SSDR - FIREWALL RECONFIGURÁVEL: ARQUITETURA E DESEMPENHO EM FPGA

Edward D. M. Ordonez e *Fábio Dacêncio Pereira*

USP-Universidade de São Paulo
UNIVEM – Centro Universitário Eurípides de Marília
UEA-Benq, Manaus, Brazil

{fabiopereira, edmoreno}@univem.edu.br

RESUMO

Existem inúmeras técnicas, hardwares, softwares para promover a segurança de informações. Neste artigo é apresentado um Sistema de Segurança Dinamicamente Reconfigurável (SSDR) em FPGAs. O SSDR possui uma arquitetura robusta que permite a implementação de políticas de segurança específicas e gerais para garantir serviços como confidencialidade, autencidade, integridade, disponibilidade, controle de acesso e auditoria de informações. Os objetivos principais do SSDR são: garantir um bom nível de segurança atingindo um desempenho temporal aceitável e uma maior flexibilidade em relação à configuração de funcionalidades e às políticas de segurança. No artigo será apresentado o módulo de Firewall Reconfigurável destacando sua arquitetura, funcionalidades e desempenho de uma implementação em um FPGA Virtex 4.

1. INTRODUÇÃO

A segurança nas transmissões de informações torna-se cada vez mais importante, exigindo que novas técnicas, algoritmos e metodologias sejam desenvolvidas para promover um ambiente de transmissão seguro e veloz.

Neste contexto o artigo descreve um Sistema de Segurança Dinamicamente Reconfigurável (SSDR), apresentando em detalhes a arquitetura do módulo de Firewall Reconfigurável, assim como, o desempenho da implementação em FPGA.

Alguns sistemas de filtro de pacotes em hardware implementam um ambiente onde a memória de regras é customizada, podendo ser reconfigurada dinamicamente atraves de uma interface [7,8]. O difrencial do sistema proposto é a integração com outros serviços de segurança descritos na sequência.

O SSDR (Sistema de Segurança Dinamicamente Reconfigurável) possui uma arquitetura robusta que permite a implementação de políticas de segurança especificas e gerais para garantir serviços como confidencialidade, autencidade, integridade, disponibilidade, controle de acesso e auditoria.

Para isso, foi proposta uma arquitetura modular e interdependente, onde cada módulo de segurança possui autonomia para reconfiguração de políticas internas específicas, mas que por sua vez estão sujeitas às políticas gerais que determinam o funcionamento global do sistema, na seção 3 apresenta-se detalhes das políticas de segurança.

O sistema é composto por quatro módulos principais de segurança, estes são: o firewall [1,2,3,4], o processador criptográfico, o módulo de detecção de intrusão e o módulo de auditoria. É importante salientar que todos possuem políticas que podem ser reconfiguradas dinamicamente.

O módulo em destaque neste artigo será o Firewall Reconfigurável apresentando sua arquitetura, políticas e regras de segurança, funcionalidades, desempenho da descrição em VHDL implementada em um FPGA Virtex 4.

2. ARQUITETURA DO SSDR

O objetivo principal do SSDR é garantir um bom nível de segurança atingindo um desempenho temporal aceitável e uma maior flexibilidade em relação à configuração de funcionalidades e às políticas de segurança. Para isso o SSDR foi dividido em seis módulos principais descritos a seguir:

- **Processador Criptográfico Reconfigurável**: este módulo é capaz de implementar o algoritmo criptográfico desejado, onde poderão ser utilizados algoritmos simétricos, assimétricos e funções de hash. Uma vez definido o algoritmo criptográfico o dispositivo será reconfigurado dinamicamente (RTR -Run Time Reconfiguration) [5,6], para atender as necessidades imposta, respeitando limitações de espaço e mapeamento interno do FPGA.
- **Firewall Reconfigurável:** módulo responsável pelo controle de acesso das informações permitindo ou bloqueando o acesso a portas, IPs, MACs, Redes, etc. funcionando como um Firewall Reconfigurável.

A definição das regras de restrição/permissão será reconfigurada em tempo de execução (RTR) conforme a necessidade do usuário ou do sistema.

- **Módulo de Detecção de Invasão Reconfigurável**: este módulo tem a função de atuar como uma sentinela do sistema detectando possíveis invasões com base em uma política definida.
- **Módulo de Auditoria Reconfigurável:** Caso houver uma invasão do sistema ou por determinação do usuário este módulo irá gerar relatórios com informações sobre todos os acessos realizados.
- **Módulo de interface com a rede:** Este módulo é capaz de realizar a interface com o ambiente de rede, sendo capaz de desmembrar os pacotes recebidos ou transmitidos fornecendo informações importantes aos módulos de segurança.
- **Unidade de controle:** organiza e sincroniza a execução e determina políticas de segurança gerais.

