

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

ACESSO REMOTO A REDES LINUX COM FERRAMENTAS GRÁFICAS

ACESSO REMOTO A REDES LINUX COM FERRAMENTAS GRÁFICAS

Monografia apresentada ao curso de
Especialização em Redes de Computadores
da Faculdade Natalense para o
Desenvolvimento do Rio Grande do Norte
como requisito parcial para a obtenção do
título de Especialista em Redes de
Computadores. **Marcelo Ferreira de Araújo**

Orientador:

Aurílio Ferreira da Rocha Neto

**NATAL/RN
2007**

NATAL/RN
2007

LIGA MARCELO FERREIRA DE ARAÚJO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

ACESSO REMOTO A REDES LINUX COM FERRAMENTAS GRÁFICAS

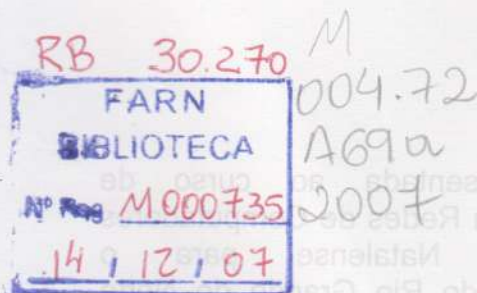
MARCELO FERREIRA DE ARAÚJO

Monografia apresentada ao curso de Especialização em Redes de Computadores da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito parcial para a obtenção do título de Especialista em Redes de Computadores.

Orientador:

Aluizio Ferreira da Rocha Neto

NATAL/RN
2007



Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Araújo, Marcelo Ferreira de
Acesso remoto a redes Linux com ferramentas gráficas / Marcelo Ferreira de
Araújo. – Natal: FARN, 2007.
46 f.

Orientador: Aluizio Ferreira da Rocha Neto (M. Sc.)
Monografia (Especialização em Redes de Computadores) – Faculdade
Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Redes de Computadores – Monografia. 2. Acesso Remoto – Monografia. 3.
Ferramentas de Acesso – Monografia. I. Título.

RN/FARN/BC

CDU 004.72

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

1	INTRODUÇÃO	10
1.1	PROBLEMA DE PESQUISA	10
1.2	OBJETIVOS	11
1.2.1	Objetivos Gerais	11
1.2.2	Objetivos Específicos	11
2	REFERENCIAL TEÓRICO	13
2.1	ACESSO REMOTO A REDES LINUX COM FERRAMENTAS GRÁFICAS	13
2.2	ESTRUTURA BÁSICA DAS FERRAMENTAS DE ACESSO REMOTO	13
2.2.1	PROTÓCOLOS DE ACESSO GRÁFICO EM REDE	13
2.2.2	PROTÓCOLO DE SEGURANÇA	14
2.3	AS FERRAMENTAS DE ACESSO REMOTO	15
2.3.1	TigerVNC	16
3	MARCELO FERREIRA DE ARAÚJO	21
3.1	METODOLOGIA	21
3.2	AS REDES	23
3.3	ESTAÇÕES DE TRABALHO	25
3.4	MONITORAMENTO DE REDES	27
3.5	CLUSTER	29
3.6	IMPLEMENTANDO O ACESSO REMOTO	37
4	ANÁLISE DE RESULTADOS	41
5	CONCLUSÃO	43
	REFERÊNCIAS BIBLIOGRÁFICAS	45
	BIBLIOGRAFIA CONSULTADA	47

Monografia apresentada e aprovada em 20 de julho de 2007, pela banca examinadora composta pelos seguintes membros.

Aluizio Ferreira da Rocha Neto, M.Sc.
Orientador

Gleydson Azevedo Ferreira de Lima, M.Sc.
Examinador

**NATAL/RN
2007**

SUMÁRIO

1	INTRODUÇÃO	10
1.1	PROBLEMA DE PESQUISA.....	10
1.2	OBJETIVOS.....	11
1.2.1	Objetivos Gerais.....	11
1.2.2	Objetivos Específicos.....	11
2	REFERENCIAL TEÓRICO	12
2.1	O QUE É ACESSO REMOTO, E PARA QUE SERVE ?	12
2.2	ESTRUTURA BÁSICA DAS FERRAMENTAS DE ACESSO REMOTO.....	12
2.2.1	PROTOCOLOS DE ACESSO GRÁFICO EM REDE	12
2.2.2	PROTOCOLO DE SEGURANÇA.....	14
2.3	AS FERRAMENTAS DE ACESSO REMOTO.....	15
2.3.1	TightVNC.....	16
3	DESENVOLVIMENTO	21
3.1	METODOLOGIA	21
3.2	AS REDES	22
3.3	ESTAÇÕES DE TRABALHOS	25
3.4	SERVIDOR - PORTAL.....	27
3.5	CLUSTER.....	29
3.6	IMPLEMENTANDO O ACESSO REMOTO.....	37
4	ANÁLISE DE RESULTADOS	43
5	CONCLUSÃO	45
	REFERÊNCIAS BIBLIOGRÁFICAS.....	46
	BIBLIOGRAFIA CONSULTADA.....	47
	Figura 24: Tela de Configuração NX Cliente opção de segurança.....	40
	Figura 25: Tela de configuração do servidor NX definição de porta e chave pública.....	40
	Figura 26: Tela de importação no CLIENTE da chave pública do SERVIDOR.....	41
	Figura 27: Tela inicial do CLIENTE NX para acesso ao SERVIDOR.....	41

LISTA DE FIGURAS

Figura 1: Estrutura básica das ferramentas de acesso remoto	12
Figura 2: Funcionamento do protocolo XDMCP remotamente	13
Figura 3: Exemplo de conexão SSH – Fonte: Technical Papel – SSH mais seguro	15
Figura 4: Resumo comparativo entre ferramentas de acesso remoto	16
Figura 5: Tela de opções do cliente TightVNC.....	17
Figura 6: Modelo CLIENTE/SERVIDOR – FreeNX	19
Figura 7: Modelo adotado por outros sistemas	19
Figura 8: Modelo utilizado pelo FreeNX	20
Figura 9: Estrutura compatível com outros sistemas (Tecnologia NX)	20
Figura 10: Estrutura Existente da Intranet – MATRIZ	21
Figura 11: Planta Baixa Flamoil Serviços.....	23
Figura 12: Tela de configuração <i>cable router</i>	24
Figura 13: Estrutura Implementada.....	25
Figura 14: Tela do software que alterna as redes	25
Figura 15: Pacote capturado pelo Ethereal.....	26
Figura 16: Log do Servidor PORTAL.....	28
Figura 17: Clusters Linux – Flamoil Serviços – MATRIZ	30
Figura 18: Tela de configuração do PVM com respectivas opções	33
Figura 19: Interface gráfica do OpenPBS – Gerenciamento dos NÓS	34
Figura 20: Tela de gerenciamento das filas no OpenPBS	35
Figura 21: Interface WEB para exibição das métricas monitoradas	36
Figura 22: Tela inicial do TightVNC Cliente.....	38
Figura 23: Tela de configuração inicial do NX Cliente	39
Figura 24: Tela de Configuração NX Cliente opção de segurança	40
Figura 25: Tela de configuração do servidor NX definição de porta e chave pública.....	40
Figura 26: Tela de importação no CLIENTE da chave pública do SERVIDOR.....	41
Figura 27: Tela inicial do CLIENTE NX para acesso ao SERVIDOR.....	41

LISTA DE TABELAS

Tabela 1: Relação de Equipamentos e Serviços.....	21
Tabela 2: Atividades a serem realizadas	23
Tabela 3: Resumo comparativo TightVNCE FreeNX.....	44

Palavras-chave: Acesso remoto, TightVNC e FreeNX.

RESUMO

Este trabalho tem por objetivo analisar uma estrutura de acesso remoto entre a matriz e a filial da empresa Flamoil Serviços Ltda, a qual cria um ambiente fácil e seguro que permite um usuário geograficamente distante acessar o centro de processamento de dados e executar tarefas remotamente. Para isso foram testadas algumas ferramentas como TightVNC (*Virtual Network Computing*) e FreeNX. Através destas o usuário pode ter acesso a interface gráfica (GUI) de outro computador e utilizar as suas funcionalidades visuais. Essas aplicações fornecem os recursos necessários para acessar remotamente da filial os recursos disponíveis na matriz. Também foram analisadas modificações na estrutura existente a fim de prover a segurança e qualidade desejável.

Palavras-chave: Acesso remoto, TightVNC e FreeNX.

Key-words: Remote Access, TightVNC and FreeNX.

ABSTRACT

This work analyzes a structure of remote access between the matrix and the branch office of the Flamoil company Ltda Services, which create an easy and safe environment that allows a remote user to have access the data processing center and to execute tasks remotely. For this some tools had been tested as TightVNC (Virtual Network Computing) and FreeNX. Through these the user can have access the graphical user interface (GUI) of another computer and use its visual functionalities. These applications supply the resources necessary to the branch office remotely have access the available resources in the matrix. Also modifications in the existing structure had been analyzed in order to provide the security and desirable quality.

Key-words: Remote Access, TightVNC and FreeNX

1.1 PROBLEMA DE PESQUISA

Da necessidade de uma melhor interação com os clientes, visto que em sua maioria encontram-se geograficamente distantes, e pretendendo eliminar tal barreira imposta pela localização, a empresa foz do projeto resolveu criar uma filial no estado do Rio de Janeiro.

Baseado nessas características se dividiu o projeto em duas fases, a primeira que consiste no estudo, reformulação e implementação das necessidades levantadas na matriz e a segunda fase composta pelo estudo, projeto e criação da filial.

1 INTRODUÇÃO

O avanço tecnológico ocorrido nos últimos anos nas Telecomunicações adveio da necessidade primordial do homem em se comunicar, e transmitir informações em um número cada vez maior, em uma velocidade cada vez maior, utilizando vários meios de transmissão.

A evolução da informática, e o surgimento das redes de computadores, bem como as novas tecnologias que surgem nesses padrões de redes estão facilitando imensamente a troca de informações entre as organizações e a possibilidade de colaboração entre as pessoas, em modos síncronos ou assíncronos. Hoje a localização geográfica deixou de ser um problema, com advento das inter-redes entre outras ferramentas de comunicação.

As empresas cada dia mais estão se posicionando em locais, próximos da matéria-prima, ou até em locais onde se tem menor custo para manter suas atividades comerciais. Porém criam pequenos escritórios em locais estratégicos para que seja possível interagir da melhor maneira com seus clientes.

Tais facilidades, alcançadas pode-se dizer que estão diretamente ligadas ao desenvolvimento do mundo das Redes.

Este trabalho abordará um estudo de caso real, de uma dessas organizações que já faz uso de alguns dos recursos ofertados no mundo das redes de computadores. E agora pretende reformular a estrutura atual de forma e ampliar o uso de tais recursos, criando um ambiente totalmente seguro, e geograficamente distribuído, eliminando custos e encurtando distâncias.

1.1 PROBLEMA DE PESQUISA

Da necessidade de uma melhor interação com os clientes, visto que em sua maioria encontram-se geograficamente distantes, e pretendendo eliminar tal barreira imposta pela localização, a empresa foco do projeto resolveu criar uma filial no estado do Rio de Janeiro.

Baseado nessas características se dividiu o projeto em duas fases, a primeira que consiste no estudo, reformulação e implementação das necessidades levantadas na matriz e a segunda fase composta pelo estudo, projeto e criação da filial.

1.2 OBJETIVOS

1.2.1 Objetivos Gerais

Esse projeto tem a finalidade fazer um estudo, analisando e implementando na empresa Flamoil Serviços à estrutura de hardware, software e serviços necessários para interligar matriz-filial, sempre avaliando os critérios de segurança e custos envolvidos. O foco principal do projeto será testar e implementar recursos que possibilitem executar processamento de dados a longa distância.

1.2.2 Objetivos Específicos

- Adequar a estrutura atual da melhor forma possível para a criação da filial;
- Pesquisar qual a melhor solução custo/benefício oferecida em termos de links.
- Levantar as necessidades para servir a filial;
- Aplicar as correções necessárias;
- Melhorar qualidade dos serviços ofertados, para os usuários da rede interna;
- Testar ferramentas de acesso remoto;
- Avaliar custos envolvidos para manutenção da rede e sugerir alternativas;

• Protocolo de Acesso Gráfico em Rede;

A Figura 1 exibe estes componentes de um acesso remoto.



Figura 1: Ferramenta básica das ferramentas de acesso remoto.

1.2.1 Protocolos de acesso gráfico em rede

Existem vários protocolos que permitem o acesso a um ambiente gráfico remoto. Trata-se de implementações independentes das aplicações que transmitem imagens de um "desktop" virtual ou não.

2 REFERENCIAL TEÓRICO

2.1 ACESSO REMOTO

Existem algumas definições para acesso remoto, dentre algumas estão: Para Charles Boldwyn, Sean (2001), "É a capacidade de acessar um computador ou uma rede de um local distante".

O acesso remoto tornou-se de uso indispensável para as atividades de administração remota, processamento remoto e acesso a informações geograficamente distantes. Para Charles Boldwyn, Sean (2001), o uso do acesso remoto está "em corporações onde as pessoas necessitam acessar suas filiais, ou pessoas em viagem que necessitam acessar a rede corporativa".

2.2 ESTRUTURA DAS FERRAMENTAS DE ACESSO REMOTO

Várias ferramentas estão sendo utilizadas, basicamente a estrutura para essas ferramentas estarem aptas a funcionarem é composta por 3 itens:

- Aplicação Servidora;
- Aplicação Cliente;
- Protocolo de Acesso Gráfico em Rede;

A Figura 1 exibe estes componentes de um acesso remoto.

