
VLSM

Segurança de redes
Ferramentas que podem auxiliar

Professor Luis Silva

Professor Luis Silva

Professor especializado em Segurança de Redes, consultor para provedores de acesso e redes corporativas, empenhado na aplicação de boas práticas operacionais e disseminação de conhecimento através de workshops, palestras e treinamentos, possui experiência com arquitetura de redes de alta performance, OSPF, MPLS, VPLS, MPLS-TE, VPWS, CGNAT, BGP e backbones IPv6.

ALGUMAS PERGUNTAS IMPORTANTES

1

Como anda a disponibilidade de sua rede?

2

Como anda a documentação da sua infraestrutura?

3

Qual o conteúdo mais utilizado na sua rede?

4

Quanto da sua infraestrutura vem sendo fornecida para os malfeitores?

5

E ai, já implementou o IPv6?

VLSM

Vamos buscar algumas soluções juntos

1 - Como anda a disponibilidade de sua rede?

	DISPONIBILIDADE ANUAL (%)	INDISPONIBILIDADE ANUAL	INDISPONIBILIDADE MENSAL
Disponibilidade Continua	99,9999999	0,03 segundos	0,003 segundos
	99,999999	0,32 segundos	0,026 segundos
	99,99999	3,15 segundos	0,259 segundos
Alta Disponibilidade	99,9999	31,54 segundos	2,592 segundos
	99,999	5,26 minutos	25,92 segundos
	99,99	52,56 minutos	25,92 minutos
Disponibilidade Básica	99,9	8,76 horas	43,20 minutos
	99,5	43,80 horas	3,60 horas
	99,0	3,65 dias	7,20 horas

A BUSCA CONSTANTE

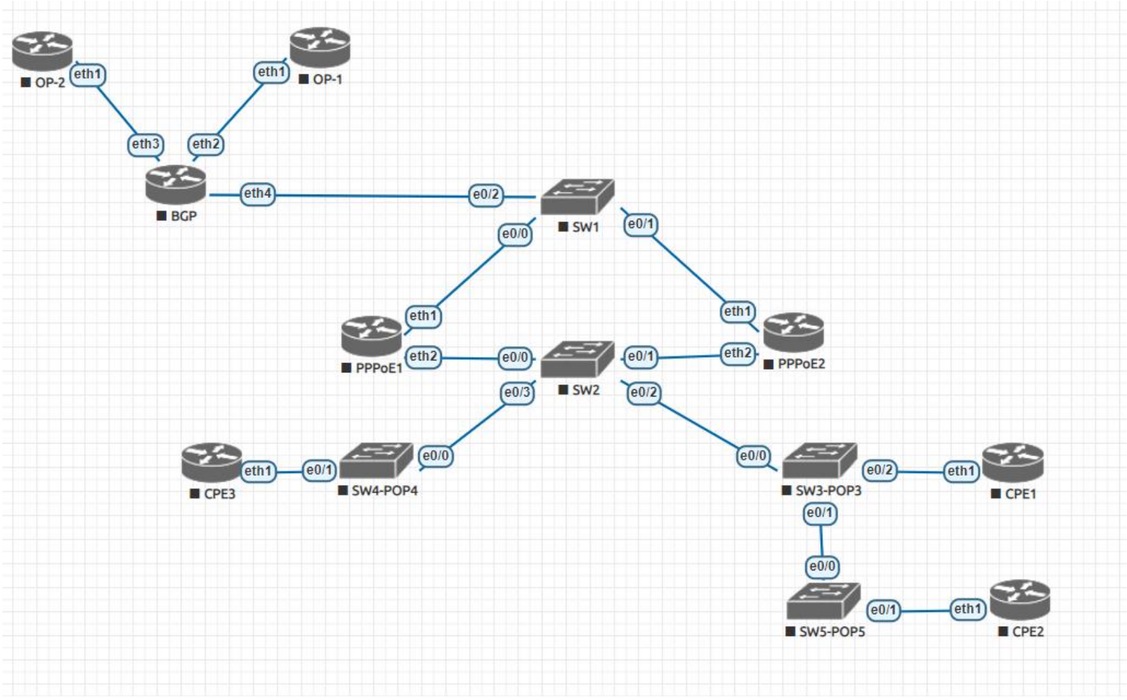
Ter 100% de disponibilidade parece absurdo, mas deve haver um foco grande em manter-se próximo a este nível de disponibilidade, 5 minutos sem internet hoje são extremamente impactantes.

