Proposta para Implantação de um Backbone Colapsado em uma rede de médio porte

Paulo Henrique de A. P. Schindler

Departamento de Informática - PUC-Rio
Marquês de São Vicente 225, Rio de Janeiro, RJ - CEP.: 22453-900
e-mail: pauloh@inf.puc-rio.br

I. INTRODUÇÃO

O Departamento de Informática (DI) da Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) teve um crescimento substancial nos últimos dois anos através de convênios mantidos tanto com empresas privadas (Itautec, IBM), quanto com empresas públicas (Petrobrás, Embratel). Atualmente o departamento conta com 4 laboratórios vinculados a projetos e 1 laboratório dedicado aos professores e alunos de graduação, mestrado e doutorado do DI, chamado genericamente de Lab-DI. Os 4 laboratórios dedicados a projetos são:

- TecGraf/ICAD - desenvolve atividades na área de computação gráfica;
- TeleMídia - desenvolve atividades na área de novas tecnologias de rede (ATM) aplicadas ao desenvolvimento de aplicações de Multimídia;
- LES - Laboratório de Engenharia de Software;
- LMF-DI - Laboratório de Métodos Formais do Departamento de Informática.

Todos estes laboratórios possuem sua própria equipe de suporte para administração de sua rede local. A equipe de suporte do Lab-DI, além de administrar as redes sob sua responsabilidade e cuidar de todas as máquinas pessoais de professores, corpo administrativo e técnico do Departamento de Informática, é ainda responsável pela integração de todas as redes locais de cada laboratório entre si e destas com a saída da PUC-Rio para a Rede Rio - atualmente feita através de um Cisco AGS+.

Existem, em média, 30 máquinas em cada um dos laboratórios descritos acima, além de outras 30 máquinas de uso pessoal de professores e staff do departamento, todas integradas em rede através de TCP/IP. A plataforma de hardware é muito diversificada. Existem estações de trabalho SUN (SLCs, Sparc Stations 2, 5 e 20), estações Axil (Axil 320 MP), estações RISC 6000 da IBM, estações Indy/Indigo 2 da Silicon Graphics, microcomputadores tipo PC e Macintoshes. Diferentes plataformas de hardware trazem como consequência diferentes plataformas de sistema operacional: SunOS 4.1.x, SunOS 5.x, AIX 3.2.5, Ultrix, MacOS, Irix 5.3, SCO Unix, DOS/W4W, Windows NT, Linux, Netware 3.11 e 4.1.

O trabalho que segue é resultado das discussões mantidas pelo grupo de segurança lógica do DI. Este grupo é composto de representantes da equipe de suporte de cada laboratório do Departamento de Informática, a saber:

- Paulo Henrique Schindler e Marcello Pignataro do Lab-DI
- Peter Hohl, Paulo Francisco Sedrez e Paulo Henrique Sant'Anna do TecGraf/ICAD
- Rodrigo Cardoso Uchôa do TeleMídia
- Cláudio Terra do LMF-DI
- Luís Fernando Barbosa do LES

Este grupo foi constituído com o objetivo de melhorar a segurança lógica dos equipamentos do Departamento de Informática, especialmente após invasões ocorridas em máquinas do Lab-DI e do TecGraf/ICAD. Cedo chegou-se a conclusão de que qualquer política de segurança seria de difícil implementação considerando-se o estado atual da rede. Como, devido ao surgimento de novos laboratórios e crescimento dos já existentes, a rede já se encontra perto do limite de sua capacidade, algumas mudanças no *layout* da rede física foram propostas. Estas mudanças permitirão uma melhoria do desempenho da rede a curto prazo e uma expansão gradual visando novas tecnologias a médio prazo. Este trabalho foi desenvolvido com o objetivo principal de tornar as redes do DI mais seguras.

II. *LAYOUT* ATUAL DA REDE DO DI

O *layout* atual das redes do Departamento de Informática pode ser visto na Figura 1.

A PUC-Rio possui endereços IP classe B (139.82.x.x) e máscara de rede igual a 255.255.255.192. Convencionou-se chamar as subredes 139.82.1.0, 139.82.2.0, 139.82.16.0 e 139.82.20.0 de rede 1, rede 2, rede 16 e rede 20, respectivamente.

O Cisco AGS+ da PUC-Rio está atualmente conectado à rede 1. A rede 1 é uma rede do tipo 10Base2, localizada no térreo do prédio do Rio Data Centro (RDC). A conexão das redes do prédio do Instituto de Tecnologia em Software (ITS) e 4º andar do RDC entre si, e de cada uma delas com o Cisco AGS+, é feita através de um PC 386DX executando o software pcroute, de domínio público. Este PC possui três interfaces de rede: uma conectando-o à rede 1, outra conectando-o à rede 2 e outra conectando-o à rede 16.

