Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

THIAGO MARCO DA SILVA ARTERO

Firewall de Borda e Roteadores Cisco
(CISCO PIX SECURITY APPLIANCE)

Assis
2012

THIAGO MARCO DA SILVA ARTERO

Firewall de borda e Roteadores Cisco
(CISCO PIX SECURITY APPLIANCE)

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientador: Me. Fabio Eder Cardoso

Assis

2012

FICHA CATALOGRÁFICA

ARTERO, Thiago Marco da Silva
FIREWALL DE BORDA E ROTEADOR CISCO (CISCO PIX SECURITY APPLIANCE) / Thiago Marco da Silva Artero. Fundação Educacional do Município de Assis – FEMA --
Assis, 2010.
39p.
Orientador: Me Fabio Eder Cardoso
Trabalho de Conclusão de Curso - Instituto Municipal de Ensino Superior de Assis - IMESA
1 – Firewall de Borda; 2 – Roteador Cisco Pix

CDD:001.6
Biblioteca da FEMA

THIAGO MARCO DA SILVA ARTERO

Firewall de borda e Roteadores Cisco
(CISCO PIX SECURITY APPLIANCE)

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientador: Me. Fabio Eder Cardoso.

Analisador: Me. Douglas Sanches da Cunha.

Assis
2012

DEDICATÓRIA

Dedico este trabalho aos meus pais, minha esposa, e a todos meus amigos que me ajudaram e apoiaram.

AGRADECIMENTOS

Á Deus que me permitiu chegar até o final, adquirindo conhecimento necessário para enfrentar todas as dificuldades e obstáculos encontrados no caminho.

Ao meu orientador e amigo Fabio Eder Cardoso, que me incentivou e ensinou a transformar estudo e esforço em conhecimento.

A minha esposa e todos os meus familiares e amigos que estiveram ao meu lado nos momentos mais difíceis desta jornada, e a todos que acreditaram na execução deste trabalho.

RESUMO

Este trabalho tem como objetivo ajudar a pessoas e empresas a se defender de invasões virtuais existentes entre redes internas e redes externas, tendo como finalidade evitar intrusos; contam também com um mecanismo de segurança, baseado em hardware ou softwares atuantes na varredura e proteção dos dados de grandes e pequenas organizações, ajudando assim, a se blindarem de pessoas mal intencionadas, estas visam atacar ou roubar dados relacionados a informações sigilosas, fazendo mal uso das contas de usuários domésticos ou corporativos em softwares em computadores. Na demonstração aplicada em testes do envio de pacotes do roteador cisco Pix Security Appliance, para o firewall de borda, acerca da metodologia utilizada no decorrer dos capítulos, filtrou-se e foi realizado o controle de tráfego de pacotes inseridos na rede de computadores. No seguinte passo os dados foram monitorados e enviados com diferentes níveis de segurança observando sua confiabilidade ou não. Após verificou-se a procedência dos pacotes enviados nos Sistemas das organizações, sejam elas de grande ou pequeno porte.

Palavras – chave: Firewall, Borda Roteador, Cisco Pix Security Appliance

ABSTRACT

This paper aims to help people and companies to defend against invasions virtual networks between internal and external networks, and aims to prevent intruders, also come with a safety mechanism, based on hardware or software operating in the scanning and data protection large and small organizations, helping thus to blinder of bad guys, they aim to attack or steal data relating to confidential information, misusing accounts of home users or corporate software on computers. In the demonstration tests applied in sending packages Pix Security Appliance cisco router, firewall to the edge, about the methodology used in the course of the chapters, filtered, and was conducted traffic control packets inserted into the computer network. In the next step the data were monitored and sent to different security levels observing its reliability or otherwise. After verified the origin of packets sent in the systems of organizations, be they large or small.

Keywords: Edge, Firewall, Cisco PIX Security Appliance Router

LISTA DE IMAGENS

SUMÁRIO

1 – Objetivos.

Este trabalho tem como finalidade de ajudar as empresas a se protegerem de invasões que existem entre redes interna e externa de computadores, com a intenção de evitar intrusos, mas isso só poderá ser possível se empresas passarem a se adquar com os mecanismos de segurança, pois, baseados em hardware ou softwares que protegem dados de grandes e pequenas organizações e as ajudam a se defenderem de pessoas más intencionadas que tentam atacar e roubar os seus dados para serem usados de má fé.

Na demonstração deste trabalho será realizada uma simulação com a ferramenta de aplicação GNS3 (Simulador de Rede), que ira enviar o pacote para o roteador cisco Pix Security Appliance, para o firewall de borda, que ira filtrar e controlar o tráfego de pacotes que existe na rede de computadores tanto na área interna e externa que ira testar se os dados que estão sendo enviados com diferentes níveis de segurança e se eles são confiáveis ou não, e também para verificar qual a procedência dos pacotes que estão tentando entrar no sistema de grandes e pequenas organizações a fim de proteger os seus dados.

2 – Justificativa.

O projeto foi desenvolvido com o propósito de suprir as necessidades de empresas de grande e médio porte trazendo assim informações sobre as novas ferramentas de segurança que existem no mercado atual, pois, com essas informações as mesmas podem se adequar melhor, assim, protegendo seus documentos com uma maior segurança, daí a necessidade de desenvolver este projeto.

3 – Motivação.

Atualmente, com o avanço tecnológico tem como foco a questão da proteção em computadores, e que de fato esta muito vulnerável a qualquer tipo de invasão seja na sua vida social e na sua rotina de trabalho, portanto a medida mais adequada seria então se enquadrarem o quanto antes no sistema de proteção, ou seja, tentando se proteger. Essa tão procurada proteção pode ser encontrada no firewall e antivírus. Mas mesmo assim corre o risco de não estarem totalmente protegidas, imagine uma empresa que tem um sistema sofisticado que faz diversas transações financeiras, tiramos como exemplo um banco que controla depósitos, saques e transferências on-line, se no mesmo não houver um sistema de segurança de uma boa qualidade qual confiança que seus clientes podem depositar nessa instituição? Por isto que hoje a grande maioria optou por darem uma atenção maior aos sistemas de seguranças como firewall e roteadores cisco para assim proteger seu maior patrimônio, ou seja, seus clientes.

4 – Metodologias de Pesquisa

Será utilizado para o desenvolvimento do trabalho um conjunto de livros, apostilas e tutoriais que servirão de base para a simulação pratica.

Recursos necessários.

Utilizaremos para a simulação de tentativas de invasão ao sistema a internet: servidor, roteador Cisco PIX Security Appliance, um computador pessoal, sistema operacional Windows e simulador GNS – 3.

E também utilizaremos o laboratório de rede para o teste que será realizado as simulações do projeto.

5 – Perspectivas de Contribuição.

A perspectiva é de que este trabalho apresente as vantagens do firewall de borda e dos roteadores cisco (Roteador Cisco PIX Security Appliance), para prevenção de ataques nos sistemas de pequenas empresas e grandes corporações e de divulgar as novas ferramentas cisco contra os ataques de pessoas más intencionadas.

6 – Introdução.

A Internet é uma ferramenta fundamental para os negócios. Porém para ter um uso efetivo, é necessário criar controle que evite muitos abusos e desperdícios. As maiorias de pesquisas revelam que o acesso á internet pode levar um usuário a desperdiçar ate 20% do seu tempo produtivo acessando conteúdo para fins pessoais. O mau uso desta ferramenta também é responsável pelo aumento da contaminação por vírus. (Retirado de: **Firewall de Borda** ”http://www.tixperts.com.br/produtos/firewall”) Ultimo acesso em: 20 de março 2012.

O Firewall de Borda é um sistema desenvolvido para prevenir o acesso não autorizado a uma rede privada, ou proveniente dela. A tarefa básica do firewall e de controlar tráfegos entre redes de computadores com diferentes níveis de confiança, como por exemplo, a rede Internet (zona não confiável), a rede de servidores (zona desmilitarizada), e a rede interna de uma empresa (zona confiável). (Retirado de: **Firewall de Borda** ”http://www.tixperts.com.br/produtos/firewall”), Acesso em: 20 de março 2012.

7 - Redes de Computadores.

As redes de computadores foram criadas a partir da necessidade para compartilhar dados e dispositivos. Com a distribuição dos dados valiosos ou não, tal ambiente passou a ser de um estudo de vulnerabilidades, tantos por partes dos administradores conscientes, contra ameaças, sabotagem ou espionagem industrial por exemplo.

Contudo, para que a comunicação de dados ocorra entre redes de computadores e necessário que uma serie etapas e de requisitos sejam compridos. Podemos dividir comunicação em redes em 4 camadas parte física (placa de redes e cabeamentos), camadas de endereços e roteamentos (responsável pelo endereçamento e pela escolha do melhor caminho para entregas do dados), e parte

do transporte (protocolo de comunicação responsável pelo transporte e integridades dos dados), e camada de aplicação(que faz a interface com o usuário). Se algum deste elemento altar não a comunicação entre os dados. (Retirado de: **Segurança em Redes** ”http://www.rmc.eti.br”), Ultimo acesso em 01 de dezembro 2012.

7.1 - Interfaces de Redes.

As interfaces de rede permitem que os servidores que executam o Roteamento e acesso remoto se comuniquem com outros computadores por meio de redes públicas ou privadas. As interfaces de rede têm dois aspectos relacionados ao roteamento e acesso remoto: o hardware físico, como o adaptador de rede, e a configuração de interface de rede.

7.1.1- Transmissões de dados Camada Física.

O principal conceito de transmissão de dados e divisão de pacotes, ou frame de redes, dependendo da camada analisada. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

Os pacotes possuem uma serie de controles para transmissão de dados, como delimitadores de inicio e fim, e uma checagem de erros (para quem receber o pacote verificar se ele chegou com erros) e uma forma de endereçamentos (para identificar a escolha da rota). Como a maioria dos meios de transmissões só permitem um acesso por vez à divisão de pacotes resolve o problema de forma inteligente. Se cada ponto que deseja transmitir, o fizer em pedaços com intervalos de tempos entre as transmissões, para o usuário parecera que a comunicação e simultânea. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

Existem outras formas de transmissões uma delas se chama toke passing, neste método de acesso ao meio cada computador transmite em uma ordem determinada, de forma que todos tenha o mesmo tempo de acesso ao meio. Outra forma seria frame switching usado em redes ATM ou frame Relay (de altíssima velocidade). (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.2 - Transmissões de dados Camada de redes.

A camada de redes e responsável primeiramente pelo endereçamento lógico de pacotes. Assim é possível determinar a origem a escolher o melhor caminho para os pacotes, por exemplo, numa rede complexa como internet, frequentemente existem vários caminhos entre seu computador e um servidor no Japão através do seu endereço de origem, alguns roteadores decidirão qual o melhor caminho, baseado em trafego de distância entre o seu servidor e o seu computador. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.3 - Transmissões de dados Camada de transportes.

Na camada de transporte são desempenhadas tarefas de controles de tráfegos nesta camada existe mecanismo que o pacote foi não transmitido corretamente se mesmo chegou a sequencia, bem como a adequação a velocidade de transmissão. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.4 - Transmissões de dados Camada de aplicação.