VLSM

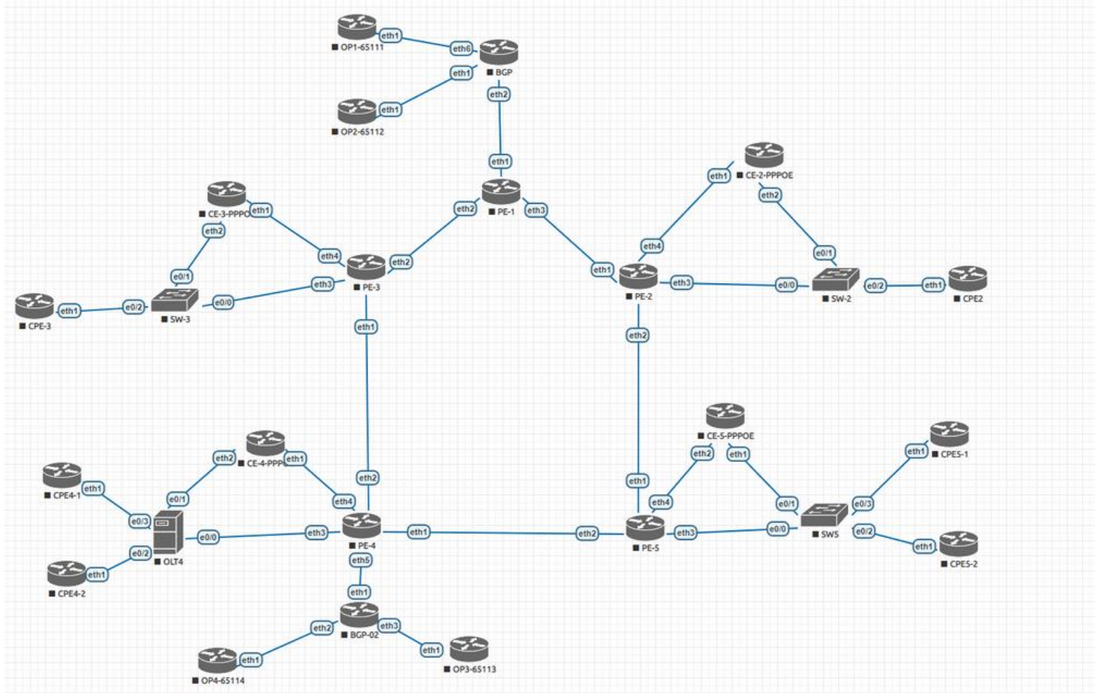
COMO SUA REDE SE PARECE

DISPONIBILIDADE AS VEZES COMEÇA COM PAPEL E CANETA...

MODELO I



MODELO II



VLSM

FERRAMENTAS QUE PODEM AJUDAR

ZABBIX

PRTG NETWORK MONITOR

Nagios®

IT Monitoring

Vamos buscar algumas soluções juntos

2 - Como anda a documentação da sua infraestrutura?

Documentar a rede é passo fundamental para otimização dos recursos da empresa, tanto no âmbito lógico, quanto na energia desprendida dos funcionários para executar determinadas tarefas, importante constar na documentação os seguintes itens:

- Documentação das rotas ópticas e conexões físicas no geral;
- IPAM (IP address management);
- Diagrama de topologia física e lógica;
- Documentação dos processos de resposta a incidentes de segurança.
- Controle de inventário;
- Controle das versões de firmware e afins;

Ferramentas que podem ajudar

NETBOX

No netbox é possível realizar a documentação de toda a rede lógica, gerenciar as alocações de IP, manter um histórico da disposição dos equipamentos no rack, bem como o controle de vlans, túneis em geral e VRFs utilizadas na infraestrutura, sua documentação está disponível em: https://docs.netbox.dev/en/stable/

LUCIDCHART

Ferramenta utilizada para o desenho da infraestrutura, o uso é bem simplificado e dispõe de diversas opções e layouts para utilização no modo gratuito, acesse através do link: https://www.lucidchart.com/

GEOGRID MAPS

Ótima ferramenta para documentação da rede física, possuí teste gratuito, porém para aproveitar todas as features é necessário adquirir uma licença, mais informações no site: https://www.geogridmaps.com.br/

