Um framework para Voz sobre IP orientado às Redes Convergentes e Seguras baseadas em Firewalls/NATs

Gustavo Passos Tourinho, Jorge Guedes Silveira, Ricardo Balbinot, Alexandre Vieira, Roberto Costa Filho

***Resumo* – A principal preocupação de instituições é com a segurança das informações. Diversos dispositivos são usados para garantir segurança, como, Firewalls, NATs, etc. Entretanto, tecnologias como Voz sobre IP apresentam incompatibilidades quando usada com os recursos descritos. Este artigo apresenta um Framework para resolver o problema de incompatibilidade e garantir a segurança da rede.**

***Palavras-Chave* – Firewall, Framework, H.323, Telefonia IP, MIDCOM, Middlebox, NAT, Segurança, SIP, VoIP.**

***Abstract* - The main concern in worldwide enterprises and academic institutions is on information security. Many resources can be used to supply security like Firewalls, IDS, NAT and others. However, new technologies like voice over IP (VoIP) present inherent problems when used in environments that use such technologies. This paper presents a Framework that was implemented in order to solve those problems regarding VoIP applications without compromising any of the security infrastructures already present in a data network environment.**

***Index Terms:* Firewall, Framework, H. 323, IP Telephony, MIDCOM, Middlebox, NAT, Security, SIP, VoIP.**

I. INTRODUÇÃO

A utilização da Telefonia IP continua crescendo no mundo empresarial e acadêmico devido às já comprovadas vantagens, técnicas e econômicas, que esta arquitetura pode trazer frente à convergência e integração de todos os serviços sobre uma mesma infra-estrutura. Entretanto, existem ainda muitas barreiras técnicas que necessitam ser resolvidas antes que esta arquitetura seja implantada, de forma simples, sobre um ambiente de rede IP já existente sem que ela venha a comprometer a segurança da rede ou obstruir a implementação de novos serviços.

Um dos problemas mais importante diz respeito à presença, nas redes, de dispositivos como Firewalls e NATs, utilizados freqüentemente em instituições públicas ou privadas tanto para garantir a segurança da rede, no caso de Firewalls, como para resolver problema de escassez de endereços IP, no caso de NAT, ou ainda um misto dos dois. A principal dificuldade encontrada em ambientes de voz sobre IP (VoIP), quando se utilizam tais dispositivos, é a extinção da conexão ponto-a-ponto; ou seja, toda conexão deve passar por eles para chegar ao seu destino e vice-versa.

Como em tráfego multimídia é utilizada uma faixa randômica de portas para a conexão [1], o Firewall deveria permitir que toda esta faixa fosse habilitada para possibilitar o tráfego na mesma. No entanto, isto implicaria em uma drástica redução da segurança da rede.

Um outro ponto importante a ser considerado diz respeito às informações contidas no *payload* do pacote. Ele contém informações úteis para o estabelecimento da conexão, porém, ao transpor o NAT apenas as informações do header são alteradas, o que ocasionaria uma incoerência dos dados.

Assim, para permitir a utilização de tais dispositivos em conjunto com as aplicações voz em telefonia sobre IP, foi especificado e implementado uma arquitetura, decomposta de Firewall/NAT onde, no entanto, podem ser identificadas entidades terceiras, que interagem diretamente com tais dispositivos no intuito de viabilizar e de realizar o tráfego multimídia. Este é, na realidade, o papel principal destas entidades, entre as quais podemos incluir os agentes MIDCOM e os proxies SIP.

Para melhor entendermos o Framework que foi especificado, apresentamos nesta sessão uma descrição sucinta de todos os dispositivos que são suportados pela arquitetura implementada.

A. Firewall

Um Firewall é ser definido em [2] como um conjunto de programas e dispositivos, geralmente localizados na borda de uma rede privada, tendo como tarefa principal a segurança dos dados mantidos na rede interna através da criação de barreiras (ou muros) para usuários externos à rede. Geralmente é implementado em conjunto com um programa de roteamento, podendo ser interno ou externo a esse dispositivo. Sua tarefa é examinar cada pacote que irá passar através dele e comparar as informações deste com uma tabela, pré-definida, de políticas de acesso. Ou seja, o pacote só poderá entrar ou sair da rede se estiver explicitamente permitido na tabela de acesso.