Nesta camada estão presentes os protocolos que fazem direta interface com o usuário, ou trata as informações da rede, nos apresentando de uma forma compreensível. Para que o usuário consiga visualizar a rede, existe nesse caso um protocolo, chamado NetBios, que torna possível aquele tipo de representação. Outro exemplo e o FTP (File transfer protocol), um protocolo de pilha TCPIP, usados para transferência do arquivo. Através dele o usuário ganha o prompt de comando, de onde ele pode enviar e receber arquivos depois de adequadamente autenticados. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

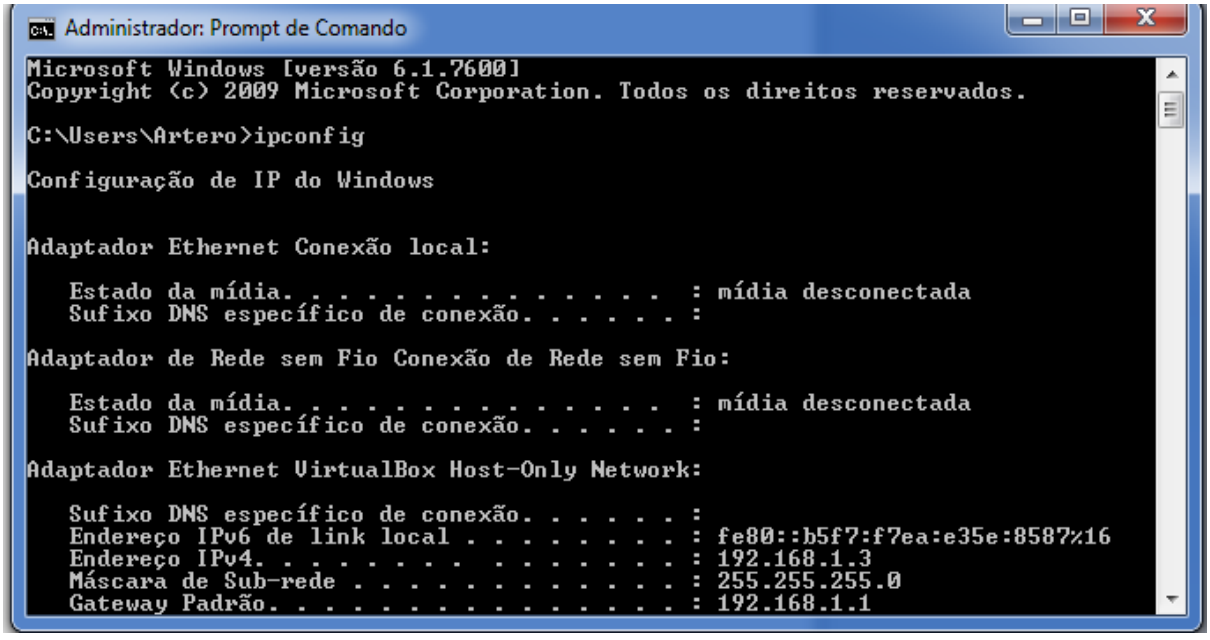

Figura 1- Exemplo do Prompt de Comando.

7.1.5 - Conexões a uma rede.

A comunicação de um computador a uma rede se da atendendo a necessidade de todas as camadas apresentado. Primeiro precisamos de umas interfaces físicas, que permite ao computador a enxergar ao meio de comunicação das redes, isto é feito geralmente através de uma placa de redes ou de um modem. A forma mais comum de conexões é através de cabeamento par trançado, ou através de cabeamentos coaxial. A maioria das redes locais usam desta tecnologia, ou, caso maior velocidade ou maior distancia seja necessária algumas tecnologias baseadas em fibra ótica ou transmissão sem fio. (Retirado de: **Segurança de Redes** “http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.6 - Interligando redes.

Dada a abrangência de alguma rede como a internet determinadas pilhas de protocolos (linguagem de comunicação de computadores), foi projetada para suportar a divisão em endereços por regiões similares ao seu bairro em nossa cidade. Estas divisões permitem uma melhor configuração da rede, como as organizações das maquinas de transmissões de dados de forma hierárquica. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.7 - TCP/IP.

TCP/IP (Transmission Control Protocol/Internet Protocol), e uma pilha de protocolo que vem sendo numerada há décadas, dez da criação de uma rede chamada ARPANET, em meados dos anos 60. Ao contrario de que muitos acham

não é apenas um protocolo de comunicação e sim uma pilha deles. Esta pilha de linguagem de comunicação permite que todas as camadas de comunicação em redes sejam atendidas e a comunicação seja possível. Todas as pilhas de protocolos, de uma forma ou de outra, tende a atender todas as camadas, para permitir que os computadores consigam trocar informações. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.8 - ARP (Anddress Resolution Protocol).

O ARP e um protocolo responsável, pelo mapeamento ou associação do endereço físico ao endereço logico, de computadores de uma mesma rede. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.9 – IP.

A Internet Protocol e o responsável logico pelo endereçamento do TCP/IP. Além disso, é responsável pelo roteamento dos pacotes, e sua fragmentação, caso a rede seguinte não possa interpretar os pacotes do mesmo tamanho.

Exemplos de endereços IP.

192.168.3.4

200.241.236.94

Apesar de aparentemente não ter muita lógica, este endereço contém uma série de informações. Estas informações são para deixar a nossas vidas mais fáceis, porque o computador entende como quatro octetos ou quatro campos de oito bits.

11110000.11000011.00110011.01011110

Para organizar os endereçamentos foram divididos em cinco classes.

Classe A

Classe B

Classe C

Classe D

Classe E

Classe A

O primeiro octeto tem o formato de binário se inicia com zero basta converter o número mínimo e máximo, de 8 bits, com o primeiro bit igual a 0.

Binário: 00000000 a 10111111

Decimal: 192 a 223.

Classe B

O primeiro octeto em binário iniciado por 10.

Binário: 10000000 a 10111111

Decimal: 128 a 191

Classe C

O primeiro octeto em binário iniciado por 110.

Binário: 11000000 a 11011111

Decimal: 192 a 223

Classe D

São usados para endereçamentos de computadores a classe D e reservada para um serviço muiltcast.

Classe E

E reservadas para experimento ambas são reservadas.

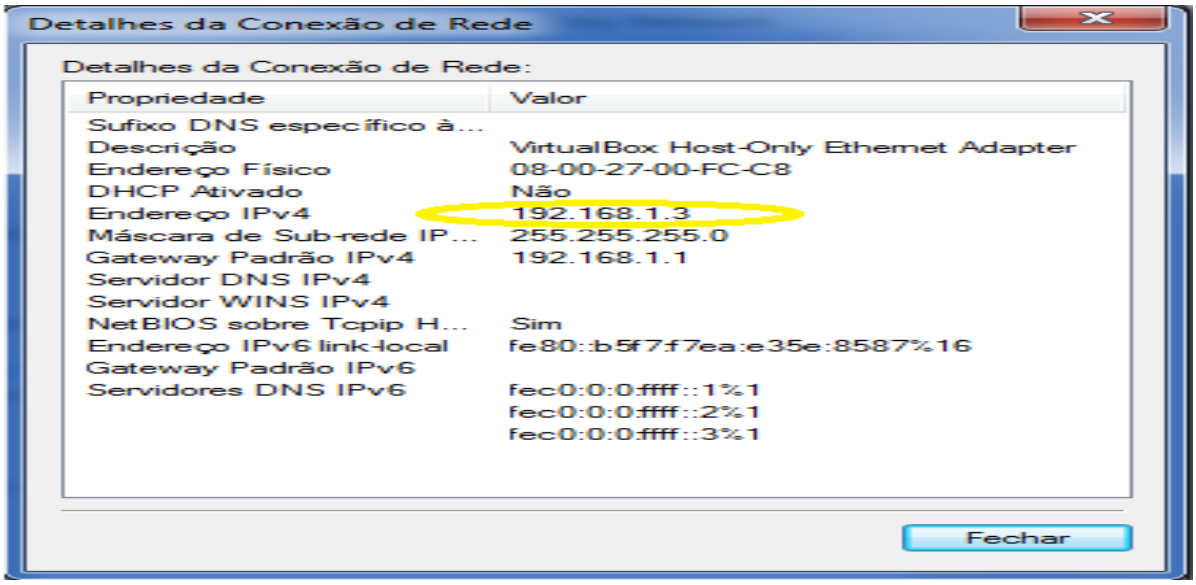

Figura 2 - Exemplo de IP.

7.1.10 - **Máscara.**

Ao contrário de nós pensarmos a classe do endereço não determina ou fixa que porções do endereço representam a rede, e proporções o endereço representa a maquina dentro da rede, isto e feito pela máscara de subredes.

Exemplo de máscara redes.

Classe A máscara 255.0.0.0

Classe B máscara 255.255.0.0

Classe C máscara 255.255.255.0

O endereço 200.241.35.46 e um endereço de classe C, e a sua máscara e 255.255.255.0.

O endereço 10.126.46.99 e um endereço de classe A, e a sua máscara e 255.0.0.0.

O endereço 190.23.56.89 e um endereço de classe B, e a sua máscara e 255.255.0.0.

Exemplo de máscara de redes.

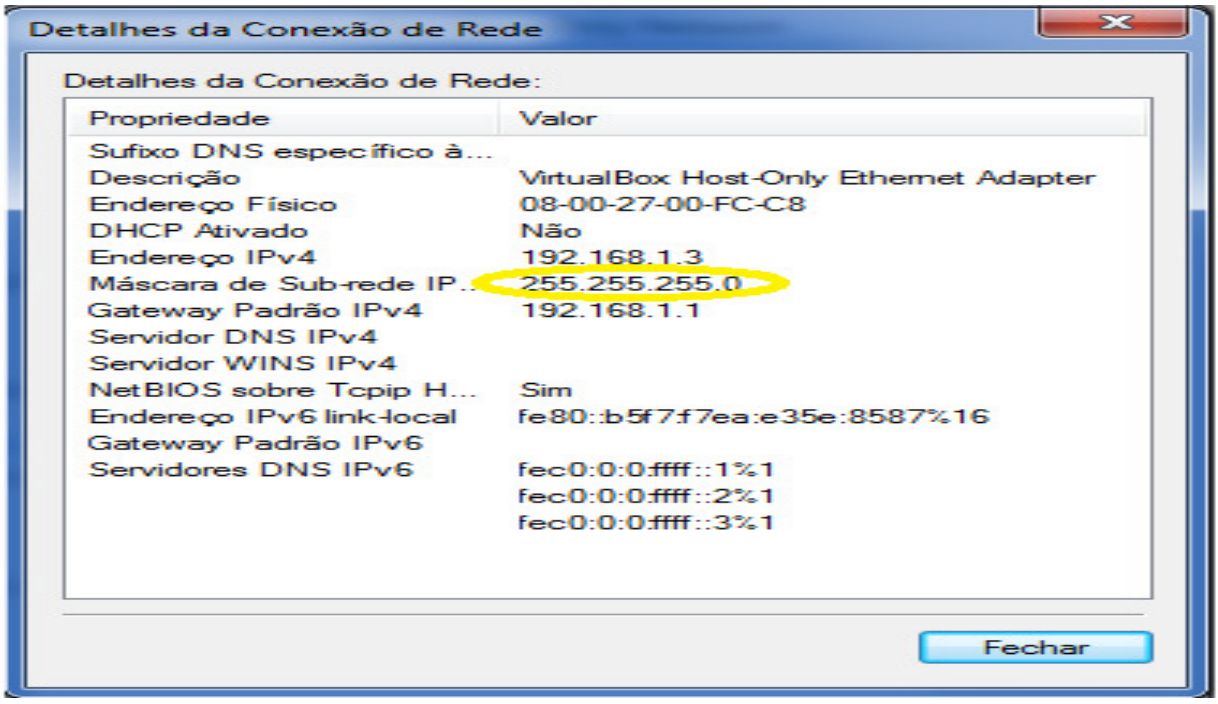

Figura 3 - Exemplo de Mascara de Redes.