Ferramentas que podem ajudar

O INVENT360 opera no ambiente de controle do inventário, otimizando o tempo e a tomada de decisão relacionada a compra de dispositivos, mais informações sobre o INVENT360 através do link:

https://ti.invent360.com.br

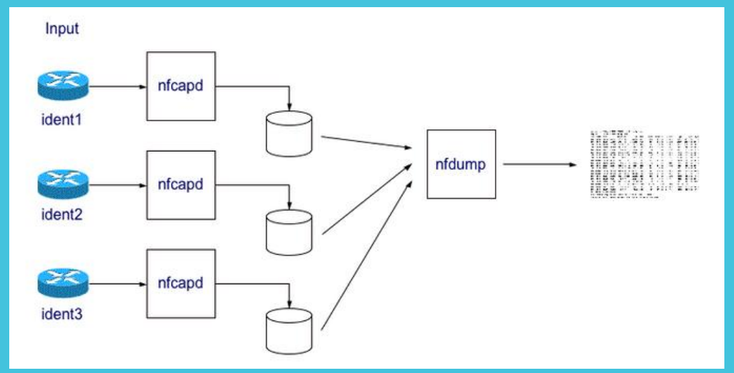
Vamos buscar algumas soluções juntos

3 - Qual o conteúdo mais utilizado na sua rede?

Entender pra onde vai seu tráfego é de suma importância para tomada de decisões estratégicas dentro da organização, dentre elas, muitos itens extremamente comentados como a aquisição da tão sonhada CDN, porém analisar a fundo o comportamento do tráfego vai além da solicitação de conteúdo, este pode ser um aliado muito forte no combate aos abusos de rede.

Vamos analisar algumas ferramentas que podem auxiliar nesse processo.

Ferramentas que podem ajudar



ELK

O Kibana é um plugin de visualização de dados de fonte aberta para o Elasticsearch. Ele fornece recursos de visualização em cima do conteúdo indexado em um cluster Elasticsearch. É possível obter dados via netflow e apresentá-los de forma organizada com a ferramenta: https://www.elastic.co/

NFDUMP+NFSEN

Conjunto de ferramentas de visualização dos dados de netflow, sua utilização é simples, porém nativamente não há opção de montar dashboards e demais facilidades, normalmente os pacotes para instalação estão disponíveis no linux via apt install.

FASTNETMON

Ferramenta utilizada para identificar possíveis anomalias voltadas ao abuso de rede, também opera utilizando netflow, é possível definir parâmetros e tomar algumas atitudes conforme o comportamento do tráfego, maiores informaçõs em: https://fastnetmon.com/

Vamos buscar algumas soluções juntos

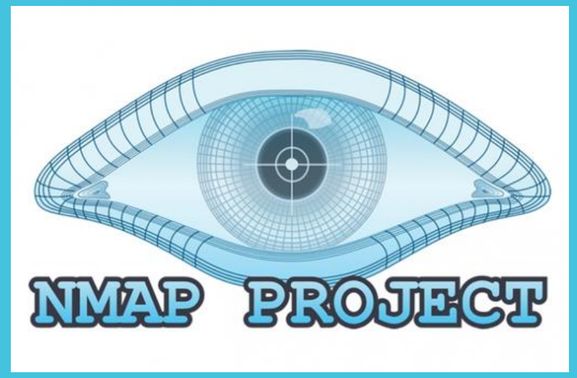
4 - Quanto da sua infraestrutura vem sendo fornecida para os malfeitores?

No atual estado dos ataques cibernéticos devemos nos preocupar não somente com ataques direcionados a nossa infraestrutura, mas também gerenciar nossas vulnerabilidades para que nossa rede não seja coparticipante de ataques pelo mundo afora.

Afinal, não queremos fornecer infraestrutura de modo gratuito para um agente malicioso.

É possível obter informações preciosas sobre sua rede a partir da internet, auditar a rede de tempos em tempos evita que tenha graves problemas com esse ambiente.

Ferramentas que podem ajudar



SHODAN

Identificar e limitar as ações dos atacantes é primordial, um site mantém uma base de scans realizados contra a internet em geral, pode ser considerado um "google do hacking" onde é possível avaliar as brechas e determinar um vetor de ataque, porém podemos utilizá-lo de forma proativa e bloquear possíveis incursões maliciosas, o site está disponível em: https://shodan.io/

NMAP

O bom e velho nmap vai te ajudar a identificar portas abertas, bem como validar suas possíveis brechas de segurança, é uma ferramenta importante para avaliar seu cenário periódicamente, existem outras opções ao nmap, como o próprio masscan que faz o processo com grande agilidade, ambos disponíveis no linux.