Na figura 1 tem-se a descrição *top-level* do SSDR destacando os módulos citados anteriormente.

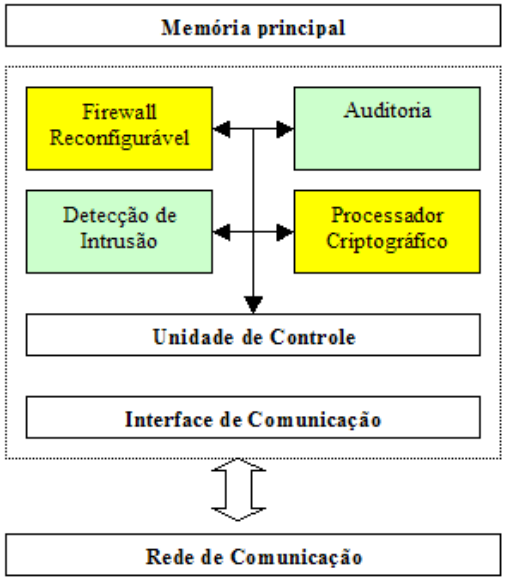

Figura 1 – Sistema de Segurança Dinamicamente Reconfigurável

3. POLÍTICAS DE SEGURANÇA

A flexibilidade de configuração das políticas de segurança é uma das vantagens do SSDR. Através destas políticas é possível estabelecer as regras de segurança de cada módulo do sistema, assim como as configurações gerais.

Políticas Internas: cada módulo pode ser configurado individualmente com suas regras particulares. O firewall poderá ser configurado com regras bloqueio e permissão de pacotes por IP, MAC, Intervalo de IPs ou uma Rede e Portas. O módulo de detecção de intrusão poderá ser reconfigurado com a política adequada sendo mais rígido ou mais flexível. O módulo de auditoria poderá ser configurado em nível de detalhes de informações que serão analisadas. O processador criptográfico pode ser reconfigurado inicialmente com os algoritmos AES, RSA e SHA-1, outros algoritmos poderão ser adaptados e integrados ao SSDR.

Políticas Gerais: Apesar de cada módulo ter sua autonomia, existem as políticas gerais do sistema que têm a função de criar um protocolo de comunicação entre os módulos citados. Assim, após definida e configurada uma política interna inicial pode-se estabelecer como os módulos irão se interagir e como as informações serão disponibilizadas para o usuário.

Um exemplo simplificado de configuração de uma política de segurança para o SDDR será descrito na seqüência:

- Inicialmente configura-se o módulo de Firewall bloqueando tudo (*block all*) e permitindo as portas 80 e 21 e o IP 192.168.0.25.
- O módulo de detecção de invasão terá uma configuração simplificada que identifica ataque por pacotes ICMP maiores de 1K (*Ping of Death*) que tem a função de tirar servidores de funcionamento.
- O processador criptográfico será configurado com o algoritmo AES, com cifragem completa da transmissão.
- O módulo de auditoria será configurado para uma captura de acessos as portas 80 e 21 (liberadas pelo firewall)

Após configurar individualmente cada módulo será realizada a configuração da política geral. Como por exemplo: Quando o módulo de detecção de invasão identificar alguma anomalia as informações serão publicadas pelo módulo de auditoria e será criada uma nova regra para o firewall bloqueando o IP que apresentou problema.

A possibilidade de configuração individual dos módulos e a configuração da política geral permitem inúmeras configurações para atender especificamente cada situação e ambiente. A flexibilidade [7] atingida pelo SSDR considerando que este será completamente implementado em hardware e o bom desempenho alcançado por cada módulo torna o SSDR um sistema de segurança robusto que integra os principais serviços de segurança.

4. FIREWALL RECONFIGURÁVEL

Este módulo tem importância fundamental para o SSDR e para qualquer sistema de segurança. Existem inúmeros códigos maliciosos que utilizam portas e interfaces de comunicações disponíveis para transitar informações não autorizadas capturadas da máquina hospedeira. Uma das formas de bloquear esse tipo de invasão é a utilização de um firewall com regras bem definidas para um determinado ambiente e/ou políticas de segurança de uma organização.

Na seqüência tem-se a descrição detalhada da arquitetura do firewall reconfigurável, as regras de

restrições e permissões e a análise de desempenho deste módulo.

4.1 Arquitetura do Firewall Reconfigurável

Nesta seção é apresentada a arquitetura do Firewall Reconfigurável descrita na figura 2. O firewall é composto basicamente por um buffer de entrada, um analisador de regras, um buffer de pacotes analisado (BAR), registradores de controle e uma memória RAM.

