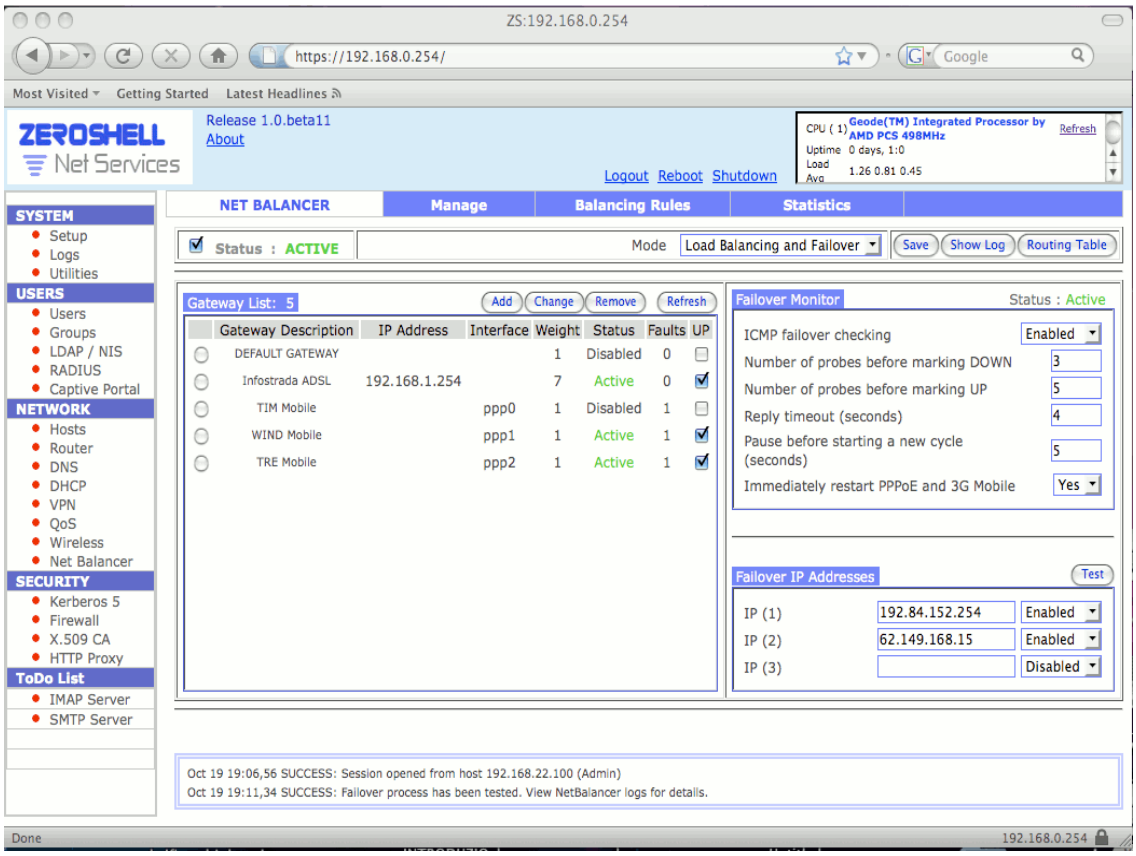
MULTIPLOS LINKS DE INTERNET, BALANCEAMENTO DE TRÁFEGO E GERENCIAMENTO DE FALHAS

O objetivo deste documento é descrever a criação de um roteador para acessar uma rede que use várias conexões de Internet, afim de equilibrar a demanda de saída da LAN e obter uma redundância de acesso à rede, gerenciar situações de falha de um ou vários links.
Para atingir nosso objetivo, vamos usar o módulo Net Balancer do Zeroshell. Por último, vamos analisar a possibilidade de agregação (colagem) de VPN destinadas a aumentar a largura de banda para conexão ponto-a-ponto entre locais remotos através da Internet.

A descrição é dividida nas seguintes seções:

- É realmente possível aumentar a largura de banda de conexão à Internet?
- Configurar gateways de acesso de Internet
- Tolerância a falhas nas ligações via Internet através do Monitor de Falhas
- O balanceamento de tráfego manual
- Agregação de VPN e largura de banda aumentando na camada 2



Balanceamento de carga e proteção por falhas com um Link ADSL e 3 UMTS / HSDPA.

