UNIVERSIDADE FEDERAL DO PARÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO
GRUPO DE PESQUISA EM REDES DE COMPUTADORES E COMUNICAÇÃO MULTIMÍDIA

Análise de Soluções de Segurança para Redes Definidas por Software no Kubernetes

Aluno: Victor Dias Leite
Orientador: Prof. Dr. Antônio Jorge Gomes Abelém

Apoio:

Agenda

- Introdução;
- Projeto OpenRAN Brasil;
- Proposta;
- Trabalhos Relacionados;
- Resultados Esperados;
- Próximos passo;
- Conclusão.

GERCOM
Research Group on Computer Networks and Multimedia Communication
UFPA - Brazil

Introdução

- A SDN tem várias vantagens em relação às abordagens tradicionais de gerenciamento de redes oferecendo muitos benefícios, principalmente em flexibilidade, escalabilidade e eficiência;
- Quando utilizada em um ambiente Kubernetes, podemos virtualizar redes inteiras e fornecer uma solução mais dinâmica e adaptável para a criação de infraestruturas de rede;
- Com o aumento da adoção de SDN e Kubernetes, é importante entender os riscos e ameaças associados a essas tecnologias e como podemos mitigá-los;

Projeto OpenRAN Brasil

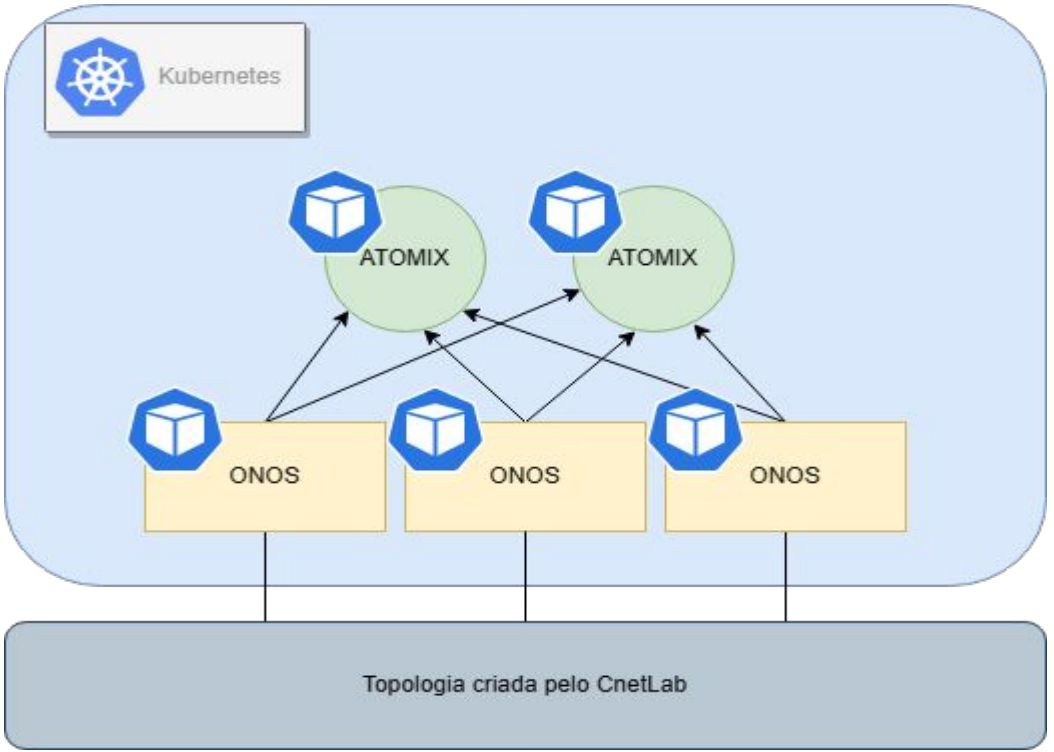
- Com o estudo e utilização do controlador SDN ONOS no Kubernetes para utilização em diferentes domínios do projeto, notou-se a necessidade entender os riscos e ameaças associados a essas tecnologias e como podemos mitigá-los;
- O gerenciamento inadequado dessas redes pode expor organizações a uma variedade de ameaças, incluindo ataques de negação de serviço, invasões de rede, roubo de dados e muitas outras.

Proposta

- Investigar os principais riscos e ameaças de segurança em ambientes de redes SDN virtualizadas em contêineres orquestrados com a plataforma Kubernetes;
- Pesquisar as principais ferramentas e técnicas utilizadas para mitigar essas ameaças;
- Realizar a exploração das implicações de compliance e governança que envolvem a segurança em ambientes SDN no Kubernetes;
- Apresentar um estudo de caso, a partir de uma análise de vulnerabilidades de um cenário proposto.