7.1.11 - ICMP (Internet Control Message Protocol).

A função do ICMP e basicamente de diagnóstico e tratamento de mensagem. Através dele é possível determinar, quanto tempo um pacote esta demorando em ir para uma maquina remota e voltar (ROUND TRIPE), bem com verificar se ouve perda de pacote durante a transmissão. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.12- TCP (Transmission Control Protocol).

O TCP e um protocolo de transporte, responsável pela entrega de pacotes e sua característica e confiabilidade, para cada endereço que enviado pacote ele espera uma confirmação do destino confirmando a entrega do pacote em seu

destino. Ele também coloca os pacotes em números de sequência para que os pacotes possam remontar os dados originais, caso eles chegam em caminhos diferentes do seu destinos. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.13– UDP.

Assim como TCP o UDP faz a mesma função do TCP de transportar os pacotes ao seu destino, mas ele não possui nenhuma checagem de erro ou de desvio do pacote caso ele se perca no caminho do seu destino. Ele e muito usado em aplicações que necessitem de trafego urgente, que não sejam tão sensíveis a perda de pacotes. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.14- DNS (Domain Name System).

O DNS foi criado para evitar transtorno. Através dele, através dele cada Host recebe um nome, mais fácil de aprender, dentro de uma hierarquia, o que ajudam ainda mais na hora de identifica-lo.

Um exemplo seria www.uol.com.br, este caso e uma referência ao servidor www dentro do domínio uol.com.br. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.15- Sockets (Soquetes de Comunicação).

Sockets é a base de comunicação de uma rede, ele faz a transferência de dados ocorrerem nas maquinas a conexão montadas por três informações.

1. Endereçamento (origem do destino)
2. Porta de origem e destino.
3.Transportes (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.16- Ping (Packet Internet Grouper).

Ele utilizado como protocolo para diagnosticar o tempo de resposta de dois computadores ligados em uma rede TCP/IP. A partir dai pode se ter uma estimativa do tráfego do pacote, bem como o tempo de latência do canal, a latência e um link ligado direto a velocidade do roteador em termos de processamento. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.17- Tracert (trancerout).

O Tracert também utiliza pacotes para fazer diagnóstico, porém ele determina qual o caminho que os pacotes irão fazer até o host. A função dele é tratar o destino dos roteadores e também mede o tempo médio em que os pacotes levarão para atingir o seu destino, ele também ajuda a verificar se os roteadores estão configurados corretamente. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.18 - DHCP (Dynamic Host Configuration Protocol).

Inicialmente, a necessidade de automatizar a requisição e distribuição do endereço IP deu-se em função da existência de estações sem disco (*diskless*). Esta demanda provocou o uso do protocolo de camada de enlace RARP.

Foi criado, então, o DHCP, uma versão estendida do BOOTP, que permite a atribuição dinâmica de endereços IP. O DHCP foi designado para resolver esse problema enquanto simplifica a administração da rede TCP/IP.

O DHCP é especificado pela **IETF - Internet Engineering Task Force** por meio dos RFCs (*Requests For Comments*).

Outro fator importantíssimo e que pode ser considerado como o principal é a locação rápida e dinâmica de um endereço IP para um equipamento conectado à rede.

ATRIBUIÇÃO DE ENDEREÇO

O DHCP pode atribuir endereço para um equipamento de rede de três formas:

- Configuração manual;
- Configuração automática;
- Configuração dinâmica.

Configuração Manual

Neste caso, é possível atrelar um endereço IP a uma determinada máquina na rede. Para isso, é necessária a associação de um endereço existente no banco do servidor DHCP ao endereço MAC do adaptador de rede da máquina. Configurado desta forma, o DHCP irá trabalhar de maneira semelhante ao BOOTP. Esse endereço "amarrado" ao equipamento não poderá ser utilizado por outro, a não ser que eles utilizem a mesma placa de rede. (Retirado de: **Segurança de Redes**

”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

Configuração Automática

Nesta forma, o servidor DHCP é configurado para atribuir um endereço IP a um equipamento por tempo indeterminado. Quando este se conecta pela primeira vez na rede, lhe é atribuído um endereço permanente. A diferença existente entre esta e a primeira configuração é que nesta não é necessária uma especificação do equipamento que utilizará determinado endereço. Ele é atribuído de forma automática. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

Configuração Dinâmica

Neste tipo de configuração, é que reside a característica principal do DHCP, que o diferencia do BOOTP. Desta forma o endereço IP é locado temporariamente a um equipamento e periodicamente, é necessária a atualização dessa locação. (Retirado de: **Segurança de Redes** “http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1“), Ultimo acesso em 01 de dezembro 2012.

Com essa configuração, é possível ser utilizado por diferentes equipamentos, em momentos diferentes, o mesmo endereço IP. Basta, para isso, que o primeiro a locar o endereço, deixe de utilizá-lo. Quando o outro equipamento solicitar ao servidor DHCP um endereço IP poderá ser fornecido ao mesmo o endereço deixado pelo primeiro. (Retirado de: **Segurança de Redes** “http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

7.1.19- RARP (*Reverse Address Resolution Protocol*).

Para entender o funcionamento do DHCP, é necessário entender como funciona o BOOTP, pois ele exige também o conhecimento do funcionamento e seus problemas do RARP. (Retirado de: **Segurança de Redes** "http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1"), Ultimo acesso em 01 de dezembro 2012.

Para um computador enviar e receber data gramas é preciso que ele possua um endereço IP de 32 bits que o identifique. O IP fica armazenado na memória do computador, carregando o boot. Quando o computador não possui um disco para iniciar o sistema para carregar o endereço do IP. (Retirado de: **Segurança de Redes** "http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1"), Ultimo acesso em 01 de dezembro 2012.

Toda a maquina possui placa de rede com identificação única que não se repete, pois a identificação e uma sequenciam de bits que fica armazenado no chip da placa que o endereço físico da maquina na placa. A estação diskless utiliza um protocolo para obter o IP que faz o uso do endereço físico da placa. (Retirado de: **Segurança de Redes** "http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1"), Ultimo acesso em 01 de dezembro 2012.

7.1.20– BOOTP.

As deficiências encontradas no RARP foram solucionadas com a criação do BOOTP (*BOOTstrap Protocol*). Por utilizar o UDP para trafegar suas mensagens, ele também é mais eficiente que este protocolo por embutir em sua mensagem e outras informações importantes para a inicialização. (Retirado de: **Segurança de Redes** "http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1"), Ultimo acesso em 01 de dezembro 2012.

A Diferença comunicação do RARP, a comunicação BOOTP se processa na camada de rede. A estação cliente lança a sua solicitação na rede utilizando um endereço IP. Os servidores BOOTP e o único a reconhecer e responder também por difusão. Esta forma de resposta é utilizada pelo fato do cliente não possuir ainda, o seu endereço IP. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

O BOOTP delega ao cliente toda a responsabilidade por uma comunicação segura, pois, porque os protocolos utilizados são passíveis de corrupção ou perda de dados. O BOOTP solicita ao UDP - User Datagrama Protocol - que faça um checksum e ainda especifica que solicitações e respostas tenham seu campo **DONT FRAGMENT** ativo para comportar clientes de memória pequena. (Retirado de: **Segurança de Redes** ”http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1”), Ultimo acesso em 01 de dezembro 2012.

8 - Firewall.

Dentre os dispositivos de segurança necessários para proteger sua empresa de acessos indevidos e outras ameaças vindas da Internet e da rede local, o Firewall é o principal.

Foi optado por se trabalhar com Firewall de borda e roteador Cisco Pix Security Appliance para dar um respaldo maior a empresas para se defenderem de invasões que possam vir a atingir redes internas e redes externas. São compostas por mecanismo de segurança, baseado em hardware ou softwares que possam proteger dados de grandes e pequenas organizações de pessoas que tenham outros tipos de intenções, assim tentando atacar ou roubar dados, prejudicando as empresas.

O roteador Cisco Pix Security Appliance tem a função de filtrar e controlar o tráfego de pacotes que existem na rede de computadores, assim com a finalidade de testar os dados que estão sendo enviados com diferentes níveis de segurança, para terem a certeza se é confiáveis, averiguando também a procedência dos pacotes que estão tentando entrar no sistema de grandes e pequenas organizações. Retirado de: **Cisco PIX 525 Security Appliance** "http://www.enfon.com/cisco-pix525-datasheet.pdf"), Ultimo Acesso em: 20 de março 2012.

8.1- O que um Firewall pode fazer para a sua segurança.

- Garante uma infraestrutura de rede mais segura.
- Permite o acesso seguro a servidores internos.
- Permite o acesso seguro entre filiais e usuários externos.
- Bloqueia o acesso a sites de rede social (Facebook, Twitter, Orkut e outros).
- Bloqueia o acesso a sites de radio, músicas e vídeos.
- Bloqueia o acesso a redes P2P, que desrespeitam o direito autoral.
- Bloqueia o acesso a sites de sexo explícito, que incorre em crime.

- Diminui o risco com problemas jurídicos, pois a empresa é corresponsável por ações ilícitas praticadas por seus funcionários.

8.1.2 - Descrição técnica.

- É firewall de borda (roteador).
- Protege contra ameaças de entrada da Internet.
- Gerencia o acesso por usuário, através de relatórios.
- Pode autenticar os usuários no Active Diretory da Microsoft ou no LDAP do Linux.
- Faz redirecionamento de portas/serviços de servidores internos.
- Faz bloqueio de um computador específico.
- Faz filtro de conteúdo (palavras).
- Faz filtro de aplicações (msn, skype e outros).
- Faz NAT (traduz endereços de rede) da rede interna para a conexão da Internet.
- Faz serviço de PROXY HTTP com CACHE (busca e armazena as páginas da Internet).
- Faz serviço de HTTP, páginas web/Internet.
- Faz serviço de VPN, rede privada virtual.
- Faz serviço de DNS, resolução de nomes de sites e equipamentos.
- Faz serviço de DHCP, distribuição dinâmica de endereços IP.
- Faz serviço de FTP, armazenamento e transferência de arquivos.
- Faz serviço de IM, mensagem instantânea corporativa.
- Faz serviço de NTP, sincronização de hora. (Retirado de: **Soluções em TI** “http://www.produnet.com.br/solucoes.php?id_produto=37”), Ultimo acesso 16 de junho 2012.

8.1.3 – Algumas ameaças mais comuns da Internet.

Aqui estão varias ameaças mais comuns da Internet, isso prova que as ameaças que a Internet nos trás, vão muito mais além do que simples trojans e keyloggers, por isso tomem cuidados, usem antivírus, Firewall, antispywares, mantenham o seu sistema operacional atualizado e o principal, sempre tome cuidado onde você entra e o que você baixa. (Retirado de: **Soluções em TI** "http://www.produnet.com.br/solucoes.php?id_produto=37"), Ultimo acesso 16 de junho 2012.