GVM OPENVAS

Para auxiliar no levantamento das CVEs relacionadas aos softwares utilizados na infraestrutura é possível utilizar o openvas, este tem a capacidade de classificar o nível de risco das vulnerabilidades identificadas, também disponível no linux.

Ferramentas que podem ajudar

Identificar as vulnerabilidades através das ferramentas descritas anteriormente é importantíssimo, porém ações devem ser tomadas, pra esse ambiente existe o Walled Garden a ferramenta é capaz de protegê-lo de mas de 140 mil agentes maliciosos, dentre eles propagadores de phishing, pedofilia, centrais de comando e controle, bots e uma infinidade de problemas de seguraça, a utilização do Walled Garden resulta na economia de recursos e tem implementação facilitada pois utiliza a estrutura de BGP para executar a limpeza de seu tráfego, mais informações em https://walledgarden.global/

A Team cymru oferece alguns serviços a comunidade de forma gratuita, os mais conhecidos são os feeds de Bogons via BGP e o UTRS.

Vamos buscar algumas soluções juntos

5 - Implementação do IPv6

Para estar 100% de acordo com o movimento de expansão da internet se faz necessário a implementação do IPv6, este foi criado para sanar o problema do número de recursos IPv4 existentes, é de suma importância criar um plano de endereçamento coerente para o IPv6, de forma organizada e devidamente documentado conforme comentamos nos slides anteriores, e por fim executar o processo de entrega em sua rede, não temos mais a desculpa que o conteúdo não existe em IPv6, tendo em vista que redes que executaram a implementação por completo já tem algo em torno de 55% - 60% do tráfego em IPv6.

Se ainda não implementou IPv6 corra, você está super atrasado...

UMA PREOCUPAÇÃO GLOBAL!

UMA PREOCUPAÇÃO GLOBAL!

IMPEDIR A PROPAGAÇÃO DE INFORMAÇÕES DE ROTEAMENTO INCORRETAS: GARANTE QUE SEUS ANÚNCIOS SEJAM SEUS BLOCOS IP E DE SEUS CLIENTES PELA DEFINIÇÃO DE POLÍTICAS DE ANÚNCIOS BGP E CRIAÇÃO DE FILTROS NO SEU ROTEADOR PARA GARANTIR QUE SUAS POLÍTICAS E DE SEUS CLIENTES ESTÃO SENDO SEGUIDAS.

IMPEDIR TRÁFEGO COM ENDEREÇOS IP DE ORIGEM FALSIFICADOS: GARANTE QUE OS ENDEREÇOS IP DE ORIGEM QUE SAEM DE SUA REDE NÃO SEJAM FALSIFICADOS APLICANDO TÉCNICAS DE "ANTISPOOFING", VER BOA PRÁTICA EM HTTPS://BCP.NIC.BR/ANTISPOOFING.

FACILITAR A COMUNICAÇÃO OPERACIONAL GLOBAL E A COORDENAÇÃO ENTRE OS OPERADORES DE REDE: GARANTE QUE SEUS CONTATOS ESTEJAM ATUALIZADOS E SEJAM ACESSÍVEIS POR TERCEIROS COM A ATUALIZAÇÃO DO REGISTRO WHOIS DO REGISTRO.BR E OUTRAS BASES DE DADOS COMO IRR E PEERINGDB.

FACILITAR A VALIDAÇÃO DE INFORMAÇÕES DE ROTEAMENTO EM ESCALA GLOBAL: O OPERADOR DE REDE DOCUMENTA PUBLICAMENTE SUA POLÍTICA DE ROTEAMENTO, OS ASNS E OS PREFIXOS QUE DEVEM SER ANUNCIADOS A TERCEIROS EM BASES EXTERNAS, COMO O IRR OU O RPKI.

ATENÇÃO

Múltiplo fator de autenticação;

Atualização dos dispositivos.

OBRIGADO

Prof. Luis Silva

Luis.silva@solintel.com.br

(43) 99168-4052

https://www.linkedin.com/in/Luis.5ilv4

https://www.instagram.com/luiss.f.silva/