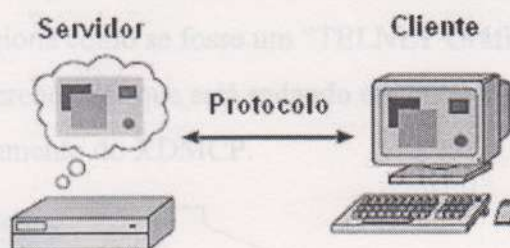


Figura 1: Estrutura básica das ferramentas de acesso remoto

2.2.1 Protocolos de acesso gráfico em rede

Existem vários protocolos que permitem o acesso a um ambiente gráfico remoto. Trata-se de implementações independentes das aplicações que transmitem imagens de um "desktop" virtual ou não.

O protocolo XDMCP (*The X Window Display Manager*), foi originado a partir do X11R3, esse protocolo faz uso da porta UDP 177. O X Server faz uma requisição para o gerenciador de janelas iniciar uma sessão enviando um pacote “*query*”. Se o gerenciador estiver habilitado a acessar o X Server, este responde enviando um pacote “*willing*”, e volta para o X Server. O X Server pode também enviar um pacote *BroadcastQuery* ou *IndirectQuery*, para iniciar uma sessão.

O gerenciador de janelas autentica-se no servidor, para fazer isso o X Server enviar um pacote “*request*” para o gerenciador de janelas, como retorno é enviado um pacote “*accept*”. Se o pacote “*accept*” tiver uma resposta esperada pelo X Server, o gerenciador de janela está autenticado. Produzindo uma resposta contendo uma chave secreta se a autenticação foi bem sucedida, o X Server enviar um pacote “*manage*” para informar quem é o gerenciador de janelas. Então o gerenciador de janela mostra a tela de login e se conecta ao X Server como um X Client.

Durante uma sessão, o servidor pode enviar pacotes *KeepAlive* para o gerenciador de janelas. Se o gerenciador falhar na resposta não enviando um pacote “*alive*” com um certo tempo. Então o servidor X presume que o gerenciado de janelas não está mais rodando e termina a conexão.

Um problema com o XDMCP é que ele é similar ao TELNET, a autenticação não é criptografada sendo possível capturar, colocando o sistema vulnerável a ataque.

O gerenciador de janelas, pode trabalhar localmente ou remotamente. Quando faz uso remotamente o XDMCP, funciona como se fosse um “TELNET Gráfico”, ou seja o protocolo se encarrega de conectar ao gerenciador que está rodando em outro computador. A Figura 2 mostra a estrutura de funcionamento do XDMCP.

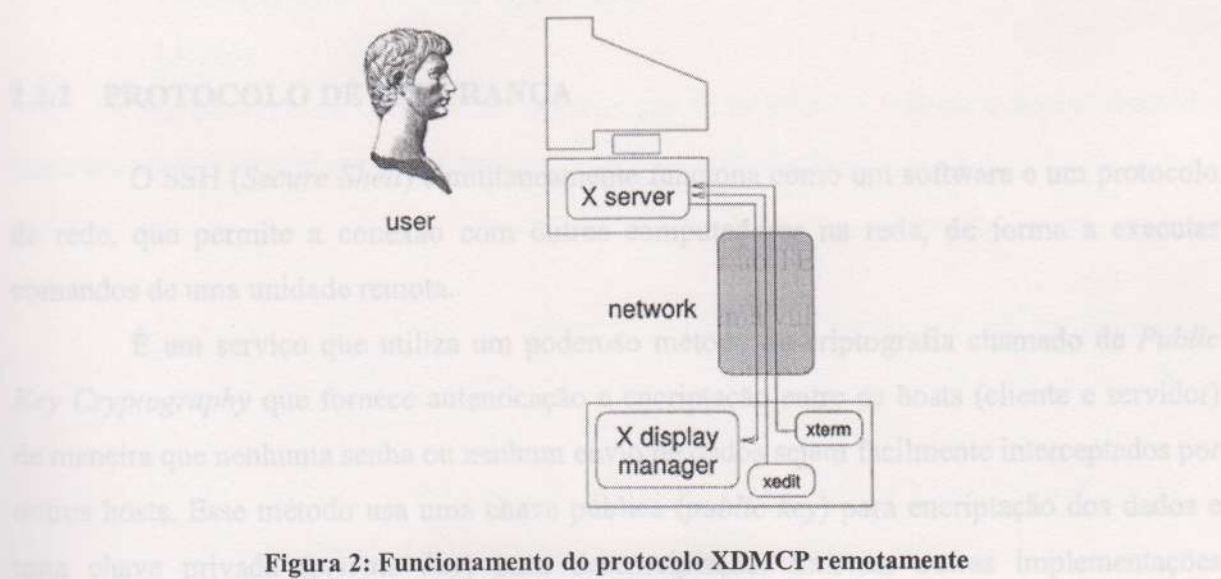


Figura 2: Funcionamento do protocolo XDMCP remotamente

Grande parte dessas ferramentas fazem uso do RFB (*Remote Framebuffer*) esse protocolo é descrito por Tristan Richardson e Kenneth R. Wood (1998), como “um simples protocolo para acesso remoto a interface gráfica do usuário”. Este protocolo pode ser usado em quaisquer sistemas que façam uso de janelas gráficas. Por ser um protocolo que funciona ao nível de “frame buffer”, ou seja, estes normalmente não enviam imagens completas do “desktop”, enviam apenas retângulos (“frames”) de atualização correspondente às partes que sofreram alteração.

O RFB é um protocolo simples que pode ou não ser mais elaborado. Tendo como principais características:

- Uma única primitiva de desenho é a colocação de uma imagem no ponto x,y do “monitor”.
- Controle de fluxo é realizado pelo cliente, o servidor não envia “frames” por iniciativa própria, apenas o faz a pedido do cliente. Este método tem a vantagem de produzir uma adaptação automática à capacidade do cliente e da rede (o cliente só pede uma atualização depois de processar a anterior).
- As respostas do servidor (“frames”) podem usar diversos formatos: “raw”; “RRE”; “coRRE”; “Hextile” e “Copy Rectangle”. Na prática os mais usados são os dois últimos.

O “Hextile” permite a melhor compressão para o tipo de imagens mais comuns nos “desktops” e o “Copy Rectangle” não é usado para enviar uma imagem, mas sim uma ordem de cópia do “framebuffer” do cliente para o seu “vídeo”.

2.2.2 PROTOCOLO DE SEGURANÇA

O SSH (*Secure Shell*) simultaneamente funciona como um software e um protocolo de rede, que permite a conexão com outros computadores na rede, de forma a executar comandos de uma unidade remota.

É um serviço que utiliza um poderoso método de criptografia chamado de *Public Key Cryptography* que fornece autenticação e encriptação entre os hosts (cliente e servidor) de maneira que nenhuma senha ou nenhum envio de dados sejam facilmente interceptados por outros hosts. Esse método usa uma chave pública (*public key*) para encriptação dos dados e uma chave privada (*private key*) para desencriptação. Existem outras implementações

baseadas no SSH, como SCP e o SFTP (*Secure File Transfer Protocol*), todos são protocolos de transferência de arquivos que utilizam criptografia. A Figura 3 mostra a troca de pacotes numa abertura de sessão SSH.

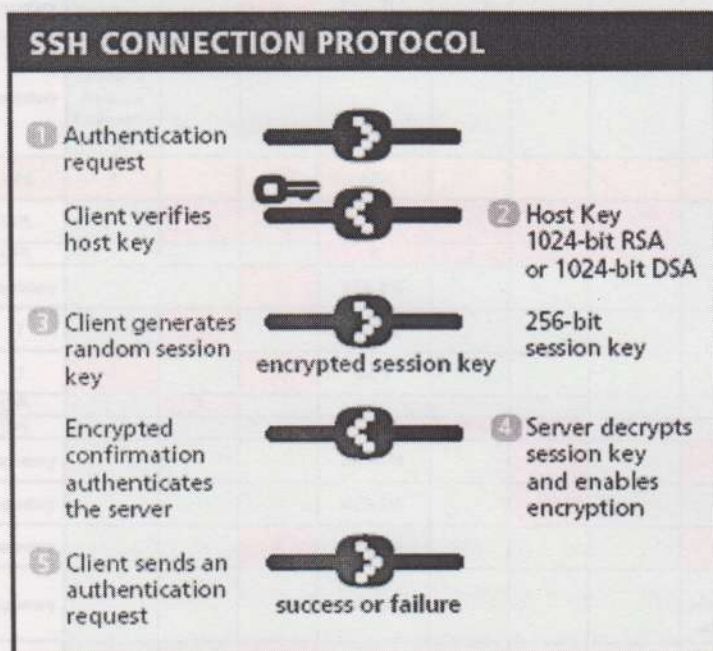


Figura 3: Exemplo de conexão SSH – Fonte: Technical Paper – SSH mais seguro

2.3 AS FERRAMENTAS DE ACESSO REMOTO

As ferramentas podem ser classificadas segundo os critérios abaixo:

- Protocolo
- Existência de Criptografia Nativa
- Portabilidade de Sistemas Operacionais
- Licença

A Figura 4 mostra diversas ferramentas que se propõem a realizar o acesso remoto e traça um comparativo elegendo as suas principais características.

2.3.1 TightVNC

O TightVNC é um projeto baseado no VNC (Virtual Networking Computing) que foi desenvolvido originalmente pela Olivetti & Oracle Research Lab. Em 1999, a AT&T adquiriu o laboratório que fechou logo em seguida em 2002.

O código aberto facilitou o surgimento de diversas implementações como o TightVNC. Porém a base do software, faz uso do protocolo RFB (Remote Frame Buffer).

Program	Protocol	License	Client	Server	Java Viewer	Native Encryption	File Transfer	Audio Support	Multiple Sessions	Linux	Mac	Windows
Desktop	VNC	Proprietary			X	AES-128		X		X		X
Chicken of the VNC	VNC	GPL		X	X	X	X	X	X	X		X
Citrix Presentation Server	RDP, ICA	Proprietary			X	SSL, TLS						
Elusiva	RDP	Proprietary	See 'Remote Desktop Connection' below								See 'Remote Desktop Connection' below	
FreeNX [1]	NX, RDP, RFB	GPL	X		X	AES					X	X
KRDC (KDE client)	RDP, VNC	GPL		X	X	X	X	X	X		X	X
MetaVNC	VNC	GPL				X	X	X	X		X	
NetOp Remote Control [2]	Proprietary	Proprietary			X	AES-256						
NX Client [3]	NX, RDP, RFB, VNC	?		X		Varies						
NX Server [4]	NX, RDP, RFB	?	X		X	AES					X	X
rdesktop	RDP	GPL		X								X
RealVNC Free	VNC	GPL				X	X	X			X	
RealVNC Personal	VNC	Proprietary				AES-128		X		X	X	
RealVNC Enterprise	VNC	Proprietary				AES-128		X				
Remote Administrator	Proprietary	Shareware			X	AES-256				X	X	
Remote Desktop Connection	RDP	Proprietary				Varies				See 'rdesktop' above		
Remote Graphics Software	Proprietary	Proprietary			X						X	
Sun Secure Global Desktop Software	AJP	Shareware				SSL, TLS (AES-256)						
TightVNC	VNC	GPL				X		X			X	
TurboVNC	VNC	GPL				X		X			Viewer only (X11)	
UltraVNC	VNC	GPL				With plugin		X		X	X	
Vine Server (OSXvnc)	VNC	GPL			X			X		X		X
XDMCP	X11	MIT			X	X	X					X
X11vnc	X11vnc	GPL	X		X	X		X				X

Figura 4: Resumo comparativo entre ferramentas de acesso remoto

Nesse trabalho foram escolhidas duas tecnologias para serem efetuados testes. São elas o FreeNX e o TightVNC. Ambas possuem licenças regidas nos termos GPL (*General Public License*) e versões disponíveis para Linux.

2.3.1 TightVNC

O TightVNC é um projeto baseado no VNC (Virtual Networking Computing) que foi desenvolvido originalmente pela Olivetti & Oracle Research Lab. Em 1999, a AT&T, adquiriu o laboratório que fechou logo em seguida em 2002.

O código aberto facilitou o surgimento de diversas implementações como a TightVNC. Porém a base do software, faz uso do protocolo RFB (Remote Frame Buffer).

Segundo Carlos E. Morimoto (2006)

TightVNCserver, é uma versão mais recente do VNC, que oferece um algoritmo de compressão mais eficiente. Ele que garante tempos de atualização de tela mais baixos (às custas de um pouco mais de processamento no cliente) e também suporte à compressão via JPG, que degrada a qualidade da imagem, em troca de uma redução considerável na banda utilizada, permitindo executar o VNC aceitavelmente mesmo numa conexão via modem.

O TightVNC também oferece algumas melhorias secundárias, como o suporte a scroll de tela usando a roda do mouse e processamento local do cursor do mouse. Para que estes recursos funcionem, é necessário que seja utilizado o TightVNC tanto no servidor quanto no cliente. Na ilustração temos o menu de opções oferecidas pelo cliente for Windows.

A segurança no TightVNC se limita à autenticação, segundo Carlos E. Morimoto (2004).

TightVNC utiliza uma chave de encriptação de mão única durante a autenticação, de forma que a senha não circula pela rede. Isso impede que alguém sniffando a rede consiga capturar sua senha do VNC como acontece no caso do Telnet por exemplo. Apesar disso, depois que a conexão é iniciada os dados são enviados de forma não encriptada, abrindo a possibilidade de que alguém capaz de capturar os pacotes transmitidos possa ver o que você está fazendo e até mesmo capturar as teclas digitadas no teclado.

