1. INTRODUÇÃO

A SISTEMAS Ltda., uma startup de sucesso focada em SaaS, está passando por uma expansão substancial e busca melhorar sua infraestrutura de tecnologia. Este trabalho multidisciplinar aborda a reestruturação das redes, segurança de dados e compliance na empresa. O objetivo é otimizar o parque computacional para atender às necessidades dos sócios e garantir a integridade dos dados dos clientes. A proposta abrange estações de trabalho, servidores, impressoras e equipamentos de rede, visando a modernização e acomodação de uma força de trabalho remota. Nossa meta é contribuir para o crescimento da SISTEMAS Ltda. enquanto protegemos a segurança dos dados e a confiança dos clientes.

Fundamentos de Redes de Dados e Comunicações

Substituição do cabeamento: Utilize o MÉTODO COMPARATIVO, indicado na metodologia, considerando 3 fatores técnicos importantes para resolver as demandas de comunicação, faça uma comparação entre cabos UTP Cat 5e, 6, 6a e 7, e indique qual é o melhor cabo, e, caso haja empate, utilize como critério de desempate o fator “melhor custo”.

Resposta:

Largura de Banda (Taxa de Transferência):

A largura de banda refere-se à capacidade do cabo de transmitir dados a taxas mais elevadas. Quanto maior a largura de banda, melhor a capacidade de suportar tráfego de rede de alta velocidade.

Cat 5e: Suporta até 1000 Mbps (1 Gbps) a uma frequência de até 100 MHz.

Cat 6: Suporta até 10 Gbps a uma frequência de até 250 MHz.

Cat 6a: Suporta até 10 Gbps a uma frequência de até 500 MHz.

Cat 7: Suporta até 10 Gbps a uma frequência de até 600 MHz.

Comprimento Máximo Suportado:

O comprimento máximo de um cabo UTP influencia a cobertura da rede. Quanto maior o comprimento suportado, mais flexibilidade no layout da rede.

Cat 5e: Até 100 metros (328 pés).

Cat 6: Até 55 metros (180 pés) para 10 Gbps, mas até 100 metros para 1 Gbps.

Cat 6a: Até 100 metros para 10 Gbps.

Cat 7: Até 100 metros para 10 Gbps.

Custo (Fator de Desempate):

O custo dos cabos pode variar significativamente. É importante considerar o custo como um fator de desempate, caso os outros fatores sejam iguais.

Agora, comparando os cabos com base nos fatores técnicos e no custo:

Largura de Banda:

O Cat 7 oferece a maior largura de banda, seguido pelo Cat 6a, Cat 6 e Cat 5e.

Comprimento Máximo Suportado:

Todos os cabos suportam até 100 metros, tornando-os igualmente adequados nesse aspecto.

Custo:

O Cat 5e geralmente é o mais econômico, seguido pelo Cat 6. Os cabos Cat 6a e Cat 7 tendem a ser mais caros.

Considerando os fatores técnicos, o Cat 7 é a opção superior em termos de largura de banda. No entanto, como todos os cabos suportam até 100 metros, e o Cat 5e é mais econômico, você pode considerar o Cat 5e como uma escolha viável se o orçamento for um fator crítico.

Portanto, a recomendação final depende do equilíbrio entre o desempenho e o orçamento. Se a SISTEMAS Ltda. puder investir mais em cabos de maior desempenho, o Cat 7 seria a melhor escolha. Caso contrário, o Cat 5e pode ser suficiente para atender às demandas de comunicação com custos menores.

Substituição dos equipamentos de rede: Considerando o parque computacional da SISTEMAS Ltda., e a necessidade de melhorar a comunicação entre as estações de trabalho, selecione os equipamentos ideais para atender a este parque computacional, defina quais são os principais fatores para a escolha de cada equipamento, e usando o MÉTODO COMPARATIVO, indique quais equipamentos de rede devem ser comprados. Em caso de empate utilize como critério de desempate o fator “melhor custo”.

Resposta:

Capacidade de Switches/Roteadores:

A capacidade de comutação e encaminhamento deve atender à demanda da rede. Quanto maior a capacidade, melhor.

A quantidade de portas disponíveis deve acomodar todas as estações de trabalho e dispositivos de rede.

Velocidade das Portas:

Escolher switches com portas Gigabit Ethernet (1 Gbps) ou superiores para oferecer alta velocidade de comunicação.

Considere portas 10 Gigabit Ethernet (10 Gbps) para melhorar o desempenho.

Gerenciamento e Recursos:

Gerenciamento avançado, como VLANs, QoS, e recursos de segurança, é importante para otimizar a rede.

Redundância e alta disponibilidade são cruciais para evitar interrupções.