A rede 16 é do tipo 10Base2 e funciona basicamente como um backbone entre as redes do anexo e a rede 1 do RDC. Cada laboratório localizado no prédio do ITS tem um equipamento interligando sua rede à rede 16, podendo este equipamento ser um PC dedicado executando um software de roteamento de domínio público (ex.: LMF-DI, Tele-Mídia), um servidor Netware 3.11 roteando IP e IPX (ex.: Lab-DI), ou uma estação de trabalho Digital (ex.: TecGraf/ICAD).

Todos os laboratórios do ITS possuem apenas um ponto de acesso à rede 16, com exceção do TecGraf/ICAD, que possui 2. O esquema de cabeamento varia no caso da rede interna de cada laboratório:

- Ethernet Fino - RG58 (10Mbps): Lab-DI, TecGraf/ICAD;
- UTP Categoria 3 (10Mbps): rede 20;
- UTP Categoria 5 (100 Mbps): LMF-DI, TeleMídia e LES.

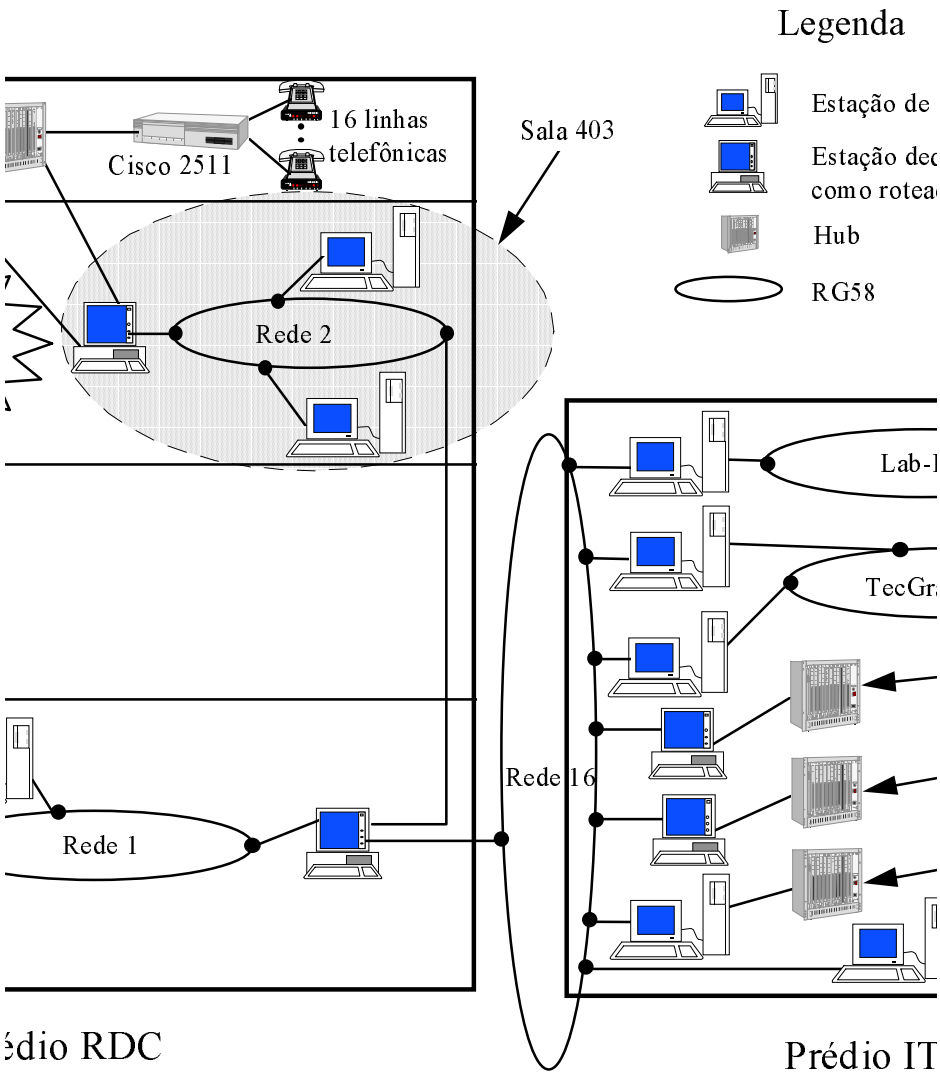
Legenda
Estação de
Estação dec
como rotea
Hub
RG58
16 linhas
telefônicas
Cisco 2511
Sala 403
Rede 2
Rede 1
Rede 16
Lab-I
TecGr
édio RDC
Prédio IT

Figura 1

A rede 2 é do tipo 10Base2 e serve basicamente para interligar a rede 20 do 4º andar às redes 1 e 16. Esta interligação é feita através de um PC 386SX dedicado, localizado em uma sala do 4º andar do RDC. Este PC também interliga a rede da Fundação Padre Leonel Franca (FPLF), 10Base2, à rede 1.

