Plano Inicial do Projeto

Links de Internet de 10 Gbps com AntiDDoS

Tribunal Regional Federal da 3ª Região

Versão 1.3
Julho/2022

Histórico de Revisões

DATA	VERSÃO	DESCRIÇÃO	AUTOR
13/07/2022	1.0	Documento inicial	Elias
17/08/2022	1.1	Revisão e atualização	Elias
19/08/2022	1.2	Revisão	Vinicius
22/08/2022	1.3	Revisão e atualização	Elias

1. Introdução

Este documento visa o estudo de solução para a contratação de dois links de Internet dedicados com larguras de banda de 10 Gbps para provimento de conexão à Internet. Os serviços serão entregues com abordagem simples, em meio terrestre, confeccionados com fibra ótica. Adicionalmente, ambos os links deverão fornecer serviço de mitigação AntiDDoS.

2. Situação Atual

No âmbito da Justiça Federal da 3ª Região – JF3R, as crescentes demandas na área de Tecnologia da Informação, principalmente dos sistemas processuais eletrônicos, requerem cada vez mais ferramentas e soluções que proporcionem segurança, disponibilidade, eficiência, escalabilidade e ganho de desempenho.

No que tange o serviço de interligação entre a JF3R e a INTERNET, ou mesmo entre unidades da JF3R, o art. 2º, inciso III da Resolução n.º 477/2018 do Conselho da Justiça Federal - CJF estabelece que a infraestrutura básica de Tecnologia da Informação do Conselho e da Justiça Federal de Primeiro e Segundo Graus observará a estrutura mínima padrão de links de comunicação de dados, redundantes sempre que justificável e possível, visando à comunicação de dados entre as unidades judiciárias e dessas com a INTERNET.

A crescente demanda por serviços em nuvem acaba por aumentar a necessidade de links de Internet adequados em quesitos como rapidez, estabilidade, resiliência, dentre outros.

Em relação à rapidez, podemos listar como as duas principais características de um link de Internet a largura de banda e a latência. Aplicações como videoconferências e streaming são responsáveis por boa parte do consumo dessa largura de banda nos links de Internet e são sensíveis a latências altas (e também a variação dos valores de latência durante um fluxo de dados). Exemplos dessas aplicações na JF3R incluem videoconferências usando o Microsoft Teams, entre equipes de trabalho, com fornecedores externos ou até mesmo em audiências judiciais. Também podemos citar transmissões ao vivo realizadas em eventos da JF3R pela plataforma do Youtube.

Além de rápido, é necessário que o link de Internet funcione dentro dos parâmetros técnicos especificados e da disponibilidade contratada. A estabilidade de

um link pode ser traduzida como um fator de confiança no serviço de conexão à Internet. Essa característica envolve fatores internos, como cabeamento e armazenamento adequados dos equipamentos no datacenter, mas também envolve fatores externos, como a garantia do provedor de serviços da disponibilidade do link respeitando o contrato firmado com a Instituição.

Sabendo que falhas podem existir, é importante considerar a capacidade de resiliência de um link de Internet. A resiliência no acesso à Internet pode ser abordada por mais de um ponto de vista, mas, especificamente em relação aos links de Internet que são objeto deste estudo, pensamos em mitigações de ataques DDoS, mais conhecidos como ataques de negação de serviço. A JF3R tem alta visibilidade na Internet para natureza de suas atividades e, também, pelo fato estar associada a um sistema autônomo (*autonomous system*, ou *AS*, em inglês). Ataques cibernéticos visando a indisponibilidade de serviços de um *AS* são cada vez mais comuns. Durante os últimos anos, inclusive, a própria JF3R passou a ser alvejada com maior frequência por ataques, o que motivou a contratação de serviço Anti-DDoS para os links de Internet atuais.

Com a previsão de aumento do percentual de servidores em trabalho presencial nas unidades da JF3R e tendo em vista o aumento da demanda de serviços em nuvem (*Onedrive*, no lugar dos servidores de arquivos locais; Correio em nuvem, no lugar do Correio Corporativo interno, entre outros), o consumo previsto é estimado bem acima da capacidade atual instalada de 3 Gbps (somando os serviços de acesso à Internet através do IX.BR, Algar e Wirelink).

No que tange o serviço de mitigação de DDoS, tem-se que ambientes corporativos estão sujeitos a riscos tecnológicos que se originam tanto dentro quanto fora da infraestrutura de rede.

Riscos externos têm como sujeitos atuantes, principalmente, crackers, que estão disseminados em diversos pontos do planeta, e riscos internos são originados do comprometimento dos dispositivos finais - *ENDPOINTs* e do comportamento incorreto de colaboradores.

Ataques de DDoS têm por objetivo esgotar os recursos disponíveis na infraestrutura de rede de uma organização, impossibilitando que usuários genuínos não consigam obter acessos aos sistemas disponibilizados, por meio de grandes

fluxos de tráfego que são oriundos de uma rede de computadores infectados, denominada BOTNET.

Em geral, os ataques de DDoS se enquadram nas seguintes categorias:

• **Ataques Volumétricos de DDoS:** Este tipo de ataque de *DDoS* tenta consumir a largura de banda dentro da rede/serviço ou entre a rede/serviço e a INTERNET.

• **Ataques DDoS de TCP State-Exhaustion:** Este tipo de ataque de *DDoS* tenta consumir as tabelas de estado da conexão que estão presentes em vários componentes de rede, como os Firewalls e os próprios servidores de aplicações. Mesmo dispositivos capazes de gerir milhões de conexões podem ser indisponibilizados.

• **Ataques DDoS de Camada de Aplicação:** Este tipo de ataque de *DDoS* pode ser muito eficaz, pois busca sobrecarregar um aspecto específico de um aplicativo ou serviço através de poucos atacantes, gerando uma baixa taxa de tráfego, tornando-o muito difícil de detectar e mitigar de forma proativa.

• **Ataques de Fragmentação**: Este tipo de ataque de *DDoS* envia inúmeros fragmentos TCP e UDP para uma vítima, sobrecarregando a capacidade da vítima de remontar os fluxos, reduzindo drasticamente seu desempenho.

Por possuir grandes corporações nacionais e internacionais, o Brasil também vem sendo alvo de ataques de DDoS, o que faz com que as organizações que aqui residam venham a se preocupar com ferramentas que possam mitigar tais ataques de modo que não gerem indisponibilidade em seus serviços.

Não diferente, a Justiça Federal da 3ª Região – JF3R é a maior instituição do poder judiciário do Brasil em volume de processos, necessitando proteger seus links de INTERNET e sua infraestrutura tecnológica de ataques DDoS.

Igualmente, a Lei n.º 13.709 - Lei Geral de Proteção de Dados – LGPD que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, que tem por objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, obriga as instituições privadas e públicas a lidar de forma organizada e sensata com os dados que estão em sua custódia, bem como investir em recursos de segurança da informação, visando protege-los de vazamento.

Conforme detalhamento descrito acima, faz-se necessária a abertura de certame licitatório para a contratação de serviços de interligação da JF3R à INTERNET através

de links com capacidade de prover redundância e *throughput* adequado, protegidos por um serviço de mitigação de DDoS que provê uma camada de segurança importante nos dias atuais.

O presente estudo tem por objetivo comparar a situação atual do acesso à Internet na JF3R, problemas encontrados com os links existentes e a proposta de contratação para melhoria do cenário.

2.1. Problemática

Com a flexibilização das normas sanitárias, o trabalho presencial passou a ser gradualmente retomado nas unidades da JF3R em SP e MS, com aproximadamente cerca de 20% do contingente de usuários.

Desde a adoção do trabalho remoto no período da pandemia de COVID-19, a a Secretaria de Tecnologia promoveu diversas mudanças na infraestrutura de serviços, principalmente para atender às novas e urgentes demandas do trabalho remoto. Isso significa que vários serviços que antes eram consumidos internamente, através de links exclusivamente privados, passaram a ser consumidos através da Internet, como atualização de endpoints (antivírus), servidor de arquivos e correio eletrônico.

Atualmente, a conexão à Internet da JF3R é fornecida por três links de Internet, cada um com largura de banda de 1 Gbps. Dois links são fornecidos pelas operadoras Wirelink e Algar. O terceiro link é uma conexão ao PTT de São Paulo, projeto conhecido com o IX.BR, através de serviço de conexão contratado da empresa WCS. Abaixo temos gráficos ilustrando o consumo destes links no último 1 ano de coleta.

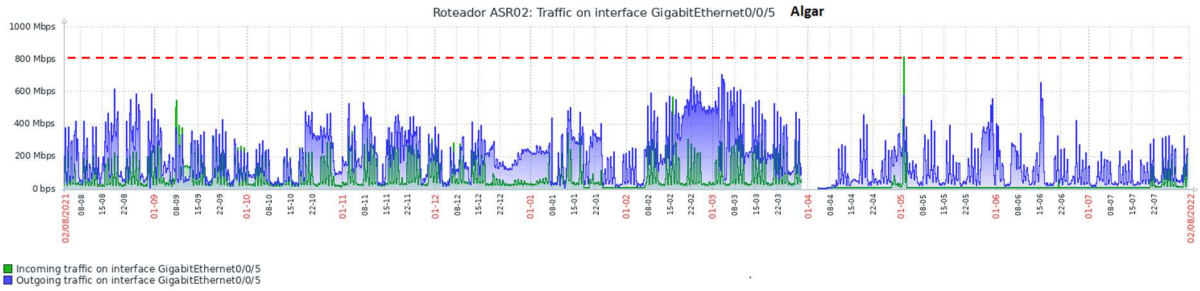

Figura 1- Consumo do Link de Internet da Algar num período de 1 ano

O gráfico acima nos mostra como se comportou o consumo de Internet no link da operadora Algar no período de 1 ano. Como podemos ver, mesmo com 20% de servidores em regime presencial, tivemos um alto consumo do link de Internet (perto ou acima de 50% da capacidade do link de 1 Gbps, ou seja, perto de 500 Mbps). Em

determinado momento, destacado pela linha tracejada vermelha, o consumo (download) alcançou valores perto de 80%. Fazendo um cálculo com regra de três, caso o percentual de servidores em regime presencial aumente para 50% (estimativa), podemos fazer uma projeção de demanda de 1,25 Gbps apenas neste link, o que não seria possível, uma vez que seu limite é de 1 Gbps.