Flash - É comum encontrar uma vulnerabilidade no flash, como ele é vastamente usado em sites, essas vulnerabilidades acabam se tornando ameaças para os usuários.

Links encurtados no Twitter - Os links encurtados postados no Twitter podem esconder malwares que estão no link original.

Scams de E-mail ou Malwares - Malwares são enviados por e-mail, junto com uma mensagem dizendo que é foto de alguém ou que você ganhou alguma coisa, enfim, vocês já conhecem essa ameaça.

Malwares escondidos em arquivos torrents - Malwares são espalhados por meio de arquivos torrents.

Malwares em sites pornográficos – Como já se sabe Malwares em sites pornográficos, resulta em processo jurídico.

Cavalos de Tróia disfarçados de codecs de vídeo - Os codecs de vídeo algumas vezes podem conter cavalos de Tróia, por isso é bom tomar cuidado onde baixa e de quem se baixa!

GPS dos SmartPhones - Você gostaria que um racker soubesse onde você esta nesse exato momento?

Sites de buscas que indicam sites com malwares - Apesar dos sites de buscas como o Google colocarem avisos de segurança em links de sites suspeitos, alguns sites maliciosos ainda passam despercebidos e acabam prejudicando o visitante.

Arquivos PDF maliciosos – Hoje é possível fazer com que um leitor de PDF executasse um programa malicioso apenas ao abrir o arquivo.

Arquivos de vídeo maliciosos - Alguns arquivos de vídeo podem conter malwares escondidos, por isso é importante baixa-los de lugares confiáveis.

Drive-by downloads - Alguns sites maliciosos fazem com que você baixe arquivos automaticamente e os execute em seu computador.

Falsos antivírus - Hoje em dia existem muitos antivírus, mas cuidado, nem todos são mesmo antivírus. Alguns programas simulam o comportamento de antivírus e avisam sobre vírus falsos, e até cobram do usuário para eliminar o falso vírus. Sempre opte por antivírus conhecidos e conceituados.

Anuncios falsos que te leva a baixar malwares - Existem vários anúncios falsos na Internet que induzem o usuário a baixar malwares, esses anúncios são encontrados até mesmo no Google.

Facebook - Nem todos os aplicativos do facebook são seguros, alguns podem colher informações dos usuários e usa-las de forma maliciosa.

Sites de cadastro que vendem informações para spammers - Acreditem, hoje em dia existem muitos sites de cadastro que vendem as informações obtidas para spammers, e não é preciso de muita coisa para fazer um site desse tipo, basta um anúncio chamativo e um formulário com campo nome e e-mail.

Phishing 2.0 em redes sociais - As redes sociais são os principais pontos de referência para a prática de Phishing, onde o invasor procura por diversas

informações, que possa servir para um ataque de força bruta, engenharia social, pesquisas, etc.

Supercompartilhamento de informações em redes sociais - Muitos usuários de redes sociais não se preocupam muito com a segurança, ou não sabem como se proteger. Muitas pessoas compartilham informações que não devem e acaba facilitando e muito a vida do invasor, tem gente que compartilha até mesmo a própria senha de sua conta. (Retirado de: **Soluções em TI** "http://www.produnet.com.br/solucoes.php?id_produto=37"), Ultimo acesso 16 de junho 2012.

Existem também vários tipos de firewall que ajuda as pessoas e empresas a se protegerem contra tentativas de invasão ao seu sistema, abaixo vocês verão alguns tipos de firewall.

Perímetro de 3 segmentos: também conhecido como 3-Leg Perimeter, esse modelo deve ser utilizado por servidores que possuem três adaptadores de rede, sendo um conectado na rede interna, outro conectado na Internet e outro conectado em uma rede de perímetro, ou DMZ, onde estão localizados alguns servidores que precisam ser acessados a partir da Internet.

Firewall Externo: também conhecido como Front Firewall, esse modelo deve ser utilizado por servidores que possuem dois adaptadores de rede. Além disso, o cenário de rede deve possuir outro firewall interno. Ou seja, deve ser utilizado em redes que possuem dois ISA Servers conectados.

Firewall Interno: também conhecido com Back Firewall, esse é o modelo de que deve ser aplicado no servidor ISA configurado como firewall interno, em cenários onde temos 2 ISA Servers conectados.

Adaptador de Rede Exclusivo: também conhecido como Single Network Adapter, esse modelo deve ser aplicado em servidores ISA que possuem apenas

um adaptador de redes. Geralmente, esse tipo de servidor é utilizado para oferecer apenas o serviço de cache ou o serviço de proxy - reverso.

9 - Roteadores Cisco.

Segundo DEAL A. Richard (p.25), “Os roteadores Cisco tem o perímetro com a funcionalidade do firewall e recursos para garantir a segurança da rede para detectar, pois, previne a navegação de serviço (DOS) ataques com TCP Intercept, (CBAC), e a limitação de taxa de técnicas Use (NBAR), assim detectando e filtrando indesejados e maliciosos tráfegos de autenticação do roteador como por exemplo essas duas ferramentas”.

9.1 - Cisco PIX Security Appliance.

Figura 4 (“Retirado de: http://www.tfr.se/rutter/cisco/pix/pdf”), Ultimo acesso 16 de junho 2012.

Oferece uma riqueza de segurança avançada e serviços de redes para empresas de médio e grande porte, e de forma confiável, pois é um aparelho especialmente construído. Este roteador tem uma ampla gama de serviços avançados de firewall, portanto, protegendo empresas de bombardeios constantes e ameaças a internet, em muitos ambientes de redes de negócios. (Retirado de: **Cisco PIX 525 Security Appliance** http://www.enfon.com/cisco-pix525-datasheet.pdf), Ultimo Acesso em: 20 de março 2012.

Originalmente desenhado para ser um NAT, o cisco lançou a série Private Internet Exchange (PIX), firewall em 1994. O PIX e um firewall de alto desempenho que utiliza a filtragem de pacotes, com a introdução de fixup. A PIX permite que o firewall aplique a politica de segurança adicionais para que as conexões sejam identificadas como utilização de protocolos específicos. (Retirado de: "http://www.netcraftsmen.net/resources/archived-articles/369-cisco-pix-firewall-basics.html"), Ultimo acesso 02 de junho 2012.

O PIX Firewall não foi desenvolvido para rodar sob UNIX e Windows da família NT, mas e baseado em um seguro sistema de real-time embarcado, conhecido como Adaptive Security Algorithm (ASA), que oferece a tecnologia de inspeção Stateful. (Retirado de: "http://www.netcraftsmen.net/resources/archived-articles/369-cisco-pix-firewall-basics.html"), Ultimo acesso 02 de junho 2012.

O ASA faz o track dos endereços de origem e destino com a sequência de números TCP, números de portas e outros flags TCP. Todo o tráfego de entrada e de saída é encontrado por politicas de segurança aplicadas nas tabelas de entrada, que armazena todas as informações. (Retirado de: "http://www.netcraftsmen.net/resources/archived-articles/369-cisco-pix-firewall-basics.html"), Ultimo acesso 02 de junho 2012.

O acesso para qualquer sistema por trás do PIX somente e permitido se esta conexão foi validada ou foi especificamente configurada. (Retirado de: "http://www.netcraftsmen.net/resources/archived-articles/369-cisco-pix-firewall-basics.html"), Ultimo acesso 02 de junho 2012.

O PIX pode ser graficamente gerenciado usando a interface de gerenciamento web integrada conhecida como o PIX Device Manager (PDM).

O PDM é uma configuração dos dispositivos PIX que e especifico, em uma ferramenta de gestão enquanto CSPM é geralmente utilizado como parte de uma grande infraestrutura de gestão de segurança e permite correlacionar as politicas de segurança da organização com uma configuração PIX. As interfaces de gerenciamento inclui linha de comando interface (CLI), Telnet, SSH (Secure Shell 1.5), porta de console, SNMP e syslong. (Retirado de:

"http://www.netcraftsmen.net/resources/archived-articles/369-cisco-pix-firewall-basics.html"), Ultimo acesso 02 de junho 2012.

9.1.2 – Serviços de segurança de rede do roteador PIX

- Advanced Application-Aware Serviços de Firewall
- Lider de Mercado de Segurança de Voz-Sobre-IP e Multimidia
- Filtragem de URL
- IPsec VPN
- Inteligencia Networking Services
- Flexibilidade Managemente Solutions.

9.1.2.1 - Segurança na camada de aplicação.

O Cisco PIX oferece uma segurança forte na camada de aplicação através de 30 motores inteligentes a aplicação de reconhecimento fiscalização que examinam fluxos de rede na camada 4-7. Para defender as redes de ataques nas camadas de aplicação e para dar maior controle sobre as aplicações e protocolos utilizados em seu ambiente, esse mecanismo de inspeção incorpora aplicação extensiva e conhecimento de protocolo para empregar a tecnologia de segurança na aplicação que inclui o protocolo de detecção de anomalias, a aplicação faz um acompanhamento de protocolo de estado, o endereço da rede (NAT), serviço de detecção de ataque e técnica de mitigação, como a aplicação no protocolo de comando de filtragem, verificação do conteúdo URL. Este mecanismo de inspeção também das empresa o controle sobre as mensagens instantâneas, peer-to-peer de compartilhamento de arquivos, e a aplicação de tunelamento, permitindo que as empresas possam reforçar as politicas de uso e proteger a banda larga para a

aplicação de negócios. (Retirado de: http://www.cisco.com/en/US/prod/collateral/.html), Ultimo acesso 02 de junho 2012.

9.1.2.2 – Filtragem de URL

Para reduzir a tarefa administrativa e melhorar a eficácia de filtragem, usar o PIX, em conjunto com um servidor separado que execute filtragem de URL, pois o PIX verifica o pedido de URL de saída com a politica definida no servidor de filtragem de URL. (Retirado de: http://www.cisco.com/en/US/prod/collateral/.html), Ultimo acesso 02 de junho 2012.

9.1.2.3 - Mult-Vector-Proteção contra ataque.

O PIX incorpora serviços de proteção multi-vector de ataque para continuar a se defender os negócios de muitas formas populares de ataques, incluindo ataques de serviços de (DOS), ataques fragmentados, ataques de repetição, ataques de pacotes mal informados. Usando uma riqueza de característica de ataque avançados de proteção incluindo o fluxo TCP remontagem, a normalização do trafego, DNSGuard, FlooGuard, FragGuard, MailGuard, IPVerify e interceptação TCP, que interrompe uma série de ataques e pode fornecer em tempo real alerta para os administradores da redes. (Retirado de: http://www.cisco.com/en/US/prod/collateral/.html), Ultimo acesso 02 de junho 2012.

9.1.2.4 - Serviços Voip.

O PIX proporciona uma proteção líder de mercado para uma ampla gama de voz-sobre-IP (VoIP), outra norma de multimídia, isso permite que as empresas de

forma segura tirar proveitos dos muitos benefícios que os dados convergentes, voz, vídeos e redes oferecem, incluindo o aumento da produtividade, redução de custos operacionais e aumento da vantagem competitiva. Ao combinar VPN e Qualidade de Serviço (QoS), com os serviços de protocolo avançadas de inspeção que Cisco Pix fornecem para estes padrões de redes convergentes, as empresas podem estender com segurança de voz e serviços de multimídias e os benefícios que ela fornecem para escritório remoto, escritório domésticos e moveis usuário. (Retirado de: http://www.cisco.com/en/US/prod/collateral/.html), Ultimo acesso 02 de junho 2012.