O *layout* atual possui diversas deficiências. A interligação entre todas as redes do ITS e a rede 1 é feita através de um cabeamento único e limitado a 10 Mbps. Este cabeamento transmite sinais elétricos, o que não é indicado na interligação entre prédios pois diferenças de potencial entre os terras dos prédios podem acarretar descargas elétricas e queimar transceivers/placas de rede, como de fato ocorreu em 1992.

A ligação entre a rede que atende quase todos os equipamentos do 4º andar (rede 20) e as redes 1 e 16 é feita através de um cabeamento único e limitado a 10Mbps (rede 2). Este cabeamento ainda tem que suportar a carga gerada por toda a Fundação Padre Leonel Franca, embora apenas parte da Fundação seja usuária das redes do Departamento de Informática - representada na figura como "DI 5º andar". Esta situação tende a piorar quando for instalado o servidor de comunicação Cisco 2511 porque mais 16 usuários a 14400 bps estarão utilizando a rede 2 e a rede 20 para acessar a Internet.

Finalmente é importante mencionar que as ligações entre todas as redes citadas acima são feitas, em sua maioria, através de microcomputadores PC não projetados para este fim, o que limita o desempenho da rede como um todo e torna extremamente difícil a implantação de mecanismos de segurança orientados a rede. Outra limitação surge como consequência destes PCs só conseguirem rotear IP, tornando impossível a integração de máquinas que executem softwares baseados em outro tipo de protocolo a nível de rede (IPX, AppleTalk, ...), a menos de soluções baseadas em mecanismos de *tunneling* em IP.

III. *LAYOUT* PROPOSTO

O *layout* proposto para a nova rede física do DI pode ser visto na Figura 2.

Neste novo *layout* existe um elemento central interligando todas as redes do Departamento de Informática e conectando-as diretamente ao Cisco AGS+ da PUC-Rio. A instalação do servidor de comunicação Cisco 2511 não acarreta carga adicional em nenhuma das redes já existentes.

A conexão do roteador central com o Cisco AGS+ é feita através de um cabo com dois pares de fibra ótica. A conexão do roteador central com o Cisco 2511 e Hub localizados no 5º andar do prédio RDC é realizada através de um cabo com 3 pares de fibra ótica. A presença de um par de fibra ótica adicional em cada ligação aumenta a confiabilidade da rede e permite expansões futuras. Os cabos condutores das fibras são de um tipo especial, resistente às condições de uso externo. A utilização de fibra ótica na ligação entre prédios elimina de uma vez por todas problemas ocasionados por diferenças de potencial entre terras.