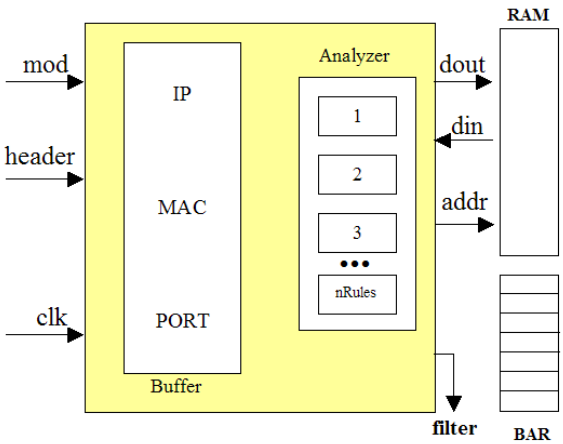

Figura 2 – Top-level do Firewall Reconfigurável

O Firewall, assim como os demais módulos, são alimentados pelo módulo de interface de rede responsável em processar os pacotes e organizar as informações necessárias para cada módulo. Na seqüência tem-se a descrição do funcionamento básico das unidades de Firewall:

- Firewall Reconfigurável recebe do módulo de interface de rede o *header* contendo IP, MAC e PORT armazenando estes dados no *buffer* de entrada.
- *mod* identifica o pacote como de saída ou entrada no sistema.
- O módulo Analyser verifica o buffer de pacotes analisados (BAR). Se o pacote atual é reincidente, pode-se decidir o bloqueio ou permissão deste ainda neste estágio, senão segue para o próximo estágio.
- O Analyzer busca na memória RAM as regras de restrição e permissões criadas pelo usuário.
- Analyzer compara as regras com os dados de armazenados no buffer de entrada julgando se o pacote será aceito ou bloqueado.
- Finalmente é gerada a saída *filter*, bloqueando ou não o pacote.

Tratamentos especiais:

Reincidência de pacotes bloqueados: Uma vez analisado um pacote este é enviado para o buffer de pacotes analisado. Caso houver a reincidência do pacote este será bloqueado/permitido sem realizar a análise das regras novamente. Se o conjunto de regras for modificado a lista de pacotes bloqueados é excluída.

CR (Rules Counter): é um registrador controla o número de regras ativas para o *Analyzer* não realizar testes desnecessários. Este é atualizado a cada regra inserida ou excluída.

Memória RAM customizada: A memória RAM possui dimensões personalizadas com o intuito de melhorar os mecanismos de busca permitindo o acesso uma regra completa em um único ciclo. A RAM é capaz de armazenar 32 regras de 96 bits.

4.2 REGRAS DE RESTRIÇÕES/PERMISSÕES

Nesta seção descreve-se como implementar as regras do Firewall Reconfigurável. Estas regras serão inseridas na memória RAM, onde a ordem de inserção é muito importante, pois esta seqüência irá determinar a prioridade de cada regra. A regra armazenada na última posição terá prioridades sobre as demais. A seguir o formato das regras:

3 bits	128 bits	1 Bit	1 Bit
ID	**IP / MAC / NET / PORT**	**I/O**	**A/B**

ID: Identifica a Regra (1-IP, 2-MAC, 3-NET, 4-PORT, 5-AlowAll, 6-BlockAll).

IP / MAC / NET / PORT: Descreve o IP, MAC, NET ou PORT que será filtrado.

I/O: Define se a regra será para pacotes de entrada(1) ou de saída (0).

A/B (Allowed/Blocked) define se é uma regra de bloqueio(1) ou permissão(0).

Através do formato especificado é possível criar um conjunto de regras para filtrar os pacotes em uma comunicação. Assim na seqüência tem-se um exemplo de regras simplificadas para bloquear todos os pacotes de saída liberando apenas a porta 80 e 21.

	ID	IP / MAC / NET / PORT	I/O	A/B
1.	6	XX	0	X
2.	4	80	0	0
3.	4	21	0	0

4. Análise de Desempenho

Nesta seção será apresentada a análise de desempenho do Firewall descrito em VHDL implementado em um FPGA Virtex 4. Serão analisados os itens tempo de propagação do circuito, taxa de utilização de componentes.

4.1 Taxa de ocupação no FPGA

Nesta implementação do Firewall Reconfigurável os testes do conjunto de pacotes já avaliados e a busca de regras na memória RAM são realizados seqüencialmente. Isso pode aumentar o tempo de análise degradando o desempenho do sistema, em contraste tem-se uma diminuição significativa de componentes utilizados na implementação.