A autenticação utiliza criptografia de mão única. A Figura 5 exibe a tela de configuração do TightVNC.

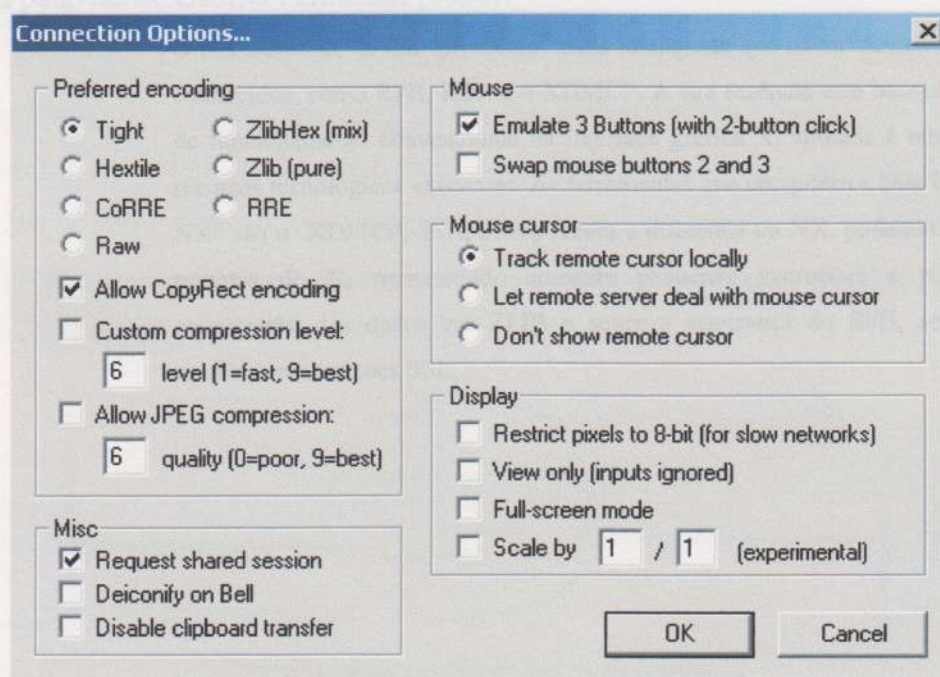


Figura 5: Tela de opções do cliente TightVNC

2.3.2 FreeNX

O projeto FreeNX, versão cliente, foi desenvolvido originalmente por *Joseph Wenniger* e *Torsten Rahn*. A versão servidor foi desenvolvida por *Fabian Franz* e *Kurt Pfeifle*. A realização deste projeto se deu devido a empresa NoMachine, que resolveu disponibilizar as bibliotecas como GPL.

A NoMachine já havia disponibilizado as bibliotecas desde 2003, mas já que ela tem seus aplicativos comerciais baseados nestes, todos ficaram confusos em relação aos direitos sobre o código. Assim entraram Fabian e o Kurt, que fizeram todo o servidor com mais ou menos 3000 linhas de código *shell script* e compatível com a maioria das distros *Linux*.

O funcionamento da ferramenta é descrita abaixo:

Ao invés de simplesmente tirar screenshots da tela e comprimir as imagens, como faz o VNC, ele abre uma seção remota do X (como ao usar o XDMCP), onde são transmitidas as instruções e pixmaps usados para montar a tela que será exibida no cliente. Estes dados são compactados usando um algoritmo próprio (mais eficiente que sistemas tradicionais de compressão de dados, como o Zlib) e encriptados usando o SSH, o que torna o FreeNX mais rápido e mais seguro que o VNC, tanto em links lentos (sobretudo conexões via ADSL ou modem) quanto em redes locais, onde banda não é problema.

Carlos E. Morimoto (2006).

Nas palavras de Gabriel Fernandes (2006):

O NX utiliza-se de um "protocolo" mais inteligente que os ambientes remotos mais conhecidos, como RFB, RDP e o XDMCP. A sua essência está baseada no método de funcionamento convencional da interface gráfica X, apoiada à um conjunto de recursos tecnológicos existentes. As ferramentas que compõem a base do "Protocolo NX" são o XDMCP, SSH, Proxy fazem a diferença no NX, podendo abrir sessões remotas do X, transmitindo somente pequenas instruções e pixmaps, com compressão dos dados em ZLIB e sobre a segurança do SSH, sendo possível estabelecer conexões SSL.



Figura 7: Modelo adotado por outros sistemas

A Figura 6 mostra um exemplo de uso do FreeNX entre clientes e um servidor.

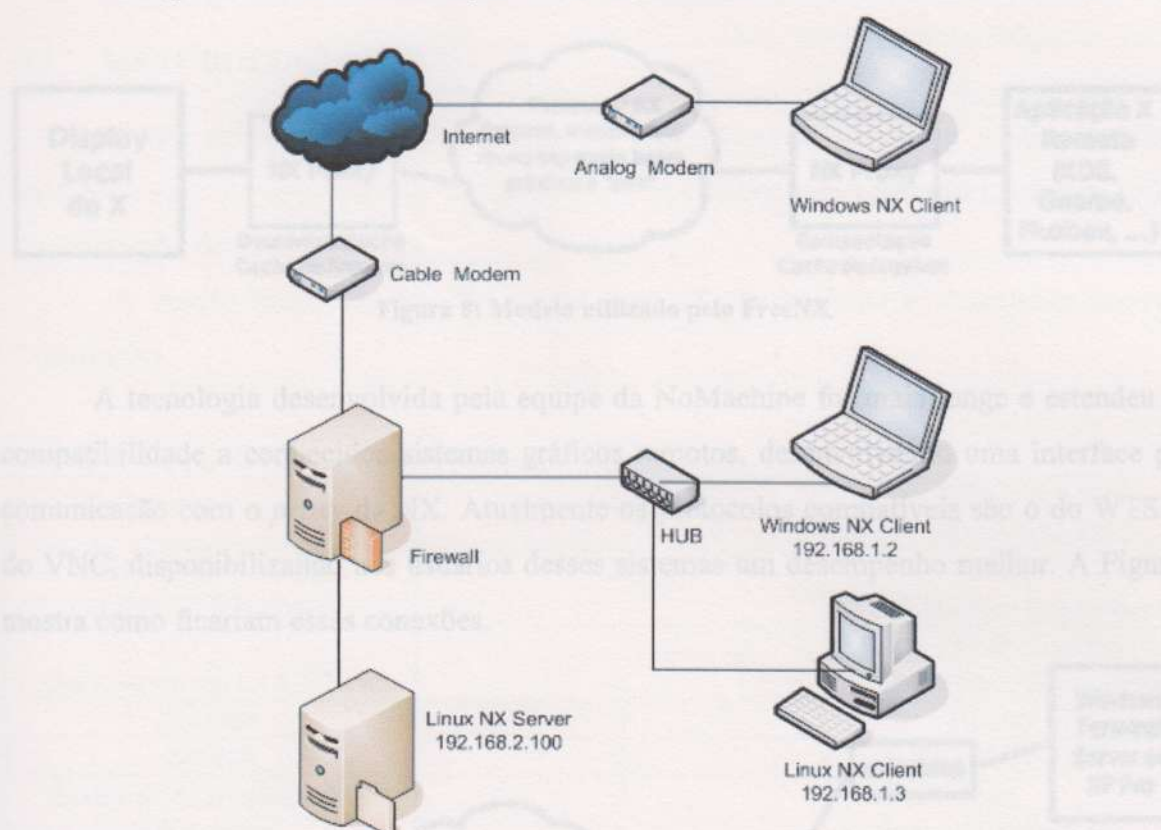


Figura 6: Modelo CLIENTE/SERVIDOR – FreeNX

O protocolo utilizado foi desenvolvido inicialmente pela NoMachine, e foi usado no FreeNX. O protocolo FreeNX, não pode ser considerado um único protocolo visto que ele é formado por um conjunto de diversos protocolos.

O diferencial do FreeNX, com relação aos outros protocolos, está por termos em cada ponta um sistema de *proxy* de arquivos, e aí está a grande sacada. O protocolo NX além de enviar somente as partes da tela que tiveram modificações, com o sistema de *cache* de arquivos que o *proxy* proporciona, quanto mais se navega melhor fica a performance, ao contrário de outros sistemas de conexão remota que sempre enviam *screenshots* da tela toda. As figuras 7 e 8 exemplificam este esquema.

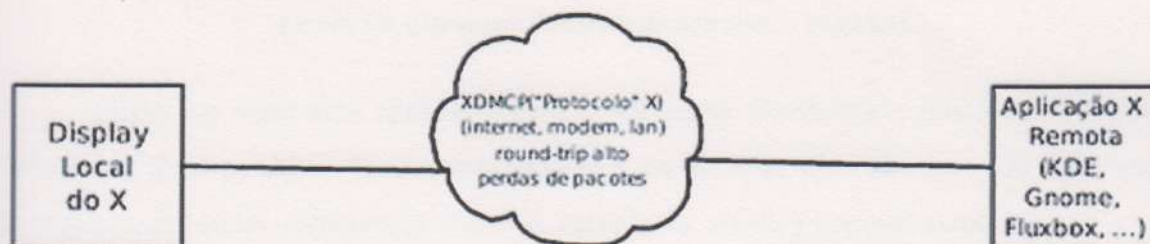


Figura 7: Modelo adotado por outros sistemas

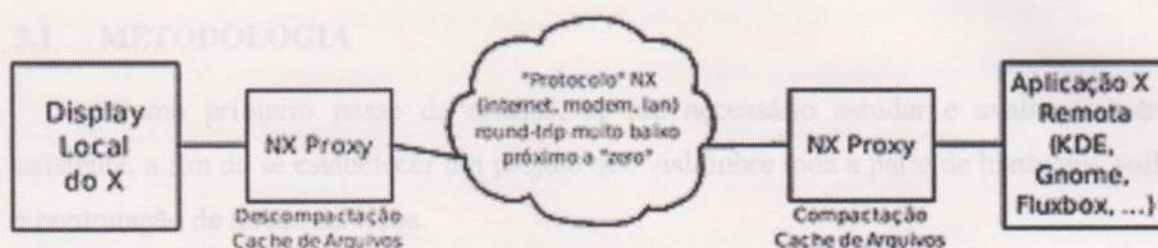


Figura 8: Modelo utilizado pelo FreeNX

A tecnologia desenvolvida pela equipe da NoMachine foi mais longe e estendeu sua compatibilidade a conhecidos sistemas gráficos remotos, desenvolvendo uma interface para comunicação com o *proxy* da NX. Atualmente os protocolos compatíveis são o do WTS e o do VNC, disponibilizando aos usuários desses sistemas um desempenho melhor. A Figura 9 mostra como ficariam essas conexões.

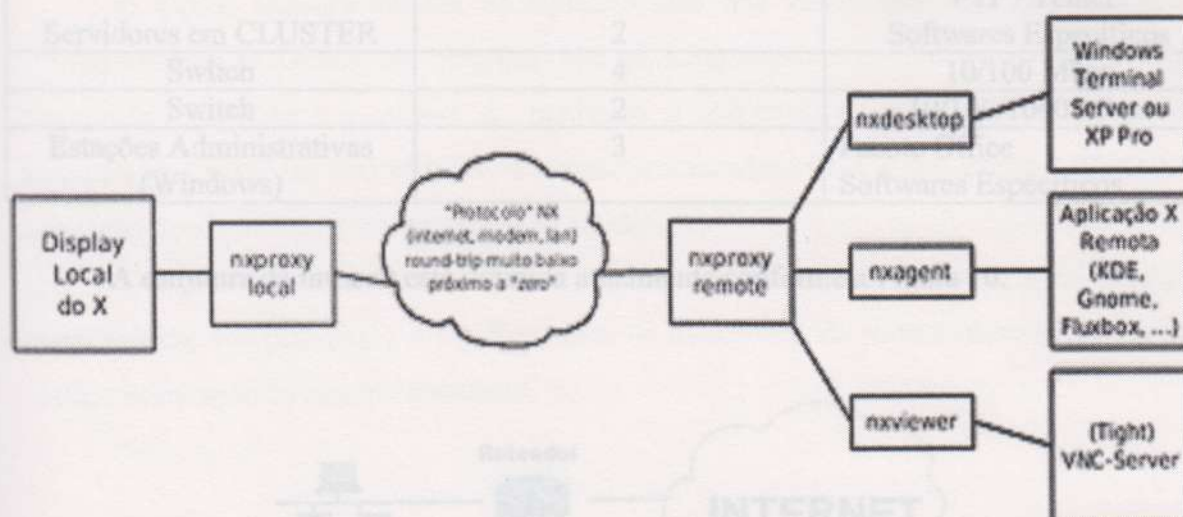


Figura 9: Estrutura compatível com outros sistemas (Tecnologia NX)

3 DESENVOLVIMENTO

3.1 METODOLOGIA

Como primeiro passo da análise, se faz necessário estudar e avaliar a estrutura existente, a fim de se estabelecer um projeto que vislumbre toda a parte de hardware, software e contratação de novos serviços.

A matriz localizada no RN, conta com 18 funcionários e o seguinte parque de informática:

Tabela 1: Relação de Equipamentos e Serviços

TIPO	QUANTIDADE	SERVIÇOS / SOFTWARES
Estações de Trabalho (LINUX/Windows)	22	Telnet / FTP Softwares Específicos
Servidores em CLUSTER	2	FTP / Telnet Softwares Específicos
Switch	4	10/100 Mbps
Switch	2	10/100/1000 Mbps
Estações Administrativas (Windows)	3	Pacote Office Softwares Específicos

A estrutura da intranet está definida atualmente conforme a Figura 10.