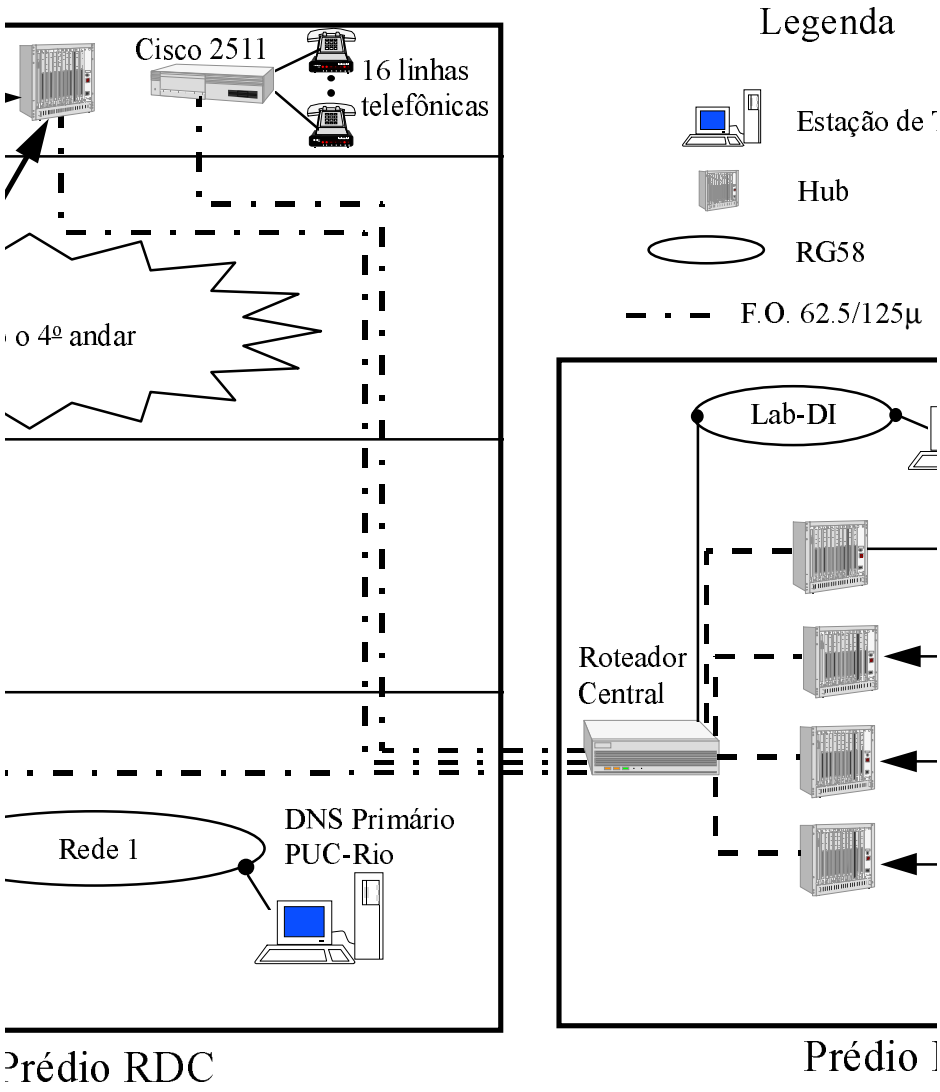
Legenda
Estação de
Hub
RG58
F.O. 62.5/125µ
Cisco 2511
16 linhas
telefônicas
o 4º andar
Lab-DI
Roteador
Central
Rede 1
DNS Primário
PUC-Rio
Prédio RDC
Prédio

Figura 2

A conexão do roteador central com cada uma das redes do ITS é feita através de cabos de par trançado sem blindagem (UTP categoria 5). Cada um destes cabos tem 4 pares, embora apenas dois sejam necessários. O equipamento de interface de cada laboratório com o roteador central é de responsabilidade do laboratório. Este equipamento pode variar desde um PC, passando por uma estação de trabalho, até um Hub ou um Switch, o que é mais indicado.

Todo o esquema de cabeamento proposto suporta velocidades de até 100 Mbps (Fast Ethernet), embora, a princípio, este será utilizado em taxa de transmissão menor - 10 Mbps. Porém caso, no futuro, seja realizado um upgrade mais amplo das redes, estas podem passar a operar a 100 Mbps sem alteração no sistema de cabeamento.

O roteador central é capaz de rotear IP, IPX, AppleTalk Phase 1/2 e outros protocolos (vide item IV.1), garantindo integração total entre máquinas que executam diferentes protocolos de rede.

IV. ALTERNATIVAS DE SOLUÇÃO EM TERMOS DE EQUIPAMENTO

Foram estudadas três alternativas para o roteador central: um Cisco 4500-M, um Cisco 4700 e um Cisco 7000. Estas alternativas estão em ordem crescente de desempenho, expansibilidade e custo.

IV.1 Características de cada alternativa

O Cisco 4500-M possui três slots para conexão de placas de interface de rede. Este atinge uma performance de 45.000 pps (pacotes por segundo), considerando-se que nenhuma filtragem de pacotes é realizada.

O Cisco 4700 também possui três slots para conexão de placas de interface de rede. Este equipamento é atualmente o topo de linha da família 4000, tendo sido lançado no segundo semestre de 1995. O Cisco 4700 utiliza tecnologia RISC e apresenta uma performance de 60.000 pps, na ausência de filtragem de pacotes.

Tanto no caso do 4500-M quanto no caso do 4700, existem placas de interface de rede para até 6 conexões RJ45 cada uma (NP-6E), o que totaliza 18 ligações possíveis de redes Ethernet. Destas 18 ligações, serão utilizadas imediatamente 9. Considerando-se atualizações tecnológicas da rede com a conexão deste roteador a um Switch ATM, um dos slots terá que ser utilizado para um módulo ATM. O número total de redes que pode ser conectado ao roteador diminui para 12, o que deixa apenas três entradas no roteador para futuras conexões.

Como consequência, propôs-se a seguinte política de alocação de portas no roteador central caso o escolhido fosse um Cisco 4500-M ou Cisco 4700: cada laboratório teria direito a apenas 1 porta no roteador central. Se o laboratório possuir mais de uma rede, cabe ao laboratório comprar um switch ou um roteador, conforme o caso, para atender as suas necessidades de expansão.