Gustavo Passos Tourinho, Jorge Guedes, Ricardo Balbinot, Alexandre Vieira, Roberto Costa Filho, PPGEE – FENG – PUCRS - Laboratório GPARC-TI - Avenida Ipiranga, 6681 – Porto Alegre – RS – Brasil, E-Mails: {gtourinho, jguedes, rbalbinot, atvieira, rcosta}@gparc.org. Este trabalho está sendo financiado pela CAPES/CNPC em parceria com a PUC-RS – FENG.

B. Network Address Translator

O NAT realiza a tradução de um endereço IP utilizado dentro de uma determinada rede para outro endereço IP diferente, conhecido e válido na outra rede [3]. Geralmente ele é usado em conjunto com um Firewall, mas isso não é uma obrigação, embora a ação de ambos reforce ainda mais a segurança da rede. Outra utilização, que inclusive originou o NAT, se refere à escassez de endereços IP válidos. Ele divide o ambiente de trabalho em uma rede interna, onde geralmente são usados endereços IP falsos (192.0.0.1 ou 10.0.0.1) e uma rede externa, usualmente a Internet, onde são usados endereços ditos válidos ou verdadeiros (200.134.17.123). Sua tarefa é realizar o mapeamento dos pacotes que saem da rede interna (192.0.0.1) para a rede externa (200.13.17.123) alterando o cabeçalho do mesmo, de modo a ser válido na rede (Internet) e vice-versa.

C. Application Level Gateways ou ALGs

ALGs [4] são entidades que possuem a inteligência específica de alguma aplicação e também o conhecimento dos serviços associados a ela. Sua tarefa é a de examinar o tráfego da aplicação em trânsito e de auxiliar o correspondente serviço em suas funções. Por exemplo, um ALG implantado em um serviço NAT deve examinar os pacotes e, se necessário, realizar alterações para que o NAT seja capaz de executar suas operações de forma mais simples e correta. O ALG pode ser tanto interno ao serviço ao qual ele está auxiliando, quanto externo, ao trocar mensagens via um protocolo apropriado em prol de beneficiar o serviço em questão.

No entanto, os ALGs são diferentes de Proxies pois eles são invisíveis para usuários finais, bem ao contrário dos Proxies que são agentes de encaminhamento e terminam sessões com ambos os usuários finais (ponto-a-ponto). Entretanto, o ALG pode, opcionalmente, modificar o conteúdo do *payload* para facilitar o fluxo dos pacotes da aplicação pelo serviço em questão, por exemplo, NAT.

D. Middlebox

Um Middlebox é um dispositivo de rede intermediário que implementa um ou mais serviços [5], que podem ser operações de NAT ou Firewall, por exemplo. Logo, um Middlebox NAT é um Middlebox implementando um serviço NAT. Geralmente eles possuem inteligência sobre a aplicação embutidas no dispositivo para suportar uma transposição específica da aplicação. Os dispositivos Middlebox que suportam o protocolo MIDCOM [6] têm a capacidade de permitir que a inteligência da aplicação fique nos Agentes MIDCOM, externas ao Middlebox.

E. Agentes MIDCOM

Agentes MIDCOM [5] são entidades que realizam funções ALG e estão logicamente externas aos Middlebox. São essas entidades que realizam a interação com os Middlebox, podendo fazer isso com um ou mais dispositivos Middlebox.

F. MIDCOM PDP

MIDCOM Policy Decision Point é antes de tudo um Ponto de Política de Decisão, sendo também utilizado como política de repositório, segurando perfis de política relacionados com MIDCOM para tomar decisões de autorização. O PDP é uma entidade lógica que realiza políticas de decisões para si ou para outros elementos da rede que necessitam de tais decisões. É também um armazenador de dados específicos, que mantém regras de políticas, suas condições e ações.

A comunicação entre o PDP e um Middlebox pode ser feita se a política de um PDP mudar ou se o Middlebox necessitar de mais informações. Portanto o MIDCOM PDP pode, a qualquer momento, notificar o Middlebox para terminar a autorização para um determinado agente.

