

GTER 51 SÃO PAULO 2022

RECUPERAÇÃO DE DESASTRES EM CGNAT EM REDES SDN



GTER 51 | GTS 37

24 E 25 DE OUTUBRO DE 2022

AMCHAM BRASIL - SÃO PAULO/SP

RECUPERAÇÃO DE DESASTRES EM CGNAT EM REDES SDN



GTER 51 | GTS 37

24 E 25 DE OUTUBRO DE 2022

AMCHAM BRASIL - SÃO PAULO/SP

CONTATO – LUCIANO FRANZ



DESASTRES MAIS COMUNS:

- Incêndio
- Inundação
- Causas externas, ataques, problemas elétricos
- Falhas de componentes ou fabricantes
- Falhas humanas

INCÊNDIO NÃO ACONTECE COMIGO

Incêndio atinge Bitcom em Caxias do Sul

19/05/2019 17:26

Procedimento iniciado de 40 mil metros de altura. Bombeiros estão trabalhando para conter o fogo



Imagem: Arquivo da Prefeitura de Caxias do Sul

Tempestade de fogo

Incêndio atingiu as instalações da Bitcom, uma prestadora de serviços de internet, telefonia e TV

BRDigital atingida por incêndio

19/05/2019 17:26

Incêndio atingiu a BRDigital, uma prestadora de serviços de internet



Imagem: Arquivo da Prefeitura de Caxias do Sul



INCÊNDIO

<https://www.cnnbrasil.com.br/tecnologia/>

Incêndio destrói servidores da maior empresa de computação ...

10 de mar. de 2021 — O maior **provedor** de serviços de computação em nuvem da Europa disse a clientes, como o governo francês e a bolsa de criptomoedas Deribit, ...

<https://www.convergenciadigital.com.br/incendio-no-...>

Incêndio no maior data center da Europa alerta para ...

10 de mar. de 2021 — Quatro **data centers** foram destruídos pelo **fogo** e um foi desligado e está sob rescaldo dos bombeiros. Diante do estrago, o maior **provedor** de ...

<https://www.baguete.com.br/noticias/maior-data-cen...>

Maior data center da França pega fogo | Notícias - Baguete

12 de mar. de 2021 — Um **incêndio** destruiu um **data center** de cinco andares e 500 metros quadrados da OVH, um dos maiores **provedores** de computação em nuvem da ...

<https://www.baguete.com.br/noticias/data-center-atr...>

Data center atrapalha Grenal | Notícias - Baguete

7 de mar. de 2018 — Um **incêndio** em um **data center** de Porto Alegre atrapalhou a venda de ... é um dos maiores **provedores** de serviços da área de **data center** e ...

<https://www.cisoadvisor.com.br/incendio-destrui-data-...>

Incêndio destrói data center da OVH, maior hosting da Europa

10 de mar. de 2021 — Manteremos você atualizado conforme mais informações estiverem disponíveis". A OVH é o terceiro maior **provedor** de serviços de **data center** do ...

<https://avalanchenoticias.com.br/ipo-com-faisca-incen...>

IPO com faísca: incêndio no data center OVHcloud ...

Esta semana, no dia 10 de março, no **provedor** de nuvem OVHcloud em Estrasburgo (França), vários **data centers** localizados na mesma área pegaram **fogo**.

NFWare

Computech
Loja

VOZ E DADOS
academy



GTER 51 | GTS 37

INUNDAÇÃO



INUNDAÇÃO

O excesso de chuvas ou o transborde de rios e córregos na região pode afetar gravemente sua operação.

Falhas na estrutura e no projeto do local como telhas, lajes, escadas são a principal causa dos problemas de inundação.

A inundação pode causar problemas elétricos, falta de energia e até incêndio.

CAUSAS EXTERNAS, ATAQUES, PROBLEMAS ELÉTRICOS

<https://www.cisoadvisor.com.br/problema-eletrico-derruba-data-center-da-aws/>

Problema elétrico derruba data center e clientes da AWS

22 de dez. de 2021 — O **data center** US-East-1 (Virginia) da AWS sofreu novamente um problema que afetou grandes serviços nos EUA e no mundo a partir das 5h35 de ...