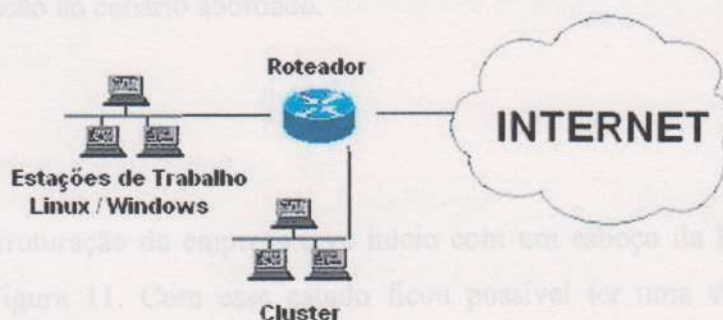


Figura 10: Estrutura Existente da Intranet – MATRIZ

Tendo em vista esse contato prévio, resolveu-se subdividir o projeto nos seguintes tópicos que abrange alguns itens que compõem a estrutura de TI (*Tecnologia da Informação*) da organização: redes, estações de trabalho, servidores, *clusters* e acesso remoto.

Tratando os itens por módulos, é possível atingir uma facilidade satisfatória no momento em que se fizer necessário identificar e solucionar os problemas.

O tópico *redes* trata de uma forma geral toda infra-estrutura da rede, incluído o cabeamento de lógica e os equipamentos de rede. A partir do estudo da estrutura existente, obteve-se como resultado um projeto da rede, e um cronograma para execução das melhorias necessárias e solução de problemas.

O tópico *estações de trabalho* abrange as máquinas que fazem uso de alguns dos serviços de rede, e servem como porta de entrada para os usuários da rede. Assim, é possível identificar os principais serviços utilizados pelos usuários e otimizar no que fosse possível, gerando principalmente soluções para problemas de segurança.

O tópico *servidores* foi criado em virtude de uma análise rápida da estrutura encontrada ao estudar a rede existente na empresa. Seria necessário incluir uma máquina com alguns serviços que possibilitasse o acesso externo a intranet, por usuários e clientes autorizados, ou seja, uma porta de entrada para a rede da empresa.

O tópico *clusters* detalha os equipamentos que são a base do CPD (*Centro de Processamento de Dados*) da empresa. Nesses equipamentos encontra-se o que existe de tecnologia de ponta em termos de hardware e software, e onde concentram todas as informações, advindas dos clientes, a serem processadas. Esse é um ponto importante na avaliação de alguma possível melhoria ou atualização.

O tópico *acesso remoto* trata da implementação das ferramentas de tal finalidade, testando duas das principais, a fim de avaliar os parâmetros de teste e obter a que apresente melhor adequação ao cenário abordado.

3.2 REDES

A reestruturação da empresa teve início com um esboço da Rede Elétrica e Lógica, conforme a Figura 11. Com esse estudo ficou possível ter uma visão geral da estrutura existente, identificando os possíveis pontos de falhas (retardo, taxa de erros, segurança e vulnerabilidades).

Substituição do Cabeamento para Categoria 6	Estações de TRABALHO (demais pontos)	55	SETEMBRO/07
---	--------------------------------------	----	-------------

O uso de equipamentos mistos *a priori* não causou grande impacto, pois o formato do quadro ethernet é o mesmo, não necessitando conversão por parte dos equipamentos. Isso dá uma tranquilidade para executar o cronograma descrito acima, sem causar impacto na estrutura da rede.

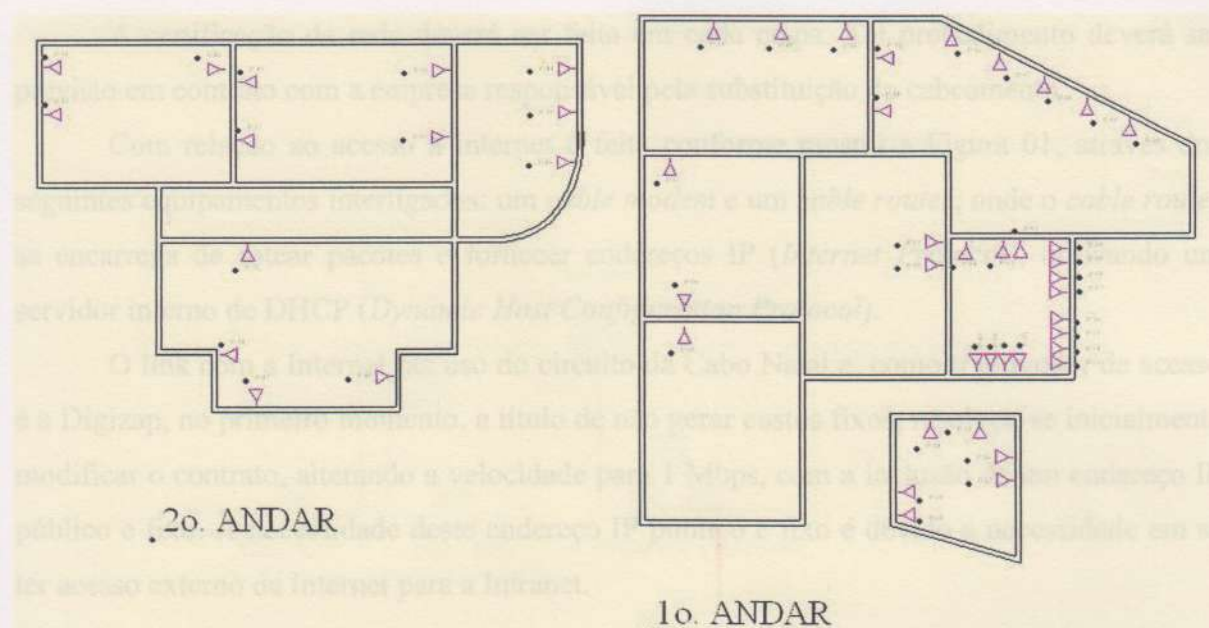


Figura 11: Planta Baixa Flamoil Serviços

Por se tratar de uma rede Ethernet, com equipamentos diversos e apresentando variações nas taxas de transmissão de 100 Mbps e 1 Gbps, o projeto levou em consideração as características gerais, e outras bem próprias de cada tecnologia, como tempo de retardo de transferência, desempenho, confiabilidade, modularidade e custo. Como base nesses pontos, a migração completa do sistema para padronizar a taxa de transmissão para 1Gbps será feita de forma gradativa.

A sistemática da substituição do cabeamento existente e dos equipamentos atenderá o cronograma abaixo.

Tabela 2: Atividades a serem realizadas

Atividade	Localização	Quantidade	Período
Substituição do Cabeamento para Categoria 6.	Estações de TRABALHO (Pontos P44, P43, P35, P6, P7).	5	JUNHO/07
Substituição dos SWITCH 10/100 Mbps por 10/100/1000 Mbps	CPD	2	JULHO/07
Substituição do Cabeamento para Categoria 6.	Estações de TRABALHO (demais pontos)	55	SETEMBRO/07

O uso de equipamentos mistos a priori não causa grande impacto, pois o formato do quadro ethernet é o mesmo, não necessitando conversão por parte dos equipamentos. Isso dá uma tranquilidade para executar o cronograma descrito acima, sem causar impacto aos usuários da rede.

A certificação da rede deverá ser feita em cada etapa. Tal procedimento deverá ser previsto em contrato com a empresa responsável pela substituição do cabeamento.

Com relação ao acesso a internet é feita conforme mostra a Figura 01, através dos seguintes equipamentos interligados: um *cable modem* e um *cable router*, onde o *cable router* se encarrega de rotear pacotes e fornecer endereços IP (*Internet Protocol*), utilizando um servidor interno de DHCP (*Dynamic Host Configuration Protocol*).

O link com a Internet faz uso do circuito da Cabo Natal e como o provedor de acesso é a Digizap, no primeiro momento, a título de não gerar custos fixos, resolveu-se inicialmente modificar o contrato, alterando a velocidade para 1 Mbps, com a inclusão de um endereço IP público e fixo. A necessidade deste endereço IP público e fixo é devido a necessidade em se ter acesso externo da Internet para a Intranet.

LINKSYS

Filters **Forwarding** Dynamic Routing Static Routing DMZ Host QoS MAC Addr. Clone Setup

PORT RANGE FORWARDING

Port forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your router, they will be redirected to the specified IP.

Customized Applications	Ext.Port	Protocol	Protocol	IP Address	Enable
		TCP	UDP		
FTP	20 To 21	☒	☒	192.168.1.2	☒
FTP2	60000 To 60100	☒	☐	192.168.1.2	☒
X11	6000 To 6001	☒	☐	192.168.1.2	☒
VNC	5900 To 5901	☒	☐	192.168.1.2	☒
X11-SSH	6010 To 6011	☒	☐	192.168.1.2	☒
VNC-2	5901 To 5902	☒	☐	192.168.1.2	☒
	0 To 0	☐	☐	192.168.1.0	☐
	0 To 0	☐	☐	192.168.1.0	☐
	0 To 0	☐	☐	192.168.1.0	☐
	0 To 0	☐	☐	192.168.1.0	☐

UPnP Forwarding Port Triggering

Apply Cancel

Figura 12: Tela de configuração *cable router*

Nas telas de configuração do *cable router*, verificou-se outras funcionalidades que poderiam ser exploradas. Um exemplo é a funcionalidade de redirecionamento de portas mostrado na tela de configuração da Figura 12. Com esta funcionalidade é possível

redirecionar o tráfego proveniente da Internet de determinadas portas do endereço IP público para qualquer estação de trabalho ou servidor da Intranet.

Estabelecido algumas mudanças iniciais, criou-se uma nova organização na rede, conforme a Figura 13.

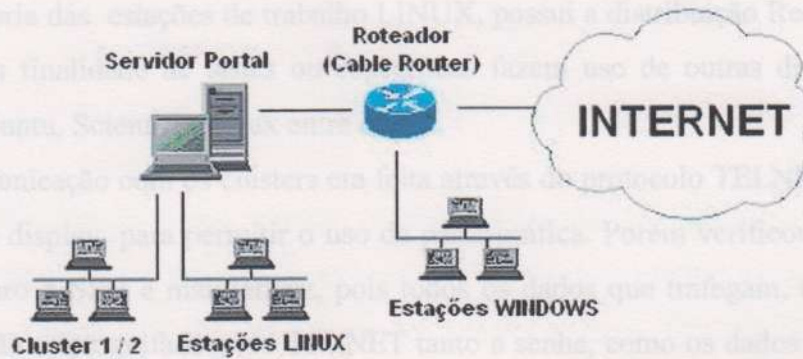


Figura 13: Estrutura Implementada

Comparando as Figuras 10, que mostra a estrutura existente e a Figura 13, que mostra a nova estrutura implantada, resolveu-se criar uma subdivisão da rede existente em duas faixas de endereços IPs distintos.

Da mesma forma que as estações de trabalho LINUX, os clusters e as estações WINDOWS receberam diferentes faixa de endereços IPs. Isto possibilita que regras de filtragem de tráfego podem ser criadas de maneira distinta, para cada faixa. Desenvolveu-se um software onde seria possível, as estações de trabalho LINUX, através de um simples botão alternar entre redes, conforme observamos na figura abaixo.

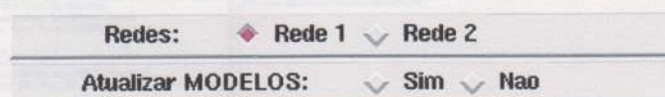


Figura 14: Tela do software que alterna as redes

O servidor implementado, denominado portal, além de receber as requisições externas, acumula a função de roteador, onde interliga as diferentes redes, quando solicitado pelo usuário.

3.3 ESTAÇÕES DE TRABALHOS

Após a análise preliminar do cabeamento e dos equipamentos que compõe a rede local da empresa e conseqüentemente, a execução das modificações iniciais. Partiu-se para analisar as estações de trabalho e os serviços nelas utilizados. Os usuários das estações, interagem de

forma dinâmica, fazendo requisições de processamento, transferência de dados seja na intranet ou Internet.

Pode-se classificar as máquinas Windows, Linux e dual Boot (Linux/Windows), mas nesse estudo será direcionado as estações de trabalho LINUX.

A maioria das estações de trabalho LINUX, possui a distribuição Red Hat 3.0 Update 2. Outras com finalidade de testes ou específicas fazem uso de outras distribuições como Mandrake, Ubuntu, Scientific Linux entre outras.

A comunicação com os clusters era feita através do protocolo TELNET, e utilizando a exportação do display, para permitir o uso da parte gráfica. Porém verificou-se que para um ambiente seguro o SSH é mais eficaz, pois todos os dados que trafegam, em uma conexão estabelecida são criptografados. No TELNET tanto a senha, como os dados passam livres de criptografia na rede, podendo qualquer usuário mal intencionado, conectado ao ambiente capturar tais informações.

O mesmo aconteceu com o protocolo FTP, utilizado para transferência de arquivos, esse também não faz uso de qualquer tipo de criptografia e foi substituído pelo protocolo SFTP ou SCP, ambos baseados no SSH e faz uso de criptografia.