G. Demilitarized Zone

DMZ [7] é uma área neutra que separa a rede local privada da rede externa ou pública, prevenindo assim, que usuários externos tenham acesso direto aos dados internos da instituição. Uma configuração típica de DMZ pode ser exemplificada por um computador que recebe as requisições dos usuários internos e realiza a conexão, agindo então como um servidor Proxy. O host DMZ não pode iniciar uma sessão externa para dentro da rede privada, ele pode apenas encaminhar os pacotes que já foram requisitados pelos usuários internos.

Os usuários da rede pública externa somente podem acessar o host DMZ. Ele tipicamente possui as páginas da instituição, através de um Middlebox Web Server, que serão abertas e servidas para o público e nenhum outro dado com maior importância. No caso de uma quebra da segurança, apenas tais páginas, que funcionam como um portal virtual propositalmente limitado no acesso, sofrerão alterações, no entanto os dados internos mais importantes continuarão protegidos na rede privada.

II. PROTOCOLOS MULTIMÍDIA

Os protocolos multimídia possuem algumas peculiaridades que, de certa forma, prejudicam ou atrapalham o funcionamento de dispositivos de rede como Firewalls e NAT. A seguir, é apresentada a atual incompatibilidade destes protocolos com o ambiente de rede seguro.

A. Preparo e Sinalização de Chamada

Os protocolos mais usados para voz e vídeo sobre IP são SIP, H.323, MGCP e Megaco, que utilizam tanto o TCP quanto o UDP para preparar a chamada. Em todos esses protocolos, o endereço IP usado na negociação da chamada é embutido em suas mensagens, ou seja, no "*payload*" e isto pode ocasionar certa incoerência nos dados transmitidos.

Um problema identificado justamente neste escopo diz respeito aos Firewalls, que possuem regras específicas de filtragem e contém portas estáticas, através das quais os dados desejados obtêm permissão para passar. O H.323,

por exemplo, utiliza portas alocadas dinamicamente e sobre uma grande faixa. Portanto, como é inviável de se especificar, no Firewall, que em toda essa faixa de portas seja permitido tráfego, ele irá bloquear as mensagens do protocolo e a sinalização da chamada certamente irá falhar.

Podemos também encontrar um problema similar no NAT. Um agente A ou "SIP User Agent (UA) A", dentro de uma rede privada e atrás de um NAT, envia uma mensagem INVITE para um "User Agent B", que está localizado externamente na rede pública. Ao receber a mensagem, este agente B extrai o endereço contido no campo de informação do pacote e envia uma outra mensagem com 200 (OK) para o respectivo endereço da origem.

Pelo fato do agente A estar localizado atrás de um NAT, o pacote do "User Agent A" deve ser transmitido através do NAT, sendo assim, apenas o cabeçalho do pacote será modificado e não haverá nenhuma outra alteração no *payload*, ou seja, a resposta do agente B (User Agent B), será então direcionada para um endereço privado (192.0.0.1 ou 10.0.0.1), bem como a conexão não será estabelecida.

III. ESPECIFICAÇÃO DE UM FRAMEWORK

Com o objetivo de resolver os problemas levantados em relação à transposição de Firewalls e NATs por tráfego de voz, de vídeo e de sinais multimídia, optamos por especificar e implementar um Framework orientado à telefonia IP, no qual são utilizadas todas as técnicas e tecnologias citadas anteriormente. Nesta seção será apresentado como elas se inter-relacionam e, sobretudo, as interfaces e entidades que foram criadas para viabilizar a arquitetura que foi implementada.