[https://g1.globo.com/noticia/2022/08/15/datacenter-](https://g1.globo.com/noticia/2022/08/15/datacenter-da-prefeitura-do-rio-sofre-ataque-hacker-g1/)

Datacenter da Prefeitura do Rio sofre ataque hacker - G1

15 de ago. de 2022 — Um **ataque hacker** ao **Datacenter** da Prefeitura do Rio tirou vários serviços municipais do ar. A ação foi percebida por volta das 2h da ...

Não encontrados: ~~derruba~~ | Precisa incluir: **derruba**

CAUSAS EXTERNAS, ATAQUES, PROBLEMAS ELÉTRICOS

Ransomware Attack – 365 Data Centers

According to the class action complaint, on **May 14, 2022**, 365 Data Centers “suffered a ransomware attack that caused the shutdown of their entire cloud network and loss of its clients’ data and critical infrastructure”. Customers of 365 “could not access their websites, customer portals, and other critical information technology infrastructure supported by 365’s network systems”.

Furthermore, the ransomware attack permanently prevented access to 365 Data Centers’ cloud infrastructure, with the company contending that the entire infrastructure must be rebuilt.

FALHAS DE COMPONENTES OU FABRICANTES

<https://www.baguete.com.br> > noticias > falha-em-switc... ▼

Falha em switch derrubou Visa | Notícias - Baguete

20 de jun. de 2018 — Ao todo, 1,7 milhão de clientes foram afetados. Sempre que o **data center** não cair. Foto: Pixabay. Tamanho da fonte: -A+A. Uma **falha** "muito ...

<https://teletime.com.br> > pane-do-whatsapp-foi-causado... ▼

Pane do WhatsApp foi causada por configuração de roteador ...

5 de out. de 2021 — "O **problema** no tráfego de rede gerou um efeito cascata na forma como nossos **data centers** se comunicam, levando à interrupção dos serviços", ...

Não encontrados: ~~derruba~~ | Precisa incluir: ~~derruba~~

<https://teletime.com.br> > pane-do-whatsapp-foi-causado... ▼

Pane do WhatsApp foi causada por configuração de roteador ...

5 de out. de 2021 — “O **problema** no tráfego de rede gerou um efeito cascata na forma como nossos **data** centers se comunicam, levando à interrupção dos serviços”, ...

Não encontrados: ~~derruba~~ | Precisa incluir: **derruba**

<https://mundoconectado.com.br> > noticias > facebook-r... ▼

Facebook revela erro de configuração como razão para ...

5 de out. de 2021 — Como muito dos funcionários estão trabalhando em home office, uma equipe precisou ser deslocada às pressas para o **data center** da companhia, em ...

Não encontrados: ~~derruba~~ | Precisa incluir: **derruba**



O que dizem os clientes, após uma falha...



Lucas Timm → CHM - 5 anos atrás

Inacreditável é um datacenter sem plano de emergência contra incêndio

6 ^ | v - Responder - Compartilhar



Milton Bonservizzi → Lucas Timm - 5 anos atrás

O que é inacreditável é um Data Center sofrer um incêndio dessa proporção!

1 ^ | v - Responder - Compartilhar



Bruno Macena → Lucas Timm - 5 anos atrás

Toda empresa tem plano de emergência contra incendio, isso não significa que não vá pegar fogo. O que deve ter é plano de contingência, seja pra desvio das comunicações, seja armazenamentos de fitas de bkp fora deste local, etc.

^ | v - Responder - Compartilhar



Gilberto Ferreira → Lucas Timm - 5 anos atrás

Tbem achei issol Como que uma empresa vende serviço de segurança de dados e não tem isso??? Lamentável!

^ | v - Responder - Compartilhar



Anderson → Gilberto Ferreira - 5 anos atrás

Ganancia. Aquela história de "nao vai dar nada, nunca vai acontecer aqui."

1 ^ | v - Responder - Compartilhar



Nicolas Wildner → Anderson - 5 anos atrás

E quem levou a culpa ainda foi o coitado do datacenter...



ENTÃO QUAIS SOLUÇÕES POSSO IMPLEMENTAR PARA ESTAR PREPARADO PARA O PIOR



SOLUÇÕES MAIS COMUNS PARA DISASTER RECOVERY

- Migração para SDN
- Obtenção fácil de componentes no mercado
- Redundância simples, barata e total



SOBRE REDES SDN

São equipamentos de rede que recebem orientação por software, ao invés de usar uma caixa de um determinado fabricante, o administrador opta por uma solução que normalmente é virtualizada em um hardware de fácil obtenção.