Selecionamos os 10 últimos dias do gráfico da Figura 1 para uma análise mais detalhada. Neste período, fica mais evidente que o comportamento atual de utilização é de cerca de 50% da capacidade do link.

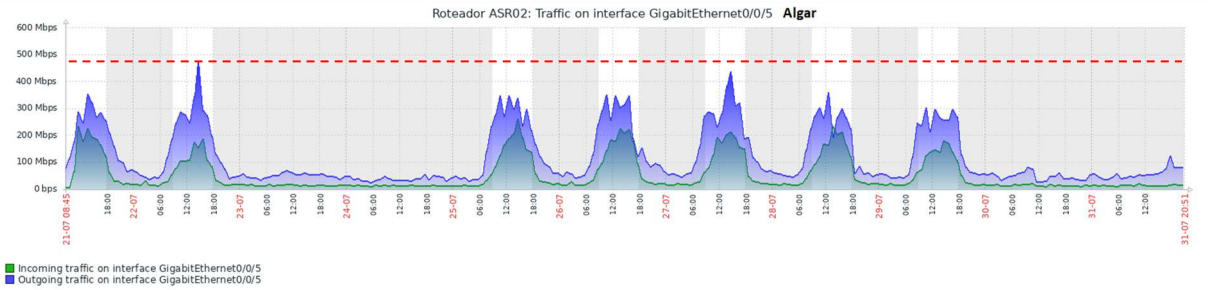

Figura 2- Consumo do Link de Internet da Algar num período de 10 dias

Aqui cabem duas observações importantes sobre o consumo capturado no ASR:

1) o tráfego pode ser originado na Torre Sul ou no Pedro Lessa. Contudo, essa é uma abstração útil no entendimento da origem da informação no *core* da rede do TRF3. Na prática, os sites Torre Sul e Pedro Lessa possuem outras origens de tráfego de locais que se conectam à eles, como o MPLS que liga interior de SP (conectado na Torre Sul), seções judiciárias do Administrativo Central e Fórum de Execuções Fiscais (conectados no Pedro Lessa), tráfego de proxy das subseções judiciárias de MS (conectados tanto na Torre Sul como no Pedro Lessa);
2) uma vez que o tráfego é analisado pelo FTD, ele é roteado para o gateway padrão, usando um IP virtual que responde pelos ASR. Uma vez que o pacote chega no ASR, a decisão de roteamento para a Internet será influenciada pelas rotas aprendidas via protocolo BGP. Isso significa que um pacote encaminhado pelo FTD do site Pedro Lessa ao ASR02 poderá ser roteado encaminhado para o link de Algar se essa operadora for a melhor rota para o destino. Caso contrário, se a melhor rota para o destino for via link da Wirelink ou IX.BR, o pacote será roteado do ASR02 para o ASR01 antes de ser encaminhado para

a Internet. O mesmo comportamento se aplica para o tráfego roteado do FTD da Torre Sul para o ASR01.

Dessa forma, também acreditamos ser interessante avaliar o tráfego interno de cada ASR destinado à Internet, pois isso nos dará uma visão da demanda por largura de banda, independente do caminho utilizado para alcançar a Internet (via ASR01 ou via ASR02, conforme explicado acima). Abaixo, temos dois gráficos demonstrando a demanda de acesso à Internet no site Pedro Lessa para os períodos de 1 ano e 10 dias, respectivamente.

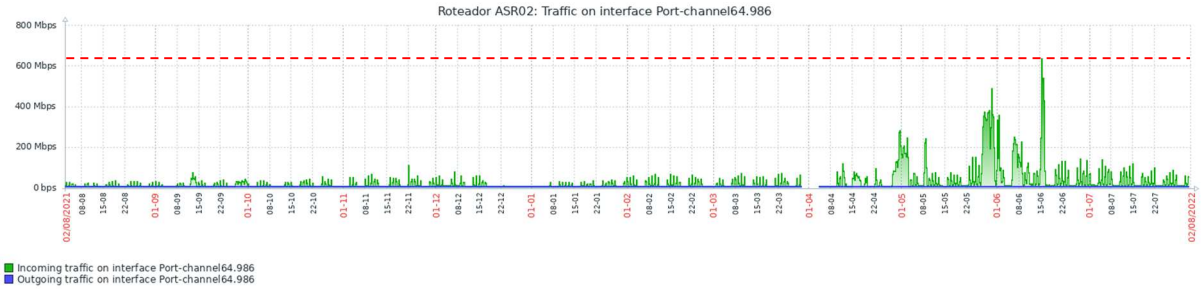

Figura 3 – Medição do tráfego de Internet no site Pedro Lessa num período de 1 ano

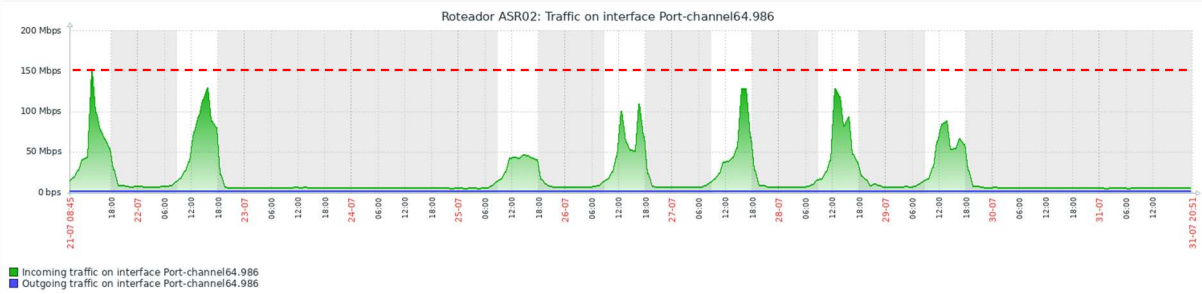

Figura 4- Medição do tráfego de Internet no site Pedro Lessa num período de 10 dias

O primeiro dado importante que temos nos gráficos acima é o pico de pouco mais de 600 Mbps de tráfego de Internet no site Pedro Lessa no mês de junho/2022. Nesse momento, independente do link por onde essa demanda foi atendida (Algar, Wirelink ou IX.BR), chama atenção que o tráfego de 20% de servidores presenciais que se origina nesse site alcance tamanho volume. Se considerarmos a capacidade total instalada de 3 Gbps para acesso à Internet, teremos 20% de consumo. Parece pouco, mas essa demanda não leva em consideração a demanda no site da Torre Sul, que será estudado em breve. Se esse mesmo comportamento se repetisse no site Torre Sul no mesmo dia, teríamos uma demanda de tráfego de 40% da capacidade instalada atualmente, porém, gerada por apenas 20% dos servidores

trabalhando presencialmente. Num cenário em que o percentual de servidores trabalhando presencialmente aumente para perto de 50%, poderíamos ter uma insuficiência de largura de banda para acesso à Internet.

O gráfico da Figura 4 nos mostra um consumo regular de cerca de 150 Mbps. Esse é um dado que, isoladamente, sugere uma boa utilização do link, um cenário de conforto para a demanda registrada. Contudo, também é interessante analisarmos esse gráfico em conjunto com a demanda interna para acesso à Internet registrada no Torre Sul. Como vimos na Figura 3, se esse valor subir rápida e expressivamente como ocorreu em junho, o estado da medição de largura de banda de Internet pode mudar de confortável para insuficiente.

A seguir, completaremos a análise do consumo de Internet observando as medições do tráfego de Internet no ASR01 e da Torre Sul.

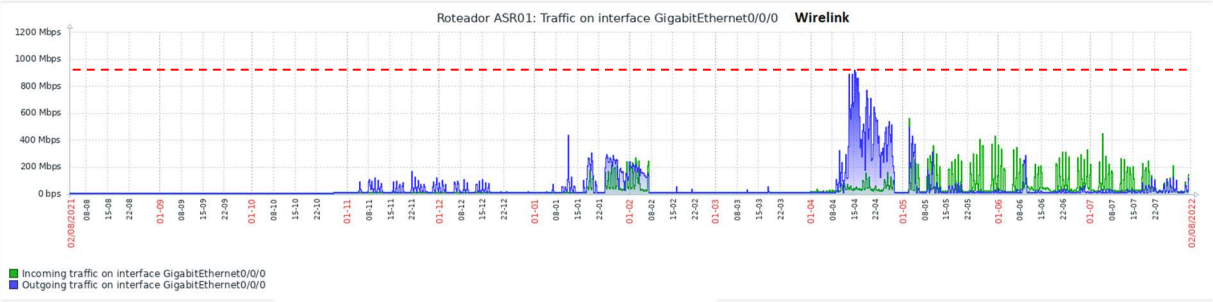

Figura 5- Consumo do Link de Internet da Wirelink num período de 1 ano

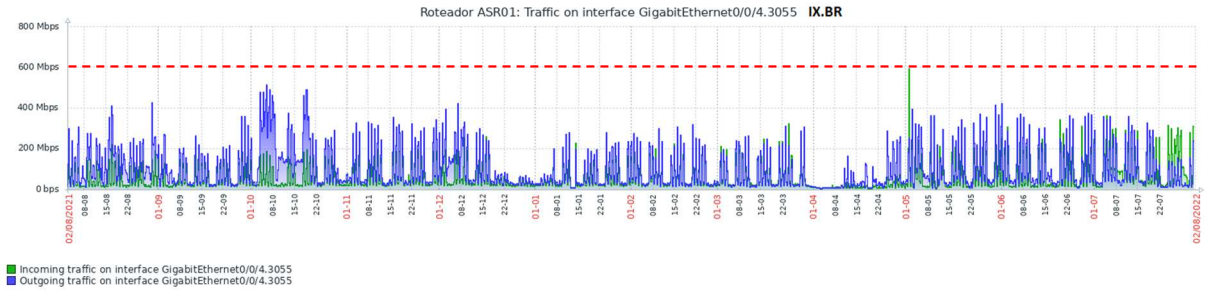

Figura 6- Consumo do Link de Internet do IX.BR num período de 1 ano

A Figura 5 exibe sintomas de problemas com o serviço da Wirelink. Por conta de uma má prestação do serviço, envolvendo demora no atendimento para identificação e resolução da causa do problema, foi necessário desligar a sessão BGP do ASR01 com a Wirelink por muito tempo. Em todo esse tempo, porém, quando vemos ausência de tráfego na Figura 5, podemos notar que o consumo de Internet estava resguardado pelo link com o IX.BR (Figura 6) e pelo link com a Algar (Figura 1). A lacuna perto do

dia 01/04/2022 representa a indisponibilidade dos serviços do TRF3 após o ataque cibernético ocorrido em 31/03/2022.