A. Interface para Agentes MIDCOM e Middlebox

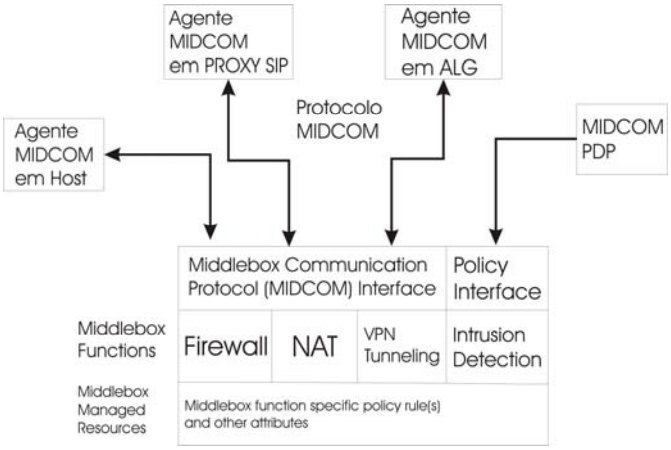

Fig. 1. Interface entre Agentes MIDCOM e Middlebox

A figura 1 acima, ilustra como os dispositivos que compõem o Framework de VoIP interagem entre si, e onde é possível identificar que existem diversos tipos de dispositivos Middlebox, além dos mostrados na figura.

A utilização do protocolo MIDCOM permite certa robustez na troca das informações devido a alguns requisitos adicionais que são necessários para implementar o mesmo, como, por exemplo, a criptografia.

Para realizar qualquer comunicação entre um agente e um dispositivo Middlebox é necessário realizar a autenticação do agente através do PDP. Toda e qualquer mensagem trocada entre eles pode e deve ser criptografada para evitar ataques do tipo *man in the middle*.

O agente PDP, além de ser responsável pelas conexões que chegam ao Middlebox, possui também a autoridade para terminar uma determinada conexão a qualquer instante.

Todos os agentes funcionam na forma de *Daemons*, ou seja, eles não têm interação com o usuário e ficam executando suas operações continuamente, desde a inicialização do dispositivo até o seu completo desligamento.

B. Framework para ambientes VoIP

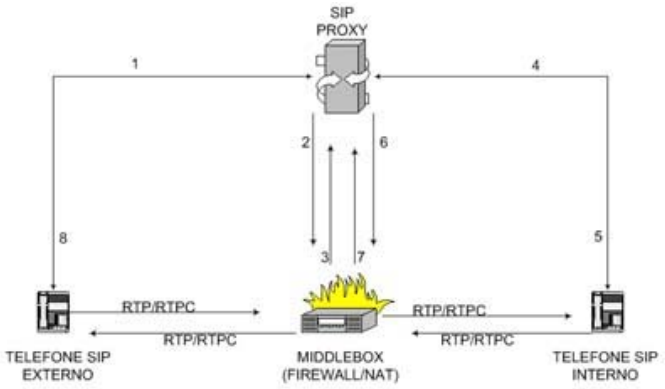

Fig. 2. Framework para ambientes VoIP

Na figura 2 acima é ilustrado como o ambiente protegido interage com suas entidades, de modo a permitir que a chamada telefônica possa ser completada com sucesso.

Inicialmente é feita uma requisição do telefone externo para um telefone interno. A troca de mensagens (SIP) entre os telefones e o Proxy é representada pelos números 1, 4, 5 e 8. Estas trocas de informações são realizadas com o intuito de transpor o Middlebox.

Os números 2, 3, 6 e 7 representam as trocas de mensagens entre o Proxy e o Middlebox, utilizando para tanto o protocolo MIDCOM. É exatamente nesse ponto preciso, quando são feitas as requisições para o Firewall permitir *pinhole*, que é executada a operação de abrir uma determinada porta para a comunicação e ao fim da operação fechar a mesma. Ou também, no caso de NAT, de realizar a troca das informações contidas no *payload* de modo a possuir informações coerentes no *payload* e no header do pacote recebido. Essa operação geralmente é feita com o auxilio de um ALG. O ALG irá receber o pacote SDP, utilizado para estabelecer a conexão e então, trocar as informações necessárias para realizar a comunicação. A seguir, o dispositivo ALG irá realizar uma

análise das informações armazenadas no seu conteúdo, e quando necessário, trocar o conteúdo da mensagem, de forma que esse pacote possa passar através do Firewall / NAT sem nenhum problema de incoerência nos dados.

A operação mais comum realizada pelo ALG, no caso de um pacote passando através do NAT, é a de realizar a tradução das informações contidas no pacote SDP, necessárias para estabilizar a conexão entre dois usuários de voz ou telefonia sobre IP. Essas informações geralmente são os endereços IP das máquinas em questão e de suas respectivas portas.

