|  |  |  |
| --- | --- | --- |
|  | UNIVERSIDADE FEDERAL DO CEARÁ  CENTRO DE TECNOLOGIA  DEPARTAMENTO DE ENGENHARIA DE COMPUTAÇÃO  CAMPUS DO PICI, CAIXA POSTAL 6007 CEP 60.755-640  FORTALEZA – CEARÁ - BRASIL  FONE (+55) 85 3366-9467 – FAX (+55) 85 3366-9468 |  |

**PROPOSTA DO PROJETO DE FINAL DE CURSO**

**I. Identificação**

|  |
| --- |
| Título:  Projeto de um IP Soft Core para Detecção de Ataque DDoS |
| Aluno:  Pedro Lucas Falcão Lima |
| Prof. Orientador (Departamento): Ricardo Jardel Nunes da Silveira  Co-Orientador: |

**II. Objetivo**

|  |
| --- |
| Este projeto objetiva realizar um estudo conceitual e também prático de um método específico de detecção em tempo real de ataques do tipo DDoS, bem como avaliar o rendimento desse método mediante a outras análises já existentes. O referido método foi concebido para ser implementado de maneira híbrida, parte em software e parte em hardware, exigindo portanto o desenvolvimento de um IP soft core. |

**III. Descrição\***

|  |
| --- |
| O ataque do tipo DoS (Denial Of Service, em inglês), também conhecido como ataque de negação de serviço, é uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores. Esses ataques se tornam cada vez mais comuns, principalmente pelo surgimento de ataques do tipo DDoS(um tipo de ataque DoS de grandes dimensões), por isso, vale ressaltar a importância da detecção desse tipo de ataques. Tendo como principal objetivo detecção de ataques DDoS em tempo real, foi escolhido uma solução de detecção em hardware, pois soluções baseadas em software são ineficientes para aplicações de tempo real, uma vez que essas exigem grande quantidade de ciclos de CPU, utilizados em todo o software. Uma arquitetura de hardware dedicada para o módulo de detecção de ataque DDoS é considerada para implementação em FPGAs. Os recentes dispositivos FPGA oferecem alto desempenho e estão aptos a receber lógicas grandes e complexas. Além disso, os FPGAs oferecem adaptabilidade dinâmica, que é importante para aplicações que requerem mudanças freqüentes em suas configurações, como a detecção de ataques DDoS que evoluem com freqüência. No trabalho será utilizado, uma solução híbrida para detecção de ataques, para a implementação da variável de correlação proposta. Por isso, os módulos do pré-processador e do gerenciador de segurança são implementados separadamente usando software. As máquinas que implementam esses módulos e o FPGA podem se comunicar usando as interfaces de E/S de alta velocidade suportadas pelos FPGAs modernos, como PCeI e Gigabit Ethernet. O módulo de detecção de ataque recebe a instância de tráfego do módulo pré-processador. Além disso, ele recebe o perfil normal e um valor limiar do banco de dados do perfil criado pelo gerenciador de segurança. Cada uma das instâncias de tráfego e o perfil normal são vetores que consistem em três recursos de tráfego. O módulo de detecção de ataque calcula primeiro o NaHiD VERC (variável de correlação) entre a instância de tráfego de entrada e o perfil normal. O valor de correlação calculado é comparado com o limite para classificar a ocorrência de tráfego recebido como ataque ou normal. O resultado da classificação é armazenado no banco de dados Log para análise off-line pelo gerenciador de segurança. Além disso, um alarme é gerado no caso de a instância ser classificada como um ataque. Em nível de arquitetura, para separar controle e computação, a unidade de controle e o datapath são desenvolvidos separadamente. No entanto, eles são tão intrinsecamente dependentes. O datapath consiste nos operadores para oscálculos, e os registros para armazenar as entradas e os resultados da computação intermediária. A unidade de controle envia os sinais de seleção do multiplexador usados ​​pelas operações e os registros para selecionar a entrada. Eles são as principais partes do módulo da FPGA para a detecção, porém existem outros elementos que vão ser de suma importância para realizar operações complexas e necessárias. |

**IV. Metodologia\***

|  |
| --- |
| A metodologia deste projeto engloba os seguintes passos: i) Revisão bibliográficaii) Realização de experimentos em software iii) Realização de experimentos e hardware ( utilizando FPGA) iv) Estudo de caso de todas as etapas anteriores. O acompanhamento do trabalho será realizado semanalmente atraveś de reuniões com o professor orientador e ferramentas de gerenciamento de versões e atividades. |

**V. Recursos Necessários**

|  |
| --- |
| Para realização das tarefas citadas, será necessária a utilização dos recursos do laboratório LESC, através da utilização de softwares para a realização dos experimentos. Além disso, serão utilizados FPGA’s. Todos esses recursos estão disponíveis no LESC para a execução deste trabalho. |

\*Não há limite para o número de linhas.

* + 1. Fortaleza, 12 de Julho de 2017
    2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Aluno

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Prof. Orientador

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Visto do Chefe do Departamento

Aprovado pela Coordenação do Curso em / /

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Coordenador do Curso de Graduação

Procedimentos e instruções:

1. Orientador encaminha a proposta à Coordenação do Curso com um visto do Chefe do Departamento ao qual ele pertence;
2. Após aprovação na Coordenação, o Coordenador envia a demanda de turmas, sob a responsabilidade dos Orientadores, ao Departamento de Engenharia de Teleinformática;
3. Não haverá mais que uma turma por Orientador, cada uma com no máximo cinco alunos.
4. Cada turma por Orientador pode ter mais de um tema de projeto.