É POSSÍVEL AUMENTAR REALMENTE A LARGURA DA BANDA DE CONEXÃO À INTERNET?

A resposta a esta pergunta não é "sim, absolutamente." Depende do que você quer dizer com o aumento da largura de banda da conexão à Internet. Em essência, o Net Balancer distribui os pedidos originários da LAN por políticas **round-robin** (pesadas) durante vários gateways de Internet. Em outras palavras, se em um determinado ponto no tempo, há somente um usuário da LAN fazendo apenas uma conexão TCP (por exemplo, ele executa apenas um download da Web), o tráfego fluirá a partir de um único gateway, portanto, não beneficiaria o equilibrio das conexões. Em vez disso, se a LAN está lotada com os usuários, cada um executando várias solicitações ao mesmo tempo, como um todo, as suas ligações terão acesso a uma maior largura de banda, igual à soma das larguras de banda de acesso único.

Concluímos então que uma única conexão nunca poderá ter mais largura de banda do que o oferecido por uma única ligação, enquanto que várias conexões simultâneas, na média total têm acesso a uma maior largura de banda, que se estenderá à soma das larguras de banda de todos os Links de internet assim equilibrando a carga.

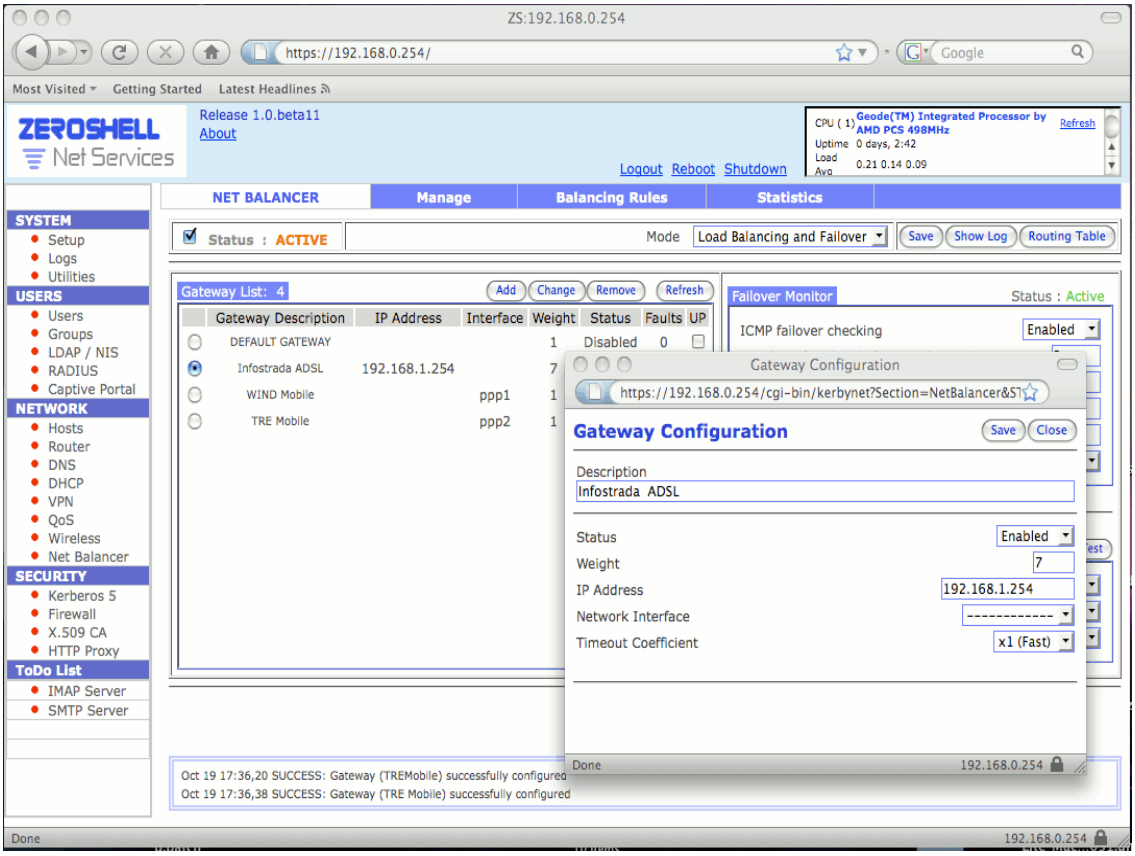
Por outro lado, a agregação da VPN é uma história diferente. Neste caso, o balanceamento de tráfego ocorre na segunda camada (Layer 2), portanto, um aumento da largura de banda também estará disponível para uma única conexão TCP / IP.