O Cisco 7000 possui 5 slots dedicados a módulos de interface, o que elimina problemas relacionados a expansibilidade da rede. Seu desempenho é de 200.000 pps, podendo chegar até 270.000 pps utilizando o módulo de switching SSP. O Cisco 7000 apresenta performance superior ao Cisco 4700, mas implementa filtragem de pacotes com menor eficiência. Quando se objetiva implementar segurança a nível de roteador, a Cisco recomenda o Cisco 7505 que atinge uma performance de 250.000 pps e possui 4 slots dedicados a módulos de interface. Tanto o Cisco 7000 quanto o 7505 permitem *hot-swap* dos módulos de interface.

Em termos de Sistema Operacional do roteador, a configuração que atende as necessidades do Departamento de Informática é a "Cisco IOS Desktop" que suporta os protocolos de rede IP, IPX (Netware), AppleTalk Phase 1, AppleTalk Phase 2, dentre outros.

IV.2 Alternativa escolhida

O Departamento de Informática da PUC-Rio resolveu implantar a solução baseada no Cisco 4700 basicamente por motivos de custo. Foi realizada uma cotação preliminar para todo o projeto junto a duas empresas - ETS e Sysnet. Os seguintes custos médios foram obtidos para cada uma das alternativas:

Roteador Central Utilizado	Custo Implantação Backbone (R$)
Cisco 4500-M	31.620,00
Cisco 4700	34.127,00
Cisco 7000	66.625,00

Como se pode verificar na tabela acima, o custo da solução utilizando o Cisco 7000 é quase o dobro do custo da solução utilizando o Cisco 4700.

Embora o critério principal de decisão tenha sido o custo, espera-se que a solução escolhida atenda as necessidades a médio prazo do Departamento de Informática. Considerando-se a pior alternativa possível em termos de tráfego atravessando o roteador, a saber:

a. Pacotes TCP com tamanho mínimo (40 bytes);
b. Todo o tráfego gerado por cada rede ethernet passando pelo roteador(*): 7 x (3000000 bps / 40 bytes) = 65.625 pps;
c. Todo o tráfego gerado pelo Cisco 2511 passando pelo roteador: 16 x (14400 bps / 40 bytes) = 720 pps.

(*) Considera-se, neste cálculo, uma taxa efetiva de transmissão de 3Mbps em vez da taxa teórica de 10 Mbps

O roteador estaria submetido a uma carga de 66.345 pps, embora sua capacidade máxima de processamento seja de 60.000 pps. Porém deve-se ressaltar que o cálculo realizado acima é extremamente pessimista pelos seguintes motivos:

- Considerou-se pacotes TCP de tamanho mínimo - que continham apenas o header IP e o header TCP. A grande maioria dos pacotes tem tamanho bem superior a 40 bytes. Por exemplo: considerando-se pacotes de 80 bytes, a carga gerada no roteador decresce para 33533 pps.
- Considerou-se que a carga gerada por todas as redes ethernet passa pelo roteador. Com exceção da rede que contem o servidor de comunicação Cisco 2511, este fato não é verdadeiro, dado o alto grau de independência de cada uma das redes do Departamento de Informática.

O desempenho do Cisco 4700 no caso de implantação de políticas de segurança que demandem filtragem de pacotes a nível de roteador será avaliado após a implantação das mesmas.

V. CONSIDERAÇÕES A RESPEITO DE SEGURANÇA LÓGICA

Neste item procura-se descrever de forma ampla as alternativas estudadas em termos de segurança lógica. A escolha de uma das propostas apresentadas reflete a política de segurança adotada. As alternativas apresentadas se basearam nos diferentes tipos de arquitetura de *firewalls* mencionados em "Building Internet Firewalls"[1].

Em termos gerais, uma política de segurança deve ter como premissas os seguintes questionamentos [2]:

- Quão importantes são os recursos ?
- Qual a probabilidade de ocorrência de uma invasão ?
- Que recursos serão protegidos ?
- Contra quem estes serão protegidos ?
- Que preço estamos dispostos a pagar pela proteção dos recursos ?

Entenda-se por preço a pagar não apenas investimentos na compra de equipamentos como também o tempo gasto na configuração dos equipamentos, o tempo gasto na manutenção da política de segurança, a queda de desempenho e do grau de conectividade das ligações entre estações internas à rede protegida e estações externas, etc..

Todas as alternativas propostas buscam proteger informações internas, com médio grau de confidencialidade, de usuários externos. Consideram-se usuários externos aqueles que não estejam devidamente autorizados a utilizar as redes do Departamento de Informática: usuários de outros departamentos ou usuários externos à própria PUC-Rio.

Para a compreensão das alternativas a serem apresentadas, torna-se necessário definir alguns conceitos [1,2,3].