A presença do IX.BR, em nossa topologia, além de desempenhar um papel de redundância, também representa um ganho de latência, já que todo tráfego dos *AS* participantes do IX.BR sempre terá um número de saltos menor que qualquer operadora contratada (Wirelink ou Algar).

Observamos, também, que houve momentos de quase saturação do link da Wirelink (*upload*, em azul). Esse foi o pico de utilização registrado na Figura 5. Comparando o mesmo momento nos gráficos das Figuras 1 e 6, observamos que uma parte do tráfego de upload, ainda que pequena, estava sendo roteada pelo link IX.BR, evitando saturação do link da Wirelink naquele momento.

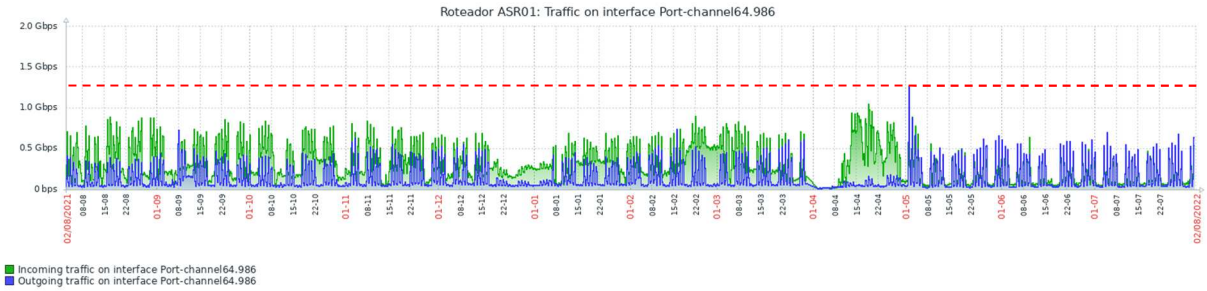

Figura 7- Medição do tráfego de Internet no site Torre Sul num período de 1 ano

Os gráficos a seguir mostram um recorte dos últimos 10 dias de cada gráfico apontando o período de 1 ano.

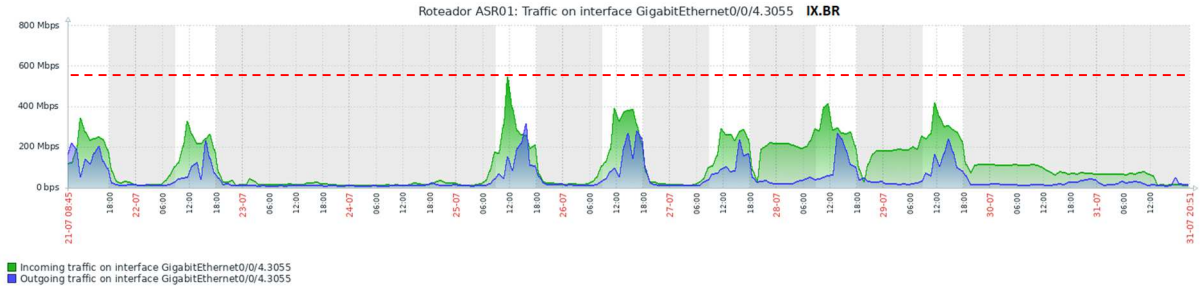

Figura 8- Consumo do Link de Internet IX.BR num período de 10 dias

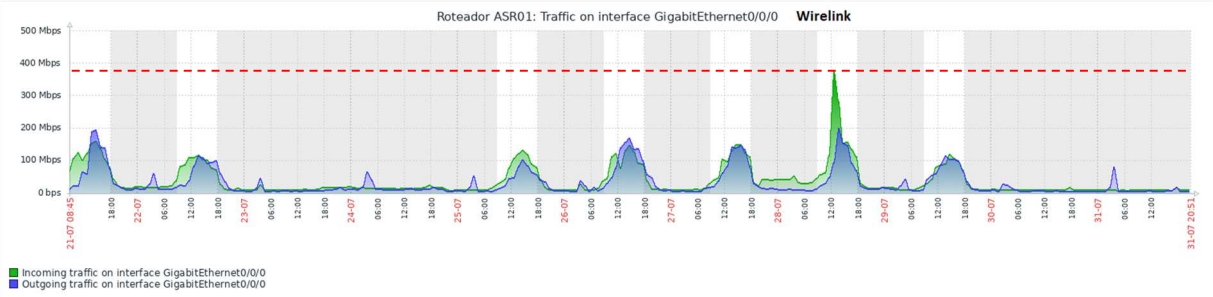

Figura 9- Consumo do Link de Internet da Wirelink num período de 10 dias

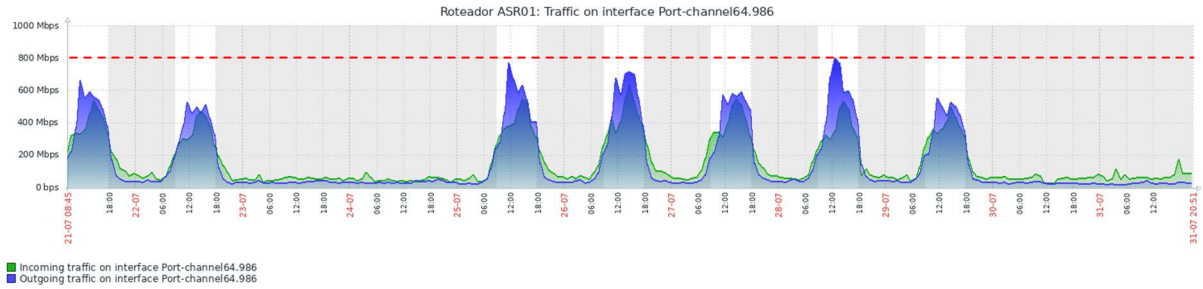

Figura 10- Medição do tráfego de Internet no site Torre Sul num período de 10 dias

Nessa amostragem mais recente, podemos perceber uma tendência de medição estável tanto para tráfego de *upload* (gráfico azul), quanto para *download* (gráfico verde). Ainda assim, notamos picos de utilização que, novamente, nos chamam a atenção pelo fato serem gerados por apenas 20% dos usuários em trabalho presencial na JF3R. Em 2022 quando o *OneDrive* substituiu os servidores de arquivo locais, notou-se uma incapacidade de os links de Internet atuais suportarem a demanda de tráfego, forçando um *rollback* daquela mudança para novamente os servidores de arquivos locais.

Para encerrar nosso ponto de vista sobre a crescente demanda e como projetamos um consumo muito maior de largura de banda dos links de Internet com o aumento do número de servidores em regime presencial, temos uma linha do tempo dos relatórios do proxy registrando o consumo semanal. Esses relatórios são gerados uma vez por semana consolidando o volume total trafegado na semana que se passou.

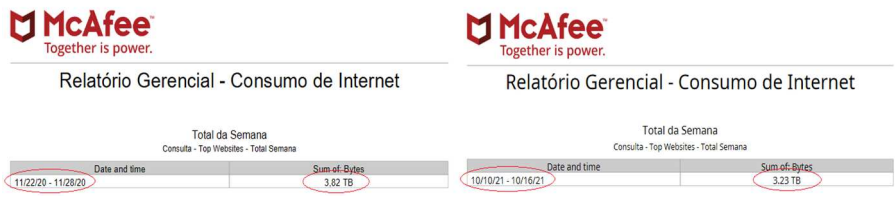

Figura 11- Consumo de Internet semanal em amostras de 2020 e 2021

McAfee
Together is power.

Relatório Gerencial - Consumo de Internet

Total da Semana
Consulta - Top Websites - Total Semana

Date and time	Sum of: Bytes
3/13/22 - 3/19/22	5.62 TB

McAfee
Together is power.

Relatório Gerencial - Consumo de Internet

Total da Semana
Consulta - Top Websites - Total Semana

Date and time	Sum of: Bytes
6/19/22 - 6/25/22	6.69 TB

Figura 12 - Consumo de Internet semanal em amostras de 2022 (maio e junho)

McAfee
Together is power.

Relatório Gerencial - Consumo de Internet

Total da Semana
Consulta - Top Websites - Total Semana

Date and time	Sum of: Bytes
7/24/22 - 7/30/22	7.13 TB

Figura 13- Consumo de Internet semanal em amostra de julho/2022

Observando as tabelas acima, notamos que durante os anos de 2020 e 2021, o consumo de Internet se manteve praticamente estável, com aproximadamente 3 TB de dados por semana. A partir de novembro de 2021, seguindo as resoluções da presidência do TRF3 e JFSP, o percentual de servidores trabalhando presencialmente em toda da JF3R passou a ser de, no mínimo, 20%. Até então, o tráfego de Internet registrado no proxy em 2020 e 2021 possivelmente estava relacionado às estações de trabalho acessadas remotamente via protocolo RDP, ou mesmo de estações que foram levadas para casa por alguns servidores. Dessa forma, o navegador usaria as configurações de rede padrão para direcionar o tráfego para o proxy Web.