9.1.2.5 – Serviços de VPN IPsec.

Usando os novos recursos de ful-featured VPN da Cisco PIX as empresas podem se conectar com segurança de redes e usuários moveis em todo mundo através de conexões de internet de baixo custo.

VPN oferece um custo eficaz e é fácil de gerenciar o acesso remoto, VPN e uma arquitetura que elimina os custos operacionais associados a manutenção das configurações dos dispositivos remotos que normalmente são exigidas por soluções de VPN tradicionais.

A VPN fornece recursos sofisticados de serviços a acesso remoto, incluindo aplicações cliente que oferecem acesso seguro e fácil de gerenciamento remoto a redes corporativas. (Retirado de: http://www.cisco.com/en/US/prod/collateral/.html), Ultimo acesso 02 de junho 2012.

10 – Simulador GNS3

Figura 5 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3) Ultimo acesso em 14 de junho 2012.

O simulador GNS3 e um software grátis, open sourse, que pode ser baixado e utilizado livremente. (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3) Ultimo acesso em 14 de junho 2012.

O GNS3 funciona com imagem IOS da Cisco reais, e que são emuladas através de um programa chamado Dynamips. (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3) Ultimo acesso em 14 de junho 2012.

Podemos dizer que o GNS3 é a interface gráfica Dynamips que é o programa que faz todo o trabalho pesado de emular os equipamentos utilizando IOS reais da Cisco. (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3) Ultimo acesso em 14 de junho 2012.

O Dynamips simula os processadores MIPS e PowerPC, que por sua vez executam imagens do IOS destinadas aos roteadores Cisco da série 1700, 2600, 3600, 3700 e 7200. Já o QEMU simula o processador x86 e executa imagens do IOS destinadas ao firewall Cisco PIX e imagens do JunOS destinadas aos roteadores Juniper. (Retirado de: "http://www.cisco.com/application/pdf/paws/15092/copyimage.pdf"), Ultimo acesso 14 de Junho 2012.

Estas imagens não são normalmente distribuídas e trata-se de software proprietário. Por outro lado, as imagens normalmente estão disponíveis nos próprios roteadores, sendo relativamente fácil fazer uma cópia de um roteador para outro, como ilustrado no próprio site da Cisco. (Retirado de: "http://www.cisco.com/application/pdf/paws/15092/copyimage.pdf"), Ultimo acesso em 14 de Junho 2012.

Com sua interface gráfica intuitiva e bem fácil de trabalhar o GNS3 se mostra como uma ferramenta poderosa, capaz de emular redes complexas e que pode ser utilizada por todos aquele que estejam em busca de uma certificação avançada da Cisco. (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3) Ultimo acesso em 14 de Junho 2012.

10.1 – Veja algumas da característica desse poderoso emulador.

- Design de topologias de redes complexas.
- Emulação de muitas plataformas de roteadores Cisco router e PIX firewall.
- Simulações de switches ethernet simples ATM e frame Relay.
- Conexão da rede simulada com o mundo real.
- Captura de pacotes utilizando o Wireshark.

10.1.2- Configuração do GNS3

O GNS3 é o front-end gráfico que permite gerenciar as simulações do Dynamips, criando topologias mais complexas com vários tipos de roteadores. Quando o GNS3 é executado pela primeira vez, ele solicita uma configuração inicial com o caminho do simulador e o caminho das imagens do IOS para os simuladores serem executados.

Esta primeira figura mostra a tela de inicio do GNS3, com as configurações do Dynamips e IOS.

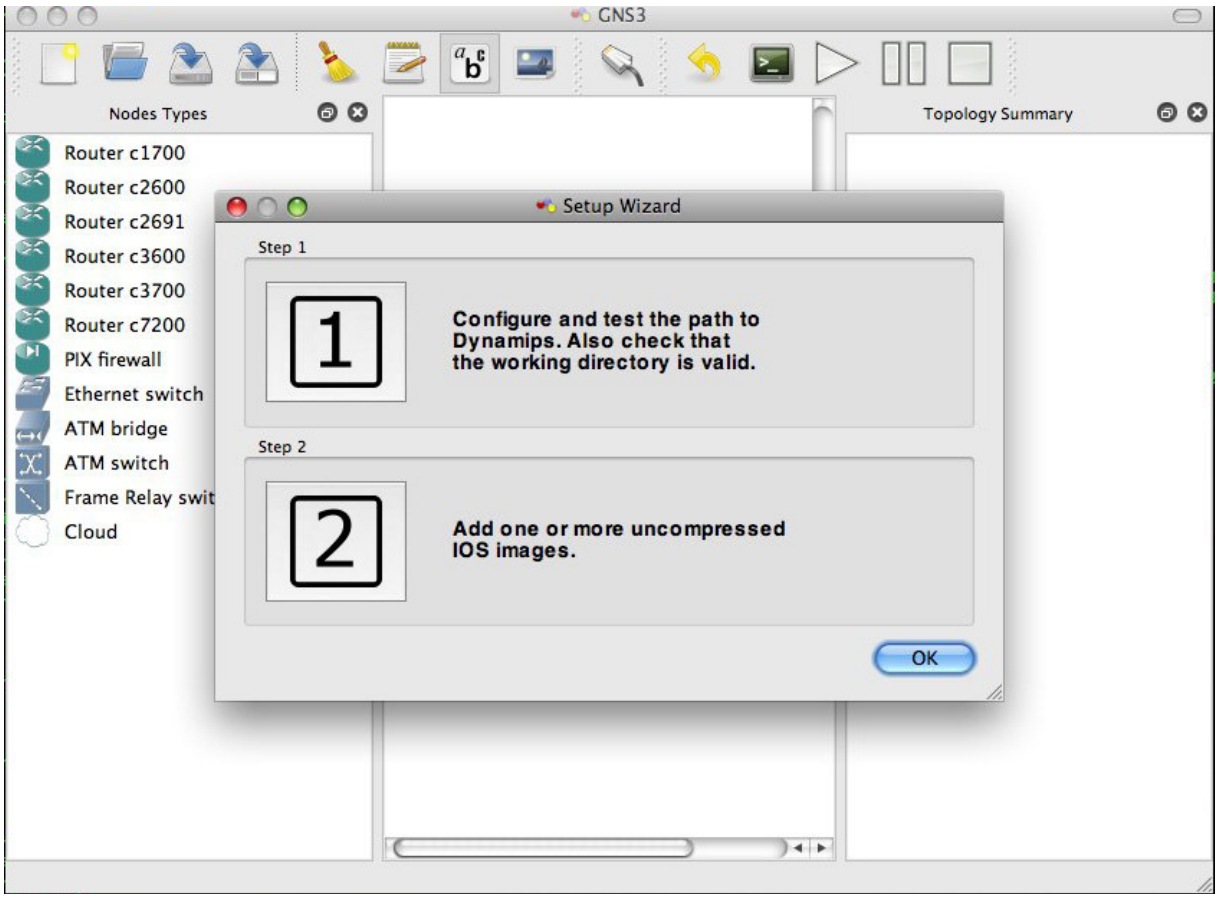

Figura 6 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho2012.

Esta tela mostra a configuração Dynamips, basta configurar o caminho correto do simulador e testar.

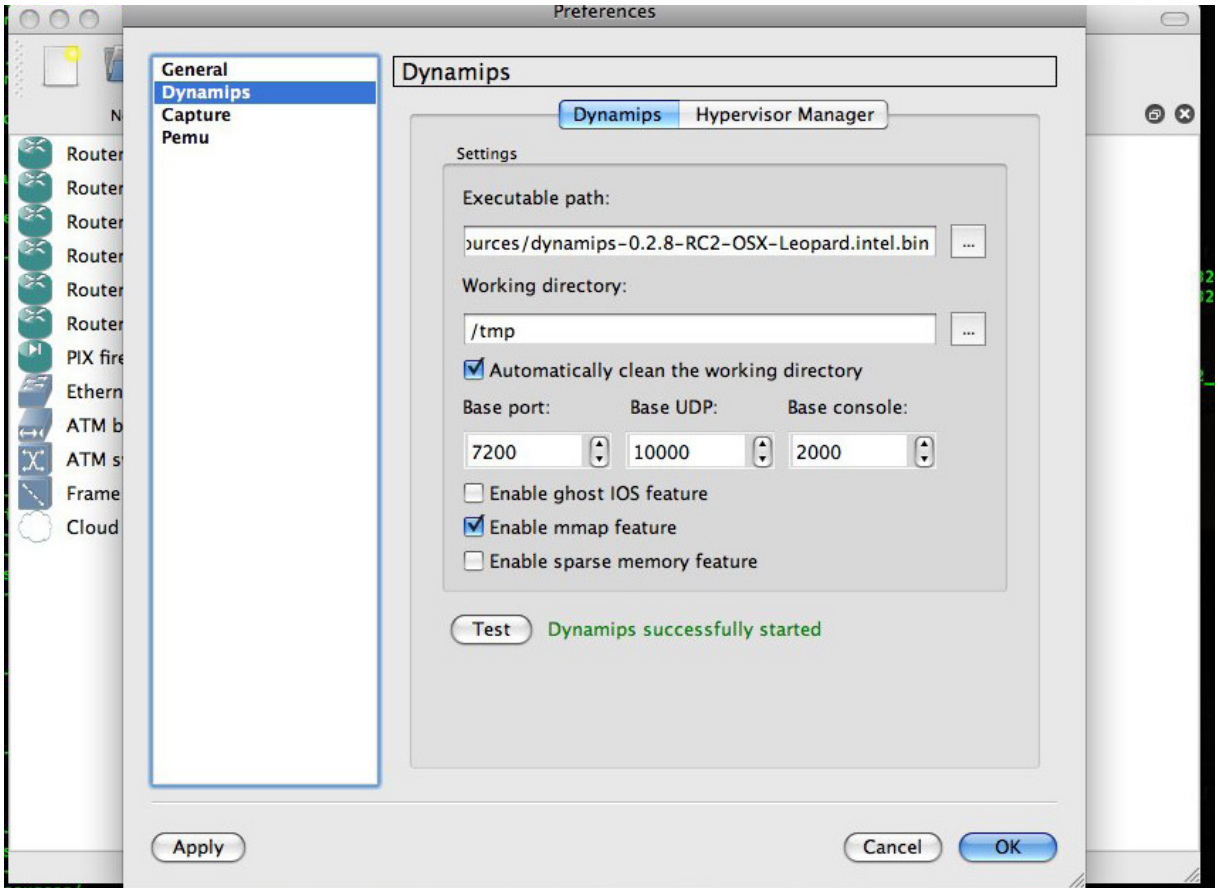

Figura 7 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Na tela abaixo basta escolher as imagem dos roteadores para fazer o teste.