Firewall

> Conjunto de componentes que restringem a comunicação entre uma rede interna e a Internet ou entre diversas redes internas, com o propósito de implantar uma política interna de segurança.

Para que um *firewall* cumpra o seu papel, é obrigatório que todo o tráfego entre as redes de acesso restrito e as redes de acesso irrestrito passe através dele.

Bastion Hosts

> Qualquer estação que funciona como o principal ponto de contato entre usuários externos e a rede de acesso restrito.

Por estarem expostos a acessos diretos, os *bastion hosts* se constituem em um dos pontos críticos, em termos de segurança, de toda a rede de acesso restrito. Estes devem possuir o menor número possível de softwares instalados, para diminuir a probabilidade de furos de segurança decorrentes de bugs ou de interações imprevistas entre os softwares. Auditorias devem ser realizadas frequentemente (de preferência, diariamente), com verificação dos logs gerados visando descobrir possíveis tentativas de invasão.

Packet Filters ou Screening Routers

> Equipamentos capazes de, a partir das informações contidas no pacote roteado, fazer distinção e impor restrições aos diferentes tipos de tráfego de rede, de acordo com os endereços de origem e destino da comunicação, e de acordo com o tipo de protocolo utilizado na transmissão das informações.

Proxy-server

> Programa que funciona como elo na comunicação entre clientes internos a rede de acesso restrito e servidores externos. Os clientes internos são chamados de *proxy-clients*.

O objetivo de um *proxy-server* é permitir a qualquer usuário da rede de acesso restrito se comunicar com um servidor externo sem que o usuário interno nem o servidor externo percebam - a menos de uma queda no tempo de resposta da transação - que a comunicação está sendo feita de forma indireta. Proxy-servers são geralmente instalados em *bastion hosts*, passando estes a funcionarem como gateways a nível de aplicação.

Perimeter Network

Rede localizada entre uma rede de acesso restrito e as redes externas, com o objetivo de criar uma barreira adicional contra invasões externas.

A seguir, apresenta-se as arquiteturas de *firewalls* consideradas.

V.1 Alternativa 1: *Screened Host Architecture*

Este tipo de arquitetura pode ser visto na Figura 3.

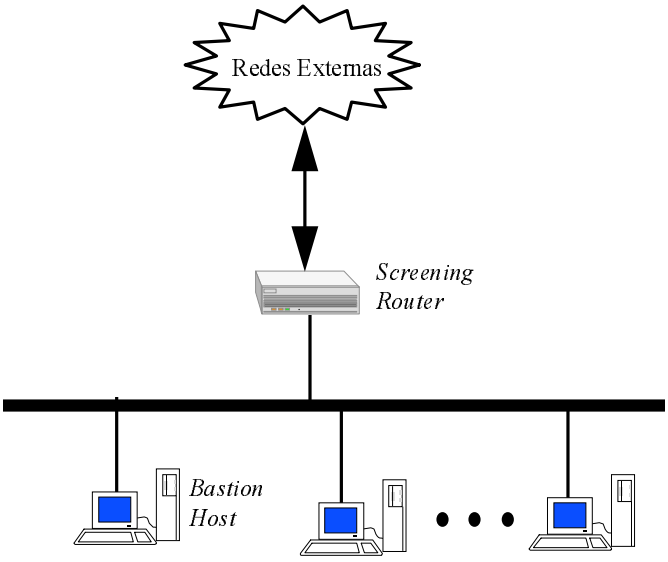

Figura 3

O *screening router*, que aparece na figura, pode ser configurado para permitir que máquinas internas à rede de acesso restrito possam se comunicar com máquinas externas, no caso de alguns tipos de serviços. Outra possibilidade consiste em configurar o *screening router* de forma a bloquear qualquer transação direta entre máquinas internas e externas. Neste caso, a única comunicação possível é feita através de *proxy-servers* instalados no *bastion host*.

Esta arquitetura apresenta um grande inconveniente: o *bastion host* se conecta diretamente à rede de acesso restrito. Uma vez comprometida a segurança do *bastion host*, a segurança de toda a rede interna está comprometida.

V.2 Alternativa 2: *Screened Net Architecture*

Esta arquitetura consiste em um melhoramento da arquitetura anterior na medida em que o *bastion host* está conectado diretamente a uma *perimeter network*, e não à rede de acesso restrito, conforme pode ser visto na Figura 4. O *screening router* pode ser configurado de forma a permitir apenas alguns tipos de comunicação entre o *bastion host* e estações localizadas na rede de acesso restrito. Este fato permite que o

comprometimento da segurança do *bastion host* não acarrete imediatamente um comprometimento da segurança da rede de acesso restrito - embora seja provável que este fato eventualmente ocorra.