CONFIGURAR GATEWAYS DE ACESSO MÚLTIPLO A INTERNET

Gateways de acesso à Internet podem incluir:

- Um roteador, por exemplo, um roteador ADSL. Neste caso, o gateway é identificado pelo Net Balancer através do seu endereço IP;
- Um modem que cria uma conexão ponto-a-ponto (PPP), como um modem ADSL PPPoE ou um modem UMTS / HSDPA. Neste caso, o gateway que naturalmente não tem um IP, é identificado e atribuído na interface Ponto-a-Ponto.

Antes de proceder com o registo das portas de acesso ao Net Balancer, temos de assegurar que sejam física e logicamente ligado ao Zeroshell. Isso significa que, um roteador, por exemplo, deve ser conectado à interface Ethernet e será atribuído um endereço IP pertencente à sub-rede do endereço IP do roteador. Por exemplo, podemos ligar o roteador com IP 192.168.1.254 para ETH01 e atribuir o IP 192.168.1.253.
Por outro lado, se o gateway é um modem, é preciso conectar fisicamente com o Zeroshell via Ethernet, no caso do PPPoE, ou via USB, em caso de conexão móvel 3G, além de criar o Ponto-a-Ponto da interface, respectivamente, a partir de [**Setup**]-[**Network**]- [**PPPoE**] Novo ou [**Setup**] - [**Network**] - [**New Modem 3G**]. Na prática, o modem será atribuído automaticamente a uma interface ponto-a-ponto do tipo ppp0, ppp1 ... Essa interface irá identificar o modem dentro do Net Balancer.



Configurando um gateway dentro do Net Balancer.

Ao clicar no botão [**Add**] para adicionar uma nova porta de entrada ou o botão [**Modify**] para modificar a porta, você irá abrir a janela de configuração do Gateway mostrado acima. Aqui está o que significam os parâmetros:

Description: Contém uma descrição textual do gateway. Ele pode conter o nome do provedor de Internet.

- **Status:** Se definido como Ativo, o Net Balancer irá considerar o gateway ativo e irá geri-lo, caso contrário, ele vai simplesmente ignorá-lo. Por exemplo, se você perceber que um link de Internet falha muitas vezes, você pode optar por desativá-lo, agindo sobre este post.

- **Weight Value:** um número inteiro que representa o peso (importância) da ligação. Sua função depende da forma como o Net balancer está configurado:
- Se o Net Balancer é definido como *Loading balance and failover*, os pedidos de saída para a Internet são classificados proporcionalmente, com base no valor do peso. O maior valor do gateway tem maior probabilidade de ser atribuído um pedido. Temos, assim que reduzir o valor do peso que deve ser fixado proporcionalmente à largura de banda que um link pode suportar. Se todos os links têm a mesma capacidade, o valor do peso pode ser definida como 1 para todos os gateways. Desta forma, as solicitações de Internet são classificados de maneira uniforme ao longo dos links.
- Por outro lado, se o Net Balancer for definido somente como *Failover*, apenas uma das portas disponíveis sera utilizada para satisfazer os pedidos de Internet. Todos os outros gateways são mantidos como reserva, pronto para operar em caso de falha de gateway ativo. A ordem do Net Balancer segue para ativar uma porta de entrada depende do valor do peso. O gateway ativo é aquele com maior valor de peso entre os que não têm falha.
- **IP Address:** o endereço IP do gateway no gateway caso é um roteador.
- **Network Interface:** É atribuído a interface, no caso do gateway é um modem PPPoE (por cabo ou DSL) ou um modem 3G (UMTS o HSDPA).
- **Timeout Coefficient:** ele ativa para gerenciar o *failover* de um link. Deve ser definido como um valor baixo para ligações rápidas e não-saturadas. Seu valor pode ser aumentado se o vínculo acaba muitas vezes em falta devido ao congestionamento. Por exemplo, para uma ligação GPRS-tipo, que tem tempos de resposta alto, este valor deve ser definido como, pelo menos, 4.