MIGRAÇÃO E VANTAGENS DO SDN

Uma coisa que deve ocupar diariamente o administrador de redes é a rede SDN:

1. Ela é de fácil recuperação
2. É mais barata
3. Não depende de componentes de nenhum fabricante



OBTENÇÃO DE COMPONENTES

Uma coisa que deve ocupar diariamente o pensamento do administrador de redes é:

1. Em quanto tempo eu consigo remontar a minha operação?
2. Quanto custa os componentes que podem estragar na minha operação
3. Em quanto tempo tenho ele de volta em caso de falha?

RECUPERAÇÃO DE DESASTRES EM CGNAT EM REDES SDN



MIGRAÇÃO PARA CGNAT SDN

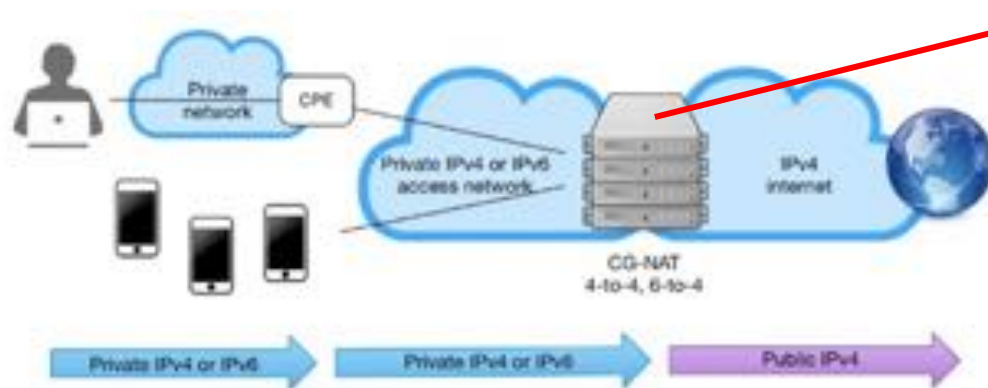
HARDWARE X SOFTWARE

CGNAT hoje permite ser migrado para SDN

Com isso superam-se problemas de redundância e obtenção de componentes

Troca-se a caixa de um determinado fabricante por um servidor de rede

SERVIDOR DE REDE COMUM
BAIXO CUSTO



REDUNDÂNCIA REAL NÍVEIS DE DISPONIBILIDADE E FORMAS DE FAZÊ-LO

REDUNDÂNCIA COM PROTOCOLOS

DIAGRAMA TÍPICO

BGP N+1

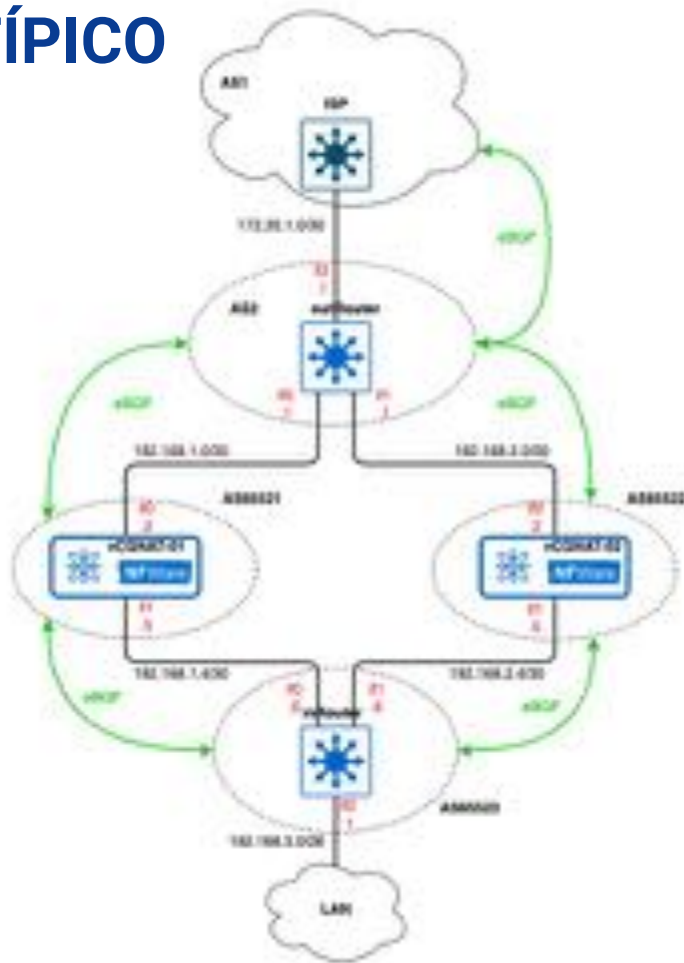
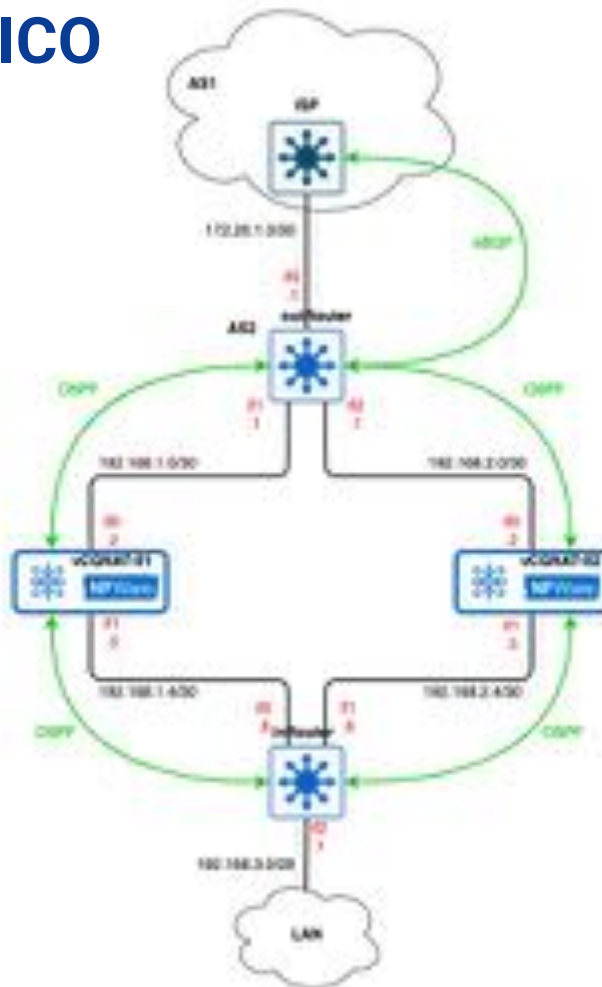