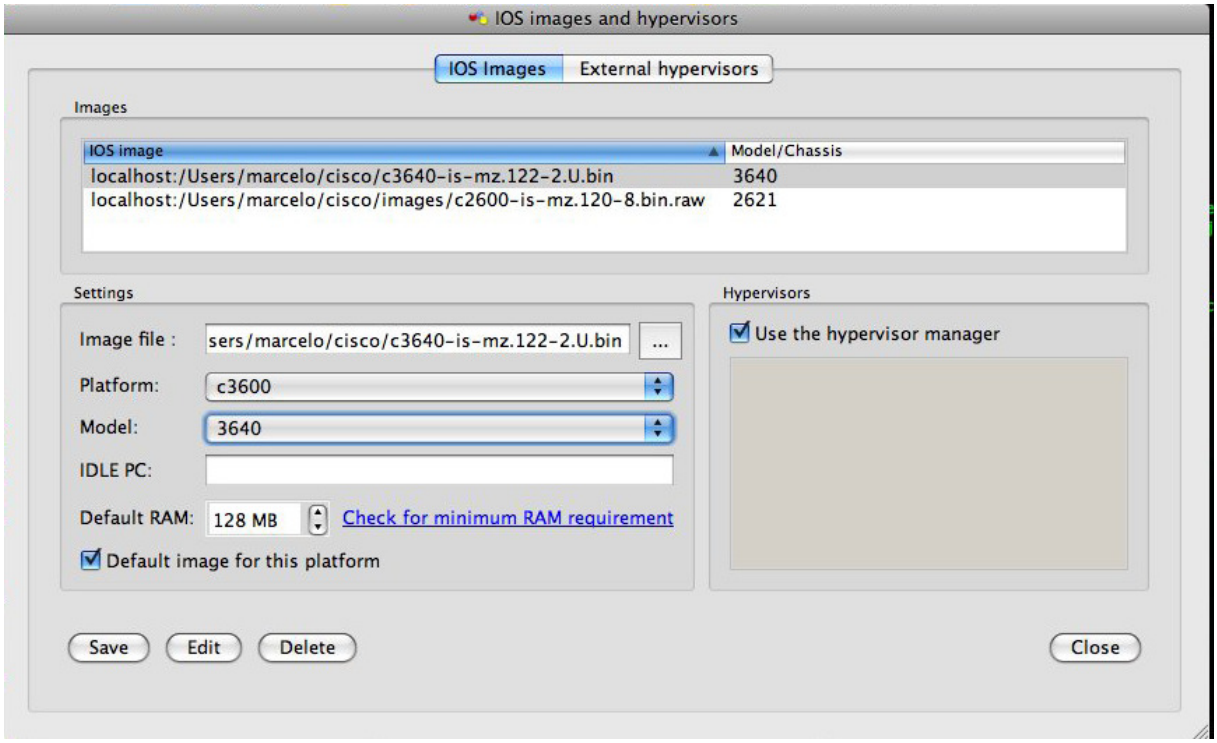

Figura 8 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Neste caso, temos dois diferentes equipamentos, o modelo 2610 com processador PowerPC e o modelo 3640 com processador MIPS, cada um utilizando sua respectiva imagem do IOS.

10.1.3 Simulador

Para simular uma rede simples de dois equipamentos, adicionamos os equipamentos clicando e arrastando, começando com os modelos 2610 e 3640.

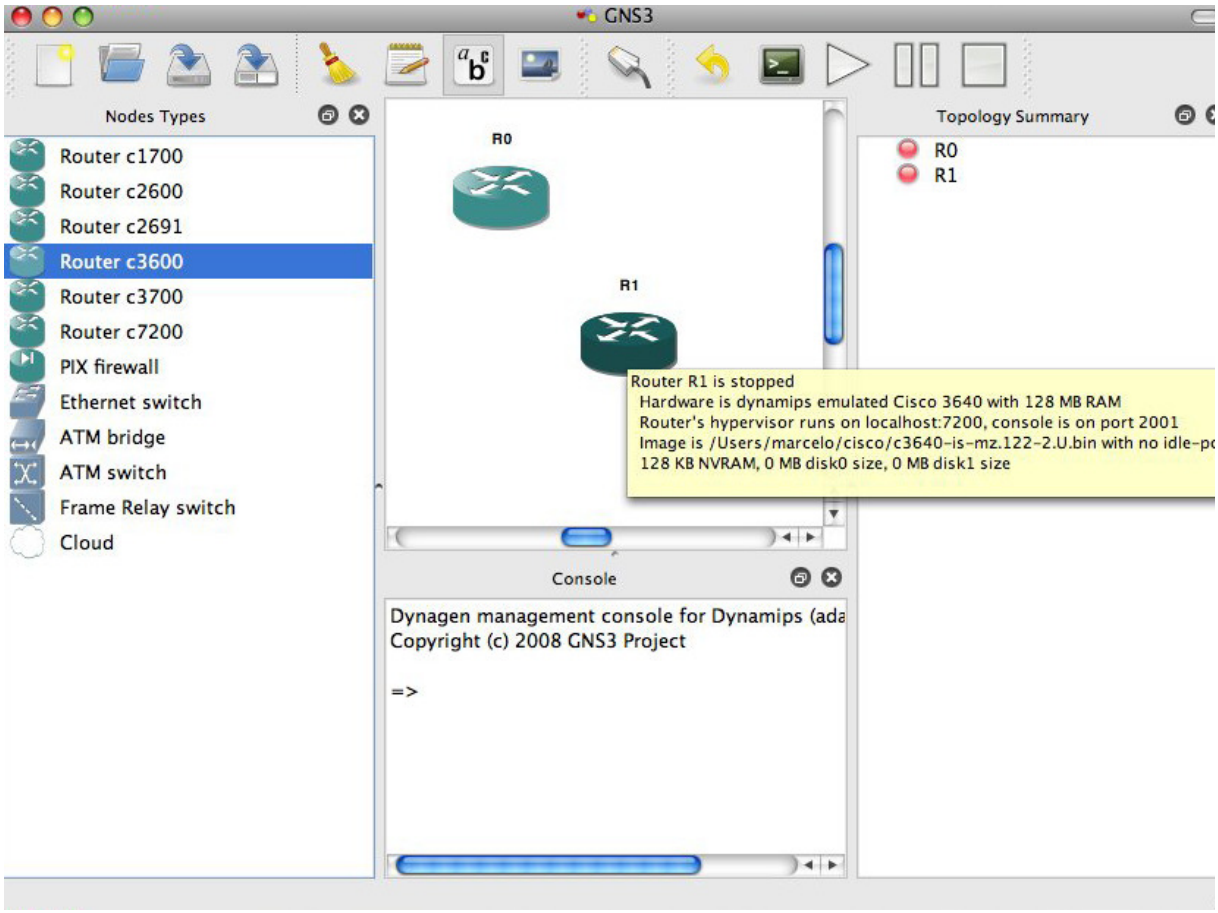

Figura 9 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Agora vamos utilizar a ferramenta de conexão é possível escolher uma série de tipos diferentes de conexões físicas para os equipamentos, nesta simulação vamos escolher a serial.

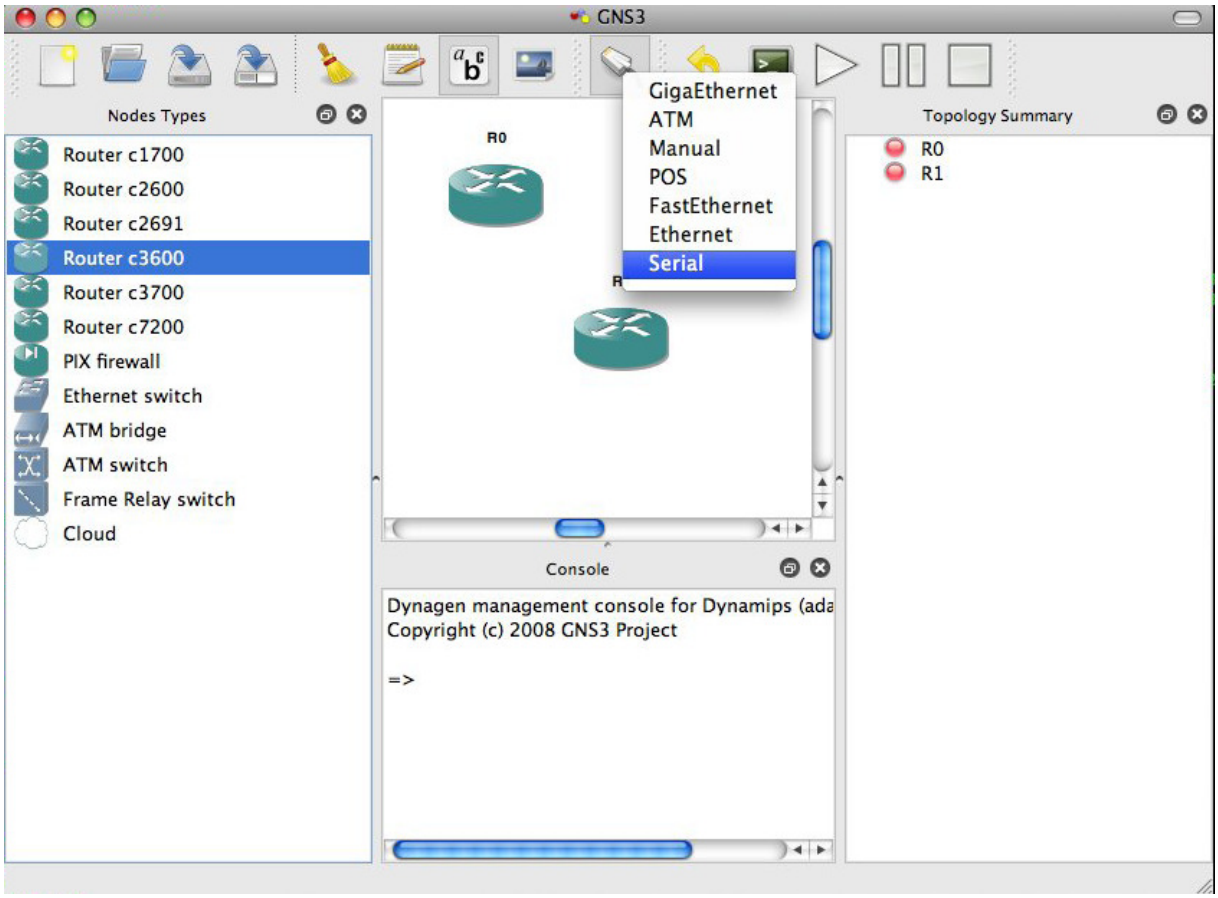

Figura 10 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Na tela abaixo temos que clicar na ferramenta **start** e então em **console**, é possível iniciar a simulação e visualizar os dois roteadores botando, porém ainda é necessário um ajuste adicional.