Com o aumento gradual de servidores em trabalho presencial, além das mudanças promovidas para migrar serviços internos para nuvem, o comportamento mostrado nas demais figuras do ano de 2022 (março, junho e julho) era o esperado, ou seja, de aumento da demanda. Em 2022, vemos que o consumo mais do que dobrou, alcançando o patamar de 7 TB por semana.

Em nossas estimativas, planejando um aumento de demanda futura, com respaldo na Resolução no. 477/2018 do CJF, um par de links com largura de banda de 10 Gbps deveria atender a demanda atual, com margem para comportar um crescimento da demanda pelos próximos 5 anos. Mantendo a preocupação com a segurança, é imprescindível que esses links sejam contemplados com uma proteção anti-DDoS.

2.2. Desafios

O principal cenário para desenho desse projeto, apoiado pela equipe técnica, é o de adicionar links de Internet de 10 Gbps de forma redundante, sendo cada link

instalado em um em datacenter distinto (Torre Sul e Pedro Lessa), usando dupla abordagem de fibra. Cada link seria conectado ao respectivo roteador ASR1001-X de cada site.

Contudo, no estudo do projeto, encontramos desafios que alteraram o seu curso, dividindo-o em dois projetos. Explicaremos esse contexto ao longo do documento.

Os roteadores ASR1001-X, da marca Cisco, desempenham um papel fundamental na nossa rede, pois é através deles que a equipe técnica de conectividade do TRF3 (RCOD) mantém as seguintes funcionalidades em operação:

- eBGP e iBGP;
- DMVPN (para conectividade com MS);
- NATs para permitir integração com a INFOVIA (rede CNJ/STJ);
- Links de Internet de 1 Gbps com IX.BR e Wirelink (site Torre Sul) e link Algar (site Pedro Lessa);
- IP no roteador;
- *Port-channel* com LAN;
- Netflow;
- HSRP;
- IPV6 configurado;
- SNMP.

Cada funcionalidade tem um papel e grau de importância, mas podemos citar que as mais críticas são o protocolo BGP e DMVPN. A JF3R é um *Autonomous System* (*AS*) e, como tal, tem liberdade e autoridade sobre suas decisões de roteamento. Para tanto, possui um bloco de endereços IPv4 e IPv6 próprios. Todos os serviços fornecidos ao público externo dependem destes endereços, com exceção dos serviços que, atualmente, encontram-se protegidos pela Akamai. O tráfego interno de Internet também faz uso desses IPs através da funcionalidade de NAT. O controle do roteamento externo (Internet, eBGP) é feito via protocolo BGP configurado no ASR1001-X, além de integração com o roteamento interno (iBGP). A equipe técnica de conectividade tem a gerência do equipamento e, quando necessário, consegue intervir de forma rápida para manutenção do roteamento relacionado à Internet.

A DMVPN é uma evolução das antigas VPN *site-to-site* que interligavam cada localidade da JFMS ao TRF3. Trata-se de tecnologia proprietária da fabricante Cisco que estabelece uma malha de comunicação entre os nós (*spokes*) e o concentrador

(*HUB*). Uma das vantagens sobre o modelo antigo é que a comunicação entre dois nós pode ser realizada sem intervenção para o concentrador. Atualmente, os dois equipamentos ASR1001-X desempenham o papel de concentrador da DMVPN. A possibilidade de fechar sessões diretamente, sem intervenção do concentrador, privilegia a latência nas comunicações entre os pontos, uma vez que encurta o roteamento entre origem e destino (por exemplo, o tráfego entre Naviraí e Coxim flui pelo *backbone* da mesma operadora local).

Durante o estudo de viabilidade, identificamos com ajuda de um parceiro que tanto os ASR1001-X quanto as suas interfaces de 10 Gbps entrariam em EoS (*End of Sale*) em 01/08/2022. Como seria impraticável adquirir todas os itens do projeto até esta data, tendo em vista os trâmites internos da JF3R (estudo, elaboração e ajustes do TR, pregão, homologação, pagamento), o primeiro desafio foi buscar um substituto para os roteadores. O parceiro também nos informou que as interfaces e estes roteadores especificamente possuem licenciamento distintos e, apesar de haver anúncio de *EOS* para licenciamento da interface, não havia, na data da consulta, um anúncio de qual seria o *part number* do licenciamento substituto.

Outro desafio para conclusão do desenho do projeto é que o prazo de entrega da Cisco para vários equipamentos estava acima de 100 dias segundo o próprio parceiro e também as operadoras que consultamos. Isso afetaria diretamente a implantação e homologação do projeto no prazo que se almejava.

Diante destes desafios, uma das opções considerada com as operadoras foi, inclusive, utilizar roteadores de outras marcas para substituir os ASR. Enquanto aguardávamos respostas das operadoras sobre opções de equipamentos que eles poderiam nos fornecer, validamos com nosso parceiro Cisco que o equipamento da borda necessariamente deveria ser da marca Cisco, devido à funcionalidade de DMVPN. Além disso, se a operadora fornecesse o equipamento como parte do serviço, a equipe técnica de conectividade necessitaria ter acesso de escrita nos roteadores da operadora para migrar todas as funcionalidades dos ASR1001-X para os novos equipamentos. Esse ponto estava em discussão com as operadoras e diretoria, porém, sabemos que existe precedente para isso no edital do CJF para contratação da solução de SD-WAN, em que foi pedido direito de escrita à contratante tanto nos equipamentos da solução contratada da operadora (roteadores e *appliances* de SD-WAN).

Com o iminente aumento do contingente de servidores em trabalho presencial para aproximadamente 50% e considerando todos os desafios descritos acima, a diretoria determinou um novo rumo para o projeto, com intuito de possibilitar a entrega de novos links de Internet com largura de banda de 10 Gbps que atendessem a demanda projetada, conforme citado no item 2.1. Para separar melhor as propostas, vamos mostrar em figuras simplificadas as topologias propostas pela equipe técnica e pela administração.

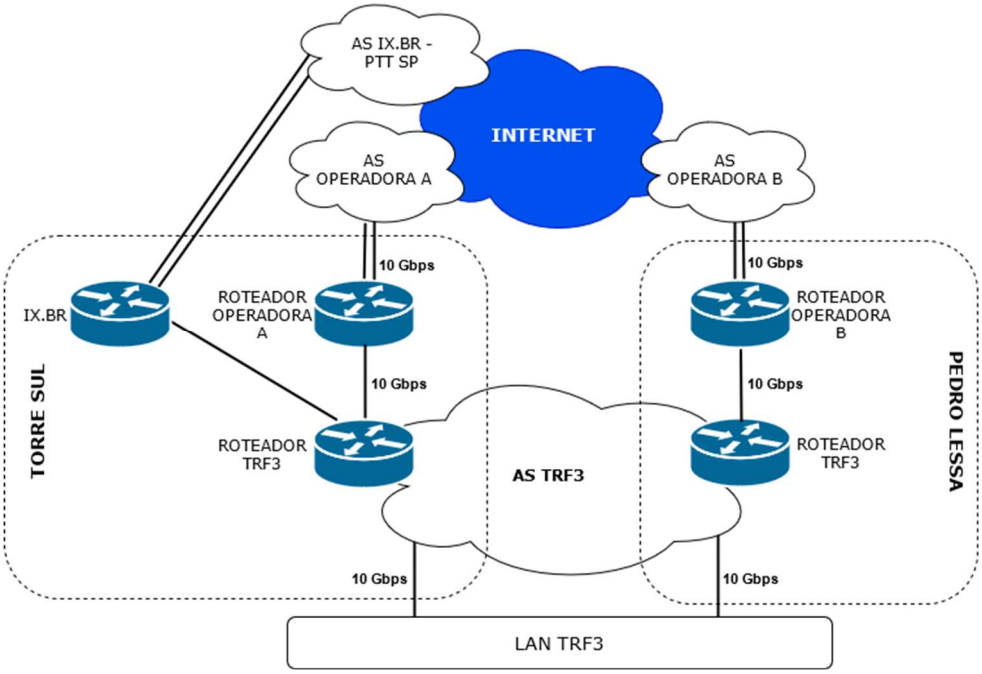

Figura 14- Topologia proposta pela equipe de conectividade do TRF3

A proposta ilustrada na Figura 14 recomenda a contratação de dois serviços de Internet dedicada de 10 Gbps, entregues com dupla abordagem nas instalações da JF3R. Cada roteador seria conectado a um roteador de borda com pelo menos 1 conexão de 10 Gbps. Esses roteadores de borda substituirão os ASR1001-X, que estão entrando no fim do seu ciclo de vida, e seriam de propriedade do TRF3, para mantermos ativo o papel do TRF3 de *AS* na Internet, com a devida autonomia na manutenção e configuração do BGP. Além disso, o link do IX.BR tem se mostrado muito útil com relação à disponibilidade, redundância, balanceamento de tráfego e latência mais eficiente para alcançar redes de grande porte. A largura de banda atual da ligação com o IX.BR é de 1 Gbps, contudo, esse valor poderia ser reavaliado na topologia proposta quanto a sua atualização ou manutenção em 1 Gbps.

A rede interna também necessitaria ser revisada para comportar todo o tráfego de 10 Gbps, com atenção especial ao ciclo de vida dos equipamentos no *core* da rede. A rede local (LAN) do TRF3 foi simplificada no desenho acima, portanto, não demonstra preocupações inerentes a esse projeto, como a redundância na rede interna e a disponibilidade de ligações adequadas de 10 Gbps. Na topologia atual, os ASR1001-X conectam-se de forma redundante a dois switches Nexus 9504. Estes, por sua vez, conectam demais equipamentos, como o Firewall Threat Defense (FTD), também de forma redundante. Ao longo do tempo, esses equipamentos também vão avançar nas etapas do seu ciclo de vida e esse fato precisará ser avaliado. Além disso, segundo o parceiro Cisco, o FTD suporta apenas interfaces de fibra ótica para uplink com os switches, ou seja, não há possibilidade de utilização de conexões UTP entre o FTD e os switches. Portanto, a disponibilidade de portas de fibra ótica nos switches também é uma preocupação do desenho acima.