Proposta

- Cenário proposto:

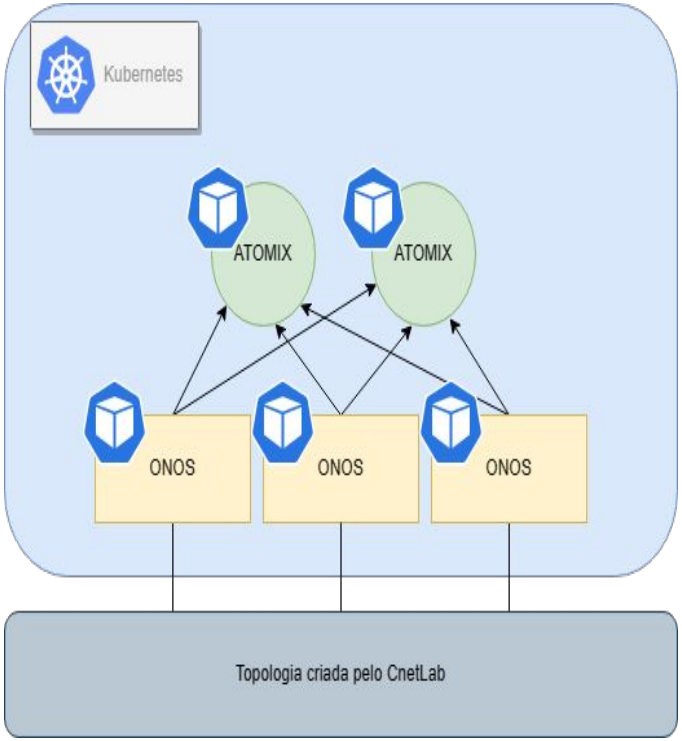


Proposta

- Principais ataques presentes em SDN:

Ataque	Camada alvo da SDN	Aspectos de segurança afetados		
		Disponibilidade	Confidencialidade	Integridade
DDoS/DoS	**Controle, Dados**	**X**		
Controlador sequestrado	**Controle, Dados e App**	**X**	**X**	**X**
Apps Maliciosos	**App**		**X**	**X**
MitM	**Controle, Dados e link entre Controle-Dados**		**X**	**X**
Buraco Negro	**Controle, Dados e link entre Controle-Dados**	**X**	**X**	
Espionagem	**Controle, Dados e App**		**X**	

Tabela: Esquematização dos tipos de ataque em SDN.

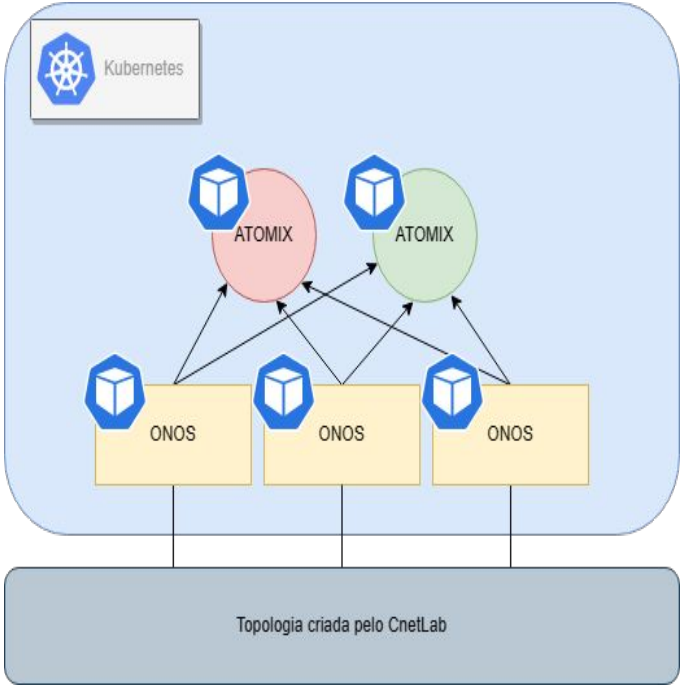


Proposta

- Exemplo de casos particulares do controlador ONOS:

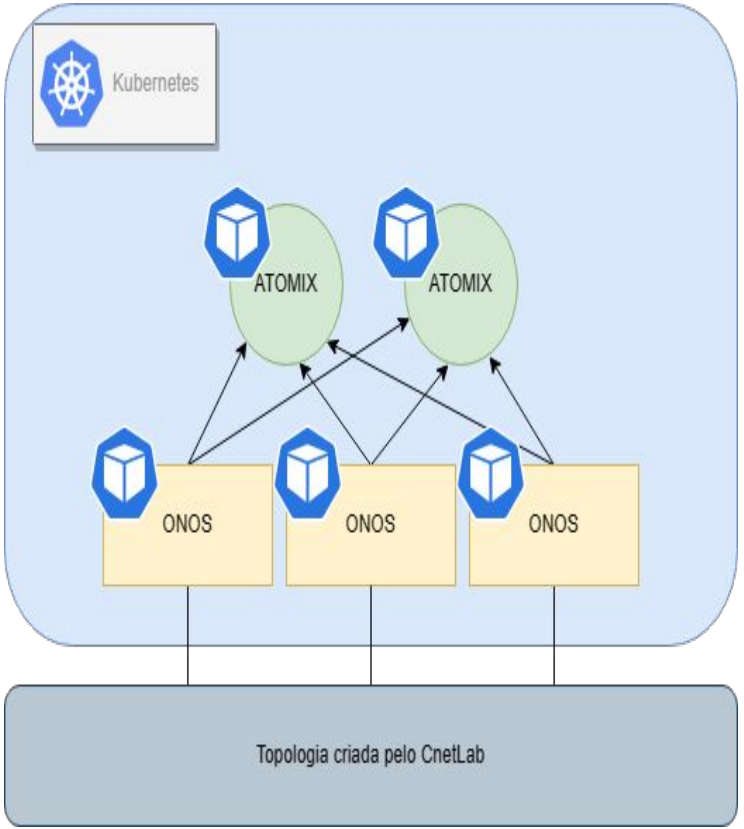
Nome	Descrição
CVE-2020-35215	O Atomix malicioso pode acessar e ler listas de primitivas usadas nos controladores ONOS.
CVE-2020-35214	Permite que um nó Atomix malicioso remova estados de armazenamento ONOS por meio do abuso de operações primitivas.
CVE-2020-35213	É um ataque negação de serviço (DoS) por meio de mensagens de evento falso enviadas para um nó mestre ONOS.

Tabela: Casos de vulnerabilidades e exposições comuns referente ao Atomix.



Proposta

- Utilização do Kubernetes:
  - Controlador ONOS está presente de forma nativa no Kubernetes;
  - Controle de acesso;
  - Possibilidade de criação de políticas e padrões de segurança;
  - Orquestração centralizada;
  - Automatização.



Trabalhos Relacionados

Título	Autores	Ano
SDN Security Review: Threat Taxonomy, Implications, and Open Challenges	Rahouti, Mohamed et. al.	2022
A Review of Solutions for SDN-Exclusive Security Issues	Spooner, Jakob et. al.	2016
ONOS Security and Performance Analysis (Report No. 2)	Secci, Stefano et. al.	2018
Security in Software Defined Networks: A Survey	Ahmad, Ijaz et. al.	2015
A Survey of Security in Software Defined Networks	Scott-Hayward, Sandra et. al.	2016
XI Commandments of Kubernetes Security: A Systematization of Knowledge Related to Kubernetes Security Practices	M. S. Islam Shamim et. al.	2020
Understanding the Security Implications of Kubernetes Networking	Minna, Francesco et. al.	2021
'Under-reported' Security Defects in Kubernetes Manifests	D. B. Bose et. al.	2021
Network Policies in Kubernetes: Performance Evaluation and Security Analysis	G. Budigiri et. al.	2021

Resultados Esperados

- Definir as melhores soluções de segurança para o ambiente SDN e o controlador ONOS;
- Definir as melhores soluções de segurança para o ambiente Kubernetes;
- Uma proposta que utilize em conjunto as automatizações de segurança possibilitadas pelo orquestrador Kubernetes e as melhores soluções de segurança em SDN;
- Contribuir com um padrão de implementação seguro para o *testbed* do projeto OpenRAN.

GERCOM
Research Group on Computer Networks and Multimedia Communication
UFPA - Brazil

Próximos passos

- Checar a viabilidade da proposta em outras áreas do projeto;
- Verificar o impacto na segurança da utilização de algumas ferramentas de automatização no cluster:
  - EMCO;
  - Nephio.

GERCOM
Research Group on Computer Networks and Multimedia Communication
UFPA - Brazil

Obrigado!

GERCOM
Research Group on Computer Networks and Multimedia Communication
UFPA - Brazil