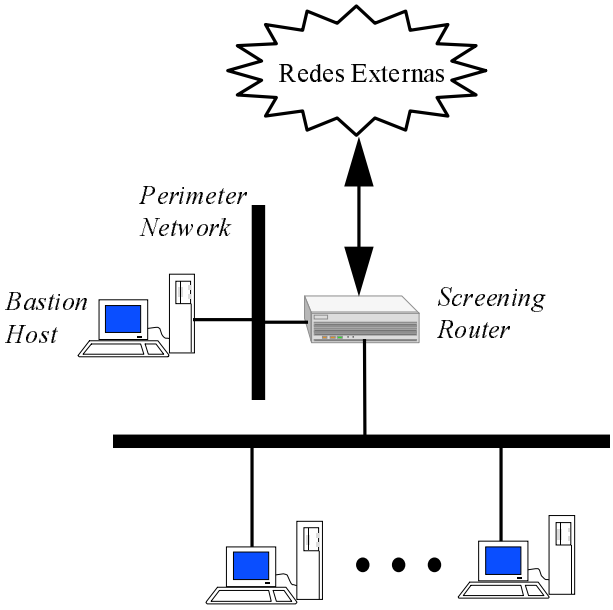

Figura 4

V.3 Alternativa 3: *Dual-Homed Host Architecture*

Neste tipo de arquitetura, uma estação é colocada entre a rede de acesso restrito e a rede externa, conforme pode ser visto na Figura 5.

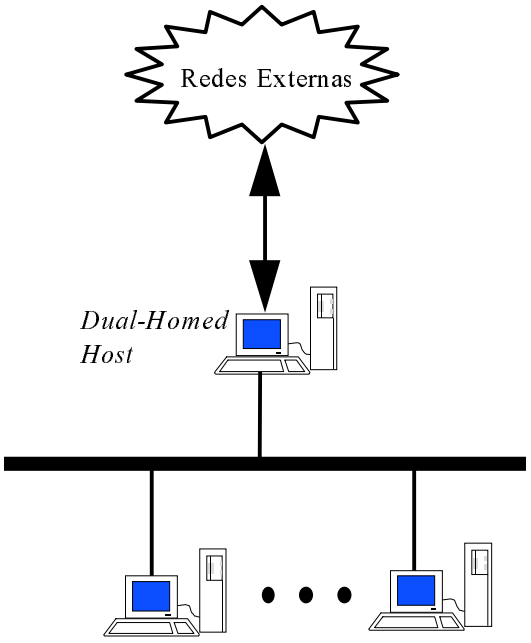

Figura 5

Um *dual-homed host* não realiza roteamento. Estações localizadas na rede de acesso restrito podem se comunicar com o *dual-homed host*. Estações externas podem se comunicar com o *dual-homed host*. Porém estações internas e externas não se comunicam diretamente.

Esta arquitetura oferece um maior isolamento da rede de acesso restrito em comparação com as arquiteturas anteriores na medida em que a comunicação pode ser controlada de forma mais discreta. Por exemplo: na arquitetura *dual-homed host*, certos comandos utilizados dentro de uma sessão de ftp podem ser bloqueados e outros liberados. Em uma arquitetura que utiliza *screening routers*, geralmente só existe a possibilidade de se bloquear a transação como um todo e não partes da mesma.

Esta arquitetura apresenta dois inconvenientes. Em primeiro lugar, o desempenho da comunicação entre a rede de acesso restrito e as redes externas fica extremamente prejudicado, já que um *dual-homed host* não apresenta o mesmo desempenho que um *screening router*. Em segundo lugar, a arquitetura *dual-homed host* apresenta o mesmo ponto crítico em termos de segurança que a arquitetura *screened host* - uma vez comprometida a segurança do *dual-homed host* a segurança de toda a rede está comprometida.

V.4 Alternativa escolhida

Nenhuma das alternativas apresentadas são excludentes do ponto de vista de compra de equipamento.

O Departamento de Informática da PUC-Rio decidiu, em uma primeira etapa, implantar a alternativa 1, por ser a de menor custo. Após testes e análise dos resultados obtidos, pode-se pensar em implantar a alternativa 2, com um *bastion host* para cada laboratório localizado em uma *perimeter network*, conforme Figura 6.

A médio prazo o Departamento de Informática não prevê a necessidade de se implantar a alternativa 3.

VI. CONCLUSÃO

Este trabalho propõe a melhoria do nível de segurança lógica das redes do Departamento de Informática da PUC-Rio através da implantação de mecanismos de segurança a nível de rede. Com o *layout* atual, é extremamente difícil a implantação de quaisquer mecanismos de segurança, a não ser aqueles orientados a estação, o que é inviável em uma rede de médio porte como a do DI. Para se obter o nível de segurança desejado, foi necessário propor mudanças no *layout* que trouxeram consigo um aumento do desempenho da rede.