Essa proposta e nossas considerações sobre como deveria caminhar o projeto de evolução da infraestrutura de conectividade do TRF3 foram discutidas com a diretoria em julho de 2022. Pelo caráter emergencial dessa contratação, tendo em vista o aumento de 20% para aproximadamente 50% do contingente de servidores em trabalho presencial, previsto para iniciar em setembro, a diretoria optou por dividir o projeto em duas propostas distintas. A proposta da Figura 14 será convertida num projeto de melhoria com foco na revisão da infraestrutura. Para esta contratação, a diretoria fez uma nova proposta, para a qual iniciamos um estudo de viabilidade de implementação, buscando um caminho mais rápido e prático. O novo desenho se assemelha à topologia da Figura 15 abaixo.

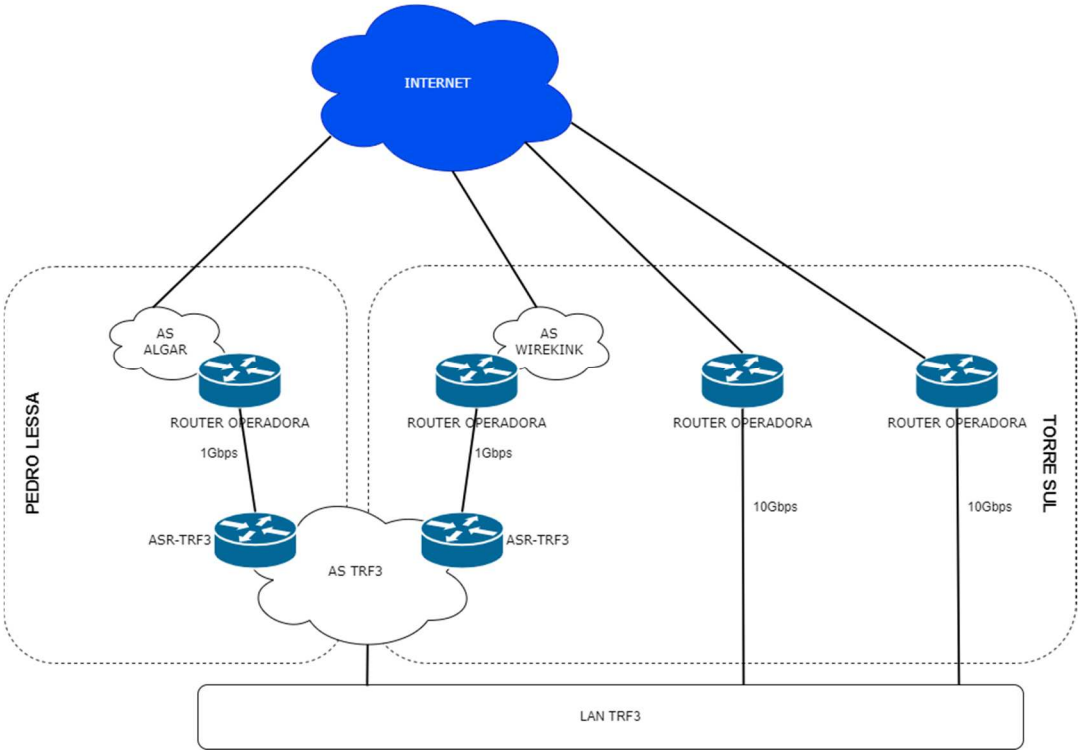

Figura 15- Topologia proposta pela diretoria

Com base na proposta da diretoria, iniciaremos o estudo de viabilidade para a implementação da topologia ilustrada na Figura 15.

3. Plano Inicial do Projeto

3.1. Objetivo

Demonstrar em cenário a proposta de contratação de 02 (duas) empresas especializadas distintas para prestação de serviços de comunicação através de acesso IP permanente, dedicado e exclusivo, em fibra óptica, para conexão do Data Center do Tribunal Regional Federal da 3ª Região – TRF3 e a rede mundial de computadores – INTERNET, incluso serviço de mitigação de ataques distribuídos de negação de serviços – DDoS, pelo período de 48 (quarenta e oito) meses.

3.2. Público Alvo

Usuários internos (magistrados, desembargadores, servidores públicos e colaboradores) e externos que utilizam das informações dos sistemas processuais e administrativos.

3.3. Análise e Planejamento de Capacidade

3.3.1. Ampliação da largura de banda dos links de Internet

Conforme explicado anteriormente ao longo do item 2 (“Situação Atual”), há uma demanda crescente por mais largura de banda. Uma análise pode ser estabelecida entre o consumo de Internet via proxy em outubro de 2021 e julho de 2022. Até outubro/2021, não havia limite mínimo de servidores em trabalho presencial estipulado na JF3R, portanto, a grande maioria dos servidores estavam trabalhando remotamente. O volume semanal de dados registrado foi de mais de 3 TB de dados, conforme exibido na Figura 11. A partir de novembro/2021, foi estabelecido o limite mínimo de 20%, momento em que o volume semanal de dados passou a registrar aumento de valores, conforme exibido na Figura 12. No último relatório disponível durante a elaboração deste estudo, em julho de 2022, o consumo semanal registrado foi acima de 7 TB. Isso representa um aumento aproximado de 233%.

Considerando que a capacidade total de largura de banda instalada atualmente é de 3 Gbps, para acompanhar essa tendência de aumento (233%), a largura de banda instalada deveria ser de, no mínimo, 7 Gbps. Contudo, em consulta com as operadoras, não é possível contratar um link de Internet com uma largura de banda de 7 Gbps, pois só são comercializados valores de 5 ou 10 Gbps, considerando a nossa necessidade. Por este motivo, necessitamos contratar um link com largura de banda de 10 Gbps. Visando a alta disponibilidade e redundância, serão contratados dois links com a mesma capacidade.

3.3.2. Detalhes da implementação

A topologia da Figura 15 exibe quatro links de Internet. Dois links (largura de banda de 10 Gbps) serão contratados de operadoras distintas entre si e outros dois links (largura de banda de 1 Gbps) estão ativos no TRF3 com contratos vigentes até 2023, pelo menos. Estes dois links já prestam o mesmo tipo de serviço (Internet dedicada). É essencial que a contratação deste projeto selecione operadoras distintas, que não tenham interligações entre si. Contudo, é possível que alguma das operadoras com contratos atualmente vigentes seja a vencedora de um dos lotes da licitação, entregando um dos links de 10 Gbps. Nesse caso, teríamos uma concentração de uma mesma operadora fornecendo acesso à Internet para a JF3R. Como exemplo, a Algar poderia ser vencedora de um lote de Internet 10 Gbps com anti-DDoS e teríamos uma mesma operadora fornecendo dois links de Internet ao TRF3. O pior cenário seria termos uma indisponibilidade num ponto de convergência de umas dessas operadoras que afetasse, simultaneamente, todos os links

contratados dela. Entretanto, entendemos que a probabilidade de esse pior cenário ocorrer é baixa. Além disso, esse risco será mitigado nessa mesma contratação, já que ambos os links serão de operadoras distintas. Adicionalmente, teremos redundância garantida através dos demais links de 1 Gbps enquanto seus contratos estiverem vigentes..

O link de IX.BR ainda tem contrato vigente até o ano de 2023, contudo, a diretoria decidiu não incluir o IX.BR na proposta, afirmando que ele não seria renovado e poderia ser desativado. Essa questão permanecerá em aberto e, se tal decisão não se confirmar, a conexão ao PTT (IX.BR) poderá ser alvo de estudo no projeto de melhoria.

Nessa estratégia, os links atuais serão mantidos conectados aos ASR1001-X, balanceados pelo BGP e servindo como a conexão de entrada do tráfego da JFMS, através da DMVPN configurada nesses roteadores. Os serviços publicados com os IPs do AS do TRF3 permanecerão trafegando pelos links de 1 Gbps.

Todo tráfego de Internet de usuários (com ou sem intermediação do web proxy) será priorizado pelos links de 10 Gbps. Dessa forma, faremos maior uso dos links de 10 Gbps para o tráfego de maior vazão, pois todas as unidades da JFSP compartilham os links existentes de 1Gbps para acesso à Internet. Nesse caso, redirecionando esse tráfego para os links de 10 Gbps, teremos uma alocação melhor de banda nos links de 1 Gbps para os serviços internos que são publicados na Internet (como PJE, por exemplo). No TRF3, o trafégo das estações (com ou sem intermediação do proxy) da TN e TS também poderá ser direcionado aos links de 10 Gbps, enquanto o tráfego das redes de servidores (VLAN 70 e DMZ) permanecerá nos links de 1 Gbps. Esta é a forma mais prática e simples de balancearmos o tráfego, sem muita interferência da rede.

A diretoria também solicitou instalarmos os novos links de 10 Gbps no modelo ativo-passivo, ou seja, o segundo link só será utilizado em casos de indisponibilidade do primeiro. Um único link de 10 Gbps deve atender a capacidade e, se em algum momento tivermos necessidade de mais largura de banda, poderemos avaliar alteração desta definição para usarmos os dois links de 10 Gbps no modelo ativo-ativo e promovermos um balanceamento melhor dos links.

Na análise técnica do roteamento, o caminho mais prático de entregar a solução proposta é alterar o gateway através de PBR (Policy-Based Routing). Todo tráfego

necessita passar pelo FTD antes de ser encaminhado à Internet, por uma questão essencial de segurança. A decisão baseada no destino é feita através de análise da tabela de roteamento nos dispositivos intermediários como FTD e Nexus Core. Quando a decisão é feita com base na origem do pacote, então precisamos recorrer à técnica de PBR que, no caso do FTD, é implementada através da funcionalidade conhecida como Flexconfig. Consultamos nosso parceiro Cisco a respeito da implementação da funcionalidade Flexconfig (PBR) no nosso desenho e analisamos a seguir as considerações dessa opção.