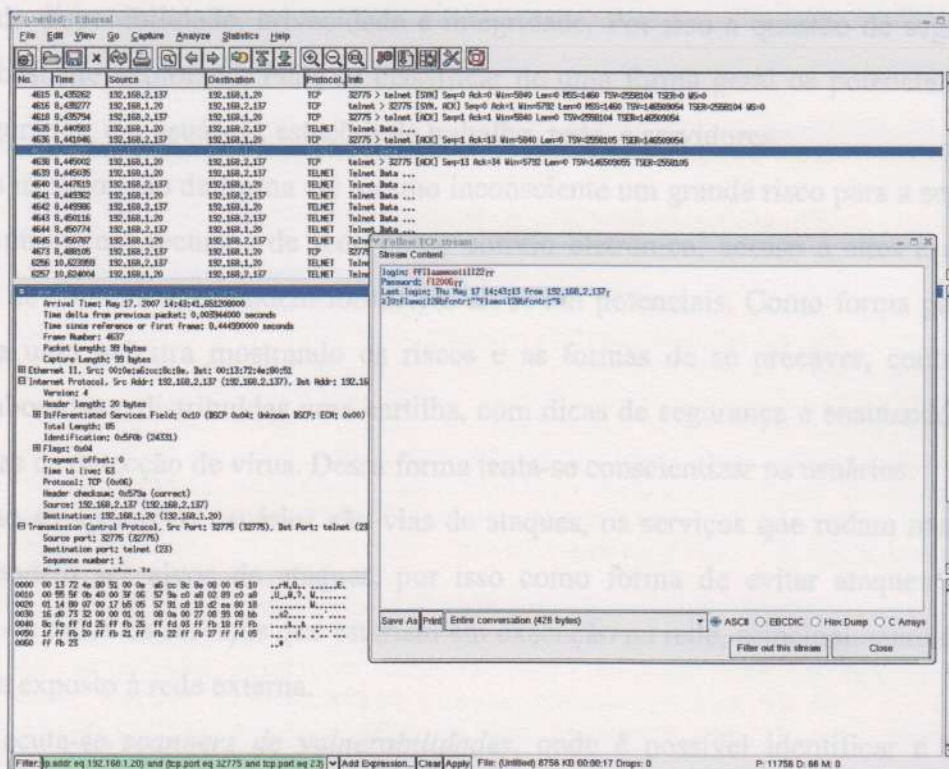


Figura 15: Pacote capturado pelo Ethereal

A figura 15, mostra uma sessão Telnet, os pacotes foram capturados usando o software *Ethereal*, pode-se observar que a senha e os dados trafegavam na rede sem qualquer tipo de criptografia, podendo ser capturados através de qualquer software de captura de pacotes.

As configurações dessas estações, foram modificadas e alguns serviços, como os citados anteriormente, substituídos por outros mais seguros.

3.4 SERVIDOR - PORTAL

Conforme dito no tópico anterior, resolveu-se instalar uma máquina, com funções de rotear os pacotes e receber requisições externas. A instalação do PORTAL com as funções de roteador, para a rede 192.168.2.X, passa ter acesso à faixa 192.168.1.X e os serviços SSH/SFTP, FTP, VNC, deixa a empresa pronta para receber as requisições externas da filial RJ e dos clientes, porém é necessário garantir a segurança exigida aos dados trafegados, a implantação de políticas de segurança se torna inevitável em se tratando de sigilo das informações.

A proteção dos dados da empresa e dos clientes é de fundamental importância para os aspectos de disponibilidade, privacidade e integridade. Por isso a questão de segurança, foi um item bastante explorado. Pode-se classificar de uma forma geral os potenciais de riscos para a segurança, em usuários, estações de trabalho, rede e servidores.

Os usuários são de forma até mesmo inconsciente um grande risco para a segurança na rede. Ao utilizarem recursos de rede como correio eletrônico, acesso a sites e até mesmo softwares de comunicação podem tornassem alvos em potenciais. Como forma paliativa, foi ministrada uma palestra mostrando os riscos e as formas de se precaver, contra ataques. Foram elaboradas e distribuídas uma cartilha, com dicas de segurança e ensinando o uso das ferramentas de detecção de vírus. Dessa forma tenta-se conscientizar os usuários.

Não só apenas os usuários são vias de ataques, os serviços que rodam nas máquinas também podem ser alvos de ataques, por isso como forma de evitar ataques e intrusos, enumerou-se todos os serviços que estariam em execução na rede, principalmente no servidor que estaria exposto à rede externa.

Executa-se *scanners de vulnerabilidades*, onde é possível identificar e corrigir os principais pontos de vulnerabilidades, buscando sempre informações das falhas reportadas, atualizações para os serviços e sistemas operacionais.

Analisa-se constantemente as políticas de segurança implantadas na empresa onde está sediado o servidor de e-mail e web. Onde se solicita constantemente qual a metodologia que

se utiliza para evitar problemas de privacidade da informação e os mecanismos de backup adotados.

Para a administração da rede interna criou-se uma seqüência de procedimentos conforme descrito abaixo:

- Verificar LOGs dos servidores;
- Atualizar antivírus, sistemas operacionais e serviços;
- Mudança das senhas periodicamente;
- Executar testes de vulnerabilidades e detecção de intrusão (IDS), a fim de identificar algum novo serviço em execução na rede e riscos oferecidos.
- Testar e atualizar regras do firewall;

```

Jul  1 21:41:20 portal sshd[15054]: Illegal user office from 222.44.33.67
Jul  1 21:41:20 portal sshd(pam_unix)[15054]: check pass; user unknown
Jul  1 21:41:20 portal sshd(pam_unix)[15054]: authentication failure;
logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=222.44.33.67
Jul  1 21:41:22 portal sshd[15054]: Failed password for illegal user
office from 222.44.33.67 port 54470 ssh2
Jul  1 21:41:26 portal sshd[15056]: Illegal user samba from 222.44.33.67
Jul  1 21:41:26 portal sshd(pam_unix)[15056]: check pass; user unknown
Jul  1 21:41:26 portal sshd(pam_unix)[15056]: authentication failure;
logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=222.44.33.67
Jul  1 21:41:29 portal sshd[15056]: Failed password for illegal user samba
from 222.44.33.67 port 54639 ssh2
Jul  1 21:41:33 portal sshd[15058]: Illegal user tomcat from 222.44.33.67
Jul  1 21:41:33 portal sshd(pam_unix)[15058]: check pass; user unknown
Jul  1 21:41:33 portal sshd(pam_unix)[15058]: authentication failure;
logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=222.44.33.67
Jul  1 21:41:35 portal sshd[15058]: Failed password for illegal user
tomcat from 222.44.33.67 port 54809 ssh2
Jul  2 14:19:08 portal sshd(pam_unix)[22182]: authentication failure;
logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=148.222.11.90
Jul  2 14:19:10 portal sshd[22182]: Failed password for illegal user www
from 148.222.11.90 port 52469 ssh2
Jul  2 14:19:15 portal sshd[22184]: Illegal user peru from 148.222.11.90
Jul  2 14:19:15 portal sshd(pam_unix)[22184]: check pass; user unknown
Jul  2 14:19:15 portal sshd(pam_unix)[22184]: authentication failure;
logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=148.222.11.90
Jul  2 14:19:18 portal sshd[22184]: Failed password for illegal user peru
from 148.222.11.90 port 52566 ssh2
Jul  2 14:19:24 portal sshd[22186]: Illegal user maria from 148.222.11.90
Jul  2 14:19:24 portal sshd(pam_unix)[22186]: check pass; user unknown
Jul  2 14:19:24 portal sshd(pam_unix)[22186]: authentication failure;
logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=148.222.11.90
Jul  2 14:19:26 portal sshd[22186]: Failed password for illegal user maria
from 148.222.11.90 port 52660 ssh2
Jul  2 14:19:31 portal sshd[22188]: Illegal user robert from 148.222.11.90

```

Figura 16: Log do Servidor PORTAL

A necessidade da configuração do servidor FTP, se deve ao fato dos clientes desconhecerem o uso do SFTP. Resolveu-se destacar a importância do detalhe no tocante a servidor FTP. Ao utilizar o modo passivo, o que é mais usado atualmente. Teve-se, que deixar uma faixa de portas altas abertas para que fosse possível o estabelecimento da comunicação. Ou seja, no modo ativo o servidor precisa ter aberta apenas a porta 22, mas em compensação o cliente precisa acessar a web diretamente e ter um conjunto de portas altas abertas no firewall. No modo passivo, os papéis se invertem: o cliente não precisa ter portas abertas, mas o servidor sim.

3.5 CLUSTER

A fim de atender a demanda computacional, a empresa possui dois Clusters de computadores tipo Beowulf.

O cluster Beowulf é o nome dado à arquitetura de multicomputadores utilizados para computação paralela ou distribuída que oferece baixo custo e alta capacidade de processamento. É normalmente composto por um conjunto de microcomputadores formado por um nó mestre e nós escravos conectados via rede, rodando um sistema operacional paralelo. Nesse modelo, o nó mestre tem a função de controlar o cluster, distribuir os arquivos e as tarefas para os nós escravos, além de servir de gateway para conexão externa.

A configuração dos clusters é composta por processadores Intel Xeon 2.8 GHz, 2 GBytes de memória de disco rígido, e acoplado ao sistema 3 storages em RAID 5, com capacidade total de 5 TBytes. Interligados por uma rede de tecnologia Gigabit Ethernet. O sistema operacional é o Linux Red Hat 3.0 Update 2. Como fonte de alimentação para o sistema a empresa possui dois nobreak um de 15 kVA e outro 4 kVA respectivamente.

Implementar melhorias. Por considerar a subdivisão uma forma de facilitar a resolução de problemas. Sistematicamente definiu-se que os problemas de funcionamento de energia, refrigeração e cabeamento, seriam considerados problemas relacionados à infraestrutura. Os problemas referentes à instalação de equipamentos, aquisição de equipamentos e manutenção de equipamentos, seria considerado como problemas de hardware, os relacionados a sistema operacional e aplicativos, seria considerados problemas de software e os fatos relacionados à integridade dos dados, privacidade dos dados e disponibilidade, problemas relacionados a segurança.

Porém não se pode esquecer que estes itens estão relacionados e o bom funcionamento do sistema está ligado de cada um desses itens.

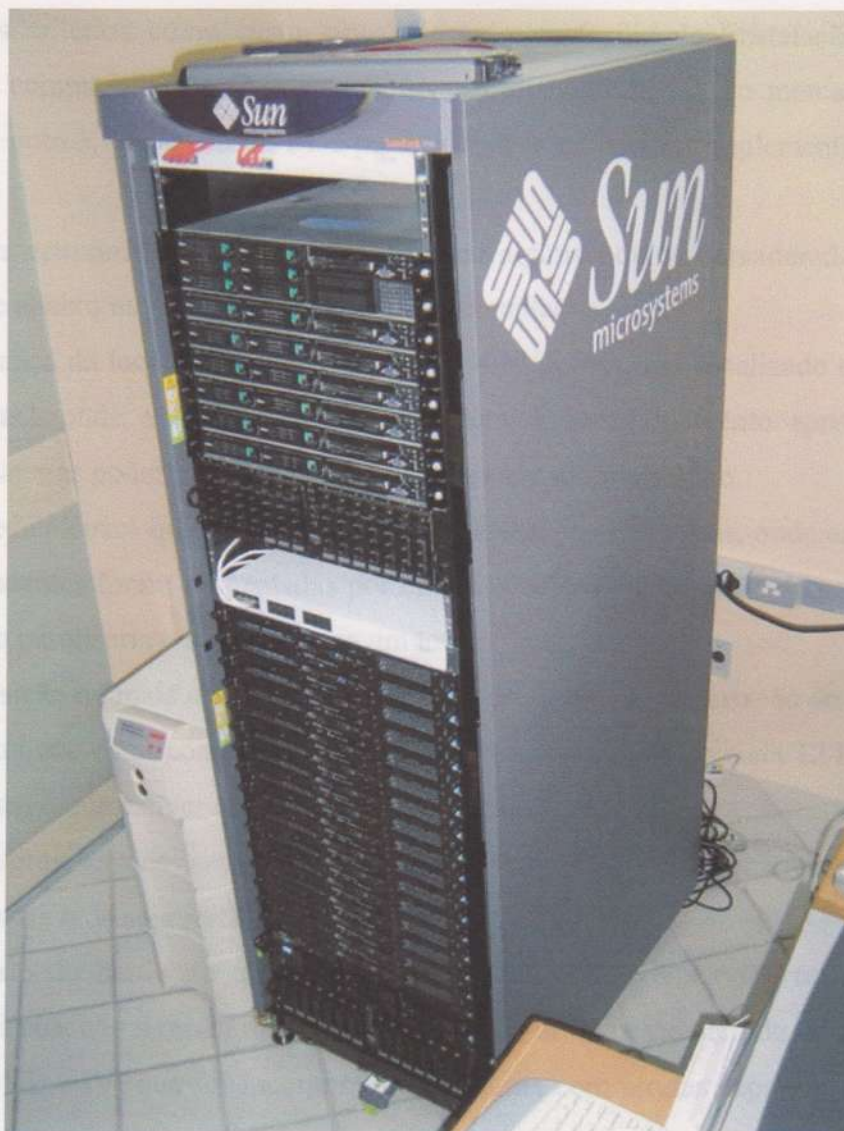


Figura 17: Clusters Linux – Flamoil Serviços – MATRIZ

Baseado no levantamento da estrutura existente, iniciou-se o estudo a fim de sugerir e implementar melhorias. Por considerar a subdivisão uma forma de facilitar a resolução de problemas. Sistemáticamente definiu-se que os problemas de fornecimento de energia, refrigeração e cabeamento, seriam considerados problemas relacionados à infra-estrutura. Os problemas referentes à instalação de equipamentos, aquisição de equipamentos e manutenção de equipamentos, seria considerado como problemas de hardware, os relacionados a sistema operacionais e aplicativos, seria considerados problemas de software e os fatos relacionados à integridade dos dados, privacidade dos dados e disponibilidade, problemas relacionados a segurança.