IV. VALIDANDO O FRAMEWORK

De forma a validar o protótipo do Framework, foram utilizadas diversas ferramentas para captura de tráfego, permitindo a avaliação do comportamento de cada pacote.

Com a utilização do ethereal [11], foi possível analisar os dados dos pacotes. Desta forma, assegurou-se que as entidades que compõem o Framework estavam modificando, de forma correta, as informações no *payload* do pacote, bem como foi possível verificarmos se essas informações estavam criptografadas. Garantindo assim, que mesmo o pacote sendo capturado por pessoas não autorizadas, estas não terão acesso às informações. Assegurou-se então, que os dados não serão obtidos de forma legível, senão pela entidade de destino.

Para validar as operações realizadas pelo Firewall, foi necessário um monitoramento constante do estado de suas regras, para os pacotes que chegam e saem da rede, para tal, utilizou-se um software de monitoramento de tráfego chamado etherape [12].

V. CONCLUSÃO

Identificou-se uma série de problemas com dispositivos que são essenciais nas redes de comunicação convergentes. Tais redes são capazes de suportar, sobre uma mesma infra-estrutura, tráfegos distintos como sinais de voz, vídeo, multimídia e dados. Recursos importantes para a segurança das redes de comunicação, como Firewalls e NATs, acabam causando transtornos inevitáveis quando as corporações desejam implantar sobre uma rede de dados protegida uma plataforma de telefonia IP.

Com o objetivo de abordar tais problemas, optamos por realizar um trabalho de especificação e de implementação completa de um Framework para VoIP ao qual foram adicionados, para integrar-se ao ambiente de rede, mais alguns dispositivos capazes de realizar operações de terceiros nos Firewalls e NATs. Os elementos de rede implementados são os agentes MIDCOM, que através do protocolo MIDCOM conseguem trocar mensagens com os dispositivos Middlebox (Firewall/NAT), com o intuito de realizar as operações necessárias para permitir um tráfego coerente através deles.

Esses novos dispositivos são transparentes para o usuário, pois toda a troca de mensagens necessária entre os agentes MIDCOM e os dispositivos Middlebox é realizada sem que o usuário tenha conhecimento da operação.

Portanto, a arquitetura implementada não é conflitante com o ambiente de rede seguro, ou seja, sua implementação não prejudica a proteção nem o funcionamento normal da rede de comunicação e pode ser utilizado tanto em redes de dados já operacionais quanto em novas redes convergentes onde o tráfego de voz deverá ter prioridade em relação ao tráfego de dados.

VI. BIBLIOGRAFIA

[1] KUO, F. *Multimedia Communications: Protocols and Applications.* Book News, Inc. Portland.

[2] WACK, J. *The Firewall Concept*. Available at http://csrc.nist.gov/publications/nistpubs/800-10/node31.html

[3] BILL, D. *The NAT handbook: implementing and managing network address translation.* John Wiley & Sons, Inc.

[4] JOHNSTON, A. *Understanding the Session Initiation Protocol.* Artech House, 2001. Norwood.

[5] SRISURESH, P. *Middlebox communication architecture and framework*. Available at http://www.ietf.org/rfc/rfc3303.txt?number=3303

[6] STIEMERLING, M. *MIDCOM Protocol Semantics*. Available at http://www.ietf.org/internet-drafts/draft-ietf-midcom-semantics-07.txt

[7] SHIMONSKI, R. *Building DMZs for Enterprise Networks.* Syngress Publishing, Inc. 2003 Rockland.

[8] RODRIGUEZ, A. *TCP/IP Tutorial and Technical Overview*. IBM Red Book, 2001.

[9] SWALE, R. *Middlebox Communications (midcom) Protocol Requirements*. Available at http://www.ietf.org/rfc/rfc3304.txt?number=3304

[10] HANDLEY, M. *SIP: Session Initiation Protocol*. Available at http://www.ietf.org/rfc/rfc2543.txt?number=2543

[11] ETHEREAL. *A Network Protocol Analyze.* Available at http://www.ethereal.com/

[12] ETHERAPE. *A graphical network monitor*. Available at http://etherape.sourceforge.net/