De acordo com o parceiro Cisco que atende o TRF3 na parte de conectividade (Teltec), o cenário do TRF3 é bem complexo e foram necessários diversos ajustes para manter a rede estável e redundante utilizando um cluster de FTD em modo ativo-ativo. Diversas configurações estão implementadas nos switches de ambos os sites (Torre Sul e Pedro Lessa) para impedir que o tráfego de Internet cruze os sites. Por exemplo, a VLAN de Internet (986) não faz parte do trunk que interliga os sites. Mas, numa eventual indisponibilidade do FTD de um dos sites, os switches estão configurados com uma automatização responsável por alterar as configurações do trunk que interliga os sites e adicionar a VLAN 986 como uma VLAN permitida no trunk. Dessa forma, o tráfego de Internet poderá cruzar os sites para ser tratado pelo FTD que estiver em operação.

O comportamento acima é necessário porque, estando em cluster, as configurações precisam ser espelhadas entre os appliances FTD. Isso inclui, por exemplo, interfaces físicas e lógicas do appliance, configurações de NAT, roteamento, etc. Se for configurada uma interface física no appliance FTD da Torre Sul, essa interface física também precisará existir no appliance FTD do Pedro Lessa. Se for criada uma interface lógica no FTD Torre Sul, automaticamente o FTD replicará essa interface para o outro appliance, através do cluster configurado entre eles. Além disso, os appliances compartilham endereços IP e MAC Address das interfaces, como a interface INSIDE (conectada à LAN e VLAN 70). Para que não ocorra um mecanismo de MAC Flapping na rede, portanto, os switches de um site não conseguem resolver o IP e MAC Address da interface INSIDE (gateway) que está no outro site.

No cenário atual, o nível de complexidade da rede aumentaria muito para configuramos o site Pedro Lessa para encaminhar o tráfego de Internet para os links de Internet de 10Gbps na Torre Sul, tendo em vista que esse tráfego teria que cruzar

os dois sites e todos os mecanismos configurados para manter estabilidade da rede necessitariam ser revistos e revalidados para não termos reincidência dos problemas de conectividade do passado.

Considerando tudo isso, a Teltec propôs uma solução mais prática para a implementação do cenário atual: mudar a operação do cluster para o modo ativo-passivo (active-standby). Nesse modelo, teríamos apenas um appliance FTD operando (ativo) e tratando os pacotes de dados; o outro appliance FTD só entraria em operação efetiva numa eventual indisponibilidade do appliance ativo.

Nesse modelo, o FTD teria duas interfaces lógicas OUTSIDE, sendo a primeira delas a interface já existente que pertence à subrede 200.9.86.248/29 (ligação com os links de 1 Gbps através dos ASR1001-X). A segunda interface, “OUTSIDE2”, é uma nova interface a ser criada e pertenceria à subrede que será configurada para o enlace com o roteador da operadora responsável pelo link de 10 Gbps primário (ativo). Para utilizar o segundo link de Internet, deveríamos ter uma outra interface, “OUTSIDE3”, com endereçamento pertencente ao enlace do segundo link de Internet de 10 Gbps (link passivo). O PBR no FTD seria responsável por encaminhar o tráfego pela devida interface OUTSIDE de acordo com a subrede de origem no pacote IP.

Esses detalhes de implementação precisariam ser melhor estudados durante a fase de execução do projeto. Contudo, já fornecem visões importantes da implementação do projeto. Um deles, inclusive, diz respeito à utilização dos dois links de 10 Gbps simultaneamente. Se em algum momento essa hipótese for aplicada na prática, poderemos ter um gargalo no FTD, segundo a Teltec. O motivo desse alerta é que estamos evoluindo a capacidade na borda da rede para além das capacidades para as quais o FTD foi projetado. No cenário do TRF3, que implementa inspeção de pacotes (IPS) e análise de aplicações, além das funcionalidades básicas de um firewall, o throughput máximo estimado do appliance é de 15.5 Gbps. Esse valor é menor que a soma de todos os links de Internet, ou seja, 23 Gbps (2 x 10 Gbps + 3 x 1 Gbps). Na prática, parece pouco provável que o FTD tenha uma demanda dessa escala. Por outro lado, esse alerta reforça o caráter essencial do projeto de revisão e melhoria da infraestrutura. A infraestrutura de rede deveria evoluir em harmonia tanto na sua porção interna (LAN) quanto na sua porção externa (WAN).

Também precisamos apresentar o tratamento necessário à tradução dos endereços IP. Atualmente, o tráfego de Internet sofre tradução de endereços (NAT)

para que os pacotes possam ser roteados na Internet. Levando em consideração que o tráfego de saída das estações e dispositivos móveis serão roteados pelos links de 10 Gbps, sem integração com o BGP, em linha com a determinação da diretoria, necessitaremos que os roteadores das operadoras implementem os NATs existentes hoje no FTD, utilizando endereços públicos IPv4 contratados de cada operadora.

Em agosto/2022 existem 10 IPs públicos do range 200.9.86.0/23 (AS TRF3) em uso na política de NAT do FTD, dentre os que foram restabelecidos após o ataque ransomware. Estes IPs estão sendo usados em seis NATs dinâmicos conforme mostrado na figura a seguir:

3		Dyna...	INSIDE	OUTSIDE	ilan.sede.grp.lan_prox	inet.nat.rang.lan_proxy_cabeada
4		Dyna...	INSIDE	OUTSIDE	ilan.sede.host.svlmwg	inet.nat.rang.svlmwgw01
5		Dyna...	INSIDE	OUTSIDE	ilan.sede.host.svlmwgc	inet.nat.host.svlmwgc05
23		Dyna...	INSIDE	OUTSIDE	ilan.sede.rang.rede_wi	inet.nat.host.rede_wifi_10_73
24		Dyna...	INSIDE	OUTSIDE	ilan.jf3r.grp.redes_usu	inet.nat.rang.rede_usuarios_sem_proxy
25		Dyna...	INSIDE	OUTSIDE	ilan.sede.grp.rede_ser	inet.nat.rang.rede_10_70_sem_proxy

Figura 16- NATs dinâmicos no FTD em Agosto/2022

O menor bloco razoável de endereços públicos IPv4 que atendem à demanda de NATs mencionada, com espaço para crescimento, seria um bloco de 32 endereços. Desconsiderando os endereços de rede (1), broadcast (1) e enlaces ponto-a-ponto redundantes (4) entre roteador e Nexus 9504, restariam 26 endereços públicos válidos.

Essa estimativa poderá ser ajustada a depender da implementação do enlace entre roteador e Nexus 9504. Para garantir um mínimo de redundância nessa topologia, necessitaremos utilizar conexões de fibra e UTP para os equipamentos. Alinhamos com a diretoria que existe uma insuficiência de portas de fibra ótica 10 Gbps (primeiro enlace físico) disponíveis nos switches Nexus 9540 primário (TS03) e secundário (TS04). Fizemos uma pesquisa nos equipamentos e listamos algumas interfaces candidatas a serem remanejadas e identificamos que as únicas alternativas viáveis nesse momento seriam:

1) utilizar a interface 3/50 do TS03, que está em desuso e, provavelmente, era uma das fibras que conectava esse switch ao switch Nexus de distribuição da Torre Norte;

2) utilizar a interface 1/49 do TS04, que é uma interface redundante de conexão a um dos switches de distribuição da Torre Sul (swcts05).

Existem outras portas candidatas, contudo, remanejá-las afetaria demais a redundância na rede interna em detrimento da comunicação com a Internet e não nos parece saudável. Para complementar essas duas conexões de fibra, portanto, também vamos utilizar conexões 10 Gbps UTP (segundo enlace físico), pois existem diversas portas deste tipo disponíveis nos Nexus 9504. Solicitaremos às operadoras que forneçam a infraestrutura física para essas conexões, incluindo cabeamento e GBICs para roteadores e Nexus 9504. Além disso, pensando no projeto futuro de melhoria, solicitaremos roteadores com duas interfaces de fibra ótica para conexão com a LAN, do tipo QSFP+ compatível com switch Nexus 9504. A interface WAN do roteador será livre escolha da operadora.

A interface UTP 10Gbps será utilizada como conexão redundante e necessitará ser configurada como um enlace lógico independente do enlace de fibra porque a tecnologia de agregação de links dos switches Cisco Nexus (conhecidas como Port-channel ou Etherchannel) não permite agregação de interfaces de diferentes meios físicos, ou seja, não é possível configurar uma agregação entre uma interface de fibra e uma interface UTP1.

Para melhor entendimento, ilustramos os detalhes descritos acima numa figura, detalhando a parte física da Figura 15, mas com foco nos elementos que serão adicionados ou alterados em nossa infraestrutura.