Após terminar de configurar os gateways para as diferentes conexões WAN, o Net Balancer poderá ser ativado. Ele irá executar o balanceamento de carga para todas as conexões à Internet imediatamente.

TOLERÂNCIA A FALHAS DE CONEXÕES DE INTERNET ATRAVÉS DO *FAILOVER MONITOR*

O Net Balancer pode ser configurado para operar em um dos dois seguintes modos para regular qual a ligação deverá ser selecionada a atender a uma solicitação específica da Internet:

- **Load Balance and Failover**: Os pedidos de acesso à Internet são automaticamente equilibrados com base no peso (peso) Valor de cada passagem. No caso de um gateway estiver danificado, ele é excluído da compensação automática para evitar a perda de pacotes IP. A atribuição de um determinado tipo de tráfego poderá ser substituída manualmente, com base em critérios próprios (IP origem, IP de destino, portas TCP / UDP, ...);

- **Failover only**: um link ativo por padrão (aquele com o maior valor de peso entre os outros). Os outros são mantidos como reserva, pronto para operarem, caso a conexão ativa seja interrompida. Apesar de o balanceamento automático não ocorrer com essa configuração, o tráfego ainda poderá ser equilibrado conforme explicado abaixo.

Nós acreditamos que a tolerância a falhas é garantida, independentemente da configuração selecionada para o Net Balancer. Para isolar um link com defeito, colocando-o em culpa, dois mecanismos entram em jogo: o primeiro monitora a conexão física com o gateway (modem ou roteador). O segundo mecanismo, conhecido como ***Failover Monitor***, realiza uma análise mais precisa da conexão para verificar a ausência de problemas de roteamento.

O primeiro mecanismo que controla as ligações físicas está implícito no Net Balancer e ativado automaticamente, sem necessidade de ser configurado, vamos discuti-lo mais adiante. Em vez disso, vamos voltar nossa atenção para o *Failover Monitor*, que, por outro lado, deve ser explicitamente ativado e configurado.

A confiabilidade da gestão de falhas é realizada por este componente e fortemente influenciada pelo nível de congestionamento das linhas de dados, conseqüentemente, pelos seus respectivos tempos de resposta. Se o *Failover Monitor* não estiver configurado corretamente, poderá erroneamente colocar uma conexão em falha quando ela estiver apenas congestionada. Pior ainda, ele pode mudar rapidamente seu estado de **ativo** para **falha** e vice-versa, causando o desligamento das conexões à Internet. Se você notar anomalias desta natureza, mesmo depois de ter configurado adequadamente os parâmetros descritos abaixo, você deve desabilitar o *Failover Monitor*.

Certamente é melhor ter um Failover Monitor desativado do que ter ele ativo e causar operações instáveis. Agora, vamos falar sobre os parâmetros de configuração:

ICMP Failover Checking: se definido como ativo, ele ativa o *failover monitor*. Para que o Monitor de falhas comece a funcionar, você deverá especificar e permitir que pelo menos um endereço IP contra falhas. Estes endereços IP deve ser de fora da sua LAN e cada um deverá ser acessível através de todos os gateways.

Number of Probes Before Marking DOWN: valor que representa o número de pings antes de um link ser comutado por falha;
Number of Probes Before Marking UP: indica o número de pings consecutivos de sucesso necessários para retornar um link com deficiência a atividade;

Reply Timeout (seconds): representa o tempo máximo de espera para uma resposta ICMP. No caso dos links estarem congestionados, aumentando este valor poderá ajudar. Tenha em mente que o tempo de espera real pode ser calculado multiplicando este valor pelo coeficiente de tempo limite indicado no parágrafo anterior