Conectividade Wi-Fi:

A necessidade de cobertura Wi-Fi deve ser atendida com a inclusão de access points de alta qualidade.

Velocidades de Wi-Fi devem ser compatíveis com os dispositivos suportados.

Segurança e Políticas:

A capacidade de implementar políticas de segurança, firewall, e detecção de intrusão é importante.

Segurança de rede deve ser robusta para proteger os dados.

Custo:

O orçamento da empresa é um fator importante. É necessário encontrar um equilíbrio entre desempenho e custo.

Agora, vamos realizar uma comparação entre dois tipos de switches e access points com base nesses fatores técnicos:

Switches:

Switch A:

Capacidade de comutação: 48 portas Gigabit Ethernet, 4 portas 10 Gigabit SFP+

Gerenciamento avançado e recursos de segurança

Redundância e alta disponibilidade

Custo: Médio

Switch B:

Capacidade de comutação: 48 portas Gigabit Ethernet, 2 portas 10 Gigabit SFP+

Gerenciamento avançado e recursos de segurança

Redundância e alta disponibilidade

Custo: Ligeiramente menor que o Switch A

Access Points:

Access Point X:

Dual-band, suporta velocidades Wi-Fi de até 1.7 Gbps

Recursos de segurança avançados

Custo: Médio

Access Point Y:

Dual-band, suporta velocidades Wi-Fi de até 1.2 Gbps

Recursos de segurança avançados

Custo: Ligeiramente menor que o Access Point X

Usando o método comparativo com base nos fatores técnicos, podemos ver que:

Ambos os switches atendem bem às necessidades de capacidade e gerenciamento.

O Switch A possui mais portas 10 Gigabit, o que pode ser uma vantagem.

Ambos os access points oferecem velocidades Wi-Fi adequadas e recursos de segurança.

Para o desempate com base no custo, o Switch B e o Access Point Y têm custos ligeiramente menores do que suas contrapartes (Switch A e Access Point X).

Portanto, com base no método comparativo, a recomendação seria adquirir o "Switch B" e o "Access Point Y". Eles oferecem um equilíbrio sólido entre desempenho e custo para atender às necessidades de comunicação da SISTEMAS Ltda.

Seleção de softwares para segurança da rede de dados: Mesmo considerando que os softwares que a empresa comercializa são SaaS e estão hospedados em nuvem, ainda assim é grande o volume de dados dos clientes que são acessados na empresa, e por isso os sócios desejam que sejam implementadas ou atualizadas as ferramentas de segurança da informação: Firewalls; Antivírus/Antimalware para redes; Gerenciamento de e-mails e AntiSpam; Softwares de Detecção e Prevenção de Intrusões (IDS/IPS); e Software de Backup e recuperação de dados. Ainda usando como metodologia o MÉTODO COMPARATIVO, defina para cada tipo de ferramenta 3 fatores importantes e 3 softwares de cada ferramenta. Ao final indique quais são os melhores softwares a serem adquiridos para cada necessidade

Resposta

Para selecionar os melhores softwares de segurança da rede de dados, é importante considerar os seguintes tipos de ferramentas de segurança: Firewalls, Antivírus/Antimalware para redes, Gerenciamento de e-mails e AntiSpam, Softwares de Detecção e Prevenção de Intrusões (IDS/IPS), e Software de Backup e recuperação de dados. Vamos avaliar três fatores importantes para cada tipo de ferramenta e, em seguida, listar três softwares para cada categoria:

Firewalls:

Recursos de Firewall: Os recursos de segurança, como filtragem de pacotes, inspeção profunda de pacotes e regras de firewall personalizáveis, são cruciais.

Facilidade de Gerenciamento: A capacidade de gerenciar regras e políticas de forma eficiente.

Integração com Outras Soluções: A capacidade de se integrar com outros sistemas de segurança.

Softwares de Firewall:

Cisco ASA (Adaptive Security Appliance)

Fortinet FortiGate

Palo Alto Networks Next-Generation Firewall (NGFW)

Antivírus/Antimalware para Redes:

Detecção de Ameaças: A capacidade de detectar e bloquear malware e ameaças em tempo real.

Atualizações de Definições: A frequência e eficácia das atualizações de definições de vírus.

Impacto no Desempenho: O software deve ser eficaz sem afetar negativamente o desempenho da rede.

Softwares de Antivírus/Antimalware para Redes:

Sophos Intercept X

Kaspersky Endpoint Security for Business

McAfee Endpoint Security

Gerenciamento de E-mails e AntiSpam:

Detecção de E-mails Maliciosos: A capacidade de identificar e bloquear e-mails maliciosos.

Personalização de Regras: A possibilidade de criar regras personalizadas para filtragem de e-mails.

Integração com E-mail Corporativo: Integração eficiente com sistemas de e-mail da empresa.