DIAGRAMA TÍPICO

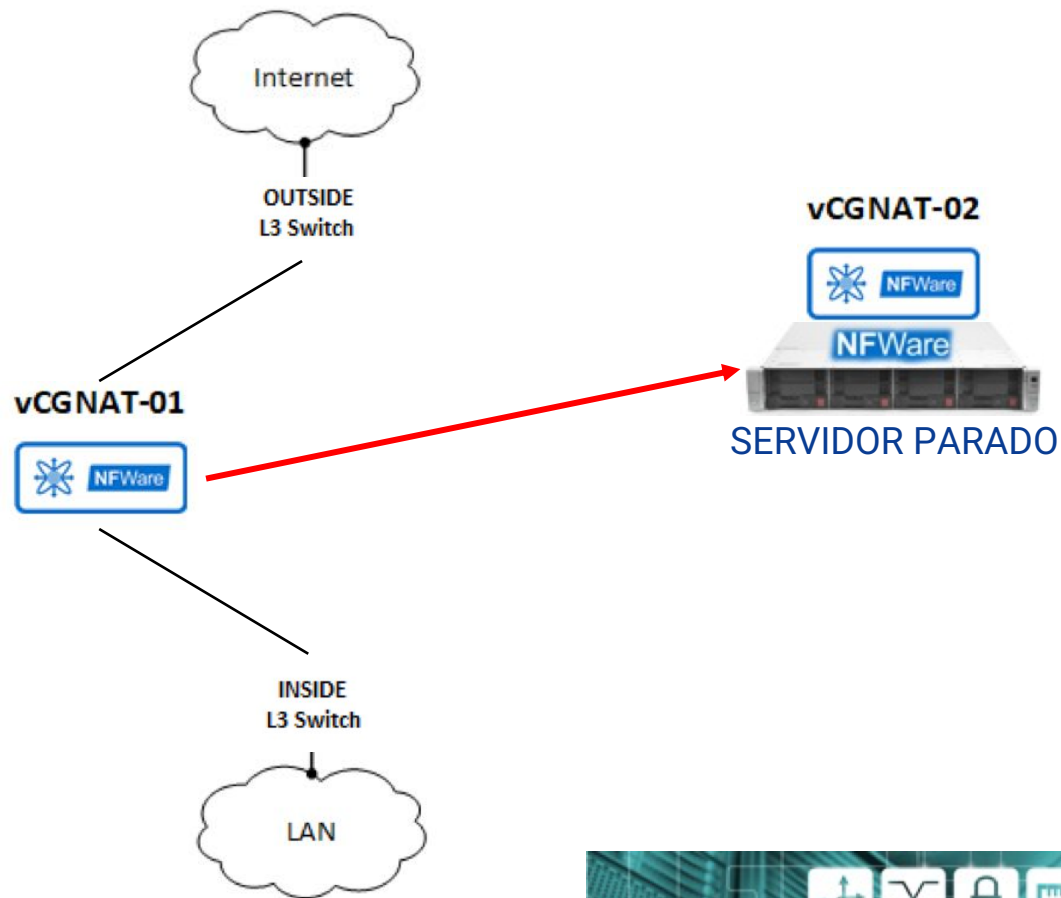
OSPF N+1



REDUNDÂNCIA INICIAL MÁQUINA ZUMBI

ACTIVE / SPARE

1+0 CGNAT



CENÁRIO

Em um cenário Active/Spare, apenas um vCGNAT estará em funcionamento.

Outro servidor ficará em SPARE e um clone do disco será feito.

Esse vCGNAT vai necessitar intervenção humana para entrar em operação.

A licença é compartilhada entre os 2 e não soma tráfego.

PRÓS E CONTRAS

PRÓS:

- Uma boa redundância por um preço extremamente barato
- Facilidade de implantação
- Pouca administração



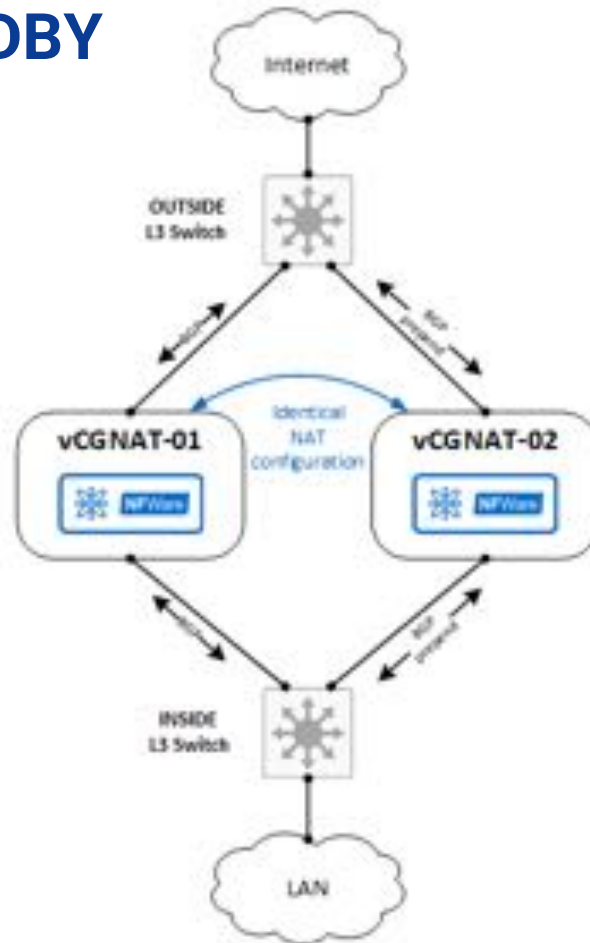
Contras:

- Demora na substituição do Hardware (em torno de 30 Minutos)
- Máquina zumbi parada
- Necessidade de Intervenção humana no hardware

REDUNDÂNCIA REAL ALTA DISPONIBILIDADE (HA) PROTOCOLOS



ACTIVE / STANDBY



CENÁRIO

Em um cenário Active/Standby scenario, cada vCGNAT tem a mesma configuração de NAT.