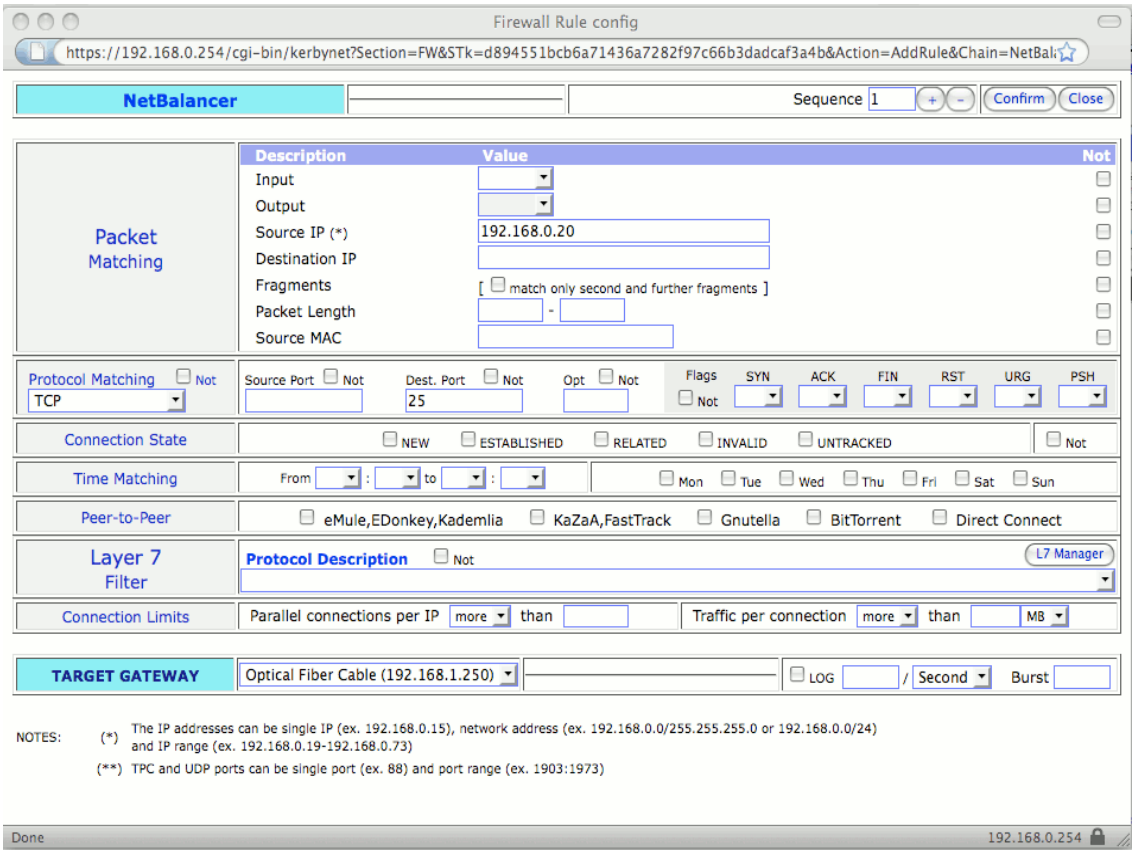
Pause Before Starting a New Cycle (seconds): ciclos de acompanhamento são separados por uma pausa, cuja duração é representada por este valor

Immediately Restart PPPoE and 3G Mobile: Se esta entrada for ativada, o ponto de conexão a falha será zerada. Isso pode resolver rapidamente o problema, embora exija a renegociação do endereço IP, se ele for dinamico.

Varias tentativas podem ser necessárias para que o sistema de sobreposição de falhas venha a atingir a configuração ideal. Em geral, é uma questão de encontrar o equilíbrio certo entre a intervir rapidamente para isolar uma conexão com a Internet funcionando e evitar falhas de conexões que estão simplesmente congestionadas.

BALANCEAMENTO DE TRÁFEGO MANUAL

Por vários motivos, pode ser necessários evitar a compensação automática de certos tipos de tráfego. Em outras palavras, as conexões específicas deveram ser limitadas a um determinado gateway. A fim de fazê-lo, o Net balancer oferece uma interface web [**Net Balancer**] - [**Balancing Rules**], que se assemelha a um firewall e as interfaces de QoS de classificação. Na verdade, as regras pelas quais se escolhe as ligações a rota manual em uma porta específica são definidas como no firewall, usando os endereços IP, portas TCP / UDP e assim por diante.

