	255.255.255.0	10.200.0.1	Hypervisor (VMware ESXi / Hyper-V)
Servidor de Segurança (Firewall/Proxy)	10.200.0.17	255.255.255.0	10.200.0.1	Firewall, Proxy, IDS/IPS
Servidor de E-mail	10.200.0.18	255.255.255.0	10.200.0.1	Servidor de E-mail (Exchange / Postfix)
Servidor Web	10.200.0.19	255.255.255.0	10.200.0.1	Site do hospital, Portal do Paciente
Servidor de Monitoramento	10.200.0.20	255.255.255.0	10.200.0.1	Zabbix / Nagios

4. Plano de Segurança de Rede

A segurança da rede hospitalar é primordial devido à sensibilidade dos dados dos pacientes e à criticidade dos serviços. As principais medidas de segurança incluem:

- **Segmentação de Rede (VLANs/Microsegmentação):** O uso de VLANs isola o tráfego de diferentes setores, contendo possíveis ataques e limitando o acesso a dados sensíveis. A microsegmentação pode ser implementada para isolar ainda mais dispositivos dentro de uma mesma VLAN.
- **Firewalls e IDS/IPS:** Firewalls robustos serão configurados na borda da rede e entre os segmentos internos para controlar o tráfego e proteger contra ameaças. Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS) monitorarão o tráfego em tempo real para identificar e bloquear atividades suspeitas.
- **Controle de Acesso Baseado em Funções (RBAC):** Garante que apenas usuários e dispositivos autorizados tenham acesso aos recursos e dados necessários para suas funções específicas, minimizando o risco de acesso não autorizado.
- **Autenticação Forte:** Implementação de senhas complexas e autenticação multifator (MFA) para acesso a sistemas críticos e dados sensíveis, adicionando uma camada extra de segurança.
- **Criptografia:** Todos os dados sensíveis em trânsito e em repouso serão criptografados para proteger a confidencialidade e integridade das informações dos pacientes.
- **Gerenciamento de Patches e Atualizações:** Manter todos os sistemas operacionais, aplicações e firmwares de equipamentos de rede atualizados é fundamental para corrigir vulnerabilidades conhecidas e proteger contra exploits.
- **Backup e Recuperação de Desastres:** Uma política robusta de backup e um plano de recuperação de desastres serão implementados para garantir a continuidade dos serviços e a recuperação rápida dos dados em caso de falhas, ataques cibernéticos ou desastres naturais.

- **Monitoramento Contínuo:** A rede será monitorada 24/7 para detectar atividades suspeitas, anomalias de tráfego e possíveis incidentes de segurança, permitindo uma resposta rápida e eficaz.
- **Treinamento de Conscientização em Segurança:** Todos os funcionários do hospital receberão treinamento regular sobre as ameaças cibernéticas e as melhores práticas de segurança para evitar ataques de engenharia social e outras vulnerabilidades humanas.
- **Conformidade com Regulamentações:** O projeto atenderá às regulamentações de proteção de dados de saúde, como a LGPD no Brasil e a HIPAA nos EUA, garantindo a privacidade e a segurança das informações dos pacientes.

5. Diagrama de Rede Conceitual

O diagrama de rede conceitual ilustra a topologia hierárquica e a segmentação por VLANs, representando a interconexão dos equipamentos de rede e servidores. (Vide arquivo `diagrama_rede_hospitalar.png`)

Referências

[1] FGV. (s.d.). *Parâmetros e Indicadores de Dimensionamento de Pessoas em Hospitais*. Disponível em: https://repositorio.fgv.br/bitstreams/ce9b66bd-5c15-497b-b674-b712458d6d62/download [2] Reddit. (2024, Julho 2). *Maneiras de abordar uma rede cheia de access points sem nome*. Disponível em: https://www.reddit.com/r/networking/comments/1dtghwy/ways_to_approach_a_network_full_of_unnamed_access/