Mesmo pool público, mesmas regras e mesmos grupos de assinantes.

Cada vCGNAT está sempre ativo e pronto para operar.

Os Switches L3 ou Routers é que irão decidir qual dos servidores de CGNAT será usado para processar o tráfego. Protocolos de Roteamento (BGP) são usados para essa seleção do caminho.

A opção AS-path prepend é usada quando um update faz passar o tráfego para o segundo servidor vCGNAT. O Roteador que receber a prioridade mais alta receberá todo o tráfego.

Em caso de falha do primeiro vCGNAT, a tabela de roteamento nos roteadores vizinhos será refeita, e o caminho irá apontar para o Segundo vCGNAT, e ele será usado. O protocolo (BFD) Bidirectional Forwarding Detection (BFD) reduz o tempo de falha em conjunto com o BGP.

PRÓS E CONTRAS

PRÓS:

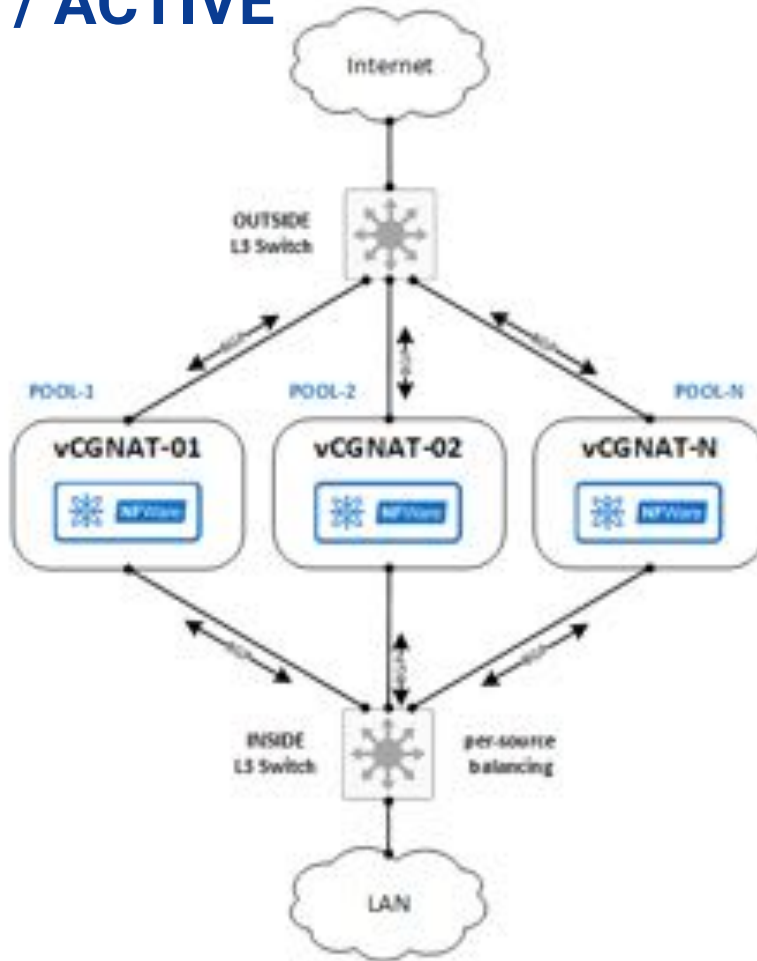
- Facilidade de implantação
- Resposta rápida à incidentes
- Pouca administração

Contras:

- Alto custo por giga trafegado
- Ter sempre zero de tráfego em um dos servidores
- Queda das sessões por alguns minutos em caso de incidente

ACTIVE / ACTIVE

N+1



CENÁRIO

Em um cenário Active/Active (N+1), cada nó vCGNAT tem uma configuração diferente. Todos ficam sempre ativos. As regras de NAT são criadas e então cada servidor vCGNAT pode lidar com o tráfego de qualquer assinante de dentro da rede, entretanto diferentes pools públicos são usados, então o tráfego é balanceado.

Para balancear o tráfego dentro da rede (LAN), o balanceamento por origem no downlink do equipamento L3 é usado. Os outros equipamentos rodam BGP para o update dos anúncios das rotas.