Por questões de custo, foi escolhido como roteador central o roteador Cisco 4700 em detrimento do Cisco 7000 ou 7500. Cálculos simples permitem demonstrar que este roteador atende com sobra as necessidades do DI, desde que este não faça parte de um *firewall*. O impacto, em termos de desempenho, do uso do roteador Cisco 4700 como *screening router*, só poderá ser avaliado a posteriori.

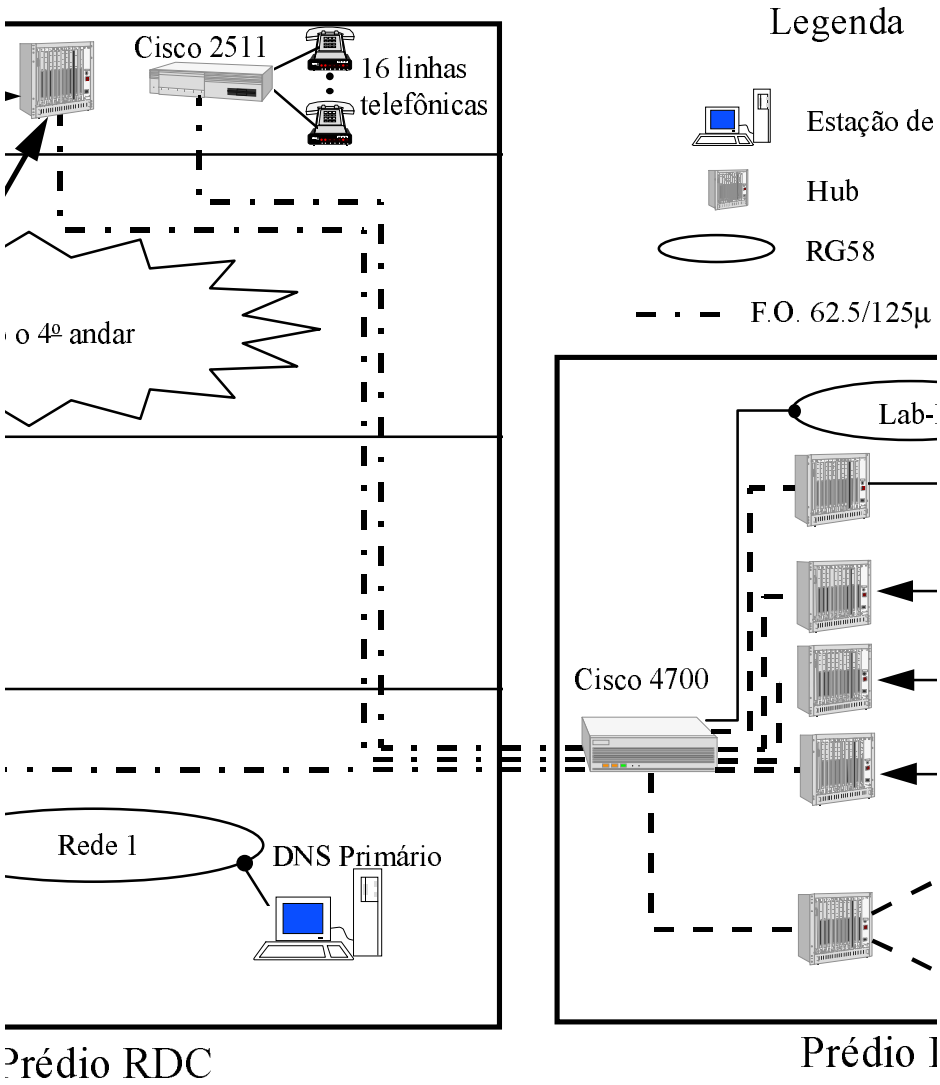
Legenda
Estação de
Hub
RG58
F.O. 62.5/125µ
Cisco 2511
16 linhas
telefônicas
o 4º andar
Lab-
Cisco 4700
Rede 1
DNS Primário
Prédio RDC
Prédio 1

Figura 6

BIBLIOGRAFIA

[1] Chapman, D. Brent; Zwicky, Elizabeth D.; "Building Internet Firewalls"; O'Reilly & Associates, 1995.

[2] Cheswick, Willian R.; Bellovin, Steven M.; "Firewalls and Internet Security - Repelling the Wily Hacker"; Addison-Wesley Professional Computing Series, 1994.

[3] Siyan, Karanjit; Hare, Chris; "Internet Firewalls and Network Security"; New Riders Publishing, 1995.