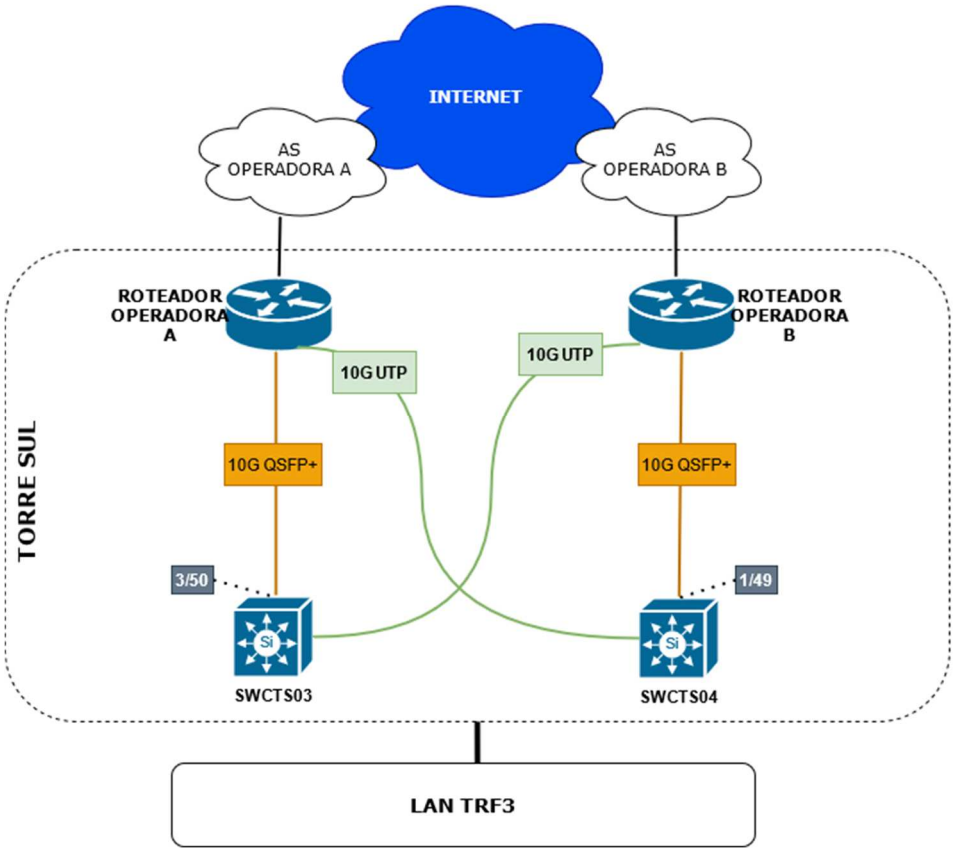

Figura 17- Detalhes conexões roteadores operaradoras com Nexus TS03 e TS04

4. Análise Custo X Benefício

4.1. Panorama geral

O projeção do aumento da capacidade discutida neste documento parece ser suficiente para comportar um maior volume de dados esperado com o aumento do número de servidores em trabalho presencial, que recorrerão aos links de Internet do TRF3 para acesso à Internet.

O custo associado ao projeto não deve ser tão elevado considerando que os links de Internet serão contratados com abordagem simples, os equipamentos serão fornecidos em regime comodato, os serviços contratados são ofertados por diversas grandes provedoras de Internet e promoveremos o reuso de infraestrutura tanto quanto possível, sem aquisição de novos equipamentos ou licenciamento.

Embora este projeto reúna esforços para atender a demanda da diretoria e da instituição da forma mais simples, prática e rápida que o negócio exige, existem pontos de atenção importantes que a equipe técnica deixará registrado neste relatório, a saber:

1) concentração dos links de 10Gbps apenas na Torre Sul;
2) subutilização do BGP e perda de autonomia no roteamento de Internet;
3) quebra de redundância interna na Torre Sul;
4) dispensa da conexão ao PTT (IX.BR);
5) encerramento de contrato de manutenção dos ASR1001-X;
6) importância do projeto de melhoria e revisão da infraestrutura.

4.2. Concentração dos links de 10Gbps apenas na Torre Sul

A Resolução no. 477/2018 do CJF, Art. 2º recomenda a seguinte estrutura mínima para o CJF e tribunais regionais federais:

I - Um ambiente principal de processamento central (Data Center) e, para o CJF e os tribunais regionais federais, mais um ambiente secundário para contingência que atendam ambos, no mínimo, aos seguintes requisitos:
*a) **locais seguros em prédios distintos**, com o ambiente secundário para contingência devendo ser, preferencialmente, implantado com a utilização de espaço físico de outro órgão da Justiça Federal ou mediante acordo com órgãos da Administração Pública Federal;*
b) sistema ativo de combate a incêndio;
c) limitação eletrônica de acesso físico;
d) circuito fechado de TV - CFTV;
e) fonte de alimentação com condicionamento de energia elétrica, por nobreaks redundantes e grupo gerador;
f) climatização redundante de precisão, automatizada e com sistema de alerta e temperatura e controle de, no mínimo, vazão de ar, condensação e umidade;
g) espaço físico suficiente para suportar os equipamentos e previsão de expansão para um horizonte de cinco anos;
h) as seções e subseções judiciárias deverão possuir infraestrutura adequada (espaço físico, rede elétrica, climatização, cabeamento estruturado, etc.) de ambiente de processamento central (Data Center) para o bom funcionamento dos serviços de tecnologia da informação.
(...)

A equipe técnica entende que a definição da diretoria de concentrar os dois links de 10 Gbps na Torre Sul vai em sentido contrário ao que dispõe essa Resolução. Também entendemos a motivação da diretoria de entregar um desenho de serviço que permita a implementação da forma mais simples e rápida possível considerando o prazo legal da Resolução PRES Nº 530/2022 do TRF3. Contudo, orientamos a revisão desse desenho o quanto antes após a implementação deste projeto, distribuindo os dois links de 10Gbps entre os sites (prédios) da Torre Sul e Pedro Lessa.

4.3. Subutilização do BGP e perda de autonomia no roteamento de Internet

O inciso II, Art. 2º da Resolução no. 477/2018 do CJF também recomenda a implementação de:

II - Ambiente que forneça, ***no mínimo, controle automático e transparente contra falhas e alta disponibilidade da solução****, com a existência de:*

Esta contratação prevê a entrega de roteadores em comodato com gerência exclusiva da operadora. A contratante (TRF3) terá privilégios de leitura nesses equipamentos. Neste formato, toda e qualquer alteração nos equipamentos, como alteração de roteamento com a LAN, alteração de NATs de Internet deverão ser solicitados à operadora via chamado, respeitando o SLA contratado. A equipe técnica não terá condições de efetuar qualquer configuração, independentemente do nível de urgência e criticidade.

Além disso, da forma como estamos contratando será mais difícil implementar a programação de controles automatizados conforme recomendação do CJF, pois todo e qualquer controle deverá ser solicitado às operadoras de cada link para implementação nos roteadores. A única forma de manipulação possível da parte do TRF3 será através de intervenção nos Nexus 9504, que são de nossa gerência.

Neste quesito, a equipe técnica também orienta a revisão do desenho possibilitando a compra de equipamentos em conjunto com garantia e suporte, com privilégios de escrita para a contratante. Essa orientação está alinhada com o desenho da figura 14. Nesse modelo, teríamos maior flexibilidade para implementar as políticas de roteamento na Internet através do protocolo BGP, que hoje encontra-se em operação nos ASR1001-X conectado aos links de 1Gbps.

Utilizando BGP, além de outros controles como IP SLA, Tracking e HSRP (protocolo de redundância de gateways) teríamos melhores condições de automatizar a redundância e alta disponibilidade conforme recomendação do CJF.

Além disso, é por meio do BGP que TRF3 exerce sua autonomia na Internet em relação às suas políticas de roteamento. Essa autonomia se refere à utilização de IPs públicos próprios para comunicação com a Internet, como, por exemplo, em enlaces de comunicação com roteadores, na publicação de serviços na Internet ou na tradução de endereços internos (NAT) para navegação dos usuários.

Algumas vezes surgiram casos de restrições ou bloqueios de nossos endereços públicos IPv4 (range 200.9.86.0/23) em redes externas, como na Caixa Econômica

Federal, AGU, OAB, STJ, entre outros. Nesses casos, o TRF3 precisa se identificar para o administrador da rede de destino e solicitar liberação do nosso bloco de endereços. Atualmente, solicitamos liberação do bloco do AS do TRF3. Contudo, utilizando roteadores e endereços públicos IPv4 das operadoras, necessitaremos fazer essa solicitação com mais frequência, pois esses IPs são reutilizados entre os clientes, podem ter relação com alguma blacklist da Internet e, principalmente, podem mudar se o TRF3 substituir a contratante, pois os IPs são da operadora.

Mesmo para serviços publicados na Akamai será necessário apontar, pelo menos, um IP público da rede do TRF3 para redirecionar o serviço à nossa rede. A cada troca de operadora, os IPs utilizados nessa configuração precisarão ser substituídos, pois perdemos direito de uso com o encerramento dos contratos.

Exercer o papel de sistema autônomo também permite que o TRF3 priorize de forma autônoma o encaminhamento de tráfego pelos links que reconhecer como melhores, utilizando balanceamento do próprio BGP ou recorrendo a configurações dos roteadores, como ACL (access control list) e prefix-list. Importante ressaltar que essas configurações são feitas pela própria contratante, em roteador próprio com privilégios de escrita.

Como o desenho atual mantém a infraestrutura do BGP restrita aos links de 1 Gbps, teremos uma subutilização do BGP e do papel de AS do TRF3. A orientação da equipe técnica é a revisão desse desenho para balancear e gerenciar os links de 10 Gbps utilizando o BGP, de forma semelhante ao que já é feito hoje com os links de 1 Gbps.

4.4. Quebra de redundância interna na Torre Sul

Para permitir a implementação do desenho da Figura 17, foi necessário encontrar portas de fibra ótica disponíveis nos Nexus 9504 da Torre Sul, conforme descrito no tópico 3.3.2 (Detalhes da implementação). Essa medida foi o caminho mais prático para atender à necessidade de interligação via fibra ótica, com o custo de fragilizar a redundância interna de interligação dos andares na Torre Sul, já que um dos switches perderá uma das conexões com o switch core swcts04.

Essa decisão precisa e poderá ser revista na revisão da infraestrutura, refazendo a redundância interna que foi afetada entre swcts05 e swcts04. Uma das medidas recomendas pela equipe técnica para melhorar esse cenário é contratar um módulo

adicional de fibras óticas com interfaces suficientes para interligação com outros equipamentos.

Em relação à redundância interna dos andares, porém, cabe ressaltar que a Torre Sul conta com dois switches Nexus de distribuição (swcts05 e swcts06) para interligação com os switches Nexus core (swcts03 e swcts04).

4.5. Dispensa da conexão ao PTT (IX.BR)

Durante as tratativas deste projeto, a diretoria se manifestou a favor de não renovar o contrato com o PTT (IX.BR) que deve se encerrar em 2023. Conforme demonstrado nas figuras 6 e 8, a conexão com o IX.BR se mostrou eficiente e útil durante seu tempo de operação. Além disso, existe uma possibilidade de melhor latência na comunicação com destinos acessíveis via PTT.