Porém não se pode esquecer que estes itens estão relacionados e o bom funcionamento do sistema está atrelado de cada um desses itens.

Alguns critérios como custo, prazo de entrega, facilidade (instalação, manuseio e manutenção), compatibilidade (hardware/software), disponibilidade no mercado, assistência técnica, entre outros, foram observados para as sugestões feitas e implementadas durante o trabalho.

A infra-estrutura interna do CPD, possuía alguns pontos considerados de risco ao sistema, segue abaixo os itens modificados e implementados;

- Mudança da localização do No-break de 4 kVA, por está localizado dentro do CPD do lado do rack onde estão instalados os clusters. Esse equipamento apresenta risco de incêndio, as baterias poderiam exalar gases tóxicos e campo magnético.

- A rede elétrica que alimenta o sistema passou por mudanças, onde as fontes na sua maioria redundantes foram alimentadas por circuitos diferentes, no caso de pane em um dos no-breaks, não paralisaria o sistema como um todo.

- Aquisição de mais um ar-condicionado de 38.000 BTUs, e criação de um sistema de automação para que os ar-condicionados tenham seu uso alternado a cada 12 horas, podendo ser ligados, caso o que estiver em uso apresente falha.

- Substituição dos switches de backup, para caso o sistema apresente falha o funcionamento da rede seja restabelecido em curto prazo de tempo.

Na parte do hardware que compõe o CPD, ou seja os servidores SUN e DELL, unidades de discos, não tiveram modificações. Foi adquirido nesse período uma nova unidade de fita tipo DLT – IV, que foi incorporada ao sistema com tarefas específicas de backup e compatibilidade com a mídia enviada pelo cliente.

A parte mais explorada do CPD, foi sem dúvida o item softwares. Onde é composto pelo sistema operacional e serviços em execução, e as aplicações específicas.

Previamente foi analisado o motivo pelo uso da distribuição Red Hat 3.0 Update 2, colocamos em questão pois se tem disponíveis atualizações para versões mais novas, a justificativa para a escolha vem do fato da principal aplicação que a empresa faz uso está homologada para essa distribuição e nessa versão. Sendo assim para facilidade de suporte resolveu-se não modificar.

Fez-se necessário verificar quais os softwares específicos que a empresa utiliza e os serviços e pacotes que os mesmos fazem uso. Com base nessa verificação iniciaram-se as instalações, configurações, atualizações e desenvolvimento de aplicações e serviços.

Os clusters em sua maioria são equipamentos que necessitam de uma estrutura básica de serviços. Por isso resolveu-se instalar alguns serviços e aplicativos disponíveis, tais como:

- *Servidor NIS (Network Information Service)*, onde a criação de um usuário de rede facilita a comunicação entre o nó de gerência e os nós de processamento. O processo de adição, exclusão ou alteração dos usuários do cluster por parte do administrador da rede, também é facilitada, visto que só se faz necessário modificar uma máquina ao invés de realizar em todos os servidores que compõe o cluster. O NIS mantém as informações da base dados em arquivos denominado mapas e faz uso das RPC (*chamadas de procedimento remoto*).

- *Servidor NFS (Network File System)*, é responsável pelo compartilhamento dos dados entre as máquinas. É de fundamental importância por exemplo, para que o servidor NIS funcione corretamente, pois o diretório do usuário deverá estar acessível e montado na máquina em que ele tentar se logar. Outras partições contendo programas e dados para uso pelos nós foram exportadas.

- *Servidor SSH/SCP/SFTP (Security Shell)*, foi colocado em execução para que usuários externos ao cluster fizessem acesso ao mesmo. Seu uso foi substituído pelo TELNET e FTP existente, devido aos problemas de segurança já exemplificados anteriormente.

- *Servidor RSH/RCP (Remote Shell)* – sua instalação se fez necessário, devido ao uso por parte das aplicações que executam comandos remotamente, a partir do nó de controle nos nós de processamento. Esses programas também fazem uso do rcp, para transferência de arquivos entre as máquinas sem necessidade de autenticação.

- *Servidor DNS (Domain Name Server)* – configurou-se o bind, para que fosse feita a resolução dos nomes em endereços e vice-versa. Definiu-se um dos clusters como DNS primário e outro como secundário.

- *Servidor DHCP (Dynamic Host Configuration Protocol)* – a configuração de um servidor DHCP, se deve ao fato não de fornecer apenas endereços IP, mais como também máscaras de rede, endereços de roteadores, endereços de servidores de DN, nome do cliente, nome do domínio DNS, rotas estáticas, entre outras opções que facilitam a vida do administrador do sistema. A configuração utilizada foi a forma manual, onde associou-se um endereço IP para cada endereço MAC (*Médium Access Control*) das máquinas que formam a rede interna do cluster.

Desenvolveu-se uma aplicação que fosse possível executar comandos a partir do nó de controle para todos os nós de processamento. Essa aplicação foi desenvolvida em Java e seu código fonte está em anexo.

Outros serviços como sendmail, servidor de notícias, que não serão utilizados, foram removidos do sistema.

Concluído a instalação de alguns serviços básicos, partiu-se para a instalação e configuração de serviços e ferramentas, específicas ao processamento e a gerência.

Banco de Dados MySQL.

Compiladores para as linguagens Fortran, C/C++, Java entre outros.

PVM (*Parallel Virtual Machine*) – é o pacote de ferramentas utilizadas, capaz de permitir a execução de aplicações de maneira paralela, fazendo com que uma coleção de sistemas computadorizados, interligados em rede, possam ser vistos como uma única máquina. A utilização de aplicações desenvolvidas utilizando o PVM, faz com que as máquinas que compõem o cluster, para o usuário se transforme em um único recurso computacional de grande capacidade. O PVM foi especialmente desenhado para interligar recursos computacionais numa rede, fornecendo ao utilizador uma plataforma paralela para correr aplicações, independentemente da localização, da quantidade ou das diferenças entre os computadores na rede.

O funcionamento do PVM é composto de duas partes a primeira, composta pelo daemon que deverá ser executado em todos os computadores que vão formar a máquina virtual. A segunda é composta por uma biblioteca de rotinas de interface, onde concentram as primitivas necessárias à comunicação com aplicações, gerência dos processos, criação e manutenção do estado da máquina virtual.

O funcionamento básico se caracteriza da seguinte forma, o usuário ou a aplicação que faz uso do PVM, executa o *daemon* pvmd3, no nó de controle que chama os demais processos pvmd3 escravos em cada computador que vai compor a máquina virtual, através do rsh (remote Shell), que previamente deverá estar configurado.

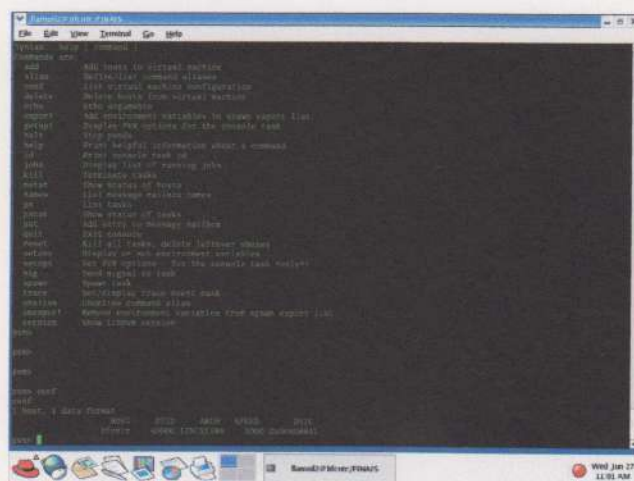


Figura 18: Tela de configuração do PVM com respectivas opções

OpenPBS (*Portable Batch System*) – a instalação deu-se em virtude, da sua função de gerência de recursos que direciona as tarefas requeridas pelo usuário para o(s) nó(s) disponível. A submissão de tarefas é realizada por meio de *scripts* ou *softwares*, onde o usuário deve escolher qual a fila que oferece os melhores recursos para a sua tarefa. Por enquanto, o fator de escolha se restringe basicamente ao tempo máximo de CPU permitido e prioridade de execução. Utilizou-se em um dos clusters, outro gerenciador de recursos similar o *TORQUE*, com código aberto baseado no PBS, que já conta com mais de 1200 correções e algumas melhorias significativas, como tolerância a falhas, aumento da capacidade de trabalhar com tarefas (2000 processos), mensagens de LOGs mais completos entre outros recursos.

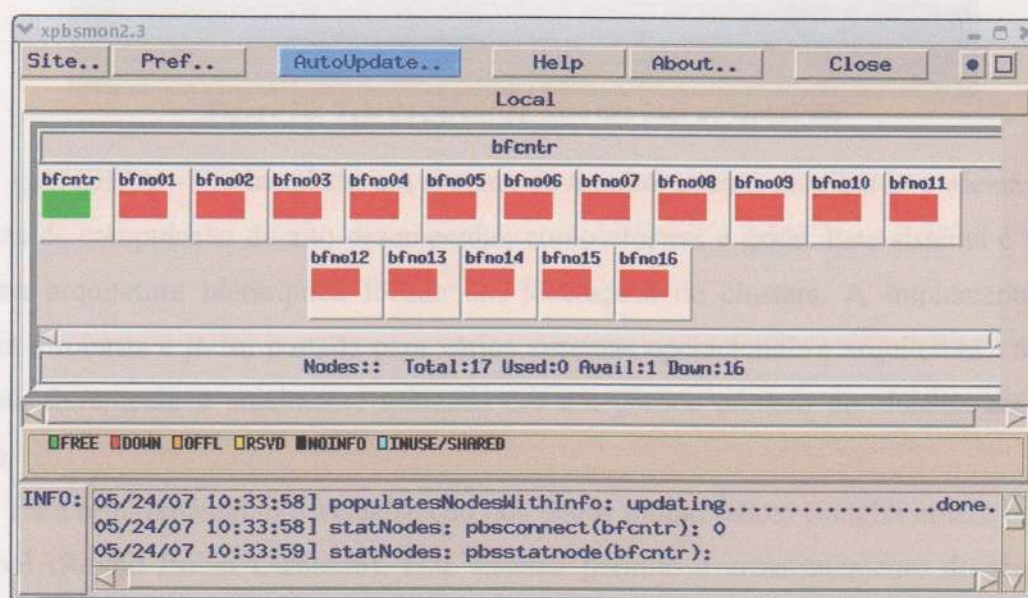


Figura 19: Interface gráfica do OpenPBS – Gerenciamento dos NÓS

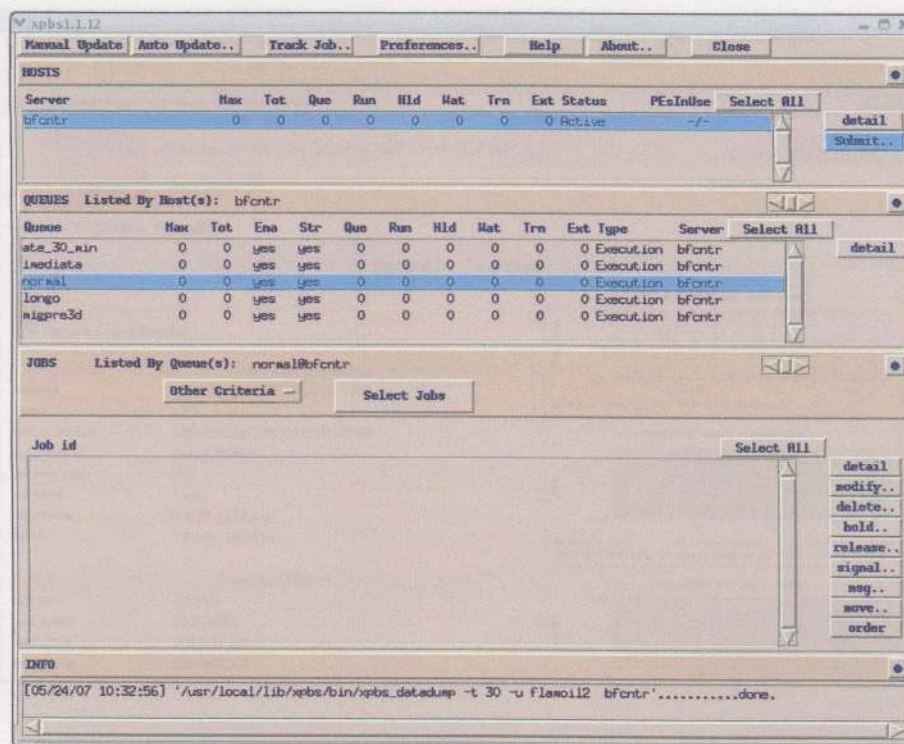


Figura 20: Tela de gerenciamento das filas no OpenPBS

GANGLIA – Foi instalado um sistema de monitoramento distribuído e escalável para sistemas de computação de alto desempenho, como clusters e grids. Este sistema é baseado em uma arquitetura hierárquica focada em federações de clusters. A implementação de Ganglia é robusta e já foi portada para vários sistemas operacionais e arquiteturas, de modo que esta ferramenta é atualmente utilizada em um grande número de clusters em todo o mundo.

Para armazenamento e visualização dos dados monitorados, Ganglia utiliza o sistema RRDtool (Round Robin Database). Este sistema permite o armazenamento de seqüências temporais de dados de forma compacta em um banco de dados circular, de tamanho constante. A partir dos dados armazenados, RRDtool gera gráficos que mostram a evolução de uma ou mais métricas ao longo do tempo.