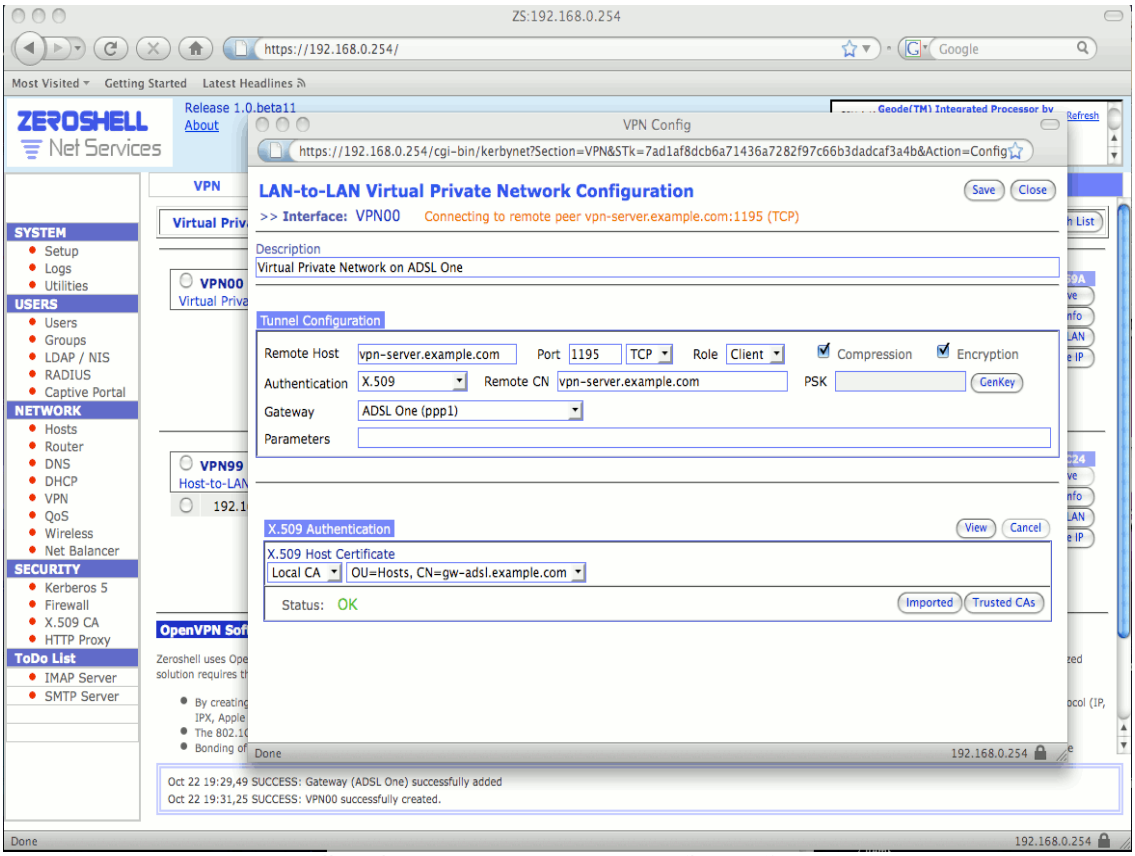


Regra para roteamento do tráfego SMTP manualmente.

O exemplo da figura ilustra a forma como o tráfego de SMTP (porta 25, TCP), gerado pelo servidor de e-mail com o endereço IP 192.168.0.20, é forçado a sair pelo router 192.168.1.250, que liga a uma linha de fibra óptica.