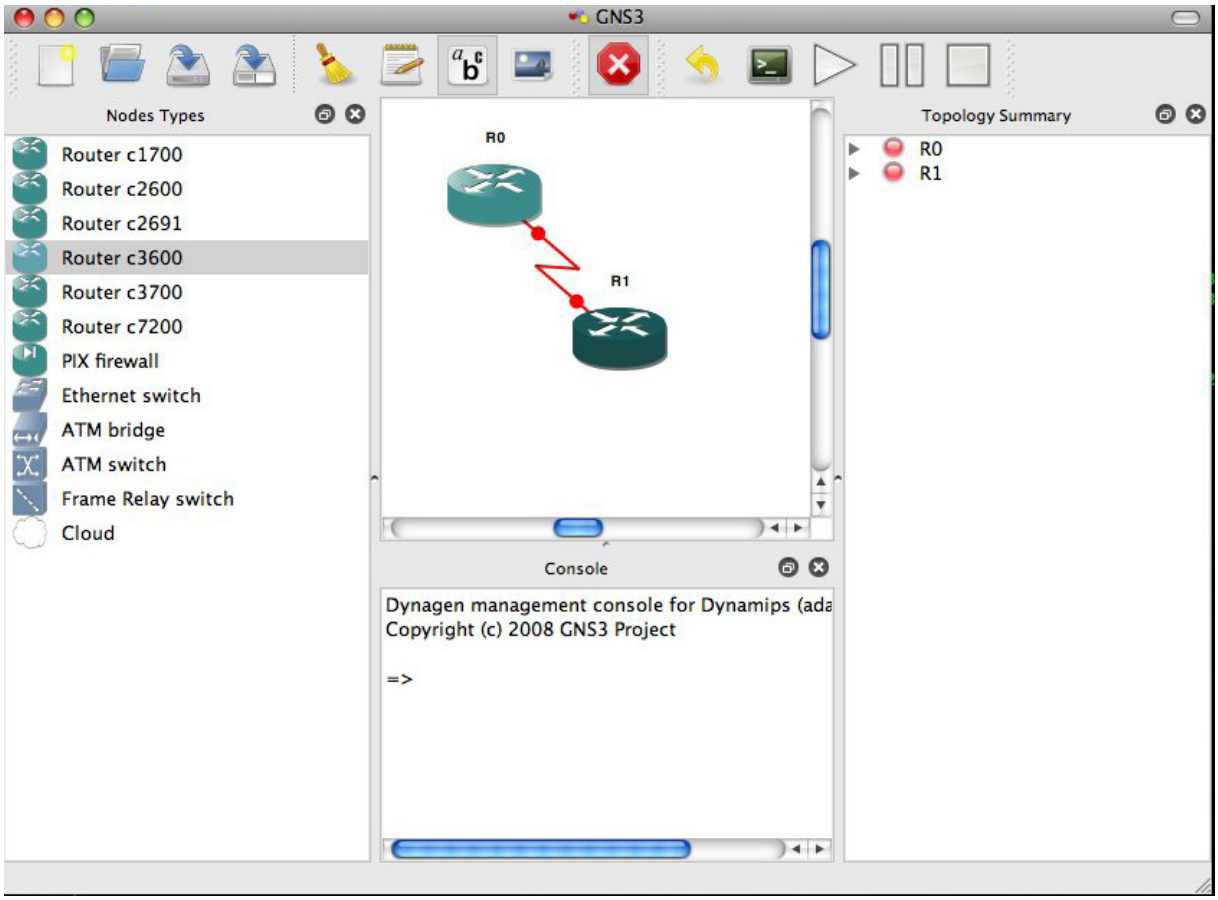

Figura 11 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Para aperfeiçoar a desempenho da simulação e evitar o consumo excessivo do processador hospedeiro, é necessário selecionar em cada roteador a opção “Idle PC”.

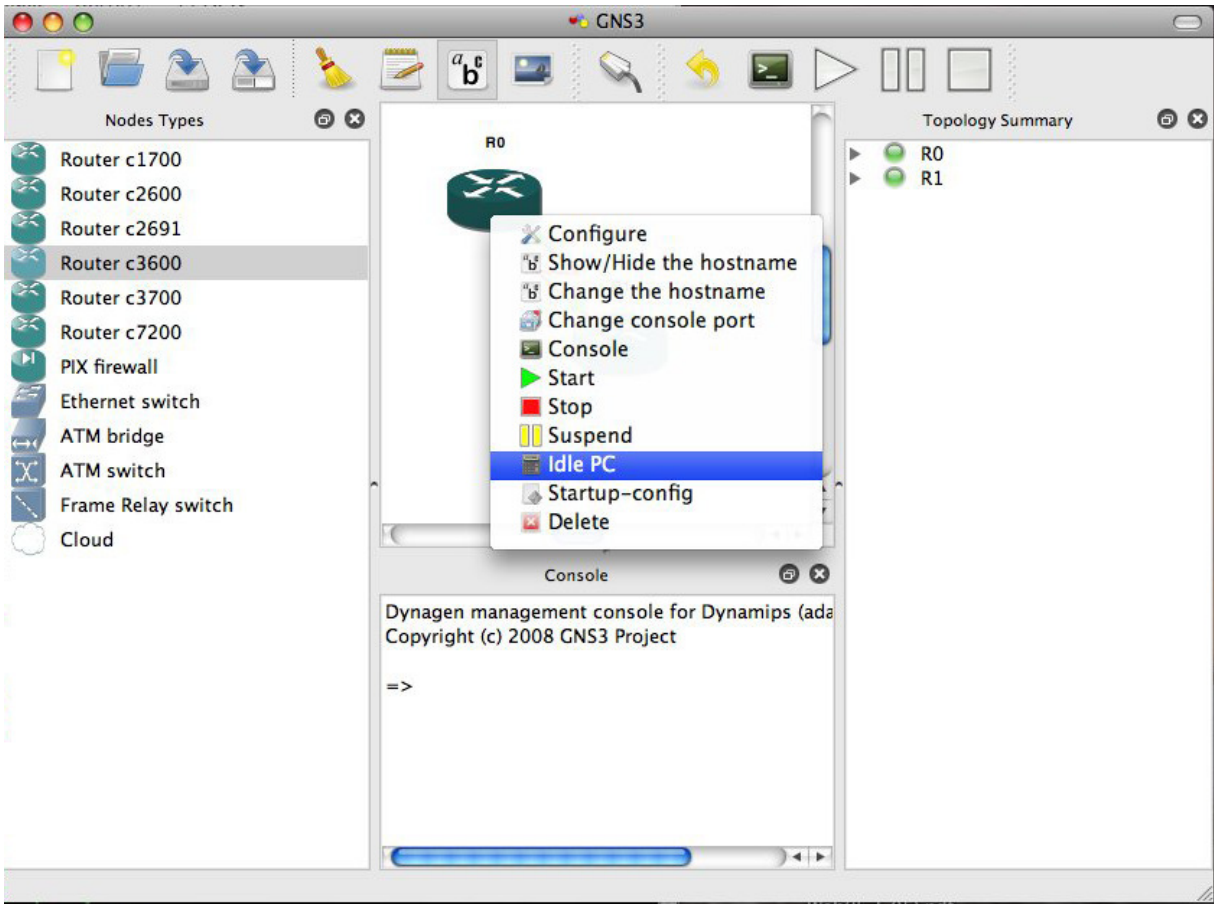

Figura 12 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Neste caso, o Dynamips determinou que o endereço indicado abaixo fosse um dos diversos pontos de idle do roteador, ou seja, um ponto onde o simulador vai escalonar para outra thread, maximizando a desempenho da simulação.

Na tela abaixo os roteadores estão ligado de ponto a ponto só aguardando as configurações.

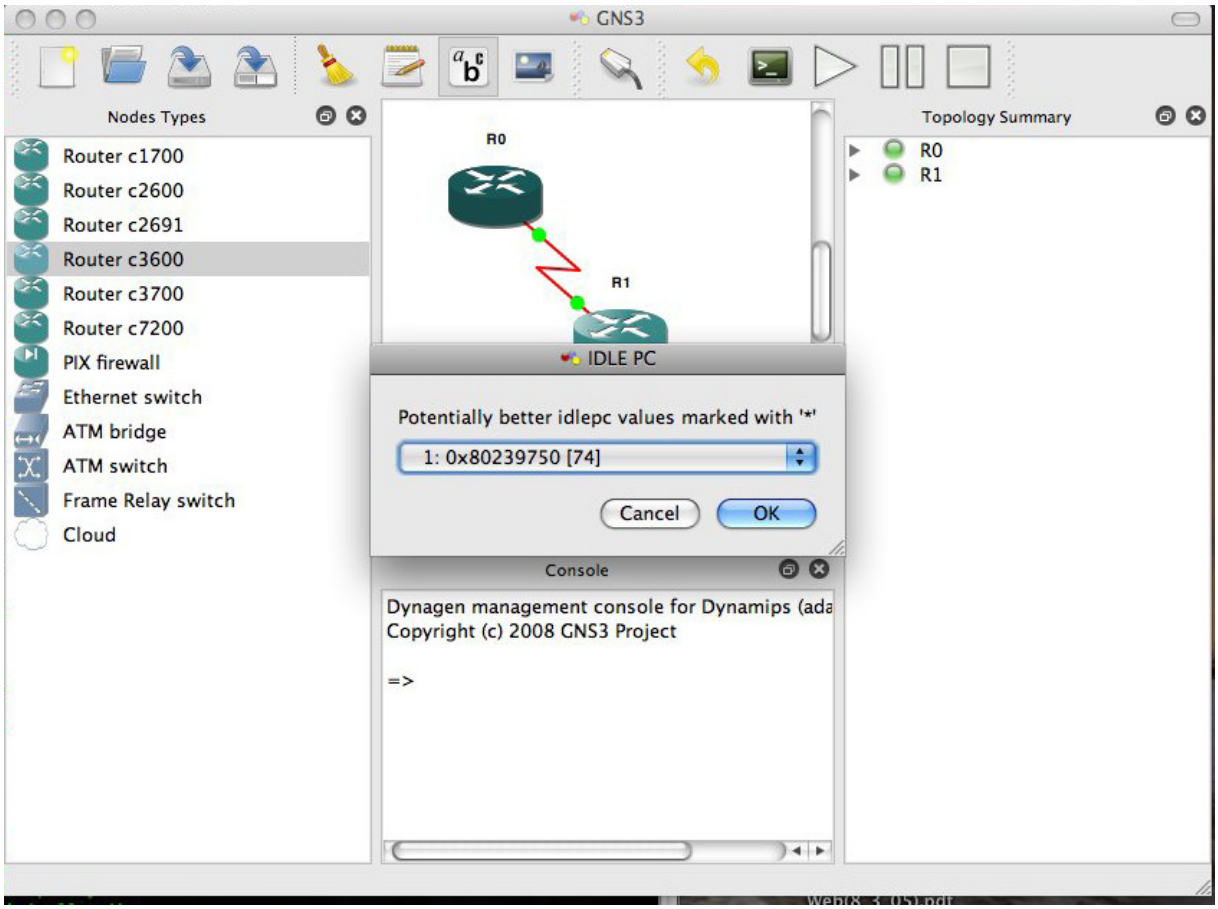

Figura 13 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Neste momento os roteadores podem ser configurados, bastante digitar “no” para o menu de configuração inicial e teclar enter para cair no prompt de comando. Para configurar as interfaces.

Roteador 2610.

```
Enable
Configure terminal
Interface serial 0/0
Ip address 192.168.0.1 255.255.255.0
Clock rete 64000
No shutdwon
^z
wr
shiw interface serial
```

Figura 14 – Exemplo da configuração do roteador 2610.(Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Roteador 3640.

```
Enable
Configure terminal
Interface serial 0/0
Ip address 192.168.0.2 255.255.255.0
No shutdown
^Z
Wr
Show interface serial 0/0
```

Figura 15 – Exemplo da configuração do roteador 3640. (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Aqui veremos a execução dos roteadores no prompt comando.