A equipe técnica recomenda um estudo do papel desse link após a implementação antes de uma decisão definitiva sobre a dispensa de comunicação com o IX.BR.

4.6. Encerramento de contrato de manutenção (ASR1001-X e Nexus linha 9000)

De acordo com o documento SEI “Informação Nº 8853149/2022 – DIAC”, o contrato dos ASR1001-X termina em 04/12/2022, sem possibilidade de renovação. Como o Termo de Recebimento Definitivo (TRD) foi assinado em 28/05/2022 e o Edital especifica um prazo de 60 meses para suporte e garantia a partir da assinatura do TRD, a empresa parceira (Teltec Solutions) deverá nos prestar serviço até 28/05/2023.

Considerando que manteremos os roteadores ASR1001-X em funcionamento conjunto com os roteadores de 1 Gbps, recomendamos atenção especial para substituição desses equipamentos em nossa infraestrutura antes de perdermos a suporte e garantia total para os itens desse contrato. Portanto, recomendamos inclusão desse projeto no orçamento para 2023, tendo em vista que essa contratação deverá ocorrer no decorrer de 2023.

4.7. Importância do projeto de melhoria e revisão da infraestrutura

Conforme informado no recorrer deste documento, o projeto inicial foi particionado em duas frentes, sendo este relatório responsável por apontar o caminho para implementação de uma solução emergencial a tempo do aumento da demanda previsto para iniciar em setembro/2022.

A segunda frente refere-se a um projeto extenso de revisão e melhoria da infraestrutura. Basicamente, esse projeto deverá investigar a melhoria do parque como um todo, para resolver as questões apontadas nos itens 4.2 a 4.7 deste documento. Um esboço do objetivo deste projeto pode ser visto na figura abaixo:

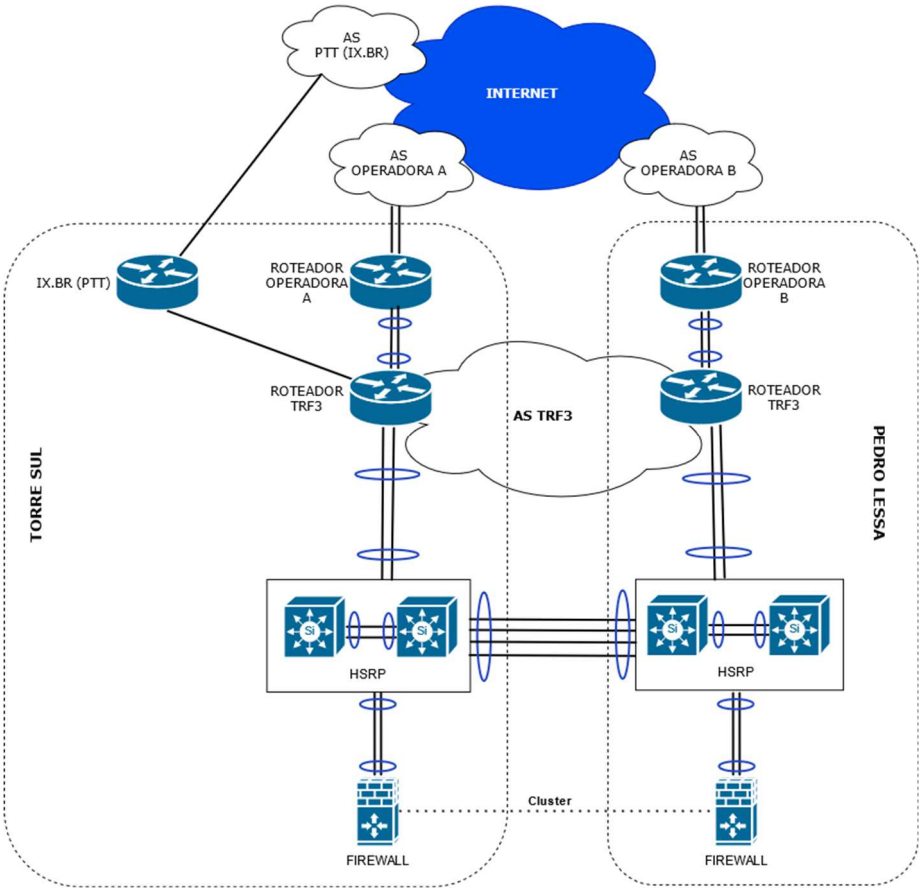

Figura 18 - Esboço do projeto de revistão e melhoria da infraestrutura

Este formato de desenho simplifica sugere decisões de topologia alinhadas com a Resolução no. 477/2018 do CJF, com equipamentos e conexões redundantes e agregadas nas redes LAN e WAN.

Existem pontos de melhorias da nossa infraestrutura que não estão representados na figura, mas merecem registro neste documento e deveriam fazer parte do projeto futuro:

1) adequação dos links de sites remotos à topologia redundante distribuída entre os prédios da Torre Sul e Pedro Lessa. Atualmente, a malha MPLS tem dois concentradores redundantes instalados apenas na Torre Sul, mas o ideal seria ter um concentrador em cada site, de forma distribuída. De forma semelhante, precisa ser estudada a possibilidade de adequação da topologia

SD-WAN para este mesmo modelo. A malha SD-WAN em SP tem previsão de início de operação em 2022;

2) estudo de um melhor balanceamento dos endereços públicos do AS do TRF3 no BGP, divulgando o bloco 200.9.86.0/23 para ambas as operadoras da figura 18, além divulgar o bloco 200.9.86.0/24 pela operadora A e divulgar o bloco 200.9.87.0/24 pela operadora B. Dessa forma, associado aos controles que mencionamos no item 4.3 (ACL, prefix-list) poderíamos ter maior flexibilidade de manipulação de download e upload na Internet através do BGP. Esse estudo também necessita considerar quais os serviços que mais demandam tráfego, para que haja uma escolha consciente de alocação destes serviços entre os dois blocos /24 citados anteriormente;
3) instituição de um plano e cronograma de testes de contingência, semelhante ao que é feito em outras instituições (como bancos privados). Esse plano é abrangente, envolveria toda a TI e serviria para testarmos nossa capacidade de resposta a um evento inesperado e o quão eficiente nossa rede está sendo para operar de forma redundante.

5. Parecer Final

Por fim, resumimos as considerações principais discutidas ao longo do documento:

- as necessidades do negócio, em especial o iminente aumento do percentual da força de trabalho em regime presencial para mais de 20%;

- as opções técnicas possíveis para implementar as decisões de desenho da diretoria;

- o prazo curto para publicação de edital licitatório, homologação e implantação de um projeto que atenda essas demandas;

- os pontos de atenção registrados ao longo do documento;

- a necessidade de revisão e melhoria da infraestrutura de rede como um todo.

Com base nessas considerações, a equipe técnica propõe a elaboração de edital para contratação de 02 (duas) empresas especializadas distintas para prestação de serviços de comunicação através de acesso IP permanente, dedicado e exclusivo, em fibra óptica, para conexão do Data Center do Tribunal Regional Federal da 3ª Região – TRF3 e a rede mundial de computadores – INTERNET, incluso serviço de mitigação

de ataques distribuídos de negação de serviços – DDoS, pelo período de 48 (quarenta e oito) meses.

Ainda, entendemos que a melhor forma de atender às determinações da diretoria pode ser resumida da seguinte forma:

- contratação de dois links de Internet dedicados de 10 Gbps, com fornecimento de 32 endereços públicos IPv4;

- contratação de proteção adicional anti-DDoS para cada um dos links, com capacidade de mitigação adequada que garanta, pelo menos, 70% de tráfego “limpo” (largura de banda mínima garantida de 7 Gbps do link de Internet), com SOC operando em 24x7;

- conexão física do roteador da operadora aos Nexus primário e secundário da Torre Sul, conforme esboço da Figura 17;

- alteração do modelo de operação do FTD de “ativo-ativo” para “ativo-passivo”. O FTD da TS será o firewall primário e o FTD do PL será o firewall secundário;

- roteamento do tráfego Internet de saída (originado na LAN) das estações de trabalho e dispositivos móveis para o(s) link(s) novo(s), exceto redes de servidores (VLAN 70), rede DMZ. Isso inclui tráfego com e sem proxy originado na LAN com destino à Internet;

- preservação dos links de 1 Gbps gerenciados pelo BGP através dos ASR1001-X. Esses links serão responsáveis pelo tráfego Internet de entrada (originado na WAN, Internet) no caso de serviços publicados/expostos na Internet e pelo tráfego Internet de saída para os hosts da rede de servidores (VLAN 70) e rede DMZ;

- os links das operadoras funcionarão no modelo ativo-passivo, sem integração com o BGP. A contratante (TRF3) terá privilégios de leitura nesses equipamentos;

- ambos os links serão instalados fisicamente na Torre Sul e terão abordagem simples;

- após a entrega dessa solução, a equipe de conectividade poderá, com apoio da diretoria, iniciar as atividades de levantamento de requisitos e estudos necessários ao projeto de revisão e melhoria da infraestrutura, visando alcançar um modelo similar ao da Figura 18, em linha com a resolução no. 477/2018 do CJF**.**

6. Referências

1- https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/92x/interfaces/configuration/guide/b-cisco-nexus-9000-nx-os-interfaces-configuration-guide-92x/b-cisco-nexus-9000-nx-os-interfaces-configuration-guide-92x_chapter_0111.pdf

Simone Sanches Alves:3311 Assinado de forma digital por Simone Sanches Alves:3311 Dados: 2022.09.15 13:26:44 -03'00'

WALDIR COSTA SOLA:3342 Assinado de forma digital por WALDIR COSTA SOLA:3342 Dados: 2022.09.15 15:26:53 -03'00'

VINICIUS SOUZA BARBOSA:3341 Assinado de forma digital por VINICIUS SOUZA BARBOSA:3341 Dados: 2022.09.16 12:03:01 -03'00'

DANIEL HENRIQUE GUIMARAES:3624 Assinado de forma digital por DANIEL HENRIQUE GUIMARAES:3624 Dados: 2022.09.16 17:45:43 -03'00'