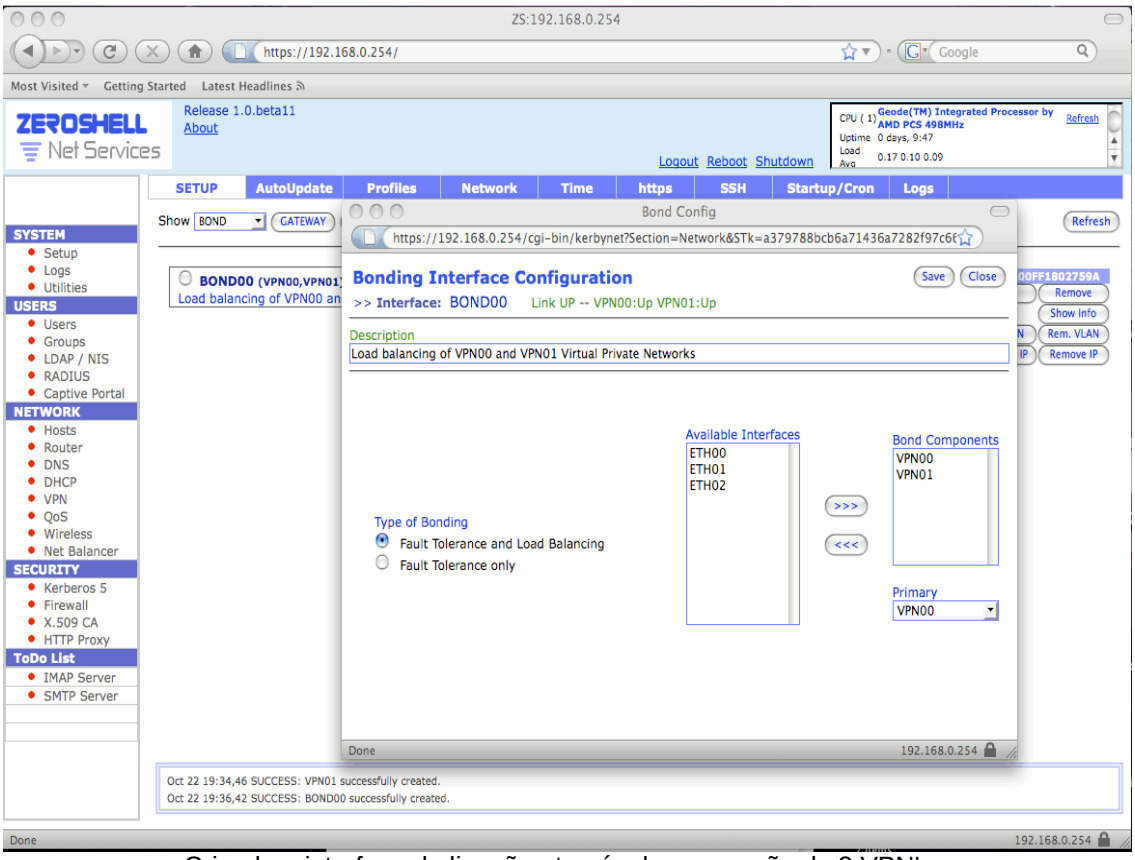
AGREGANDO VPN E INCREMENTANDO LARGURA DE BANDA NA CAMADA 2 MODELO OSI

Uma VPN LAN-to-LAN pode ser configurada no Zeroshell, podendo ser obtidas usando o OpenVPN e interfaces TAP virtuais. O último inteiramente semelhante a uma interface de rede Ethernet real e, como tal, podem ser agregadas através de uma ligação. Esta funcionalidade está disponível desde a primeira versão do Zeroshell. No entanto, para a ligação VPN ser justificada, cada túnel VPN pertencente ao vínculo deve fluir a uma ligação Internet em separado. Antes do Net Balancer ter sido introduzido ao meio, isto é feito através de rotas estáticas que são exigidas pelo menos em um ponto de ter dois IP público. Agora, graças ao Net Balancer, o formulário de configuração de VPN site-to-site permite que você escolha um gateway para configurar a conexão criptografada. Isso simplifica muito a configuração de nenhuma rota estática e exigindo mais dois endereços IP públicos.



Escolhendo um gateway para a configuração VPN..

Uma vez que as VPNs são criadas e atribuídas a seus respectivos gateways, a interface de ligação pode ser criada, como mostrado na figura abaixo:



Criando a interface de ligação através da agregação de 2 VPN's..

A interface BOND00 criada é equivalente a uma interface Ethernet: pode conter endereços IP, adicione VLAN 802.1q, ou ser atribuída a uma ponte. Como mencionado no início, uma vez que o balanceamento de carga na ligação se efetue em quadros Ethernet, mesmo um único TCP / IP irá desfrutar de uma banda maior, graças à presença de vários links

.