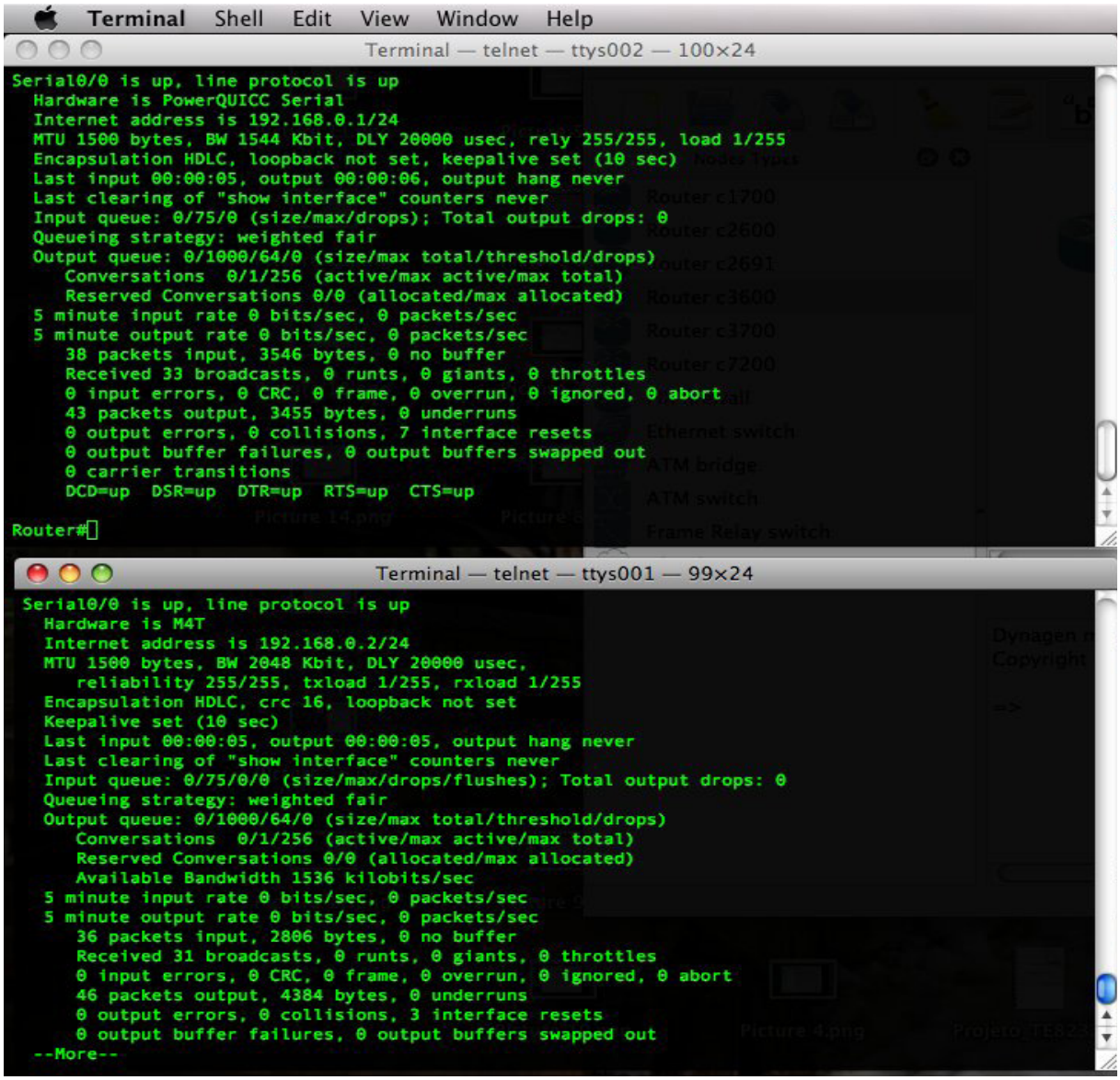

Figura 16 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Quando observamos a serial up e o protocolo up, temos indicação que as interfaces seriais síncronas estão devidamente conectadas e operando com protocolo HDLC (default para interfaces seriais da Cisco), com um clock de 64kHz fornecido pelo 2610. Em condições reais ambos os roteadores estarão conectados à uma operadora de longa distância, de modo que o clock será fornecido pela operadora e será síncrono com a rede TDM da operadora.

Uma vez configurado, o roteador irá manter sua a configuração no GNS3, podendo ser desligado e ligado quantas vezes for necessário.

E com esse software de simulação GNS3 que será feita a demonstração do trabalho.

11 – Firewalls de Borda

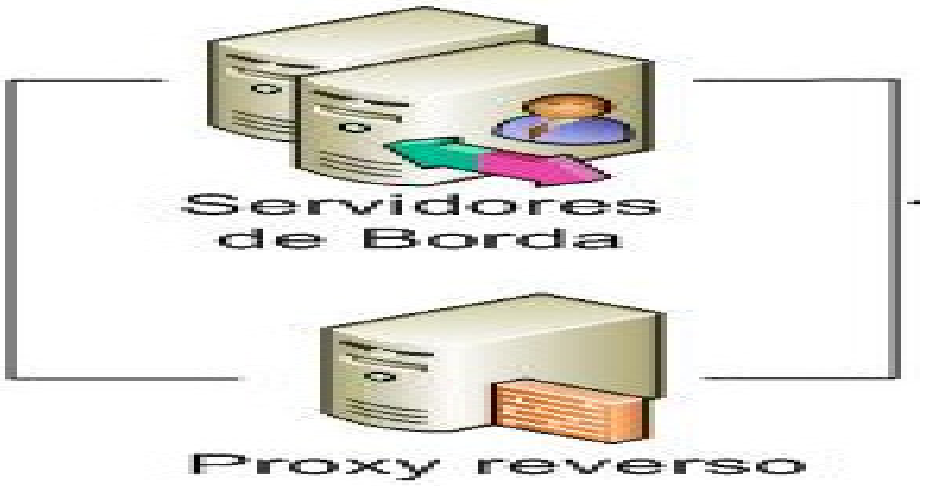

Figura 17 (Retirado de: **Firewall de Borda** ”http://www.tixperts.com.br/produtos/firewall”), Ultimo acesso em: 20 Março 2012.

O Firewall de Borda é um sistema desenvolvido que controla os tráfegos entre redes de computadores com diferentes níveis de confiança, como por exemplo, a rede Internet (zona não confiável), a rede de servidores (zona desmilitarizada), e a rede interna de uma empresa (zona confiável). (Retirado de: **Firewall de Borda** ”http://www.tixperts.com.br/produtos/firewall”), Ultimo acesso em: 20 Março 2012.

12 – Conclusão

Com o este trabalho é possível concluir que uma política de segurança aplicada ao firewall borda e roteador Cisco PIX security appliance, não é apenas a programação do bloqueio de portas e serviços, mas sim um conjunto de regras e recursos que devem ser cuidadosamente ativados para manter uma rede com segurança sem desperdiçar desempenho e garantindo a integridade das informações.

Para estabelecer as políticas de segurança em um firewall, será necessário analisar quais os tipos de informação que trafegam pela rede, e preferencialmente bloquear tudo o que não for apropriado para o tráfego da mesma, assim não estarão sendo desperdiçados recursos que devem ser utilizados para o propósito da organização.

Pode-se concluir também que firewall borda e roteador Cisco PIX security appliance, alvo do trabalho apresentado, é uma solução bastante completa, que possui um número elevado de recursos e funções, os quais têm como objetivo principal fornecer segurança para a rede sem limitar os serviços que ela pode oferecer.

Pois o roteador Cisco PIX atua desde a camada de rede até a camada de aplicação, é uma solução que pode ser utilizada em qualquer tipo de rede, desde que a mesma trabalhe sobre a pilha do Protocolo TCP/IP.

Entretanto, o roteador Cisco PIX security appliance não é uma solução gratuita, pois o roteador PIX tem um valor bem elevado o que se torna um de seu único problema apesar de ser uma ferramenta cara, ela é muito utilizado no mundo corporativo as empresas tem atualizado o seu recurso de segurança de redes, e como esta ferramenta é de extrema importância para que a mesma possa proteger seus dados.

O roteador Cisco PIX não é difícil de ser configurado e gerenciado, mesmo porque, possui uma interface gráfica voltada para navegadores que propõe a administração de suas funções sem a necessidade de acessar o modo shell do sistema, pois o roteador tem o IOS, e um sistema operacional da cisco onde que é aplicada as configurações do roteador Cisco PIX.

Por fim, podemos observar que o roteador Cisco PIX security appliance e o Firewall de borda é uma solução para redes que dependem de segurança, e que não possuem tempo para desperdiçar em implantações de diversos firewalls sem ter garantia de serviço, pois o roteador Cisco PIX security appliance e Firewall de borda já possui diversos recursos de segurança habilitados por padrão e além de ser uma ferramenta que garante a proteção da rede sem perder o desempenho e funcionalidades, possui suporte completo fornecido pela Cisco Systems.

13 – Referências Bibliográficas

DEAL A. Richard. **Cisco Router Firewall Security**. Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA 2004.

Firewall de Borda <"http://www.tixperts.com.br/produtos/firewall"> Acessado em: 20 Março 2012.

Cisco PIX 525 Security Appliance <"http://www.enfon.com/cisco-pix525-datasheet.pdf.">. Acessado em: 20 Março 2012.

CAMY, Alexandre Rosa; SILVA, Evandro R.N.;RIGUI, Rafael. **Seminário de firewalls.** 2003. 27 f. Seminário – Curso de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis.

EQUIPE CONECTIVA. **Segurança de redes:** firewall. [Curitiba] Conectiva S.A.; 2001.

MORAES P. S. M. Alexandre, **Cisco Firewalls,** Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA 2011.

MANSON G. Andrew; NEWCOMB J. Mark, **Cisco Secure Internet Security Solutions**, Cisco Press 201 West 103RD Street Indianapolis, 46290 USA 2001.

PRODUNET. **Soluções em TI,** <"http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1">, Ultimo acesso em 01 Dezembro 2012.

Segurança de Redes <http://www.eba.com.br/content/segurança-de-redes-conceitos-basico-1>, Ultimo acesso em 01 Dezembro 2012.

Alexei, Simulador de Redes GNS3. 2011 disponível em: <"http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3"> (Ultimo acesso em 14 de junho 2012).

Figura 4 ("Retirado de: http://www.tfr.se/rutter/cisco/pix/pdf"), Ultimo acesso 16 de junho 2012.

Figura 5 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3) Ultimo acesso em 14 de junho 2012.

Figura 6 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho2012.

Figura 7 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Figura 8 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Figura 9 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Figura 10 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Figura 11 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Figura 12 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Figura 13 – Exemplo da configuração do roteador 2610. (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Figura 14 – Exemplo da configuração do roteador 3640. (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Figura 15 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Figura 16 (Retirado de: http://www.dltec.com.br/blog/cisco/simulador-de-redes-gns3), Ultimo acesso em 14 de junho 2012.

Figura 17 (Retirado de: **Firewall de Borda** "http://www.tixperts.com.br/produtos/firewall"), Ultimo acesso em: 20 Março 2012.