Na primeira versão a unidade que mais consumiu componentes foi o *Analyser*, ocupando 55% da área total do circuito. A comparação entre as regras definidas pelo usuário e o cabeçalho do pacote que está sendo analisado não pode ser considerada complexa, mas exige uma quantidade significativa de SLICES CLBs do FPGA.

Percebendo este consumo excessivo de componentes foi implementada uma nova versão utilizando portas lógicas básicas (96 portas XOR e 96 portas OR e um comprador de 1 bit). A economia foi de 26% da área do circuito. Na tabela 1 apresenta-se o consumo de componentes do firewall reconfigurável implementado em um FPGA Virtex 4.

Tabela 1 – Taxa de ocupação do Firewall no FPGAVirtex 4.

	CLBs total	CLBs consumidas
Firewall	**5472**	**887(~16%)**

Desta forma, o Firewall Reconfigurável com processamento seqüencial é indicado para aplicações onde a disponibilidade de componentes é limitada.

4.2 Taxa de Propagação

A taxa de propagação do circuito implementado é uma das principais métricas para avaliar seu desempenho. O Módulo do Firewall Reconfigurável atingiu a uma Taxa de propagação de 5,865ns podendo atingir um *clock* global máximo de 170,515MHz. Com esse dado pode-se calcular o desempenho total do firewall no melhor e no pior caso.

Melhor caso: Pacote já foi analisado e esta na lista de pacotes reincidentes. Neste caso levaria 8 ciclos para a análise, ou seja, levaria 8x5,865 = 46,92ns.

Pior caso: Pacote nunca foi analisado e o usuário criou 32 regras. Neste caso o firewall irá verificar a lista de pacotes reincidente e analisar as 32 duas regras consumindo 234,6ns (8x5,865 + 32x5,865)

Para atingir a taxa de propagação de 5,865ns foi necessário criar algumas restrições de implementação. A síntese do circuito em modo padrão (*default*) realizada pelo software XST apresentou um tempo de propagação 8,829ns (113.267MHz), após aplicar algumas restrições personalizadas o desempenho melhorou atingindo em 5,865ns (170.515MHz), consumindo 2% a mais de unidades lógicas (CLBs).

Este desempenho foi considerado bom devido a complexidade e robustez do circuito. Como trabalho futuro pretende-se realizar a paralelização de funcionalidade, através de técnicas de *pipeline* e duplicação de unidades funcionais.

5. Conclusão

Neste artigo foi apresentado um Sistema de Segurança Dinamicamente Reconfigurável (SSDR), destacando o módulo do Firewall Reconfigurável. Foi apresentada sua arquitetura, políticas e regras de segurança e seu desempenho em um FPGA Virtex 4. O desempenho de 5,865ns atingido pelo Firewall pode ser considerado bom visto sua robustez e complexidade.

A reconfiguração de regras e políticas gerais do sistema aumenta a flexibilidade e a aplicabilidade permitindo a sua adequação em diversos ambientes.

A integração dos módulos de segurança (firewall, processador criptográfico, detecção de intrusão e auditoria) faz do SSDR um sistema robusto capaz de atender os principais serviços de segurança conhecidos.

6. Referências

[1] Feldhofer, M., Rapid Prototyping of a SPARC V8-based Firewall-on-Chip, AutroCHIP 2003.

[2] Kayssi, A. Harik, L. Ferzli, R. Fawaz, M. , FPGA-based internet protocol firewall chip , IEEE International Conference on Electronics, Circuits and Systems, ICECS 2000.

[3] Katayama, M., A 10Gb/s Firewall System for Network Security in Photonic Era, IEICE Transactions on Communications 2005.

[4] Alistair, A. McEwan, J. S., A High Speed Reconfigurable Firewall Based On Parameterizable FPGA-based Content Addressable Memories, Journal of Supercomputing, 2001.

[5] Hagemeyer, J., Kettelhoit, B., Porrmann, M., Dedicated Module Access in Dynamically Reconfigurable Systems, RAW'2006, 2006.

[6] Silva, M. L., Canas J., Exploiting dynamic reconfiguration of platform FPGAs: Implementation Issues, RAW'2006, 2006.

[7] Michael Attig and John Lockwood, SIFT: Snort Intrusion Filter for TCP, IEEE Symposium on High Performance Interconnects, 2005.

[8] T. K. Lee, et al, ,Irregular Reconfigurable CAM Structures for Firewall Applications, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, ISSN 0302-9743, Computer Science, Volume 2778/2003, Field-Programmable Logic and Applications, 2003.