Softwares de Gerenciamento de E-mails e AntiSpam:

Barracuda Email Security Gateway

Symantec Email Security.cloud

Proofpoint Email Protection

Softwares de Detecção e Prevenção de Intrusões (IDS/IPS):

Detecção de Ameaças em Tempo Real: A capacidade de identificar intrusões e ameaças em tempo real.

Personalização de Regras: A flexibilidade para criar regras personalizadas de detecção.

Relatórios e Análise: A qualidade das informações e relatórios de ameaças.

Softwares de IDS/IPS:

Snort

Suricata

Cisco Firepower Threat Defense (FTD)

Software de Backup e Recuperação de Dados:

Recursos de Backup: A capacidade de fazer backups completos e incrementais.

Tempo de Recuperação: Quão rápido os dados podem ser recuperados em caso de falha.

Segurança dos Dados Armazenados: Proteção eficaz dos dados armazenados.

Softwares de Backup e Recuperação de Dados:

Veeam Backup & Replication

Acronis Backup

Veritas NetBackup

A escolha dos melhores softwares depende das necessidades e orçamento da SISTEMAS Ltda. No entanto, considerando um equilíbrio entre recursos, desempenho e custo, as recomendações seriam:

Firewall: Fortinet FortiGate

Antivírus/Antimalware para Redes: Sophos Intercept X

Gerenciamento de E-mails e AntiSpam: Barracuda Email Security Gateway

Software de Detecção e Prevenção de Intrusões (IDS/IPS): Snort

Software de Backup e Recuperação de Dados: Veeam Backup & Replication

Essas escolhas oferecem um equilíbrio entre proteção de segurança, desempenho e custo para atender às necessidades de segurança da rede de dados da empresa.

Laboratório de Arquitetura e Redes de Computadores (LARC) Usando como ferramenta o CISCO PACKET TRACER e considerando o parque computacional da SISTEMAS Ltda., elabore uma topologia física (apresentando os elementos interconectados em rede) e Lógica (apresentando as configurações de rede dos dispositivos: IP, máscara de rede, gateway e DNS). Considere também que os colaboradores das áreas de desenvolvimento e comercial acessam os serviços e dados da empresa remotamente. No elemento DESENVOLVIMENTO, no tópico PROTOCOLOS E SERVIÇOS DE REDE, apresente e explique as soluções propostas para a situação-problema. Descreva no mesmo tópico as topologias e testes feitos no CISCO PACKET TRACER. Apresente as topologias (foto/imagem) como Anexo do trabalho.

Como não é possível criar imagens ou diagramas no formato de anexo aqui, vou descrever uma topologia básica de rede no Cisco Packet Tracer e sugerir configurações gerais que podem ser aplicadas aos dispositivos nessa topologia. No entanto, a topologia real deve ser configurada de acordo com as necessidades específicas da SISTEMAS Ltda.

Topologia Física no Cisco Packet Tracer:

Vamos criar uma topologia simples com os seguintes dispositivos:

Roteador (representando a conexão com a internet)

Switch (representando a rede interna)

Servidor (representando o servidor de hospedagem de aplicativos)

Desktops/Notebooks (representando estações de trabalho)

Impressoras (representando as impressoras em rede)

Access Point (representando a rede Wi-Fi)

Configurações Gerais:

Roteador:

Configurar as interfaces WAN e LAN do roteador com os IPs públicos e privados, respectivamente.

Definir rotas estáticas para encaminhar o tráfego entre as redes.

Switch:

Configurar VLANs para segmentar a rede (por exemplo, uma VLAN para desenvolvimento e outra para a equipe comercial).

Configurar troncos para permitir a passagem de várias VLANs para o roteador.

Servidor:

Configurar o servidor com os serviços de hospedagem de aplicativos.

Definir IPs estáticos para garantir a consistência.

Desktops/Notebooks:

Configurar IPs, máscaras de sub-rede, gateway e servidores DNS nas estações de trabalho.

Impressoras:

Configurar as impressoras em rede e definir os IPs apropriados.

Access Point:

Configurar o Access Point para fornecer uma rede Wi-Fi segura.

Definir um SSID e configurar a segurança Wi-Fi (por exemplo, WPA2).

Configurações Lógicas (Exemplo):

Roteador:

Interface WAN: IP público

Interface LAN: IP privado (por exemplo, 192.168.1.1)

Configurar rotas estáticas para redirecionar o tráfego entre VLANs.

Switch:

Configurar VLAN 10 para a equipe de desenvolvimento (por exemplo, 192.168.10.0/24).

Configurar VLAN 20 para a equipe comercial (por exemplo, 192.168.20.0/24).

Configurar tronco para a interface do roteador.

Servidor:

Definir um IP estático dentro da faixa da VLAN relevante.

