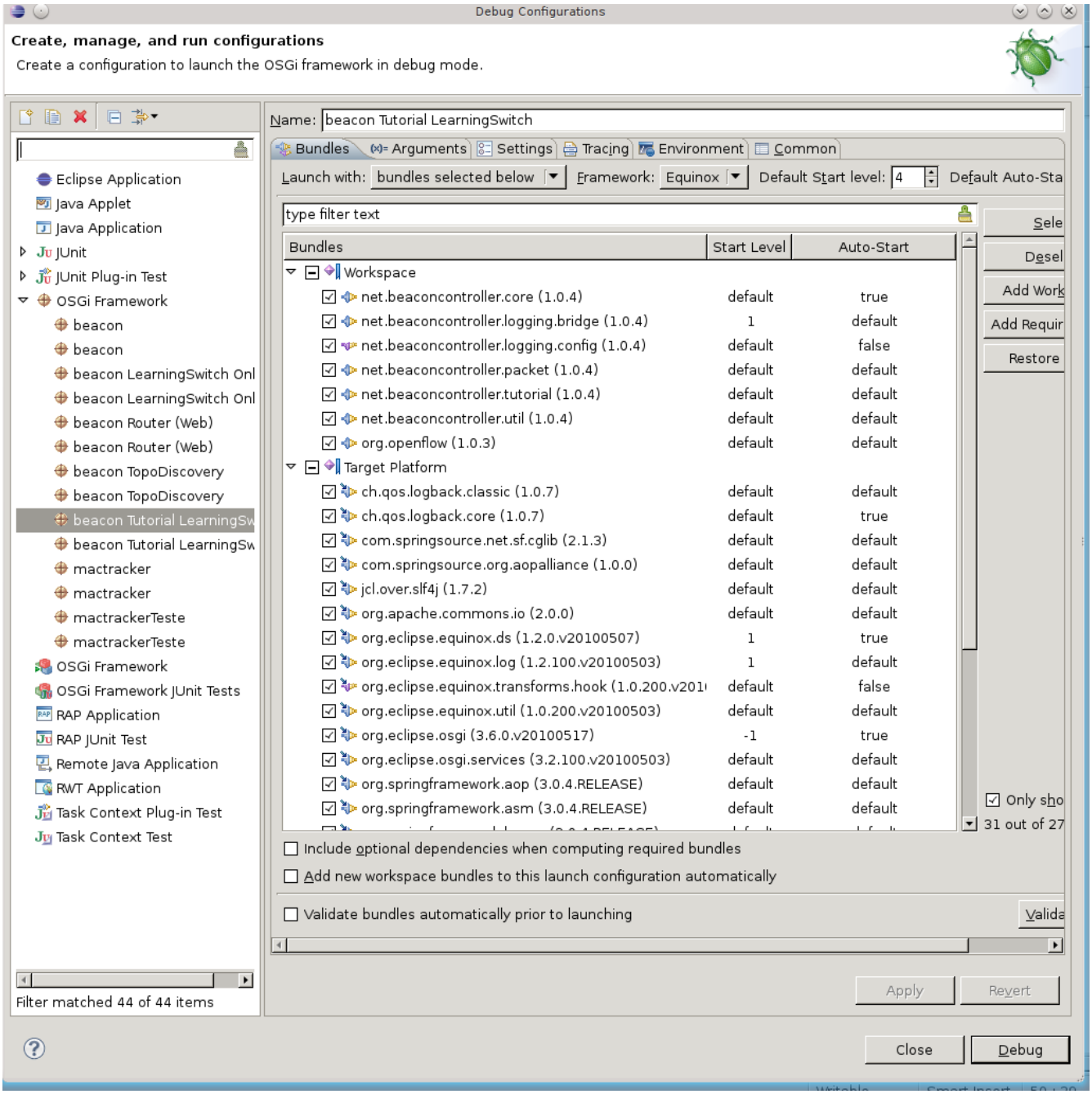
Of-IDPS

Passos para a execução do Of-IDPS:

1. Iniciar o controlador utilizando o *Eclipse/Run/DebugConfigurations*. Escolha "*beacon Tutorial LearningSwitch*" e clique em *debug*. Depois de iniciado o controlador escutará a porta 6633, tome cuidado para não ligar mais de um controlador ao mesmo tempo! Caso isso ocorra vai ocorrer um erro dizendo que a porta já está sendo utilizada, esse erro é bem comum. Caso o erro ocorra utilize o comando `netstat -a --tcp -np | grep 6633` para descobrir o processo da porta em execução e o comando `kill` para liberar a porta e execute o controlador novamente.