A figura abaixo ilustra a interface Web de Ganglia para visualização das métricas monitoradas.

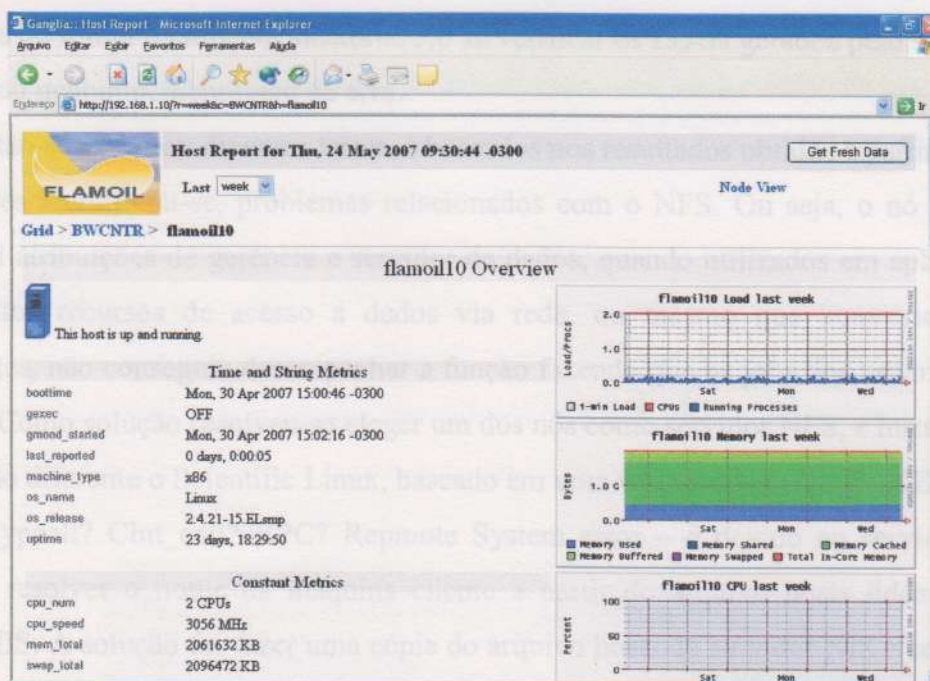


Figura 21: Interface WEB para exibição das métricas monitoradas

Existem diversas métricas pré-existent, como as que monitoram o uso da CPU, uso da rede, detecção de ociosidade e balanceamento de cargas, entre outras. O pacote ainda conta com a possibilidade de serem desenvolvidas métricas específicas de acordo com a necessidade do administrador do sistema.

O *SystemImager* – após a conclusão da instalação do sistema e realização das configurações necessárias, verificou-se a necessidade, devido ao grande número de máquinas e o provável crescimento, criar uma forma para manter o sistema das máquinas que compõe o cluster, atualizados de forma automáticas e instaláveis. Escolheu-se o *systemimager*, como uma ferramenta que permite-nos instalar de forma simples várias estações *Linux* a partir de uma imagem, tornando o processo de instalação o simples trabalho de ligar a máquina.

Basicamente o programa funciona da seguinte maneira, é gerado uma ou mais imagens das estações, elas são armazenadas em um servidor, neste caso o nó de controle de cada cluster, para posterior instalação, e através de um disquete, cd ou um servidor de boot pela rede, como *atftpd*, é carregado um kernel que irá iniciar o processo de cópia das imagens para as estações.

O processo de restauração da imagem, é todo automatizado exigindo uma interação mínima para que ocorra.

Após concluir todos os procedimentos de instalações e atualizações, alguns usuários reportaram problemas com o uso de um dos softwares de produção, que abortava os processos

submetidos de forma totalmente aleatória. Ao se verificar os LOGs gerados pelo software não se encontrou nenhuma mensagem de erro.

Então se executou diversos testes, e baseados nos resultados obtidos a partir de estudos preliminares identificou-se, problemas relacionados com o NFS. Ou seja, o nó controlador que possui atribuições de gerência e servidor de dados, quando utilizados em aplicações que exigem altos recursos de acesso a dados via rede, ou mesmo que houvesse processos concorrentes, não conseguia desempenhar a função fazendo que os jobs dos usuários viessem a abortar. Como solução resolveu-se eleger um dos nós como servidor NFS, e instalou-se uma distribuição diferente o Scientific Linux, baseado em uma versão mais atual do KERNEL

O_ypcall? Clnt_call? RPC? Repmote System error – é devido ao servidor rsh não conseguir resolver o nome da máquina cliente a partir do arquivo hosts lidos através do servidor NIS. A solução foi fazer uma cópia do arquivo hosts do servidor NIS e colocá-los no lugar de /etc/hosts do servidor onde está sendo utilizada a alternativa de se acessar por rsh.

O nó de controle também serve de roteador entre a rede interna do cluster e a rede externa, ou seja para que os nós de processamento tenham acesso a rede externa do cluster.

3.6 IMPLEMENTANDO O ACESSO REMOTO

Atualmente pode-se encontrar diversas ferramentas que promovem o acesso remoto. Tais ferramentas desenvolvidas utilizando diversos critérios e finalidades.

Pode-se subdividir o uso das ferramentas de acesso remoto, em basicamente dois grupos:

- Administração;
- Processamento;

Existem diversas ferramentas disponíveis para os mais variados sistemas operacionais, como Linux e Windows.

No foco do trabalho serão abordados duas ferramentas, o VNC (Virtual Networking Computing) e o FreeNX. Ambas as ferramentas encontram-se disponíveis para plataformas de sistemas operacionais Windows e Linux, as particularidades de cada uma serão analisadas a fim de traçar um modelo comparativo, que justifique a escolha por uma delas, levando em consideração critérios de segurança, rapidez e praticidade de uso.

Ambas as ferramentas fazem uso de três partes, o cliente, o servidor e o protocolo.

A implementação do VNC se deu de forma simples, por ser uma ferramenta disponível por padrão na distro Red Hat 3.0 Update 2, utilizada no Cluster. Para isso bastando inicializar

o serviço. Da primeira vez que é executado, ele pede para definir uma senha de acesso, que deve ser fornecida pelos clientes. O VNCserver abre uma seção separada do servidor X, independente da tela :0 que você vê no monitor. Isto permite que outras pessoas acessem o mesmo servidor sem atrapalhar quem está trabalhando nele.

O VNC por padrão faz uso da porta TCP 5900 a 5906, onde cada nova execução do vncserver gerará uma porta 5901, 5902 e assim por diante.

Estando o servidor VNC configurado basta agora escolhermos o cliente VNC ou VNCviewer, de acordo com o sistema operacional utilizado na máquina cliente. Para acessar basta digitarmos o número IP ou o nome da máquina seguido de dois pontos o número da seção.

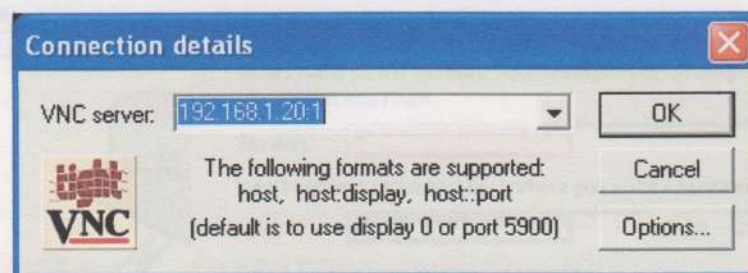


Figura 22: Tela inicial do TightVNC Cliente

O FreeNX é um pouco mais complicado, por fazer uso do protocolo SSH, precisa-se estar com esse serviço ativo, para que funcione.

Estando o servidor SSH rodando, e devidamente configurada no arquivo `/etc/sshd_config`, as opções:

`X11Forwarding=yes`

`AllowUsers user1 user2 ... userN`

Após a configuração do servidor SSH, se fez necessário o download dos pacotes RPM do FreeNX e do NXserver e como root executar os comando mostrados abaixo:

```
rpm -Uvh nx-1.5.0-4.rh.0.1.i386.rpm
rpm -Uvh freenx-0.4.4-2.rh.0.src.rpm
```

Após sua instalação precisa-se definir uma senha para o usuário nx, criado por padrão durante a instalação do pacote.

Sabendo que o NX faz uso do SSH pode-se testar o seu funcionamento executando os procedimentos abaixo:

Copiar a chave gerada durante a instalação que se encontra no diretório:

```
ssh nx@{NXSERVER}
```

```
HELLO NXSERVER - Version 1.4.0-02 OS_(GPL)
```

```

NX> 105 quit
quit
Quit
NX> 999 Bye
Connection to {NXSERVER} closed.

```

Após a configuração do servidor irá se configurar o cliente. Primeiramente executa-se um download do software no site www.nomachine.com, a estação está rodando Windows XP Professional, executa-se o executável e após a instalação iniciou-se a seguinte configuração:

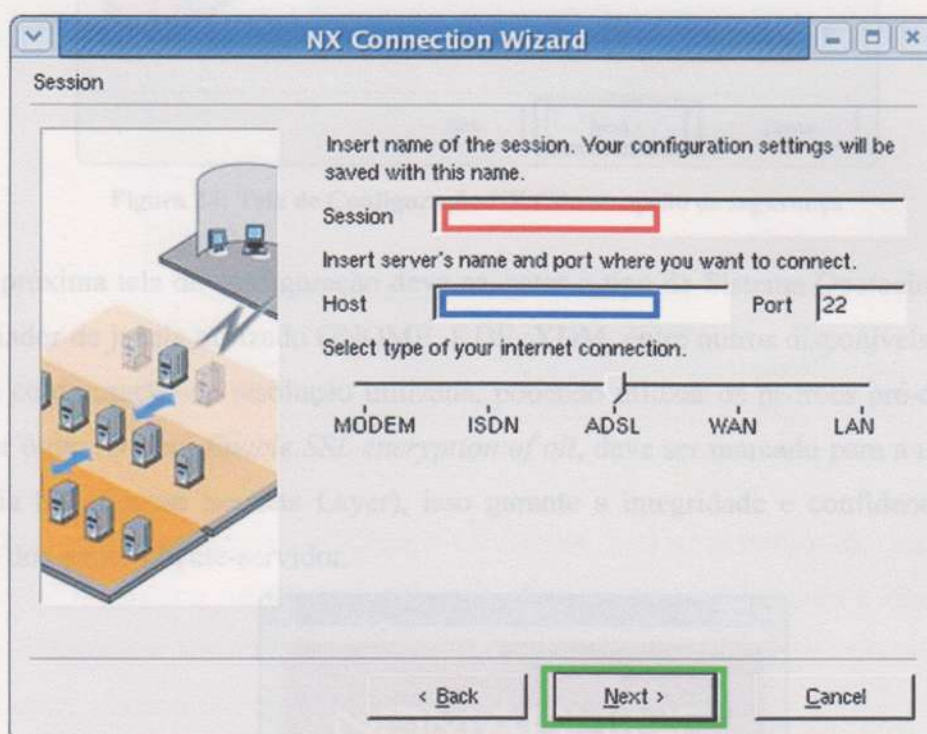


Figura 23: Tela de configuração inicial do NX Cliente

Atribuiu-se um nome a seção “Cluster 2” no campo *Session*, em *Host* deverá ser preenchido com o endereço IP do servidor FreeNX, o campo *Port* já vem por default preenchida com a porta padrão TCP 22, utilizada pelo SSH.

Figura 24: Tela de configuração do servidor NX definição da porta e chave pública

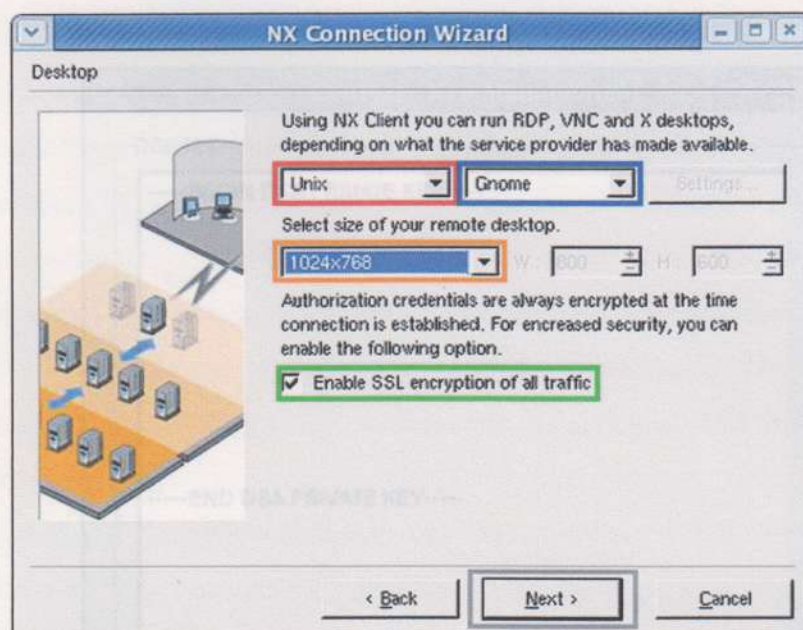


Figura 24: Tela de Configuração NX Cliente opção de segurança

A próxima tela de configuração deve-se, setar o tipo de Sistema Operacional e o tipo de gerenciador de janela utilizado GNOME, KDE, XDM, entre outros disponíveis. Possibilita também a configuração da resolução utilizada, podendo utilizar os padrões pré-definidos ou customizar outra. O item *Enable SSL encryption of all*, deve ser marcado para a utilização da criptografia SSL(Secure Sockets Layer), isso garante a integridade e confidencialidade no transporte dos dados cliente-servidor.