Desktops/Notebooks:

Configurar IPs, máscaras de sub-rede, gateway e servidores DNS com base na VLAN.

Access Point:

Configurar o SSID Wi-Fi com segurança (WPA2) e senha.

Testes:

Verifique a conectividade entre as estações de trabalho e o servidor.

Teste a conectividade da equipe de desenvolvimento e da equipe comercial.

Verifique a conectividade da rede Wi-Fi.

Teste a conectividade com a internet por meio do roteador.

Essa é uma topologia básica e configurações gerais. Para implementar a solução completa, é recomendável trabalhar com um especialista em redes que possa personalizar a configuração com base nas necessidades específicas da SISTEMAS Ltda. Além disso, é importante considerar a segurança da rede, implementar firewalls e medidas de proteção de dados.

Ética e Legislação Profissional Considerando que os sócios possuem uma especial preocupação com a proteção dos dados dos clientes e que grande parte dos colaboradores tem de forma direta ou indireta acesso a esses dados, você deve elaborar um Plano de Compliance com foco em determinar quais devem ser os cuidados com os dados de clientes, os dados pessoais e dados sensíveis. O plano deve dar ênfase às "Diretrizes Gerais de Segurança e Governança", "Condutas Vedadas" e "Práticas de Segurança" relacionadas à segurança da informação, além das "Medidas Disciplinares".

Plano de Compliance para Proteção de Dados de Clientes, Dados Pessoais e Dados Sensíveis

Objetivo:

O objetivo deste plano de compliance é estabelecer diretrizes e práticas que garantam a segurança e a privacidade dos dados de clientes, dados pessoais e dados sensíveis da SISTEMAS Ltda. Isso inclui a proteção de informações confidenciais, o cumprimento das leis de proteção de dados e a promoção de uma cultura de segurança da informação.

1. Diretrizes Gerais de Segurança e Governança:

1.1. Política de Segurança da Informação:

Estabelecer uma política de segurança da informação que defina os princípios, objetivos e responsabilidades relacionados à proteção de dados.

1.2. Classificação de Dados:

Classificar os dados armazenados e processados em categorias, como dados de clientes, dados pessoais e dados sensíveis, para aplicar medidas de segurança apropriadas.

1.3. Acesso Controlado:

Implementar um sistema de controle de acesso que restrinja o acesso apenas a colaboradores autorizados com base em princípios de necessidade e mínimo privilégio.

1.4. Criptografia:

Utilizar criptografia para proteger dados em trânsito e em repouso, especialmente dados sensíveis.

1.5. Monitoramento e Auditoria:

Implementar sistemas de monitoramento e auditoria para detectar e responder a eventos de segurança.

1.6. Treinamento em Segurança:

Fornecer treinamento em segurança da informação para todos os colaboradores.

2. Condutas Vedadas:

2.1. Divulgação Não Autorizada:

É vedada a divulgação não autorizada de informações confidenciais, incluindo dados de clientes, dados pessoais e dados sensíveis.

2.2. Acesso Não Autorizado:

É proibido o acesso não autorizado a sistemas e dados confidenciais.

2.3. Uso Não Autorizado:

É vedado o uso não autorizado de dados confidenciais para fins pessoais ou não relacionados ao trabalho.

3. Práticas de Segurança:

3.1. Segurança de Redes:

Implementar medidas de segurança de rede, como firewalls, IDS/IPS e atualizações regulares de segurança.

3.2. Backup e Recuperação:

Estabelecer rotinas de backup regulares e procedimentos de recuperação de desastres.

3.3. Segurança de E-mails:

Implementar filtros de anti-spam e antivírus para proteger contra ameaças por e-mail.

3.4. Gestão de Senhas:

Exigir senhas fortes e a troca periódica de senhas.

4. Medidas Disciplinares:

4.1. Não Conformidade:

Colaboradores que violarem as políticas de segurança e as condutas vedadas estarão sujeitos a medidas disciplinares, que podem incluir advertências, suspensões ou demissão, dependendo da gravidade da violação.

4.2. Ação Legal:

Violações graves podem resultar em ação legal, se necessário, de acordo com as leis aplicáveis.

5. Legislação Aplicável:

As práticas de segurança e políticas de proteção de dados devem cumprir todas as leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil.

6. Revisão e Atualização:

O plano de compliance deve ser revisado regularmente para garantir que esteja alinhado com as necessidades em constante evolução da empresa e as regulamentações aplicáveis.

A implementação deste plano de compliance garantirá que a SISTEMAS Ltda. esteja em conformidade com as leis de proteção de dados, promovendo a segurança e a privacidade dos dados dos clientes, dados pessoais e dados sensíveis. Além disso, ele cria uma cultura de segurança da informação entre os colaboradores.