2. Iniciar a execução da máquina virtual com o mininet:
   a) Acessar via SSH a máquina virtual com o mininet. IP 192.168.1.200 usuário *mininet* senha *mininet*. O controlador deverá ter o IP 192.168.1.113. Comando:

      ```
      $ ssh -Y mininet@192.168.1.200
      ```

   b) Dentro da máquina virtual via SSH iniciar o ambiente que irá simular. O controlador deve ter o IP 192.168.1.113:

      ```
      $ sudo mn –custom \
      /home/mininet/mininet/custom/cenarioTesteLAN-WAN.py
      ```

3. No controlador: monte uma pasta entre o controlador e o computador com a mininet para compartilhar as mensagens geradas pelo IDS:

   ```
   $ sshfs mininet@192.168.1.200:/var/log/snort/ \
   /mnt/armazem/openflow/tmp/alertas/
   ```

4. Inicie o script que processa os alertas gerados pelo IDS na pasta compartilhada no passo 3. Acesse o diretório onde estão os arquivos de alerta que serão processados pelo controlador. Comando:

   ```
   $ cd /mnt/armazem/openflow/tmp/dadosSwitchesOF/
   ```
   Se desejado apague o arquivo existente:

   ```
   $ rm formatted_log.csv
   ```

   Então execute o script que ira a partir dos logs do snort gerar as mensagens de alerta no padrão que o controlador Of-IDPS reconhece com o comando:

   ```
   $ python snort_fast_alert_processor.py
   ```

   Observação 1 – Para executar o passo 4 é necessário que o passo 3 seja realizado com sucesso e que exista o arquivo `/mnt/armazem/openflow/tmp/alertas/alert.fast` que será processado pelo script do passo 4. Por fim, para que o controlador comece a processar os alertas é necessário que o passo 4 gere o arquivo `/mnt/armazem/openflow/tmp/dadosSwitchesOF/formatted_log.csv` que será consumido pelo software Of-IDPS do controlador. O script que automatiza o teste demora uns 5 segundos para iniciar justamente para dar tempo de executar o passo 3, então assim que for executado o passo 2b espere uns 2 segundos e execute o passo 4.

   Observação 2 – As regras do IDS são enviadas para serem processadas pelo controlador através do script do passo 4. O Of-IDPS trabalha com o primeiro alerta que casar com o fluxo ganha, ou seja se temos primeiro um fluxo X com prioridade 3 que terá a sua largura de banda reduzida e depois um outro alerta para o mesmo fluxo X com prioridade 1 que será bloqueada o comportamento do Of-IDPS é aplicar a regra do primeiro e apenas do primeiro então esse fluxo X terá a sua largura de banda reduzida e não será bloqueado! Por isso, em testes pode ser

interessante apagar as regras já existentes para ver o comportamento do Of-IDPS com as regras novas que serão geradas

5. Ao final do teste os arquivos com os resultados dos testes (tcpdump) estarão na máquina virtual mininet no diretório `/var/log/tcpdump`. E os logs do Snort estão em `/var/log/snort`. Todo teste executado cria arquivos compostos com nomes relacionados a data/hora da execução, assim os arquivos de um teste não sobrepõem outros testes. Os arquivos de logs de execuções passadas no Snort ficam no diretório `/var/log/bkpSnort`.

Resumo:

controlador/eclipse – F11 – Já escolhido "*beacon Tutorial LearningSwitch*"

```
controlador$ ssh -Y mininet@192.168.1.200

mininet$ $ sudo mn –custom \
/home/mininet/mininet/custom/cenarioTesteLAN-WAN.py


*controlador$ sshfs mininet@192.168.1.200:/var/log/snort/ \
/mnt/armazem/openflow/tmp/alertas/

**controlador$ rm \
/mnt/armazem/openflow/tmp/dadosSwitchesOF/formatted_log.csv
**controlador$ python \
/mnt/armazem/openflow/tmp/dadosSwitchesOF/snort_fast_alert_processor.
py
```

* - Execute o comando sshfs só uma vez pois depois que o diretório estiver montado ele ficará montado até desligar a máquina ou de desmontagem. Como é uma montagem via SSH verifique que a conexão de rede esteja sempre ativa e em caso de dúvida "desmounte" e "mounte" novamente.

** - Deixe sempre um terminal pronto para fazer esses passos rapidamente após iniciar o comando `mn` no mininet.

Observação final: Para executar testes manuais comente a linha de teste automático no arquivo `/home/mininet/mininet/custom/cenarioTesteLAN-WAN.py` e retire o comentário da linha para teste manual. As instruções para isso estão comentadas no arquivo `/home/mininet/mininet/custom/cenarioTesteLAN-WAN.py`.