Cada anúncio vCGNAT anuncia sua sub-rede que corresponde a um pool de endereços públicos para traduções NAT. Portanto, o tráfego reverso da Internet sempre retorna ao mesmo nó vCGNAT que lida com o tráfego da rede interna.

PRÓS E CONTRAS

PRÓS:

- Facilidade de implantação
- Resposta rápida à incidentes
- Média administração

Contras:

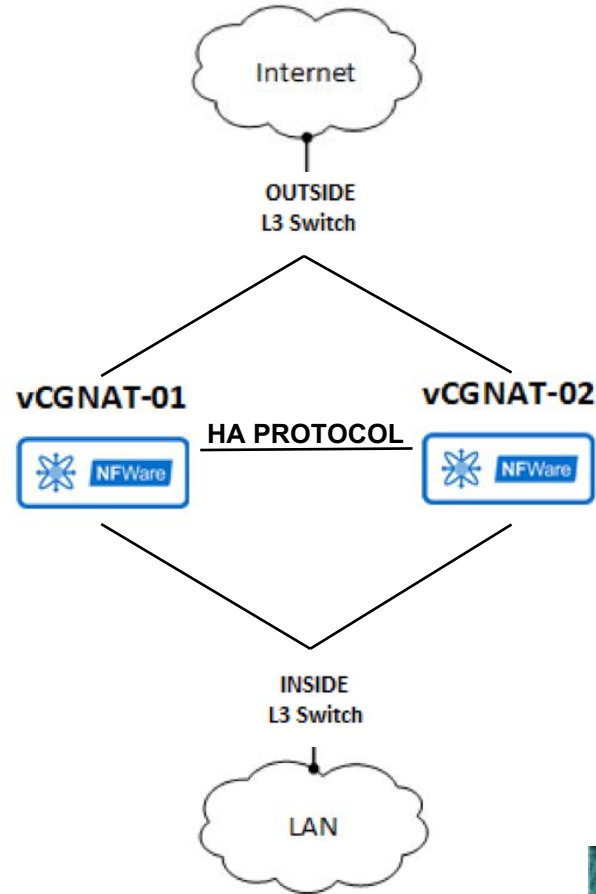
- É preciso ter pelo menos 3 servidores com no máximo 66% do tráfego em cada um deles para obter o benefício em caso de queda de um deles
- Queda das sessões por alguns minutos em caso de incidente

REDUNDÂNCIA REAL ALTA DISPONIBILIDADE (HA) REDUNDÂNCIA DE SESSÃO



ACTIVE / ACTIVE

1+1 DUAL NAT



CENÁRIO

Em um cenário Active/Active (1+1) DUAL NAT, cada vCGNAT tem a mesma configuração, mas rodam um protocolo de HA entre eles.

Chamado de Link Statefull vCGNAT.

A mesma sessão vCGNAT subirá em ambos os servidores e ficará carregada em memória em uma sincronização perfeita.

Qualquer falha ou alternância de serviços o outro servidor entrega a seção para o assinante

PRÓS E CONTRAS

PRÓS:

- Resposta imediata à incidentes
- Não há queda de sessão em caso de incidentes
- Baixa administração

Contras:

- Custo da solução, servidores ligeiramente mais caros
- O dobro de memória ram nos servidores

CONSIDERAÇÕES FINAIS



10 VALIOSAS OBSERVAÇÕES

1. Mitigação de falhas e ataques deve ocupar o centro do pensamento
2. Tudo deve ser feito com foco em SDN VCGNAT
3. Pergunte sempre: Em quanto tempo eu me recupero disto?
4. CGNAT hoje é uma atividade de missão crítica em qualquer ISP.
5. Provedores com + DE 3000 assinantes já precisam de soluções redundantes
6. O CGNAT precisa ser montado de forma a ser recuperado de forma rápida
7. O projeto de redundância deve acompanhar o crescimento do ISP.
8. A escalabilidade é importante
9. Nunca devo empilhar caixas de mesma função



CONTATO – LUCIANO FRANZ



ANTES DE INSTALAR SEU CGNAT PENSE:

- Se queimar meu CGNAT como fico?
- Minha rede é SDN ?
- Como eu lido com as falhas?
- Eu ainda uso Roteador para CGNAT ?
- E se eu precisar crescer a banda?
- Se eu comprar outro provedor?



QR CODE – CONTATO