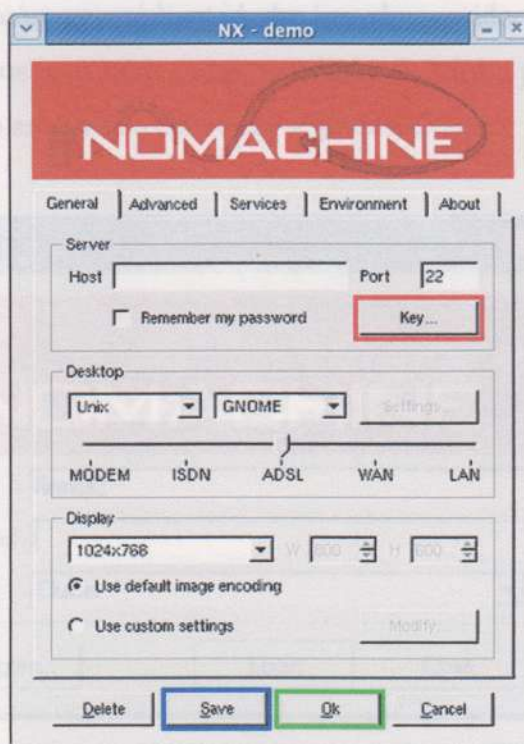


Figura 25: Tela de configuração do servidor NX definição de porta e chave pública

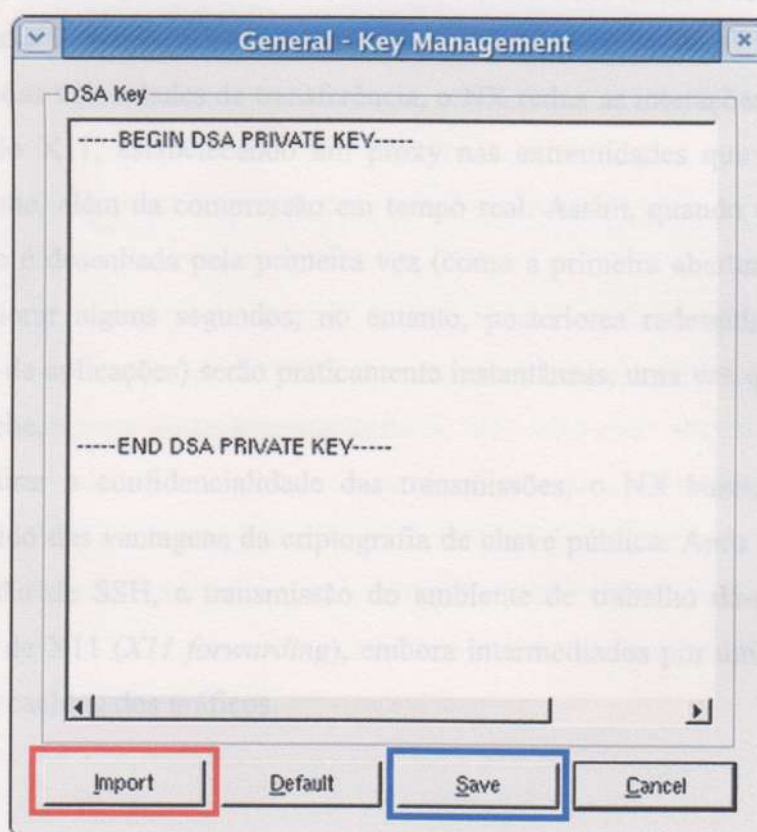


Figura 26: Tela de importação no CLIENTE da chave pública do SERVIDOR

O item principal na configuração do NX Cliente, está na definição da chave, para isso deve-se copiar o arquivo `/etc/nxserver/client.id_dsa.key` do servidor para a pasta de cada cliente e certificar-se que todos os usuários têm permissão de leitura para o arquivo. Clica-se no botão *Import* escolhendo o arquivo da chave em seguida salvando.



Figura 27: Tela inicial do CLIENTE NX para acesso ao SERVIDOR

Após a configuração quando se executa o cliente, basta adicionar a senha no campo password, para que seja feito o login no servidor NX.

Para atingir boas velocidades de transferência, o NX reduz as interações entre cliente-servidor do protocolo X11, estabelecendo um proxy nas extremidades que irá fazer uso, também, de uma cache, além da compressão em tempo real. Assim, quando uma região do ambiente de trabalho é desenhada pela primeira vez (como a primeira abertura do menu de aplicações), irá demorar alguns segundos; no entanto, posteriores redesenhos (expansões posteriores do menu de aplicações) serão praticamente instantâneas, uma vez que essa região já se encontra em cache.

Para assegurar a confidencialidade das transmissões, o NX baseia-se em SSH, permitindo tirar partido das vantagens da criptografia de chave pública. Após a autenticação regular de uma sessão de SSH, a transmissão do ambiente de trabalho dá-se através dos mecanismos nativos de X11 (*X11 forwarding*), embora intermediados por um *proxy* que irá fazer a compressão e caching dos gráficos.

Versões antigas do VNC tinham problemas com a configuração em teclados ABNT, isso foi resolvido nas versões recentes. No FreeNX a configuração do teclado é independente do servidor, você pode configurar o teclado no servidor da forma que for necessária, pois vale a configuração do cliente.

O TightVNC trabalha tirando screenshots da tela e compactando as imagens antes de enviar via rede. Ao chegar no cliente, as imagens precisam ser descompactadas, montadas e só então exibidas na tela. É possível que tanto o servidor quanto o cliente sejam relativamente rápidos para obter uma boa velocidade. O FreeNX usa o sistema de comunicação de X, combinado com compressão e encriptação via SSH, uma combinação que consome bem menos processamento, tanto no cliente quanto no servidor.

O TightVNC a criptografia só existe a título de autenticação, que faz uso do algoritmo DES quando se trabalha com senhas de 8 caracteres tem uma chave de 56 bits. Porém não existe encriptação dos dados, ou seja todos os outros tráfegos passam livremente, podendo ser explorados principalmente quando se utiliza o programa via Internet. Para resolver o problema, você pode usar um tunnel via SSH para obter uma conexão segura, mas isso torna a conexão mais lenta e a configuração mais trabalhosa.

O FreeNX já oferece encriptação nativamente, embora seja possível desabilitar este recurso para diminuir um pouco o uso de recursos do sistema, porém não é aconselhável.

4 ANÁLISE DE RESULTADOS

Existem muitas diferenças na forma como o FreeNX e o TightVNC trabalham, no TightVNC, as seções ficam abertas depois de fecharmos a janela, o que permite trabalhando na mesma seção, mesmo depois de ir para outro micro. No FreeNX, é possível se reconectar à uma seção suspensa apenas a partir do mesmo cliente.

No TightVNC é preciso rodar o comando "vncserver" no servidor (que remotamente é geralmente feito conectando primeiro via SSH) para abrir cada seção, e o comando "vncserver --kill :1" (onde o :1 é o número da seção) para fechá-la, tudo feito manualmente. No FreeNX, o servidor principal fica residente e as seções vão sendo abertas automaticamente conforme os usuários se conectam. Cada usuário loga-se usando seu próprio login e senha.

No TightVNC não oferece suporte a *antialiasing* de fontes e outros recursos gráficos, o que faz com que a qualidade da imagem não seja a mesma que ao usar a máquina localmente, o que no FreeNX estes recursos são melhores suportados.

Versões antigas no VNC tinham problemas com a acentuação em teclados ABNT, isso foi resolvido nas versões recentes. No FreeNX a configuração do teclado é independente do servidor, você pode configurar o teclado no servidor da forma que for necessária, pois vale a configuração do cliente.

O TightVNC trabalha tirando screenshots da tela e compactando as imagens antes de enviar via rede. Ao chegar no cliente, as imagens precisam ser descompactadas, montadas e só então exibidas na tela. É preciso que tanto o servidor quanto o cliente sejam relativamente rápidos para obter uma boa velocidade. O FreeNX usa o sistema de comunicação do X, combinado com compactação e encriptação via SSH, uma combinação que consome bem menos processamento, tanto no cliente quanto no servidor.

O TightVNC a criptografia só existe a título de autenticação, que faz uso do algoritmo DES quando se trabalha com senhas de 8 caracteres tem uma chave de 56 bits. Porém não existe encriptação dos dados, ou seja todos os outros tráfegos passam livremente, podendo ser capturados principalmente quando se utiliza o programa via Internet. Para amenizar o problema, você pode usar um túnel via SSH para obter uma conexão segura, mas isso torna a conexão mais lenta e a configuração mais trabalhosa.

O FreeNX já oferece encriptação nativamente, embora seja possível desabilitar este recurso para diminuir um pouco o uso de recursos do sistema, porém nada aconselhável.

O TightVNC não oferece nenhum sistema para transferir arquivos entre o servidor e o cliente, é preciso manter um servidor FTP, SSH, Samba ou NFS aberto para isso. No FreeNX é possível usar o próprio SSH para transferir arquivos, usando o sftp.

Abaixo segue um resumo das diferenças encontradas.

TightVNC	FreeNX
Sessão fica aberta após fechamento da janela, podendo ser reconectada a partir de outra máquina.	Sessão só poder ser usada no mesmo cliente.
Sessões novas só podem ser abertas a partir da execução do “vncserver”, isso só pode ser feito através de um prévio acesso ao servidor, geralmente feito através de SSH.	Sessões novas podem ser abertas automaticamente bastando a conexão do usuário.
Dependência de configurações prévias no servidor. Exemplo: Teclados ABNT	Configurações feitas a partir do cliente
Encriptação de dados não nativas.	Encriptação de dados nativa
Impossibilidade de transferência de arquivos utilizando o próprio software	Possibilidade de transferência de dados “nativa” usando o sftp

Tabela 3: Resumo comparativo TightVNCe FreeNX

Analisando as características das duas ferramentas resolvemos optar pelo FreeNX, a sua segurança “nativa”, facilita o trabalho de configuração, a possibilidade de transferência de informações MATRIZ-FILIAL, sem necessidade de utilizar outro tipo de solução, como FTP, o que facilita bastante.

O desempenho também foi levado em consideração, o FreeNX, apresentou taxas superiores de transferência.

5 CONCLUSÃO

Tendo em vista a oportunidade de se aplicar os conhecimentos adquiridos no decorrer da especialização em um caso real, temos um projeto que une a prática e a teoria.

O projeto que tinha como foco inicial à criação de uma estrutura que garantisse o acesso externo a empresa.

No seu decorrer foi modificado, de forma a não se deter no acesso externo. Pois analisando de uma forma geral e tendo o conhecimento que a empresa faz uso de diversas tecnologias de redes de computadores distintas, não poderíamos deixar de analisar os itens que fazem parte dessa estrutura .

Observamos que a estrutura de rede, não pode ser considerado um item totalmente isolado de outras estruturas como elétrica, logística e refrigeração. Para que o sistema como um todo seja cada vez mais, confiável, disponível e redundante.

No desenvolvimento do estudo, surgiram varias implementações de novas tecnologias e reestruturação das existentes, que obtivemos atualizações e parametrizações que melhorem desempenho.

A interação com os usuários, foi de fundamental importância, para solução de problemas relacionados a segurança. Sendo ele principal foco de problemas, segundo estatísticas. Medidas paliativas utilizadas tendem a amenizar os problemas causados pelos usuários finais.

REFERÊNCIAS BIBLIOGRÁFICAS

- TANENBAUM, A. S. **Redes de Computadores**. 4ª ed. Rio de Janeiro: Campus, 2003.
- MORAES, A. F. **Redes de Computadores – Fundamentos**. 1ª ed. São Paulo. Editora Erica, 2004.
- MORIMOTO, C. E. **Redes e Servidores Linux**. 3ª ed. Paraná: GDH Press e Sul Editores, 2006.
- MORIMOTO, C. E. **Entendendo e Dominando o Linux**. 7ª ed. Paraná: GDH Press e Sul Editores, 2004.
- DARLEN, Daniel. *Introdução à Criptografia RSA*. Disponível em: <http://www.dicna-leon.br/dicna-120070611.php>. Acessado em 20 de Junho de 2007.
- PINZARI, Gian Filippo. *Introduction to NX technology*. Disponível em: <http://nomachine.com/documentation/html/intr-technology.html>. Acessado em 5 de maio de 2007.
- WIKIPEDIA. Disponível em: <http://www.wikipedia.org>. Acessado de 7 à 18 de julho de 2007.

BIBLIOGRAFIA CONSULTADA

COMITÊ TÉCNICO DE MIGRAÇÃO PARA CÓDIGO ABERTO. Disponível em <<http://www.prt15.gov.br/sistemas/bancoDocumento/documentos/docs/ataa0a080f42e6f13b3a2df133f073095dd.pdf>>. Acessado em 7 de Fevereiro de 2007.

Technical Paper. SSH mais rígido e seguro. Disponível em <<http://br.attachmate.com/NR/rdonlyres/FCECB83D-E27D-4C80-88C6-657BE1D4A74/0/WhitePaperSSHMaisRigidoPortugu%C3%A9s.pdf>>. Acessado em 10 de Fevereiro de 2007.

DARLEN, Daniel. *Introdução à Criptografia RSA*. Disponível em: <<http://www.dicas-l.com.br/dicas-l/20070611.php>>. Acessado em 20 de Junho de 2007.

PINZARI, Gian Filippo. *Introduction to NX technology*. Disponível em: <<http://nomachine.com/documentation/html/intr-technology.html>>. Acesado em 5 de maio de 2007.

WIKIPEDIA. Disponível em <<http://www.wikipedia.org>>. Acessado de 7 à 18 de Julho de 2007.